

Universidade Federal de Santa Catarina
Programa de Pós-Graduação em Engenharia de Produção

Uma Abordagem de Plano de Controle Para QoS Dinâmica em Fluxos de Voz nas Redes IP

Tese apresentada à Universidade Federal de Santa Catarina para obtenção do título de
Doutor em Engenharia de Produção.

Fernando Antonio Cerutti

Orientador: Prof. Paulo José de Freitas Filho, Dr. Eng.

Florianópolis, março de 2006.

Fernando Antonio Cerutti

Uma Abordagem de Plano de Controle Para QoS Dinâmica em Fluxos de Voz nas Redes IP

Esta tese foi julgada e aprovada para obtenção do título de Doutor em Engenharia de Produção no Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina.

Florianópolis, março de 2006.

Edson Pacheco Paladini, Dr.
Coordenador do Curso

Banca examinadora

Paulo Freitas Filho, Dr. Eng. – UFSC
Orientador

Luiz Fernando Jacintho Maia, Dr. – UFSC
Moderador

Tereza Cristina Melo de Brito Carvalho, Dra.-LARC-USP
Examinador Externo

Alexandre Moraes Ramos, Dr.- UNIVALI
Examinador Externo

Elizabeth Specialski, Dra. Eng.- ÚNICA
Membro

Mario Antonio Ribeiro Dantas, Ph.D.-INE-UFSC
Membro

Agradecimentos

Este trabalho, que estuda os melhores caminhos, não seria possível sem a ajuda de um grande número de pessoas, e de pessoas amigas dessas pessoas, que entre outras coisas, me incentivaram, mantiveram meu astral, aconselharam, riram, emprestaram livros, CDs, DVDs. Essas pessoas aceitaram CDs, DVDs, livros e fingiram aceitar conselhos. Elas também re-arranjaram minhas rotas, mostaram-me, enfim, que os caminhos são esses mesmos, e a caminhada também é importante para torná-los os melhores.

Gostaria de agradecer a todas elas, e em especial algumas:

Edison Melo, do comitê gestor da RNP, e NPD-UFSC, pela amizade, pelo exemplo profissional e pela revisão do conteúdo. Com a dedicação de um artesão, esse cara cuida das doses industriais de bytes que trafegam nos enlaces da rede acadêmica de Santa Catarina, enquanto projeta o futuro, traçando os caminhos.

Sidinei Rodrigo Basei, pela codificação do protótipo, e acompanhamento da fase experimental. A intimidade desse cara com a linguagem Java é algo surpreendente. O Sidnei não acredita em caminhos impossíveis.

Paulo Burin, pela implantação da base de dados, e cálculos dos valores das amostras. Reduziu nosso tempo de cálculo em aproximadamente 1000 vezes. O Paulão é um cara que vê todos os caminhos com serenidade.

Dra. Silvia Nassar, do Departamento de Informática e Estatística da UFSC, pela ajuda no uso da ferramenta estatística, análise dos resultados e revisão do conteúdo. E pela imensa paciência, que ajudou a frear minhas ansiedades com os dados, mostrando-me que os caminhos matemáticos são rudes, mas também são alentadores.

Dra. Maria Ines Castiñeira, pelo exemplo de ser humano, pela amizade e por revisar o conteúdo. A Ines, por ser uma espécie de alquimista da paz, parece não errar os caminhos, e por isso estar ao lado dela é estar no melhor caminho.

Dr. Mauro Madeira, coordenador dos cursos de Computação e Sistemas de Informação da UNISUL, pelo incentivo constante e revisão do conteúdo.

Dr. Paulo Freitas, meu orientador. Todos nós deveríamos perceber os caminhos como esse cara percebe.

Aos membros da banca, por aceitarem o convite, e contribuírem significativamente para a versão final desta tese.

Katia Juca, do NPD-UFSC, pela amizade e revisão do conteúdo.

Prof. **Daniel Cadorin** e aos caras do laboratório de redes da UNISUL.

Aos PCs 1,2,7,6,8 e 5 do meu ambiente de estudos. Eles ouviram xingamentos e elogios com a serenidade de quem precisava manter a razão quando tudo em volta tornava-se irracional.

Meus pais, **Avelino e Ilda Cerutti**, por terem me conduzido pelos primeiros caminhos. Esses caras foram demais (minha mãe continua sendo), e acreditaram sempre nos caminhos que escolhi quando comecei a usar minha própria tabela de rotas. Essa maneira de confiar só se poderia aprender com pessoas especiais.

Minha esposa **Claudete Schilling Mendonça**, pessoa feita de luz, para quem os caminhos não precisam existir, desde que ela tenha uma pequena chance de inventar algum.

Minhas filhas, **Jéssica e Luisa**, pela paciência, compreensão, afagos, amor e apoio incondicional. Quando eu comecei este projeto a Jéssica era uma criança, e a Luisa estava em caminhos imaginários.

Dedicatória

Luisa, Jéssica, Claudete e Ilda, as
mulheres que eu amo e com as quais eu aprendo.

Sumário

| | |
|--|-----|
| 1. Introdução | 1 |
| 1.1. Motivações e Origem do trabalho | 1 |
| 1.2. Definição do problema | 9 |
| 1.3. Proposta de solução | 15 |
| 1.4. Objetivos do trabalho de Pesquisa | 19 |
| 1.5. Relevância do trabalho de pesquisa | 20 |
| 1.6. Originalidade | 21 |
| 1.7. Contribuições | 23 |
| 1.8. Limitações e escopo | 26 |
| 1.9. Estrutura do trabalho | 28 |
| 2. O Cenário da Internet Atual e os Fluxos de Voz | 30 |
| 2.1. Tipos de tráfego | 31 |
| 2.2. Histórico da convergência | 34 |
| 2.3. Sistemas de comunicação digitais | 38 |
| 2.4. Sumário do Capítulo | 46 |
| 3. Qualidade de Serviço | 47 |
| 3.1. Histórico | 47 |
| 3.2. Definições de QoS | 48 |
| 3.3. Definições de serviços | 50 |
| 3.4. Métricas de QoS | 54 |
| 3.5. Disciplinas de filas | 66 |
| 3.6. Serviços Integrados | 73 |
| 3.8. Sumário do capítulo | 78 |
| 4. Roteamento IP baseado em QoS | 80 |
| 4.1. Algoritmos dos Protocolos IGP (Interior Gateway Protocol) | 80 |
| 4.2. Re-encaminhamento dos pacotes | 82 |
| 4.3. Técnicas de roteamento não convencionais | 83 |
| 4.4. Gerência de rotas | 83 |
| 4.5. Roteamento baseado em QoS | 85 |
| 4.6. Engenharia de Tráfego | 92 |
| 4.7. Re-roteamento (rerouting) | 98 |
| 4.8. Arquiteturas de QoS | 106 |
| 4.9. Sumário do Capítulo | 110 |
| 5. Plano de controle para QoS em fluxos de voz na Internet | 111 |
| 5.1. Introdução | 111 |
| 5.2. Definições | 115 |
| 5.3. Dinâmica do plano de controle | 118 |
| 5.4. Ambiente de estudos de laboratório | 119 |
| 5.5. Ferramenta de medição lperf | 122 |
| 5.6. Protótipo QoS-Path | 127 |
| 5.7. Sumário do capítulo | 127 |
| 6. Desempenho | 128 |
| 6.1. Considerações gerais sobre o problema | 129 |
| 6.2. Metodologia | 131 |
| 6.3. Obtenção de dados de desempenho de uma rede | 138 |
| 6.4. Análise do desempenho | 146 |
| 6.5. Projeto de experimentos | 148 |

| | | |
|------|---|-----|
| 6.6. | Ambientes de experimentação..... | 154 |
| 6.7. | Limitações da Experimentação | 157 |
| 6.8. | Análise de dados: ANOVA..... | 158 |
| 6.9. | Sumário do capítulo | 158 |
| 7. | Resultados | 159 |
| 7.1. | Ambiente 26,4 kbps - Jitter médio..... | 159 |
| 7.2. | Ambiente 26,4 kbps - Médias de Perdas | 172 |
| 7.3. | Ambiente 1 pps - Jitter médio | 184 |
| 7.4. | Ambiente 1 pps - média de perdas Perdas..... | 188 |
| 7.5. | Árvore de eventos para o Jitter média de perdas nos dois ambientes..... | 190 |
| 7.6. | Árvore de eventos para as médias de perdas nos dois ambientes..... | 191 |
| 7.7. | Conclusões do capítulo..... | 191 |
| 7.8. | Evidências das limitações dos experimentos..... | 194 |
| 8. | Conclusões | 195 |
| 8.1. | Sugestões de continuidade..... | 199 |
| | Referências Bibliográficas | 201 |
| | Apêndice 1 | 207 |
| | Apêndice 2 | 217 |

Lista de figuras

| | |
|---|------------|
| Figura 1-1 - Evolução de arquiteturas de rede | 5 |
| Figura 1-2 Exemplo de cenário multi-serviço possível com IP | 6 |
| Figura 1-3 - Capacidade das Fibras Ópticas | 7 |
| Figura 1-4 - Polarização combinada com WDM | 8 |
| Figura 1-5 Troca de caminhos em vários níveis. | 11 |
| Figura 1-6 - Estrutura de QoS fim-a-fim para grandes corporações | 14 |
| Figura 1-7 – Arquitetura de Políticas do IETF/DTMF | 16 |
| Figura 1-8 - Relações entre o modelo de referência e o plano de controle | 17 |
| Figura 1-9 - Componentes dos planos de controle e de dados | 17 |
| Figura 1-10 – Plano de controle para Roteamento através de Políticas para TE | 18 |
| Figura 1-11 - Estação de Gerência de Políticas (Controle/Sinalização) | 18 |
| Figura 2-1 - Tipos de tráfego na Internet | 31 |
| Figura 2-2 - Evolução das redes | 35 |
| Figura 2-3 - Diagrama de blocos para os sistemas de comunicação digitais | 38 |
| Figura 2-4 - Rede de voz sobre IP | 39 |
| Figura 2-5 - Arquitetura de Voz sobre rede IP – VoIP | 41 |
| Figura 2-6 - Empacotamento dos frames de voz no segmento UDP e datagrama IP | 41 |
| Figura 2-7 - Empacotamento G.711+RTP/UDP/IP+Ethernet | 43 |
| Figura 2-8 - Cabeçalhos RTP comprimidos. | 43 |
| Figura 2-9 - Compressão e enfileiramento dos pacotes RTP | 43 |
| Figura 3-1- Diagrama de interações dos conceitos de QoS - Usuário e rede | 49 |
| Figura 3-2 - Linha de tempo para o atraso nos serviços de voz | 53 |
| Figura 3-3 - TIPHON – Parâmetros de QoS | 53 |
| Figura 3-4 - Estruturas e tecnologias auxiliares para prover QoS em redes IP | 54 |
| Figura 3-5 - Atraso em redes de pacotes | 57 |
| Figura 3-6 - buffers para evitar diferenças de atrasos (jitter) | 58 |
| Figura 3-7 - Relação entre o atraso e as perdas de pacotes em um buffer de jitter | 58 |
| Figura 3-8 - Atraso de enfileiramento | 60 |
| Figura 3-9 - Efeito do Jitter na percepção da fala | 61 |
| Figura 3-11 -Método de cálculo do jitter segundo RFC 1889 | 64 |
| Figura 3-12 - Sistemas de filas nas interfaces: Software e Hardware | 66 |
| Figura 3-13 - Bypass da fila de software | 67 |
| Figura 3-14 - Componentes de uma fila (classificação, inserção, escalonamento) | 68 |
| Figura 3-15 - Weighted Fair Queue | 69 |
| Figura 3-16 – WRED | 71 |
| Figura 3-17 - Priority Queue | 72 |
| Figura 3-18 – Fluxograma para classificação dos pacotes nas filas PQ | 73 |
| Figura 3-21 - Sinalização RSVP | 75 |
| Figura 4-1 - Tabela de distâncias do Roteador E até os demais, usando algoritmo de vetor de distâncias | 81 |
| Figura 4-2 – Re-encaminhamento convencional de pacotes pelo IP | 82 |
| Figura 4-3 - Processo de Engenharia de tráfego | 93 |
| Figura 4-4 - Problema do peixe | 97 |
| Figura 4-5 - Arquitetura da gerência baseada em políticas (PBM) | 109 |
| Figura 5-1 - Planos necessários nas redes de próxima geração | 111 |
| Figura 5-2 Gerência de mecanismos de VoIP | 112 |
| Figura 5-3 - Estado dos enlaces (banda, atraso, custo) de uma topologia de rede | 114 |
| Figura 5-4 -Enlaces e fluxos de medição do plano de controle | 117 |
| Figura 5-5 - Plano de controle e as camadas do modelo OSI | 117 |
| Figura 5-6 - Dinâmica do plano de controle | 119 |
| Figura 5-7 -Ambiente de estudos - Laboratório | 120 |
| Figura 5-8 - Blocos básicos para a topologia dos roteadores. | 121 |
| Figura 5-9 -Conexão back-to-back com cabos V-35 | 122 |
| Figura 5-10 - Ambiente de estudos com o plano de controle | 122 |
| Figura 5-11 – Classificação das ferramentas para avaliação de desempenho TCP/IP | 123 |
| Figura 5-12- Uso da ferramenta Iperf | 124 |
| Figura 5-13 - Probs para medição das métricas nos enlaces - Fluxos de medição | 125 |
| Figura 5-14 - Sentido dos fluxos de medição da qualidade do enlace | 125 |

| | |
|--|------------|
| Figura 5-15 - Modelo para os experimentos | 126 |
| Figura 6-1 - Modelo de Desempenho de sistema computacional | 128 |
| Figura 6-2 - Correlação de pacotes perdidos | 135 |
| Figura 6-3 - Medidas de desempenho agregadas e de serviços (fim a fim) | 139 |
| Figura 6-4 - Cenário de teste para determinação de QoS no núcleo da rede | 142 |
| Figura 6-5 Pilha de protocolos nas medições no nível da camada de aplicação | 143 |
| Figura 6-6 - estrutura de um pacote de medição – Fonte: TIPHON, 2002 | 143 |
| Figura 6-7- Identificação dos enlaces e dos fluxos de voz (I2, I6, I8) a serem preservados | 148 |
| Figura 6-8 -Fluxos competidores pelos recursos (fatores J57 e J76) | 152 |
| Figura 6-9 -Ambientes de amostragem | 154 |
| Figura 6-10 - Diagrama dos fatores do ambiente 26,4 kbps | 155 |
| Figura 6-11 - Ambiente 1 pps e os fatores analisados | 156 |
| Figura 7-1 - Efeitos dos fatores sobre o Jitter no ambiente 26,4 kbps | 162 |
| Figura 7-2 - Jitter médio em relação aos cenários | 162 |
| Figura 7-3 - Jitter médio em relação aos tamanhos dos pacotes dos fluxos de voz | 164 |
| Figura 7-4 - Jitter médio em relação aos tamanhos dos pacotes dos fluxos de medição | 165 |
| Figura 7-5 - Jitter médio em relação a disciplina de filas | 167 |
| Figura 7-6 - Jitter médio em relação ao destino | 167 |
| Figura 7-7 - Rotas preferenciais do protocolo OSPF | 168 |
| Figura 7-8 - Relações entre os destinos e os fluxos competidores | 169 |
| Figura 7-9 - Jitter médio em relação aos fluxos competidores | 169 |
| Figura 7-10 - Arvore de eventos para variável jitter -ambiente 26,4 kbps | 171 |
| Figura 7-11 - Efeitos nas perdas – Ambiente 26,4 kbps | 173 |
| Figura 7-12 - Perdas médias em relação aos protocolos | 174 |
| Figura 7-13 - Trocas consecutivas de caminhos no cenário b2, até a estabilização abaixo do limiar de 1% | 176 |
| Figura 7-14 - Perdas médias em relação ao tamanho dos pacotes | 176 |
| Figura 7-15 - Perdas médias em relação aos fluxos de medição | 177 |
| Figura 7-16 -Perdas médias em relação às políticas de fila | 178 |
| Figura 7-17 - Perdas médias em relação a disciplina de filas e tamanho do pacote no fluxo de medição. | 179 |
| Figura 7-18 - Perdas médias em relação aos destinos | 180 |
| Figura 7-19 Média de perdas e as influências do destino e fluxos competidores | 181 |
| Figura 7-20 - Perdas médias em relação aos fluxos competidores | 181 |
| Figura 7-21 -Perdas em relação aos cenários, destinos e fluxos competidores | 182 |
| Figura 7-22 - árvore de eventos para PERDAS no ambiente 26,4 kbps | 183 |
| Figura 7-23 -Efeito dos fatores sobre o Jitter médio - Ambiente 1 pps | 184 |
| Figura 7-24 - Jitter médio em relação aos protocolos | 185 |
| Figura 7-25 - trocas sucessivas de rotas | 186 |
| Figura 7-26 - Arvore de eventos para variável jitter - ambiente 1 pps | 187 |
| Figura 7-27 - Média de perdas em relação aos cenários | 189 |
| Figura 7-28 - Árvore de eventos - Jitter para os dois ambientes | 190 |
| Figura 7-29 - Árvore de eventos - Perdas para os dois ambientes | 191 |
| Figura 7-30 - Medianas para o jitter em relação aos cenários | 194 |

Lista de Quadros

| | |
|---|------------|
| Quadro 1-1 - Campo ToS no OSPF | 12 |
| Quadro 2-1 Suscetibilidade das aplicações em relação as métricas clássicas (considerando-se a confiabilidade como um reflexo das perdas) de QoS. | 32 |
| Quadro 2-2- Padrões de CODEC do ITU-T | 40 |
| Quadro 2-3 Taxa necessária para encapsular fluxos de voz em frames ethernet | 44 |
| Quadro 2-4 - Calculo da banda necessária para os diferentes CODECs | 45 |
| Quadro 3-1 Classes de atrasos para os serviços de Internet | 51 |
| Quadro 3-2 - Classes de QoS e as aplicações | 51 |
| Quadro 3-3 Tipos de serviços mais comuns atualmente na Internet | 52 |
| Quadro 3-4 Referência para degradação da rede de transporte | 62 |
| Quadro 4-1 Técnicas de roteamento não convencionais | 84 |
| Quadro 4-2-Comparação entre métodos de sinalização RSVP-TE e CR-LDP | 104 |
| Quadro 4-3 Propostas de métodos para Re-Rotamento | 107 |
| Quadro 5-1 - exemplo de tabela da QNS com as métricas de QoS | 115 |
| Quadro 5-2 Dispositivos de rede do ambiente de estudos | 121 |
| Quadro 5-3 Microcomputadores Pentium 4 - SO Fedora Core 3 | 121 |
| Quadro 6-1 - Passos para avaliação de desempenho | 131 |
| Quadro 6-2- Serviços e resultados esperados na avaliação de desempenho | 133 |
| Quadro 6-3 RFCs e métricas IPPM | 134 |
| Quadro 6-4 Níveis de monitoração e características medidas em uma rede. | 138 |
| Quadro 6-5 Relações entre as características e os objetos medidos | 141 |
| Quadro 6-6 - Campos de informação nos pacotes de medição. | 144 |
| Quadro 6-7 Exemplo de atributos para função ServicePolicyRule (IBM QoS Server) | 147 |
| Quadro 6-8 - Exemplo de atributos para função ServiceCategory (IBM QoS Server) | 147 |
| Quadro 6-9 - Fluxos de entrada e saída nas interfaces dos PCs utilizados no plano de controle | 149 |
| Quadro 6-10 -Algoritmo de disparo do gatilho para alteração dos caminhos | 151 |
| Quadro 7-1 relações entre variáveis da “equação do jitter” e os fatores experimentais usados neste trabalho de pesquisa | 160 |

Lista de Tabelas

| | |
|---|-----|
| <i>Tabela 5-1 - Saída para a estação servidora (30.0.0.1) do Iperf.</i> | 126 |
| <i>Tabela 7-1 - Valores de F e P para teste ANOVA - Ambiente 26,4 kbps - variável: jitter</i> | 160 |
| <i>Tabela 7-2 Estimativa dos efeitos para Jitter Médio- valores de P e teste t - Ambiente 26,4 kbps</i> | 161 |
| <i>Tabela 7-3 - jitter médio em relação às disciplinas de filas</i> | 163 |
| <i>Tabela 7-4 Jitter médio para os tamanhos dos pacotes dos fluxos de voz</i> | 164 |
| <i>Tabela 7-5 Jitter médio para os tamanhos dos pacotes dos fluxos de medição</i> | 165 |
| <i>Tabela 7-6 - jitter médio em relação às disciplinas de filas</i> | 166 |
| <i>Tabela 7-7 - jitter médio em relação ao destino do fluxo de voz</i> | 168 |
| <i>Tabela 7-8 - jitter médio em relação ao fluxo competidor – ambiente 26,4 kbps</i> | 170 |
| <i>Tabela 7-9 Jitter médio em relação aos fluxos competidores – ambiente 1 pps</i> | 170 |
| <i>Tabela 7-10 - Estimativa dos efeitos para média de perdas</i> | 172 |
| <i>Tabela 7-11 – Média de Perdas em relação ao cenário</i> | 175 |
| <i>Tabela 7-12 – Média de perdas em relação ao tamanho dos pacotes dos fluxos de voz</i> | 177 |
| <i>Tabela 7-13 – Média de perdas em relação ao tamanho dos pacotes dos fluxos de medição</i> | 178 |
| <i>Tabela 7-14 – Média de perdas em relação às políticas de filas</i> | 178 |
| <i>Tabela 7-15 – Média de perdas em relação aos destinos dos fluxos de voz</i> | 180 |
| <i>Tabela 7-16 – Média de perdas em relação aos fluxos competidores pelos recursos</i> | 182 |
| <i>Tabela 7-17 - Efeitos dos fatores no Jitter médio - Ambiente 1 pps</i> | 184 |
| <i>Tabela 7-18 - Jitter médio para os cenários a1, b1 e b2</i> | 186 |
| <i>Tabela 7-19 - Efeitos dos fatores nas médias de perdas - Ambiente 1 pps</i> | 188 |
| <i>Tabela 7-20 – Média de perdas em relação aos cenários</i> | 189 |

LISTA DE SIGLAS

| | |
|----------|--|
| 3GPP | -Third Generation Partnership Project |
| ADPCM | -Adaptive Differential Pulse Code Modulation |
| AS | -Autonomous System |
| ASON | - Automatically Switched Optical Networks |
| ATM | -Asynchronous Transfer Mode |
| CAC | -Connection Admission Control |
| CAPEX | -Capital Expenditures |
| CBQ | -Class Based Queue |
| CBR | -Constraint Based Restrictions |
| CIM | -Common Information Model |
| CLI | -Command Line Interface |
| CODEC | -Codify-Decodify |
| COPS | -Common Open Policy Services |
| CPU | -Central Processor Unit |
| cRTP | -Compressed Real Time Protocol |
| DAST | -Distributed Application Support Team |
| DiffServ | -Differentiated Services |
| DWDM | -Dense Wavelength Division Multiplexing |
| EGP | -External Gateway Protocol |
| ETSI | -European Telecommunications Standards Institute |
| FEC | -Forwarding Equivalence Classes |
| FIFO | -First In First Out |
| FTP | -File Transfer Protocol |
| GMPLS | -Generalized Multi Protocol Label Switching |
| HTTP | -Hyper Text Transfer Protocol |
| HW | -Hardware |
| ICMP | -Internet Control Message Protocol |
| IEEE | -Institute of Electrical and Electronics Engineers |
| IETF | -Internet Engineering Task Force |
| IGP | -Internal Gateway Protocol |
| IN | -Intelligence Networks |
| IntServ | -Integrated Services |
| IP | -Internet Protocol |
| IPDV | -Internet Protocol Delay Variation |
| IPPM | -Internet Protocol Performance Measurements |
| IPSEC | -IP security |
| IpvX | -Internet Protocol version X |
| IS-IS | -Intermediate System to Intermediate System |
| ISA | -Integrated Services Architecture |
| ISP | -Internet Service Provider |
| ITU-T | -International Telecommunications Union-Telecommunications section |
| LAN | -Local Area Network |
| LDAP | -Lightweight Directory Access Protocol |
| LDP | -Label Distribution Protocol |
| LMP | -Link Management Protocol |
| LPC | -Linear Predictive Coding |
| LS | -Link State |
| LSP | -Label Switched Path |
| MOS | -Mean Opinion Score |
| MPC | -Multi Path Constrained |
| MPLS | -Multi Protocol Layer Switch |
| MTU | - Maximum Transfer Unit |
| NAT | -Network Address Translation |
| NNI | -Network Node Interface |
| OPEX | -Operational Expenditures |
| OSI | -Open System Interconnection |
| OSPF | -Open Shortest Path First |
| PBM | -Policy Based Management |

| | |
|--------|---|
| PC | –Personal Computer |
| PCM | –Pulse Code Modulation |
| PCPO | –Path Constrained Path Otimization |
| PDP | –Policy Decision Point |
| PDU | –Protocol Data Units |
| PDV | –Packet Delay Variation |
| PEP | –Policy Enforcement Point |
| PIB | –Policy Information Base |
| PNNI | –Private Network – Network Interface |
| POTS | –Public Open Telephony Service |
| PPP | –Point to Point Protocol |
| PQ | –Priority Queue |
| QNS | –QoS Network Server |
| QoS | –Quality of Service |
| RED | –Random Early Detection |
| RFC | –Request for Comments |
| RIP | –Routing Information Protocol |
| RSVP | –Resource Reservation Protocol |
| RTP | –Real Time Protocol |
| RTT | –Round Trip Time |
| SDH | –Synchronous Digital Hierarchy |
| SDP | –Session Description Protocol |
| SGBD | –Sistema Gerenciador de Base de Dados |
| SIP | –Session Initiation Protocol |
| SLA | –Service Level Agreement |
| SLS | –Service Level Specifications |
| SMTP | –Simple Mail Transfer Protocol |
| SNMP | –Simple Network Management |
| SPF | –Shortest Path First |
| SQL | –Structured Query Language |
| SSH | –Secure Shell |
| TCP/IP | –Transfer Control Protocol / Internet Protocol |
| TE | –Traffic Engineering |
| TDM | –Time Division Multiplexing |
| TIPHON | –Telecommunications and Internet Protocol Harmonization Over Networks |
| ToS | –Type of Services |
| TxQ | –Transmission Queue |
| UDP | –User Datagram Protocol |
| UNI | –User Network Interface |
| VAD | –Voice Activity Detection |
| VoIP | –Voice over Internet Protocol |
| VPN | –Virtual Private Networks |
| VTC | –Vehicular Technology Conference |
| WAN | –Wide Area Network |
| WDM | –Wavelength Division Multiplexing |
| WFQ | –Weighted Fair Queue |
| WRED | –Weighted Random Early Detection |

Resumo

Com a convergência das redes de dados e de voz/vídeo para transporte através do TCP/IP, várias necessidades apontam para as redes de nova geração, capazes de atender à diversidade dos serviços, mantendo a qualidade. Este trabalho de pesquisa propõe um plano de sinalização dinâmica, que monitora a condição dos enlaces fim-a-fim e adapta as rotas de forma a manter a QoS dentro de parâmetros desejáveis de *jitter* e *perdas* aos fluxos de voz. A proposta possui a vantagem de se adaptar às condições do tráfego, rearranjando os caminhos com base em métricas dinâmicas, sem aumentar a carga nos roteadores, usando os recursos de estações de sinalização. O plano de controle foi testado experimentalmente sob condições variadas de tráfego, e a proposta se mostrou efetiva para as condições analisadas.

Palavras-Chaves: Engenharia de tráfego, re-roteamento, roteamento baseado em QoS, desempenho de redes IP, convergência, medições de *jitter* e perdas de pacotes.

Abstract

With data and voice/video networks converging to TCP/IP transport, a large number of tasks are pointing out to next generation networks. These networks may be capable to supply a wide range of services, while they sustain the quality requirements. This study proposes a dynamic control plane, which monitors end-to-end link state, re-routing the voice streams to maintain the QoS levels of *jitter* and packet loss. This proposition has the main advantage of adapting network to best paths, based on dynamic metrics, without routers overloads. The proposed control plane was tested under a range of traffic conditions, and shows to be effective for the traffic conditions presented.

Key-words: Traffic Engineering, rerouting, QoS routing, IP Performance, converging networks, jitter and packet loss measurements

1. Introdução

Neste capítulo são apresentadas as motivações que deram origem a este trabalho, bem como o contexto onde a pesquisa está inserida. São levantados os problemas abordados, mostrando a proposta para solucioná-los. São esclarecidos os objetivos da pesquisa e se procurará mostrar a relevância e a originalidade do trabalho. Por fim, se resumem as principais contribuições que o trabalho de pesquisa pretende deixar, bem como as limitações e o escopo. O capítulo termina com uma descrição da estrutura geral de todo o trabalho, incluindo os conteúdos que serão abordados em cada capítulo.

1.1. *Motivações e Origem do trabalho*

A motivação para este trabalho reside na necessidade de mecanismos dinâmicos para estabelecimento e manutenção dos fluxos de voz com Qualidade de Serviço - QoS em redes IP. Neste trabalho de pesquisa será utilizada prioritariamente a sigla em inglês (QoS – *Quality of Service*) para designar Qualidade de Serviço. A sigla é normalmente usada pela comunidade científica. Tais necessidades são crescentes, uma vez que as aplicações consomem recursos cada vez maiores, e os fluxos de voz necessitam de garantias mínimas de qualidade por parte da rede. Sabe-se que os tráfegos de Internet não são previsíveis como o são os tráfegos de voz. As abordagens clássicas para estabelecimentos de caminhos baseados em métricas estáticas (protocolos IGP/EGP) têm se mostrado gradativamente mais insuficientes, uma vez que tais protocolos são baseados sempre na escolha do menor caminho, enquanto outras métricas que podem indicar disponibilidade dos recursos (atraso, perdas, vazão) são ignoradas (Alwayn, V. , 2002). Os roteadores são compartilhados por pacotes de fontes diversas, que possuem diversos perfis de necessidades. Quando ignoradas, essas necessidades geram atrasos imprevisíveis nos pacotes.

A infraesrutura necessária para as redes de próxima geração deve ser baseada em flexibilidade e na habilidade de reagir às demandas dinâmicas (Iovana, P.; Sabela, R. & Settembre, M., 2003). Essas redes devem possuir um plano de controle, associado a um

plano de transporte e um plano de gerência, por determinação dos principais organismos de padronização das redes de comunicações (IETF e ITU-T) (Jajszczyk, A. & Rozycki, P., 2006).

Tal plano de controle basicamente deve ser responsável pela conexão e gerência dos recursos. Definido como um plano baseado no IP, pode ser associado ou separado da rede de transporte.

Existe um consenso, nos meios acadêmicos e entre os principais fabricantes de equipamentos de rede, de que a Internet está se transformando em um meio multi-serviços, suportando a convergência de voz, vídeo e comunicação de dados (Shand, M. & Bryant, S., 2006), (Alwayn, V. , 2002), (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005), (Choudhury, D., 2001), (Park, K. I., 2005). O tráfego na Internet está crescendo em progressão geométrica (Weiser, M., 2001). Embora o mercado de longo prazo na Internet seja de difícil previsão, um fator permanece constante: o crescimento.

O modelo original de roteamento do protocolo IP contempla os fluxos tradicionais de dados, para os quais foi projetado, mas não é eficiente para as novas demandas, notadamente fluxos de voz e vídeo (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998). Até este momento, os grandes provedores de Internet responderam ao desafio do crescimento através da implantação de três iniciativas complementares (Alwayn, V. , 2002) :

1. Arquiteturas de redes escaláveis;
2. Expansão da capacidade;
3. Engenharia de tráfego.

As duas primeiras iniciativas são mais fáceis de implementar, e os grandes provedores Internet têm expandido sua arquitetura e capacidade. A terceira questão envolve problemas lógicos de configuração e implementação de políticas, que devem ser baseadas em medições e levantamentos estatísticos. Alguns projetos mundiais buscam fornecer subsídios para essas medidas, trazendo aplicação automática de caminhos e bandas para provimento de QoS, partindo do estado atual da rede e dos requisitos das aplicações. Exemplos de tais projetos podem ser <http://www.caida.org>, voltada para o desempenho e os grupos de trabalho da Internet2, e a própria Internet 2, <http://www.internet2.edu/working-groups.html> buscando tecnologias para suprir as novas demandas, originadas pelo “uso agressivo” das aplicações avançadas. No Brasil,

a RNP – Rede Nacional de Pesquisas – patrocina o GT-MED, (Grupo de Trabalho de Medições), responsável pelos levantamentos para caracterização do tráfego acadêmico e governamental.

Este trabalho de pesquisa pode ser enquadrado na terceira iniciativa, Engenharia de tráfego, através de técnicas de re-roteamento.

Historicamente, o sobre-provisionamento de banda tem sido a solução adotada pelos provedores de Internet para suprir as carências do roteamento pelo melhor esforço (Nelakuditi, S. Zhang, Z.; Tsang, R. P. & Du, D. H. C., 2002). Quando os recursos não podem ser aumentados, pois aumentam as despesas de capital, as aplicações devem adaptar-se ou os recursos devem garantir o desempenho melhor para certas aplicações. Essa última solução é conhecida como qualidade de serviço, ou QoS (Roy, A., 2001). Notadamente a solução de prover QoS aumenta os custos operacionais, pela elevação da complexidade.

Deve-se perceber que, na competição pelo mercado, os provedores de serviço Internet (ISPs, ou *Internet Service Providers*) precisam considerar os custos de capital e os operacionais. Tais fatores são denominados CAPEX (Capital Expenditures) e OPEX (Operational Expenditures). As despesas de capital (CAPEX) levam a uma busca de uso da estrutura com eficiência máxima. Os custos operacionais (OPEX) buscam automatização e suavidade na utilização da tecnologia .

Com a convergência dos sinais de voz, vídeo e dados para uma rede única (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005), (Choudhury, D., 2001), (Park, K. I., 2005), (Vegesna, S., 2001) - os métodos tradicionais de roteamento da camada IP, como os Internal Gateway Protocols (IGPs, como o OSPF, IS-IS e RIP) e os EGPs (BGP4) não aparecem mais como as melhores soluções para a otimização do tráfego. O tráfego gerado pelas redes locais cresce continuamente, e altera suas características (Ali, M.; Chirivalu, G. & Ge, A., 2005), (Roy, A., 2001). Tais protocolos não oferecem possibilidade de controle de tráfego como relatórios de disponibilidade e utilização.

Uma vez convergidos, os protocolos perdem seu aspecto dinâmico, e não alteram mais as direções dos fluxos nas redes, independente das alterações de demandas ou das condições de degradação dos recursos.

Os algoritmos de roteamento, *distance vector* e *link state*, tendem a convergir o tráfego para os mesmos enlaces e interfaces, o que contribui para um aumento

significativo do congestionamento (desbalanceamento) da rede nos caminhos escolhidos, devido ao uso desigual. Nesse caso, os caminhos preteridos ficam subutilizados, mesmo possuindo condições de tráfego.

Pode-se perceber claramente uma inversão das abordagens originais entre as redes de telecomunicações e as redes de dados. Neste sentido, as telecomunicações tiveram sempre a intenção de simplificar as bordas das redes, criando terminais com pouca ou nenhuma necessidade de processamento (Armitage, G., 2000-a). As estruturas das redes de dados são essencialmente de comutação de pacotes, com os roteadores funcionando como os nós de comutação (Stallings, W., 2002), sem nenhuma preocupação com as extremidades. O núcleo foi mantido simples, e os terminais se encarregavam de executar as tarefas complexas, nas camadas superiores a camada de rede. Os novos serviços, a demanda crescente do tráfego e os avanços tecnológicos estão levando a uma nova abordagem, alterando a arquitetura original das redes de dados. Simplificadamente, a questão pode ser demonstrada na Figura 1-1.

A possibilidade de se trocar por ATM toda a tecnologia de redes locais Ethernet, as redes de longa distância baseadas na comutação de pacotes e os roteadores baseados em datagramas IP não se mostrou viável (Raisanen, V., 2003), principalmente devido aos fatores econômicos (CAPEX) e complexidades operacionais (OPEX). A tecnologia ATM possui capacidades avançadas para suportar serviços múltiplos, e adicionalmente suporta altas taxas de bits (Stallings, W., 2002). Mas, como resultado de um longo percurso durante os esforços de padronização, o padrão final do ATM é altamente complexo, e falhou na implementação fim-a-fim. Um dos fatores mais evidentes após a implantação da tecnologia em ambientes de produção foi a complexidade da gerência dessas redes. O problema fica potencializado pela necessidade de gerenciar também as camadas inferiores de protocolos (SDH, - Synchronous Digital Hierarchy - por exemplo) e as superiores, como o IP. Como consequência, dentro dos domínios da Internet, as redes ATM são usadas nos grandes backbones, onde as configurações são estáticas.

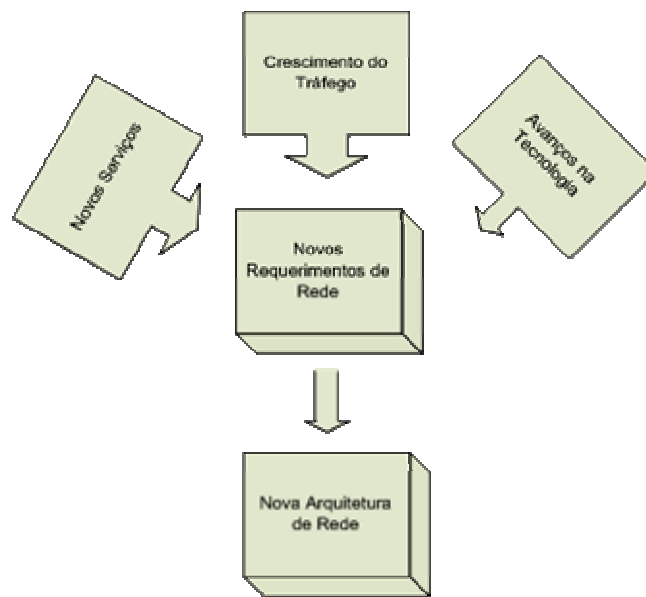


Figura 1-1 - Evolução de arquiteturas de rede - Fonte: (El-Sayed, M. & Jaffe, J., 2002)

A interligação dessas redes precisa ser re-arranjada para a nova situação. Essa tendência de interligar as redes foi denominada convergência. O protocolo IP começou a dar sinais de que iria vencer a convergência no final da década de 1990. (Raisanen, V., 2003). Provavelmente as maiores razões para este fato residem na adoção em larga escala do protocolo, e a inexistência de “propriedade” sobre a implantação do IP, que não está sob controle de nenhum fabricante ou corporação. Uma funcionalidade do projeto da Internet, como já foi declarado, é a manutenção da simplicidade nos dispositivos de rede, e a responsabilidade pela conexão e manutenção da comunicação residir nos sistemas finais. Isso certamente reduz o custo dos projetos dos equipamentos. A escolha do IP como camada de convergência faz sentido também quando observamos sua flexibilidade para funcionar sobre múltiplas implementações da camada de enlace, inclusive o ATM.

No lado das aplicações, o IETF mantém em desenvolvimento um grande conjunto de protocolos para comunicar diferentes tipos de serviços com o IP, usando o transporte da camada 4. Particularmente, a interface de programação socket entre o IP e o protocolos de transporte TCP e UDP é muito conhecida.

O rápido crescimento da Internet em termos de capilaridade e volume de tráfego levou os engenheiros e operadores a perseguirem o ideal de otimizar a pilha de protocolos. Pode-se considerar que a proposta de pilha formada por IP sobre ATM, que

funcionaria sobre SDH, tendo ainda o WDM -*Wavelength Division Multiplexing* - na camada óptica não é uma pilha simples de implantar e manter (nem para o ponto de vista do CAPEX nem para os custos operacionais). Todas as camadas requerem suporte de hardware e software, bem como pessoal treinado para implantação e manutenção.

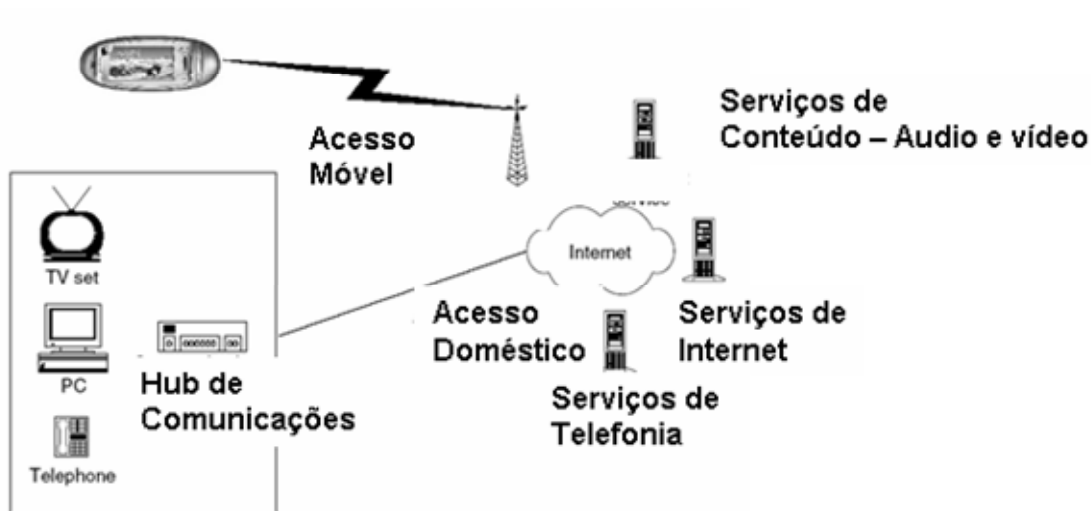


Figura 1-2 Exemplo de cenário multi-serviço possível com IP - Fonte: Raisanen, V., 2003

Os avanços tecnológicos permitem ainda o sobre-provisionamento. A capacidade de transmissão nos canais de fibra tem crescido exponencialmente com a evolução das técnicas de sinalização, como pode ser percebido na Figura 1-3, que mostra a capacidade de sinalização de cada técnica ao longo do tempo.

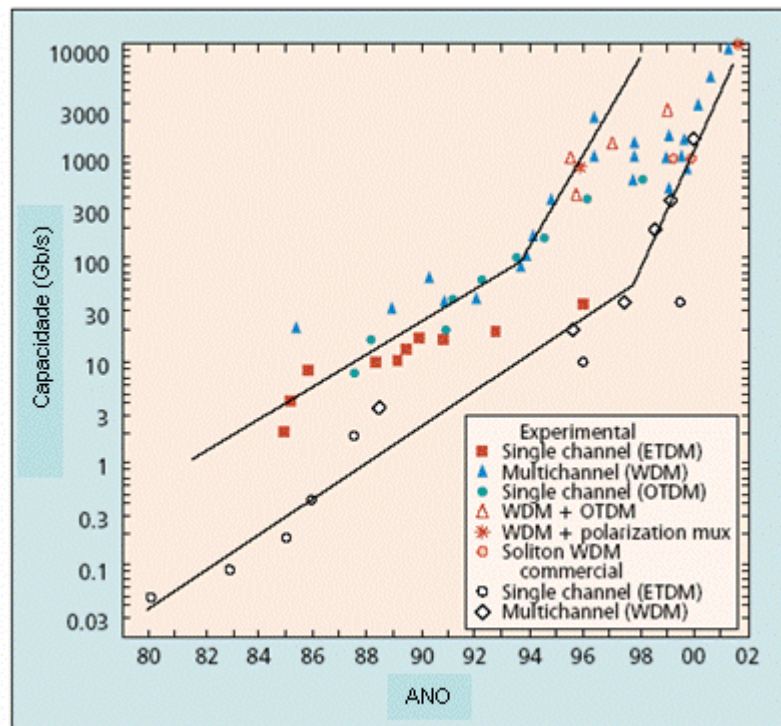


Figura 1-3 - Capacidade das Fibras Ópticas (El-Sayed, M. & Jaffe, J., 2002)

Com a introdução das novas técnicas de polarização combinadas com WDM (Figura 1-4), no momento têm-se registros de transmissões de 6,4 Tbps em um enlace (os testes podem ser encontrados em www.necus.com/companies/8/NECHighDensityDWDM.htm). A polarização permite a criação de canais onde o eixo de propagação das ondas tem um deslocamento ortogonal, possibilitando a transmissão de dois canais simultâneos em planos diferentes. Segundo (Dixit, S. (ed), 2003), a largura de banda disponível nas fibras tem dobrado a cada ano. Atualmente, 40 comprimentos de onda, cada um com um canal OC-48 (2.5 Gbps), são comuns em um par de fibras. Muitos sistemas novos são desenvolvidos com capacidade de transportar 160 canais de 10-Gbps (ou seja, 1.6 Tbps) sobre um único par de fibras. Sistemas capazes de rodar a 80 Gbps em cada canal tem sido demonstrados em laboratório. Nesta taxa, 160 canais seriam iguais a 12.8 Tbps de capacidade. A plenitude da capacidade ainda pode crescer, sendo o limite teórico em volta de 10^{15} (1 Peta bits por segundo - Pbs) (Dixit, S. (ed), 2003).

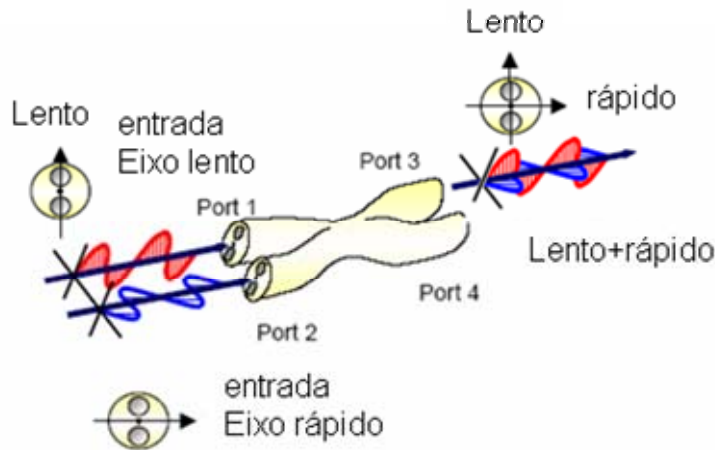


Figura 1-4 - Polarização combinada com WDM (www.necus.com)

Somando-se a capacidade muito grande das tecnologias de transporte, percebe-se ainda um crescimento elevado nas taxas de transmissão das interfaces de redes locais e metropolitanas, capacitando o sobre-provisionamento como possibilidade concreta.

A convergência das tecnologias aponta para o protocolo IP como o padrão na camada de rede (Park, K. I., 2005). Mas foram necessárias varias implementações complementares para garantir a qualidade do serviço (RSVP, DiffServ, MPLS, Engenharia de Tráfego, Roteamento Baseado em Restrições, Policy Routing). Mesmo essas técnicas não garantem manutenção dos caminhos em caso de alterações imprevistas nos parâmetros acordados nos SLAs. A maior parte dos esquemas de roteamento para QoS tem base na troca de informações entre os roteadores, o que causa sobrecarga na rede e na CPU dessas máquinas (Nelakuditi, S. Zhang, Z.; Tsang, R. P. & Du, D. H. C., 2002). Por outro lado, se os esquemas de roteamento são mantidos inalterados por períodos prolongados, o desempenho do sistema degrada-se.

A convergência das redes em direção ao IP não é possível sem as tecnologias auxiliares que garantem a Qualidade de Serviço para que as aplicações exigentes consigam as condições de tráfego mínimas. A criação de um plano de controle para garantir esse auxílio a QoS de forma dinâmica é a proposta abordado neste estudo. A manutenção dinâmica dos melhores caminhos é o problema definido na seção a seguir.

1.2. Definição do problema

O problema abordado neste trabalho pode ser definido como:

Fluxos de voz em redes TCP/IP necessitam de escolhas dinâmicas dos melhores caminhos para garantir a QoS, baseadas em restrições nos valores das métricas de jitter e perdas de pacotes.

O *jitter* foi escolhido pela importância na qualidade dos fluxos de voz e pela inexistência de trabalhos tentando preservar os valores dessa variável nas redes IP. Como os projetos de redes e dispositivos tendem a reduzir o *jitter* nos equipamentos finais, existe uma caracterização do retorno às arquiteturas de redes de dados, com a complexidade nos terminais, como descrito anteriormente. A tentativa de manutenção do *jitter* pelo plano de controle insere o paradigma de “complexidade nas redes”, permitindo o uso de terminais mais simples pelos usuários das aplicações..

As perdas foram escolhidas em conjunto com o *jitter* por serem também um fator limitante (juntamente com o ataso e a vazão, mais o *jitter*, as perdas formam o conjunto de métricas clássicas de QoS). Além desse motivo, existia a necessidade de comparação da qualidade dos caminhos em relação a mais de uma métrica, e a ferramenta de medição disponibiliza em um mesmo registro, os valores de perdas e *jitter*.

Para se resolver a questão proposta, deve-se enfrentar outras questões relacionadas:

- Medir e computar as condições dos caminhos para fazer a escolha do melhor entre eles

- As métricas que devem-se usar como parâmetro para a troca dos caminhos.

- Escolher um caminho para um fluxo em uma rede, sem interferir demasiadamente nessa rede, uma vez que:

- a) A disponibilidade de recursos da rede muda a cada estabelecimento ou encerramento de fluxo, e as necessidades de uso dos enlaces também se alteram;

b) A troca de informações entre os roteadores para manter um mapa global dos estados dos enlaces pode degradar a CPU e o próprio enlace;

c) A condição da troca dinâmica pode afetar os fluxos já existentes no novo caminho.

Essa questão aborda a alteração das condições de tráfego em redes IP onde a manutenção de níveis adequados de atraso e de perdas é importante. Além dos fluxos que exigem mais que o melhor esforço, notadamente voz e vídeo, podem-se incluir reservas para dados privilegiados ou alternância dos privilégios (preempção).

Os sistemas atuais de escolha de melhores caminhos de forma a manter os enlaces em condições de prover as necessidades dos fluxos de tráfego baseiam-se em trocas de informações entre os roteadores, e priorizam os caminhos mais curtos. Este sistema não permite visões atualizadas dos enlaces por todos os roteadores, porque isto gera *overhead* aumentando o uso dos enlaces e das CPUs (Nelakuditi, S. Zhang, Z.; Tsang, R. P. & Du, D. H. C., 2002).

Como consequência, as informações obtidas em um nó rapidamente ficam desatualizadas. Novas reservas ou cancelamentos podem ocorrer com base em informações errôneas.

Quando os roteadores tentam obter uma visão global da topologia, inclusive dos estados dos enlaces, pode ocorrer um problema conhecido como “problema de sincronização”: Após uma atualização dos estados dos enlaces, muitos roteadores escolhem os caminhos que parecem com melhor estado, sobrecarregando-os. Na próxima atualização, estes enlaces não serão escolhidos para construção dos caminhos, causando uma sub-utilização (Doyle, J., 1998), (Clark, D., 1995).

Devido a essas contradições, já foi demonstrado que, quando a dinâmica de atualização tem intervalos maiores que a dinâmica dos fluxos, o desempenho global decai severamente (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998).

A qualidade de serviço relaciona-se ao problema de como selecionar um fluxo tal que os requisitos das aplicações sejam atingidos. Para se fazer a escolha certa na seleção dos caminhos, é imperativo que tenhamos algum conhecimento sobre o estado da QoS global da rede, ou seja, a distribuição da matriz de tráfego.

Portanto, ao projetarmos esquemas de roteamento de QoS, devemos contemplar os pontos chaves a seguir:

- a) Como obter algum conhecimento do estado global da rede;
- b) Tendo este conhecimento, como selecionar um caminho para um fluxo;
- c) Após selecionar o caminho, selecionar qual a técnica a ser usada para sinalizar a escolha.

Soluções para estes problemas afetam o desempenho e os custos no roteamento de QoS.

Algumas propostas de alteração dos caminhos em níveis mais inferiores como o óptico e enlace (Jajszczyk, A. & Rozycki, P., 2006) enfrentam o problema da distância da camada de aplicação. Segundo a RFC 3469 -(Sharma, V. & Hellstrand, F., 2003), alterar os caminhos em níveis muito baixos pode causar desperdício em relação as aplicações que não estavam necessitando uma troca (Figura 1-5). Pela figura, percebe-se que a alteração de um caminho óptico pode afetar vários caminhos na camada de enlace, e que cada caminho nessa camada pode afetar muitas rotas na camada de rede, multiplicando o problema.

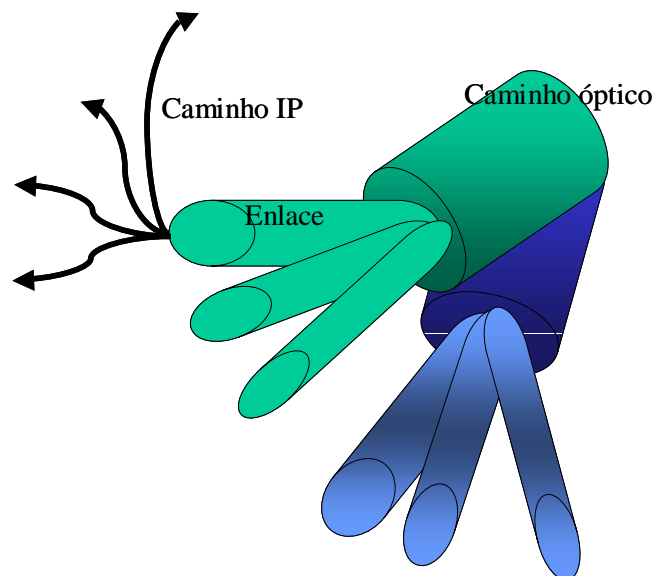


Figura 1-5 Troca de caminhos em vários níveis. Quanto mais inferior o nível da troca, mais conexões são afetadas (com base na RFC 3469).

A maioria das soluções propostas (Nelakuditi, S. Zhang, Z.; Tsang, R. P. & Du, D. H. C., 2002), (Yuan, X. & Zheng, W., 2004), (Shand, M. & Bryant, S., 2006) requer uma troca periódica

de informações entre os roteadores, para obter uma visão global dos estados dos links com respeito aos parâmetros de QoS.

Algumas iniciativas (Jajszczyk, A. & Rozycki, P., 2006) estão prevendo o uso do protocolo LSM (Link State Management – RFC 4204 - Lang, J. Ed., 2005) para construção de planos de controle.

Além disso, as métricas previstas pelos protocolos tradicionais, como o OSPF, que poderiam ser usadas pela configuração do campo ToS do cabeçalho do Ipv4 (listado no Quadro 1-1), normalmente são suprimidas das configurações pelos administradores, pois:

- a) Precisam estar configuradas em todos os roteadores da área;
- b) São estáticas, em sua maioria (exceção ao ToS 16);
- c) Potencialmente alteram os caminhos para todos os pacotes trafegando

no enlace (Figura 1-5).

Quadro 1-1 - Campo ToS no OSPF – adaptado de Stallings, W., 2002 – (pág 437-438)

| Campo | Nome | Função |
|--------|-------------------------|--|
| ToS 0 | Normal | Métrica padrão, entendida por todos os roteadores. Pode ser designada arbitrariamente, mas normalmente é configurada para 1 a cada hop |
| ToS 2 | Minimize monetary costs | Pode ser usado se os custos monetários puderem ser associados a rede. |
| ToS 4 | Maximize reliability | Pode ser pré-configurada ou baseada nos históricos recentes de queda (<i>outage</i>) ou em taxas de erros medidas anteriormente |
| ToS 8 | Maximize Throughput | Pré-configurada baseada na taxa de transferência da interface. Tipicamente, é a taxa de um bit em unidades de 10-nanosegundos. Uma eth 10Mbps, tem um valor de 0 e um enlace de 56Kbps tem valor de 1785 |
| ToS 16 | Minimize Delay | Medida do período de trânsito ou retardo em um hop em particular. Tipicamente, consiste no retardo de propagação somado ao retardo de enfileiramento. É medido dinamicamente por cada roteador, para cada uma de suas interfaces ativas. |
| | | |

Fonte: (Stallings, W., 2002)

Os valores do campo ToS poderiam ser inseridos dinamicamente pela estação de monitoração. Porém, ao trocar as métricas (*metric manipulation*) (Alwayn, V. , 2002) dos enlaces além de potencialmente alterar o caminho de todos os pacotes que percorrem o enlace, não consideram-se as características dos tráfegos e as restrições da capacidade da rede quando tomam as decisões de roteamento.

O campo ToS foi denominado DSCP – DiffService Code Point com a especificação da arquitetura DiffServ pelo IETF.

A tecnologia MPLS foi projetada com o plano de controle separado do plano de transporte. Este conceito foi estendido pela GMPLS, que permite que o plano de controle atue fisicamente separado do plano de transporte associado a ele (Jajszczyk, A. & Rozycki, P., 2006), (Banerjee, A.; Drake, J.; Lang, J.; Turner, B.; Awduche, D.; Berger, L.; Kompella, K. & Rekhter, Y., 2001). Para implementação deste dispositivo físico, o modelo adota o uso de uma estação servidora de QoS (QNS – *QoS Network Server*, ou Servidor de QoS da Rede). Tal dispositivo é uma entidade funcional essencial na rede com QoS (Finenberg, V., 2002). O QNS possui uma visão geral da rede, e poderia suportar uma variedade de funções, como CAC (*Connection Admission Control*), cálculos das restrições de roteamento, acesso aos bancos de dados e diretórios, controle de políticas, levantamentos de utilização da rede (para tarifação, se for o caso) e outras funções, de maneira centralizada. O QNS foi idealizado com base na tecnologia Softswitch, descrita em (Lakshmi-Ratan, R., 1999).

1.2.1. Hipóteses

Algumas arquiteturas e conjuntos de tecnologias foram criadas para buscar uma melhoria do tráfego na Internet. A Arquitetura de Serviços Integrados (ISA), através do Protocolo de Reserva de Recursos (RSVP – Resource Reservation Protocol) e a arquitetura de Serviços Diferenciados (DSA), através da marcação dos pacotes. A Engenharia de Tráfego (TE – Traffic Engineering), através do MPLS – Multiprotocol Layer Switching abrange um conjunto de métodos (como o re-roteamento), protocolos (OSPF-TE, RSVP-TE, MPLS-TE) e técnicas (distribuição de rótulos, criação de circuitos virtuais) para melhoria do tráfego. Não existe uma solução definida para todos os ambientes e serviços disponíveis após a convergência das redes de dados e de voz. Isoladamente tais abordagens não são suficientes para prover e manter dinamicamente os parâmetros de QoS fim-a-fim, bem como evitar os problemas inerentes aos congestionamentos e conseqüentes atrasos, variações nos atrasos e descartes de pacotes. O uso de protocolos de roteamento convencionais, mesmo com métricas de QoS como o atraso, não possuem suficiente sensibilidade para alterar os caminhos fim-a-fim tão logo tais caminhos sofram degradação.

As hipóteses centrais desta tese são:

1 - É possível prover e manter o estado das comunicações fim-a-fim, otimizando os caminhos sob demanda, por meio de métricas dinâmicas, melhorando as condições finais dos fluxos de voz.

2 – É viável utilizar-se um plano de controle baseado em ferramentas de medição fim-a-fim, sem usar os recursos dos dispositivos de rede, com a finalidade de manter uma topologia atualizada constantemente, em termos de *jitter* e perdas.

Para comprovação dessas hipóteses, um modelo integrado é proposto, no capítulo 5, com uma estação de monitoramento e sinalização em um plano de controle. Ao mesmo tempo em que mantém um mapa do estado dos enlaces, a arquitetura pode configurar os equipamentos, segundo o conceito de Ponto de execução de Políticas.

Algumas tentativas de unir as abordagens citadas (ISA, DSA e TE) tornam-se bastante complexas (Chen, X. et al, 2003), demonstrando que não existe solução trivial para a equação devido ao grande número de componentes envolvidos (Figura 1-6).

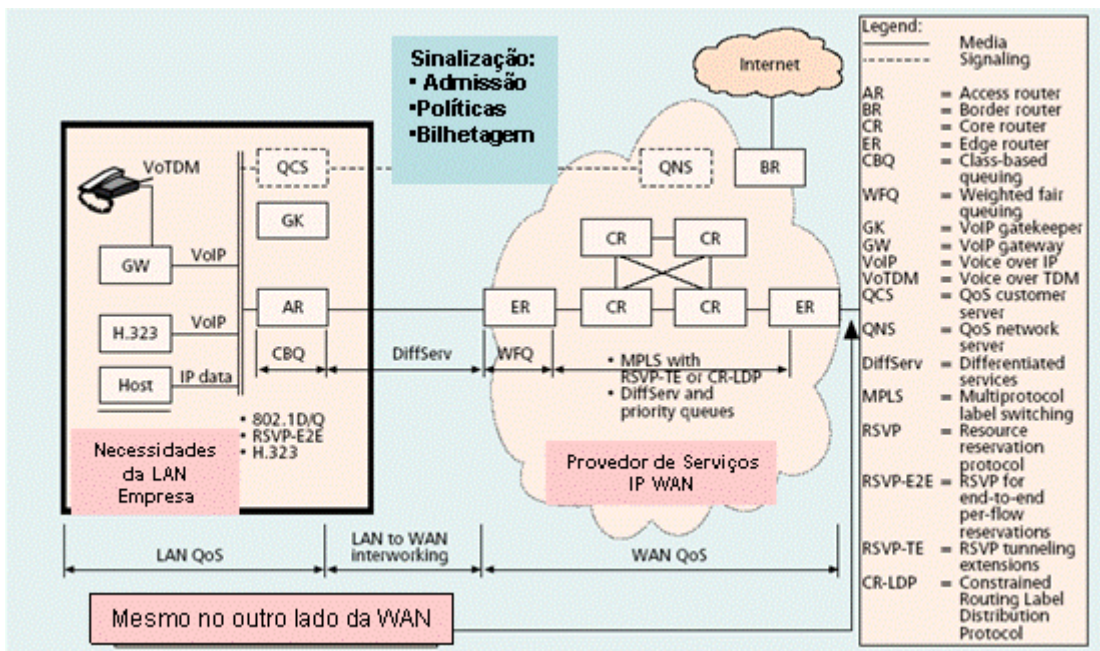


Figura 1-6 - Estrutura de QoS fim-a-fim para grandes corporações - Fonte: (Finenberg, V., 2002)

1.3. Proposta de solução

Este trabalho propõe um plano de controle dinâmico, para implantação de políticas de roteamento que auxiliam na manutenção dos melhores caminhos, em redes baseadas no protocolo IP. O plano de controle está descrito em detalhes no capítulo 5.

A situação de complexidade ilustrada na Figura 1-6 levou algumas iniciativas como o Qbone, da Internet 2 a reduzirem as expectativas de implantação de serviços fim-a-fim. As ações a respeito da Qualidade de Serviço plena, fim a fim, na Internet estão se reduzindo aos serviços intra-domínio (essa tendência pode ser constatada em <http://qbone.internet2.edu>). Chegou-se a conclusão que dificilmente se poderia criar classes de serviço do “*tipo Premium*”, que na concepção do Qbone seriam tão próximas quanto possível de linhas privadas virtuais dentro da internet. As classes de serviço são descritas com mais detalhes na seção 3.7, que trata da arquitetura de serviços diferenciados, proposta para melhorar o desempenho de aplicações com necessidades de QoS.

A proposta deste trabalho baseia-se nas especificações ASON (Automatically Switched Optical Networks) (Jajszczyk, A. & Rozycki, P., 2006) e GMPLS (Generalized Multiprotocol Label Switching) (Liu, H.; Pendarakis, D.; Komaee, N. & Tellium, D. S., 2002), de responsabilidade do ITU-T e IETF; no paradigma softswitch (Lakshmi-Ratan, R., 1999), nos Servidores de QoS da Rede (QNS – QoS Network Server) (Finenberg, V., 2002) e no re-roteamento do IP (Shand, M. & Bryant, S., 2006).

Os caminhos são escolhidos através de uma adaptação do algoritmo de roteamento de Dijkstra (Dijkstra, E. W., 1959), onde as métricas de otimização são inseridas pelo administrador da rede. Algumas práticas de engenharia de tráfego, notadamente o re-roteamento, que possibilitam a criação de caminhos baseados em políticas que não necessariamente elegem a menor distância, são aplicadas na solução.

A proposta encontra semelhanças com os elementos básicos sugeridos na “Arquitetura de políticas do IETF/DTMF” – Figura 1-7.

- Uma ferramenta de gerência de políticas;
- Um repositório de políticas;

- Um ponto de decisão de políticas (PDP);
- Um ponto de execução de políticas (*Policy Enforcement Point-PEP*).

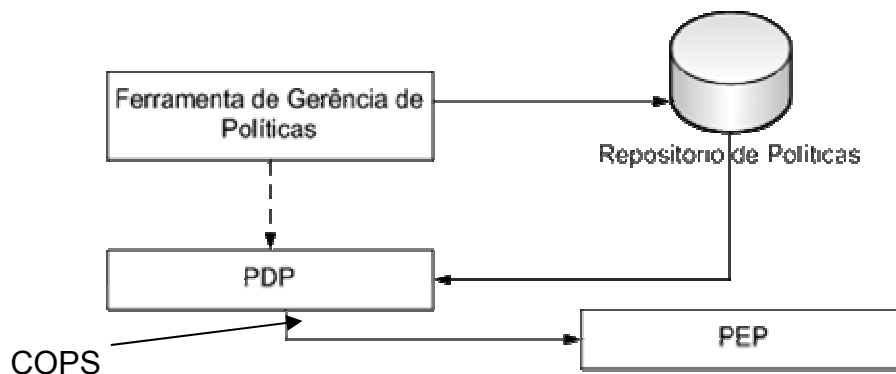


Figura 1-7 – Arquitetura de Políticas do IETF/DTMF - adaptado de (Verma, D., 2000) e (Durham, D.; Boyle, J.; Cohen, R.; Herzog, S.; Rajan, R.; & Sastry, A., 2000)

A arquitetura de políticas compõe o plano de controle do modelo, conforme visualizado na Figura 1-9 (Lemma, H. G., 2003), onde a sinalização proposta deve ser efetuada através de mensagens pelo protocolo RSVP, ou outro método de distribuição de políticas de roteamento, como os scripts.

Este ponto de execução de políticas (denominado por Finenberg (Finenberg, V., 2002) como Ponto de Troca de Políticas) deve incluir tarefas como marcação de pacotes, controle de admissões, priorização de usuários, roteamento explícito, descarte de pacotes, reação ao congestionamento, e outras. Essa solução será discutida mais detalhadamente na seção 4.8.1. Segundo as propostas de anexação de QoS no protocolo OSPF, pela RFC 2676 (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998), a seleção das rotas pode ser pela identificação do próximo salto somente, ou pela especificação dos nós intermediários, num modelo de roteamento explícito. Embora as diferenças entre os métodos impactem no tipo de retorno da informação, a operação básica do algoritmo de seleção não será afetada. Essa solução, bem como outras alternativas para manutenção da QoS inerente aos fluxos de voz será discutida na seção 4.3, que trata de técnicas de roteamento não convencionais.

Neste trabalho, o QNS utiliza técnicas de re-configuração da camada IP (Shand, M. & Bryant, S., 2006) para manter os caminhos em condições adequadas aos fluxos de voz. O modelo sugerido, representado na Figura 1-10, possui uma interação com diferentes camadas do modelo de referência OSI. Na camada de aplicação, existe uma interface

de interação da estação de gerência e controle de QoS (QNS) e os agentes de QoS (Figura 1-8). Na camada de transporte é utilizado o protocolo de transporte (UDP) pela ferramenta de medição. Na camada de rede o modelo inclui algoritmo de roteamento baseado nos estados dos enlaces.

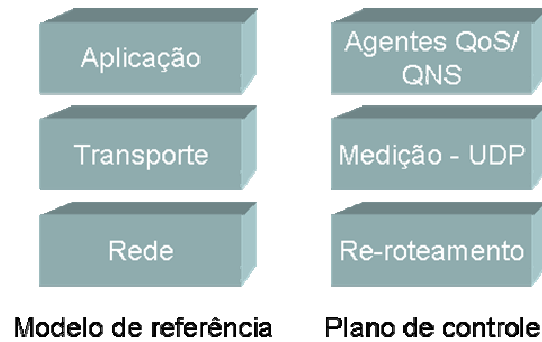


Figura 1-8 - Relações entre o modelo de referência e o plano de controle

A Figura 1-9 demonstra a relação dos protocolos e tecnologias com os planos de dados (também denominado plano de transporte por Jajszczyk, A. & Rozycki, P., 2006) e com o plano de controle.

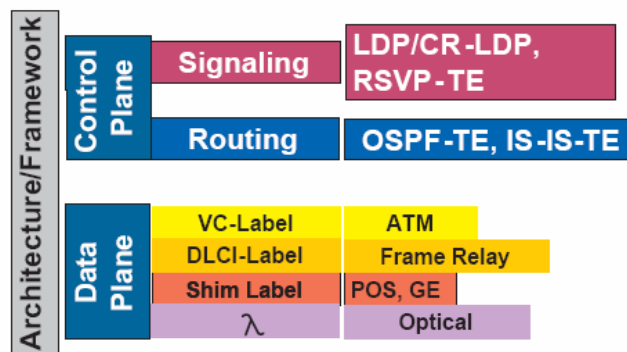


Figura 1-9 - Componentes dos planos de controle e de dados - Fonte:(Lemma, H. G., 2003)

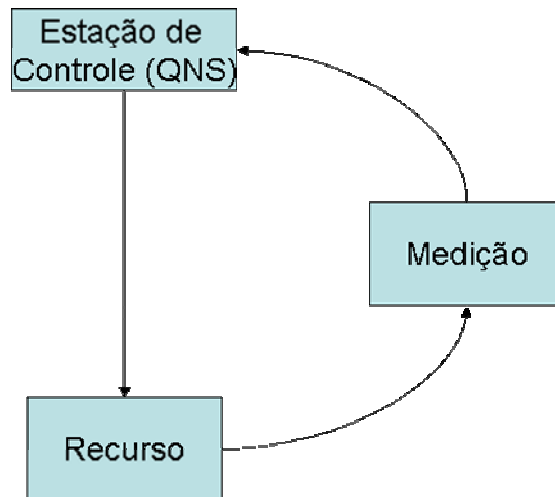


Figura 1-10 – Plano de controle para Roteamento através de Políticas para TE

A estação de controle das políticas (QNS – Servidor de QoS da Rede) segue o modelo proposto em (Verma, D., 2000)– mostrado na Figura 1-11.

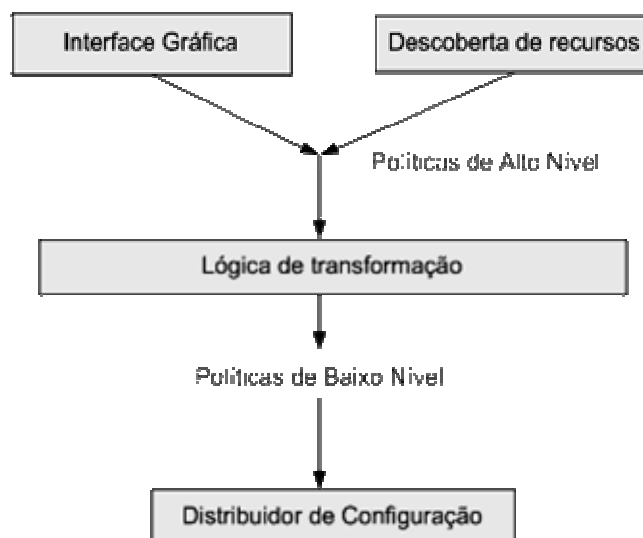


Figura 1-11 - Estação de Gerência de Políticas (Controle/Sinalização)

As medições são baseadas em pontos de coleta distribuídos na topologia da rede, através de softwares de monitoração (Blum, R., 2003), (Hassan, M. & Jain, R., 2004) . Os valores informados pelos agentes são armazenados na base de dados do repositório de políticas, para serem utilizados pelo PDP. As regras são processadas e transformadas em regras de baixo nível, para então serem distribuídas. As tarefas de cálculo e distribuição de configurações no PDP são efetuadas pelo protótipo QoS-Path, desenvolvido para dar suporte ao plano de controle proposto neste trabalho. Os detalhes do plano de controle se encontram no capítulo 5.

1.4. Objetivos do trabalho de Pesquisa

Nesta seção se descrevem os objetivos gerais e específicos deste trabalho.

1.4.1. Objetivos gerais

Esta tese propõe um plano de controle para prover políticas de roteamento com métricas de QoS estáveis, com alterações dinâmicas dos caminhos, em função das condições dos enlaces. Pretende-se demonstrar ainda que a utilização das técnicas de re-roteamento sob demanda permitem uma eficiência maior nos recursos de rede fim-a-fim, mantendo as métricas dentro de limites aceitáveis pelos fluxos de voz.

1.4.2. Objetivos específicos

Como objetivos específicos, a presente tese pretende:

- Criar um protótipo de monitoração e reconfiguração da rede;
- Implantar um servidor de roteamento com QoS, com base nos cálculos de rotas pelo melhor caminho, através do algoritmo de Dijkstra;
- Comparar teoricamente as diversas alternativas de roteamento não convencional descritas no capítulo 4.3, em termos de aplicabilidade para o problema de manutenção dos fluxos de voz.
- Projetar experimentos para comprovação ou refutação das hipóteses principais deste trabalho;
- Analisar o comportamento dos parâmetros escolhidos para avaliação do desempenho do plano de controle;
- Avaliar as condições dos ambientes necessários para o funcionamento do plano de controle;
- Avaliar as condições onde os probs de medição possam interferir nas próprias medidas;
- Se existir interferência (previsível, uma vez que trata-se de uma medição ativa), quais os limites onde a situação inviabiliza a efetividade da solução.

1.5. Relevância do trabalho de pesquisa

A otimização do desempenho das redes IP de larga escala é um problema importante, devido às características críticas que essas redes atingiram. Atualmente, tais redes suportam atividades econômicas, educacionais e sociais. Existe consenso que o IP será o protocolo de rede para os diversos serviços (dados, voz e vídeo). Identifica-se também que este protocolo tem limitações de confiabilidade e alcançabilidade (Doyle, J., 1998), (Stallings, W., 2002). Apesar delas, as redes IP modernas apresentam características que destacam sua importância e os problemas potenciais (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002):

- Fornecem serviço em tempo real;
- Tornaram-se de missão crítica;
- Seus ambientes operacionais são muito dinâmicos e complexos.

Manter a qualidade dos fluxos em tal ambiente tornou-se um dos principais campos de pesquisa na área de redes de comunicações. O desempenho destes sistemas deve ser otimizado sem que os custos para tal inviabilizem sua disseminação. Isso não se consegue apenas com sobreprovisionamento, pois nem sempre é possível aumentar os recursos disponíveis.

Mesmo em condições de funcionamento ideais, as falhas nos enlaces são inevitáveis. Os avanços nos projetos dos roteadores têm conseguido reduzir o tempo de ruptura na comunicação de vários segundos para menos de um segundo, o que ainda não é suficiente para os serviços emergentes na Internet, que necessitam de períodos com ordens de magnitude menores que isso (Shand, M. & Bryant, S., 2006).

As redes de próxima geração (NGN – *Next Generation Networks*) necessitam de planos de controle, segundo os organismos de padronização IETF e ITU-T (Jajszczyk, A. & Rozycki, P., 2006). Esses planos, como o proposto neste trabalho de pesquisa, possibilitam a gerência dos recursos da rede.

Os mecanismos necessários para tráfegos de voz sobre o protocolo IP exigem alternativas para a manutenção de QoS em uma rede projetada para os tráfegos *Best Effort* (Chen, X. et al, 2003).

1.6. Originalidade

Pode-se dividir os assuntos tratados neste trabalho em algumas questões fundamentais, cada uma das quais com abordagens clássicas dos problemas estudados. A seguir, procura-se demonstrar as questões que podem ser consideradas inovadoras em cada uma dessas áreas:

1.6.1. Escolha dos melhores caminhos

Normalmente as métricas para escolha dos melhores caminhos resumem-se a contagem do número de hops (*hop count*) (Doyle, J., 1998). Quando se utilizam métricas diferentes, normalmente são medidos o atraso ou a vazão como parâmetros adicionais a contagem de saltos. Neste trabalho, o *jitter* será uma das métricas que irão determinar os caminhos de melhores condições para os fluxos. O *jitter*, ou PDV (*Packet Delay Variation*) é uma variável bastante sensível às condições dos enlaces, existindo poucos trabalhos de pesquisas (Demichelis, C.; Chimento, P., 2002) sobre as técnicas de medição, monitoração e preservação dessa métrica como parâmetro de QoS. Além do *jitter*, as perdas serão estudadas nas mesmas condições, tornando a proposta mais genérica em termos de desempenho da rede.

1.6.2. Políticas de roteamento

As políticas de roteamento são usadas como mecanismos de proteção dos fluxos diferenciados, mas possuem uma configuração estática, ou seja, os caminhos não se alteram sob demanda. Quando mais de um fluxo é classificado com a mesma prioridade, as políticas podem falhar no sentido de não prover o recurso para todos os fluxos prioritários em uma mesma fila, pois a prioridade passa a ser invariavelmente na política FIFO. Os gatilhos de re-roteamento tradicionalmente ocorrem quando um ou mais enlaces tornam-se fisicamente inoperantes. Este trabalho trata da troca de rotas instantaneamente após a geração da demanda, caracterizada pela falta de condições de serviço dos fluxos de voz.

1.6.3. *Monitoramento e sinalização de conexões fim-a-fim*

Normalmente aborda-se o problema do ponto de vista dos dispositivos de núcleo da rede (Hassan, M. & Jain, R., 2004), (Roy, A., 2001). Este trabalho enfoca a administração dos recursos dos enlaces, segundo as políticas definida pelos administradores da rede. Isso é obtido através dos agentes de medição e monitoração e do servidor de QoS da rede (QNS). Os componentes do núcleo fazem parte do enlace “agregado”, ou seja aquele que envolve todo o segmento fim-a-fim entre as aplicações que estão se comunicando.

1.6.4. *Dinâmica do ambiente de QoS*

O ambiente extremamente variável que caracteriza uma rede de serviços Internet dificulta um compromisso razoável entre a estabilidade das rotas e o balanceamento das cargas, uma vez que, se as rotas são fixadas para gerar estabilidade, não pode garantir que os caminhos considerados melhores não sejam congestionados, uma vez que serão sempre os preferidos. Este trabalho propõe um balanceamento das cargas de forma centralizada, minimizando o problema das alterações inócuas. Tal situação é comum quando, para não afetar os recursos, as rotas são calculadas e inundadas lentamente, a partir do ponto afetado, possibilitando o uso de um caminho já congestionado como se estivesse ainda em boas condições.

1.6.5. *Manutenção do desempenho*

A maior parte dos trabalhos de pesquisas visando provimento ou manutenção dos melhores caminhos para os fluxos das aplicações baseiam-se na troca de informações sobre os estados dos enlaces entre os roteadores (Osborne, E. & Simha, A., 2003). Normalmente isso implica em certa perda de desempenho. Por outro lado, uma troca de informações de caminhos em intervalos mais breves pode acarretar em re-configurações demasiadas, consumindo CPU e banda. Na proposta apresentada neste trabalho, as rotas são re-arranjadas sem a necessidade de convergência dos protocolos, definindo agilidade e eficácia nas trocas, inclusive quando são necessárias trocas sucessivas de caminhos.

1.6.6. *Re-roteamento e recuperação de caminhos*

O re-roteamento baseado na camada 3 é lento para suportar as necessidades dos núcleos de rede, e não provê habilidades para assegurar proteção de banda para fluxos específicos (por exemplo VoIP, Virtual Leased Lines). Normalmente as técnicas somente são utilizadas em momentos de falha completa dos enlaces. Utilizando-se o plano de controle proposto, o re-roteamento garante a manutenção e a recuperação da condição dos caminhos, podendo inclusive melhorá-los, sem que seja necessário uma falha. Além disso, o tempo necessário é bem menor que o da convergência tradicional.

Deve-se notar ainda que existe uma relação entre o nível de monitoração e comutação dos caminhos e a percepção das condições sob o ponto de vista das aplicações. Quanto mais inferior o nível, mais grosseira a percepção que a camada tem das necessidades das aplicações. As técnicas de comutação ópticas, no nível 0, podem melhorar o desempenho de uma aplicação ao trocar um caminho óptico. Mas estariam desperdiçando recursos do ponto de vista de muitas outras aplicações. O mesmo pode acontecer com as comutações de camada 2, como o MPLS. Quando os caminhos são escolhidos a partir da camada 3 (como é proposto neste trabalho), o desperdício pode não ser o ideal, mas fica reduzido a uma rede de destino. Portanto, mais próximo das necessidades de uma aplicação.

1.6.7. *Independência da arquitetura e simplicidade*

O plano de controle utiliza ferramentas que podem ser configuradas em qualquer ambiente, independente inclusive dos fabricantes dos roteadores. A solução não necessita hardware especializado, utilizando estações de trabalho que estejam conectadas aos enlaces que se quer monitorar.

1.7. *Contribuições*

Esta tese contribui com algumas áreas de pesquisa. As contribuições mais evidentes estão descritas a seguir, separadas pelas áreas de pesquisa.

1.7.1. Medições

Os problemas enfrentados pelas técnicas de medição são diversos, e parece consenso entre os autores da área que os erros nas medidas são inevitáveis, mesmo para as variáveis mais comportadas - RFC 2330 - Framework for IP Performance Metrics - (Paxson, V. et. al, 1998). Certamente este não é o caso do *jitter*, sensível a um número muito grande de fatores, desde os algoritmos implementados nos equipamentos, intensidade dos fluxos, erros de transmissão, re-transmissões, as políticas de filas, tamanhos dos pacotes, número de saltos. Neste trabalho foram efetuadas medições em relação ao *jitter*, e muitos destes fatores puderam ser comparados.

Os dois ambientes utilizados nos experimentos contemplam níveis bem diversos para os fatores potencialmente influentes nas variáveis de resposta (*jitter* e perdas), especialmente os tamanhos dos pacotes.

1.7.2. Re-roteamento

As questões relativas à estação de gerência de QoS poderão ser utilizadas pelos administradores de redes para quaisquer requisições por parte dos usuários de aplicações, como videoconferência ou bancos de dados. Para tanto, deve-se apenas decidir qual é a métrica a ser utilizada, e a ferramenta de medição. O resultado da medição pode ser enviado ao QNS, que se encarrega da escolha dos melhores caminhos e do re-arranjo das rotas.

Normalmente o re-roteamento é efetuado somente em caso de queda de um ou mais enlaces. O plano de controle proposto pode efetuar um re-arranjo preventivo, em caso de degradação das métricas escolhidas.

Os métodos de escolha dos caminhos com base em métricas de QoS podem auxiliar algumas implementações em softwares de roteamento. A integração de várias soluções (roteamento convencional, métricas dinâmicas) deve gerar um modelo flexível, atendendo a necessidades de topologias e arquiteturas abrangentes, com cenários múltiplos.

1.7.3. Manutenção de métricas

O roteamento baseado em QoS tenta selecionar um caminho que satisfaça um conjunto de restrições, enquanto procura uma utilização eficiente dos recursos da rede. Neste trabalho de pesquisa, não existe um conjunto de restrições. Os melhores caminhos são encontrados com base no *jitter* ou nas perdas, nunca simultaneamente. Essa proposta, enquanto simplifica a solução, demonstrou ainda que sempre que o plano de controle melhora a qualidade do caminho em função de uma variável, a condição geral da outra variável também melhora.

1.7.4. VoIP

Este trabalho apresenta contribuições significativas na “convergência” dos temas de fluxos de voz (redes de telecomunicações) e redes de dados, uma vez que os assuntos normalmente são tratados em separado. As discussões dos dois temas, com base na literatura oriunda dessas duas áreas, propicia um enfoque híbrido, reunindo posições de órgãos de padronização distintos como IETF e ETSI. Existe neste trabalho de pesquisa uma visão denominada de *INFOCOM* (Iovana, P.; Sabela, R. & Settembre, M., 2003), uma nova geração de sistemas de comunicação, que seria o resultado da soma entre os paradigmas de Telecom e Datacom.

1.7.5. Análise de desempenho

Os modelos gerados podem auxiliar nas pesquisas de desempenho, pois possuem inovações no sentido de reagir às condições adversas, alterando os caminhos conforme a demanda dos recursos. Este dinamismo das respostas gera algumas fontes de novas dúvidas, como o tempo ideal para manutenção dos novos caminhos - devem ser reconstituídos após a passagem dos fluxos que se quer preservar? Quais os melhores momentos para os disparos dos gatilhos? Qual a real influência da alteração dos valores das médias imediatamente após uma reconfiguração?

1.7.6. Provedores de Serviço Internet (ISPs)

Sob a ótica dos provedores de Serviço Internet (ISP, *Internet Service Providers*), este trabalho pode contribuir na implantação de um modelo de gestão dos recursos que garantam os Acordos de Níveis de Serviços (SLAs), especificados com os clientes. Tais acordos possuem base legal (Jha, S.; Hassan, M., 2002), e devem garantir disponibilidade e os serviços constantes na especificação (SLS - Service Level Specification), principalmente pela relação custo/benefício, uma vez que o modelo é abrangente e não exige hardware especializado.

Segundo a RFC 3052 (Eder, M. & Nag, S., 2001) a gerência dos serviços de rede está para se tornar um problema maior nas redes futuras. Uma vez que não será mais possível prover um “serviço igual para todos”, como até agora se apresentavam os protocolos da Internet, a utilização de métodos de baixo custo para manter os níveis de QoS necessários é uma contribuição efetiva. Este aspecto é ainda mais relevante quando observa-se a comunidade IP, normalmente relutante na abordagem dos serviços de rede.

1.8. Limitações e escopo

Este trabalho abrange algumas áreas do conhecimento da Internet, notadamente a engenharia de Tráfego, o roteamento de pacotes e as métricas de desempenho IP, principalmente perdas e *jitter*. São estudados alguns protocolos auxiliares para manutenção do IP como aglutinador dos esforços de convergência de redes. O roteamento com extensões de QoS têm destaque. Algumas técnicas de sinalização foram estudadas e foi gerado um plano de controle para roteamento dinâmico, baseado em métricas de QoS, sinalizado fora de banda. O modelo foi testado em ambiente controlado e homogêneo, com todos os roteadores do mesmo fabricante e rodando as mesmas versões de sistema operacional. Todo o hardware também foi mantido em condições de igualdade, em termos de memória e CPU.

Foram realizadas comparações entre várias propostas da literatura para resolução do problema de cálculo e manutenção dos melhores caminhos com base nas métricas clássicas de QoS.

As transmissões de voz foram usadas como parâmetro para os requisitos de QoS, para simplificar o número de variáveis, uma vez que não é necessário controle detalhado sobre a vazão, as conexões TCP e outros fatores (Chen, X. et al, 2003). As métricas monitoradas como variáveis de resposta dos testes de desempenho foram a variação do atraso, e as perdas, para efeito de simplificação da metodologia. A utilização do atraso fim-a-fim e da vazão ou banda disponível é possível, mas serão mantidas como propostas futuras.

Para tornar viável a proposta deste trabalho, algumas limitações foram delineadas, uma vez que muitos aspectos que poderiam auxiliar na solução e abrangência do problema também demandariam esforços de implementação.

Este trabalho de pesquisa limita a proposta de manutenção da QoS em uma solução fim-a-fim, usando medidas externas ao núcleo da rede, sem monitoração dos dispositivos centrais em relação as variáveis de resposta.

Este trabalho de pesquisa limita-se às questões de roteamento dentro de um único sistema autônomo (intra-AS). Procura-se ainda limitar o escopo ao provisionamento de QoS de forma a que a pilha TCP/IP possa ser testada em condições de roteamento dinâmico, através de sinalizações fora de banda. A solução foi desenvolvida em ambiente de laboratório, uma vez que experimentos dessa magnitude interromperiam ambientes produtivos de forma muito freqüente.

Vários protocolos não farão parte dos testes, embora existam de forma abundante na Internet (NAT, VPN, IPsec). Tais protocolos exigiriam doses extras de esforço de programação e potencializariam as dificuldades em termos de roteamento. Os ambientes estudados serão baseados na forma “pura” do TCP/IP.

Não se terão preocupações com os níveis de segurança que normalmente essas soluções exigiriam, para simplificar a implementação da solução. Dessa forma, senhas exigidas por protocolos como telnet trafegam em forma de *plain text*, e autenticações não serão implementadas.

Os testes de desempenho não irão considerar as características do hardware utilizado (routers, switches, estações e servidor), pois o desempenho será comparado de forma global, desde a estação emitente do fluxo de voz, até o destinatário.

Todos os fluxos das aplicações de voz analisados são *unicast*, embora alguns tipos de sinalizações em *multicast* e *broadcast* façam parte dos protocolos de roteamento.

As métricas de vazão e atraso não são utilizadas na proposta, uma vez que a vazão têm menor importância nos fluxos de voz, e o atraso é uma medida que tornaria a solução proposta fora do nível de simplicidade pretendido.

Considerações a respeito do IPv6 não fazem parte deste trabalho, fundamentado no ambiente de IPv4.

A classificação e o mapeamento dos pacotes não são contemplados, bem como não são as associações das eventuais classes geradas nos sistemas finais (clientes e servidores dos fluxos de voz) com os recursos disponíveis na rede.

Não foram testados ambientes com conexões TCP.

1.9. Estrutura do trabalho

Este trabalho de pesquisa está dividido em oito capítulos. Neste primeiro capítulo foi mostrado o contexto onde o trabalho pretende ser inserido, bem como os objetivos, as principais hipóteses que se pretende comprovar e as maiores inovações na abordagem dos problemas. O escopo foi delimitado, e as principais contribuições na área de estudos também foram demonstradas. No capítulo 2 são apresentadas as fundamentações do trabalho com relação ao ambiente atual da Internet, os tipos de tráfegos e as exigências das aplicações que utilizam fluxos de voz, notadamente a telefonia IP. No capítulo 3, são discutidas as principais implementações que dão sustentação a QoS nas redes baseadas no IP, originalmente projetadas para serviços tolerantes a faixas amplas de perdas e atrasos. No capítulo 4 são abordadas as principais técnicas de roteamento, com ênfase nas alternativas que procuram manter os caminhos em níveis pré-concebidos para as necessidades das aplicações. Essas alternativas foram denominadas de “técnicas de roteamento não convencionais”. No capítulo 5 está descrito o funcionamento do plano de controle proposto. No capítulo 6 são selecionadas as técnicas para medição do desempenho necessário aos fluxos de

voz. Descrevem-se também os experimentos, e a metodologia de amostragem. No capítulo 7 são apresentados os resultados, com base em avaliações estatísticas. No final do capítulo, são desenvolvidas algumas conclusões importantes a respeito dos resultados alcançados. O capítulo 8 apresenta as conclusões gerais do trabalho, e indicações de trabalhos futuros. A última sessão é dedicada a listagem das referências citadas no texto. E o apêndice 1 apresenta resultados e gráficos demonstrativos dos fatores que influenciaram as variáveis *jitter* e percentual de perdas relacionados com os fluxos de voz. O apêndice 2 apresenta conteúdos relacionados a codificação dos canais de voz, que possuem relacionamento com os atrasos e tamanhos de pacotes necessários para os fluxos de voz. O apêndice 3 apresenta a terminologia utilizada em Engenharia de Tráfego.

2. O Cenário da Internet Atual e os Fluxos de Voz

Neste capítulo são analisadas as condições atuais da Internet, e são caracterizados os tipos de tráfego. Em seguida, uma análise das necessidades inerentes dos fluxos de voz são apresentadas, em função das características da digitalização e transmissão em uma rede originalmente não confiável.

Conforme a Internet e as interconexões privadas cresceram em escala, exponencialmente durante os últimos anos, as aplicações diferenciaram-se. As conversações de pequeno porte, antes representadas pelo TELNET, agora foram substituídas por massivas trocas em aplicações cliente-servidor (Stallings, W., 2002), e outras, consideradas “*bandwidth hungry*” (Roy, A., 2001). Os protocolos que suportam as comunicações precisam de novas funcionalidades para comportar os novos serviços e as aplicações emergentes (Jajszczyk, A. & Rozycki, P., 2006), (Chen, X. et al, 2003), (Vegesna, S., 2001). Como foi visto anteriormente, uma abordagem para solucionar este problema é o sobreprovisionamento, mas isso não contempla a eficiência em relação aos custos.

As duas abordagens do IETF para suportar tais perfis de tráfego são a Arquitetura de Serviços Integrados (ISA) e os Serviços Diferenciados (DS), apresentados no capítulo 3.7. Outros métodos incluem o Roteamento Baseado em Restrições (RBR) e MPLS, que possibilitam melhorias de desempenho através da “Engenharia de Tráfego” (TE). Várias alternativas ao roteamento convencional são encontradas na literatura, e algumas inclusive tornaram-se propostas oficiais do IETF, como as extensões de QoS para o OSPF, documentadas na RFC 2676 (Apostolopoulos, G. et al, 1999). Tais alternativas são discutidas em detalhes no capítulo 4.3.

2.1. Tipos de tráfego

Os tráfegos em uma rede podem ser classificados em dois grupos: Elásticos e Inelásticos (Stallings, W., 2002). Outros autores consideram estes grupos como sendo Tempo real e não tempo real. A classificação pode ser observada na Figura 2-1 e encontram-se mais detalhes, entre outros, em (Peterson, L. L. & Davie, B. S., 1999).

2.1.1. Tráfegos elásticos

Tráfegos elásticos (não tempo-real) são aqueles que podem se ajustar a uma faixa muito grande de variações de atraso e vazão, através de uma interconexão de redes, permanecendo em concordância com as necessidades das suas aplicações. Este é o tipo de tráfego tradicional da Internet, e o tipo para o qual toda a arquitetura original do TCP/IP foi projetada. As aplicações que geram este tipo de tráfego são usuárias do TCP e do UDP como protocolo de transporte.

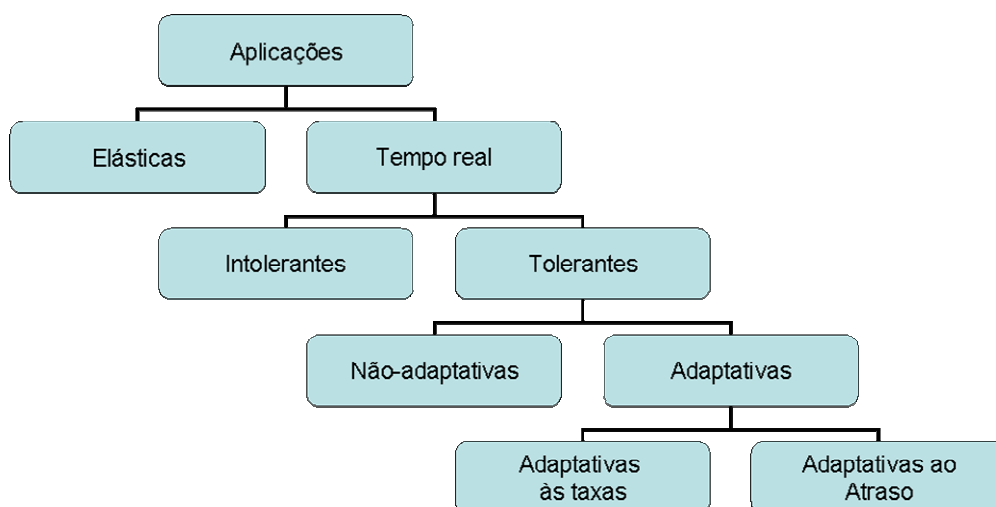


Figura 2-1 - Tipos de tráfego na Internet – Fonte: Peterson, L. L. & Davie, B. S., 1999

Os tráfegos de tempo real são considerados por alguns autores como uma categoria separada de tráfego inelástico, devido as suas exigências restritivas (Stallings, W., 2002).

Caso a aplicação utilize UDP, toda a capacidade disponível do enlace será utilizada, se a aplicação gerar os dados nessa taxa. No caso do TCP, a aplicação usará o enlace na taxa máxima disponível, até atingir a taxa que o receptor dos dados pode

aceitar. O tráfego das conexões individuais ajustam-se ao congestionamento, pela redução das taxas de inserção na rede. Este controle é efetuado por vários mecanismos do TCP, como RTT-backoff e partida lenta. Exemplos de protocolos da camada de aplicação que utilizam tráfegos elásticos são SMTP, FTP, SNMP, SSH, HTTP. Ainda que dentro da mesma categoria, tais protocolos possuem exigências diferentes de suporte da rede (Stallings, W., 2002):

-E-mail geralmente é insensível as alterações de atraso, mas exige confiabilidade

-Na transferência de arquivos, quando on-line, o usuário espera um tempo que seja proporcional ao tamanho do arquivo. Então, existe alguma sensibilidade a vazão/banda.

-Existe alguma sensibilidade ao atraso quando é necessária interatividade, como no HTTP e SSH/Telnet

Quadro 2-1 Suscetibilidade das aplicações em relação as métricas clássicas (considerando-se a confiabilidade como um reflexo das perdas) de QoS.

| Classe | Aplicações | Confiabilidade | Atraso | Jitter | banda |
|--------------------------|---------------------------|----------------|--------|--------|-------|
| Elásticas | Correio eletrônico | Alta | Baixa | Baixa | Baixa |
| | Transferência de arquivos | Alta | Baixa | Baixa | Média |
| | Acesso http | Alta | Média | Baixa | Média |
| | Login remoto | Alta | Média | Média | Baixa |
| Tempo real – Inelásticas | Áudio sob demanda | Baixa | Baixa | Alta | Media |
| | Video sob demanda | Baixa | Baixa | Alta | Alta |
| | Telefonia | Baixa | Alta | Alta | Baixa |
| | Videoconferência | Baixa | Alta | Alta | Alta |

Fonte: Adaptada de Tanenbaum, 2003.

O atraso percebido pelo usuário nos tráfegos elásticos é o tempo de transferência de um objeto da aplicação, e não as diferenças entre os tempos de pacotes. Devido aos controles do fluxo e congestionamento do TCP, não ocorrem grandes variações no atraso (Clark, D., 1995). Segundo o autor, quando se deparam com congestionamentos, tais controles permitem que o aumento do atraso percebido seja apenas modesto. O

usuário destas aplicações percebe o tempo dos elementos, que podem ser uma linha de comando, uma página da web. Para elementos muito pequenos, o tempo total é determinado pelo atraso em toda a Internet. Para elementos maiores, o tempo total é determinado pelas janelas deslizantes do TCP, ou seja, pela vazão encontrada pelas conexões do TCP. Portanto, nestes objetos maiores o tempo é proporcional ao tamanho e ao grau no qual a fonte fica mais lenta devido ao congestionamento.

2.1.2. Tráfegos Inelásticos

Os tráfegos inelásticos praticamente não se adaptam às flutuações de atraso e vazão da Internet (exemplos são os fluxos de voz e vídeo). Este tipo de tráfego é o que exige o controle das métricas de QoS (perdas, atraso, variação do atraso e vazão) para obter um desempenho satisfatório. Estes parâmetros são difíceis de se controlar no ambiente variável da Internet, com atrasos variáveis e perdas por congestionamento.

As aplicações que geram este tipo de tráfego precisam tratamentos especiais na rede, devendo conseguir isso antecipadamente, através do consumo de tempo extra para que alguma função reserve estes recursos, ou durante o fluxo, pelo meio dos campos do cabeçalho IP. Existem dúvidas sobre qual das abordagens é a mais eficaz, e ambas deram origem a arquiteturas diferentes para o tratamento de QoS. Tais arquiteturas (IntServ para a reserva e DiffServ para a marcação) serão discutidas no próximo capítulo.

2.1.3. Tráfego de tempo-real

Os requerimentos dos tráfegos de tempo real são diferentes daqueles tráfegos de alta-velocidade somente, fornecidos pelas redes locais atuais de alta capacidade. Com as aplicações em voga na Internet (usando HTTP, FTP, SMTP), as métricas mais importantes são a vazão e o atraso, e alguma preocupação com a confiabilidade. Além disso, alguns mecanismos foram adicionados para assegurar a ausência de perdas, erros e falta de ordenação dos pacotes. As aplicações de tempo real estão mais relacionadas a temporização (Stallings, W., 2002). Na maior parte dos casos, os dados devem ser entregues em taxas constantes e iguais às taxas com a qual estão sendo enviados pelo remetente (tráfego isócrono). Em outros casos, blocos de dados estão associados com deadlines, a partir das quais os dados não possuem utilidade.

Como exemplo, pode-se analisar uma aplicação de áudio que emite um pacote de 160 bytes a cada 20 ms. O computador que está recebendo os pacotes reproduz o

áudio em tempo real, assim que recebe os dados. Devido as diferenças nos atrasos (*jitter*) estes 20 ms entre cada pacote não são mantidos na recepção, sendo necessária a criação de um *buffer de jitter*. Este *buffer* não soluciona completamente o problema, pois gera também um atraso, e será discutido com mais detalhes na seção 3.4.1.

A comunicação de tempo real idealmente possui as seguintes características, algumas a serem providas pela rede (Stallings, W., 2002):

- *Jitter* baixo;
- Atraso baixo;
- Habilidade para integrar facilmente serviços de tempo real e tráfegos elásticos;
- Adaptáveis as condições dinâmicas da rede e do tráfego da rede;
- Bom desempenho em redes grandes e com muitas conexões;
- Requisitos baixos de *buffers* dos componentes de rede;
- Alta capacidade de utilização efetiva.

2.2. Histórico da convergência

O tráfego de voz sempre foi tratado em redes de telecomunicações, projetadas com paradigma totalmente diverso – complexidade na rede - das redes comutadas por pacotes – complexas nos terminais. Nos últimos anos, a importância das tecnologias de Qualidade de Serviço para as redes de comutação de pacotes cresceu rapidamente, e tornou-se atualmente uma das peças centrais das tecnologias de redes de dados.

Cada uma das duas redes iniciais foi projetada com objetivos claros de transportar um tipo específico de informação (Figura 2-2). As redes de telefonia, mais antigas, possuíam inicialmente um terminal que era um simples transdutor projetado para produzir uma corrente elétrica que flutuava com a pressão acústica do auto-falante. Para todos os propósitos práticos, esta era toda a funcionalidade deste dispositivo. A rede em si, por outro lado, era mais complexa que o terminal, e possuía a “inteligência” necessária para prover vários tipos de serviços de voz.

Uma conexão de telefone é dedicada a uma conversa durante todo o período. Quando uma conversa termina, os circuitos são usados para configurar outras chamadas. Os circuitos utilizados para configurar as chamadas são denominados “trancos”, em oposição aos “loops”, que são linhas dedicadas permanentemente a um usuário individual. No início das redes de telefonia, existiam duas medidas-chaves para a qualidade do serviço. A primeira era a possibilidade de bloqueio de uma chamada (call blocking), o que ocorria devido a indisponibilidade de circuitos nos trancos. Uma vez que uma tentativa de chamada obtivesse sucesso e a conexão fosse estabelecida, a próxima medida da qualidade era a qualidade da voz. Essa medida dependia da qualidade da transmissão, como perdas, ruídos, eco. Essas redes, portanto, eram projetadas com dois objetivos principais: A certeza de eliminar o call blocking ou reduzi-lo a patamares aceitáveis, como por exemplo 1%.

O segundo objetivo do projeto era uma rede fim-a-fim com o plano de transmissão otimizado para voz, de forma que os problemas de rede como perdas, ruídos, eco e atrasos fossem razoáveis. A voz é um serviço de tempo real, e não existiam filas nas redes originais para armazenar os sinais de voz e entregá-los mais tarde.

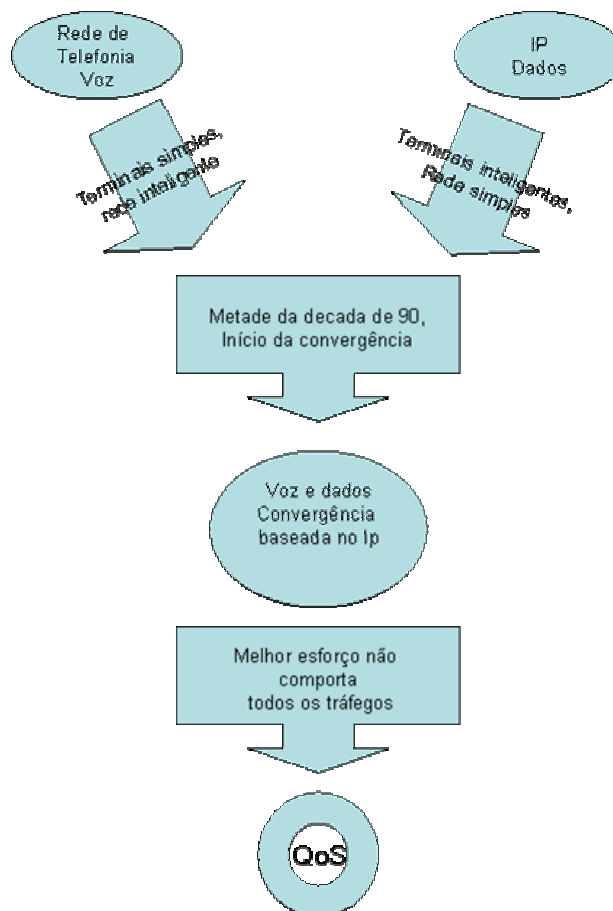


Figura 2-2 - Evolução das redes – fonte: (Park, K. I., 2005)

As redes IP originais eram um tipo de rede com outro paradigma. Ao contrário da voz, os tráfegos de dados são elásticos (Quadro 2-1), basicamente serviços tipo “não tempo-real”. Se os dados forem transmitidos com erro, podem ser retransmitidos. A filosofia do projeto das redes IP é a simplicidade da rede. A maior função da rede é retransmitir os pacotes de um nó até o outro. Todos os pacotes são tratados da mesma forma e armazenados em um *buffer* único, sendo retransmitidos em uma ordem *FIFO* (*First-in, First-out*). Neste tipo de rede, a maioria da inteligência foi centrada principalmente nos dispositivos terminais, os quais tipicamente são um computador. Tome-se como exemplo a comunicação entre os *hosts*, numa conexão virtual do TCP: A entrega de pacote com erros determina o não envio dos aceites desde o destinatário até o emissor, que irá dessa forma retransmitir o pacote. Toda essa capacidade de retransmitir os pacotes com erros foi colocada nos terminais. A rede ficou isenta deste controle.

O paradigma de projeto de rede simples foi possível devido a este tratamento único dos pacotes, no serviço denominado “*best effort*”, para tráfegos elásticos. O grande objetivo do projeto das redes IP era ter a certeza de que os terminais do usuário, com os protocolos adequados, garantiriam a confiabilidade, deixando a rede o mais simples possível.

Com essas características de tráfego diferentes, as duas redes desenvolveram-se separadamente, até que iniciaram uma conjunção, na metade dos anos 90. A palavra chave nessa época era a “convergência” de voz e dados. A idéia era criar uma rede única, que pudesse transportar os dois tipos de tráfego (elásticos e inelásticos). Nessa época a proposta mais destacada eram as redes ATM. Como visto no capítulo 1, as redes ATM tornaram-se complexas operacionalmente, e dispendiosas em termos de recursos. E a disseminação do IP tornou este protocolo o alvo da convergência. Com a pilha de protocolos da Internet, as operadoras de voz vislumbraram operações mais eficientes e econômicas. O desafio que emergiu dessa decisão é tornar viável os diversos perfis de tráfego, muitas vezes conflitantes, de forma a manter as exigências de desempenho de cada um. As técnicas de QoS parecem apontar para os caminhos mais viáveis. Porém, como será visto no capítulo 3, não existe consenso a respeito do uso de um ou outro recurso, método ou conceito.

Os aspectos comerciais e tecnológicos, em termos de novos produtos e especialistas também devem ser considerados. Avanços na tecnologia de voz “empacotada” (packetized voice) possibilitaram novos ambientes de rede (Caputo, R., 2000). Estes ambientes prometem redução de custos, flexibilidade e aplicações melhoradas para elevar a produtividade e a eficiência. Melhorias recentes no hardware e software, bem como nos projetos de protocolos impulsionam essa nova estrutura convergida. Toda essa tecnologia traz novos desafios operacionais e de gerência.

Algumas das maiores vantagens de usar-se a rede baseada no IP para transportar os fluxos de voz estão listadas a seguir (Caputo, R., 2000):

- Eficiência maior da multiplexação estatística sobre o TDM convencional;
- Eficiência melhorada com técnicas de compressão de voz e supressão do silêncio (detecção de atividade);
- Redução dos custos nas ligações pela distribuição das chamadas dentro das redes de dados privadas;
- Redução dos custos administrativos pela consolidação dos componentes de infra-estrutura;
- Possibilidade de novas aplicações integrando telefonia e computação;
- Conectividade de voz nas aplicações de dados (web, SQL);
- Maximização da estrutura da rede de dados;
- Redução dos custos de enlaces dedicados de voz;
- As novas tecnologias de dados (10Ge, DWDM) fornecem enlaces a custos menores que a conectividade TDM padrão;
- Integração com redes de vídeo, videoconferência no desktop, fax em tempo real são possibilidades atrativas para corporações geograficamente distribuídas.

2.3. Sistemas de comunicação digitais

Para se compreender as métricas de QoS necessárias aos fluxos de voz, são descritos alguns embasamentos a respeito dos sistemas de comunicação digitais, representados no diagrama da **Figura 2-3**.

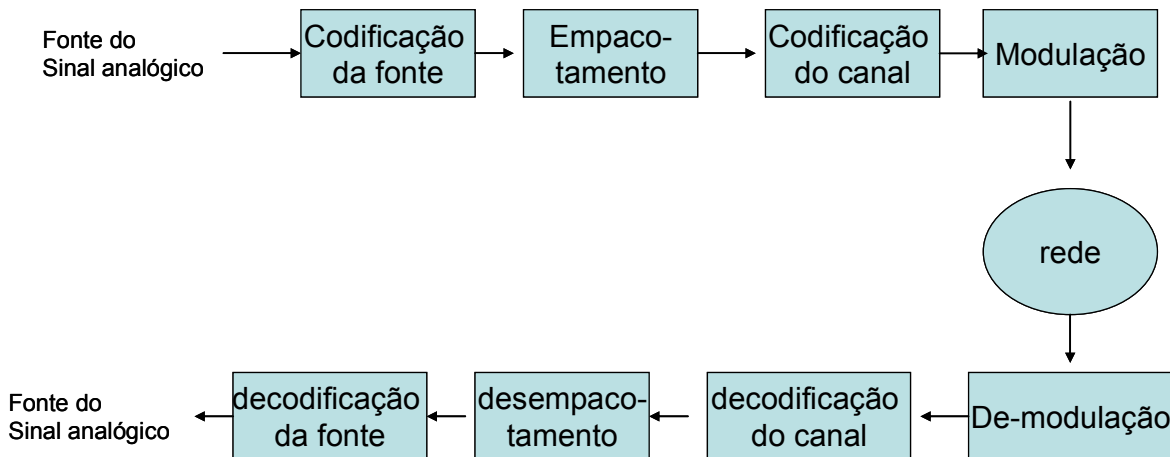


Figura 2-3 - Diagrama de blocos para os sistemas de comunicação digitais – Fonte: (Park, K. I., 2005).

Para transportar sinais analógicos, como voz e vídeo sobre as redes de pacotes, baseadas em sistemas digitais os sinais analógicos devem passar pelos seguintes processos, nas extremidades fonte e destino:

- Codificação/ decodificação da fonte;
- Empacotamento/desempacotamento;
- Codificação/decodificação do canal;
- Modulação/demodulação do sinal.

Uma rede comutadora de pacotes transportando voz pode ser representada como na **Figura 2-4**.

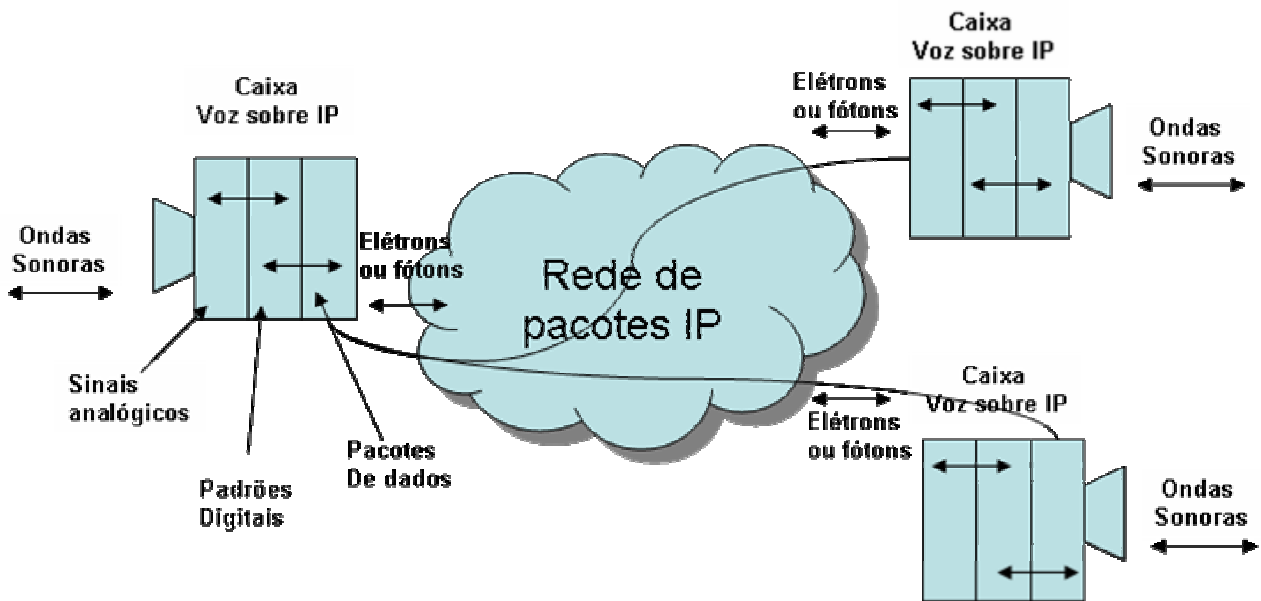


Figura 2-4 - Rede de voz sobre IP – Fonte: (Caputo, R., 2000)

2.3.1. Codificação da fonte

A codificação do sinal analógico em sinais digitais é o passo inicial para inserir os fluxos de voz em uma rede de dados. Este processo de digitalização do sinal da fonte é conhecido como “codificação da fonte”. No lado do destinatário, o processo inverso deve ocorrer, ou seja, a “decodificação da fonte”, que converte os sinais digitais nos correspondentes analógicos. O dispositivo que executa essas tarefas é denominado CODEC (codificador-decodificador).

O tipo de codificação da fonte vem sendo extensivamente pesquisado (Quadro 2-2) uma vez que influencia diretamente na qualidade da voz transportada, na taxa mínima do canal de voz e nos tempos de entrega do sinal (atrasos de codificação e congestionamentos devido as exigências de vazão).

Quadro 2-2- Padrões de CODEC do ITU-T

| Codificação | Padrão ITU-T | Taxa de bits, kbps | MOS | MIPS | Tamanho do quadro, (ms) | Atraso de Codificação (ms) |
|-------------|--------------|--------------------|------|------|-------------------------|----------------------------|
| PCM | G.711 | 64 | 4.1 | 0.34 | 0.125 | 0.75 |
| ADPCM | G.726 | 32 | 3.35 | 14 | 0.125 | 1 |
| LD-CELP | G.728 | 16 | 3.61 | 33 | 0.525 | 3-5 |
| CS-ACELP | G.729 | 8 | 3.92 | 20 | 10 | 10 |
| CS-ACELP | G.729a | 8 | 3.7 | 10.5 | 10 | 10 |
| MP-MLQ | G.723.1 | 6.3 | 3.9 | 16 | 30 | 30 |
| ACELP | G.723.1 | 5.3 | 3.65 | 16 | 30 | 30 |

Fonte:[ITU-T]

Existem dois tipos básicos de codificação da fonte: Codificação do formato da onda (*Waveform coding*) e codificação linear preditiva (LPC - *linear predictive coding*).

Uma descrição destes tipos está contemplada no Apêndice 2.

2.3.2. Empacotamento/desempacotamento

Uma vez digitalizada, a voz é transformada em um fluxo de bits, e torna-se uma forma de dados que a rede IP precisa transportar. Para isso, precisa ser empacotada. Nas redes de voz tradicionais, comutadas por circuitos a rede configura um circuito físico fim-a-fim, e transmite os sinais codificados. As redes IP não estabelecem estes circuitos, e as informações precisam ser colocadas em unidades de dados (PDUs – Protocol data units), que no caso do IP são denominados datagramas. O datagrama deve ser considerado como a informação contida no pacote IP (Hall, E., 2000). Como muitas vezes essa informação excede a MTU da camada de enlace (normalmente ethernet, MTU=1500 bytes), os datagramas devem ser fragmentados em pacotes. Cada fragmento de datagrama é um pacote IP. Além disso, os pacotes podem ser perdidos ou descartados. A informação original continua contida no datagrama.

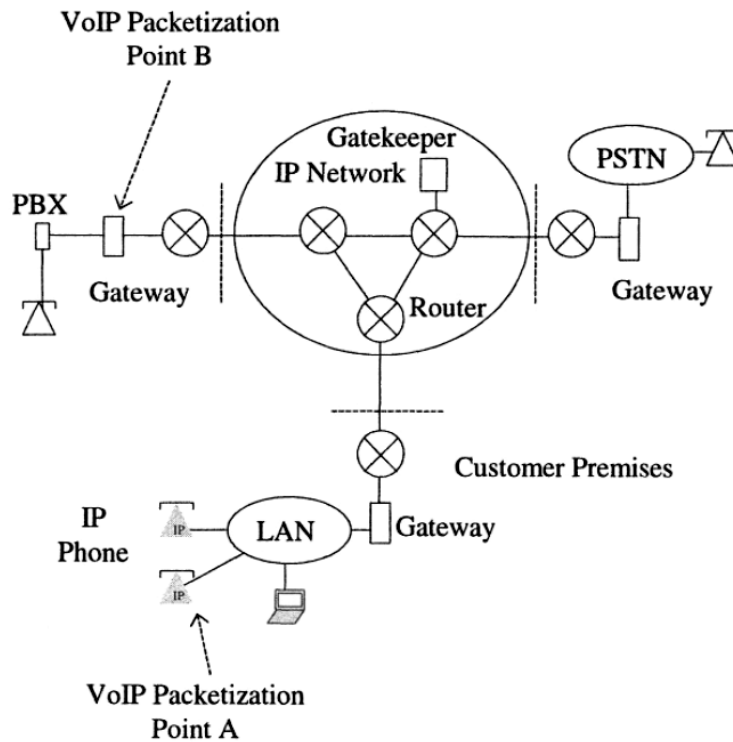


Figura 2-5 - Arquitetura de Voz sobre rede IP – VoIP – Fonte: Park, K. I., 2005

O empacotamento dos sinais de voz para uso do IP pode ser executado em dois pontos distintos da rede (pontos A e B na Figura 2-5). No ponto A, o próprio telefone do usuário possui este recurso. No ponto B, um gateway entre as redes de telefonia e IP executa a tarefa.

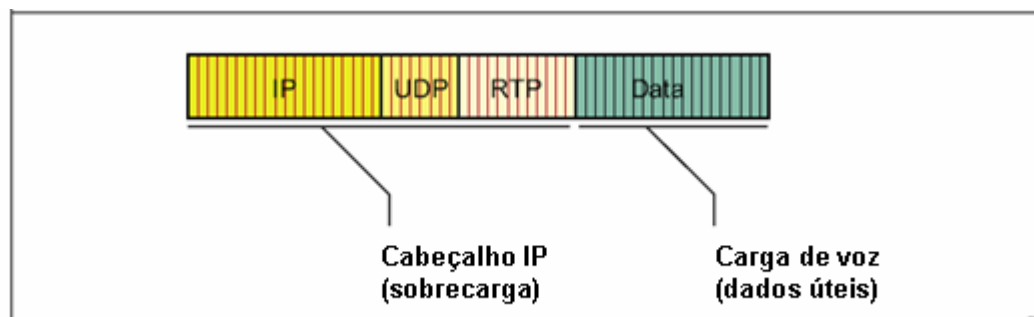


Figura 2-6 - Empacotamento dos frames de voz no segmento UDP e datagrama IP – Fonte: Newport Networks

A escolha do número de frames amostrados para encapsular em um pacote de dados é um compromisso entre atraso e sobrecarga. Períodos de amostragem longos, com muitos frames produzem atrasos também longos, o que pode afetar a qualidade da conversação (Hersent, O.; Gurle, D. & Petit, J. P., 2000). Com base nessa questão,

quanto menor o período de amostragem, melhor a qualidade da voz percebida. O contraponto é o aumento da sobrecarga dos cabeçalhos para os pacotes muito pequenos. Para os pacotes menores, pode-se ter metade da banda consumida pelo cabeçalho.

Os frames de voz são encapsulados nos segmentos RTP (12 bytes de cabeçalho), UDP (8 bytes de cabeçalho) antes de serem inseridos no datagrama IP (20 bytes de cabeçalho), como pode ser observado na Figura 2-6. Pelo uso dos cabeçalhos, a sobrecarga para os frames deve ser de 40 bytes (RTP/UDP/IP). Este custo é necessário, pois os protocolos têm funções bem definidas no processo de entrega dos pacotes:

- RTP (Real Time Protocol): Verifica as medidas de atraso e *jitter*,
- UDP – Estabelece o fluxo do transporte porta a porta entre os *hosts*;
- IP – Realiza o encaminhamento ao *host* de destino.

A carga útil gerada pelo CODEC G.711 no período de 20 ms de amostragem é de 160 octetos. Somados com os 40 dos cabeçalhos RTP/UDP/IP, significam 200 octetos ou 1600 bits transmitidos 50 vezes em um segundo, o que gera uma banda necessária de 80.000 bits por segundo. Ainda não foram considerados os bits de controle na camada de enlace (Ethernet e PPP são os enlaces utilizados neste trabalho de pesquisa – como descrito na seção 5.4). No caso dos enlaces PPP, é possível se utilizar compressão do RTP (cRTP) (Wisely, D.; Eardley, P. & Burness, L., 2002), o que possibilitaria redução da sobrecarga de 40 para 4 ou até 2 octetos. Embora não seja comum ainda, o uso do cRTP será difundido nas redes móveis 3G. O cRTP está descrito na RFC 2508, de 1999 (*Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*). O uso do cRTP em links PPP de grande atraso e altas taxas de perdas foi especificado na RFC 3545, de 2003 (*Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering*).

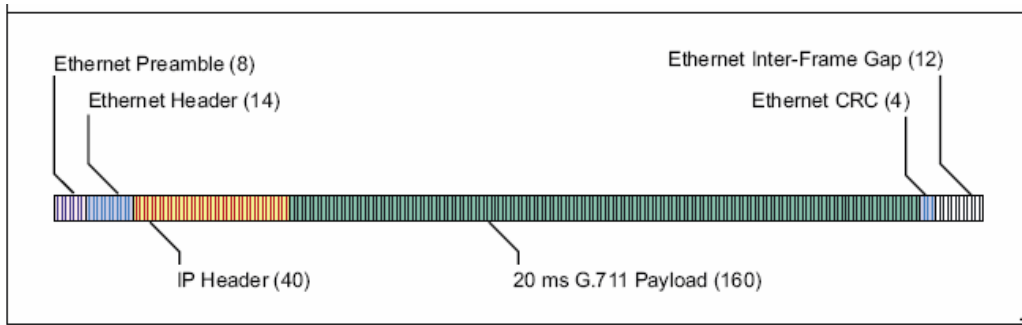


Figura 2-7 - Empacotamento G.711+RTP/UDP/IP+Ethernet

A compressão dos cabeçalhos IP/UDP/RTP em um pacote cRTP pode reduzir com eficiência a requisição de banda, pois os cabeçalhos deixam de ocupar 40 bytes para ocupar somente 2 (sem checksum) ou 4 (com checksum) - Figura 2-8.

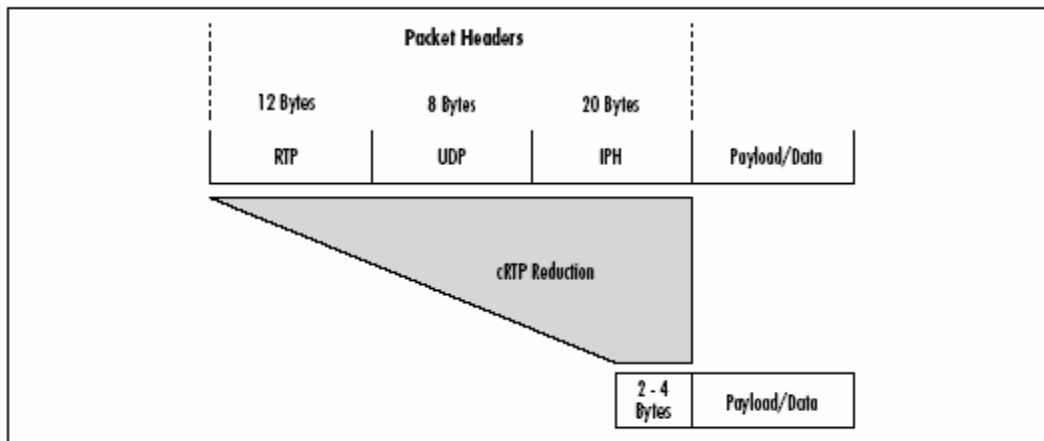


Figura 2-8 - Cabeçalhos RTP comprimidos. Fonte: Caputo, R., 2000.

Na Figura 2-9 está representado o processo de enfileiramento dos pacotes cRTP. A entrada na fila é anterior a compressão. O dispositivo determina quais pacotes são RTP, e encaminha para a compressão. A seguir, todos os pacotes passam para a interface de saída.

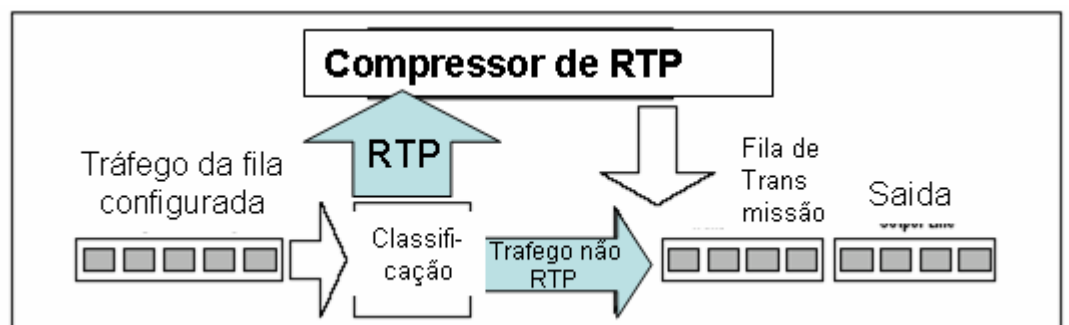


Figura 2-9 - Compressão e enfileiramento dos pacotes RTP

Empacotamento na camada de enlace

Neste trabalho, duas tecnologias são utilizadas para encapsular os datagramas: Fast-ethernet nas interfaces de LAN e PPP para as interfaces WAN. No caso dos frames ethernet/fast-ethernet, a sobrecarga dos cabeçalhos fica em 8 octetos de preambulo, mais seis de endereço destino, seis de endereço fonte, 2 octetos para o tamanho da unidade de dados e 4 de detecção de erros. Somados com 12 octetos de espacamento entre os frames, o total é de 38 octetos. A carga gerada pelo CODEC é de $64000/50 = 160$ octetos. Somados com os 40 octetos dos os cabeçalhos RTP/UDP/IP, enviados 50 vezes por segundo, totaliza uma banda necessária de $(160+40+38) \times 50 \times 8 = 95.200$ bits por segundo (Figura 2-7).

Se a codificação utilizada for G.729a, a banda necessária é menor. Um pacote é emitido a cada 20ms, ou 50 a cada segundo. O fluxo é de 8Kbps, ao invés de 64Kbps do G.711. A carga é de $8000/50 = 160$ bits, ou 20 octetos. Somados aos 40 dos cabeçalhos RTP/UDP/IP e 38 do ethernet, tem-se 98 octetos. A banda necessária para o fluxo de voz é de $98 \times 50 \times 8 = 39.200$ bits por segundo. As necessidades de banda para outros codificadores utilizando as mesmas tecnologias de camada 4, 3 e 2 podem ser observadas no Quadro 2-3.

As técnicas de supressão do silêncio (VAD – Voice Activity Detection) podem reduzir a demanda em até 50%, uma vez que normalmente somente uma das extremidades da conexão está sinalizando o canal, enquanto a outra ouve.

Quadro 2-3 Taxa necessária para encapsular fluxos de voz em frames ethernet

| Codec | Bandwidth | Sample period | Framesize | Frames/ Ethernet Bandwidth packet | |
|------------------------|-----------|---------------|-----------|-----------------------------------|-----------|
| G.711 (PCM) | 64 kbps | 20 ms | 160 | 1 | 95.2 kbps |
| G.723.1A (ACELP) | 5.3 kbps | 30 ms | 20 | 1 | 26.1 kbps |
| G.723.1A (MP-MLQ) | 6.4 kbps | 30 ms | 24 | 1 | 27.2 kbps |
| G.726 (ADPCM) | 32 kbps | 20 ms | 80 | 1 | 63.2 kbps |
| G.728 (LD-CELP) | 16 kbps | 2.5 ms | 5 | 4 | 78.4 kbps |
| G.729a (CS-CELP) | 8 kbps | 10 ms | 10 | 2 | 39.2 kbps |
| AMR (ACELP) | 4.75 kbps | 20 ms | 12 | 1 | 36.0 kbps |
| AMR (ACELP) | 7.4 kbps | 20 ms | 19 | 1 | 38.8 kbps |
| AMR (ACELP) | 12.2 kbps | 20 ms | 31 | 1 | 43.6 kbps |
| AMR-WB/G.722.2 (ACELP) | 6.6 kbps | 20 ms | 17 | 1 | 38.0 kbps |

Quando a camada de enlace utiliza PPP como protocolo, as taxas necessárias devem considerar o cabeçalho de 6 octetos, totalizando (para CODEC G.729a):

Carga=8000/50 = 160 bits (20 octetos)

Cabeçalhos RTP/UDP/IP = 40 octetos

Cabeçalho PPP = 6 octetos

Total = 66 octetos

Essa carga deve ser enviada 50 vezes por segundo, totalizando $50 \times 8 \times 66 = 27600$ bits por segundo, ou 26.4 Kbps. Pode-se perceber que a taxa fica como a calculada por (Caputo, R., 2000), próxima da necessária usando-se a codificação G.723.1A (MP-MLQ) sobre ethernet, que precisa de 27.2 Kbps. Neste trabalho de pesquisa, a taxa de 26.4 kbps será considerada a necessária para fluxos de voz. Os experimentos deste trabalho- capítulo 6-são baseados nessa necessidade, uma vez que os enlaces PPP possuem as maiores restrições de banda no ambiente de estudos (128 Kbps).

Quadro 2-4 - Cálculo da banda necessária para os diferentes CODECs

| Voice Compression Algorithm | Payload Size, bytes* | Packet Size w/o CRTP, bytes [†] | Packetization Overhead, % | Total Bandwidth Requirements, kbps |
|-----------------------------|----------------------|--|---------------------------|------------------------------------|
| G.723.1 MP-MLQ | 30 | 76 | 153 | 20.3 |
| G.729 CS-ACELP | 20 | 66 | 230 | 26.4 |
| G.726 ADPCM | 80 | 126 | 57.5 | 50.4 |
| G.711 PCM | 160 | 206 | 28.8 | 82.4 |

*Per packet.

[†]Including G-byte data-link header.

Fonte: Caputo, R., 2000

2.4. Sumário do Capítulo

Neste capítulo, foram analisadas as condições dos tráfegos na Internet atualmente, especialmente os fluxos de voz. Foi abordada a classificação dos tráfegos em tráfegos elásticos e inelásticos, bem como os tráfegos de tempo real. A seguir, tratou-se da convergência das redes em direção ao protocolo IP, e analisaram-se as condições de inserção dos pacotes de voz nas redes de dados. Os sistemas de codificação e os tamanhos dos pacotes gerados, bem como as necessidades de banda de cada técnica também são discutidas.

A análise demonstra que os tráfegos inelásticos, como os fluxos de voz, exigem que as redes possuam técnicas mais eficientes que o clássico serviço *best effort*. Tais técnicas necessitam gerenciamento dos recursos e controle sobre as conexões de rede, o que pode ser obtido através da criação de um plano de controle, como o proposto neste estudo, para as redes de próxima geração.

No próximo capítulo, serão analisadas os principais mecanismos de manutenção das métricas de qualidade nas redes convergidas. Para isso, é realizada uma revisão dos conceitos de Qualidade de Serviços, com base nos principais órgãos de padronização. As disciplinas de enfileiramento e as métricas de QoS importantes para os fluxos de voz são discutidas em detalhes.

3. Qualidade de Serviço

Este capítulo apresenta um breve histórico das técnicas utilizadas para manter um certo equilíbrio nos recursos utilizados na Internet, na tentativa de evitar problemas como congestionamentos e perdas de pacotes. Uma definição de Qualidade de serviço é apresentada, bem como um detalhamento das principais métricas atualmente utilizadas como parâmetro de qualidade (perdas, atraso, variação do atraso e vazão). A seguir, algumas técnicas de tratamento de filas e as arquiteturas atuais de serviços integrados e diferenciados são descritas brevemente.

3.1. Histórico

A qualidade de serviço nas redes IP já foi prevista pelos fundadores do protocolo, provendo o campo de “Tipo de Serviço” – ToS – no cabeçalho, o que facilitaria a utilização da marcação de pacotes pelos serviços diferenciados. A especificação inicial para o campo ToS (composto por um byte no cabeçalho IP) é a seguinte (RFC 791):

“O tipo de serviço fornece uma indicação de parâmetros abstratos da qualidade de serviço desejada. Os parâmetros são usados para embasamento da seleção dos parâmetros de serviço na transmissão de datagramas por uma rede”.

Durante o período da Internet não comercial, o uso do ToS no cabeçalho do IP foi ignorado, uma vez que as exigências acadêmicas da rede eram supridas satisfatoriamente. Praticamente todas as aplicações ignoravam o byte ToS do cabeçalho. Os roteadores também não usavam o campo para determinar tratamentos diferenciados.

As funções iniciais de QoS voltaram-se para os *hosts*. Inicialmente, um problema grande para os enlaces WAN eram os segmentos TCP de tamanho pequeno, que geravam *overhead* excessivo nos enlaces (Vegesna, S., 2001). O algoritmo de Nagle (Nagle, J., 1984), o qual resolve este problema, é suportado por todas as implementações do IP nos *hosts*. O algoritmo de Nagle pode ser considerado o marco

inicial das funcionalidades de QoS no protocolo IP. Em 1986, Van Jacobson desenvolveu o conjunto de mecanismos para evitar congestionamentos nos sistemas finais, implementado atualmente no TCP (partida lenta e prevenção ao congestionamento). Estes mecanismos podem ser considerados o segundo conjunto de ferramentas de QoS para Internet.

Adicionalmente, foram implantados em 1990 a retransmissão rápida a recuperação rápida, para fornecer desempenho otimizado durante os períodos de perdas de pacotes. Estes recursos adicionais melhoraram bastante o desempenho das redes IP, mas foi necessário focar os roteadores para que a QoS pudesse ser vista como solução fim-a-fim. Inicialmente as filas dos roteadores eram do tipo FIFO, causando descartes na cauda (tail drop), o que não protegia as aplicações bem comportadas. As filas *Weighted Fair Queuing (WFQ)*, baseadas num algoritmo de escalonamento (seção 3.5.1) são amplamente utilizadas na Internet para suprir essa necessidade de proteção para as aplicações que não são grandes consumidoras de banda. O desenvolvimento da QoS continuou com o a criação das arquiteturas de serviços integrados e de serviços diferenciados, pelo IETF, por meio de seus grupos de trabalho.

3.2. Definições de QoS

O conceito é complexo, e sempre será relacionado com expectativas e percepções tão divergentes quanto as do provedor de serviços e do usuário, e mesmo sob a perspectiva das aplicações, que possuem diferentes tipos de sensibilidades às alterações das variáveis de tráfego .

a) Na área de redes, o termo é usado para definir a habilidade da rede em prover diferentes níveis de garantias de serviços para os diferentes perfis de tráfego. A QoS possibilita ao administrador designar prioridades de algum tráfego sobre os demais (Flanagan, M. E. (ed), 2001).

b) O termo “qualidade” traz uma série de significados que tendem a apontar para várias direções simultaneamente. Isso é, sempre vai depender da perspectiva, a lente pela qual tentamos focar o assunto. Sob a ótica do usuário, qualidade de um serviço é

uma indicação de quanto um serviço é bom. E normalmente é dimensionado no singular, como sinônimo de “excelência”, ou “grau”. Na verdade, o termo qualidade é multidimensional, pois são muitos os fatores que irão determinar o nível de QoS percebido pelo usuário (**Hardy, W. C., 2001**). Essa quantidade de fatores diz respeito a percepção do usuário e as variáveis do serviço que está sendo avaliado.

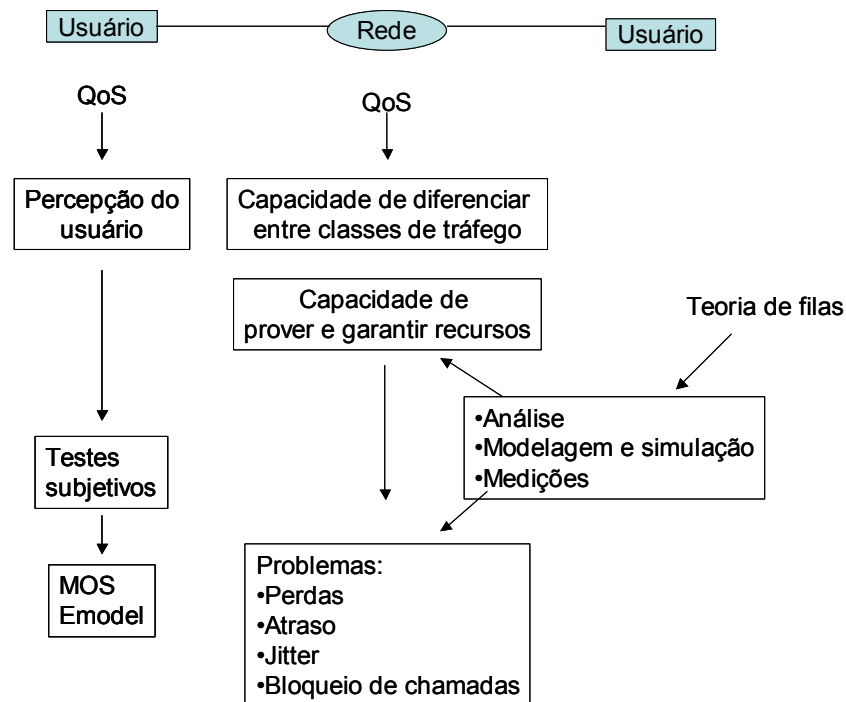


Figura 3-1- Diagrama de interações dos conceitos de QoS - Usuário e rede – Fonte: **Park, K. I., 2005** – Adaptado.

c) A definição do ITU-T (International Telecommunication Union’s – Telecommunications section) segundo a especificação E.800 e G.1000 designa que QoS é o “efeito coletivo do desempenho dos serviços”, o qual determina o grau de satisfação do usuário.

d) Segundo a definição do IETF (RFC 2386 – **Crawley, E.; Nair, R.; Rajagopalan, B.& Sandick, H., 1998**) Qualidade de Serviço é “um conjunto de requerimentos de serviços a serem alcançados pela rede, enquanto transporta um fluxo”.

A questão é que são muitos os atributos que podem formatar a percepção de qualidade. Além disso, os atributos são independentes, de forma que não adianta tentar ofuscar a inabilidade em tratar um deles, apenas excedendo a expectativa do usuário em outros. Em termos práticos, significa que medir QoS de forma efetiva envolve medir um conjunto de parâmetros, com relações complexas entre as funções da rede e percepções do usuário (Figura 3-1). Portanto, não pode-se afirmar existir uma medida única de QoS.

3.3. Definições de serviços

Na Internet, a definição de serviço é em geral um problema difícil (RFC 3052 - **Eder, M. & Nag, S., 2001**). As características de Internet como um ambiente de padrões abertos torna possível o desenvolvimento de serviços com uma liberdade muito maior que no ambiente das redes de telefonia (Intelligence Networks - IN). O framework SIP (Session Initiation Protocol) do Internet Engineering Task Force (IETF), por exemplo, fornece a matéria prima para os serviços de alcançabilidade e identificação. Em conjunto com o Session Description Protocol (SDP) torna possível sinalizar os requerimentos da aplicação entre as duas extremidades da comunicação. Uma consequência prática destes fatos é que a idéia de padronizar serviços não é válida - RFC3052 (**Eder, M. & Nag, S., 2001**).

Pode-se, entretanto, adotar uma visão mais ampla e classificar os serviços. Na indústria de telecomunicações, existe grande experiência em implementar serviços. A razão básica para isso é que nas redes de telefonia as garantias de serviços são promovidas pela própria rede, enquanto os terminais (telefones) são relativamente simples. Como existem muitos operadores comerciais, foi necessária a definição precisa dos requerimentos para prover QoS fim-a-fim.

Além disso, a implementação dos serviços de telefonia móvel requer uma definição muito sofisticada das requisições de QoS. Por essa razão, os serviços de telecom são usados como referência e ponto de comparação para a Internet atual.

Segundo o paradigma de Redes Inteligentes, o sistema de telefonia pública (POTS) permitiu a criação de novos serviços no mundo da telefonia de comutação de circuitos. Através das IN (*intelligent Networks*) foi possível adicionar serviços a telefonia de voz original, como a busca automática (*call forwarding*), caixa-postal de voz, e identificador de chamadas.

Serviço – Um serviço de telecomunicações é um conjunto de funções independentes que são uma parte integral de um ou mais processos de negócios. Este conjunto funcional consiste de componentes de *hardware* e *software*, bem como o sistema de comunicações subjacente.

O ITU-T define uma grande lista de tipos de serviços de Internet na especificação G.1010 (Quadro 3-1). Na especificação Y.1541, existe um resumo da classificação para QoS sobre IP (Quadro 3-2). Essas classes relacionam-se com as aplicações do Quadro 3-3. onde as aplicações mais exigentes (Voz e Vídeo) pertencem a classe de QoS 0, onde os atrasos devem ficar em torno de 100 ms.

Quadro 3-1 Classes de atrasos para os serviços de Internet

| Parâmetro de desempenho | Natureza do objetivo do desempenho | Classe 0 | Classe 1 | Classe 2 | Classe 3 | Classe 4 | Classe 5 |
|-------------------------|------------------------------------|----------|----------|----------|----------|----------|----------|
| IPTD | Porção superior da média | 100 ms | 400 ms | 100 ms | 400 ms | 1 s | U |

Fonte: ITU-T – Especificação Y.1541

Quadro 3-2 - Classes de QoS e as aplicações

| Classe de QoS | Aplicações |
|---------------|--|
| 0 | Tempo real, sensíveis ao <i>jitter</i> , alta interatividade (VoIP, VTC) |
| 1 | Tempo real, sensíveis ao <i>jitter</i> , interatividade (VoIP, VTC) |
| 2 | Dados transacionais, altamente interativos (sinalização) |
| 3 | Dados transacionais, interativos |
| 4 | Apenas pequenas pedas (transações curtas, dados, fluxos de vídeo) |
| 5 | Aplicações tradicionais das redes IP padrão |

Fonte: ITU-T – Especificação Y.1541

Genericamente, pode-se dividir os serviços atuais da Internet em 3 grupos – (Raisanen, V., 2003) :

a) Entrega de conteúdo em tempo-real, como áudio ou vídeo. Isso inclui:

- conferência (bidirecional, com interatividade) ;
- conteúdo de stream, armazenado, unidirecional ou sem interação.

b) Entrega de conteúdo tipo dados, como e-mail.

Aplicações cliente-servidor com interatividade. Essa categoria inclui navegação e mensagens envolvendo um servidor de rede. Existem muitos graus de urgência nessa categoria, variando desde navegação web até controle remoto de máquinas em tempo real.

c) Serviços iniciados pelo servidor - Server-initiated services. Essa categoria inclui serviços “não solicitados” como o recebimento de avisos. Embora o conteúdo atual possa ser classificado como data-type ou real-time type discutidos acima, essa categoria é separada pelo fato de não ser solicitada pelo terminal.

Um resumo (não criterioso) dos tipos mais comuns de conteúdo que podem ser entregues pela Internet atualmente pode ser encontrado no Quadro 3-3. A natureza diversa destes tipos de serviços acarreta em necessidades diferentes de suporte para a QoS na Internet.

Quadro 3-3 Tipos de serviços mais comuns atualmente na Internet

| Serviço de Internet | Requisição/ resposta? | Tempo de entrega do conteúdo | Conteúdo contínuo? |
|---------------------------------------|-----------------------|------------------------------|--------------------|
| E-mail | Não | Não crítico | Não |
| Página HTTP | Sim | Interatividade requerida | Não |
| Conteúdo <i>streamed</i> | Sim | Médio | Sim |
| Mensagens/chat | Sim | Interatividade requerida | Não |
| <i>Download</i> de arquivos de música | Sim | Não crítico | Não |
| Anúncios tipo “ <i>push</i> ” | Não | Não aplicável | Não |
| Conversações <i>multimídia</i> | Não | Pequeno | Sim |

Fonte: (ITU-G .1010)

Os dados do Quadro 3-1 podem ser visualizados graficamente na Figura 3-2, relacionados aos serviços de voz.

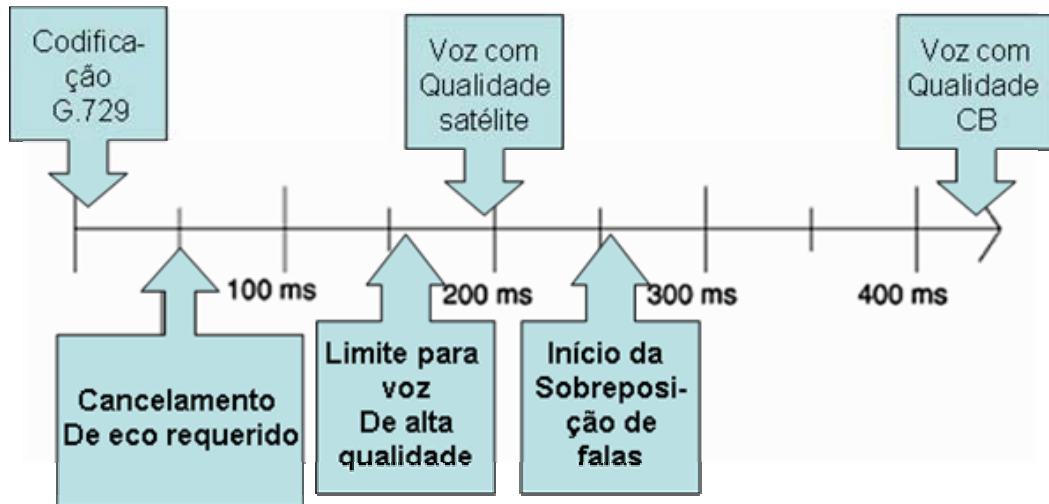


Figura 3-2 - Linha de tempo para o atraso nos serviços de voz – Fonte: Raisanen, V., 2003

O TIPHON - *Telecommunications and Internet Protocol Harmonization Over Networks* - do instituto ETSI (*European Telecommunications Standards Institute*) possui uma separação dos parâmetros de QoS baseado em 3 camadas, denominado por alguns autores (Raisanen, V., 2003) “TIPHON QoS model”, embora a organização denomine apenas de parâmetros de QoS (TIPHON, 2002-1).

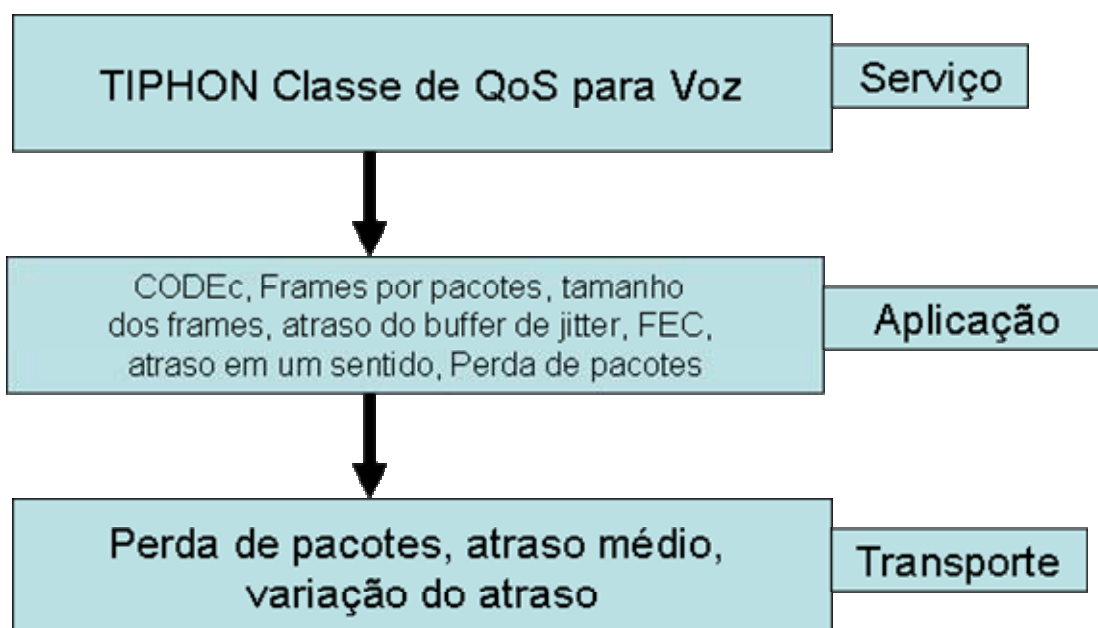


Figura 3-3 - TIPHON – Parâmetros de QoS - Fonte: (TIPHON, 2002-1)

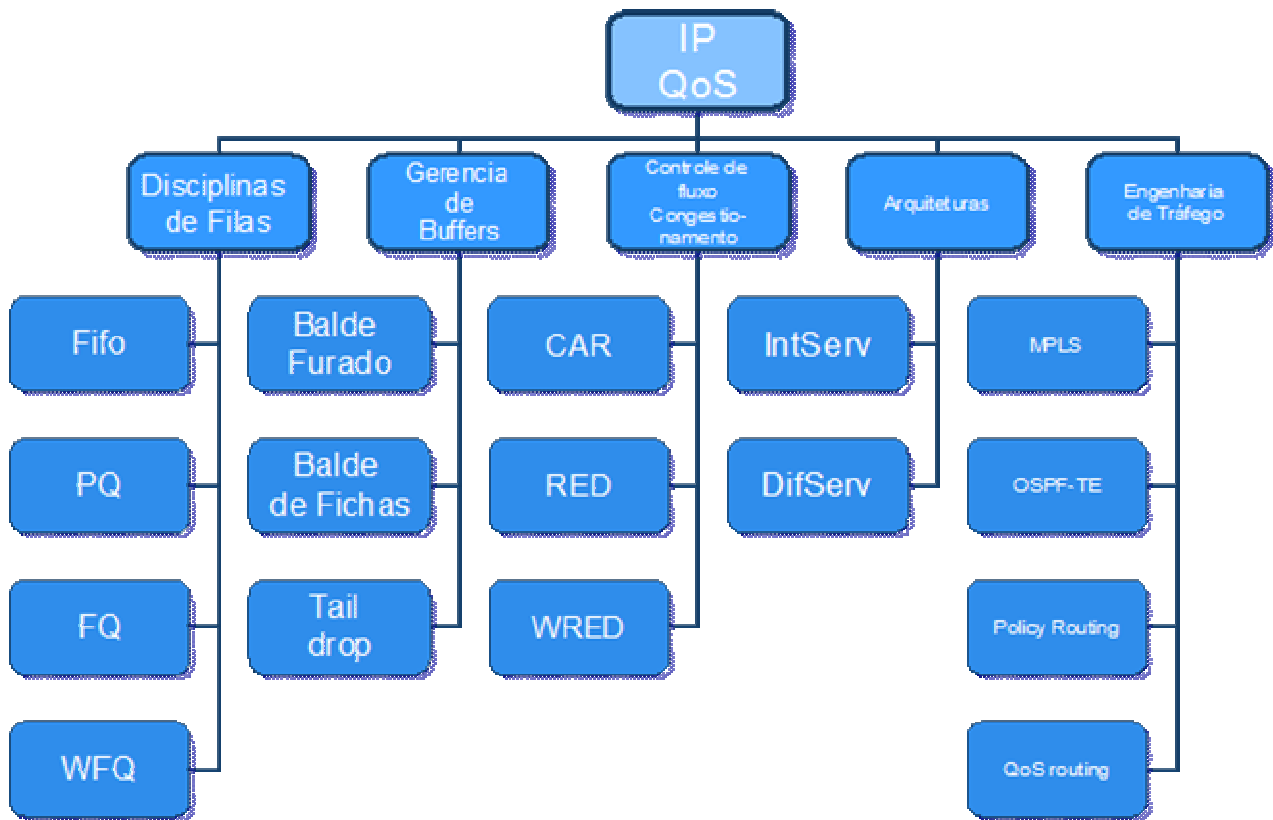


Figura 3-4 - Estruturas e tecnologias auxiliares para prover QoS em redes IP

3.4. Métricas de QoS

A entrega dos pacotes nas redes comutadas exige alguns limites nas métricas que comumente são ignoradas para os tráfegos elásticos. Este tópico analisa as quatro métricas mais aceitas como índices de Qualidade de Serviço nas redes de comutação de pacotes: Atraso, variação do atraso (*jitter*), perdas e vazão (Vegesna, S., 2001), algumas vezes medida como largura de banda residual. Para os fluxos de voz, especificamente, tem-se ainda alguns fatores que afetam a qualidade percebida pelo usuário, independentes da rede de comutação: o call blocking, controle de eco e a escolha do CODEC (Park, K. I., 2005).

Dentro dos serviços de telefonia IP, a classe de serviço de QoS é subjetiva, e determinada por um grande número de parâmetros de engenharia, entre os quais fazem parte (TIPHON, 2002-1):

- Equipamento do usuário;
- Equipamento da rede;
- Desempenho da rede em si.

Como exemplo de tais parâmetros, pode-se citar a escolha do CODEC, a aplicação de técnicas de correção de erro, o algoritmo de empacotamento utilizado, o tamanho do frame gerado pelo CODEC, os algoritmos utilizados para tratar a variação do atraso na recepção, o atraso gerado pelos *buffers de jitter (dejittering delay)*, cancelamento de erros pelo decodificador e atrasos de processamento pelo equipamento. No nível de aplicação, os acordos de QoS devem relacionar os equipamentos de usuário e dos provedores de serviço. Na prática, a maior parte destes parâmetros são determinadas pelo equipamento do usuário. Além deles, o controle de QoS fim-a-fim irá reduzir a necessidade de monitorar um número reduzido de parâmetros:

- Atraso máximo fim-a-fim;
- Variação máxima do atraso fim-a-fim;
- Perda máxima de pacotes.

Segundo o TIPHON, o controle fim-a-fim destes parâmetros é necessário e suficiente para garantir qualidade de voz através de um determinado caminho. Quando múltiplos domínios da rede de transporte forem envolvidos em uma chamada, o conjunto de parâmetros deve ser especificado e controlado em cada domínio. A QoS alcançada pela aplicação irá depender fundamentalmente do desempenho da rede de transporte nas camadas inferiores, as quais suportam o serviço de telefonia IP. Neste plano de transporte, portanto, o atraso médio fim-a-fim, a variação do atraso e a perda de pacotes devem ser controladas (TIPHON, 2002-1).

3.4.1. Atraso

Atraso nas redes de pacotes é considerado o tempo transcorrido desde o envio do pacote pela origem até o recebimento no destino. O atraso nos pacotes, também

chamado de latência, têm várias fontes, e normalmente elas são estudadas em separado. O atraso afeta primariamente os fluxos de voz e vídeo (tráfegos inelásticos).

O atraso pode ser medido nos dois sentidos da comunicação (Atraso round-trip, RFC 2681) ou em um sentido somente (one-way, RFC 2679).

O atraso num sentido possui um limite máximo e um mínimo. O atraso máximo é limitado pelo tempo após o qual o pacote é considerado perdido (Almes, G.; Kalidindi, S. & Zekauskas, 1999). E o mínimo é dado pela soma dos atrasos de propagação, transmissão e processamento nos nós de comutação, considerando que os outros atrasos – como o de filas – podem ser nulos.

Para os fluxos de voz, pode-se considerar importantes os seguintes atrasos (Vegesna, S., 2001), (Park, K. I., 2005):

- Atraso de enfileiramento;
- Atraso de propagação;
- Atraso de transmissão ou serialização;
- Atraso de processamento (ou comutação);
- Atrasos devido a codificação da fonte;
- Atraso devido ao empacotamento;
- Atraso da codificação do canal (entrelaçamento e correção de erros);
- Atraso devido ao *buffer anti-jitter*.

As influências da codificação da fonte, do canal, empacotamento e do *buffer anti-jitter* são devidas ao CODEC, e as três primeiras já foram analisadas no capítulo 2.3. Os demais tipos de atraso (exceção ao *buffer anti-jitter*) são devidos as redes de pacotes, e serão discutidos a seguir.

Atraso devido ao *buffer anti-jitter*

Seja t_{AB} o tempo que um pacote IP necessita para percorrer o caminho entre A e B. Este período é determinado pelos instantes $t_{chegada_destino} - t_{saida_origem}$. O retardo é composto por uma parte fixa, determinada pelo atraso de propagação, e uma porção variável, caracterizando o *jitter* (Hersent, O.; Gurle, D. & Petit, J. P., 2000). Tal variação é

causada pelo tamanho inconstante das filas, alterações nos padrões de tráfego nos enlaces e outros fatores, como retransmissões.

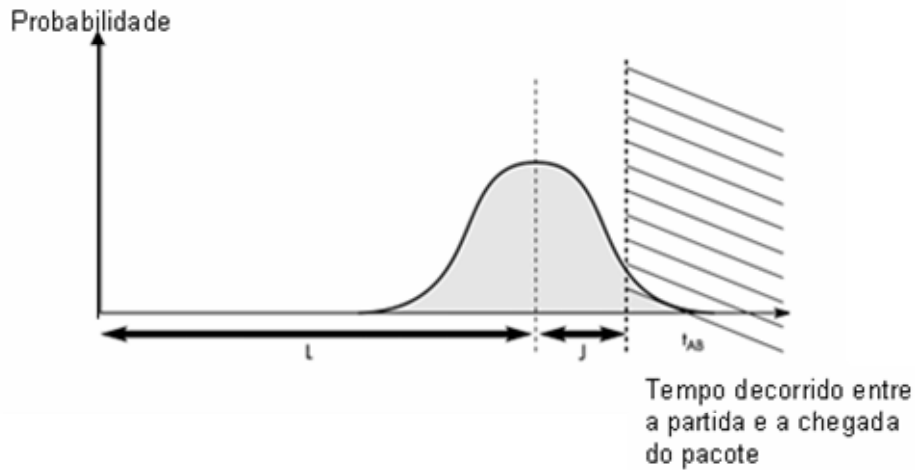


Figura 3-5 - Atraso em redes de pacotes – Fonte: (Hersent, O.; Gurle, D. & Petit, J. P., 2000)

Os equipamentos terminais utilizam o *buffer* de *jitter* para minimizar os efeitos do *jitter*. Este *buffer* mantém os pacotes na memória até que

$$T_{\text{buffer}} - T_{\text{saida_origem}} = L + J$$

A situação do atraso está representada na Figura 3-5. L representa o atraso de propagação somado ao atraso médio das filas, e aqui considerado como uma parte fixa do atraso para um dado percurso. J representa a parte variável do atraso inserida pelos *buffers* de *jitter* (Figura 3-6).

O tempo de saída de cada pacote é determinado usando-se o *timestamp* do cabeçalho do RTP. Pelo aumento do valor de J, o terminal consegue re-sincronizar mais pacotes. Os pacotes que chegarem muito tarde ($T_{\text{chegada}} > T_{\text{buffer}}$) são descartados.

Os terminais utilizam técnicas eurísticas para ajustar J ao melhor valor. Se J é muito pequeno, muitos pacotes serão descartados. Se muito grande, o atraso adicional pode ser inaceitável para o usuário. Para alguns terminais a configuração do *buffer* de *jitter* é estática. Essa abordagem não é a melhor quando as condições da rede são instáveis. Outros equipamentos podem ajustar dinamicamente seus *buffers* de *jitter*, usando

técnicas heurísticas. Tais abordagens podem demandar algum tempo, pois o terminal precisa analisar as condições da rede para avaliar o *jitter*. Pode iniciar com um *buffer* muito pequeno e progressivamente aumentar, até que o percentual de perdas fique abaixo de 1%. Essa situação está representada também na Figura 3-7, onde o tempo de permanência no *buffer* varia para que as diferenças entre a saída da origem e a saída do *buffer* sejam constantes (linhas paralelas na Figura 3-6).

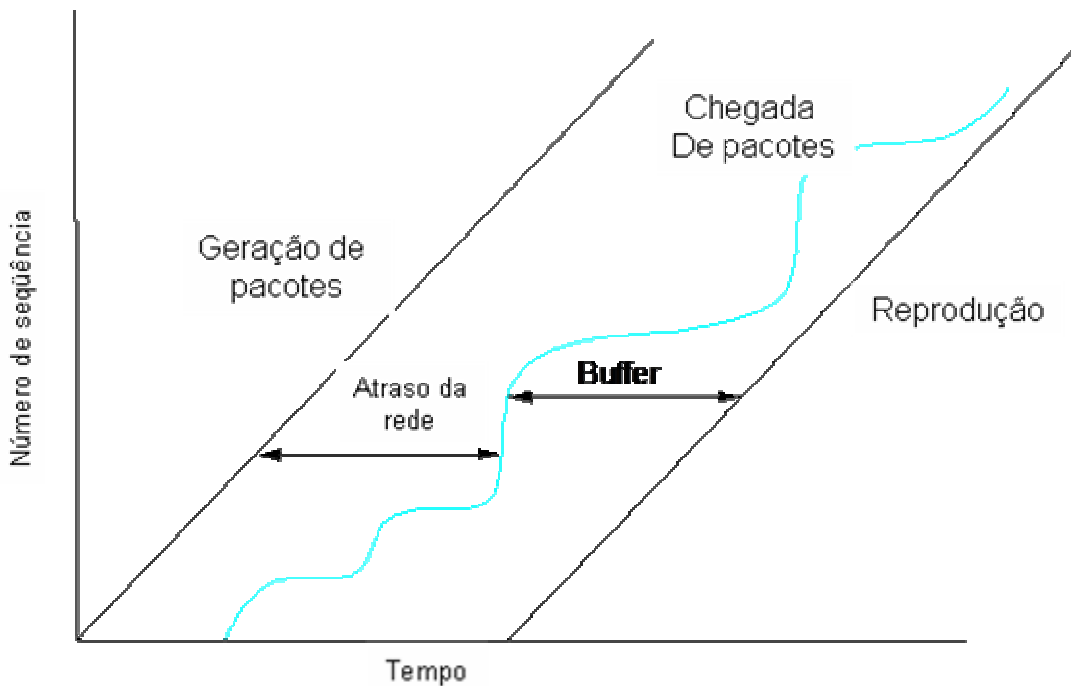


Figura 3-6 - *buffers* para evitar diferenças de atrasos (*jitter*) – Fonte: (Peterson, L. L. & Davie, B. S., 1999)

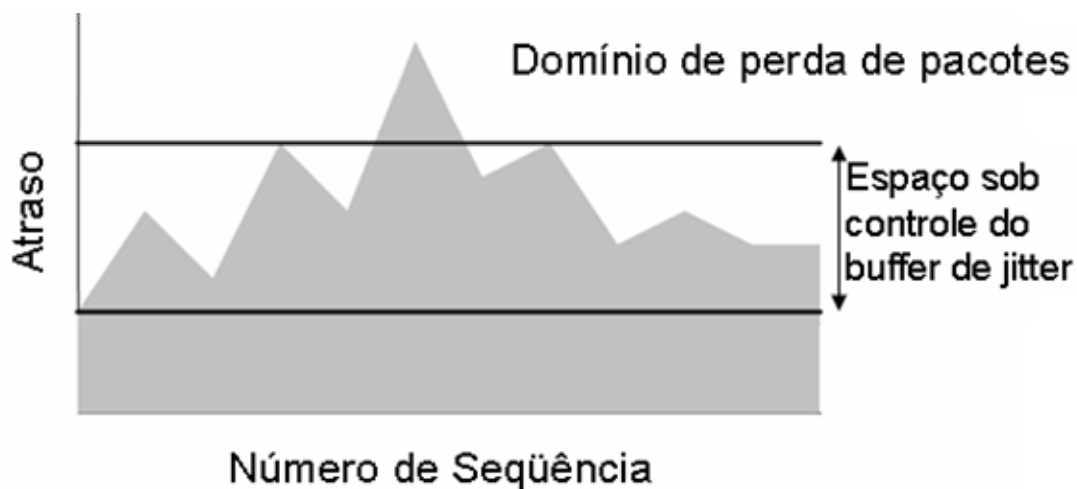


Figura 3-7 - Relação entre o atraso e as perdas de pacotes em um *buffer* de *jitter* – Fonte: Raisanen, V., 2003.

Atraso de transmissão ou serialização

É o tempo que uma interface dispende para inserir um quadro no meio físico. Tipicamente, o atraso de transmissão pode ser representado por:

$$A=C/T$$

onde:

A=atraso de transmissão (seg)

C=Comprimento do frame (bits)

T=Taxa de transmissão da interface (bps)

Como exemplo, pode-se calcular o atraso de transmissão das interfaces FastEthernet IEEE 802.3u, para um frame típico de 1518 bytes:

$$1518 \text{ bytes} * 8 = 12.144 \text{ bits}$$

$$A = 12.144 / 100.000.000 \text{ bits/seg} = 0,0012144 \text{ segundos, ou } 1,21 \text{ ms}$$

Atraso de Enfileiramento

O atraso de fila é um dos mais complexos e por isso o mais estudado. No próximo capítulo, onde se analisam os tipos de filas e sua influência nas técnicas de QoS, pode-se perceber a grande quantidade de tentativas para minimizar os efeitos deste tipo de atraso.

Nas filas tipo FIFO (First In, First Out) o primeiro pacote a chegar é o primeiro a ser processado e repassado. Os demais frames somente serão processados após o processamento dos antecessores. Uma fila típica em um roteador está representada na Figura 3-8. O tamanho da fila irá depender da taxa de chegada dos frames (λ), do tamanho de cada frame (no caso do ethernet, 1518 bytes) e da capacidade do processamento (T_s), descontada a utilização da CPU.

Quando a taxa de chegada dos frames for maior que a capacidade de processamento, o tempo de espera tende a crescer indefinidamente. Como os

recursos para armazenar as filas dos pacotes são finitos, os pacotes que excedem os recursos são descartados. Do ponto de vista dos sistemas finais, é como se o pacote tivesse entrado na rede de um lado e não emergisse no outro.

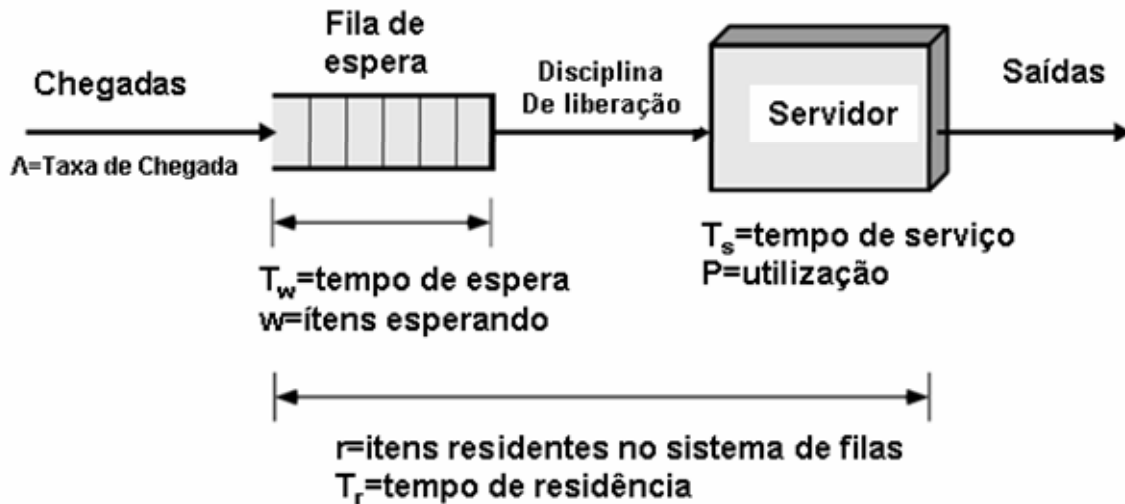


Figura 3-8 - Atraso de enfileiramento. Fonte: Stallings, W., 2002

Atraso médio em sentido único

O atraso pode se medido em um sentido ou em ambos (round trip). Pela definição do ETSI (TIPHON, 2002), “o atraso médio em um sentido é o tempo em milisegundos usado por um sinal de teste para sair da origem da voz, atravessar a rede, chegar ao destino e voltar ao ponto de origem, dividido por 2”. Segundo o Instituto, a métrica deve ser a média de 10 medidas ou 90% do maior atraso, o que for maior. Os atrasos devem ser medidos a cada 30 segundos.

3.4.2. Variação do atraso

A variação do atraso (*Jitter*), como métrica de desempenho de uma rede de pacotes está definida na RFC 3393 – IP Packet Delay Variation (IPDV) Metric for IP Desempenho Metrics (IPPM) (Demichelis, C.; Chimento, P., 2002). Segundo o documento, essa métrica é baseada na diferença no atraso em uma direção (One-Way-Delay) de pacotes selecionados. Essa diferença entre os atrasos é denominada "IP Packet Delay Variation (ipdv)". A medida é válida para *hosts* que possuam os relógios sincronizados e também para os que não possuem essa condição. Essa possibilidade

confere a variação do atraso uma robustez muito grande, pois os erros de cálculo são da mesma magnitude daqueles introduzidos na sincronização dos relógios.

A variação do atraso pode ser introduzida nas redes devido a 3 motivos básicos (Hardy, W. C., 2001):

- a) Variações nos tempos de transmissão devido a percursos físicos de distâncias diferentes;
- b) Variações nos tempos de tratamento dos pacotes durante a passagem por nós diferentes ao longo do percurso;
- c) Variações nas filas enfrentadas pelos pacotes.

Destaca-se como uso dessa métrica o cálculo do tamanho necessário para os *buffers anti-jitter* (Figura 3-6), necessários para as aplicações que exigem entregas dos pacotes em tempos regulares (fluxos de voz e vídeo). O que pode ser considerado mais importante neste caso é a variação máxima do atraso. Outra utilização de destaque é a dinâmica de filas, onde as alterações da variação do atraso podem se relacionar as variações nos tamanhos das filas em um enlace ou em um conjunto de enlaces. Tal utilização está em conformidade com o terceiro motivo (c) da lista acima.

Os efeitos da variação do atraso os fluxos de voz são bastante perceptíveis aos usuários, se não houver correção das variações através do uso dos *buffers* (Figura 3-9).

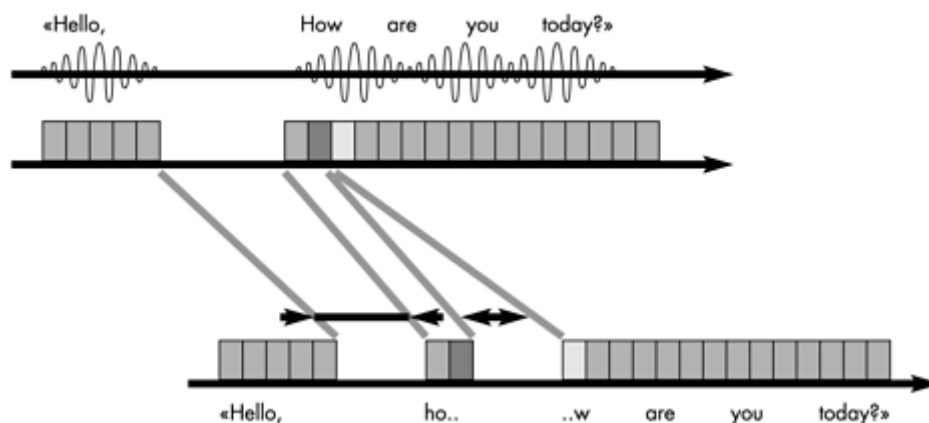


Figura 3-9 - Efeito do *Jitter* na percepção da fala – Fonte: (Hersent, O.; Gurle, D. & Petit, J. P., 2000)

Segundo a RFC 3393, o termo “*jitter*” é ambíguo e deve ser evitado quando se trata da variação do atraso. O documento destaca dois significados usados em contextos diferentes. O primeiro seria sinônimo de “wander”, métrica utilizada para medir a qualidade de circuitos emulados, relacionada com sincronismo dos sinais.

O segundo significado é o de variação de uma métrica (que pode ser atraso, por exemplo), e deve ser usada como relação a uma medida de referência (por exemplo atraso médio ou mínimo). Este é o significado usado na computação e segundo os autores freqüentemente, mas não sempre, se refere a variação no atraso. Neste trabalho de pesquisa, o termo *Jitter* é utilizado com este significado, embora o termo “variação do atraso” pareça ser mais correto. A opção pelo uso dos dois termos deve-se a disseminação do termo *Jitter* nos documentos de redes de pacotes, principalmente após o início da convergência.

Os valores aceitáveis de perdas e jitter para fluxos de voz na Internet normalmente não são consensuais, e muitos autores preferem as medidas de satisfação dos usuários (MOS) como parâmetro da qualidade final do serviço. (Hersent, O.; Gurle, D. & Petit, J. P., 2000), (TIPHON, 2002), (Raisanen, V., 2003), (Park, K. I., 2005). Essa situação é compreensível, uma vez que os diferentes equipamentos terminais e CODECs utilizam algoritmos diferentes para tratar os problemas da rede de transporte (TIPHON, 2002). Uma tentativa de estabelecer uma referência para a degradação das condições da rede é encontrada em (Hersent, O.; Gurle, D. & Petit, J. P., 2000), mostrada no Quadro 3-4. Os autores admitem que o uso do modelo de distribuição normal (Gaussiana) é controverso, mas ressaltam a inexistência de consenso para os valores de referência.

Quadro 3-4 Referência para degradação da rede de transporte

| | Média (dist normal) de perdas de pacotes % | Pico (dist normal)de jitter ms (desvio padrão na metade do pico) |
|----------|---|---|
| Perfeito | 0 | 0 |
| Bom | 3 | 75 |
| Medio | 15 | 125 |
| Ruim | 25 | 225 |

Fonte: (Hersent, O.; Gurle, D. & Petit, J. P., 2000).

Medição do *Jitter* – (PDV ou *Packet Delay Variation*)

A definição, segundo (TIPHON, 2002), para a variação do atraso entre dois pontos é:

“*PDV é a diferença entre os percentuais maiores e menores na distribuição do atraso dos pacotes*”.

A variação entre dois pontos utiliza dois pontos de monitoração. As medições utilizam as diferenças entre os tempos de saída e de chegada entre dois pacotes. Segundo a especificação, as medidas necessitam sincronização entre os dois pontos de medição.

Embora a especificação do TIPHON seja considerada neste trabalho, as medições de *jitter* e atraso se fazem pela especificação do IETF, através das RFCs listadas no Quadro 6-3.

Cálculo do Jitter

Neste trabalho foi utilizado o método de cálculo do *jitter* proposto pelo IETF, através da RFC 1889, que especifica o *Real Time Transport Protocol* (RTP) (Schulzrinne, H.; Casner, S.; Frederick, R. & Jacobson, V., 1996). Este cálculo foi estabelecido pela ferramenta de medição utilizada no plano de controle proposto, conforme descrito no capítulo 5.

Segundo o documento, o *jitter* entre chegadas (*interarrival jitter*) é a variação estatística dos tempos de chegada entre os pacotes de dados RTP, medida em unidades de *timestamps*, e expressa como "*unsigned integer*". O *jitter* entre chegadas é definido como o desvio médio da diferença D no espaçamento nos pacotes no receptor comparado com o remetente, para um par de pacotes. É a medida equivalente entre as diferenças nos tempos de trânsito relativo entre os dois pacotes. Essa diferença é o *timestamp* do pacote e o clock do receptor no momento da chegada.

Sendo S_i o *timestamp* do RTP e R_i o tempo da chegada para o pacote i , então, para dois pacotes, i e j , a diferença D pode ser expressa como:

$$D(i,j)=(R_j-R_i)-(S_j-S_i)=(R_j-S_j)-(R_i-S_i)$$

O *jitter* entre chegadas é calculado continuamente conforme cada pacote de dados é recebido oriundo da fonte, usando essa diferença D para aquele pacote e o anterior $i-1$, na ordem de chegada (não necessariamente na seqüência), de acordo com a fórmula:

$$J = J + (|D(i-1,i)| - J) / 16$$

A Figura 3-10 mostra o método de cálculo sugerido pela RFC, conforme (Hersent, O.; Gurle, D. & Petit, J. P., 2000).

Ainda segundo a RFC 1889 (Schulzrinne, H.; Casner, S.; Frederick, R. & Jacobson, V., 1996), o parâmetro de ganho $1/16$ possibilita uma boa redução do ruído e mantém uma taxa de convergência razoável.

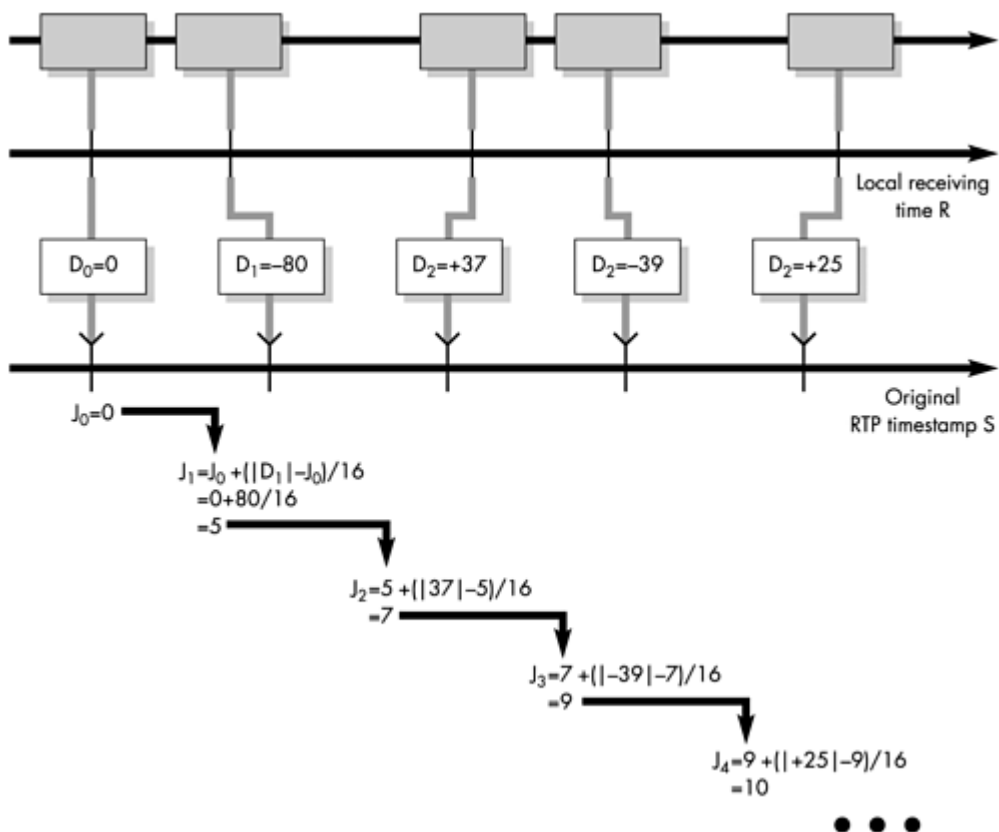


Figura 3-10 -Método de cálculo do jitter segundo RFC 1889- Fonte©Hersent, O.; Gurle, D. & Petit, J. P., 2000)

3.4.3. Perdas

Algumas aplicações não funcionam bem ou até mesmo não funcionam, se as perdas de pacotes entre os *hosts* forem grandes, em relação a um valor de limiar. O limiar preciso é dependente da aplicação.

A motivação para se fazer a medição dos atrasos em sentido único (*one-way*), ao invés de ida e volta (*round trip*) tem base nos seguintes fatores, segundo a RFC 2680 A One-way Packet Loss Metric for IPPM) (Almes, G.; Kalidindi, S. & Zekauskas, 1999):

- As rotas assimétricas da Internet atual, onde os caminhos de ida podem não ser os da volta, e as medições *round trip* medem as condições de dois caminhos em conjunto. Mesmo se os caminhos forem simétricos, podem ter desempenhos diferentes devido ao enfileiramento assimétrico;
- O desempenho de uma aplicação pode depender em sua maior parte, do desempenho em uma única direção. Como exemplo, os autores citam o desempenho de uma transferência de arquivos pelo TCP, onde a direção do fluxo de dados influencia mais que a sinalização através dos aceites (*ACK*);
- Além disso, nas redes com QoS, o provisionamento em um sentido pode ser muito diferente que os recursos no sentido contrário. Medindo os caminhos de forma independente permite que se verifiquem as condições em ambos os sentidos.

O plano de controle proposto neste trabalho (descrito no capítulo 5) realiza as medições fim-a-fim, nos dois sentidos dos enlaces.

3.4.4. Vazão

Existe controvérsia na literatura sobre a utilização dos termos vazão e largura de banda.

“O termo largura de banda é usado para descrever a capacidade de vazão de um determinado meio físico, de um protocolo ou de uma conexão”. (Vegesna, S., 2001)

“É a faixa de freqüências que pode passar pelo enlace com perdas mínimas” (Kurose, J. F.; Ross, K. W., 2003).

“É a quantidade de sinal, em bits, que uma interface pode inserir em um enlace em um segundo” (Peterson, L. L. & Davie, B. S., 1999).

Como a vazão, por si só, não apresenta garantias em relação a manutenção da QoS para os tráfegos inelásticos, essa métrica não será considerada neste trabalho. Deve-se considerar, entretanto, que a vazão é importante nas aplicações de dados (baseadas em HTTP, FTP, SMTP) - (Stallings, W., 2002). O uso da vazão ou da banda disponível pode ser utilizado em análises futuras.

3.5. Disciplinas de filas

As filas existem em um roteador ou comutador para que ele consiga reter os pacotes até que existam recursos para repassá-los para a interface de saída (egress port). Se não existir congestionamento no roteador, os pacotes serão repassados imediatamente, sem a formação da fila.

As filas nas redes são usadas para atender a natureza de rajadas dos tráfegos, que atingem as interfaces de uma forma mais rápida que essa interface possa atender. Isso acontece quando a interface de saída é mais lenta que a de entrada ou existem várias interfaces de entrada alimentando a de saída.

Neste caso, a fila coloca os pacotes em espera, de forma que a interface de saída possa processar os pacotes na sua taxa. Normalmente os roteadores possuem dois sistemas de enfileiramento em cada interface (Figura 3-11):

Uma fila de hardware, necessária para a transmissão dos pacotes um a um. Neste sistema, denominado fila de transmissão ou TxQ, o tratamento é sempre FIFO. E um sistema de software, que vai escalonar os pacotes na fila de hardware, com base nos requisitos de QoS de cada fluxo.

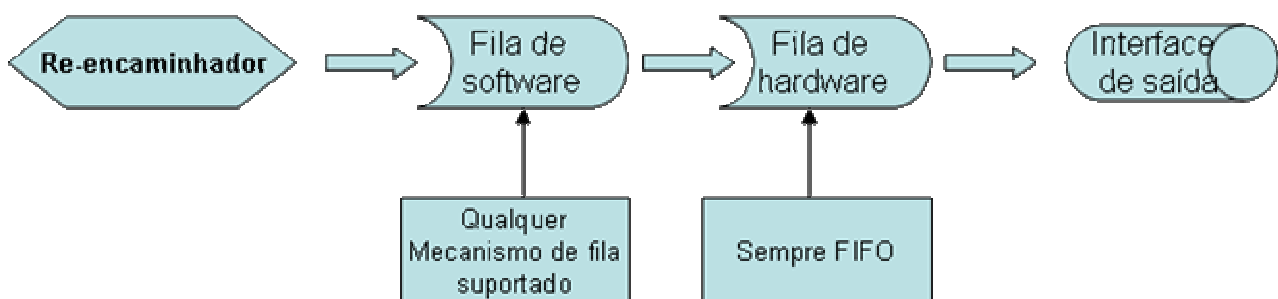


Figura 3-11 - Sistemas de filas nas interfaces: Software e Hardware

A utilização de dois sistemas de filas possui influência no resultado final do processo de filas. Como o software de filas possui alguma razão para ser usado, um tamanho muito grande de filas de hardware irá reduzir a eficiência dessa estratégia, uma vez que neste sistema todos os pacotes usam política FIFO. Todo o projeto de fila com QoS ficaria prejudicado com o uso de *buffers* muito grandes nas filas de Hardware.

Por outro lado, a redução da fila de hardware para tamanhos muito pequenos (por exemplo, 1 pacote) iria forçar todos os pacotes a passarem pela fila de software, sendo escalonados um a um na interface para transmissão. Este método possui dois problemas:

- A cada tempo de transmissão, o driver da interface interrompe a CPU e solicita mais pacotes para serem entregues a fila de hardware. Alguns mecanismos de fila possuem agendamento complexo para os pacotes, o que demanda algum tempo para entregar mais pacotes. A interface fica ociosa durante este tempo, levando a uma ineficiência no uso do enlace, sempre que a fila de hardware estiver vazia.
- A CPU iria escalonar os pacotes um a um, ao invés de vários a cada intervalo de interrupção, causando um consumo dos recursos.

Existem duas situações onde o roteador não utiliza a fila de software (Figura 3-12):

- Quando a fila de software estiver vazia;
- Quando a fila de hardware não estiver cheia.

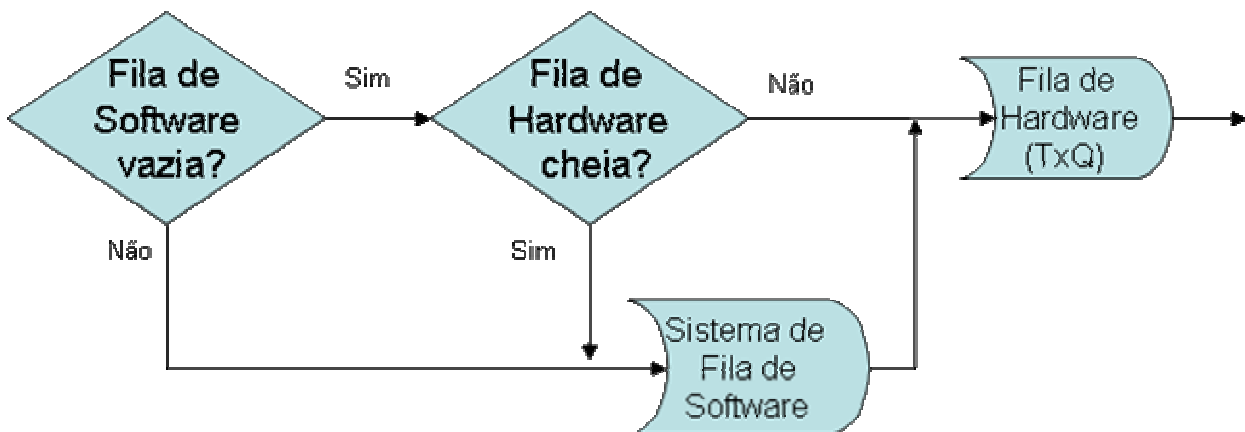


Figura 3-12 - Bypass da fila de software

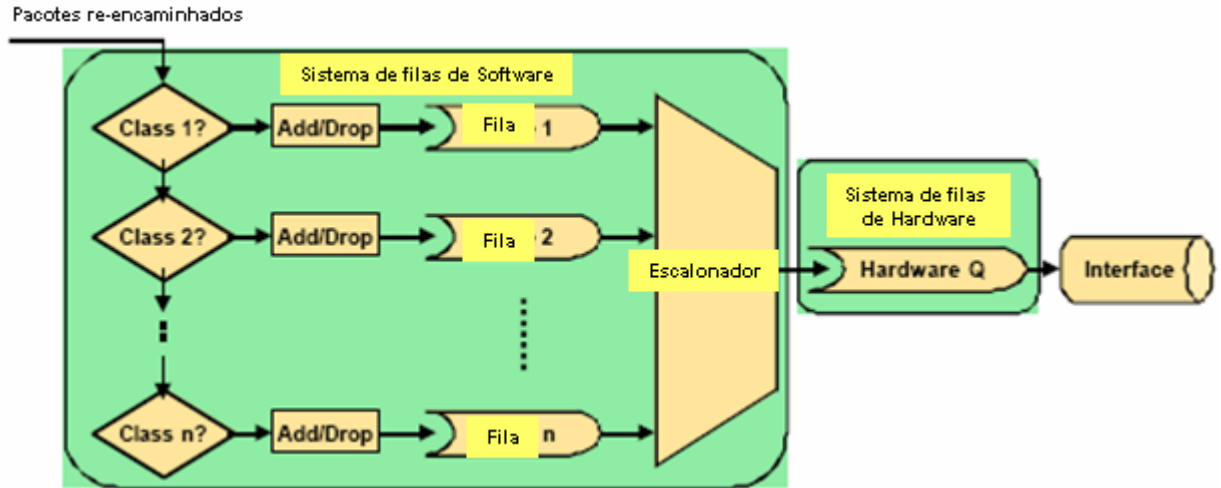


Figura 3-13 - Componentes de uma fila (classificação, inserção, escalonamento)

Cada mecanismo de fila possui 3 componentes para sua definição (Figura 3-13):

- Classificação dos pacotes (seleciona a classe)
- Política de inserção (determina se o pacote pode ser enfileirado ou deve ser descartado)
- Política de Serviço (Escalonamento dos pacotes para colocá-los na fila de hardware)

A classificação pode ser feita de forma automática, como nas filas WFQ. Outros mecanismos necessitam de uma configuração para a classificação (Priority e Custom Queue). Uma vez classificados, o roteador analisa a política de inserção, para decidir se pode encaminhar o pacote para a fila ou se descarta o pacote. A maioria das filas usa o tail-drop como política de descarte. Outros usam esquemas mais inteligentes (WFQ) ou um sistema randômico de descartes (WRED). Cada pacote aprovado para uma fila irá enfrentar um sistema FIFO dentro de sua classe. Por fim, o pacote deixa a fila da sua classe para entrar na fila de transmissão TxQ, ou fila de hardware.

3.5.1. Weighted Fair Queuing (WFQ)

A política WFQ classifica os fluxos de tráfego e coloca-os em filas individuais. O mecanismo assegura acesso às interfaces através de um algoritmo de atribuição de

pesos para as filas. O tráfego é classificado com base nas informações dos cabeçalhos de camada 3 e 4, bem como nas taxas de tráfego e nos tamanhos dos pacotes. Com base nessas informações, os pacotes adquirem um “tamanho virtual”, onde os fluxos que consomem menos banda têm mais prioridade, o que previne que sejam inviabilizados pelos fluxos de maior banda. Nessa situação, os fluxos de voz possuem prioridade 5, e um fluxo de dados normal, prioridade 0. Um fluxo de voz terá o mesmo “direito” de acessar a fila de hardware que 6 fluxos de dados somados. Este comportamento pode resultar em atrasos mais previsíveis tanto para sessões de grande consumo de banda, como as transferências de arquivos, bem como para as sessões de pouco consumo, como telnet e chat.

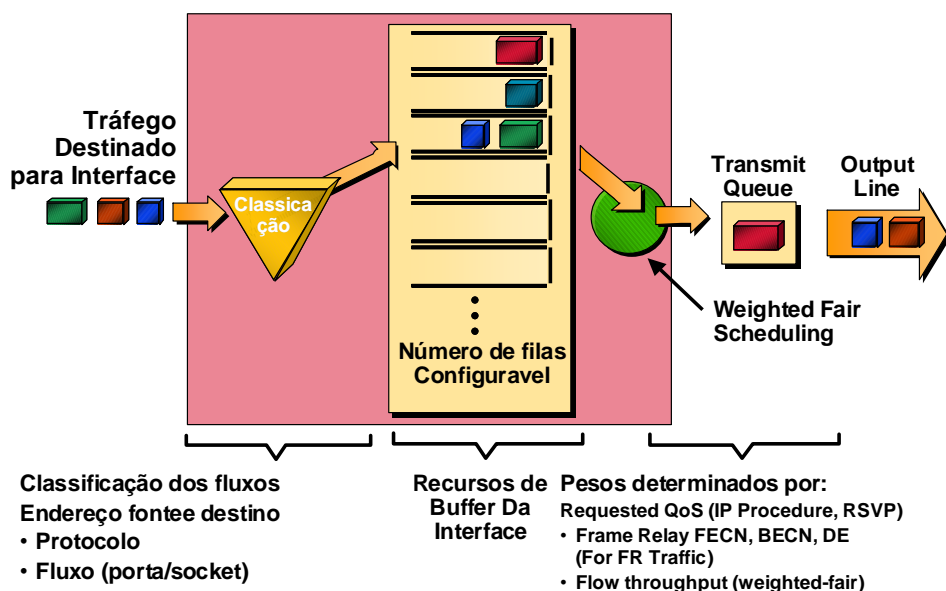


Figura 3-14 - Weighted Fair Queue – Fonte: Cisco Systems™

O mecanismo de tratamento de filas WFQ é importante nos ambientes de voz porque prioriza estes tipos de fluxos. Este mecanismo é o padrão de enfileiramento para os roteadores utilizados neste trabalho de pesquisa, para os enlaces com largura de banda menores que 2 Mbps.

Tratamento WFQ na integração de fluxos de dados e de voz.

Assumindo-se um ambiente como o que foi utilizado neste trabalho – capítulo 5.4, onde os enlaces possuem 128 kbps de taxa, um CODEC G.729 para codificar a voz,

pode-se usar uma banda necessária de aproximadamente 30 kbps para os fluxos de voz. Na precedência usada pela WFQ, um fluxo de voz tem precedência 5, sendo equivalente a 6 sessões de dados.

Considerando-se que um fluxo de voz esteja disputando a fila com 5 sessões de dados, tem-se

Banda para voz= $6/(6+5)*128=69$ kbps, suficiente para uma sessão de voz.

Se o mesmo fluxo estiver disputando com 20 sessões de dados, tem-se

Banda para voz= $6/(6+20)*128=29$ kbps, poderiam ocorrer descartes.

3.5.2. Weighted Random Early Detection

WRED é um mecanismo para evitar congestionamentos que possibilita melhorias de uso dos enlaces (Hassan, M. & Jain, R., 2004). O mecanismo de detecção antecipada de congestionamentos monitora o enlace e os fluxos de tráfego, descartando randomicamente os pacotes de fluxos individuais (Figura 3-15). Os protocolos de camadas superiores podem então se adaptar a essas condições de congestionamento.

A técnica otimiza as taxas de transmissão de fluxos individuais, e previne problemas de sincronização e colapsos por congestionamento. Este mecanismo fornece recursos para suportar vários níveis de prioridades, cada um com diferentes limiares de descartes. O Descarte Antecipado Randômico Balanceado - WRED – pode auxiliar os serviços de voz pelo fornecimento de preferência, enquanto otimiza a eficiência dos enlaces para os serviços diversos.

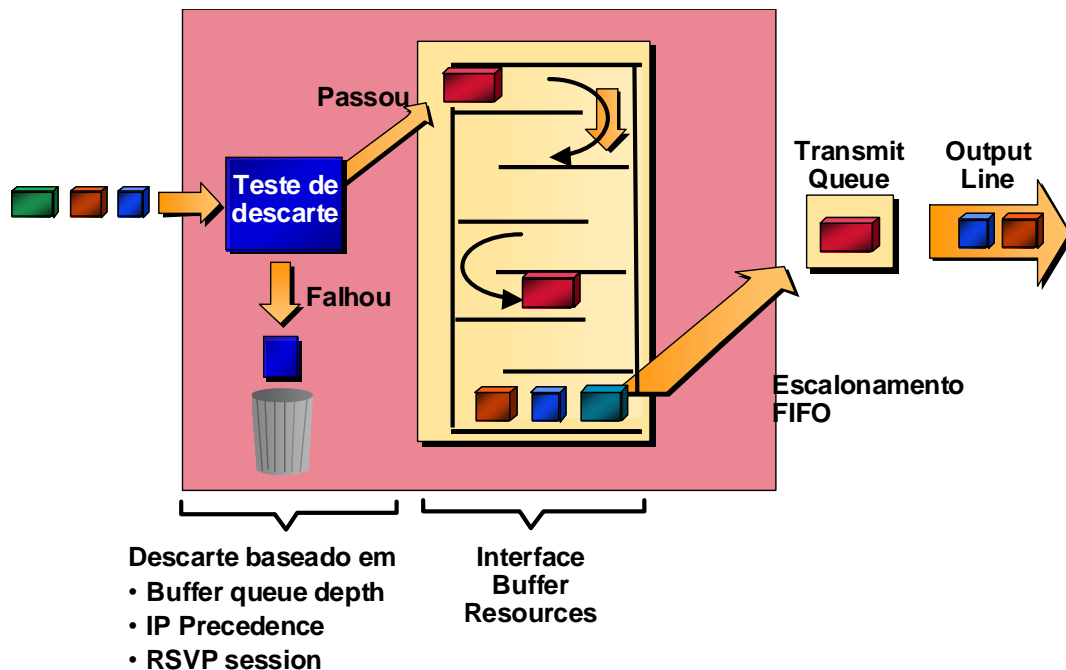


Figura 3-15 – WRED– Fonte: Cisco Systems™

3.5.3. Priority Queue

O mecanismo de filas por prioridade mantém 4 subfilas de saída (Figura 3-16):

- Alta
- Media
- Normal
- Baixa

A ordem de prioridade é decrescente, ou seja, os pacotes da subfila de saída alta são tratados primeiro. O administrador pode classificar os fluxos para pertencer a uma dessas sub-filas. Quando a fila de alta prioridade fica vazia, o tráfego da próxima fila de maior prioridade é tratado (Stallings, W., 2002). Nenhum pacote de prioridade média é transmitido se houver pacote na fila de alta prioridade. Este mecanismo foi projetado para ambientes onde dados de missão crítica necessitam ser categorizados com a maior prioridade, mesmo que isso signifique o bloqueio do tráfego de menor prioridade em momentos de congestionamento. Durante estes momentos, os dados de missão crítica podem, potencialmente, tomar 100% da banda.

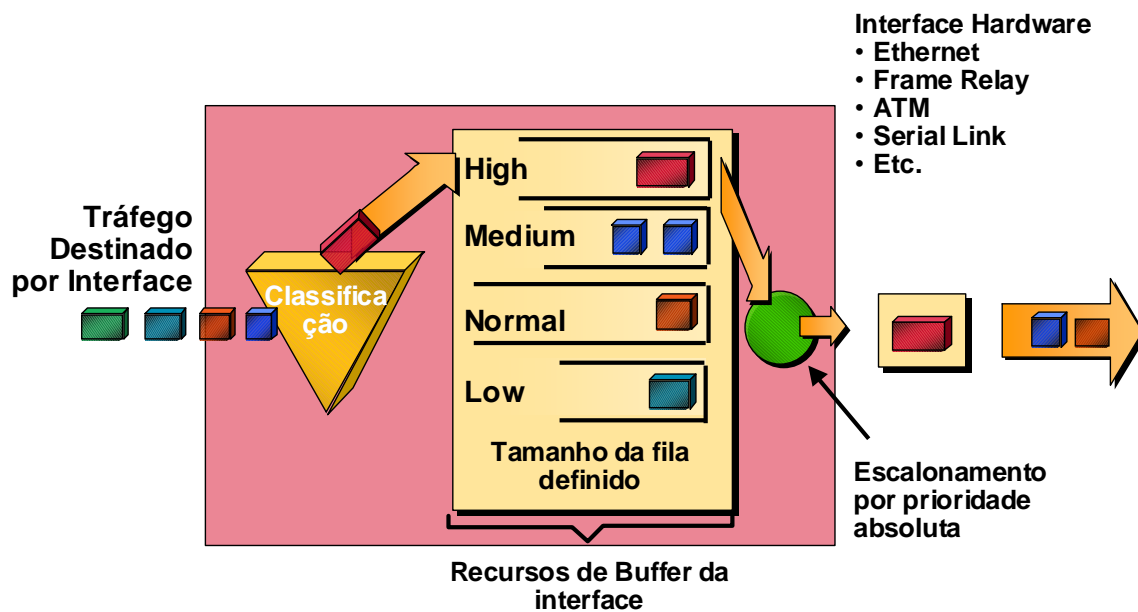


Figura 3-16 - Priority Queue – Fonte: Cisco Systems™

Se o tráfego de alta prioridade se iguala ou excede a banda por um período de tempo, essa política de filas sempre irá deixar passar o tráfego de mais alta prioridade antes de processar o tráfego com o próximo nível de prioridade. No pior caso, o tráfego de controle também é descartado. O tráfego que não for classificado é tratado como sub-fila normal. Os pacotes dentro de uma sub-fila são tratados em ordem FIFO.

A fila de prioridades é basicamente um conjunto de quatro filas FIFO paralelas. Cada uma delas sofre todos os problemas da fila FIFO dentro da sua classe (injustiça, bloqueio, atraso, *jitter*). O sistema de descarte para cada classe é o *tail-drop*, quando a fila estiver cheia. Cada fila pode ser configurada com o máximo de pacotes que serão permitidos.

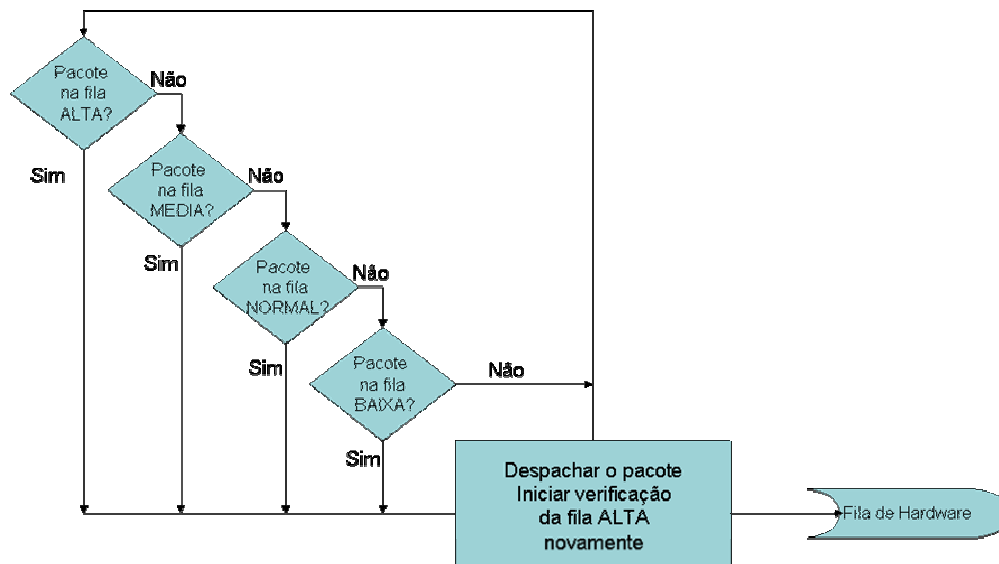


Figura 3-17 – Fluxograma para classificação dos pacotes nas filas PQ- – Fonte: Cisco Systems™

3.6. Serviços Integrados

Essa seção trata da abordagem para manutenção dos valores das métricas de desempenho através dos Serviços Integrados (*IntServ*), primeiro padrão adotado pelo IETF para garantias de QoS na Internet. A Arquitetura de serviços Integrados foi definida em termos genéricos pela RFC 1633 (Braden, R.; Clark, D. & Shenker, S., 1994). Pela abordagem, o tráfego pode ser dividido em dois grupos: Elástico e Inelástico, gerando dois tipos básicos de fila, uma com QoS e outra do tipo Best Effort.

Uma das forças da arquitetura *IntServ/RSVP* é a garantia de QoS (Verma, D., 2000). Se a reserva do RSVP tiver sucesso, é assegurada à conexão um determinado nível de desempenho fim-a-fim. Além disso, o protocolo ajusta automaticamente as alterações de roteamento na rede. As mensagens PATH e RESV automaticamente seguem as rotas dos pacotes normais do IP (Figura 3-18), e reservam ou cancelam automaticamente os recursos. Outra vantagem é a associação do protocolo com o roteamento Multicast.

Entretanto, o RSVP tem limitações, principalmente em relação à escalabilidade. Um aspecto relacionado à escalabilidade é a carga gerada pela sinalização, feita no mesmo canal de dados (inband). Porque cada fluxo de aplicação precisa gerar

mensagens periódicas de PATH e RESV, os roteadores precisam processar essas mensagens, em grande número para cada fluxo (Verma, D., 2000). Além disso, o processo de reserva inclui uma latência no processo de comunicação, pois é necessário reservar antes de iniciar-se o envio dos pacotes. Dessa forma, qualquer abordagem de reservas mostra dificuldades em relação aos tráfegos de rajadas tradicionais nas redes de dados, com taxas de transmissão variáveis.

Optando-se pelo modelo de serviços diferenciados na camada de transporte, tem-se priorizações garantidas no núcleo da rede, mas em situações de carga elevada o fluxo de alta prioridade poderia congestionar os roteadores de borda, penalizando o tráfego de baixa prioridade. Em situações extremas, os fluxos de alta prioridade também poderiam sofrer degradação de desempenho. Isso porque essencialmente, o modelo procura uma degradação diferenciada de desempenho, ou nenhuma degradação, quando diferentes tráfegos atingem os nós congestionados em uma rede. Se o congestionamento puder ser evitado, todos os fluxos terão bom desempenho, mesmo na ausência do modelo.

3.6.1. Sinalização

Assumindo que diferentes sistemas de filas e escalonamento em cada *hop* podem ser oferecidos precisa-se definir como se fará a alteração do comportamento atual da rede. Um termo genérico para o processo de coordenação dos comportamentos dos enlaces é sinalização (Armitage, G., 2000-a). Este termo significa o ato de informar cada nó ao longo de um ou mais caminhos como reconhecer o tráfego para o qual é necessário um tratamento especial no processamento. A sinalização pode ser obtida de várias formas, variando os graus de precisão temporal, flexibilidade e intervenção humana. Em um extremo situam-se as sinalizações dinâmicas de uma borda a outra (dynamic edge-to-edge signaling), na qual a rede é informada a cada vez que uma nova classe de tráfego requisita suporte específico.

A rede por si só responde sob demanda pelo estabelecimento de informações adicionais (ou alterando informações já existentes) em cada salto para chegar no comportamento desejado fim a fim. Exemplos de sinalização sob demanda incluem a UNI ATM (User Network Interface (UNI) e a Network Node Interface (NNI). O protocolo

RSVP, sendo de reservas, também é exemplo de sinalização sob demanda. Neste trabalho de pesquisa, as demandas serão disparadas pela degradação das métricas, e a sinalização vai ocorrer a partir de uma estação QNS (capítulo 5).

3.6.2. Protocolo de Reserva de Recursos (RSVP – *Resource ReserVation Protocol*)

Em 1997, através da RFC 2205 (Braden, R. et al., 1997), o RSVP foi definido como protocolo padrão para sinalização na Arquitetura dos Serviços Integrados, cujo processo de sinalização está representado na **Error! Reference source not found.**

Mensagens RSVP

O RSVP possui 2 tipos principais de mensagens e sua operação básica: PATH e RESV (Jha, S.; Hassan, M., 2002) .

A fonte transmite as mensagens PATH a cada 30 segundos (Figura 3-18). As mensagens RSVP trafegam hop-by-hop, com o próximo hop sendo determinado pela tabela de roteamento. Os roteadores mantêm um registro da origem da mensagem, o que é denominado “route pinning”. As mensagens são enviadas em um datagrama IP bruto, com o número 46 no campo de protocolo. Os sistemas finais que não têm capacidade de enviar datagramas em estado bruto podem encapsular o RSVP em segmentos UDP. Os datagramas são remetidos aos roteadores com a opção de alerta configurada em seus cabeçalhos, denotando necessidade de tratamento especial.

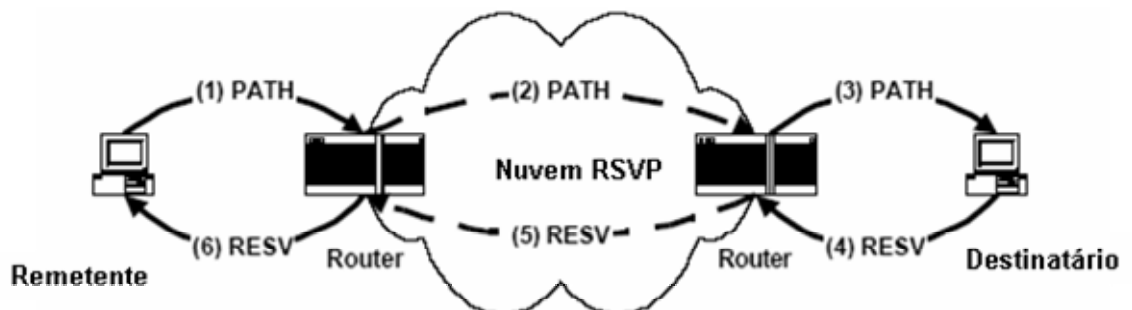


Figura 3-18 - Sinalização RSVP – Fonte: (Choudhury, D., 2001)

3.7. Serviços Diferenciados

O modelo de serviços diferenciados (DiffServ) é correntemente um tópico de pesquisa popular por ser um método de baixo custo que possibilita implementar QoS nos backbones da Internet atual.

A arquitetura de Serviços Diferenciados (*DiffServ architecture*) é muito mais simples que os Serviços Integrados e o RSVP, e portanto tem menores funcionalidades. Porém, tem escalabilidade bem maior. Outra vantagem é que pode coexistir com os protocolos de segurança do IP, pois o campo ToS do cabeçalho pode ser marcado sem interferir na autenticação e na criptografia. O RSVP necessita processamento de filtros em cada roteador, e mostra problemas quando a informação da camada de transporte é criptografada.

Nas redes de *Backbone* é desejável o emprego do DiffServ, em detrimento do RSVP. Este último continua com funções úteis nas sinalizações de reservas nas bordas das redes, especialmente para tráfegos de voz e vídeo, que exigem reservas de longo termo e banda mais elevada.

Para se obter uma garantia fim-a-fim, pode-se utilizar RSVP nas bordas e DiffServ no núcleo da rede.

Essencialmente, um Serviço Integrado é um agrupamento de demandas de tráfego. Tal agrupamento forma um domínio, ou porção da Internet que implementa uma instância particular da Arquitetura de Serviços Integrados). O provedor de IS percebe a rede como um total de demanda atual de tráfego e

- Limita a demanda que é fornecida para o montante que pode ser provido pela capacidade atual da rede e;
- Reserva recursos dentro do domínio IS para prover uma QoS particular para demandas específicas.

Em contraste, os Serviços diferenciados não percebem os montantes de tráfego, e tampouco reservam recursos da rede. Essa arquitetura classifica o tráfego em grupos. Cada grupo é rotulado, e os serviços oferecidos pela rede dependem do grupo ao qual o pacote pertence, com diferentes rótulos sendo tratados de forma diferente.

A tecnologia MPLS foi inicialmente introduzida como um mecanismo WAN que poderia facilitar o repasse de pacotes utilizando roteamento baseado nos rótulos de camada 2, ao invés do endereço IP na camada 3 (Finenberg, V., 2002). Outro propósito inicial era o provimento de QoS diferenciada. Entretanto, o desenvolvimento de novas tecnologias de redes (por exemplo, processamento de terabits nos roteadores, DiffServ para QoS), uma das mais importantes aplicações para o MPLS passou a ser a Engenharia de Tráfego (TE) (Armitage, G., 2000-a). A TE possibilita roteamento por caminhos específicos, (possivelmente não ótimos em termos de métricas convencionais) para habilitar roteamentos diversos, balanceamento da carga do tráfego, e outros meios de otimizar os recursos da rede. A tecnologia MPLS força o tráfego por essas rotas, ou LSPs (label switched paths.)

Uma abordagem mais conservadora poderia manipular as métricas dos enlaces usadas pelos protocolos link-state (Doyle, J., 1998). Isso poderia levar a um balanceamento de carga baseado em custos desiguais. Entretanto, este método não provê redundância dinâmica e não considera as características do tráfego (Alwayn, V., 2002). Tampouco avalia as restrições de capacidade da rede nas decisões de roteamento.

Todas as utilizações possíveis das redes IP estão exigindo demandas por algum tipo de previsibilidade, mesmo na presença de congestionamentos transitórios (Armitage, G., 2000-b). Essa demanda por proteção relativa ou absoluta de outro tráfego ou segmento da rede aplica-se a qualquer largura de banda usada nos enlaces, desde um acesso discado até enlaces OC-48/STM-16, ou até taxas maiores. Essa demanda leva a três requisitos técnicos importantes (Armitage, G., 2000-b):

a.QoS localizado nos nós (Per-hop QoS). O menor elemento controlável na rede é o nó (roteador ou comutador) que faz a ligação entre dois ou mais enlaces. Estes nós devem ser baseados em uma arquitetura que permita agendamentos e filas diferenciadas para aplicação em cada nó. Devem ser capazes ainda de utilizar apropriadamente as características de QoS dos enlaces.

b.Roteamento e Engenharia de tráfego. Onde existem múltiplos caminhos paralelos através da rede, distribuir o tráfego pode reduzir a carga média. Essa prática

melhora a QoS aparente da rede, porque os roteadores imprimem menos *jitter* e descartam menos pacotes. Nessas abordagens, são necessários mecanismos para descobrir e impor o encaminhamento de pacotes pelos caminhos diferentes do menor caminho (*non-shortest-path*).

c.Sinalização e Provisioamento. A QoS controlável nos hops e o encaminhamento pelos caminhos diferentes do menor caminho (*non-shortest-path forwarding*) tem pouco uso se não for facilmente gerenciável. Uma solução prática requer algum grau de distribuição automática dos parâmetros de QoS e/ou restrições de Engenharia de Tráfego para todos os nós (roteadores e comutadores) da rede. A informação nova deve se distribuída sempre que os requerimentos de QoS fim-a-fim ou borda-a-borda forem alterados ou impostos pelo cliente.

3.8. Sumário do capítulo

Neste capítulo, foram analisadas as principais técnicas, mecanismos e arquiteturas utilizadas na Internet atual para preservar a qualidade dos serviços nas redes IP, visando quebrar o paradigma inicial do *best-effort*.

Os conceitos de Qualidade e de Serviços foram discutidos com base em diversos órgãos de padronização, e se verificou que não existe um consenso, embora a maior parte pareça concordar que a qualidade fim-a-fim deva ser o principal objetivo, pois envolve o ponto de vista dos usuários dos serviços.

Foram analisadas as disciplinas de filas e políticas de descarte mais utilizadas. Discutiram-se as métricas de QoS, e a forma de cálculo para o *jitter* e as perdas. Analisaram-se brevemente as duas arquiteturas propostas pelo IETF para provisionamento de Qualidade de serviços: IntServ e DiffServ.

No próximo capítulo, serão discutidas as soluções para manutenção das métricas que baseiam-se nas técnicas de roteamento. Analisam-se as questões do cálculo dos melhores caminhos, com base em métricas alternativas ao simples número de saltos, comumente usado pelos protocolos atuais. Essas técnicas alternativas de roteamento foram denominadas “técnicas não convencionais”. Uma atenção especial é dada a Engenharia de Tráfego e ao re-roteamento, técnicas utilizadas neste trabalho.

4. Roteamento IP Baseado em QoS

Este capítulo discute abordagens de dois momentos distintos da implementação dos protocolos de roteamento: Uma abordagem original, que trata todos os serviços de forma igualitária e sem nenhuma confiabilidade, e outra abordagem que emergiu diante das necessidades mais recentes, notadamente a metade da década de 1990, com o advento da convergência das redes de dados, voz e vídeo (como foi discutido no capítulo 2). Na primeira abordagem, são demonstrados os princípios dos algoritmos que são utilizados na implantação da proposta deste trabalho de pesquisa. Na abordagem subsequente, denominada técnicas de roteamento não convencionais, são discutidas e catalogadas várias alternativas aos métodos de escolha dos caminhos com base no número de saltos.

4.1. Algoritmos dos Protocolos IGP (*Interior Gateway Protocol*)

Todos os protocolos de roteamento são construídos com base em um algoritmo, que deve especificar, no mínimo os seguintes procedimentos (Doyle, J., 1998):

- Passar as informações de alcançabilidade das redes aos outros roteadores;
- Receber as informações de alcançabilidade das redes dos outros roteadores;
- Determinar rotas ótimas baseadas nas informações de alcançabilidade e armazenar essas informações em uma tabela de roteamento;
- Procedimentos para reagir, compensar e anunciar alterações na topologia.

Problemas comuns para um protocolo são a determinação dos caminhos, métricas, convergência e balanceamento de cargas.

4.1.1. Distance Vector

O cálculo dos custos menores são realizados de forma distribuída. Estes algoritmos são denominados Bellman-Ford, em homenagem aos autores da proposta. O mais

comum dos protocolos baseados neste algoritmo é o RIP (*Routing Information Protocol*).

Nos algoritmos de vetor de distância, os nós armazenam as informações em uma tabela de distâncias, que contém as informações (destino, direção, custo), como ilustrado na Figura 4-1. Ao final da computação de caminhos, cada nó irá possuir sua própria tabela de caminhos.

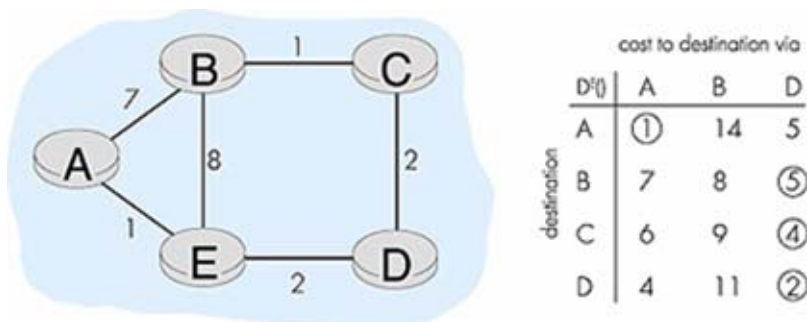


Figura 4-1 - Tabela de distâncias do Roteador E até os demais, usando algoritmo de vetor de distâncias. Fonte: (Kurose, J. F.; Ross, K. W., 2003)

4.1.2. Link State

Os nós da rede possuem um conhecimento global dos estados dos enlaces. O algoritmo mais conhecido que emprega este método é o de Dijkstra. O protocolo mais comum com este algoritmo é o OSPF (*Open Shortest Path First*).

A idéia básica por trás de um algoritmo LS (Link State, ou de Estado do Enlace) é simples:

Cada roteador é responsável por encontrar seus vizinhos e descobrir seus nomes.

Cada roteador constrói um pacote conhecido como Pacote do Estado do Enlace (*link state packet*, ou LSP), o qual contém uma lista dos nomes e dos custos até seus vizinhos.

O pacote LSP é transmitido a todos os demais roteadores (em broadcast ou multicast), e cada roteador armazena o LSP mais recente de cada um dos outros roteadores.

Cada roteador, que agora dispõe de um mapa completo da topologia (a informação dos LSPs permite a montagem de tal mapa), calcula os caminhos para cada destino.

4.2. Re-encaminhamento dos pacotes

Pelos métodos convencionais de re-encaminhamento (forwarding), o protocolo IP baseia-se na tabela de rotas. A tabela é computada no roteador e alterada manualmente ou através dos protocolos. Em cada roteador, existe um número finito de portas de saída para as quais os pacotes podem ser re-encaminhados. Os pacotes que chegam são inicialmente mapeados para um grupo pequeno de classes denominado *Forwarding Equivalence Classes* (FECs). Todos os pacotes em uma FEC são roteados para a mesma porta de saída. Do ponto de vista do roteamento, portanto, todos os pacotes agrupados na mesma FEC são indistinguíveis, e serão repassados da mesma maneira.

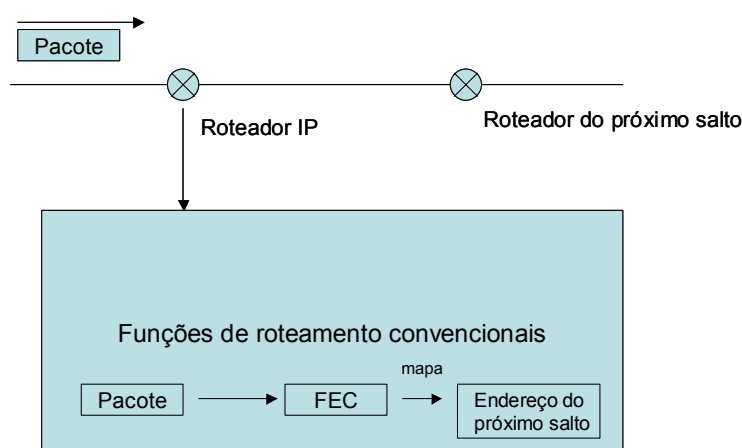


Figura 4-2 – Re-encaminhamento convencional de pacotes pelo IP – Fonte: (Park, K. I., 2005)

Quando um pacote chega ao roteador (Figura 4-2) o cabeçalho do pacote é examinado, e o pacote é mapeado em uma FEC. A partir daí, a tabela do roteador designa a porta pela qual o pacote daquela FEC deve ser re-encaminhado. Os roteadores convencionais suportam um número muito limitado de FECs. Uma classificação FEC multidimensional é difícil devido ao processamento dos pacotes e escalabilidade. (Doyle, J., 1998), (Park, K. I., 2005). Em cada roteador o processo é repetido: o pacote tem o cabeçalho re-examinado, e é re-mapeado para uma FEC. Este procedimento consome de recursos e dispende tempo, aumentando o atraso (denominado por alguns autores como atraso de processamento – seção 3.4).

4.3. Técnicas de roteamento não convencionais

Neste tópico serão analisadas algumas soluções que parecem ter uma fundamentação comum, embora vários nomes tenham sido encontrados para a técnica de rotear com base em objetivos diferentes que o menor caminho (inclusive nas tabelas de roteamento) até o endereço de destino (inserido no cabeçalho do IPV4). Este conjunto de abordagens foi agrupado neste trabalho sob o título de “Técnicas de Roteamento não-convencionais”, para fins de simplificação, embora algumas abordagens possam ser um tanto diferentes. Essas diferenças foram tabeladas (Quadro 4-1) , na tentativa de comparar-se mais facilmente as técnicas.

Nessas técnicas, o caminho para um fluxo de tráfego é o mais curto que preenche os requerimentos (ou restrições) em termos de banda, meio físico e prioridade do próprio tráfego.

4.4. Gerência de rotas

Um dos aspectos a serem considerados neste trabalho é a manutenção dos estados dos enlaces. Uma vez que tenham sido escolhidas as rotas com QoS, como se vai evitar alterações desnecessárias nas tabelas? Deve-se acompanhar as métricas, para se descobrirem as potenciais rotas novas em caso de degradação dos estados dos enlaces. Segundo a terminologia proposta pela RFC 2676, uma rota é dita “fixada” (pinned) quando seu estado especifica que não é necessária uma nova consulta de roteamento. Tal rota será considerada “não-fixada” (un-pinned) caso contrário. O maior problema é definir como, quando e onde as rotas estão para tornarem-se fixadas ou não-fixadas.

Quadro 4-1 Técnicas de roteamento não convencionais

| Técnica | Objetivo da abordagem | Métricas | Protocolo de referencia | Principais autores/órgãos |
|--------------------------------------|---|---|--------------------------------|--|
| CR (Constraint-based Routing) | Flexibilizar as métricas | Eventos e recursos | MPLS-TE/LDP | IETF |
| QoS based routing | Disponibilidade dos recursos, necessidades dos fluxos | Perdas, atraso, <i>jitter</i> e banda disponível | OSPF-TE IS-IS-TE | IETF |
| Policy Routing | Tornar flexível em relação ao campo de destino do IPV4 | Precedencia IP, tamanho do pacote, endereço fonte, fluxo determinado, ToS, interatividade do tráfego. | nenhum | Vegetna, Marsh. |
| Policy Management Networks | Tratamento diferenciado do tráfego | | COPS | Verma, IETF |
| Server Based QoS Routing | Organização centralizada, redução de requisições de rotas com QoS na rede | | OSPF | G. Apostolopoulos |
| Path Caching | Computar os caminhos com antecedência, re-usá-los. | | ATM-PNNI | M. Peryravian, G. Apostolopoulos |
| Rerouting | Alteração dos caminhos após queda ou degradação do enlace | Métricas de QoS | OSPF, IS-IS | Este trabalho de pesquisa, Lemma, Shand & Bryant |

Isso tipicamente irá depender do mecanismo utilizado para requisitar as rotas de QoS. Por exemplo, quando o mecanismo utilizado é o protocolo RSVP, é desejável que a gerência de caminhos se mantenha o mais sinérgica possível com os estados

existentes do RSVP. Em outras palavras, a fixação e a liberação das rotas devem ser coordenadas com os estados *soft* do RSVP, e estruturados de forma que requeiram uma alteração mínima nas regras de processamento do RSVP.

4.5. Roteamento baseado em QoS

Existem muitos estudos na literatura a respeito do roteamento baseado em QoS (Jajszczyk, A. & Rozycki, P., 2006), (Shand, M. & Bryant, S., 2006), (Iovana, P.; Sabela, R. & Settembre, M., 2003), (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998). A RFC 2386 (Crawley, E.; Nair, R.; Rajagopalan, B. & Sandick, H., 1998) trata de um framework para resolver este problema. Segundo os autores, o roteamento baseado em QoS tem sido considerado uma “peça perdida” na evolução dos serviços com QoS oferecidos na Internet. Existem muitas facetas envolvidas no problema, passando pela complexidade dos algoritmos (Ma, Q. & Steenkiste, P., 1997), (Peyravian, M. & Kshemkalyani, 1997), sobrecargas nos protocolos (Shand, M. & Bryant, S., 2006), (Apostolopoulos, G. et al, 1999), até a escalabilidade das soluções (Iovana, P.; Sabela, R. & Settembre, M., 2003), (Guérin, R., 2002), que podem envolver Sistemas Autônomos (AS) diversos.

Roteamento baseado em QoS é um mecanismo de roteamento no qual os caminhos para os fluxos são determinados com base em algum conhecimento da disponibilidade de recursos na rede, bem como dos requerimentos de QoS dos fluxos (Crawley, E.; Nair, R.; Rajagopalan, B. & Sandick, H., 1998) Do ponto de vista do fluxo, o maior problema do serviço best-effort seria que os pacotes de um mesmo fluxo podem seguir caminhos diferentes (Vegetsna, S., 2001).

O roteamento baseado em QoS estende os paradigmas de roteamento de três maneiras básicas (RFC 2386):

a. Para suportar o tráfego usando as classes de serviços dos serviços integrados, múltiplos pares de nós devem ser computados. Algumas dessas novas classes irão requerer métricas de roteamento adicionais, como atraso ou banda. Se alguma dessas

métricas se alterar com frequência, a atualização das rotas consumirá banda dos enlaces e CPU dos roteadores.

b. O roteamento “oportunista” irá trocar de caminho tão logo uma rota melhor seja encontrada. O tráfego será redirecionado mesmo quando a rota atual pode suprir as necessidades do tráfego existente. Se o roteamento baseia-se em cálculos de métricas muito oscilantes, como a banda disponível, são introduzidas oscilações no tráfego, conforme alteram-se os caminhos para uma ou outra rota. As alterações frequentes de rota elevam os atrasos e o *jitter*.

c. Os algoritmos para encontrar o caminho ótimo não suportam rotas alternadas. Se a melhor rota não pode admitir um fluxo novo, o tráfego associado não será transportado, mesmo se existirem rotas alternativas.

Segundo a RFC 2676 (Apostolopoulos, G. et al, 1999) o suporte para roteamento de QoS pode ser visto como um conjunto de 3 componentes:

- a. Obter a informação necessária para computar os caminhos de QoS e selecionar um caminho capaz de atingir as necessidades de uma dada requisição.
- b. Estabelecer o caminho selecionado para acomodar a nova requisição;
- c. Manter o caminho assegurado para o uso de uma dada requisição.

Um caminho possível seria aquele com recursos residuais (não utilizados) suficientes para satisfazer as restrições de QoS de um fluxo. A função básica do roteamento baseado em QoS é encontrar este caminho (Chen, S. & Nahrstedt, K., 1998). Adicionalmente, a maioria dos algoritmos consideram uma métrica abstrata, denominada *custo*, para otimizar o uso dos recursos. O custo total de um caminho é a soma dos custos dos enlaces deste caminho. O problema de otimização é encontrar o caminho de menor custo dentre os possíveis para os requisitos de QoS.

Para suportar QoS, métricas relevantes como atraso cumulativo fim-a-fim em uma rota, e o gargalo da capacidade do link (banda disponível), taxa de perdas e *jitter* são usados nos algoritmos de QoS para encontrar os caminhos. Tais métricas são transportadas pelos protocolos IGP com extensões para Engenharia de Tráfego. O IGP deve calcular não somente o caminho ótimo, mas todos os múltiplos caminhos

possíveis, baseado nas disponibilidades de QoS. Cada fluxo deve transportar as requisições de QoS com ele. Essas requisições podem ser marcadas no campo ToS do cabeçalho do IP, e as rotas são determinadas de acordo com essas necessidades (Vegesna, S., 2001).

Tipicamente, é criado um grafo virtual dos roteadores e dos enlaces, aos quais se associam métricas de custo (Norden, S., 2002). Baseados na métrica, o caminho de menor custo é computado, usando-se algoritmos padrões como o de Dijkstra e Bellman-Ford. O caminho é armazenado nos roteadores, permitindo aos pacotes um roteamento pelo caminho de menor custo. As rotas podem ser calculadas sob demanda, para todos os pacotes, mas na prática, uma rota padrão é armazenada, e os pacotes seguem o caminho já computado. Os caminhos são tipicamente recalculados quando ocorrem certos eventos, como falhas nos enlaces, que invalidam certos caminhos. Os roteadores trocam informações de estado para informar os vizinhos de tais falhas.

Os mecanismos atuais de roteamento usam métricas estáticas para decidir o caminho de menor custo. Uma métrica estática, como a contagem de hops, não considera a carga da rede. Como resultado, não existe balanceamento, e todo o tráfego é roteado pelo caminho com o menor número de hops. Tais caminhos podem então ser facilmente saturados em ambientes com muita carga, levando ao descarte de pacotes e bloqueio de sessões (possivelmente reservas). O roteamento QoS se propõe a remediar este problema, pelo uso de métricas dinâmicas na seleção das rotas. Entretanto, a maioria das abordagens correntes é de alta complexidade, sobrecarregando os roteadores, bem como requerendo freqüentes trocas de estado para atingir algum ganho de desempenho sobre o roteamento tradicional. Isso pode resultar até mesmo em possibilidade de bloqueio das máquinas. Tais métodos, em consequência, não são de fácil aplicação em redes reais.

Alguns estudos demonstram técnicas e algoritmos de roteamento baseado em QoS (Ma, Q. & Steenkiste, P., 1997), (Chen, S. & Nahrstedt, K., 1998), (Yuan, X. & Zheng, W., 2004). Sabe-se que utilizar mais de uma métrica de QoS para encontrar o melhor caminho é um problema NP-Completo (Ma, Q. & Steenkiste, P., 1997). Tal solução

seria análoga às soluções de se encontrar em um grafo o “menor caminho com restrições”.

Segundo estes autores, existem duas classes de problemas NP-completos em roteamento:

- Roteamento com restrições de caminho e otimização de caminho (PCPO, ou path-constrained path optimization);
- Roteamento com multiplas restrições (MPC – multi-path-constrained).

Um exemplo de PCPO é o roteamento de menor custo com restrições de atraso, que procura o menor caminho com limites para o atraso. E um exemplo de MPC é o roteamento com restrições de atraso e *jitter*, que procura um caminho com limite de atraso e limite de *jitter*.

Para que exista de fato a característica NP-Completo, assume-se duas condições:

- as métricas são independentes;
- é possível que sejam números reais ou números inteiros sem limites.

Se todas as métricas, com exceção de uma, são números inteiros limitados, o problema pode ser resolvido em tempos polinomiais, com algoritmos extendidos de Dijkstra (ou Bellman-Ford). Se todas as métricas forem dependentes de uma métrica em comum, o problema também é solúvel em tempos polinomiais. Por exemplo, os piores casos de atraso e *jitter* nas redes usando filas WFQ são funções da largura de banda. Nessas redes, o roteamento com restrições de atraso e jitter seria resolvido em tempos polinomiais (Ma, Q. & Steenkiste, P., 1997).

4.5.1. Extensões de QoS para o OSPF

O protocolo *Open Shortest Path First* (OSPF) foi desenvolvido pelo *Internet Engineering Task Force* (IETF) como um substituto do RIP e é agora o protocolo IGP - *Interior Gateway Protocol* – recomendado pelo IETF. Como o nome está indicando, o OSPF usa um algoritmo SPF - *Shortest Path First*, baseado no algoritmo de Dijkstra. É um protocolo de estado dos enlaces, e é aberto, no sentido de não ser propriedade de um fabricante ou organização. Evoluiu através de várias RFCs. A versão 1 do protocolo foi especificada na RFC 1131, que nunca passou de um estágio experimental. A versão 2, que é a corrente, foi especificada inicialmente na RFC 1247,

e evoluiu com a RFC 2178, que seria substituída mais tarde pela RFC 2328. Um conjunto de especificações auxiliares pretende manter o OSPF apto a suportar rotas com QoS. Tais extensões estão documentadas na RFC 2676 (Apostolopoulos, G. et al, 1999).

Como todos os protocolos LS, as maiores vantagens do OSPF sobre os protocolos de vetor de distância são a convergência mais rápida, a escalabilidade e menor susceptibilidade a erros. Outras características do protocolo são:

- O uso das áreas, que reduz os impactos nos recursos computacionais, contém o fluxo do tráfego do protocolo de roteamento e permite a construção de topologias de interligação hierárquicas;
- Uma métrica arbitrária adimensional.;
- Uso de endereço multicast reservado para reduzir o impacto nos dispositivos onde o protocolo não está operacional;
- Suporte a autenticação;
- Suporte ao campo ToS do cabeçalho IP. Como este suporte nunca foi amplamente implementado, a RFC 2328 retirou a opção de roteamento ToS.

Existem algumas simplificações no modelo para facilitar a introdução de roteamento com QoS. Somente a largura de banda e o retardo foram adicionados como restrições. Além disso, o atraso é tratado pelas políticas, de forma que o algoritmo de seleção dos caminhos tem o foco unicamente na largura de banda. Os enlaces com grandes atrasos de propagação são eliminados antes de selecionar uma rota para uma requisição sensível ao atraso.

Para tratar as necessidades relativas ao atraso, uma extensão simples ao algoritmo de seleção de caminhos pode contabilizar o atraso. Em geral, múltiplas políticas podem ser utilizadas para capturar necessidades diferentes, cada qual apresentando o algoritmo de seleção dos caminhos correspondendo a uma topologia de rede podada, (*pruned*) na qual o mesmo algoritmo pode ser usado para gerar um caminho apropriado (Iwata, A. & Fujita, N., 2000). A idéia é similar a poda de topologia executada pelo protocolo PNNI. Outra consideração a ser feita é o custo computacional do roteamento por QoS, que deve ser similar aos algoritmos de roteamento tradicionais.

Anúncios dos estados dos enlaces

No OSPF a atualização da informação sobre os estados dos enlaces é executada a cada 30 minutos. O roteamento por QoS precisa que as informações sobre os estados dos enlaces sejam atualizadas com mais frequência, para perceber as alterações rapidamente, evitando decisões incorretas. Existe um compromisso entre a sobrecarga do protocolo pelas atualizações freqüentes e a precisão da informação sobre o estado da rede. A idéia básica é disparar os anúncios somente quando houver uma alteração significativa no valor das métricas desde o último anúncio (Iwata, A. & Fujita, N., 2000). Enquanto as alterações não acontecem, um gatilho periódico pode ser adicionado, para reduzir o período entre os anúncios. Dessa forma os pacotes de comunicação do protocolo aumentam consideravelmente, mas ocupam pequena largura de banda.

Extensões do protocolo OSPF

Existem duas propostas para codificar a QoS no OSPF (Q-OSPF):

- Baseado no campo ToS ;
- LSA-Opaco.

Na literatura, encontra-se um destaque para o uso do campo TOS (Apostolopoulos, G. et al, 1999, Doyle, J., 1998) O campo de opções do OSPF está presente nos pacotes HELLO do protocolo, pacotes de descrição da base de dados e em todos os pacotes de anúncio do estado dos enlaces (LSA).

O bit menos significativo na especificação original do OSPF indicava a capacidade de roteamento pelo tipo de Serviço (TOS). Essa característica foi removida da especificação por falta de utilização. Por razões de compatibilidade, os roteadores ainda podem anunciar métricas baseadas no TOS através dos pacotes LSA. Nas extensões de QoS, o bit T é re-utilizado para indicar a capacidade de QoS do OSPF, sendo denominado bit "Q". O roteador pode configurar o bit Q nos seus pacotes HELLO, para indicar que é capaz de suportar roteamento baseado em QoS. Se o bit estiver configurado, significa que existem campos com informações de QoS para serem processadas nos pacotes. Em uma rede, o campo configurado anuncia, através dos

LSAs, capacidades de QoS na rede. A versão 2 do OSPF especifica 5 tipos diferentes de serviços, podendo suportar até 16. Pelo uso de 5 bits no campo TOS, 32 combinações estão disponíveis para recursos de QoS.

Algoritmo para seleção do caminho

O algoritmo procura satisfazer as requisições de banda do fluxo, enquanto busca minimizar o número de hops necessários. O menor custo computacional deve ser preferido. Um algoritmo para QoS sob demanda é caro em termos de recursos computacionais e não é prático na maioria dos casos. Segundo (Guérin, R., 2002) o algoritmo de Dijkstra pode ser aplicado para computação sob demanda, com pequenas modificações. Outro bom candidato para pré-computação dos caminhos é o algoritmo de Bellman-Ford, que pode tratar uma segunda métrica (numero de saltos) sem aumentar a complexidade.

4.5.2. Roteamento baseado em Restrições-*Constraint-based routing* (CR)

O Roteamento baseado em Restrições (CR, ou *Constraint-based routing*) é um mecanismo usado para se alcançar as necessidades da Engenharia de Tráfego (Jamoussi, et al., 2002). O CBR foi proposto por (Awduche, D.; Malcolm, J.; Agogbua, J.; O'Dell, M. & McManus, J., 1999). Segundo os autores, a terminologia atual refere-se a essa técnica muitas vezes como Roteamento QoS, (QoS Routing) genericamente. Na RFC 2702, o termo escolhido é "*constraint-based routing*" por expressar melhor a idéia, que normalmente envolve o roteamento de QoS como um subconjunto.

A tecnica de CR possibilita um paradigma de roteamento voltado para eventos e reservas de recursos, convivendo com os IGPS (e o paradigma de SPF). Um Framework de roteamento CR utiliza os seguintes atributos como entrada:

- a. Atributos associados aos agrupamentos de tráfego (traffic trunks).
- b. Atributos associados aos recursos
- c. Outras informações associadas ao estado da topologia.

Um processo CR, com base nessas informações, automaticamente computa rotas explícitas para cada agrupamento de tráfego que esteja sendo originado em um nó da rede. Neste caso, uma especificação pode ser enviada pelas técnicas de sinalização discutidas no capítulo 5.4.

Um framework para CR poderia reduzir bastante o nível de configurações manuais e intervenções necessárias para atualizar as políticas de engenharia de tráfego.

4.5.3. Roteamento baseado em políticas

Uma política é uma diretiva especificada pelo administrador de um sistema (no escopo deste trabalho, uma rede), que maneja certos aspectos do resultado esperado da interação entre usuários e aplicações. A política fornece um roteiro sobre como os diferentes dispositivos (roteadores, servidores, firewalls) devem tratar o tráfego resultante dos diferentes usuários e aplicações (Verma, D., 2000).

Basicamente, a idéia do roteamento baseado em políticas é uma tentativa de minimizar as limitações do roteamento tradicional, que decide os caminhos dos pacotes com base no seu destino. Aplicando-se a técnica, pode-se decidir o caminho com base em parâmetros diferentes, como o tamanho do pacote, o endereço da fonte do fluxo, os bits de precedência do campo ToS do cabeçalho do IPv4 (Vegesna, S., 2001). As fontes de pacotes (aplicações mais avançadas) estão com habilidades de determinar o tipo de caminhos que seus pacotes irão necessitar. Entretanto, essa mudança de paradigma não deveria reduzir a robustez original do protocolo IP, ou seja, sua capacidade de contornar os caminhos que apresentem falhas (Verma, D., 2000).

4.6. Engenharia de Tráfego

Engenharia de Tráfego Internet é definida como aquele aspecto da Engenharia de redes Internet que trata das questões de avaliação de desempenho e otimização de desempenho de redes IP operacionais. Abrange a aplicação de princípios científicos e tecnologia para medir, caracterizar, modelar e controlar o tráfego na Internet - RFC-3272 (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002).

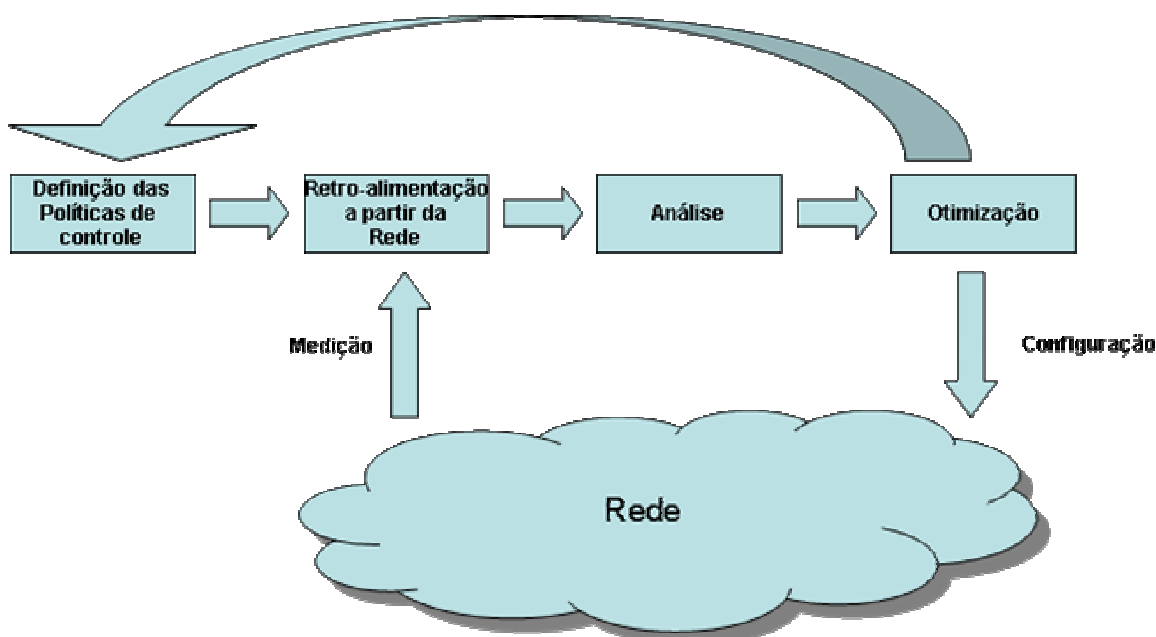


Figura 4-3 - Processo de Engenharia de tráfego - Fonte: (RFC 3272)

Uma definição prática pode ser encontrada em (Osborne, E. & Simha, A., 2003), que declaram ser a engenharia de tráfego “a manipulação do tráfego para condizer com a rede, enquanto a engenharia de redes é a manipulação da rede para manter o tráfego”.

Muitos estudos sobre estas técnicas podem ser encontrados na literatura (Iovana, P.; Sabela, R. & Settembre, M., 2003), (Ali, M.; Chirivalu, G. & Ge, A., 2005).

O processo de engenharia de tráfego é definido como constituído de quatro fases partes (demonstradas na Figura 4-3) com base na RFC 3272. Essas partes serão descritas nas próximas seções, a seguir.

4.6.1. Definição de políticas de controle relevantes

Este processo (fase 1) pode ser considerado externo ao circuito de engenharia de tráfego atual, sendo um controlador do seu progresso. Naturalmente as políticas de controle podem e são ajustadas com base nas observações de desempenho.

Os mecanismos de alimentação para este processo podem ser a qualidade de serviço requerida para suportar os diferentes tipos de tráfego e os algoritmos de otimização. Por exemplo, a rede pode ter uma configuração para as horas de grande ocupação (pico de alta) e outra para as horas de baixo uso.

4.6.2. Mecanismos de retro-alimentação

Tais mecanismos compõem a 2ª. Fase e são usados pela aquisição de dados de medições da rede de produção. De acordo com a RFC 3272, este segundo estágio nos processos de Engenharia de Tráfego não devem se limitar a obtenção da rede somente, mas também utilizar cargas sintéticas, caso os resultados imediatos não estejam disponíveis a partir da rede de produção. A sintetização da carga pode ser baseada em resultados anteriores, por exemplo. Se tratar-se de rede multi serviços a sintetização pode ser mais complexa, mas mesmo assim necessária.

4.6.3. Análise do estado da rede e caracterização da carga do tráfego

Essa terceira fase do modelo pode ser proativa e/ou reativa. A análise proativa identifica os problemas potenciais. A análise de desempenho reativa identifica os problemas existentes e determina suas causas através de diagnósticos. Avaliar abordagens alternativas para remediar o problema, quando necessário. Várias técnicas quali e quantitativas podem ser utilizadas no processo de análise, inclusive análises baseadas em modelagem e simulação. A fase analítica do processo pode envolver a investigação da concentração e distribuição do tráfego na rede, identificando a carga, gargalos potenciais e patologias como enlaces ineficazes, pontos únicos de falha, etc. As patologias da rede podem ser resultado de fatores diversos, como arquitetura inferior da rede, projeto e problemas de configuração. Uma matriz de tráfego pode ser construída como parte do processo de análise. A análise da rede pode ser ainda descritiva ou prescritiva.

4.6.4. Otimização do desempenho da rede

A quarta fase do modelo é a otimização do desempenho da rede. Envolve um processo de decisão que seleciona e implementa um conjunto de ações. As ações de otimização podem incluir técnicas de controle do tráfego oferecido ou controlar a distribuição do tráfego através da rede. Pode envolver adição de enlaces ou aumento da capacidade, com os ajustes necessários dos parâmetros de roteamento e gerência

de tráfego. Pode envolver planejamento para melhorias no projeto da rede, como capacidade e tecnologias, e a configuração dos componentes para acomodar crescimentos.

Como demonstra a Figura 4-3, os processos de engenharia de tráfego são interativos, e evocam da sequência indução/dedução na filosofia da ciência (Raisanen, v., 2003). Como regra geral, os conceitos e mecanismos de Engenharia de Tráfego devem ser específicos para atingir necessidades conhecidas, mas simultaneamente flexíveis para prever demandas.

A melhoria de desempenho das redes é vista como um desafio constituído de duas partes: (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002)-RFC 3272: Gerência de capacidade e gerência de tráfego. Essas gerências operam em escopos diferentes, e em escalas de tempo também diferentes, tomando-se por base o comportamento da rede. Gerência de capacidade trata da organização do desempenho usando a alocação de capacidades em partes de rede ou em todo o domínio. A gerência de tráfego trata do suporte aos serviços, focando-se nos nós individuais.

A otimização do desempenho da rede é visto como um processo contínuo, não um processo que ocorre uma única vez. As metas da otimização também podem variar com o tempo. A automação dos controles dos problemas para otimização de desempenho é um desafio a parte neste escopo. Quando atingida essa meta, a auto-otimização da rede não deve levar a instabilidades no comportamento dessa rede.

O objetivo da engenharia de tráfego em uma rede multi-serviços é manter uma utilização ótima dos recursos, dada uma composição do tráfego nessa rede. A gerência de capacidade consiste das seguintes tarefas:

- Planejamento de capacidade;
- Controle do roteamento;
- Gerência de recursos (capacidades dos enlaces, espaço nos *buffers*, recursos computacionais).

Planejamento de capacidade envolve o planejamento para os recursos necessários para rede, incluindo a vazão nos roteadores e a capacidade dos enlaces. A computação dos valores iniciais dos parâmetros de cada elemento de rede como os condicionadores de tráfego, tamanho dos *buffers*. Dependendo da topologia o controle

do roteamento é uma ferramenta que afeta a distribuição do tráfego na rede. Para um ambiente de roteamento com OSPF, ajustar as métricas do protocolo é uma forma de controlar o roteamento. O controle do roteamento pode ser aplicado na granulometria dos pacotes, fluxos e no suporte a QoS. Sabe-se que a maior parte dos serviços se beneficiam com valores de *jitter* sendo os menores possíveis.

A Gerência de tráfego, por sua vez consiste nas seguintes tarefas:

- Controle de tráfego por nó (condicionadores de tráfego, gerência de filas, escalonamento);
- Outros controles de fluxos.

Os problemas de engenharia de tráfego normalmente podem ser associados com problemas de otimização dos enlaces (Ali, M.; Chirivalu, G. & Ge, A., 2005),(Swallow, G., 1999). Podem também relacionar-se com a otimização dos fluxos. Os objetivos chave de desempenho associados com a Engenharia de Tráfego podem ser classificados como (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002):

- Orientados ao tráfego. Objetivos que pretendem preservar os fluxos.
- Orientados aos recursos. Visam maximizar o uso dos recursos, evitando a necessidade de sobreprovisionamento.

Uma situação típica de roteamento na Internet é utilizada para ilustrar a importância da Engenharia de Tráfego (TE), denominada “Problema do Peixe” (Figura 4-4) (Osborne, E. & Simha, A., 2003) na otimização dos recursos.

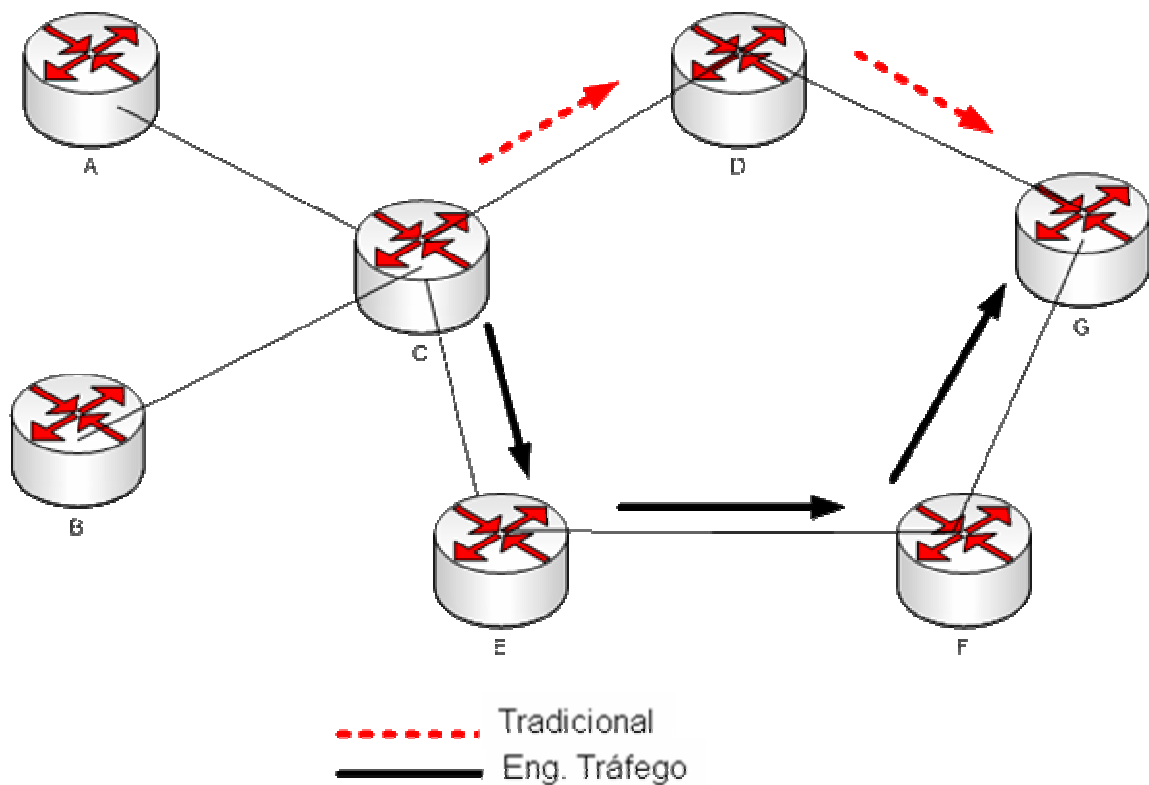


Figura 4-4 - Problema do peixe – Fonte: (Osborne, E. & Simha, A., 2003)

Este problema mostra a ineficácia dos protocolos IGP (OSPF, IS-IS) em determinar o melhor caminho, uma vez que suas métricas classicamente escolhem os caminhos mais curtos (são protocolos dito SPF – shortest path first). Isso implica em montar a topologia da rede pela minimização do número de saltos. Como consequência, todos os roteadores com o protocolo dentro de um sistema autônomo obtém um panorama completo de todos os roteadores e enlaces nesta rede. Cada roteador então usa essa informação para computar o menor caminho para todas as subredes usando este algoritmo. O roteador monta então uma tabela de repasse, associando um prefixo de endereço com o enlace do next-hop. Quando um pacote alcança o roteador, a tabela de repasse é consultada, e os pacotes são repassados ao enlace apropriado com base no endereço de destino. Essa abordagem funciona bem quando a topologia apresenta poucos roteadores. Quando a densidade de máquinas aumenta, problemas de balanceamento de carga podem surgir. Com este algoritmo, pode-se prever que os caminhos mais longos sempre serão preteridos, mesmo que a ociosidade do enlace ou suas condições de tráfego permitissem maior desempenho até o destino. A Engenharia de Tráfego permite que se adotem caminhos alternativos, mesmo que não sejam os menores. A idéia é melhorar o desempenho e otimizar os recursos das redes.

4.7. Re-roteamento (rerouting)

A técnica de re-roteamento pode ser utilizada tanto em MPLS (label switching) como em comutação de pacotes (packet switching) (Lemma, H. G., 2003). O re-roteamento pode ser definido, segundo a RFC 3469 - *Framework for multi-protocol label switchinfg (MPLS)-based Recovery* –(Sharma, V. & Hellstrand, F., 2003) como “o estabelecimento de um novo caminho ou segmento na demanda pelo re-estabelecimento do tráfego após a ocorrência de uma falha”. Desta maneira, pode ser visto como um mecanismo no qual a recuperação de um caminho ou segmento é criada dinamicamente, após a detecção de falha no caminho atual. Nesta perspectiva, é necessário um caminho alternativo além do caminho primário usado pelo tráfego. Os caminhos primário e de reserva devem ser totalmente desvinculados. Os componentes de rede consistem de enlaces e nós. A falha de um nó causa a falha dos enlaces adjacentes conectados a este nó. Assim, pode-se considerar a falha de um enlace como uma falha na rede.

Nas topologias utilizadas normalmente na Internet, sempre que se analisa um período de tempo razoável, pode-se perceber que as topologias de rede não são estáveis (Shand, M. & Bryant, S., 2006). Um sistema de engenharia de tráfego deve responder as mudanças de forma eficiente. Para manutenção da QoS, a habilidade de transportar os dados com confiabilidade e eficiência é um componente importante.

Deve-se considerar que os protocolos de roteamento, embora robustos, podem demandar um período de tempo significativo para se recuperar de uma falha (Shand, M. & Bryant, S., 2006). Este período pode ser de muitos segundos (para os IGPs) até minutos (para os EGPs) (Sharma, V. & Hellstrand, F., 2003). Uma falha com essa magnitude de tempo causa uma interrupção nos serviços de algumas aplicações (tráfego de voz, Virtual leased lines, tráfego de vídeo). Este aspecto negativo também compromete as arquiteturas consideradas clássicas para manutenção de QoS, como o IntServ e DiffServ. Segundo os autores da RFC, um valor de tempo aceitável seria na ordem de segundos ou dezenas de milisegundos.

Ainda segundo a RFC 3469, o roteamento IP pode não ser capaz de recuperar a largura de banda, que tem por objetivo prover não só uma rota alternativa, mas também uma banda equivalente àquela disponível no caminho original.

O re-roteamento é necessário em duas escalas de tempo diferentes: Re-roteamento rápido (Shand, M. & Bryant, S., 2006) e re-roteamento otimizado (Swallow, G., 1999). O modo rápido minimiza o rompimento dos serviços para os fluxos afetados por uma queda. O re-roteamento otimizado re-otimiza os fluxos para uma topologia alterada. Neste trabalho de pesquisa, adota-se o re-roteamento otimizado, uma vez que o objetivo específico das alterações de caminho é a manutenção da qualidade dos serviços de forma pró-ativa, o que deve acontecer antes das quedas ou mesmo das degradações mais severas.

Quando um enlace do caminho principal falha, o processo de restauração inicia-se automaticamente. Uma técnica de re-roteamento completa pode ser encontrada na RFC 3469 (Sharma, V. & Hellstrand, F., 2003), e é constituída de vários passos. Basicamente, esses procedimentos são detecção da falha, notificação da falha, computação do caminho alternativo, re-roteamento para esse novo caminho, reversão do tráfego.

4.7.1. Detecção da falha

A rede deve ser capaz de detectar falhas nos enlaces. Isso pode ser função de um hardware específico ou através de software nos nós finais dos enlaces. Neste trabalho, os fluxos de medição geram os relatórios nas estações colocadas nos pontos finais dos enlaces (capítulo 5). A detecção se dá em termos de limiares para as métricas, não sendo necessária uma falha no enlace. O software dos agentes de monitoração, ao efetuarem a leitura dos relatórios das medições, são os responsáveis pela detecção dessa ultrapassagem do limiar.

4.7.2. Notificação da falha

Os nós que detectam uma falha no enlace, denominados nós de alerta, devem notificar certos nós. Quais os nós que serão notificados depende da técnica de re-

roteamento utilizada. Os nós de alerta iniciam o processo de restauração de falhas de acordo com o método para determinar os enlaces com falhas, e enviar a mensagem de notificação, requisitando uma busca por caminhos alternativos ao nó na direção do núcleo da rede. No plano de controle sugerido neste trabalho, esta função é desempenhada pelos agentes de monitoração, que avisam da degradação do fluxo de voz ao QNS.

4.7.3. Computação do caminho alternativo

O nó mais próximo do núcleo da rede executa a computação do caminho alternativo logo que receba a mensagem de notificação. Se este nó não for responsável pelo redirecionamento do tráfego, ele deve repassar para o roteador mais interno. No plano de controle proposto neste trabalho, a computação do novo caminho é executada pelo QNS.

4.7.4. Re-roteamento para o novo caminho

Este processo redireciona o tráfego para o caminho determinado no processo anterior. Este processo completa a restauração dos caminhos após a falha. No plano de controle proposto, esta função está a cargo do QNS, que executa a reconfiguração dos roteadores caso o gatilho de deterioração dos caminhos seja disparado pelos agentes de monitoração.

4.7.5. Reversão do tráfego

Este é o processo que retorna o tráfego do caminho alternativo para o caminho original, após a restauração da falha do enlace. Quando este processo é utilizado, o mecanismo deve detectar a recuperação total do enlace que falhou. Neste trabalho de pesquisa, o QNS efetua reversão do tráfego após o término do fluxo de voz a ser preservado.

Na arquitetura MPLS, qualquer Label-Switched Path (LSP) pode ser dinamicamente trocada de um caminho congestionado para um alternativo. Isso representaria um

aumento de eficiência sobre os métodos tradicionais de operação das redes IP, porque garante aos administradores uma troca de caminhos emergencial em caso de congestionamento. Além disso, os administradores podem fazer uso de otimizações globais, e não somente localizadas. O ISP pode ter uma utilização muito maior de seus links, enquanto provê um serviço com menores custos, se comparado ao sobreprovisionamento.

Entretanto, na tecnologia MPLS (seção 4.7.7), o cálculo dos caminhos é realizado segundo o método CSPF, ou Constrained Shortest Path First (menor caminho primeiro, com restrições), considerando Largura de banda, Atributos do link (um rótulo de 32 bits para “descrever” o link) e Pesos administrativos (Osborne, E. & Simha, A., 2003) . As métricas de jitter e perdas não podem ser utilizadas, e o atraso somente pode ser inferido pelo uso da banda. O plano de controle proposto neste trabalho, ao contrário, possui características de monitoração e reconfiguração praticamente instantâneas, baseadas no jitter ou nas perdas.

A Engenharia de tráfego através do controle explícito de rotas, é uma parte importante de qualquer solução para prover QoS (Armitage, G., 2000-b), embora seu impacto maior seja notado na eficiência geral da rede, e seja menos visível ao usuário final. Com essa abordagem, devido ao descarte das informações oriundas dos protocolos de roteamento tradicionais, os administradores precisam suprir uma fonte de informação externa para controlar o tráfego. Neste trabalho, essa fonte é representada pelo QNS, Servidor de QoS da Rede.

O controle explícito das rotas pode ser obtido por uma variedade de métodos, tanto evitando quanto permutando as decisões convencionais dos protocolos. No nível do protocolo IP, os métodos mais discutidos incluem:

- Opção de roteamento rígido e independente da fonte;
- Tabelas de repasse com busca em outros campos do cabeçalho IP (ToS, por exemplo);
- Tunelamento IP;
- Multiprotocol Label Switching (MPLS).

4.7.6. Inundação (*Flooding*)

A maioria das implementações de Engenharia de Tráfego exige que os protocolos Link State sejam estendidos para atingir as métricas necessárias para a manutenção da QoS. Tais protocolos trabalham unicamente com as informações UP e Down dos enlaces, desconhecendo a banda máxima ou a residual (reservável).

Dado que é necessário re-calcular estes caminhos com base em estados mais dinâmicos (como a taxa de perdas de um enlace), pode-se incorrer no problema da sinalização. Isso significa que os novos protocolos podem inundar demasiadamente os enlaces com informações sobre os estados (*flooding*) (Jha, S.; Hassan, M., 2002). As propostas de melhorias dos IGPs - RFCs 3630 (Katz, D.; Kompella, K. & Yeung, D., 2003) - e 2676 – (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998)) baseiam-se logicamente na troca das informações *inband*, o que potencializa o problema do *flooding*. Uma das contribuições deste trabalho de pesquisa é o melhoramento das estratégias de troca de informações sobre os estados, minimizando a inundação.

Com o uso criterioso e uma quantidade bem dosada de métricas, as mensagens podem ser trocadas entre uma estação de gerência de QoS (QNS) e os roteadores sem afetar o desempenho.

4.7.7. Engenharia de Tráfego MPLS (MPLS-TE)

Basicamente, a idéia das arquiteturas que implementam Engenharia de Tráfego na Internet (a MPLS-TE é uma delas), é permitir aos roteadores a construção de caminhos usando informações outras que não o caminho mais curto do IP (SPF, ou *Shortest Path First*).

Na abordagem da MPLS-TE, as informações que são distribuídas e que permitem este cálculo mais inteligente são as seguintes:

- a. Banda disponível por interface, com prioridades, para permitir que alguns túneis precedam a outros;
- b. Flags de atributos por interface (32 bits em hexa);
- c. Pesos administrativos por interface.

Cada uma dessas informações é anunciada com base em cada enlace. Em outras palavras, um roteador anuncia a banda disponível, os flags de atributos e as métricas administrativas para todos os enlaces envolvidos na MPLS-TE.

Existem duas abordagens diferentes para este tópico, em estudos no *IETF MPLS Working Group*. Elas caracterizam a porção de “sinalização” na engenharia de tráfego dentro do MPLS. Existem duas maneiras de implementar um caminho de comutação de rótulos (LSP):

- Hop a hop, orientado ao controle, que utiliza o protocolo de distribuição de Rótulos (*Label Distribution Protocol* – LDP);
- Roteamento explícito LSP (ER-LSP).

As duas abordagens da engenharia de tráfego são :

- TE-RSVP :Engenharia de Tráfego RSVP;
- CR-LDP: LDP baseada em contenção.

Essas duas abordagens representam a utilização do ER-LSP, ou Roteamento Explícito LSP. Isso implica em que, por ter a habilidade de implementar a rota usando as CoS e QoS pré definidos, o LSP ótimo para um tráfego específico pode ser assegurado.

Um dos serviços mais importantes que podem ser oferecidos pela utilização do MPLS em geral e pelo protocolo de distribuição de rótulos (LDP) em particular é o suporte para o roteamento baseado em restrições (CR).

O roteamento baseado em restrições (CR) 4.5.2) é um mecanismo utilizado para alcançarem-se as requisições de Engenharia de Tráfego. O roteamento explícito é um subconjunto da técnica de CR, como proposto pelo grupo de trabalho MPLS WG do IETF.

Na tecnologia MPLS os pacotes são encapsulados nos pontos de ingresso, e etiquetados com rótulos que serão usados para repassá-los ao longo da rota de comutação por etiquetas (LSP, ou Label Switched Paths). Os ISPs podem utilizar uma LSP com garantia de largura de banda como componente de uma Rede Virtual Privada (VPN, ou Virtual Private Network). Tal garantia de banda seria usada para cumprir os

acordos de níveis de serviços (SLA, ou Service Level Agreement) praticados com os usuários (Kodialam, M. S.; Lakshman, T. V.; Sengupta S., 2000). Estes caminhos podem agregar o tráfego através da classificação dos pacotes que estão chegando nos roteadores de borda de uma rede MPLS, dentro de classes de equivalência ou Forwarding Equivalence Classes (FEC). Essa classificação dentro das classes de equivalência é feita usando-se filtros de pacotes para examinar os cabeçalhos (informações sobre endereço fonte, destino, bits ToS). As regras do filtro determinam que as classes de equivalência para repasse (FEC) podem ser estabelecidas através de interações com protocolos de roteamento, por exemplo. O propósito da classificação é possibilitar engenharia de tráfego na rede do ISP, e rotear cada uma das classes de uma maneira específica. Isso é possível mapeando-se os pacotes que chegam nas interfaces e pertencem a determinada FEC para uma LSP associada a ela. A LSP deve ter sido configurada antes do mapeamento, através de um protocolo de sinalização, como por exemplo o RSVP (pode-se utilizar também o LDP – *Label Distribution Protocol*).

Uma questão importante a respeito das LSPs é a sua capacidade de serem roteadas explicitamente através de caminhos específicos. Isso significa que todo o caminho intermediário entre os roteadores de ingresso e saída na rede pode ser especificado. As rotas M-LSP (multicast LSP) podem ser implementadas sem extensões na sinalização (Kodialam, M. S.; Lakshman, T. V.; Sengupta S., 2000).

Quadro 4-2-Comparação entre métodos de sinalização RSVP-TE e CR-LDP

| | RSVP-TE | CR-LDP |
|--|--|--|
| História | Extensões a RFC 2205 –RSVPv1 | Extensões a RFC 3036 – LDP |
| Transporte | IP – protocolo 46 | UDP 646 (<i>hello & discovery</i>) |
| Estado da sessão | Soft – redução do refresh | Hard – TCP |
| Recuperação de falhas | Sem conexões TCP para manter através dos nós | Perda da conexão TCP causa perda do LSP |
| Direção da reserva | Direção reversa | Direção direta (em frente) |
| Controle de admissão da chamada | Sim, na direção reversa | Sim, na direção direta |
| Parâmetros de sinalização de tráfego | Banda, afinidade dos enlaces | Banda, afinidade dos enlaces |
| Objeto de registro da rota | Sim | Sim |
| Registro da origem da rota (<i>pinnig</i>) | Sim | Sim |
| Políticas | Sim | Sim |
| Re-roteamento rápido | Sim | Sim |
| Métodos de distribuição de rótulos | Downstream sob demanda | Downstream sob demanda |
| Preempção | Prioridades na configuração e manutenção | Prioridades na configuração e manutenção |
| Re-otimização do roteamento | Sim | Sim |
| Segurança | Sim –MD5 | Conexão TCP e MD5 |

Fonte: (Alwayn, V. , 2002)

Em redes onde a Engenharia de tráfego não é aplicada, os protocolos IGP devem se encarregar das alterações com base em suas próprias métricas. Em uma rede sem MPLS-TE, o IGP propaga informação sobre os enlaces em 3 casos (Alwayn, V. , 2002):

1. Quando um enlace é interrompido ou estabelecido.
2. Quando uma configuração de um enlace é alterada (quando um custo é modificado, por exemplo).
3. Quando se atinge o tempo periódico de re-inundar as informações dos roteadores pelo IGP.

Uma grande variedade de temporizadores está associada com essas ações. Eles diferem em função de qual o IGP está sendo utilizado (Doyle, J., 1998).

As técnicas de Engenharia de Tráfego mais recentes, usando por exemplo MPLS, adicionam mais um motivo para a ação de inundação: A alteração da largura de banda. Quando um túnel é montado, a banda disponível diminui. Quando ele é desativado, a banda disponível aumenta. Neste trabalho, incluímos as métricas de perdas, atraso e variação do atraso como parâmetros considerados importantes no disparo dos gatilhos de re-roteamento, efetuado através da sinalização fora de banda.

Uma questão importante é o momento do anúncio da mudança. Se for muito rápido, as inundações podem ser imensas, porque as alterações podem ser em intervalos pequenos. Deve-se considerar que podem existir vários milhares de túneis em uma rede utilizando Engenharia de tráfego com MPLS-TE, por exemplo.

Existem 3 regras para os compromissos de divulgação (flooding thresholds) (Alwayn, V. , 2002):

1 - Divulgar as alterações significativas imediatamente. Cada vez que a banda é reservada, as reservas são re-consideradas. Se o total de banda alterada é suficiente para passar um threshold, a informação sobre este link é divulgada imediatamente.

2 - Divulgar as alterações não significativas periodicamente, a intervalos menores que o IGP (Default = 180 seg).

3 - Se uma alteração ainda não anunciada reconhecidamente causará um erro, divulgar imediatamente.

É possível que uma rota escolhida logo no próximo instante possa não ser mais a melhor, em virtude de alterações nas condições da rede. Neste trabalho, essa situação ficou bem clara em vários momentos, onde o plano de controle precisou trocar o caminho escolhido mais de uma vez durante um período de amostragem (capítulo 7). Essas questões estão tipicamente dentro do escopo da área de “gerência de rotas”, segundo a RFC 2676 (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998).

4.8. Arquiteturas de QoS

Várias propostas de arquiteturas ou frameworks para manutenção das métricas de desempenho têm sido propostas na literatura (Iovana, P.; Sabela, R. & Settembre, M., 2003), (Finenberg, V., 2002), (Jajszczyk, A. & Rozycki, P., 2006), (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005), (Liu, H.; Pendarakis, D.; Komaee, N. & Tellium, D. S., 2002), (Ma, Q., 1998), (Marsh, M. G., 2002). Dada a dinâmica do comportamento das aplicações no uso dos enlaces, uma forma de rearranjar os caminhos pode ser considerada crítica.

Algumas preocupações básicas devem ser consideradas sempre que a manutenção das métricas de desempenho para QoS estiver sendo abordada:

- Interrupção dos enlaces;
- Freqüência da troca de informações a serem transferidas para sinalizar os caminhos;
- Métricas usadas nos cálculos;
- Quais os fluxos/conexões que serão protegidos;

Todos os ambientes com estabelecimento prévio de caminhos, como é o caso do IntServ e do MPLS, têm problemas quando um dos enlaces for interrompido (Alwayn, V., 2002). As propostas para o reestabelecimento das conexões podem ser divididas em centralizadas e distribuídas. Tanto uma quanto a outra podem ser classificadas em planejadas ou dinâmicas. E os modos de restauração dos caminhos usados também se dividem em locais ou globais.

Quadro 4-3 Propostas de métodos para Re-Rotamento

| Classificação das Propostas de Restabelecimento de Rotas | | |
|--|------------------|--------------|
| Quanto às responsabilidades dos dispositivos | Centralizadas | Distribuídas |
| Quanto à dinâmica | Pré-estabelecida | Dinâmica |
| Quanto a abrangência | Local | Global |

Fonte: (Lemma, H. G., 2003)

A restauração centralizada, como é a proposta deste trabalho de pesquisa, possui a vantagem de sempre possuir uma informação global dos estados dos enlaces, mesmo durante as falhas. Essa técnica permite uma utilização efetiva dos recursos ociosos, e utiliza menos a rede (Shand, M. & Bryant, S., 2006). Por outro lado, o re-arranjo dos caminhos pode ser mais lento.

Nas propostas que consideram a técnica distribuída, visando otimizar o tempo de restauração dos caminhos, cada nó da rede tem condições de tratar as falhas. A percepção da falha é rápida nas proximidades do nó que falhou, mas a troca de informações para o re-arranjo da topologia global pode consumir tempo e recursos da rede.

4.8.1. *Common Open Policy Service (COPS)*

O protocolo COPS (*Common Open Policy Service*) foi definido através da RFC 2748 (Durham, D.; Boyle, J.; Cohen, R.; Herzog, S.; Rajan, R.; & Sastry, A., 2000). O propósito do COPS é trocar informações de política entre o PDP (Policy Decision Point – demonstrado na Figura 1-7) e os seus clientes, denominados PEP (Policy Enforcement Points). O protocolo emprega o modelo cliente/servidor, sendo o PDP o servidor e os PEPs os clientes. Como emprega conexões TCP para transporte, não existe necessidade de mecanismos de confiabilidade no protocolo. O COPS suporta 2 modelos de funcionamento: Fontes externas e provisionamento de política. O provisionamento é suportado pela arquitetura dos serviços diferenciados (DiffServ – seção 3.7). Neste modelo, o usuário contacta o PDP. O tipo *outsourcing* é suportado pelo modelo de Serviços Integrados/RSVP (seção 3.6), onde a abordagem do usuário é

no PEP (um roteador, por exemplo), e este contacta o PDP. Para suportar provisionamento de políticas, foi adicionado um novo tipo de cliente, denominado COPS-PR (COPS for provisioning), definido na RFC 3084 (Chan, K. et. al, 2001). Este protocolo é independente do tipo de política, e pode transportar informações de segurança, VPN e QoS. O COPS-PR possui um modelo de dados com base no conceito das Bases de Informações de Políticas – PIB. O espaço de nomes da PIB é comum ao PEP e a PDP. A PIB não faz parte da especificação do COPS-PR. Para fornecer segurança de alto nível, as mensagens COPS usam algoritmo HMAC, IPSEC e outros mecanismos. Dessa forma, o canal de comunicação entre o PEP e a PDP está protegido.

4.8.2. Gerência baseada em políticas (PBM)

A simples existência das técnicas para melhoria da QoS (DiffServ, RSVP, MPLS) não são suficientes sem que se tenham formas de gerenciar as configurações dos dispositivos de redes (routers, switches, firewalls, *hosts*) (Raisanen, V., 2003). O número de conjuntos de configurações que precisam ser gerenciadas cresceu rapidamente. Um desafio próximo seria a gerência de usuários e serviços de rede ao invés dos tradicionais dispositivos de rede (Kosiur, D., 2001). A redução do número de interfaces para configuração, redução do risco de falhas por erros acidentais de configurações manuais, são tópicos que devem pautar os projetos que visam a configuração das redes. Outro compromisso desejável é a utilização de agentes inteligentes, capazes de assumir a delegação do controle de elementos de rede.

Um novo paradigma para automatizar as tarefas de configuração de uma rede é a gerência baseada em políticas. Essa gerência pode também delegar poderes limitados de configurações aos dispositivos de rede.

Do ponto de vista da engenharia de tráfego, a gerência baseada em políticas é um segmento da área de configuração, embora tenha status bem mais elevado do ponto de vista da gerência (Verma, D., 2000). A gerência baseada em políticas integra dois organismos de padronização: O IETF, através da RFC 3060, e o DMTF - Distributed Management Task Force, através do Common Information Model (CIM - a versão 2.2 da especificação está disponível em http://dmf.org/standards/cim/cim_spec_v22).

Os temas centrais da gerência baseada em políticas são as bases de informações de gerência, e a habilidade de delegar capacidade de decisão aos elementos de rede.

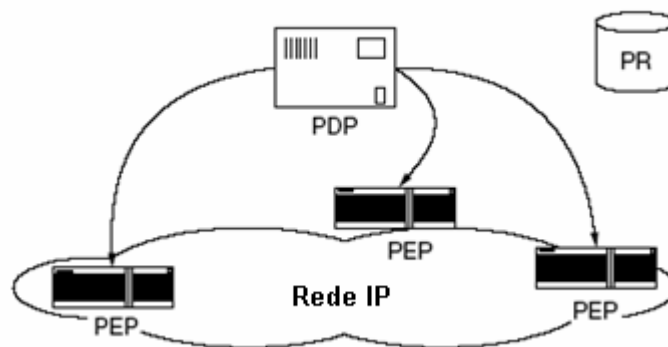


Figura 4-5 - Arquitetura da gerência baseada em políticas (PBM) – Fonte: (Verma, D., 2000)

PR=repositório de políticas

PDP=Ponto de decisão de políticas

PEP=Ponto de execução de políticas

As políticas são armazenadas no repositório, onde são escolhidas pelo PDP, o ponto de Decisão de Políticas. As políticas são implementadas nos pontos de execução de políticas (PEPs). Dentro de um PEP, a implementação de uma política é refletida como uma configuração.

Ponto de decisão de Política (PDP)

O PDP é responsável pelas funções listadas abaixo (Verma, D., 2000):

- Localização do conjunto de regras que são aplicáveis a qualquer PEP que ele esteja gerenciando e recuperando as regras para o repositório.
- Transformação do conjunto de regras que ele recupera do repositório de políticas para formatos e sintaxes compreensíveis pelas funções do PEP.
- Verificação do estado corrente da rede e validação de que as condições requeridas para a aplicação de qualquer política estejam satisfeitas. Um exemplo disso é a verificação de que o tempo atual condiz com o período de tempo no qual a política é aplicável.
- Manter um histórico das alterações nas políticas, pela monitoração do repositório ou por uma notificação da estação de gerência.

Um PDP pode ser uma aplicação de software em um servidor que recupera as políticas de um repositório e configura a rede para obedecer as políticas especificadas. Neste sentido, a QNS do plano de controle proposto neste trabalho – capítulo 5- pode ser caracterizada como um PDP. Outro exemplo de um PDP é um servidor COPS que configura vários roteadores para ficarem em conformidade com uma política especificada.

Ponto de execução de política (PEP-*Policy Enforcement Point*)

O PEP é o responsável pela execução das políticas definidas pelo PDP (Verma, D., 2000). É também o responsável pela monitoração das estatísticas ou de outras informações relevantes para sua operação, e também por reportar essas informações aos locais adequados. Normalmente, os PEPs são os componentes que são invocados ao longo do trajeto dos pacotes do tráfego. Exemplos comuns são os roteadores, firewalls, pilhas TCP/IP nos *hosts* finais, proxies e gateways.

4.9. Sumário do Capítulo

Neste capítulo, foram discutidas as principais alternativas aos modelos de roteamento baseados na determinação dos menores caminhos (*Shortest Path First*). Analisaram-se algumas técnicas de engenharia de tráfego e os conceitos utilizados para manutenção do desempenho.

Analisaram-se ainda as técnicas de re-roteamento, com as vantagens e os problemas. O protocolo COPS e a gerência baseada em políticas também foram discutidos.

Com base nessa discussão, se pode afirmar que muitas técnicas são propostas para determinação das rotas, e sempre que é buscada uma alternativa ao método clássico de contagem de saltos para determinar os caminhos, é necessário agregar controles adicionais, como na engenharia de tráfego, re-roteamento ou roteamento baseado em políticas. Em todas essas alternativas, fica demarcada a necessidade de um plano de controle para gerenciar os estados dos enlaces e manter as métricas dentro de valores aceitáveis para os tráfegos inelásticos.

No próximo capítulo, está descrita a proposta deste trabalho de pesquisa para manutenção e controle das métricas de *jitter* e percentual de perdas de pacotes. Descreve-se ainda o ambiente de estudos, e a metodologia adotada para as medições.

5. Plano de Controle para QoS em Fluxos de Voz na Internet

Neste capítulo descrevem-se a proposta para o plano de controle, e o funcionamento básico do protótipo para o servidor de QoS, o QNS ou *QoS Network Server* (Finenberg, V., 2002) já discutido na seção 1.3 . Uma breve descrição das ferramentas auxiliares (usadas na coleta e monitoração) também está contemplada no capítulo.

5.1. Introdução

O ITU-T e o IETF apontaram para a necessidade da criação dos planos de controle nas tecnologias Automatically Switched Optical Networks (ASON) e Generalized Multiprotocol Label Switching (GMPLS) (Jajszczyk, A. & Rozycki, P., 2006).

Pelas determinações dos órgãos de padronização, os modelos de redes de próxima geração contém três planos (Figura 5-1):

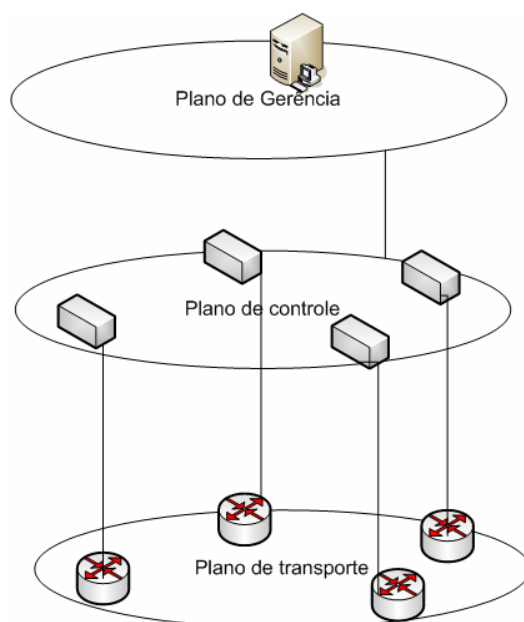


Figura 5-1 - Planos necessários nas redes de próxima geração – Fonte: (Jajszczyk, A. & Rozycki, P., 2006)

a. Plano de transporte

É também referenciado como plano de dados, responsável pelo transporte do tráfego e pela comutação.

b. Plano de controle

Responsável pela conexão e gerência dos recursos. Definido como um plano baseado no IP, pode ser associado ou separado da rede de transporte.

c. Plano de gerência

Responsável pela supervisão e gerência de todo o sistema, inclusive dos planos de transporte e controle.

Segundo (Chen, X. et al, 2003), um plano de controle (Figura 5-2) tem como tarefas principais a gerência efetiva de chamadas e conexões (estabelecimento, encerramento e manutenção), bem como a gerência de recurso da rede. As soluções apontadas pelos Órgãos (ITU-T, IETF, 3GPP - *Third Generation Partnership Project*) incluem: IS-IS, OSPF e BGP para roteamento; CR-LDP, RSVP-TE para sinalização; LMP (*Lnk Management Protocol* - RFC 4204 - Lang, J. Ed., 2005) para gerenciar a sinalização dos canais e os enlaces entre os nós.

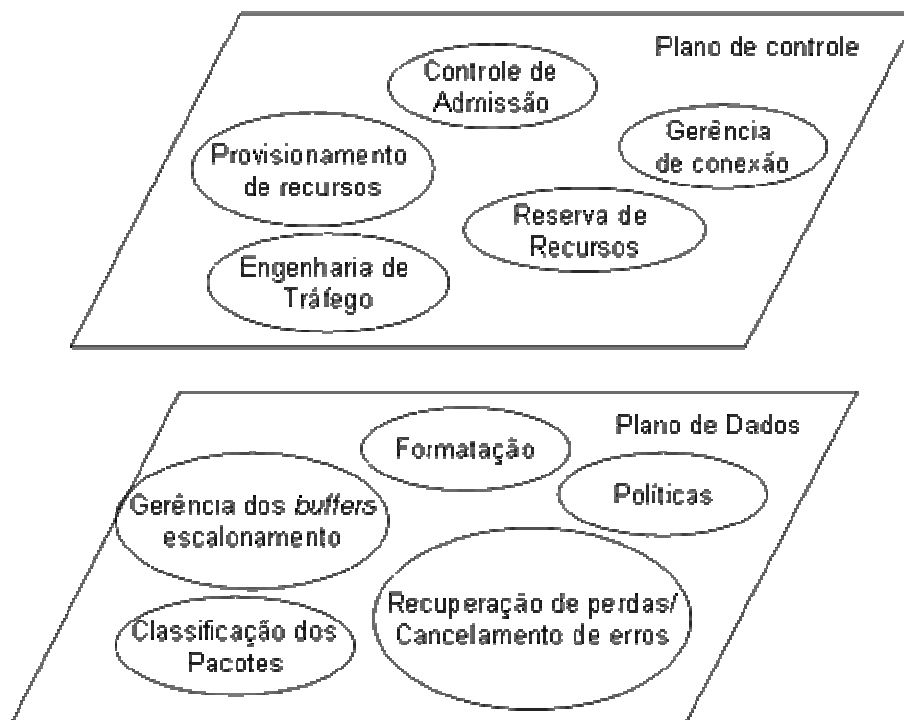


Figura 5-2 Gerência de mecanismos de VoIP – Fonte: Chen, X. et al, 2003.

As medições de desempenho de variáveis na Internet possuem duas abordagens principais: Internas e Externas, utilizadas no plano de controle como técnica auxiliar da engenharia de tráfego, para gerência de conexões, controles de admissão, reserva e provisionamento de recursos.

A abordagens Internas são as medições efetuadas nos dispositivos de rede (switches e routers), de forma ativa (enviando-se probs pelos dispositivos que se quer monitorar, como no uso de pacotes ICMP), ou passiva (esperando-se que alguma variável seja alterada e então efetuando a medida, como na utilização do SNMP).

(Um *prob*, no contexto de medições, é uma PDU – Protocol Data Unit – com informações de controle, capazes de monitorar alguma métrica).

As medições internas possuem muitas limitações potenciais (Duffield, N. G., 2004):

- Podem não estar disponíveis para a maioria dos usuários;
- Podem não cobrir todos os caminhos de maior interesse;
- As medidas podem ser desativadas durante os períodos de maior carga;
- Existem problemas de escala e correlação das medições em redes de maior tamanho ;
- Compor várias medidas salto a salto para se obter uma visão fim-a-fim é um grande desafio.

Essas questões motivaram o surgimento das abordagens externas, que procuram diagnósticos através de medidas fim-a-fim, sem assumir a necessária cooperação dos elementos de rede. Existem muitos estudos sobre o desempenho fim-a-fim na Internet (Bolot, J., 1993, Zhang, H., 1990), (Ma, Q. & Steenkiste, P., 1997), (Paxson, V. et. al, 1998), (C. Fraleigh et al, 2003).

Neste trabalho, são utilizadas as medições externas, fim-a-fim, com as estações gerando um fluxo em uma extremidade do conjunto de enlaces e medindo o resultado na outra extremidade. A medida do desempenho de tal conjunto de enlaces é denominado por (Raisanen, V., 2003) de “desempenho agregado”, e será discutido com mais detalhes no capítulo 6.

No plano de controle proposto, a restrição do valor da métrica é utilizada somente para o disparo do gatilho de busca de um caminho melhor que o atual. Eventualmente, um enlace com valores maiores que as restrições podem ser utilizados, desde que componham o melhor caminho.

Dado que as restrições implicam na transformação do algoritmo de menor caminho em um problema NP-Completo, este trabalho utiliza somente uma métrica para cálculo

do melhor caminho. Para as aplicações sensíveis ao *jitter*, essa métrica deve ser usada no plano de controle.

Além disso, as computações dos caminhos não consideram um limite para as métricas, mas sim os menores valores para aquela métrica. Essa forma de simplificação pode ser considerada uma “relaxação” para o problema. Relaxação é a adoção de um procedimento que permita a busca de um conjunto de soluções o mais próximo possível da solução ótima (Sedgewick, R., 1983). Para isso, podem ser considerados limiares superiores e inferiores.

Além dessa métrica o plano de controle proposto será testado também para o percentual de perdas de pacotes. Em conjunto com o atraso e o *jitter*, são as métricas mais influentes na necessidade de um fluxo de voz, conforme visto na seção 3.4. Essa abordagem é considerada roteamento com necessidade específica. Alguns dos algoritmos estudados partem do princípio que os mapas dos estados dos enlaces da rede sempre serão imprecisos (Kowalik, K. & Collier, M., 2003), uma vez que é difícil para os roteadores manter uma informação atualizada de toda topologia.

Como exemplo de uma manutenção de tabela de informações sobre os estados globais dos enlaces em determinada topologia pode-se utilizar a Figura 5-3, supondo-se que as métricas componham um vetor de estados como (banda,atraso,*jitter*).

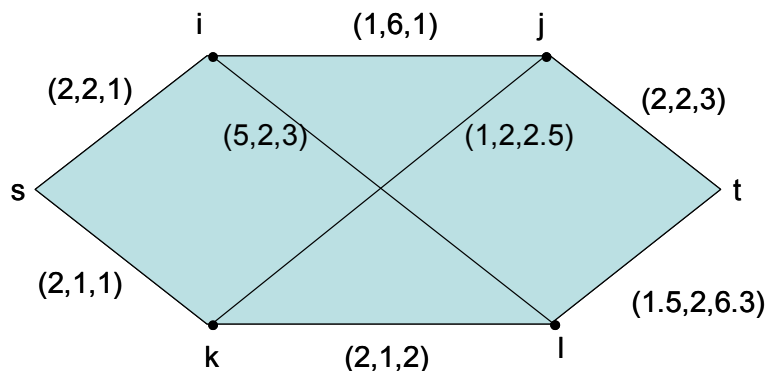


Figura 5-3 - Estado dos enlaces (banda, atraso, custo) de uma topologia de rede

Neste trabalho, consideram-se os estados dos enlaces com relação a duas métricas, separadamente, para o estabelecimento dos caminhos:

- variação do atraso (*jitter* ou PDV – Packet delay variation);

-Taxa de perdas de pacotes.

Neste cenário, os roteadores fonte do fluxo devem selecionar um caminho com base nas informações anunciadas pela QNS.

A tabela de armazenamento da estação QNS contém os registros exemplificados no Quadro 5-1.

Quadro 5-1 - exemplo de tabela da QNS com as métricas de QoS

| Data | Hora | RouterID | Enlace | Jitter | Perdas | % perdas | Pacotes |
|----------|------------------|----------|--------|-----------|--------|----------|---------|
| Ddmmaaaa | <i>Timestamp</i> | 2 | 2-7 | 41.606 ms | 2 | 1 | 200 |

Conforme foi discutido na seção 4.6, existem duas vertentes de abordagens para escolher o custo de um enlace. Por um lado, alguns autores afirmam que os algoritmos devem limitar o número de saltos como forma de economizar recursos para conexões futuras. Outro segmento defende o uso de mecanismos para balanceamento de carga, o que iria maximizar a utilização da rede. Deve-se atentar também para a influência das topologias, e mesmo quando se tem um conjunto limitado de topologias, pode levar a resultados imprecisos (Kowalik, K. & Collier, M., 2003).

Alguns algoritmos foram propostos para tolerar a imprecisão da informação sobre os estados globais dos enlaces: safety-based routing, randomized routing, multi-path routing, localized routing e static multi-path routing. Existem na literatura comparações sobre o desempenho destes algoritmos (Kowalik, K. & Collier, M., 2003), (Mieghem, P. V. & Kuipers, F. A., 2004).

5.2. Definições

O plano de controle proposto é constituído por quatro módulos básicos:

1. Ferramenta de medição Iperf, responsável pela geração das informações a respeito dos fluxos de voz e da qualidade dos enlaces.
2. agentes QoS para monitoração das informações e envio ao servidor;
3. servidor QNS para cálculo do melhor caminho;
4. Módulo de reconfiguração dos caminhos quando os limiares de degradação são ultrapassados.

Embora os termos sejam conhecidos, o plano de controle proposto (Figura 5-5) possui algumas implementações que necessitam ser definidas.

- a) Plano de controle: Conjunto de ferramentas e recursos computacionais projetados para monitorar a qualidade dos enlaces com base em métricas de QoS. O plano de controle também é capaz de reconfigurar e manter os melhores caminhos encontrados.
- b) Fluxo: definido normalmente como uma abertura socket com endereços IP de origem, destino, protocolo e portas do cliente e do servidor. Neste trabalho, os fluxos referem-se unicamente ao protocolo UDP.
- c) Fluxo de voz: Fluxo caracterizado pela taxa de 26,4 kbps e pelo tamanho do pacote de 66 bytes.
- d) Fluxo de medição: Um fluxo que utiliza a ferramenta Iperf para gerar o tráfego numa estação cliente e medir as variáveis na estação servidora, gerando um arquivo com as medidas no lado servidor (Figura 5-4). Os agentes do protótipo QoS-Path fazem a leitura deste arquivo.
- e) Monitoração: Ação executada pelos agentes QoS-Path, que consiste em ler a última linha do arquivo gerada pelo servidor do fluxo de medição e remeter o valor das métricas para o QoS-Path através da porta TCP 9999.
- f) Medição: Ação executada pelos probs da ferramenta Iperf, que consiste em gerar o tráfego no lado cliente, fazer a leitura e reportar no lado servidor.
- g) Reconfiguração: Ação executada pelo protótipo QoS-Path, que consiste em calcular um caminho melhor que o atual baseado nas métricas dos enlaces e adicionar rotas estáticas nos roteadores sempre que o algoritmo de gatilho aciona o processo.
- h) Agentes QoS-Path: Agentes que fazem a leitura do arquivo na estação servidora dos fluxos de medição, enviando as informações para a QNS, através de conexões TCP.
- i) QoS-Path: Protótipo que recebe os valores das métricas dos fluxos de medição e dos fluxos de voz (jitter e perdas), enviadas pelos agentes QoS-Path. Monitora essas métricas com o objetivo de mantê-las abaixo do limiar estipulado pelo administrador do plano de controle. Caso o limiar seja ultrapassado, o algoritmo de gatilho é acionado e, se necessário, um novo

caminho é computado com base nas métricas dos enlaces, geradas pelos fluxos de medição e enviadas pelos agentes QoS-Path. O cálculo do melhor caminho é efetuado pelo algoritmo de Dijkstra. Os roteadores são acessados pelo plano de controle através de scripts ExpectJ, através da porta TCP 23 (telnet), usando-se uma conexão secundária. Uma rota estática é adicionada na configuração do roteador. (Para as baterias de testes, após o final de cada fluxo de voz amostrado (180 segundos) as rotas adicionadas são retiradas, para que o ambiente volte ao controle do OSPF, garantindo equidade entre as amostras.

- j) Enlaces: Para o plano de controle de QoS, um enlace é considerado todo o segmento físico desde o cliente até o servidor dos fluxos de medição (fim-a-fim) - Figura 5-4. Esta abordagem para medições é definida por (Raisanen, V., 2003) como “medição agregada”. No plano de controle, estes enlaces são constituídos por uma parte Fast Ethernet, comunicando o PC cliente ao switch e o switch ao router, um segmento PPP entre dois roteadores e outra porção Fast Ethernet do roteador de destino ao switch e deste ao PC servidor.

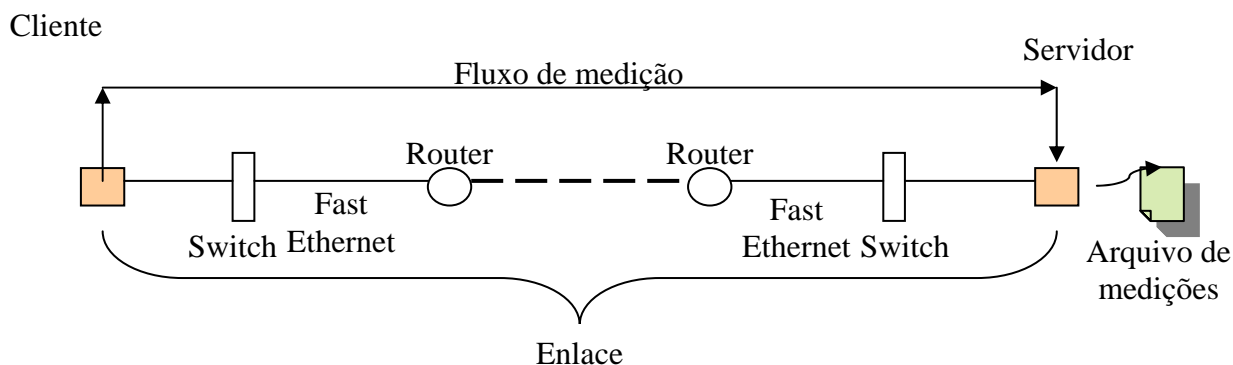


Figura 5-4 -Enlaces e fluxos de medição do plano de controle

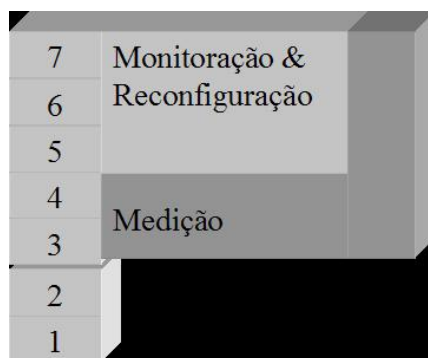


Figura 5-5 - Plano de controle e as camadas do modelo OSI

5.3. *Dinâmica do plano de controle*

O plano de controle proposto (Figura 5-6 – perceber a relação com o processo de engenharia de tráfego -Figura 4-3) é responsável pelas as seguintes tarefas:

- a) Medição do fluxo de voz pelos probs lperf;
- b) Medição dos enlaces pelos probs lperf;
- c) Leitura dos relatórios do servidor lperf pelos agentes QoS-Path;
- d) Envio das métricas dos fluxos de medição e fluxos de voz para a QNS;
- e) Verificação das condições da topologia e computação do gatilho;
- f) Caso o gatilho seja disparado, um caminho melhor que o atual é computado (Dijkstra) com base na métrica em vigor;
- g) Os roteadores necessários para elaboração do melhor caminho são acessados por scripts ExpectJ, simultaneamente;
- h) São adicionadas rotas estáticas para construir um caminho melhor para o fluxo de voz.

Estas tarefas estão ilustradas na Figura 5-6, que demonstra as estações monitorando os enlaces através dos fluxos de medição. Um relatório é enviado desde a estação até o QNS, que irá atuar nos roteadores através de telnet, caso as métricas monitoradas (perdas e *jitter*) ultrapassem os limiares estabelecidos pelo administrador.

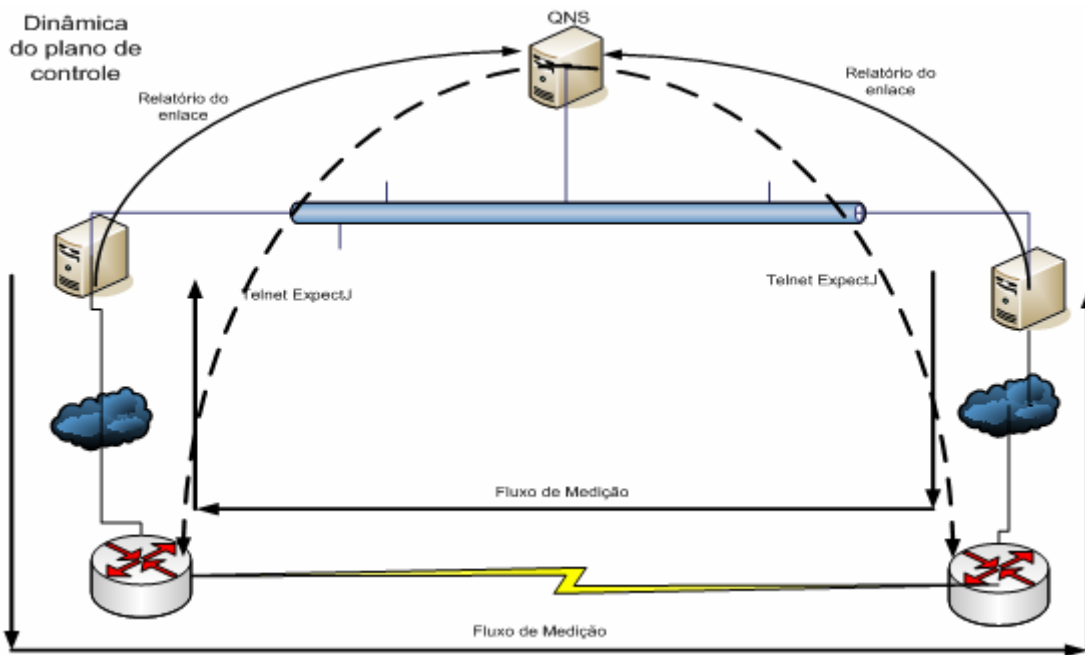


Figura 5-6 - Dinâmica do plano de controle

5.4. Ambiente de estudos de laboratório

Neste ambiente foram utilizados 6 roteadores Cisco modelo 1760, IOS 12.2 e 2 switches camada 2 modelo 2950 (Quadro 5-2), dispostos na topologia ilustrada na Figura 5.7. Essa estrutura está localizada no Laboratório de Redes de Computadores, do curso de Ciencia da Computação da UNISUL (Universidade do Sul de Santa Catarina), campus Pedra Branca. Sete estações de trabalho baseadas no processador Pentium 4 completam os recursos computacionais (Quadro 5-3).

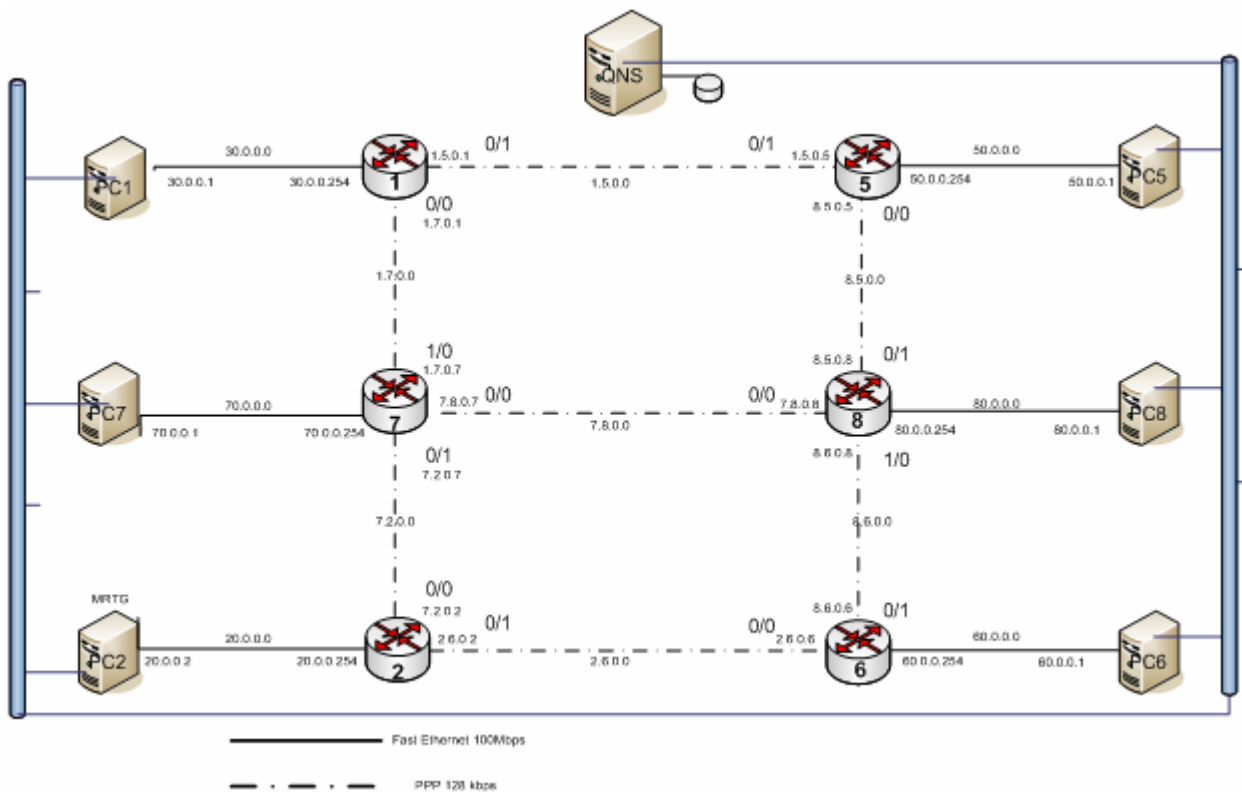


Figura 5-7 -Ambiente de estudos - Laboratório

As conexões entre os roteadores utilizam enlaces PPP. A topologia de conexão é uma malha, semelhante a utilizada em **Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998**, que utilizam o conceito de blocos básicos de construção. No caso deste trabalho, os blocos básicos possuem um enlace a menos que a proposta dos autores (Figura 5-8). Os links WAN não irão utilizar modems, uma vez que os cabos de conexão V-35 possibilitam a geração de clock nas interfaces. Os cabos conectam diretamente um roteador ao outro (conexão back-to-back - Figura 5-9). Os enlaces PPP foram configurados para uma banda de 128 Kbps, necessariamente, em função do tipo de interface serial (WIC 2A/S) disponível nos roteadores. Tal banda pode ser considerada suficiente para reproduzir a maioria das necessidades encontradas nos ambientes reais para poucos fluxos de voz (CODEC PCM).

Quadro 5-2 Dispositivos de rede do ambiente de estudos

| ID-loopback | Dispositivo | Interfaces configuradas (LAN/WAN) | Modelo | Softwares | Função |
|-------------|-------------|-----------------------------------|--------|--------------|--------------|
| 1.1.1.1 | Roteador | ½ | 1760 | IOS-12.2-11T | OSPF |
| 2.2.2.2 | Roteador | ½ | 1760 | IOS-12.2-11T | OSPF |
| 5.5.5.5 | Roteador | ½ | 1760 | IOS-12.2-11T | OSPF |
| 6.6.6.6 | Roteador | ½ | 1760 | IOS-12.2-11T | OSPF |
| 7.7.7.7 | Roteador | 1/3 | 1760 | IOS-12.2-11T | OSPF |
| 8.8.8.8 | Roteador | 1/3 | 1760 | IOS-12.2-11T | OSPF |
| | Switches(2) | 14/0 | 2950 | 12.1 | Comutação L2 |

Quadro 5-3 Microcomputadores Pentium 4 - SO Fedora Core 3

| Nome | Endereço IP | Memória RAM (MB) | Softwares | Função |
|------|-------------|------------------|---------------------|------------------------|
| QNS | 10.4.30.211 | 256 | QoS-Path | QNS |
| PC1 | 30.0.0.1 | 256 | Iperf NTP Server | Probe Sincronizador |
| PC2 | 20.0.0.2 | 256 | Iperf MRTG | Gerência Probe |
| PC7 | 70.0.0.1 | 256 | Iperf MySQL | Probe SGBD |
| PC5 | 50.0.0.1 | 256 | Iperf | Probe |
| PC6 | 60.0.0.1 | 256 | Iperf | Probe |
| PC8 | 80.0.0.1 | 256 | Iperf | Probe |

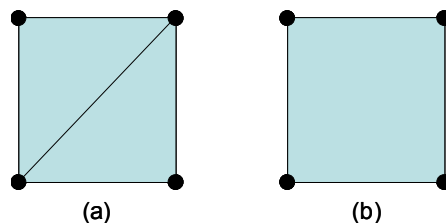


Figura 5-8 - Blocos básicos para a topologia dos roteadores (a) Apostolopoulos, G. et al, 1999 (b) este trabalho.



Figura 5-9 -Conexão back-to-back com cabos V-35

A Figura 5-10 mostra a estrutura do laboratório de estudos com o plano de controle instalado.

5.5. Ferramenta de medição Iperf

O software de medição para análise de desempenho (Iperf) é proposto pela Cooperative Association for Internet Data Analysis (<http://www.CAIDA.org>). Embora existam muitas alternativas, como descrito por (Blum, R., 2003), a única descrita como capaz de medir a variação do atraso é o IPerf. Segundo (Hassan, M. & Jain, R., 2004), as ferramentas de medição podem ser classificadas quanto a um grande número de características:

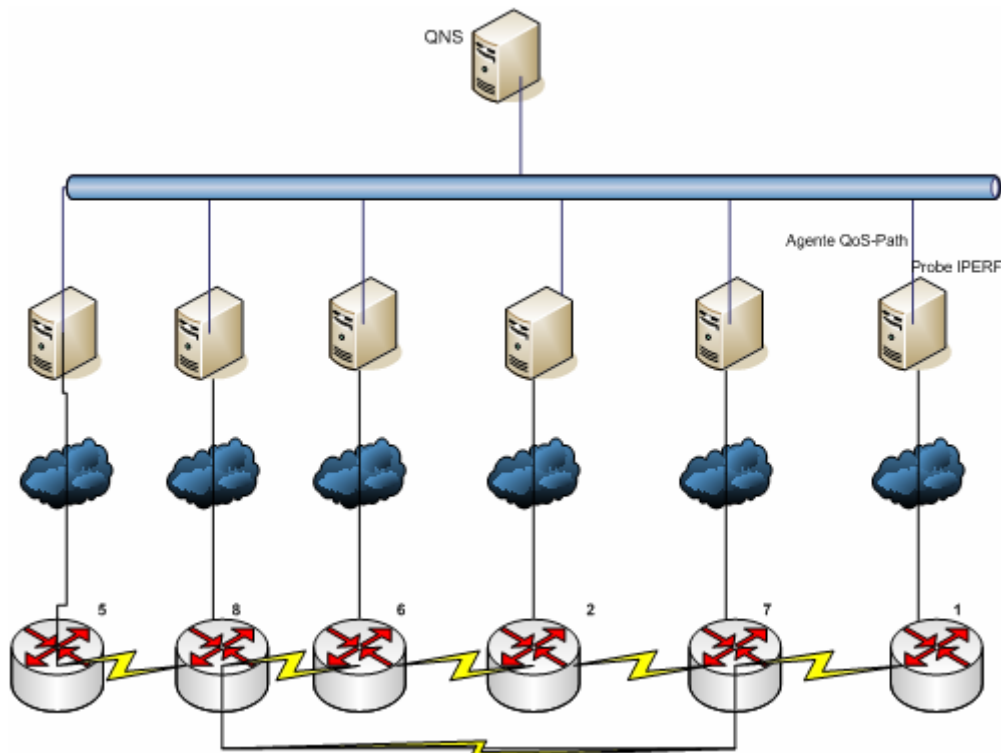


Figura 5-10 - Ambiente de estudos com o plano de controle

- a) Propósito das medições
- b) Nível das tarefas
- c) Tipo da implementação

A classificação quanto ao propósito das medições leva a dois grupos de ferramentas (demonstradas na Figura 5-11): Monitoração e Benchmarking. As ferramentas de monitoração (por exemplo, *tcpdump*), são amplamente utilizadas pelos implementadores de protocolos, e gerentes de redes. Essas ferramentas capturam os pacotes trafegando pela rede, permitindo análise dos cabeçalhos. As ferramentas de *benchmarking* geram tráfego através da rede e medem o desempenho através de várias métricas, ou índices, como a vazão, atraso, *jitter* e estimativas de banda disponível. A ferramenta *Iperf*, usada neste trabalho, está nessa classe de softwares.

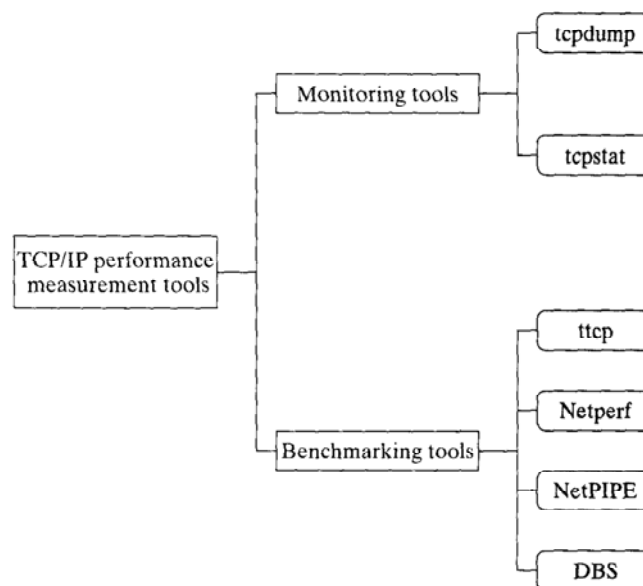


Figura 5-11 – Classificação das ferramentas para avaliação de desempenho TCP/IP- Fonte: Hassan, M. & Jain, R., 2004

O *Iperf* está disponível atualmente no site da Distributed Applications Support Team (DAST), equipe que pertence ao National Laboratory for Applied Network Research (<http://dast.nlanr.net/Projects/Iperf/>). Segundo o site da equipe de suporte, a ferramenta cria um fluxo bastante artificial para o protocolo UDP, similar a comunicação de voz.

As perdas são detectadas pelos IDs do cabeçalho dos datagramas. Para se obter uma media das perdas de pacotes ao invés de datagramas, deve-se utilizar a opção `-l` para reduzir o datagrama a um único pacote IP. O tamanho padrão do segmento UDP é de 1470 bytes, que pode ser transportado por um segmento ethernet sem fragmentação.

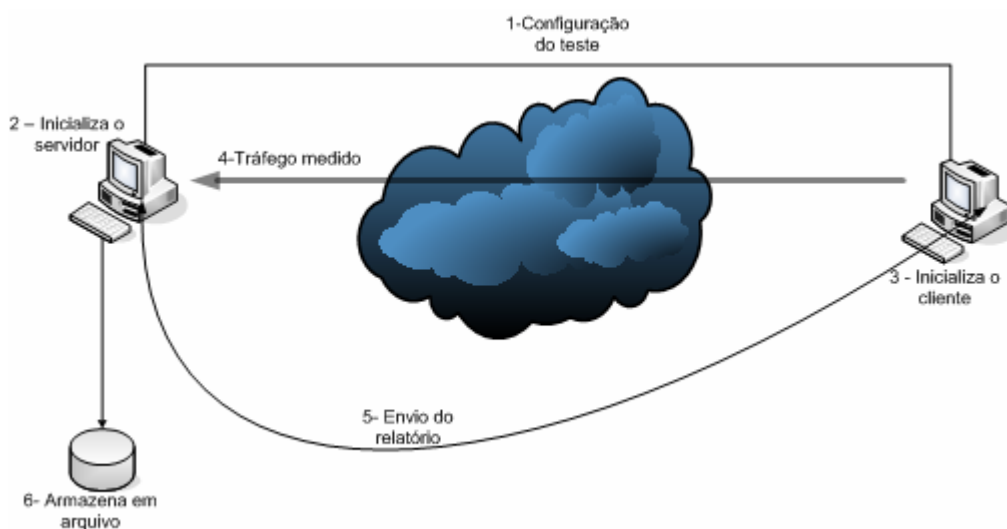


Figura 5-12- Uso da ferramenta Iperf

O cálculo do *jitter* é computado continuamente pelo servidor, como especificado na RFC 1889 (RTP) (Schulzrinne, H.; Casner, S.; Frederick, R. & Jacobson, V., 1996). O cliente grava um timestamp de 64 bit no pacote. O servidor computa o tempo relativo a trajetória, subtraindo o tempo da chegada com o tempo de saída. Não é necessário sincronizar os relógios, uma vez que as diferenças são retiradas pelo cálculo do *jitter*. O relatório é elaborado como a média “suavizada” das diferenças entre os tempos de trajetórias consecutivas. A metodologia para calculo do *jitter* está descrita na seção 3.4.2.

5.5.1. Metodologia das medições

Os 6 microcomputadores foram configurados para atuar como servidores e como clientes dos fluxos UDP. Cada computador envia para os vizinhos um fluxo no sentido anti-horário e outro no sentido horário, atuando como cliente do fluxo. O vizinho recebe os fluxos, atuando como servidor, e por sua vez envia para seus vizinhos, atuando como cliente (Figura 5-13). Esta sistemática foi necessária para que os enlaces fossem utilizados de maneira *full-duplex*, o que corresponde às situações reais.

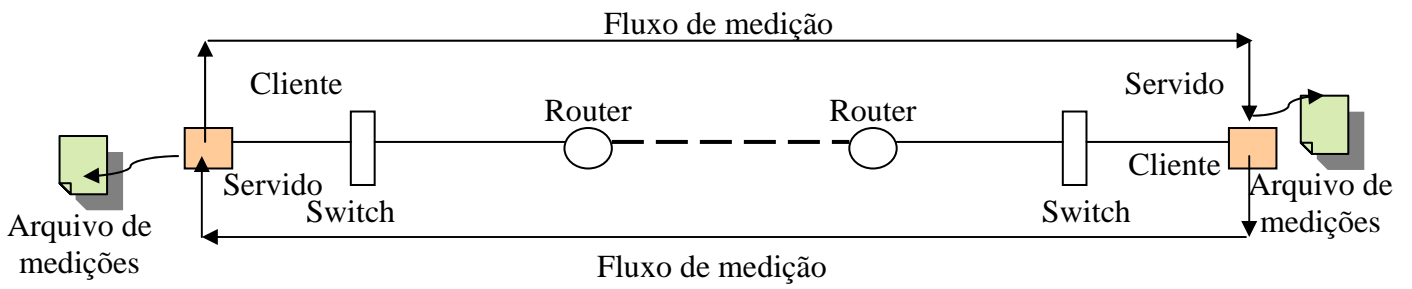


Figura 5-13 - Probs para medição das métricas nos enlaces - Fluxos de medição

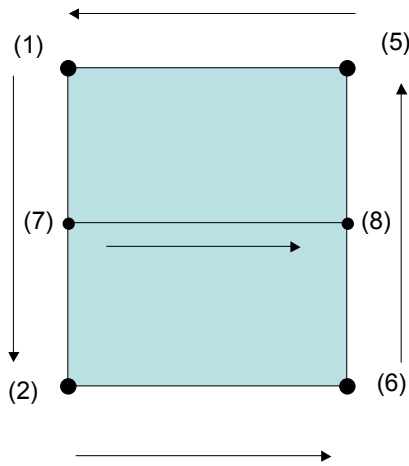


Figura 5-14 - Sentido dos fluxos de medição da qualidade do enlace

5.5.2. Modelo para os experimento

Nos ambientes de amostragem, determinados enlaces podem ser utilizados por até três fluxos simultaneamente, conforme o modelo da Figura 5-15.

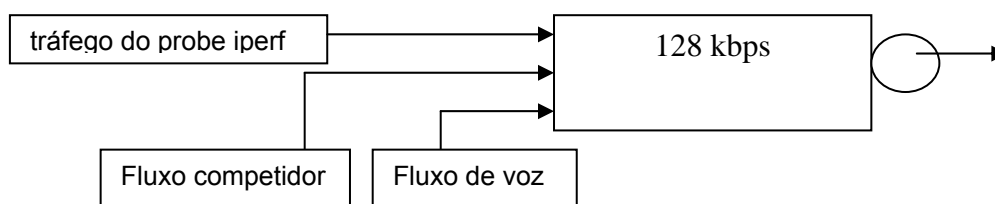


Figura 5-15 - Modelo para os experimentos

```

-----
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 108 KByte (default)
-----
( 3) local 30.0.0.1 port 5001 connected with 20.0.0.2 port 34720
( 3) 0.0- 1.0 sec 14.4 KBytes 118 Kbits/sec 3.345 ms 0/ 10 (0%)
( 3) 1.0- 2.0 sec 15.8 KBytes 129 Kbits/sec 5.240 ms 0/ 11 (0%)
( 3) 2.0- 3.0 sec 14.4 KBytes 118 Kbits/sec 6.118 ms 0/ 10 (0%)
( 3) 3.0- 4.0 sec 15.8 KBytes 129 Kbits/sec 6.602 ms 0/ 11 (0%)
( 3) 4.0- 5.0 sec 15.8 KBytes 129 Kbits/sec 6.854 ms 0/ 11 (0%)
( 3) 5.0- 6.0 sec 14.4 KBytes 118 Kbits/sec 23.865 ms 0/ 10 (0%)
( 3) 6.0- 7.0 sec 15.8 KBytes 129 Kbits/sec 15.336 ms 0/ 11 (0%)
( 3) 7.0- 8.0 sec 14.4 KBytes 118 Kbits/sec 11.421 ms 0/ 10 (0%)
( 3) 8.0- 9.0 sec 15.8 KBytes 129 Kbits/sec 9.215 ms 0/ 11 (0%)
( 3) 9.0-10.0 sec 15.8 KBytes 129 Kbits/sec 8.138 ms 0/ 11 (0%)
( 3) 10.0-11.0 sec 14.4 KBytes 118 Kbits/sec 8.438 ms 0/ 10 (0%)
( 3) 11.0-12.0 sec 15.8 KBytes 129 Kbits/sec 8.338 ms 0/ 11 (0%)
( 3) 12.0-13.0 sec 14.4 KBytes 118 Kbits/sec 8.448 ms 0/ 10 (0%)
( 3) 13.0-14.0 sec 14.4 KBytes 118 Kbits/sec 11.361 ms 0/ 10 (0%)
( 3) 14.0-15.0 sec 14.4 KBytes 118 Kbits/sec 67.954 ms 0/ 10 (0%)
( 3) 15.0-16.0 sec 15.8 KBytes 129 Kbits/sec 39.449 ms 0/ 11 (0%)
( 3) 16.0-17.0 sec 15.8 KBytes 129 Kbits/sec 22.993 ms 0/ 11 (0%)
( 3) 17.0-18.0 sec 14.4 KBytes 118 Kbits/sec 15.429 ms 0/ 10 (0%)

```

Tabela 5-1 - Saída para a estação servidora (30.0.0.1) do Iperf. O PC2 (20.0.0.2) está enviando datagramas de 1470 bytes, em taxas de 128 kbps.

Segundo a RFC 2330 - Framework for IP Performance Metrics - (Paxson, V. et. al, 1998), mesmo a melhor metodologia de medição, para a métrica mais bem comportada, vai apresentar erros. As pessoas responsáveis pelos métodos de medição devem, portanto:

- Minimizar suas incertezas/erros;
- Entender e documentar as fontes de incertezas /erros;
- Quantificar os montantes de incertezas/erros.

5.6. Protótipo QoS-Path

A programação do protótipo QoS-Path da QNS é baseada nas linguagens Java e scripts ExpectJ. A aplicação servidora possui as seguintes tarefas básicas:

- Manter as conexões dos clientes (agentes QoS), receber as mensagens de atualização das métricas de *jitter* e perda dos enlaces e armazenar em uma tabela interna.
- calcular um novo caminho sempre que o gatilho de degradação das métricas for disparado, baseado nas métricas dos enlaces no momento.
- Configurar os roteadores necessários para que os fluxos de voz entre os *hosts* de origem e destino percorram um caminho melhor que o atual

5.7. Sumário do capítulo

Neste capítulo, foi descrito o funcionamento do plano de controle proposto para manutenção das métricas de QoS para os fluxos de voz. Foi descrito o ambiente de estudos, e se analisou a ferramenta utilizada para medições.

Percebe-se que as redes de próxima geração devem ter um plano de controle, um plano de gerencia e um plano de dados, segundo os órgãos de padronização. As metodologias e arquiteturas analisadas no capítulo 4 servem de base para a elaboração do plano de controle descrito neste capítulo, que usa os conceitos de QNS e *probs* de medição, bem como técnicas de re-roteamento baseado em políticas.

No próximo capítulo, é descrita a metodologia utilizada para análise de desempenho do plano de controle em relação as métricas *jitter* e perdas. Estão descritas e classificadas as técnicas de medição nas redes atuais, com base nos órgãos de padronização e nos principais autores da área. Os ambientes experimentais e os fatores analisados são apresentados.

6. Desempenho

Este capítulo apresenta a metodologia utilizada na avaliação do desempenho do plano de controle proposto neste trabalho para a redução dos valores de *jitter* ou de perdas. Os métodos de análise basearam-se em (Jain, R., 1991). As medições dos parâmetros de rede seguem as propostas de (Raisanen, V., 2003) e das RFCs 2330, 2680, 3393 e 3432. Além dessas especificações, tomaram-se como referência a recomendação ITU-T I.380 (ITU-T, 1999) e do ETSI- European Telecommunications Standards Institute, através da recomendação (TIPHON, 2002).

Para elaboração do modelo de políticas de roteamento foi utilizado um ambiente de laboratório, que permite condições de tráfego sob controle, e não inviabiliza os experimentos, que seriam impraticáveis em ambientes de produção.

Um modelo de desempenho computacional é uma maneira de estimar o valor das métricas de desempenho com base em dois fatores: um modelo de carga – uma representação sintética da carga atual - e nos parâmetros de configuração do sistema Menascé, D. A., 2003 - Figura 6-1.

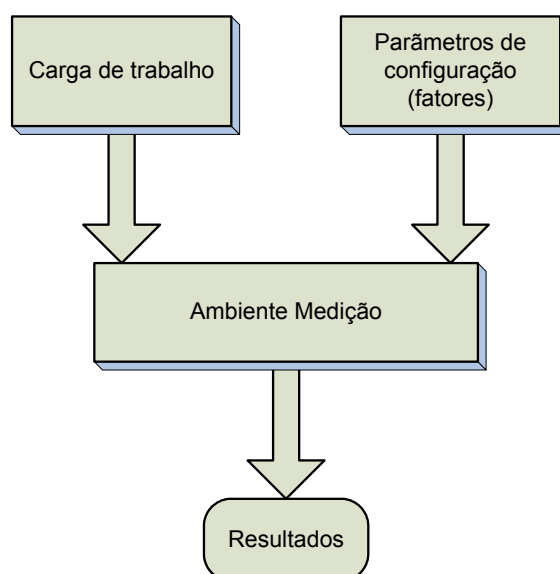


Figura 6-1 - Modelo de Desempenho de sistema computacional – Fonte: Adaptado de Menascé, D. A., 2003

O IETF, através do grupo de trabalho IPPM (*IP Performance Metrics* - <http://www.ietf.org/html.charters/ippm-charter.html>) desenvolve um conjunto de métricas padrões que podem ser aplicadas para a qualidade, desempenho e confiabilidade dos serviços de entrega na Internet. Segundo este grupo de estudos, é importante que as métricas não utilizem juízo de valor, mas forneçam uma medida quantitativa imparcial do desempenho.

6.1. Considerações gerais sobre o problema

Neste trabalho são utilizadas duas das quatro métricas de desempenho para QoS (Perdas e Variação do Atraso). As métricas não serão consideradas em conjunto, uma vez que o plano de controle proposto pode ter somente uma métrica como limiar de troca de caminhos. A vazão poderia ser utilizada como parâmetro para estimar a banda residual, que ainda estaria disponível para ser usada no enlace para novas conexões. As informações sobre as métricas são obtidas a cada segundo pela QNS, que dessa forma tem condições de avaliar a topologia a qualquer momento.

Para se trocar um caminho determinado devem-se considerar alguns fatores (Norden, S., 2002):

- O tempo. Quando realmente deve-se trocar o caminho? Quando se deve aguardar uma melhora do enlace sem interferência?
 - Neste trabalho de pesquisa foram considerados 10 segundos como o tempo máximo permitido para caminhos degradados. Esse período foi considerado como razoável para caracterizar uma degradação da qualidade em função do tempo de amostragem, de 180 segundos. O limite de 10 segundos pode ser ajustado na configuração das ferramentas do plano de controle, dependendo das necessidades individuais de uso dos enlaces. Os caminhos foram considerados degradados quando os limites de perdas passaram de 1% e a variação do atraso passou de 27 ms.
O limiar de perdas foi considerado com base no CODEC G.729. Segundo (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005), o uso deste

padrão requer perdas menores que 1% para evitar erros perceptíveis. Os autores tomaram como referência a documentação da Cisco Systems.

O limiar de 27 ms para *jitter* foi escolhido com base em testes preliminares nos ambientes de estudo.

- As prioridades para troca. Devem ser mantidas as prioridades originais quando do estabelecimento das conexões ou a velocidade deve ser o critério, calculando-se quais conexões serão rearranjadas apenas em função da disponibilidade dos enlaces? Neste caso uma conexão de prioridade mais alta poderia ser preterida.
 - Neste trabalho, não se consideraram as conexões.
- Quais as métricas que devem ter um peso maior no disparo do gatilho de rearranjo dos caminhos? Para algumas aplicações as perdas são mais importantes que os atrasos, ou as variações do atraso.
 - Nesta questão, se optou pela variação do atraso e pelas perdas como métricas. Poderiam ser as quatro métricas de QoS para fluxos de voz, mas optou-se pela variação do atraso, uma vez que poucas tecnologias utilizam essa métrica. As perdas foram incluídas como alternativa pois são um problema resolvido com técnicas de filas bastante avançadas. Além disso, começam a interferir na conversação após atingirem níveis elevados.
- A métrica deve ser mantida em conjunto com a prioridade? Ou, se uma conexão de alta prioridade não tem relação com a variação do atraso, como é o caso de uma transmissão de FTP. E a métrica que disparou o gatilho de troca de caminhos foi a variação do atraso, essa conexão deve permanecer no caminho “degradado” ou ser re-encaminhada? Isso mostra que um caminho degradado para uma conexão (fluxo) pode não o ser para outra.
 - Essa questão não foi considerada, pois todos os fluxos foram classificados com a mesma prioridade.

- Quando re-encaminha-se uma conexão para um novo enlace, esta conexão que está ganhando os recursos do enlace pode degradar as métricas deste novo caminho, afetando conexões pré-existentes, talvez com níveis prioritários superiores (isso poderia caracterizar comportamento preemptivo).
 - Neste trabalho não se consideraram as prioridades, porém o re-encaminhamento de um fluxo pode realmente afetar a qualidade dos demais. Considera-se que a estação QNS está apta a detectar as degradações geradas pela sua própria alteração nos caminhos, e neste caso, recalcular o melhor caminho. Este fato foi realmente comprovado pelos experimentos.

6.2. Metodologia

A metodologia utilizada para avaliação de desempenho neste trabalho segue aquela proposta por Jain (**Jain, R., 1991**), que divide este tipo de trabalho em 10 etapas (Quadro 6-1), descritos a seguir sob a óptica deste trabalho.

Quadro 6-1 - Passos para avaliação de desempenho

| Passos para estudo de avaliação de desempenho |
|---|
| • Determinar os objetivos do trabalho de pesquisa e definir as fronteiras do sistema. |
| • Listar os serviços do sistema e possíveis resultados. |
| • Selecionar as métricas de desempenho. |
| • Listar os parâmetros do sistema e da carga. |
| • Selecionar os fatores e seus valores. |
| • Selecionar as técnicas de avaliação. |
| • Selecionar a carga. |
| • Projetar os experimentos. |
| • Analisar e interpretar os dados. |
| • Apresentar os resultados. Iniciar novamente, se necessário. |

Fonte: (Jain, R., 1991)

6.2.1. Determinar os objetivos do trabalho de pesquisa e definir as fronteiras do sistema.

Este deve ser o primeiro passo em qualquer projeto de avaliação de desempenho. Deve-se conhecer as metas e saber exatamente o que constitui o sistema pela delimitação de suas fronteiras. Isso é necessário pois, dados os mesmos conjuntos de hardware e software, as definições do sistema pode variar dependendo dos objetivos do trabalho. A escolha dos limites do sistema pode afetar as métricas de desempenho bem como as cargas utilizadas para comparar os sistemas.

O objetivo da avaliação, neste trabalho de pesquisa, será determinar o desempenho dos enlaces, perante as escolhas dos caminhos efetuadas pela estação de gerência de QoS. Tal desempenho será confrontado com o dos caminhos escolhidos pelos protocolos IGP tradicionais, neste caso o OSPF. O desempenho das soluções em termos de convergência não serão medidos.

Serão usados 6 roteadores interconectados diretamente pelas interfaces WAN, como ilustrado na Figura 5-9. Isso significa que os atrasos de propagação, tal como definidos na seção 3.4.1, devido a proximidade física e dimensões do cabeamento, serão negligenciados nos ambientes de trabalho. Para os efeitos do trabalho de pesquisa, e devido ao tamanho reduzido do ambiente, o OSPF será configurado com apenas uma área, o que facilita a comparação dos desempenhos, pois nenhum roteador será considerado de borda (Isso obrigaria a máquina a manter mapas topológicos separados (Doyle, J., 1998)).

6.2.2. Listar os serviços e os possíveis resultados

Cada sistema fornece um conjunto de serviços. A próxima fase na análise de um sistema é listar os serviços (Quadro 6-2). Quando um usuário requisita um destes serviços, existe um número de resultados possíveis. Alguns são desejáveis, outros não.

Os protocolos utilizados objetivam prover QoS na rede. Para tanto, o estabelecimento dos fluxos deve percorrer os caminhos com as melhores métricas. Ao

iniciarem-se os experimentos, uma suposição era a de que as medições sobre os IGP, (OSPF) provavelmente não teriam resultados satisfatórios em relação aos melhores caminhos, uma vez que estes protocolos buscam os menores caminhos, quando a única métrica é o hop count. Esperava-se uma melhora nessas condições com alteração dos custos para os caminhos deteriorados. A proposta deste trabalho supõe a manutenção de um desempenho mais equilibrado, embora fosse esperada alguma queda durante os períodos de re-roteamento.

Quadro 6-2- Serviços e resultados esperados na avaliação de desempenho

| Serviço | Resultado esperado |
|---|--|
| Roteamento IGP (OSPF) (caminhos dinâmicos apenas em função de queda do enlace) | Degradação das métricas sempre que os caminhos escolhidos estejam saturados, mesmo que outros estejam sub-utilizados (problema do peixe – Figura 4-4). Curto período até a degradação. |
| Roteamento de QoS <i>statefull</i> (caminhos pré-determinados e fixos) | Desempenho mais estável, tempo maior até o estágio de congestionamento. Porém, sob congestionamentos intensos, as métricas devem se degradar, devido a impossibilidade de re-roteamento. Conexões novas devem ser recusadas por falta de recursos (enlaces e <i>buffers</i> saturados) |
| Roteamento “<i>semi-stateless</i>” - caminhos dinâmicos em função das métricas | Desempenho estável, tempo maior até o estágio de congestionamento. Quando o caminho se mostrar degradado, novas rotas devem ser escolhidas, recuperando as métricas. |

6.2.3. Selecionar as métricas de desempenho.

Segundo a RFC 2330 (Paxson, V. et. al, 1998), as métricas de desempenho e confiabilidade para os caminhos na Internet devem obedecer aos seguintes critérios:

- Devem ser concretas e bem definidas

- Uma metodologia para uma métrica deve ser reprodutível. Se ela for utilizada múltiplas vezes sob as mesmas condições, deve levar a resultados idênticos.
- Não devem apresentar tendências (*bias*) para as nuvens IP implementadas com tecnologias idênticas;
- Devem exibir tendências pequenas e compreensíveis para nuvens IP de tecnologias não-idênticas;
- Devem ser úteis para usuários e provedores no entendimento do desempenho que estão experimentando ou provendo.
- Devem evitar a indução de metas de desempenho artificial.

Classicamente, se utilizam quatro métricas para medir o desempenho em uma rede que procura manter QoS (Campbell, A. T., 1996), (Ferguson, P. & Huston, G., 1998) (Vegesna, S., 2001), (Xiao, X.; Ni, L., 1999): Perdas, atraso, variação do atraso ("IP Packet Delay Variation – ipdv) e vazão (a vazão não é considerada por alguns autores como métrica de desempenho para QoS. Outros preferem utilizar a largura de banda em lugar da vazão). Algumas métricas já estão definidas como métricas de desempenho em RFCs pelo IPPM (Quadro 6-3).

Quadro 6-3 RFCs e métricas IPPM

| | Métrica | RFC |
|---|---------------------------|------------|
| 1 | Atraso <i>one-way</i> | 2679 |
| 2 | Atraso <i>round-trip</i> | 2681 |
| 3 | Variação do atraso | 3393 |
| 4 | Perdas (<i>one-way</i>) | 2680 |

Neste trabalho, são utilizadas as métricas variação do atraso (*jitter*) e perdas (*one-way*). As perdas serão medidas *one-way* pelo fato de representarem melhor o comportamento de um enlace, uma vez que o caminho de volta dos pacotes pode não ser o mesmo da ida (Barford, P. & Sommers, J., 2004). A opção pelo uso do *jitter* como métrica se deu pela importância da variável (discutida nos capítulos 2 e 3), bem como a pequena quantidade de estudos sobre o *jitter* como fator de desempenho para os enlaces e roteamento. As perdas, além da importância para todas as aplicações, foram

medidas pela facilidade gerada pela ferramenta de medição, que dispõe o relatório de perdas percentuais em conjunto com o *jitter*.

Segundo a especificação da Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) – (TIPHON, 2002), a taxa de perdas de pacotes é dada por:

$$L = \frac{M}{N_{pack}}$$

Onde M é o número de pacotes recebido pela camada de aplicação e Npack é o número total de pacotes transmitidos.

Pela especificação, existe a métrica de “correlação de perdas de pacotes”, uma função das seqüências de perdas em um fluxo (Figura 6-2). Na figura, existem três seqüências de perdas, LS1, LS2 e LS3. O tamanho da seqüência indica o número de pacotes perdidos naquela seqüência, que são 1, 2 e 3, respectivamente.

A “correlação de pacotes perdidos” é o número de pacotes perdidos dividido pelo número de seqüência de perdas (no exemplo da figura foram 3 seqüências). Nesse caso, (1+2+3)/3=2. Essa medida dá uma noção do tamanho das rajadas de perdas.

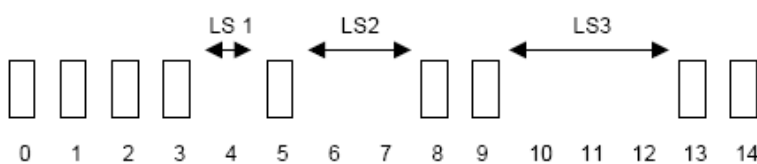


Figura 6-2 - Correlação de pacotes perdidos. Fonte: (TIPHON, 2002)

6.2.4. Listar os parâmetros do sistema e da carga.

São todos os parâmetros que afetam o desempenho. A lista pode ser dividida em parâmetros do sistema (Hardware e software, normalmente imutáveis durante os experimentos) e parâmetros da carga (requerimentos do usuário, normalmente

variáveis entre os experimentos). A lista pode não ser completa, pois após a primeira bateria de análises se podem descobrir novos parâmetros afetando o desempenho.

6.2.5. Selecionar os fatores e seus valores.

A lista de parâmetros pode ser dividida ainda em dois grupos: Os que irão variar durante os experimentos (fatores) e em que graus de intensidade (chamados de níveis). Em geral uma lista de fatores e seus possíveis níveis são maiores que os recursos irão permitir. Deve-se começar com uma lista pequena, escolhendo como fatores os parâmetros cuja variação afeta de forma mais intensa o desempenho.

Os fatores considerados neste trabalho estão discutidos na seção 6.5.1

6.2.6. Selecionar as técnicas de avaliação.

Existem 3 técnicas básicas: Modelagem analítica, simulação e medições em sistemas reais. Neste trabalho de pesquisa, é são realizadas medições em sistemas reais.

Nas recomendações dos princípios para Engenharia de Tráfego na Internet (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002), as técnicas de simulação podem ser utilizadas para verificar e validar as aproximações analíticas. Entretanto, a simulação pode consumir recursos computacionais demasiados, e nem sempre produz as respostas suficientes. Segundo os autores uma abordagem apropriada para avaliação do desempenho pode envolver uma combinação de técnicas analíticas, simulações e métodos empíricos.

6.2.7. Selecionar a carga.

Este item corresponde a uma lista de requisitos de serviços ao sistema. Podem ser usados padrões de tráfego sintético ou traces de sistemas reais, se a técnica de avaliação for a simulação. Existem traces disponíveis para tráfegos Internet (<http://ita.ee.lbl.gov>). Um arquivo exemplo deste site é o *lbl-conn*, coleta de 30 dias das conexões TCP entre a LBL e outros pontos do planeta0 (Hassan, M. & Jain, R., 2004). É possível coletar os traces de sistemas reais através de ferramentas como o *tcpdump* atuando em interfaces espelhadas dos switches.

As cargas devem ser bem definidas e representar o tráfego real. Neste trabalho será utilizado o software *Iperf* (Figura 5-12) para padrões de tráfego do tipo transferência massiva de dados e interatividade (tipo requisição/resposta).

Os tipos de carga e os parâmetros de variação escolhidos para as avaliações estão listados no ítem 6.5.1 - Descrição dos fatores.

6.2.8. Projetar os experimentos.

Devem-se selecionar os experimentos que gerem o máximo de resultados com o mínimo de esforço. As primeiras fases contemplam mais fatores e menos níveis, passando-se para vários níveis nos fatores que mais influenciaram no desempenho.

6.2.9. Analisar e interpretar os dados.

É importante reconhecer que os resultados dos experimentos e simulações são quantidades randômicas, e que repetições devem levar a números diferentes. Comparando-se duas alternativas, é necessário considerar a variabilidade dos resultados. A comparação das médias puras pode levar a erros. Técnicas estatísticas devem ser empregadas na análise.

6.2.10. Apresentar os resultados. Iniciar novamente, se necessário.

A apresentação deve ser fácil de ser compreendida. Deve ser na forma gráfica, evitando jargões estatísticos. Os gráficos devem ter cuidados de escala. Neste ponto, deve-se considerar uma volta aos passos iniciais e retomada dos experimentos, com base nos valores alcançados. Isso pode melhorar as definições de escopo, alteração dos fatores e níveis. O trabalho de pesquisa completo pode ser composto de vários ciclos.

6.3. Obtenção de dados de desempenho de uma rede

Segundo (Raisanen, V., 2003), a obtenção dos dados para monitoração de desempenho de uma rede pode advir de um número grande de fontes e em diferentes níveis de abstração. Iniciando-se com os métodos mais detalhados, os elementos de rede individuais podem ser consultados para informações. Os elementos de rede podem fornecer mecanismos de notificação caso alguma condição pré-definida seja ultrapassada. Em algumas situações, como nas tabelas de rotas de um protocolo Link-state, como o OSPF, um elemento de rede pode fornecer informações sobre porções grandes da rede. Níveis de abstrações maiores que um único elemento de rede podem ser obtidos pelos sistemas de gerência (NMS – Network Management System).

O NMS pode fornecer médias e análises de tendências em adição a um estado abstrato e momentâneo da rede. Finalmente, o retorno da rede pode ser em forma de qualidade de serviço. Isso exige uma maneira de estimar o desempenho no nível do serviço. O nível de abstração está comparado no Quadro 6-4.

Quadro 6-4 Níveis de monitoração e características medidas em uma rede.

| Nível de monitoração | Características típicas medidas |
|-----------------------------|--|
| Por elemento de rede | Carga geral e estatística de tráfego |
| Sistema de gerência IP | Dados em escala de toda rede, médias e análises de tendências |
| Desempenho agregado | Atraso, <i>jitter</i> , perdas de pacotes e banda disponível |
| Nível de serviço | Componentes de especificação os níveis de serviço (disponibilidade, confiabilidade...) |

Fonte: (Raisanen, V., 2003).

Dois tipos de medidas podem ser relevantes para a engenharia de tráfego nas redes IP (Raisanen, V., 2003):

- **Medidas agregadas de desempenho para o tráfego**, (Figura 6-3) relevantes para otimização de parâmetros típicos de um domínio DiffServ. Tais medidas servem também para controle dos roteadores, e são efetuadas como um conjunto de vários elementos de rede. Tais medições podem ser consideradas

equivalentes às abordagens de medições externas citadas por (Duffield, N. G., 2004) e já discutidas na seção de introdução ao capítulo 5.

- **Medidas de carga nos dispositivos** são utilizadas tipicamente para controle do roteamento e também para propósitos de avaliação de necessidades de expansão. Tais medidas são equivalentes as medidas internas citadas por (Duffield, N. G., 2004).



Figura 6-3 - Medidas de desempenho agregadas e de serviços (fim a fim). Fonte: (Raisanen, V., 2003). AD=Domínio DiffServ, NE=Elemento de rede

6.3.1. Medições agregadas de desempenho do tráfego

Incluem o efeito de múltiplos elementos de rede como parte da definição da medição. Este tipo de medição pode necessitar de menos processamento que uma tentativa de combinar dados dos elementos de rede individuais. Basicamente existem três tipos de métodos para medições agregadas:

- a. Passivas (não intrusivas);
- b. Ativas (intrusivas);
- c. Piggybacking (inserção de *timestamping* na carga do pacote).

Os dados de medição obtidos por um ou mais destes mecanismos podem ser processados de diferentes maneiras para se obterem as características relevantes (Raisanen, V., 2003). Um exemplo é o cálculo do modelo de correlação de perdas -Figura 6-2- sugerida por (TIPHON, 2002), que fornece uma medida para o tamanho das rajadas de perdas. A recomendação I.380 do ITU-T (ITU-T, 1999) relaciona as seguintes métricas

para QoS de voz: Atraso de transmissão dos pacotes, variação do atraso (PDV – packet delay variation), taxas de erros nos pacotes e taxa de perdas de pacotes.

Segundo (TIPHON, 2002), o efeito de baixos níveis de PDV na qualidade da voz é substancialmente menor que a taxa de perdas de pacotes. As duas métricas estariam muitas vezes correlacionadas na medida em que níveis elevados de variação do atraso levam a um aumento no descarte de pacotes.

Métodos adequados para as medições, incluindo amostragens adequadas são importantes para se obterem resultados significativos, como descrito na RFC 2330 (Paxson, V. et. al, 1998). Os resultados de uma medição devem formar uma amostra representativa do comportamento da rede, de forma a tornar aplicáveis as técnicas de otimização – RFC 3432 - (Raisanen, V. ; Grotefeld, G. & Morton, A., 2002). Com essa finalidade os cenários com os pontos de medição devem ser definidos cuidadosamente, segundo a recomendação ITU-T I.380 (ITU-T, 1999).

a. Métodos de medição passivos

Não necessitam adição de tráfego, que na medição ativa seria injetado na rede operacional. O tráfego normal da rede é monitorado. Um ou mais pontos de medição podem ser utilizados. Se os fluxos de medição incluem timestamping e números de seqüência, como é o caso do RTP, pode-se medir o *jitter* e as perdas de pacotes. Segundo a RFC 3432 (Raisanen, V. ; Grotefeld, G. & Morton, A., 2002) deve-se observar que os efeitos da implementação da pilha TCP/IP dos *hosts* e da rede de acesso podem ser significativos nas medições. Isso pode ser contornado pela combinação de medições passivas e ativas medindo um fluxo de teste, onde as propriedades de tal fluxo sejam bem conhecidas (Raisanen, V., 2003). Com dois pontos de medição, o atraso pode ser medido sem timestamps, desde que um elevado grau de sincronização possa ser implantado entre os pontos de medição. Apesar de não acrescentar tráfego na rede, as medições passivas requerem mais processamento, e podem necessitar o uso de grandes volumes de dados. No núcleo da rede, as medições passivas requerem alto desempenho para os probes de medição. Outros problemas com essa abordagem podem ser a criptografia, e a privacidade.

O Quadro 6-5 apresenta uma relação entre as métricas, tipos de medições e entidades (fluxo, interface, nós, caminho) envolvidas.

Quadro 6-5 Relações entre as características e os objetos medidos

| Entidades basicas | Fluxo (passiva) | Interface, nó (passiva) | Par de nós (ativa e passiva) | Caminho (ativa e passiva) |
|-----------------------|-----------------|-------------------------|------------------------------|---------------------------|
| Volume de tráfego | X | X | X | X |
| Tempo médio de espera | X | | | X |
| Banda disponível | | X | | X |
| Vazão | | | X(4) | X(4) |
| Atraso | | X(2) | X(4) | X(4) |
| Variação do atraso | | X(2) | X(4) | X(4) |
| Perdas de pacotes | | X | X | X |
| | | | | |

Fonte: (Raisanen, V., 2003)

2-medidas em um ponto

4-Medições ativas baseadas em métricas IPPM são usadas atualmente para pares de nós. Pode também ser aplicadas aos caminhos, mas sem os meios de se controlar o roteamento não existiria necessariamente uma correspondência um a um.

b. Métodos de medição ativos

As medições ativas, como é o caso deste trabalho, são baseadas em testes de transmissões controladas através da rede medida. Tais medições podem ser implantadas de forma relativamente fácil. Os pacotes de medição tipicamente transportam timestamps e números de seqüência para comportar as medições de perdas e latência. O aspecto obviamente negativo deste método é o consumo da capacidade da rede. Tais métodos são mais usuais nos segmentos de alta capacidade da rede, mas também podem ser utilizados para resolução de problemas (Raisanen, V., 2003).

As técnicas de medição ativas são objetos de padronização pelo IETF (IP Desempenho Metrics working group (IPPM WG), ITU-T (I.380), e European Telecommunications Standards Institute – ETSI -TIPHON.

Com essas medições, se pode obter diretamente os valores de atraso, variação do atraso, perdas e correlação de perdas, para avaliar-se o desempenho de segmentos inteiros fim-a-fim. Precisa-se determinar a população de interesse (tipos dos pacotes

que serão medidos) e também aquela porção que não deve ser considerada na medição.

Simulação de fluxos para calibração de QoS

Neste trabalho foi utilizado um padrão de medições ativas, com simulação dos fluxos para calibração de QoS segundo as especificações do TIPHON (TIPHON, 2002), usando-se o cálculo da variação do atraso pela especificação IPPM – RFC 3393 – (Demichelis, C.; Chimento, P., 2002).

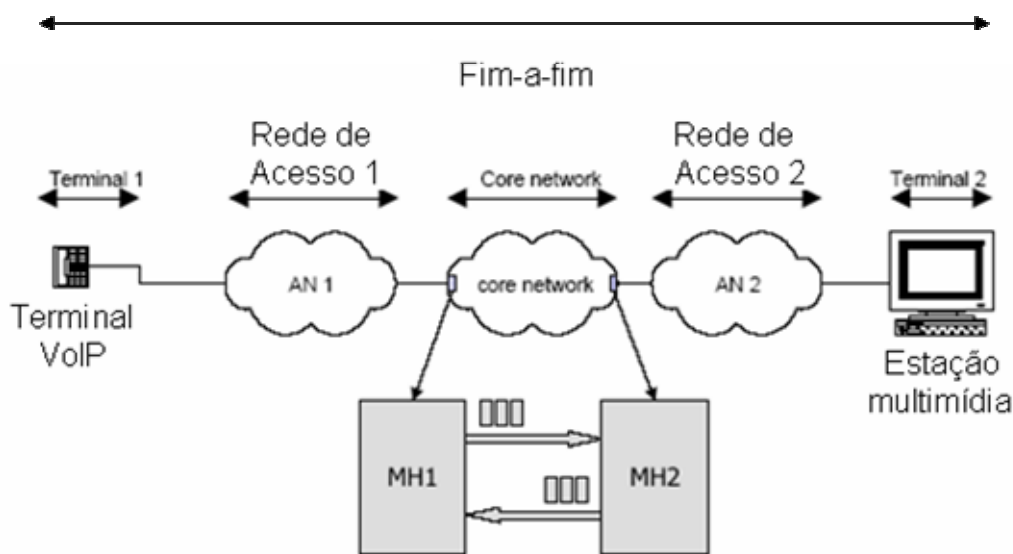


Figura 6-4 - Cenário de teste para determinação de QoS no núcleo da rede. Fonte: (TIPHON, 2002)

A medição deve ser feita transmitindo-se um fluxo VoIP simulado entre os dois *hosts* de medição. É importante que o fluxo simulado represente um tráfego VoIP de serviço, o qual a rede irá transportar. A medida deve ser round-trip (MH1-MH2-MH1) para emular uma chamada full-duplex, mas se podem efetuar medidas em um sentido (MH1-MH2 e MH2-MH1) como parte de uma medição round-trip. Os *hosts* de medição podem ser incluídos em um mesmo domínio ou em domínios diferentes. A metodologia de medição é independente dos caminhos fim-a-fim onde os *hosts* estão localizados. Localizando-se os *hosts* de medição em partes diferentes da rede permite que várias partes da rede sejam qualificadas.

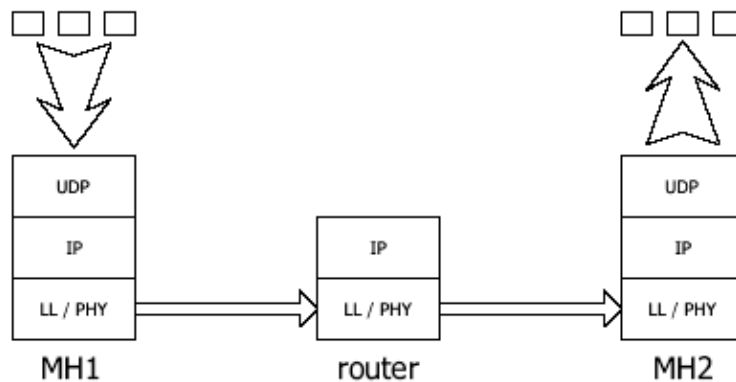


Figura 6-5 Pilha de protocolos nas medições no nível da camada de aplicação – Fonte: (TIPHON, 2002)

A medição é efetuada no nível da aplicação usando a mesma pilha de protocolos que uma aplicação VoIP . Os fluxos devem ser transmitidos através das interfaces UDP de ambos os *hosts* - Figura 6-5.

c. Piggybacking

Essa abordagem de medições é a mais orientada a pesquisas atualmente. Uma informação de seqüência e um timestamping são introduzidos na carga dos pacotes (Figura 6-6). A sobrecarga das medições, bem como para a inserção e remoção dos campos de medição (Quadro 6-6) devem ser considerados.

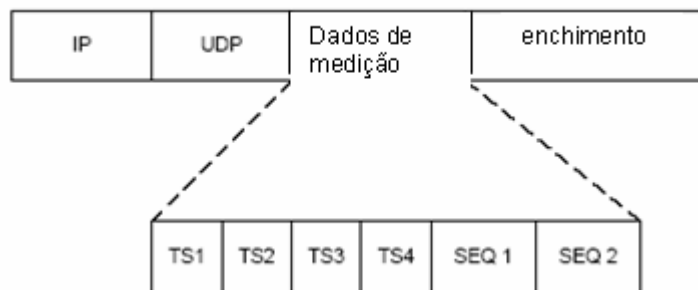


Figura 6-6 - estrutura de um pacote de medição – Fonte: TIPHON, 2002

As medições ativas geram mais tráfego, mas exigem menos processamento que as medições passivas. Além disso, podem ser usadas para monitoração dos níveis de serviço. As medições passivas são mais adequadas as redes de acesso. As medições passivas e ativas podem ser combinadas pela monitoração passiva dos fluxos usados nas medições ativas. Essa é a estratégia usada pelo plano de controle proposto neste trabalho de pesquisa, onde os agentes QoS monitoram os fluxos gerados pelos probs de medição, informando a QNS sobre os estados dos enlaces e dos fluxos de voz 5.3.

Quadro 6-6 - Campos de informação nos pacotes de medição.

| Campo | Descrição | Preenchimento |
|-------|--|--|
| TS1 | Tempo da transmissão no <i>host 1</i> | Imediatamente antes de enviar o pacote ao <i>host 2</i> através da interface UDP |
| TS2 | Tempo da recepção no <i>host 2</i> | Imediatamente após o recebimento do pacote no <i>host 2</i> , na interface UDP |
| TS3 | Tempo da transmissão no <i>host 2</i> | Imediatamente antes de enviar o pacote ao <i>host 1</i> através da interface UDP |
| TS4 | Tempo da recepção no <i>host 1</i> | Imediatamente após o recebimento do pacote no <i>host 2</i> , na interface UDP |
| Seq 1 | Número de seqüência transmitido no <i>host 1</i> | No <i>host 1</i> |
| Seq 2 | Número de seqüência recebido no <i>host 2</i> | No <i>host 2</i> |

Fonte: (TIPHON, 2002)

Relação entre medições agregadas e desempenho do nível de serviço fim-a-fim

As medições dos níveis de serviço, de uma forma geral, podem ser implementadas das seguintes maneiras (Raisanen, V., 2003):

- Usando-se retornos no pontos-finais (endpoints feedbacks);
- Estimando-se a partir das medições agregadas (tomadas fim-a-fim, passando por varios elementos da rede);
- Estimando-se a partir dos dados de cada elemento de rede.

Um ponto final de comunicação deve ser capaz de relatar a qualidade de serviço obtida, como nas mensagens RTCP, que transportam informações do *jitter* e das perdas. Além disso, o desempenho do sistema final é afetado por outros fatores, inclusive pelo sistema final em si.

A especificação ITU-T I.350 determina que o desempenho no nível de serviço seja medida nos pontos de acesso ao serviço, enquanto as medições de desempenho da rede sejam medidas nos limites da conexão dos elementos.

6.3.2. Medidas nos dispositivos

Os dados mais importantes para o controle de roteamento são os níveis de carga dos enlaces individuais, e as características do desempenho agregado (envolvendo vários segmentos). A obtenção de informações precisas a respeito da carga nos enlaces nas redes puramente baseadas nos protocolos de roteamento IP é importante principalmente devido a dois fatores:

- 1-A natureza não orientada a conexão do IP;
- 2-A natureza distribuída dos protocolos de roteamento.

Como resultado dessas duas características, os volumes de tráfego podem variar em um determinado enlace, potencialmente em função das rajadas, compartilhamentos de cargas e quedas em enlaces. Essas informações de cargas são importantes também para projetos de engenharia de tráfego baseadas em MPLS (Osborne, E. & Simha, A., 2003). Os níveis de tráfego em um enlace afetam não só o atraso de fila médio, mas também aumentam a variabilidade dos atrasos nas filas (Raisanen, V., 2003).

As propriedades dos fluxos transportados em segmentos particulares da rede, bem como as implementações de escalonamento nos elementos individuais afetam as dependências da carga, atraso de fila e variabilidade das filas. A teoria de filas pode ser usada para estimar o atraso e a variação do atraso em roteadores individuais quando as distribuições dos processos de chegada (tráfego ofertado) e o tempo de serviço (tamanho dos pacotes) são conhecidos. Normalmente estes fatores variam com a hora do dia ou em ciclos sazonais.

6.4. Análise do desempenho

A grande maioria dos protocolos de roteamento utiliza um modelo distribuído para manter as informações sobre os caminhos de destino. (Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998).

As tarefas de medições seguirão a proposta de (Hassan, M. & Jain, R., 2004), que dividem as medições em quatro tarefas básicas:

1. Coleta de dados;
2. Análise;
3. Apresentação;
4. Interpretação;

Como visto anteriormente, na seção **Error! Reference source not found.**, o problema de encontrar um caminho que atenda as múltiplas restrições de QoS é considerado NP completo. Neste trabalho, os caminhos buscados procuram atender somente os caminhos de menor variação do atraso ou perdas, (não simultaneamente) sem atender a todas as métricas.

6.4.1. QNS (QoS Network Server)

Funções de responsabilidade do Servidor de QoS da rede:

- a) Manter uma tabela com as métricas
- b) Verificar as necessidades dos fluxos, através da análise de requisições (Call Admission Control)
- c) Calcular os caminhos disponíveis que obedeçam as restrições do fluxo
- d) Sinalizar as roteadores para o estabelecimento das conexões.

Para a distribuição das políticas, podem-se utilizar vários métodos (Verma, D., 2000):

- Frameworks de gerência
- Scripts
- LDAP
- SNMP
- *Common Open Policy Service (COPS - 4.8.1)*
- Web Servers

No protótipo apresentado neste trabalho, se utilizam funções Java e scripts ExpectJ em um conjunto gerenciado pela QNS. O protocolo COPS é analisado como alternativa no capítulo 4.8.1. Como exemplo de parâmetros gerenciados e possivelmente distribuídos pelo servidor, encontram-se no Quadro 6-7 e Quadro 6-8 as sugestões de (Verma, D., 2000) que podem ser acrescentadas no QoS-Path quando forem necessárias implementações de políticas nos ambientes de produção.

Quadro 6-7 Exemplo de atributos para função ServicePolicyRule (IBM QoS Server)

| Atributo | Descrição |
|-------------------------|---|
| PolicyName | O nome da política. |
| SelectorTag | String unica para busca de políticas relevantes para o dispositivo. |
| DaysOfWeekMask | Dias da semana de validade da política. |
| TimeOfDayRange | Faixa de horário da validade da política. |
| PolicyScope | IntServ ou DiffServ. |
| ServiceReference | Nome da categoria do serviço. |
| ProtocolNumber | Número do protocolo no cabeçalho do IP. |
| SourceAddressRange | Endereço fonte dos pacotes aos quais se aplicam as políticas. |
| DestinationAddressRange | Endereço destino dos pacotes aos quais se aplicam as políticas. |
| SourcePortRange | Numero da porta fonte onde as políticas se aplicam |
| DestinationPortRange | Numero da porta destino onde as políticas se aplicam. |

Fonte: (Verma, D., 2000)

Quadro 6-8 - Exemplo de atributos para função ServiceCategory (IBM QoS Server)

| Atributo | Descrição |
|----------------|---|
| ServiceName | O nome da ServiceCategory. |
| SelectorTag | String unica para busca de políticas relevantes para o dispositivo. |
| DaysOfWeekMask | Dias da semana de validade da política. |
| TimeOfDayRange | Faixa de horário da validade da política.. |
| MaxRate | Taxa maxima do fluxo nesta classe. |
| OutgoingToS | O campo ToS nos pacotes de saida. |
| Priority | A priordade das filas na Interface Local. |

Fonte: (Verma, D., 2000)

6.5. Projeto de experimentos

Os experimentos foram projetados para responder as seguintes questões básicas:

- O plano de controle consegue reduzir o *jitter* para os fluxos de voz quando a métrica usada no algoritmo de Dijkstra é o *jitter*?
- O plano de controle consegue reduzir as perdas para os fluxos de voz quando a métrica usada no algoritmo de Dijkstra é o percentual de perdas?
- Se uma ou ambas as respostas forem verdadeiras, se quer saber se um caminho onde o plano de controle reduz a degradação baseado em uma das duas métricas (*jitter* ou perdas) produz melhorias também na outra métrica.
- Quais os fatores dentre os escolhidos para os experimentos, são os mais influentes nas respostas das métricas que se quer monitorar.

Para fins de identificação nos cálculos da rotina de melhores caminhos e tabelas do banco de dados, os enlaces foram denominados com os números dos roteadores e sentidos dos fluxos. Assim, o enlace entre o roteador 2 e 6 foi denominado 26. Entre o 6 e o 8, 68 e assim sucessivamente (Figura 6-7).

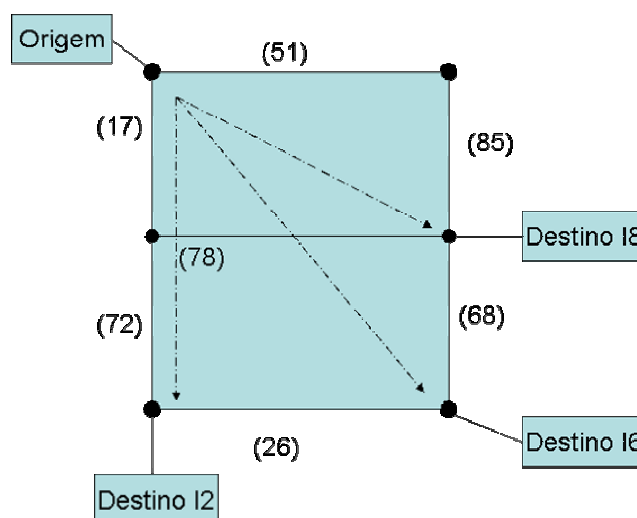


Figura 6-7- Identificação dos enlaces e dos fluxos de voz (12, 16, 18) a serem preservados

As colisões entre as medições podem ocorrer com bastante intensidade. Durante a fase de testes e calibração do plano de controle pode-se perceber que a quantidade de fluxos de medição que estão sendo computados em cada interface também interferem nas medidas. A proposta para o plano de controle foi projetada de forma que cada interface recebesse ou emitisse o mínimo possível de fluxos simultâneos, conforme o Quadro 6-9. Procurou-se preservar a interface do PC1 (30.0.0.1), mantendo-se somente os fluxos de monitoração, por ser a fonte dos fluxos de voz.

Quadro 6-9 - Fluxos de entrada e saída nas interfaces dos PCs utilizados no plano de controle

| If (PCs) | Sentido | |
|----------|---|---|
| | In (IP origem do fluxo de medição + fluxo do experimento) | Out (IP destino do fluxo de medição + fluxo do experimento) |
| 30.0.0.1 | 50.0.0.1+70.0.0.1 | Voz +50.0.0.1+70.0.0.1 |
| 70.0.0.1 | 20.0.0.2+80.0.0.8+30.0.0.1+ 57 | 30.0.0.1+20.0.0.2+80.0.0.8+ 76 |
| 20.0.0.2 | 60.0.0.1+70.0.0.1+ 12 | 70.0.0.1+60.0.0.1 |
| 60.0.0.1 | 80.0.0.8+20.0.0.2+ 16+76 | 20.0.0.2+80.0.0.8 |
| 80.0.0.8 | 70.0.0.1+50.0.0.1+60.0.0.1+ 18 | 60.0.0.1+70.0.0.1+50.0.0.1 |
| 50.0.0.1 | 30.0.0.1+80.0.0.8 | 80.0.0.8+30.0.0.1+ 57 |

6.5.1. Descrição dos fatores

Os fatores foram divididos dentro de dois ambientes (26,4 kbps e 1 pps - Figura 6-9). Cada ambiente possui 3 cenários. O primeiro corresponde ao roteamento utilizando-se somente OSPF, que serve como referência para a atuação do plano de controle utilizado nos outros dois cenários. O segundo cenário corresponde ao plano de controle proposto atuando para manutenção do *jitter*, e o terceiro com o plano de controle atuando para manutenção das perdas. Os cenários são comparados em termos de desempenho, medidos pelas métricas de perdas e *jitter*. O conjunto dos 3 cenários pode ser analisado pelo comportamento dos fatores, mantidos através dos experimentos.

Cada um dos três cenários possui os seguintes fatores:

- Tamanho do pacote no fluxo de voz;
- Intensidade do fluxo de medição
- Política de fila
- Destino do fluxo de voz
- Fluxo competidor

A seguir, os cenários e os fatores são descritos separadamente.

Cenário A.1 – OSPF

O OSPF (cenário A.1) foi utilizado como cenário para se constatar os valores de *jitter* e perdas através dos caminhos escolhidos pelo protocolo, comumente utilizado nos sistemas autônomos como IGP. O OSPF não sofreu nenhuma configuração adicional além da área (todas as redes foram consideradas área 0, para simplificação do ambiente). Todas as rotas foram divulgadas com suas métricas calculadas pela razão 1/banda, resultando no valor 1 para as redes alcançáveis pelas interfaces fast ethernet e 781 para as interfaces seriais PPP de 128 kbps.

Cenário B1. Dijkstra com métrica jitter

Este Cenário foi utilizado para testar a eficácia do plano de controle na redução do *jitter* para os fluxos de voz. Neste cenário, os agentes de monitoração do protótipo QoS-Path efetuam a leitura dos dados dos probs no servidor dos fluxos e enviam as condições dos enlaces em relação ao *jitter*, para que a QNS tenha uma visão da topologia caso seja necessária uma troca de caminhos.

Cenário B.2 Dijkstra com métrica perdas

Este cenário foi utilizado para testar a eficácia do plano de controle na redução das perdas para os fluxos de voz. Neste cenário, os agentes de monitoração do protótipo QoS-Path efetuam a leitura dos dados dos probs no servidor dos fluxos e enviam as condições dos enlaces em relação às perdas, para que a QNS tenha uma visão da topologia caso seja necessária uma troca de caminhos.

Fator D – Tamanho dos pacotes dos fluxos de voz

Neste trabalho, foi denominado *fluxo de voz* aquele que se quer manter em condições consideradas aceitáveis em relação a variação do atraso.

A geração de tráfego é efetuada pela própria ferramenta de medição (Iperf), usando o protocolo UDP. Optou-se por utilizar um fluxo de voz de 26.4 Kbps, conforme calculado na seção 2.3.2. Este valor está em conformidade com um fluxo gerado pela codificação G.729a usando PPP na camada de enlace. Os pacotes UDP são de 66 octetos, correspondendo a soma da carga gerada pelo CODEC e a sobrecarga dos cabeçalhos. No ambiente de estudos, o PC1 (origem) é a fonte do fluxo (cliente), enviando tráfego UDP na taxa especificada para o PC6 (destino), para o PC8 e PC2. Tais fluxos foram denominados 16, 18 e 12 conforme a Figura 6-7. O fluxo de voz monitorado tem a duração de 3 minutos, e dispara os gatilhos para troca de rotas segundo o algoritmo descrito a seguir (Quadro 6-10).

Quadro 6-10 - Algoritmo de disparo do gatilho para alteração dos caminhos

```

//Tipo-mensagem= gatilho (emitido pelos probs do fluxo de voz, quando está degradado) ou
//informativa (oriundo dos probs de medida dos enlaces)
Valor-máximo =10;
Erros =0;
Acertos =0;
Caminho-degradado=0;
Se tipo-mensagem=gatilho
    Se Erros >= Valor -maximo
        Caminho-degradado= Caminho-degradado ++;
        Se Caminho-degradado > Valor -maximo
            Dispara gatilho;
        Fim se
    Senão
        //introdução de uma medida conservadora, para evitar alterações muito
        //frequentes, o que desestabilizaria os caminhos.

        Acertos= Acertos++; //linhas de leituras boas
        Se Acertos >=3
            Erros= Erros - -; // diminui um erro
        Fim se
    Fim se
Senão
    //a mensagem é de um enlace
    Atualiza métrica do enlace (enlace(jitter,perdas));
Fim se

```

Fator J - Fluxos competidores

Foram denominados fluxos competidores (Figura 6-8) aqueles projetados para alocar recursos nos ambientes sendo utilizados pelos fluxos de voz. Nos ambientes de amostragem, um fluxo era originado no PC5, tendo como servidor o PC7 (fluxo com a identificação J57 nos fatores dos ambientes de amostragem). Em um segundo momento das amostragens, um fluxo competidor foi gerado no PC7 dirigido ao servidor no PC6. Como estes fluxos foram considerados fatores nos cenários, eles não foram simultâneos.

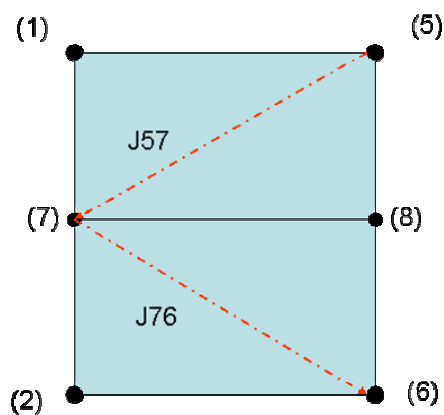


Figura 6-8 -Fluxos competidores pelos recursos (fatores J57 e J76)

Como o ambiente de laboratório possui limitações (poucos fluxos, protocolos e usuários, interferências minimizadas, como por exemplo outras aplicações interagindo com as interfaces, cpu e memória das estações) dificilmente poderá ser uma reprodução fiel da realidade. Entretanto, os testes criteriosos (reprodução dos ambientes controlados, em conjunto com a percepção clara das limitações e das condições do ambiente) têm levado a resultados satisfatórios, como pode ser constatado em (Hassan, M. & Jain, R., 2004), (Pawlikowski, K., 1990), (Jain, R., 1991).

Fator E - fluxo de medição

Os fluxos de medição foram escolhidos com base no seguinte compromisso:

- Deveriam possuir semelhança com fluxos de voz;
- Deveriam interferir minimamente nas medidas.

Desde o início dos experimentos, este foi um fator difícil de calibrar, pois a variável de resposta *jitter* mostrou-se sensível a um número muito grande de influências, como por exemplo o número de fluxos entrando ou saindo da interface utilizada para a medição (Quadro 6-9).

Segundo (Barford, P. & Sommers, J., 2004), não existem estudos na literatura para determinar uma escolha de tamanho dos pacotes utilizados em medições ativas (probs) para medir perdas na Internet. Estes autores utilizaram probs UDP de 256 bytes em intervalos regulares, baseados no compromisso de evitar consumos, e devido ao fato de este ter sido o tamanho utilizado por outros autores.

Alguns roteadores podem utilizar técnicas de *buffer* denominadas *buffer carving* que organizam as filas por pacotes, e não por bytes. Nessa situação, o tamanho do pacote não influencia nas perdas.

Foram utilizados pacotes de 66 bytes e de 1470 bytes em diferentes taxas dependendo do ambiente.

Fator H – Disciplina de filas

As filas foram escolhidas com base na disponibilidade dos equipamentos e sistemas operacionais, bem como na simplicidade de configuração. Este último critério demonstrou-se importante nos períodos de amostragem, quando 20 interfaces precisavam ser re-configuradas em cada situação de troca deste fator. Não se adotaram políticas de fila nas interfaces dos PCs, nem nas interfaces dos switches de camada 2. Somente as interfaces seriais e as fast ethernet dos roteadores foram configuradas com filas.

As filas escolhidas foram:

H1- WFQ: padrão para o IOS nas interfaces de baixa velocidade (< 1Mbps);

H2 – RED, utilizada para evitar congestionamentos nas conexões TCP;

H3 – Priority Queue, com prioridade para pacotes menores de 100 bytes.

Fator I – destinatário dos fluxos

Em todos os experimentos se considerou que a origem do fluxo de voz a preservar é o PC1, e os destinatários, o PC6 (fluxo 16), PC2 (fluxo 12) e PC8 (fluxo 18) - (Figura 6-7). Os destinatários foram escolhidos com base na disponibilidade das interfaces de medida, uma vez que já se tinha percebido que muitos fluxos na interface de medida alteram o valor do *jitter*.

6.6. Ambientes de experimentação

Para a análise do desempenho do plano de controle, foram elaborados dois ambientes para experimentação (Figura 6-9).

6.6.1. Ambiente 26,4 kbps

O primeiro ambiente foi denominado “Ambiente 26,4 kbps” (Figura 6-10), onde os fluxos dos agentes de amostragem possuíam taxas de 26,4 Kbps, com dois tamanhos de pacotes: 1470 bytes (datagrama UDP convencional) e 66 bytes, datagrama com tamanho para fluxos de voz em protocolo PPP.

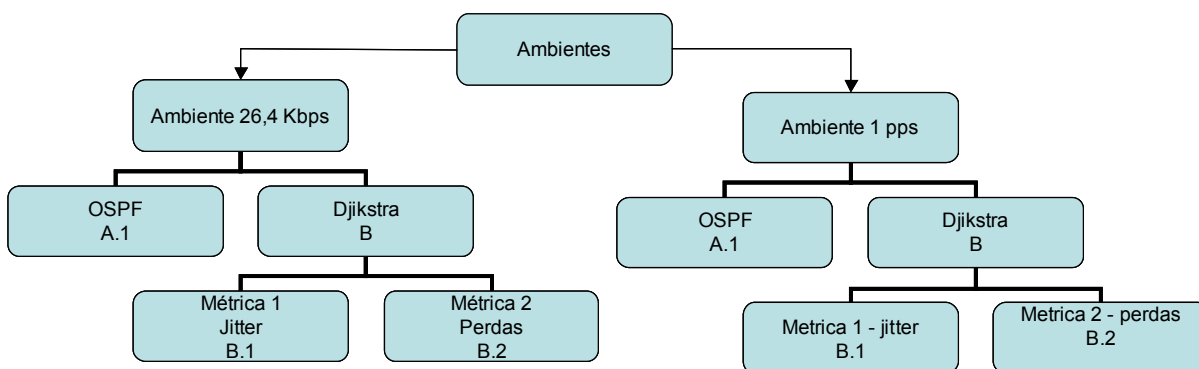


Figura 6-9 -Ambientes de amostragem

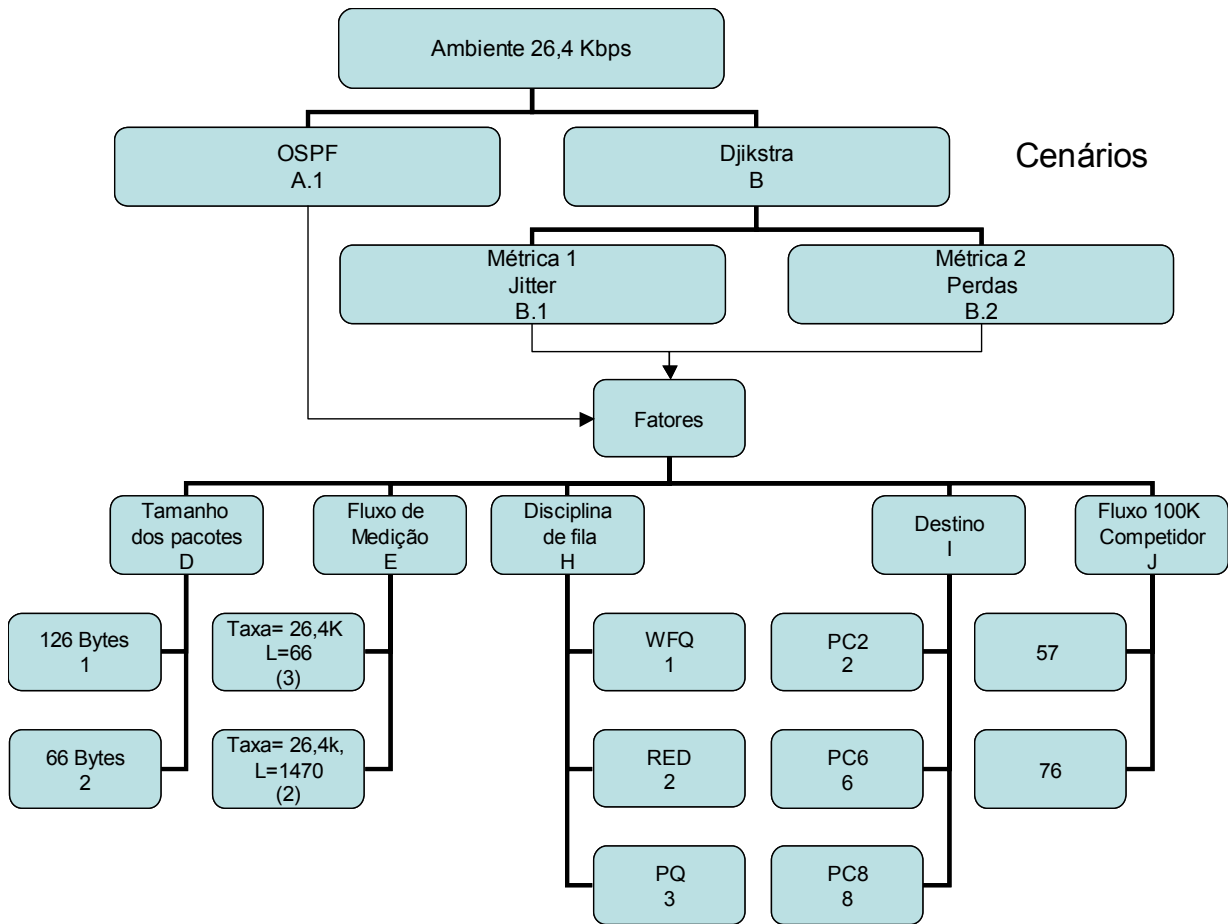


Figura 6-10 - Diagrama dos fatores do ambiente 26,4 kbps

6.6.2. Ambiente 1 pps

6.6.3. No segundo ambiente, denominado “Ambiente 1 pps” (

Figura 6-11) as taxas dos fluxos de medição foram reduzidas para minimizar uma possível interferência dos probs de medição nas próprias medidas. Neste segundo ambiente, tais fluxos foram de 1.44 Kbps com pacotes de 1470 bytes, e de 528 bps para os pacotes de 66 bytes, caracterizando um pacote de medição por segundo (1 pps), seguindo o modelo das requisições ICMP através do utilitário ping, dentro das implementações padrão dessa ferramenta.

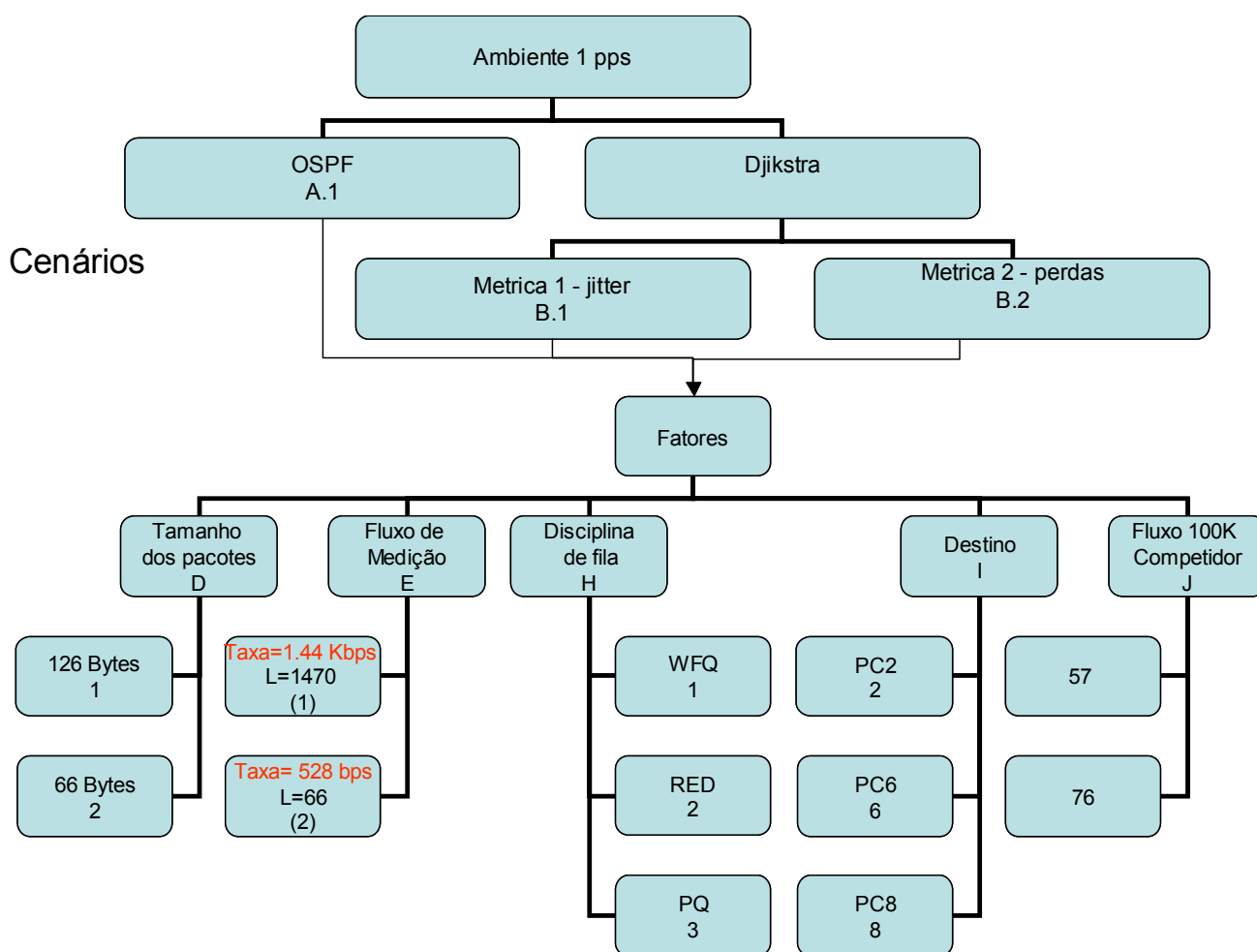


Figura 6-11 - Ambiente 1 pps e os fatores analisados

6.6.4. Amostragem

Nos dois ambientes as amostragens foram de 180 segundos para cada fluxo de voz. Os agentes de medição que atuaram como servidores foram configurados para reportar os valores medidos a cada segundo, gerando um arquivo monitorado pelos agentes de monitoração. Os valores reportados para os fluxos de voz foram armazenados em uma tabela de banco de dados MySQL para posterior cálculo das médias, do desvio padrão e dos valores de *jitter* e percentual de perdas máximos e mínimos.

Cada amostra foi coletada 3 vezes, de forma não consecutiva, na seguinte seqüência:

- 1) Todos os fatores são configurados;
- 2) a origem dos fluxos de voz, PC1 dispara um fluxo de voz com 180 segundos de duração em direção ao destino PC2, depois em direção ao PC6 e depois em direção ao PC8 (seqüência de amostras denominadas amostras A);
- 3) Outra seqüência idêntica é disparada pelo PC1, iniciando novamente com destino no PC2, PC6 e PC8, e as amostras agora eram denominadas amostras B para os mesmos fatores;
- 4) A terceira seqüência, denominada amostras C é disparada;
- 5) Muda-se um parâmetro, por exemplo, o tamanho dos pacotes do fluxo de voz.
- 6) Volta-se ao passo 2.

Como cada amostra gera um arquivo de dados, foram gerados 644 arquivos com 180 leituras cada no ambiente 26,4 kbps e 500 arquivos com 180 leituras cada no ambiente 1 pps (pacote por segundo). Os arquivos de medição dos enlaces também foram armazenados, para que se pudesse sanar eventuais dúvidas sobre a situação dos ambientes em instantes determinados.

6.7. Limitações da Experimentação

O ambiente 1 pps não foi amostrado no cenário B.2 (Dijkstra com métrica em perdas) para as filas RED e PQ. Essa é uma limitação quando se deseja comparar os dois ambientes ou mesmo no ambiente 1 pps, quando desejar-se comparar os cenários A.1 e B.1 com o B.2, ou as disciplinas de filas dentro ambiente. Não poderia-se concluir, dentro dessas limitações, qual a melhor disciplina de filas nos dois cenários, em relação as perdas, por exemplo.

As amostras têm um tamanho de 180 segundos, o que pode ser insuficiente para reduzir as médias com o uso do plano de controle em algumas amostras. Esse fato pode ser motivado pela grande alteração nos valores das variáveis no momento das alterações de rotas.

6.8. Análise de dados: ANOVA

O tratamento estatístico dos dados obtidos nos experimentos foi efetuado com o uso do software Statistica (<http://www.statsoft.com>) versão 6.0. Segundo o manual do software, quando existem fatores com mais de dois níveis, em conjunto com fatores com dois níveis, deve-se utilizar a análise através de 2 e 3 níveis fatoriais mistos. Tal análise se aplica a variações de resposta não linear, como os tipos de filas ou os destinos dos fluxos de voz, que poderia possuir muitos níveis e, no caso destes trabalho, possuem 3 níveis. Quando as respostas acompanham fatores (variáveis independentes) com variação linear (temperatura, por exemplo) é comum se utilizarem somente 2 níveis.

6.9. Sumário do capítulo

Neste capítulo foi descrita a metodologia utilizada para a avaliação do desempenho do plano de controle proposto. Foram descritos os ambientes de experimentações, bem como os fatores utilizados. Foi analisada a técnica de amostragem e as limitações dos experimentos.

Pode-se considerar que a elaboração do ambiente experimental e o plano de mostragens exigem realmente re-alimentações, e novos testes devem ser configurados a cada resultado experimental, até que o ambiente seja realmente conhecido e os fatores tenham suas influências bem caracterizadas.

No próximo capítulo serão analisados os resultados, e o comportamento dos fatores nos dois ambientes de experimentação. Ao final do capítulo são apresentadas as conclusões a respeito da proposta, com base nesses resultados.

7. Resultados

Neste capítulo são analisados os resultados encontrados, em relação aos experimentos do ambiente de 26,4 kbps e de 1pps descritos no capítulo anterior. Para cada ambiente, as variáveis de resultado (*jitter* e perdas) são analisadas separadamente, através de tabelas e gráficos.

7.1. Ambiente 26,4 kbps - Jitter médio

Neste ambiente foram executadas 644 amostragens, para análise do *jitter* e das perdas. Quando analisado sob os valores do teste ANOVA, demonstrou que poucos fatores tiveram influência significativa nas médias da variável *jitter* .

Segundo (Ma, Q. & Steenkiste, P., 1997) e (Zhang, H., 1990), o *jitter* em um determinado determinado salto dentro de um caminho de pacotes é dado por:

$$J(p, r, b) = \frac{b}{r} + \frac{n \cdot L \max}{r} \quad (\text{equação do jitter})$$

Onde:

J= *jitter*

p=caminho

r=banda

b=buffer

n=numero de saltos no caminho p

Lmax=tamanho máximo do pacote no caminho

Pela equação, deve-se esperar uma influência direta (negativa) no *jitter* pelos seguintes fatores: Tamanho do pacote, Número de saltos, Tamanho do *buffer* .

A largura de banda deve influenciar positivamente, reduzindo os valores da variável.

Pelos fatores utilizados nos experimentos, pode haver uma relação entre as variáveis como listado no Quadro 7-1. Deve-se perceber que a relação não é linear, como no caso da relação entre o tamanho do *buffer* e a disciplina de filas. Significa apenas que as disciplinas de filas podem apresentar valores diferentes de *buffer* . O

mesmo acontece com os fluxos competidores em relação a banda disponível. A existência de um fluxo competidor não significa necessariamente uma competição pela banda no caso de uma amostra, uma vez que em algumas situações de amostragem os fluxos competidores e os fluxos de voz não percorrem os mesmos caminhos. O número de saltos relaciona-se da mesma forma com o destino. Não existe necessariamente uma relação linear, mas existe uma possibilidade grande que o número de saltos varie em função do destino. Para as amostragens com o cenário OSPF (A.1), por exemplo, o destino i6 (Figura 7-7) sempre vai possuir maior *hop count* que os demais destinos.

Quadro 7-1 relações entre variáveis da “equação do jitter” e os fatores experimentais usados neste trabalho de pesquisa

| EQUAÇÃO DO JITTER | | Fatores utilizados neste trabalho de pesquisa | |
|--------------------------|-------|---|-------|
| Variável | Sigla | Fatores | Sigla |
| Banda (r) | R | Fluxo competidor, fluxo de medição. | (j) |
| Tamanho máximo do pacote | Lmax | Tamanho pacote | (d) |
| Tamanho do <i>buffer</i> | B | Disciplina de filas | (h) |
| Numero de saltos | N | Destino | (i) |

Dos 6 fatores utilizados, apenas os valores dos tamanhos dos pacotes do fluxo de voz, disciplinas de filas e destinos dos fluxos de voz foram significativos (valores de $p \leq 0,05$) - Tabela 7-1.

Não influenciaram os fluxos de medição, os cenários e os fluxos competidores.

| | df | F | P |
|--|----|----------|----------|
| Cenários | 2 | 1,4236 | 0,241620 |
| Tam dos pacotes do fluxo de voz | 1 | 129,4990 | 0,000000 |
| Fluxo de medição | 1 | 0,1465 | 0,702020 |
| disciplina de filas | 2 | 31,5867 | 0,000000 |
| Destino dos fluxos de voz | 2 | 195,2084 | 0,000000 |
| Fluxos competidores | 1 | 2,6067 | 0,106910 |

Tabela 7-1 - Valores de F e P para teste ANOVA - Ambiente 26,4 kbps - variável: *jitter*

Quando analisam-se os valores do teste t, comparando-se os fatores em um mesmo nível, pode-se perceber uma tendência de influência dos cenários na variável *jitter*, com valor de $p=0,009427$. Nessa situação, os fluxos competidores também têm uma tendência de influenciar o *jitter* ($p=0,106910$).

| Fatores | t | p |
|---------------------------------|---------|-----------------|
| Cenários | 1,6758 | 0,094270 |
| Tam dos pacotes do fluxo de voz | 11,3798 | 0,000000 |
| Fluxo de medição | 0,3828 | 0,702020 |
| disciplina de filas | 0,7787 | 0,000000 |
| Destino dos fluxos de voz | 6,7845 | 0,000000 |
| Fluxo competidor | 0,6145 | 0,106910 |

Tabela 7-2 Estimativa dos efeitos para Jitter Médio- valores de P e teste t - Ambiente 26,4 kbps

A análise da Tabela 7-2 e da Figura 7-1 onde estão listados os valores de influência dos fatores no comportamento do *Jitter* Médio como variável de resposta dos experimentos, demonstra que os fatores influentes este ambiente são o destino, a disciplina de filas e o tamanho do pacote do fluxo de voz. O fluxo de medição não mostrou diferenças significativas nas médias para pacotes de 1470 ou de 66 bytes. Os protocolos também não demonstraram influência significativa no *jitter*, embora pareça haver uma tendência ($p=0,094270$), a qual pode ser observada na Figura 7-2.

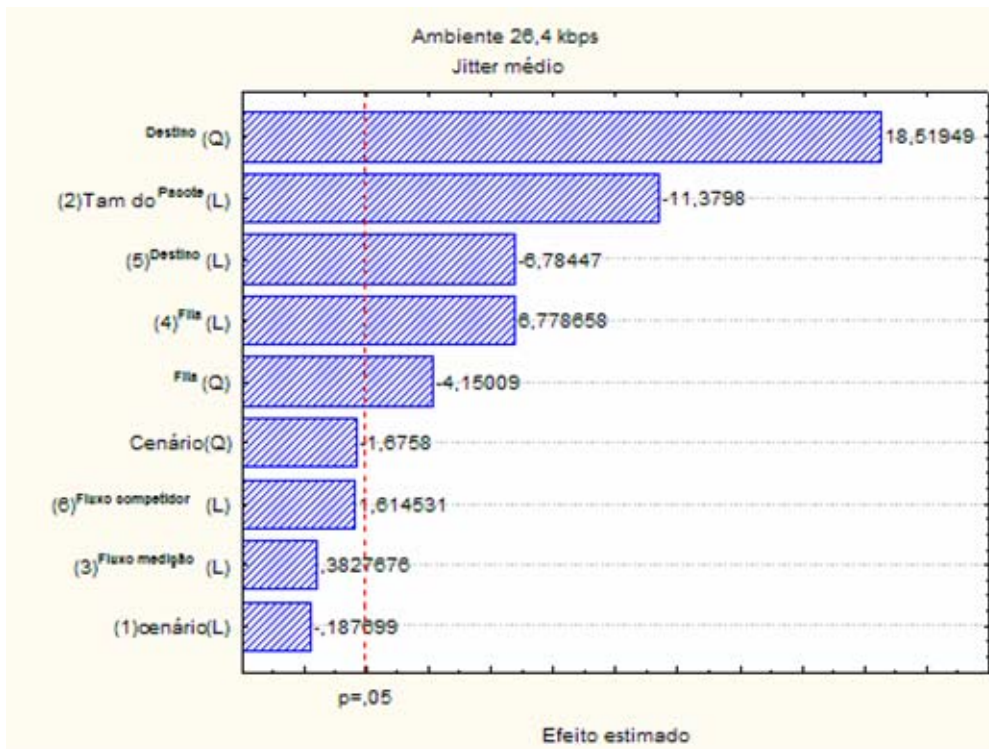


Figura 7-1 - Efeitos dos fatores sobre o Jitter no ambiente 26,4 kbps

7.1.1. Jitter e os cenários (a1, b1 e b2)

Na Figura 7-2 pode-se notar uma tendência de redução do *jitter* quando se utiliza o algoritmo de Dijkstra disparado sempre que o fluxo de voz atingir um limiar de 27 ms (cenário b1).

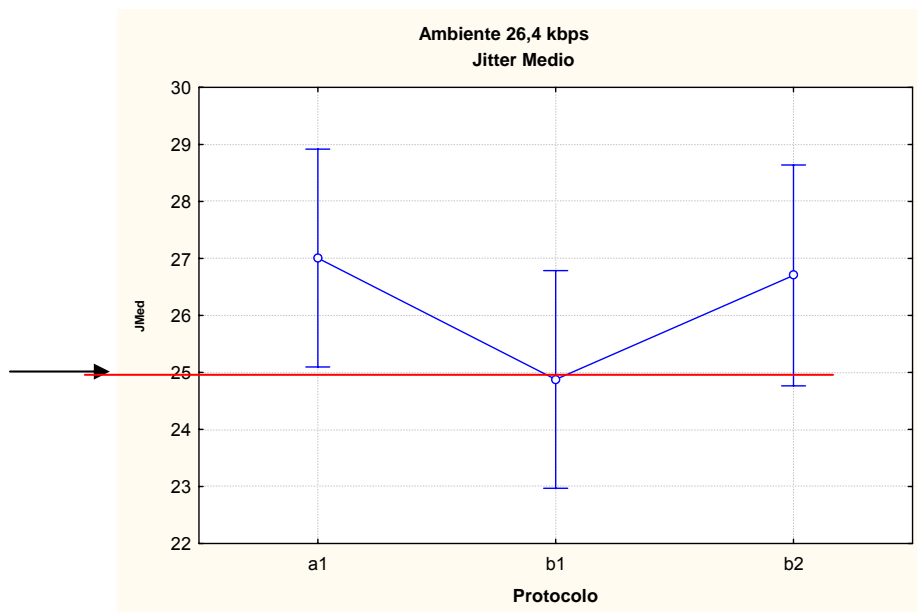


Figura 7-2 - Jitter médio em relação aos cenários (a1=OSPF, b1=Dijkstra para jitter e b2= Dijkstra para perdas. A seta aponta para o limiar desejado para a variável.

| Jitter (ms) | Cenário | | |
|---------------|-----------|----------------------|----------------------|
| | OSPF (A1) | Dijkstra/jitter (b1) | Dijkstra/perdas (b2) |
| media | 27,006 | 24,844 | 26,856 |
| Desvio Padrão | 17,962 | 18,868 | 22,119 |

Tabela 7-3 - jitter médio em relação às disciplinas de filas

Embora estatisticamente não exista uma influência da utilização do plano de controle nessa variável, pode-se perceber pela figura e pela Tabela 7-3 que o plano de controle consegue manter as médias de *jitter* dentro da faixa pretendida, abaixo dos 27 ms, com um intervalo de confiança de 95%.

As diferenças nas médias ficaram evidentes no ambiente de 1 pps (Figura 7-23 e Figura 7-24), demonstrando, na comparação entre os dois ambientes, que existe uma provável influência da intensidade do fluxo de medição (probs lperf) no valor da variável *jitter* médio.

7.1.2. Jitter e os Tamanhos dos pacotes dos fluxos de voz (fatores d1 e d2)

Na Figura 7-3 pode-se perceber que os pacotes menores nos fluxos de voz possuem menor variação no atraso para o ambiente de 26,4 kbps, o que foi confirmado pelo ambiente 1 pps (Apêndice I). Este comportamento está em conformidade com o esperado, uma vez que os pacotes menores devem sofrer menor influência nas transmissões das interfaces, otimizando os intervalos de transmissão entre os pacotes. Além disso, pela equação do *jitter* (Ma, Q. & Steenkiste, P., 1997), quanto maior o tamanho do pacote, maior o *jitter*.

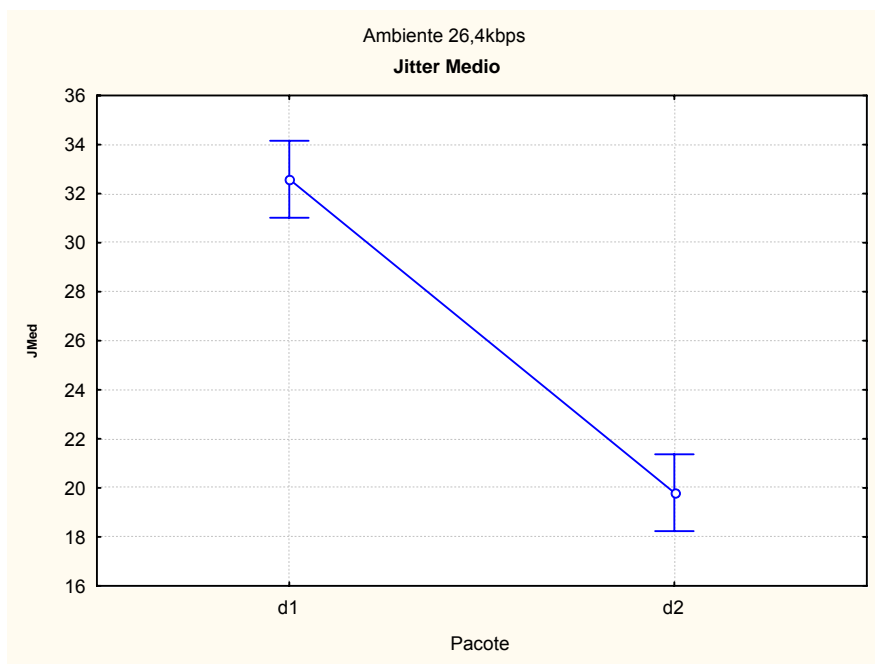


Figura 7-3 - Jitter médio em relação aos tamanhos dos pacotes dos fluxos de voz. D1=126 bytes, D2=66 bytes

A Tabela 7-4 mostra as médias de *jitter* em relação aos tamanhos dos pacotes nos fluxos de voz para o ambiente 26,4 kbps.

| <i>Jitter</i> (ms) | Tamanho do pacote do fluxo de voz | |
|--------------------|-----------------------------------|---------------|
| | 126 bytes (d1) | 66 bytes (d2) |
| Media | 32,65177 | 19,83326 |
| Desvio Padrão | 22,24939 | 14,16210 |

Tabela 7-4 Jitter médio para os tamanhos dos pacotes dos fluxos de voz

7.1.3. *Jitter* e os Tamanhos dos pacotes nos fluxos de medição (*probs*)

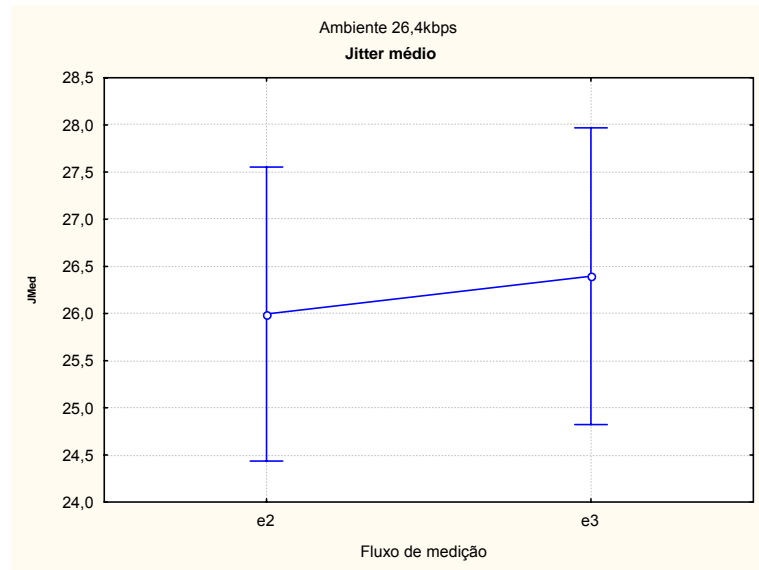


Figura 7-4 - Jitter médio em relação aos tamanhos dos pacotes dos fluxos de medição. E2=1470 bytes, E3=66 bytes (Ambos com taxa de 26,4 Kbps)

Pela Figura 7-4 e a Tabela 7-5 confirma-se a inexistência de influência do tamanho dos pacotes dos fluxos de medição. Apesar de existirem diferenças entre as médias, não é significativa no nível de 5% de significância. Percebe-se também a grande variação nos valores dentro deste intervalo de confiança.

| Jitter (ms) | Tamanho do pacote do fluxo de medição | |
|---------------|---------------------------------------|------------------|
| | 1470 bytes (e2) | 66 bytes (e3) |
| Media | 25,99435 | 26,49378 |
| Desvio Padrão | 18,41246 | 20,96415 |

Tabela 7-5 Jitter médio para os tamanhos dos pacotes dos fluxos de medição

7.1.4. *Jitter* e a Disciplina de filas

As disciplinas de filas tiveram uma influência no jitter semelhante aos resultados encontrados por (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005), onde a disciplina WFQ é mais eficiente para o *jitter* que a disciplina PQ. Ao contrário deste trabalho de pesquisa,

aqueles autores não utilizaram o tratamento RED, tendo preferido as filas do tipo FIFO como terceira técnica de enfileiramento.

A Figura 7-5 mostra a grande diferença entre as médias para a variável *jitter* neste ambiente, em relação as disciplinas de filas. A fila do tipo PQ apresentou maior média para o *jitter*. Embora estes resultados ainda devam ser analisados com precaução, uma vez que existe a suspeita da influência dos probs de medição no valor do *jitter*, os resultados mantiveram essa ordem no ambiente 1 pps, onde os valores de *jitter* foram mais reduzidos. A fila RED confirmou as médias mais baixas no ambiente 1 pps (Apêndice I).

| <i>Jitter</i> (ms) | Fila | | |
|--------------------|----------|----------|------------------|
| | WFQ (h1) | RED (h2) | PQ (LT 100) (h3) |
| média | 23,210 | 22,929 | 32,530 |
| Desvio Padrão | 11,416 | 12,857 | 28,446 |

Tabela 7-6 - jitter médio em relação às disciplinas de filas

Pela Tabela 7-6 pode-se perceber também os valores elevados de desvio padrão para a fila PQ. Essa observação também se repetiu no ambiente 1pps.

Analisando-se os valores das médias nas filas, em relação a Tabela 7-6, e a “equação do *jitter*”, uma possível explicação para esses valores seriam os tamanhos dos *buffers* nessas filas. Como essa variável não foi monitorada nos experimentos, a relação precisa ser melhor estudada.

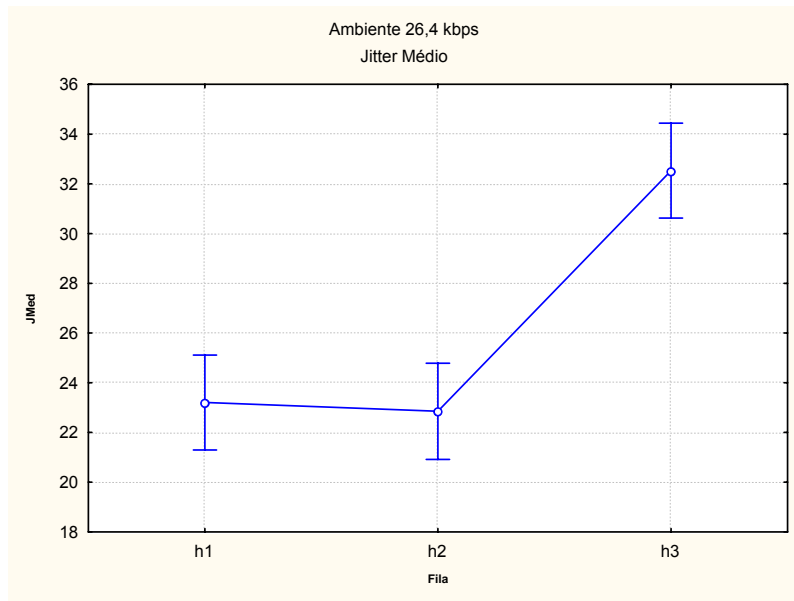


Figura 7-5 - Jitter médio em relação a disciplina de filas

7.1.5. Jitter e o Destino dos fluxos de voz

A Figura 7-6 mostra a média do *jitter* para cada um dos destinos do fluxo de voz, fator de maior influência na médias, tendo-se obtido um valor de estatística do teste $t=18,5195$.

Existe relação do número de saltos com o destino (Figura 7-7). Pela equação do *jitter* sabe-se que quanto maior o número de saltos, maior o *jitter*. Assim, é de se esperar maiores médias para o destino i6 (2 interfaces de PCs e mínimo de 4 roteadores).

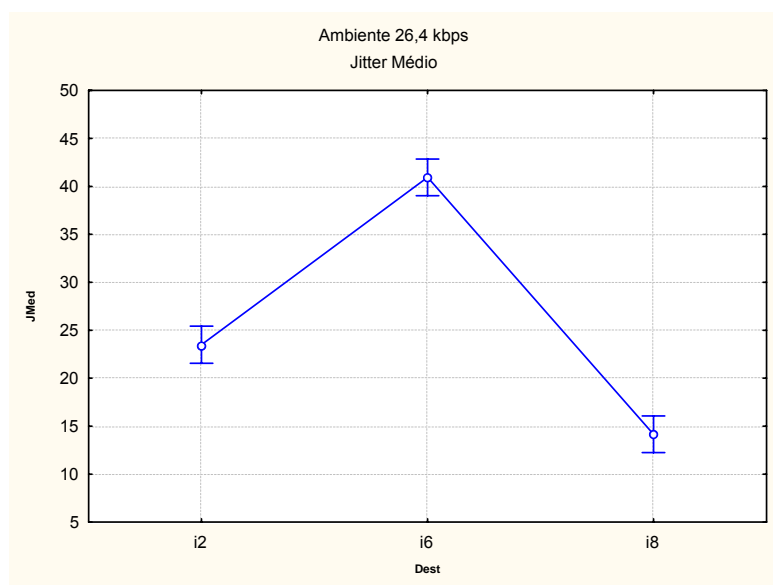


Figura 7-6 - Jitter médio em relação ao destino

O destino com o menor *jitter* foi o PC8, provavelmente por possuir menos saltos e os melhores caminhos mesmo com o protocolo tradicional. Deve-se considerar que o OSPF escolhe normalmente a rota 15-58-85 (Figura 7-7), que apresenta caminhos não degradados pelos fluxos competidores. O fluxo de voz com destino ao PC6 (fator i6 nas amostragens) possui os caminhos menos favoráveis nas rotas do cenário a.1 (OSPF): 17-78-86, onde enfrenta ambos os fluxos competidores, tanto para as amostras com fator j57 como para aquelas com fator j76. Este caminho não foi representado na Figura 7-7 para efeitos de clareza.

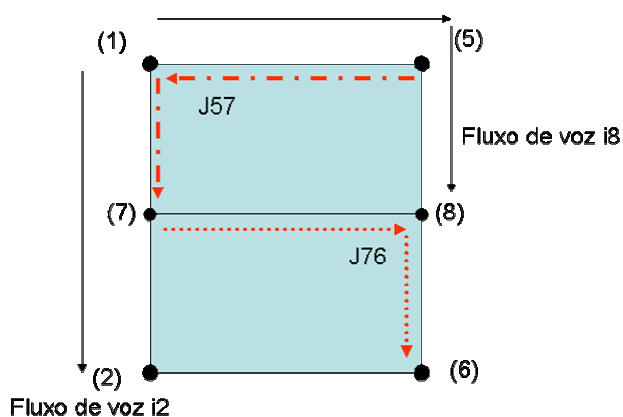


Figura 7-7 - Rotas preferenciais do protocolo OSPF - cenário a.1. Linhas pontilhadas correspondem aos fluxos competidores – Fator J

Essa relação fica aparente quando os destinos são plotados em conjunto com os fluxos competidores (Figura 7-8). O PC6 foi o destino com maior média de *jitter*. A grande variabilidade das médias pode ser causada, entre outros fatores, pelas diferenças obtidas nesse destino quando os fluxos competidores se alternaram (Figura 7-8) do 57 (médias menores) para o 76 (médias maiores).

| <i>Jitter</i> (ms) | Destino | | |
|--------------------|----------|----------|----------|
| | PC2 (i2) | PC6 (i6) | PC8(i8) |
| Média | 23,58187 | 40,93911 | 14,15730 |
| Desvio Padrão | 12,25218 | 25,17525 | 3,12558 |

Tabela 7-7 - jitter médio em relação ao destino do fluxo de voz

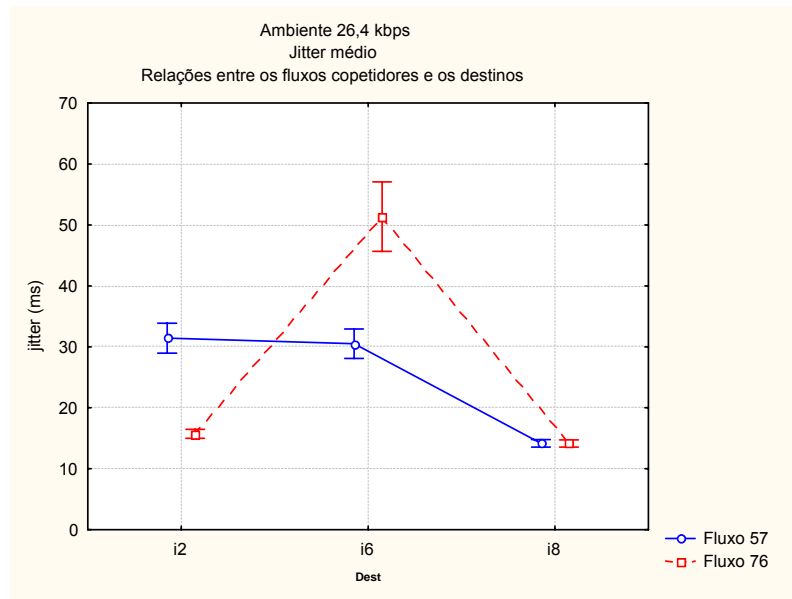


Figura 7-8 - Relações entre os destinos e os fluxos competidores

7.1.6. Jitter e os Fluxos competidores

Os fluxos competidores não influenciaram as médias de *jitter* significativamente, embora demonstrem uma influência aparente ($p=0,1069$). Essa tendência fica realçada quando se analisam os destinatários dos fluxos de voz separadamente, demonstrado na Figura 7-8. Pela ‘equação do *jitter*’ e pelo possível relacionamento entre as variáveis da equação e os fatores deste trabalho (Quadro 7-1), é de se esperar que os fluxos competidores, em alguns enlaces, reduzam a banda disponível, aumentando o *jitter*.

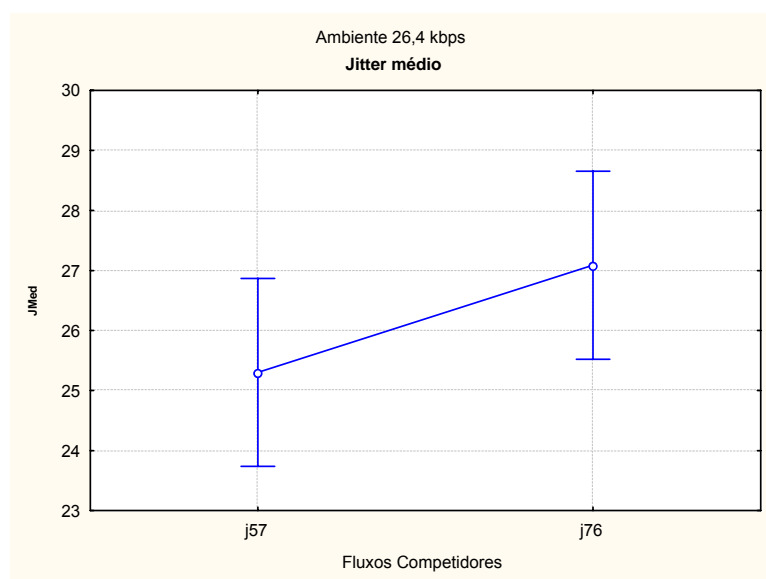


Figura 7-9 - Jitter médio em relação aos fluxos competidores

Como o fluxo 76 afeta diretamente a interface usada como destino na estação 6, usando a rota OSPF 78-86 (Figura 7-7), era de se esperar que sua atuação nas médias fosse maior, uma vez que o fluxo 57 deve degradar somente uma parte dos caminhos, e não afeta diretamente uma interface de destino.

| <i>Jitter</i> (ms) | Fluxo competidor | |
|--------------------|------------------|----------|
| | 57 | 76 |
| Média | 25,33319 | 27,15184 |
| Desvio Padrão | 13,17600 | 24,55092 |

Tabela 7-8 - *Jitter* médio em relação ao fluxo competidor – ambiente 26,4 kbps

Essa situação fica mais evidente na análise dos fatores para o ambiente de 1 pps (Tabela 7-9 e Apêndice I), onde se constata que as médias foram menores para este ambiente e o fluxo 57 é mais degradante, provavelmente pela sua influência na banda disponível nos enlaces, ficando em conformidade com a “equação do *jitter*”.

| <i>Jitter</i> (ms) | Fluxo competidor | |
|--------------------|------------------|----------|
| | 57 | 76 |
| média | 23,17066 | 21,09331 |
| Desvio Padrão | 11,43692 | 12,61404 |

Tabela 7-9 *Jitter* médio em relação aos fluxos competidores – ambiente 1 pps

7.1.7. Árvore de eventos – *jitter* no ambiente 26,4 kbps

Considerando-se o conjunto de fatores e a sua influência na média, pode-se traçar uma árvore de eventos para as condições que reduzem o *jitter* no ambiente 26,4 kbps (

Figura 7-10).

Pode-se concluir que em relação aos 3 cenários não houve diferença significativa entre as médias, com uma tendência a serem menores as médias do cenário Dijkstra/métrica *jitter* ($p=0,094270$ com relação a t). Este cenário, combinado com os

níveis a seguir deve levar aos melhores desempenhos com relação as médias para essa variável:

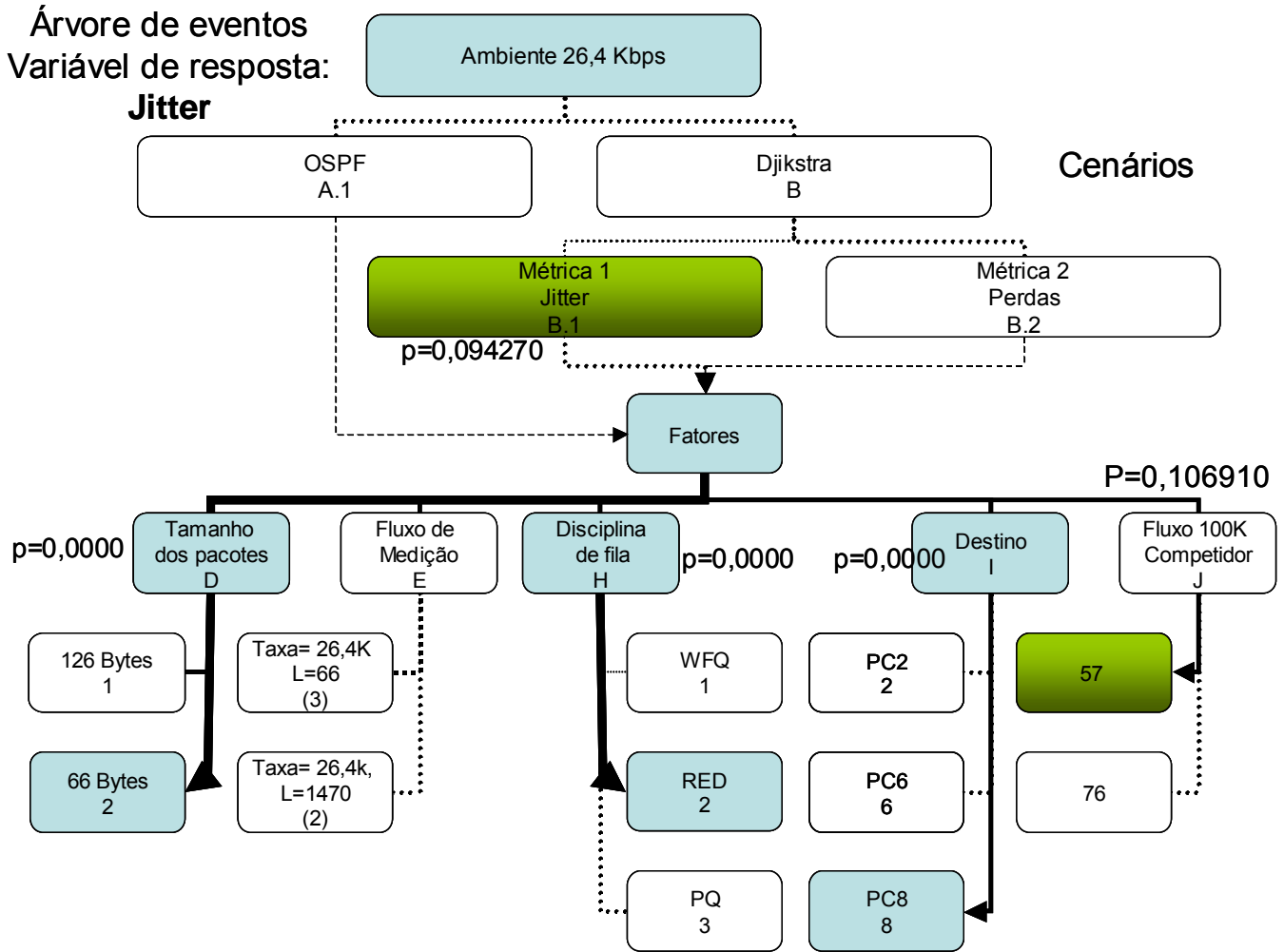


Figura 7-10 - Árvore de eventos para variável jitter -ambiente 26,4 kbps

- fluxos de voz constituídos por pacotes de 66 bytes;
- os roteadores com uma disciplina de filas RED;
- um destino com poucos saltos e caminhos não utilizados normalmente pelos fluxos competidores.
- Ausência de fluxo competidor na mesma interface de destino do fluxo de voz

7.2. Ambiente 26,4 kbps - Médias de Perdas

Normalmente as perdas de pacotes podem se dar por congestionamentos (buffers cheios) ou erros (nas interfaces, nos cabeçalhos) (C. Fraleigh et al, 2003). Como os ambientes estudados foram projetados para que ocorressem congestionamentos em alguns enlaces, e os erros normalmente são em número reduzido nas redes atuais, é de se esperar que as perdas tenham sido motivadas pelo enchimento dos *buffers*. Como tais *buffers* medem a capacidade em bytes, e não em número de pacotes, (alguns roteadores podem utilizar essa medida para os *buffers*, denominada *buffer carving*, mas não é o caso dos modelos utilizados nos experimentos dessa trabalho) - espera-se que os pacotes menores tenham taxas de perda maiores.

| | df | F | P |
|----------------------------|-----------|----------|----------|
| Cenários | 2 | 50,39423 | 0,000000 |
| Tamanho dos pacotes | 1 | 5,99023 | 0,014656 |
| Fluxo de medição | 1 | 3,67767 | 0,055595 |
| Disciplina de Fila | 2 | 62,64509 | 0,000000 |
| Destino | 2 | 86,89106 | 0,000000 |
| Fluxo competidor | 1 | 10,24502 | 0,001439 |

Tabela 7-10 - Estimativa dos efeitos para média de perdas

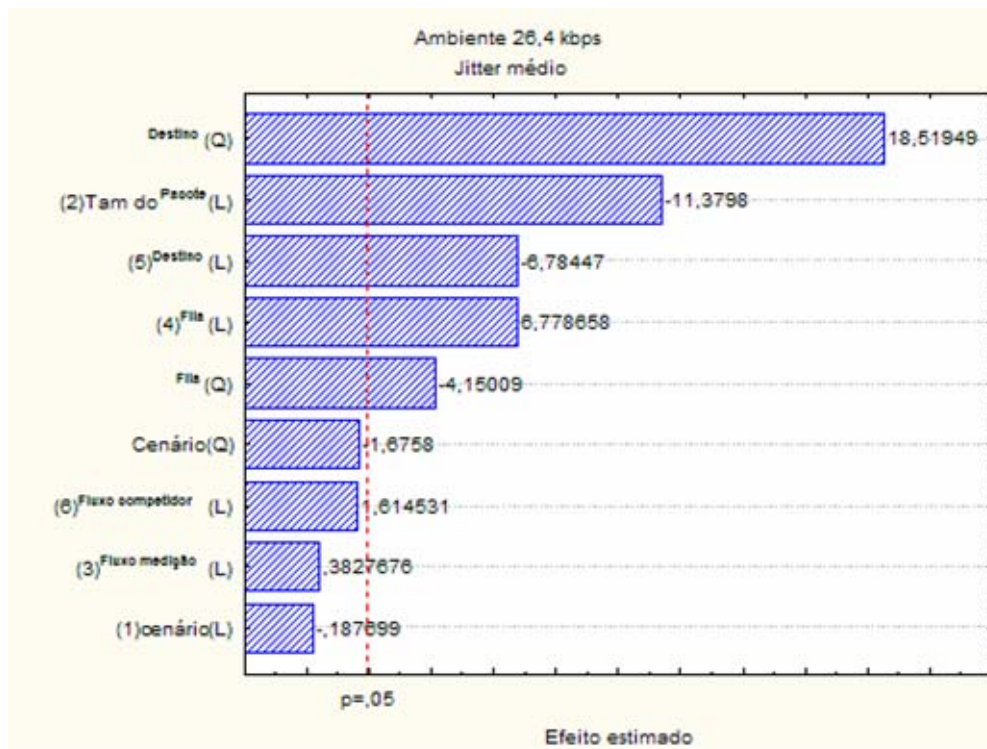


Figura 7-11 - Efeitos nas perdas – Ambiente 26,4 kbps

A análise da Tabela 7-10 e da Figura 7-11 demonstra que todos os fatores influenciaram nas médias da variável perdas, num nível de significância de 5%. O destino foi a variável mais influente, pelo gráfico de Pareto, seguido da disciplina de filas e dos cenários, onde são confrontados o OSPF e o plano de controle proposto neste trabalho.

7.2.1. Perdas e os Cenários (a.1, b.1 e b.2)

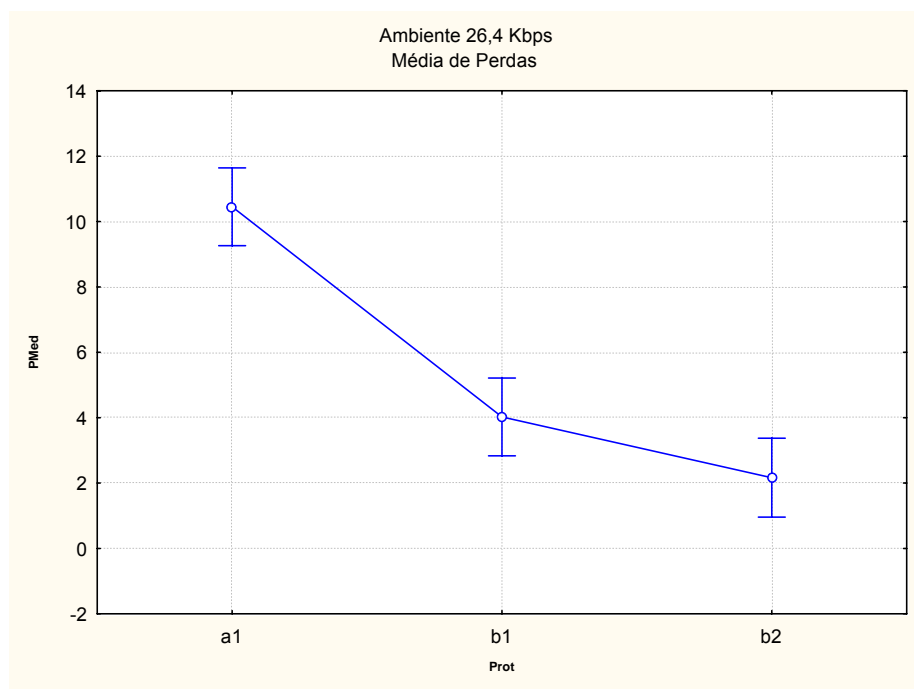


Figura 7-12 - Perdas médias em relação aos protocolos

Na Figura 7-12 está representada a redução das médias obtida pelo plano de controle (cenários b1 e b2) em relação ao protocolo de roteamento convencional OSPF (cenário a1). A Tabela 7-11 mostra os valores numéricos das médias. Percebe-se que o plano de controle com métrica nas perdas conseguiu reduzir a média de perdas de 10,45% no cenário OSPF para 2,16%. Pode-se notar também que as perdas foram menores quando o plano de controle estava configurado para encontrar melhores caminhos com base no *jitter* (cenário b.1), obtendo nessa situação uma média de perdas de 4,02 %.

| Perdas (%) | Cenário | | |
|---------------|----------|---------------------|---------------------|
| | OSPF-a.1 | Dijkstra-Jitter b.1 | Dijkstra-perdas b.2 |
| média | 10,45203 | 4,02143 | 2,16339 |
| Desvio Padrão | 15,42647 | 9,15409 | 5,50021 |

Tabela 7-11 – Média de Perdas em relação ao cenário

Embora a média de perdas tenha sido bastante reduzida pelo plano de controle, o valor ficou acima do limiar estipulado de 1%. Provavelmente, este limiar pode ser atingido com amostragens mais prolongadas, uma vez que em algumas situações, o plano de controle faz mais de uma tentativa para encontrar um caminho que se mantenha abaixo do limiar (Figura 7-13). Sabe-se também que amostragens maiores podem levar a médias mais próximas da situação real, embora também possam tornar significativos estatisticamente valores insignificantes na população.

As tentativas sucessivas para encontrar um caminho melhor são compreensíveis, uma vez que o fluxo desviado para um caminho melhor tende a degradar este novo caminho e melhorar as condições do caminho antigo.

Considerando-se que a reconfiguração dos melhores caminhos seja efetiva, pode-se prever uma provável redução da taxa de perdas ao longo do tempo. Embora não se tenha a comprovação estatística, este fato talvez possa ser comprovado pelo uso de um tempo maior de amostragem.

Trocas de rotas por Perdas - Bb2d1e2h2i6j76

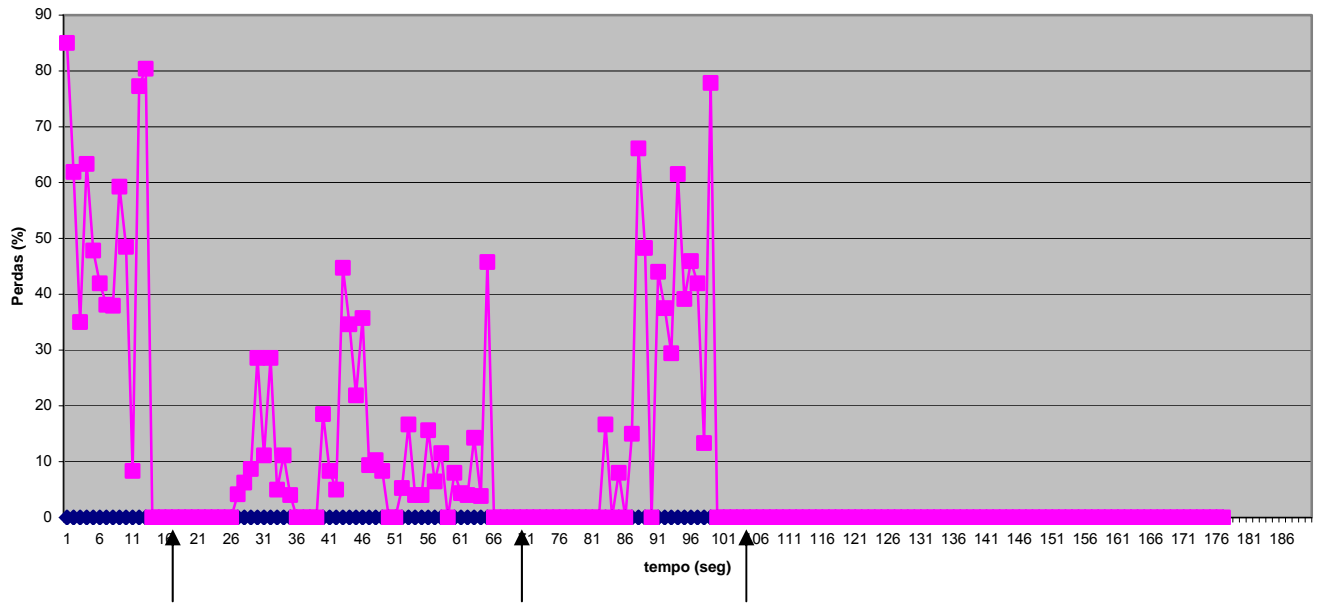


Figura 7-13 - Trocas consecutivas de caminhos no cenário b2, até a estabilização abaixo do limiar de 1%

7.2.2. Perdas e os Tamanhos dos pacotes dos fluxos de voz

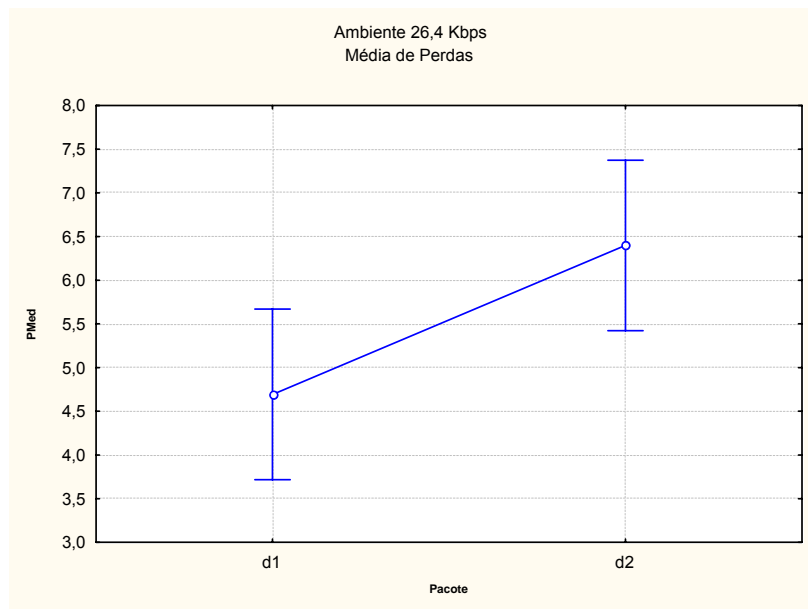


Figura 7-14 - Perdas médias em relação ao tamanho dos pacotes - d1 = 126 bytes - d2=66 bytes

Na Figura 7-14, percebem-se as diferenças nas médias (significativas ao nível de 95%) para os tamanhos de pacotes de 66 e 126 bytes. A Tabela 7-12 mostra os valores numéricos para essas médias.

| Perdas (%) | Tamanho dos pacotes do fluxo de voz | |
|---------------|-------------------------------------|---------------|
| | 126 bytes (d1) | 66 bytes (d2) |
| média | 4,692849 | 6,398380 |
| Desvio Padrão | 10,05610 | 12,56901 |

Tabela 7-12 – Média de perdas em relação ao tamanho dos pacotes dos fluxos de voz

Embora a política de filas PQ apresente uma tendência de melhorar as médias, em relação a política RED, (como pode ser constatado pela Figura 7-17), não foi efetiva para garantir a quantidade maior de pacotes gerada pelo fluxo de voz de 66 bytes. A atuação dessa fila pode ser menos eficiente na presença de mais de um fluxo com pacotes menores de 100 bytes, pois neste caso se caracteriza uma fila do tipo FIFO. Este é o caso quando o fator E – fluxo de medição – é do nível 3 – pacotes de 66 bytes (Figura 7-15).

7.2.3. Perdas e os Tamanhos dos pacotes no fluxo de medição

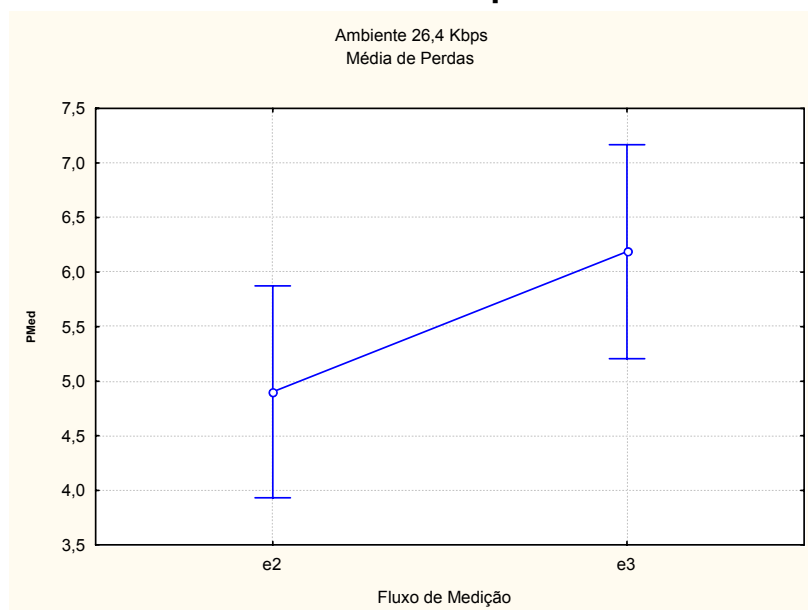


Figura 7-15 - Perdas médias em relação aos fluxos de medição – e2=1470 bytes – e3=66 bytes, ambos com 26,4 Kbps

A influência do tamanho do pacote nos fluxos de medição foi o único parâmetro não capaz de alterar significativamente as médias ($p=0,055595$), embora demonstre uma tendência a taxas de perdas maiores com pacotes menores. Como as taxas de

transmissão são as mesmas (26,4 kbps) pode-se esperar que se percam mais pacotes pequenos quando as filas estiverem congestionadas.

| Perdas (%) | Tamanho do pacote no fluxo de medição | |
|---------------|---------------------------------------|---------------|
| | 1470 bytes (e2) | 66 bytes (e3) |
| média | 4,903359 | 6,187870 |
| Desvio Padrão | 9,84210 | 12,77542 |

Tabela 7-13 – Média de perdas em relação ao tamanho dos pacotes dos fluxos de medição

7.2.4. Perdas e as Políticas de filas

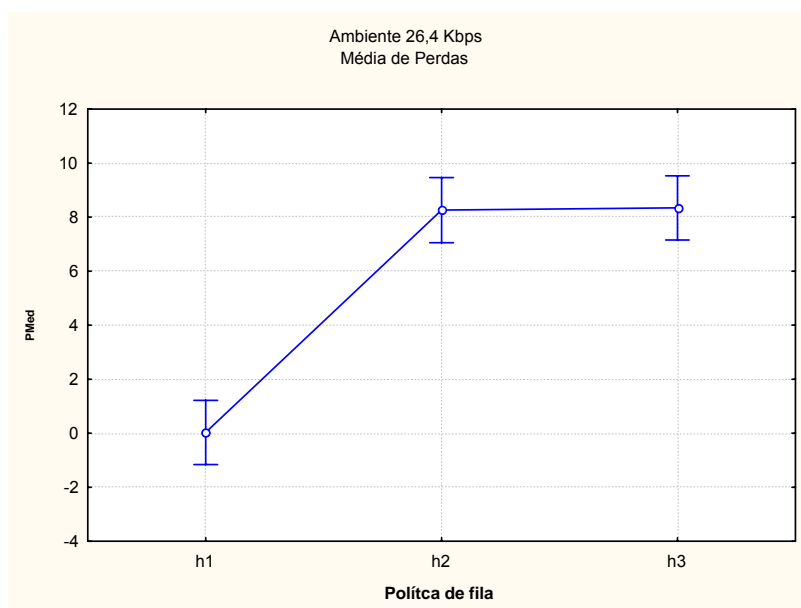


Figura 7-16 -Perdas médias em relação às políticas de fila

| Perdas (%) | Fila | | |
|---------------|----------|----------|-------------|
| | WFQ (h1) | RED (h2) | PQ (lt 100) |
| média | 0,029754 | 8,261804 | 8,345284 |
| Desvio Padrão | 0,07178 | 12,31317 | 13,91944 |

Tabela 7-14 – Média de perdas em relação às políticas de filas

A política de fila mais eficiente em relação às perdas para os fluxos de voz no ambiente 26,4 kbps foi a WFQ. Embora a configuração da política PQ possua como classe de mais alta prioridade os fluxos com pacotes menores de 100 bytes, a competição no ambiente demonstrou que uma fila mais balanceada (WFQ) é mais

eficiente do que uma do tipo que ou permanece na fila ou descarta, como a PQ. A política RED não teve eficiência para perdas, uma vez que foi projetada para uso com protocolo TCP.

A Figura 7-17 demonstra a tendência leve de redução das perdas da fila PQ (h3) em relação a RED (h2) quando os pacotes de voz são menores de 100 bytes (d2). Essa influência não foi efetiva dentro da própria fila PQ, onde os fluxos de pacotes menores tiveram perda maior.

A influência da fila PQ nas médias de perdas não ficou bem esclarecida, e necessita de acompanhamentos mais detalhados, como o de uso dos *buffers* e dos descartes nos roteadores.

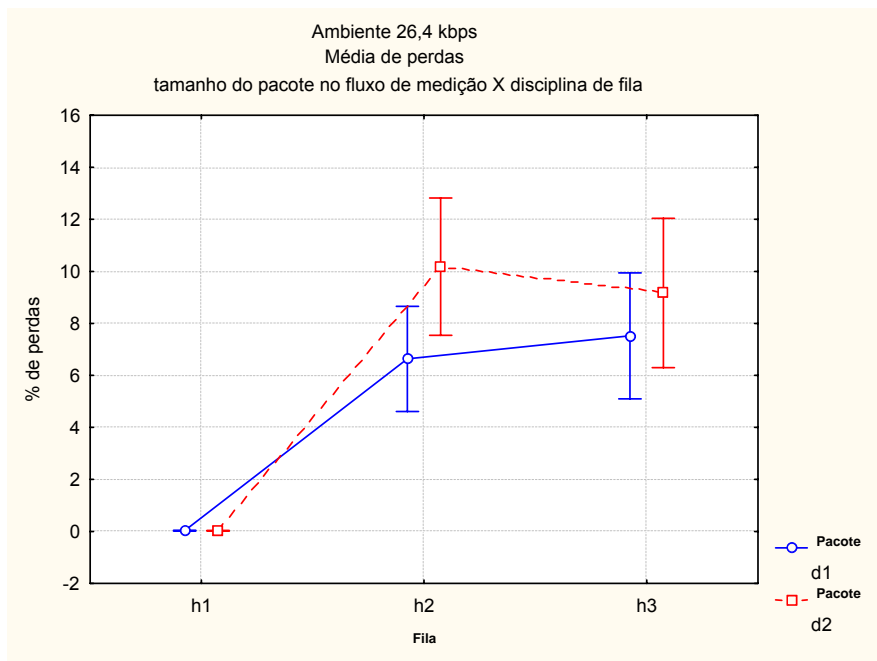


Figura 7-17 - Perdas médias em relação a disciplina de filas e tamanho do pacote no fluxo de medição.

7.2.5. Perdas e o Destino dos fluxos de voz

A Figura 7-18 mostra a influência dos destinos nas médias de perdas. Basicamente dois fatores podem estar influenciando essas médias: A quantidade de interfaces da origem até o destino (isso significa atrasos de transmissão, filas adicionais) e as condições dos enlaces.

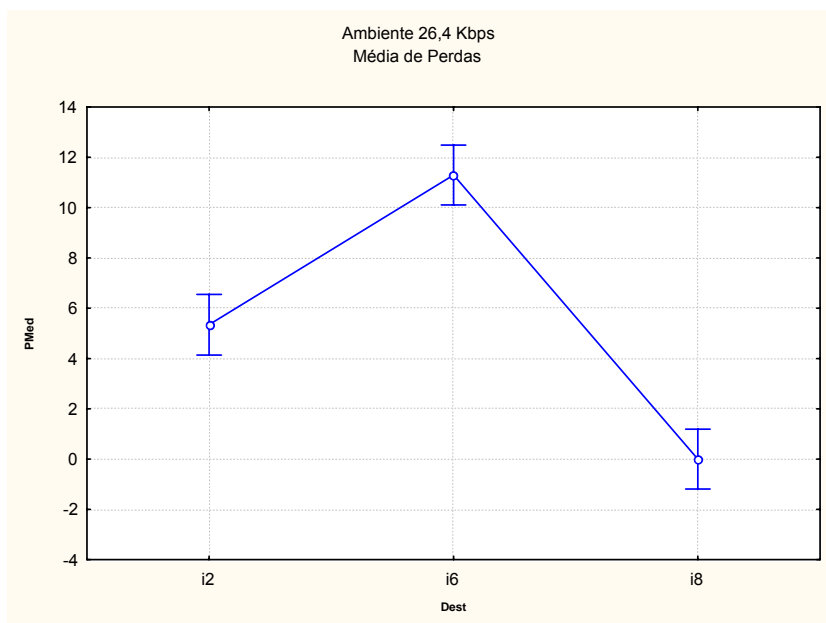


Figura 7-18 - Perdas médias em relação aos destinos

| Perdas (%) | Destino | | |
|---------------|----------|----------|---------|
| | PC2 (i2) | PC6(i6) | PC8(i8) |
| Média | 5,34187 | 11,29432 | 0,00065 |
| Desvio Padrão | 11,23461 | 14,18064 | 0,00718 |

Tabela 7-15 – Média de perdas em relação aos destinos dos fluxos de voz

O primeiro fator explicaria as perdas maiores para o destino mais distante (I6, com um mínimo de 5 saltos – PC1=> R1 => R7=>R2=> R6=> PC6, por exemplo). E as condições dos enlaces nos caminhos até o PC8, normalmente menos congestionados pelos fluxos competidores (Figura 7-7).

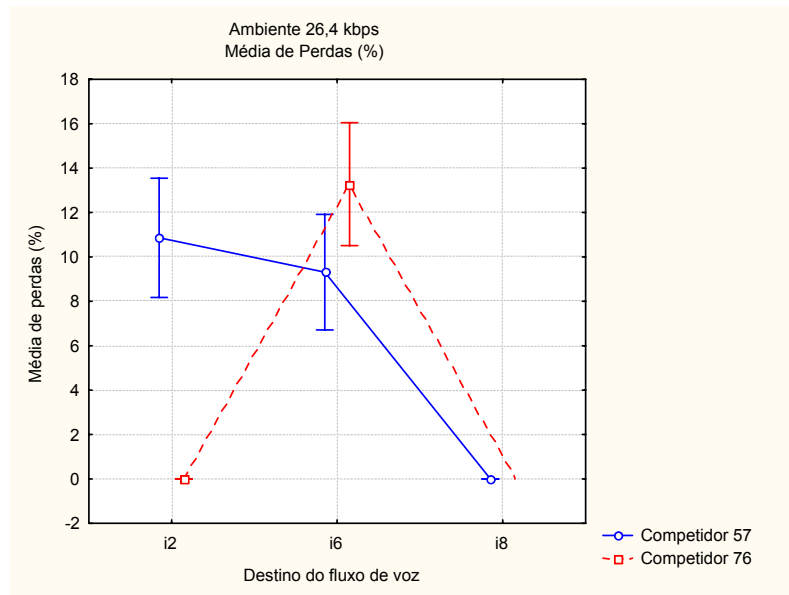


Figura 7-19 Média de perdas e as influências do destino e fluxos competidores

A Figura 7-19 mostra o comportamento esperado para as perdas em relação aos fluxos competidores. Quando a interface de destino do fluxo de voz (i6) recebe também um fluxo competidor (j76), as perdas são elevadas. Quando isso não ocorre (i2 e i8) as perdas são reduzidas. Os destino i2 e i6 possuem perdas altas quando competem com j57 porque os enlaces utilizados são os mesmos, em pelo menos um segmento (do roteador 1 ao roteador 7, enlace 17), quando o protocolo é o OSPF (A Figura 7-7 mostra as rotas do OSPF para os fluxos).

7.2.6. Perdas em relação aos fluxos competidores

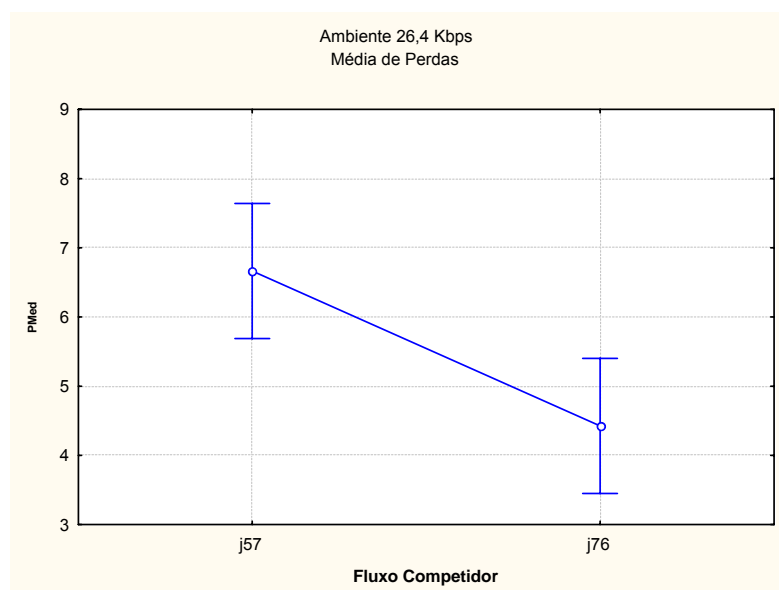


Figura 7-20 - Perdas médias em relação aos fluxos competidores

| Perdas (%) | Fluxo competidor | |
|---------------|------------------|----------|
| | J57 | J76 |
| Média | 6,665437 | 4,425792 |
| Desvio Padrão | 12,18582 | 10,46709 |

Tabela 7-16 – Média de perdas em relação aos fluxos competidores pelos recursos

Conforme discutido na seção acima, o fluxo competidor 57 influencia no enlace 17 usado pelos fluxos i2 e i6, elevando a média de perdas, principalmente quando o protocolo é o OSPF. Isso fica bem claro na Figura 7-21, que mostra o OSPF com médias bem maiores quando o competidor é o 57, destacando-se o problema nos destinos i2 e i6.

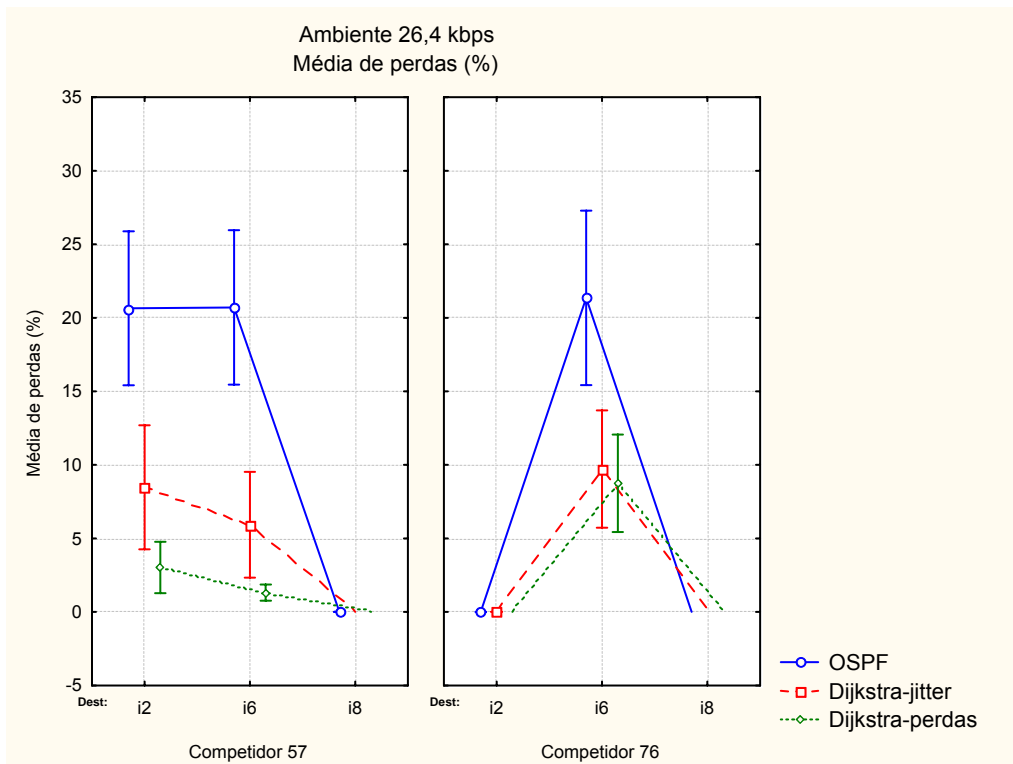


Figura 7-21 -Perdas em relação aos cenários, destinos e fluxos competidores

7.2.7. Árvore de eventos para perdas no ambiente 26,4 kbps

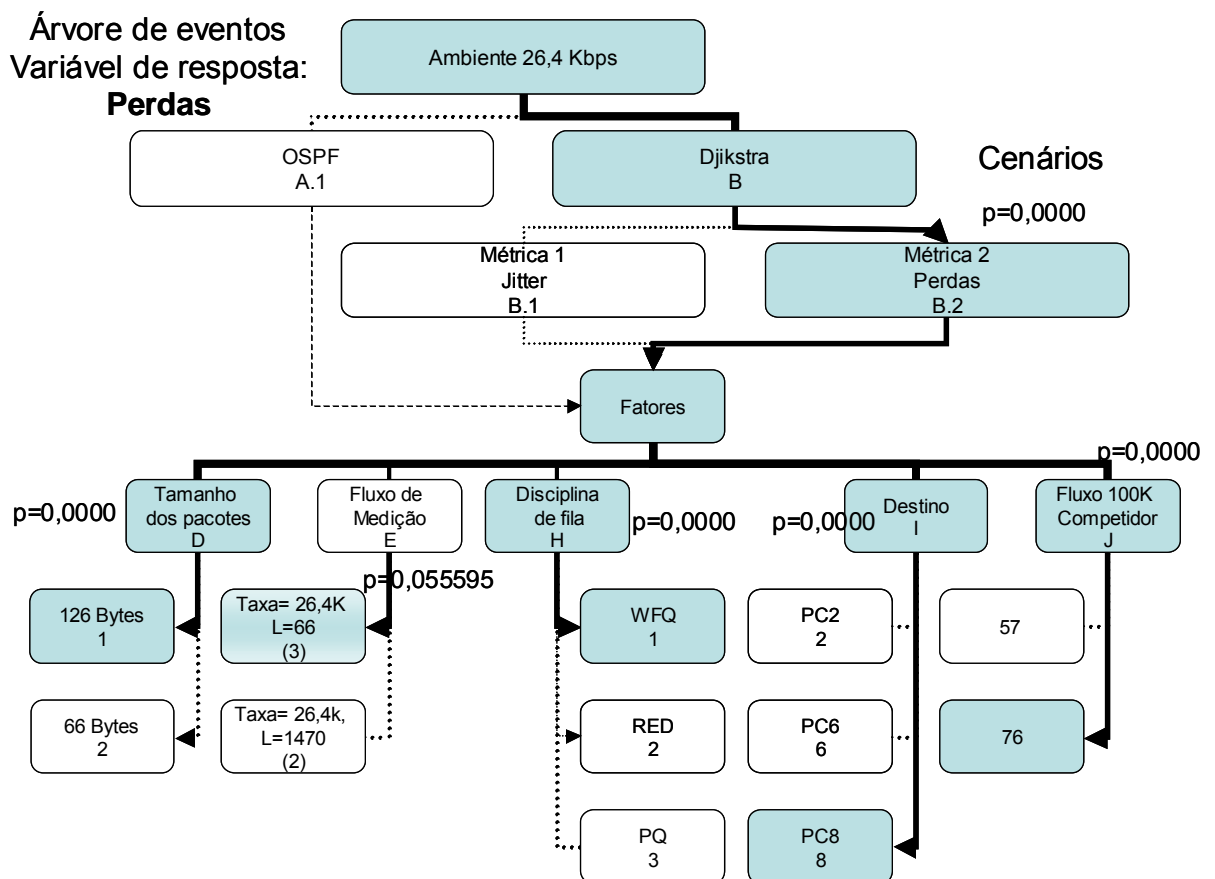


Figura 7-22 - árvore de eventos para PERDAS no ambiente 26,4 kbps

Na Figura 7-22 tem-se um resumo das condições para redução de perdas no ambiente 26,4 kbps.

Pode-se concluir que em relação aos 3 cenários houve diferença significativa entre as médias, demonstrando a eficiência do plano de controle na redução das perdas para este ambiente ($p=0,0000$). Este cenário, combinado com os níveis a seguir deve levar aos melhores desempenhos com relação as médias de perdas:

- Fluxos de medição com pacotes pequenos
- Filas com disciplinas WFQ
- Destinos sem competidores, tanto para interface quanto pelos enlaces

7.3. Ambiente 1 pps - Jitter médio

Pela análise da Tabela 7-17 e da Figura 7-23 pode-se constatar que os cenários (protocolos) foram efetivos na formação das médias, sendo inclusive o fator mais influente ($F=109,334$ e $p=0,0000$).

| | df | F | p |
|---------------------------|----|----------|----------|
| Cenários | 2 | 109,3340 | 0,000000 |
| Tam pacote voz | 1 | 95,3561 | 0,000000 |
| fluxo medicao | 1 | 20,3372 | 0,000008 |
| Disciplina de fila | 2 | 15,1072 | 0,000000 |
| Destino | 2 | 101,0289 | 0,000000 |
| fluxo competidor | 1 | 7,7507 | 0,005577 |

Tabela 7-17 - Efeitos dos fatores no Jitter médio - Ambiente 1 pps

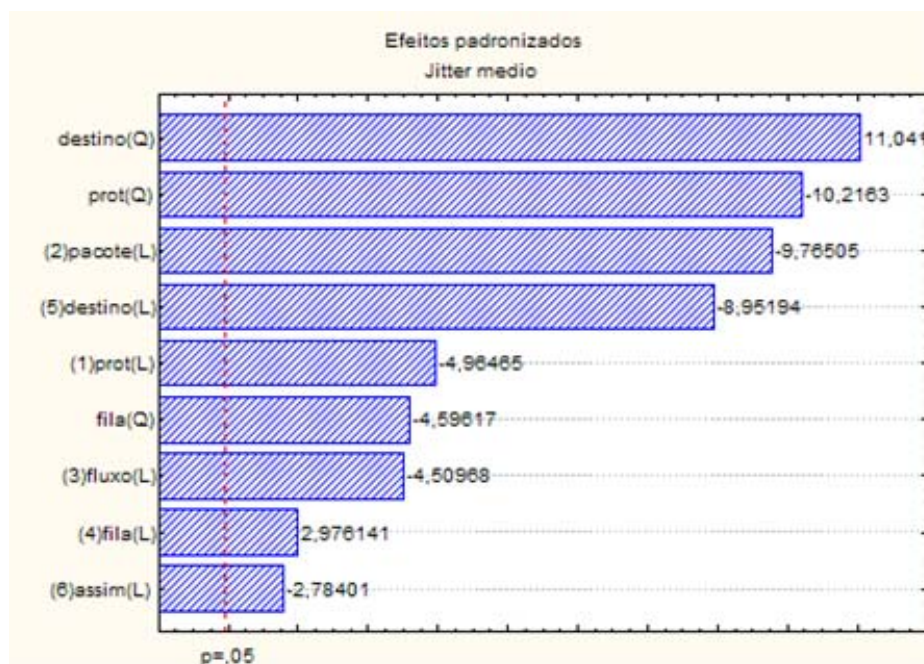


Figura 7-23 -Efeito dos fatores sobre o Jitter médio - Ambiente 1 pps

Percebe-se ainda que todos os fatores têm influência significativa no *jitter*.

7.3.1. Jitter em relação aos cenários

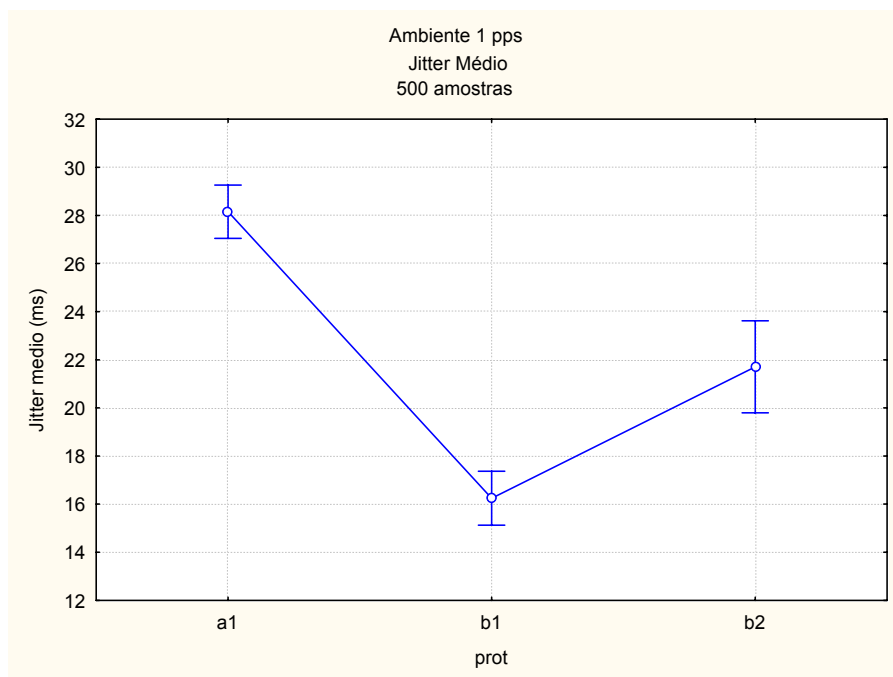


Figura 7-24 - Jitter médio em relação aos protocolos - a1=OSPF - b1 =Dijkstra com limiar para Jitter – b2=Dijkstra com limiar para perdas

Pela Figura 7-24 pode-se constatar a grande diferença entre as médias para o cenário a1-OSPF. Observando-se os valores da Tabela 7-18, percebem-se os valores que comprovam a eficácia do plano de controle na redução do *jitter* para os limiares pretendidos (27 ms) neste ambiente. As médias ficaram em 16,25 quando o plano de controle encontrou os caminhos melhores até o destino, tendo sido acionado pela métrica *jitter*. Em relação ao ambiente 26,4 kbps, este resultado pode estar demonstrando que existem condições ideais para o funcionamento dos probs de medição, uma vez que naquele ambiente foi registrada apenas uma “tendência” na redução das médias, não comprovada para o nível de 95% de intervalo de confiança.

Percebe-se que o plano de controle diminui o *jitter* também quando é acionado para reduzir as perdas (cenário b2), obtendo uma média de 21,709 ms contra 28,159 ms para o OSPF.

| Jitter (ms) | Cenário | | |
|---------------|-----------|----------------------|----------------------|
| | OSPF (a1) | Dijkstra/jitter (b1) | Dijkstra/perdas (b2) |
| Media | 28,15888 | 16,24604 | 21,70910 |
| Desvio Padrão | 11,77977 | 8,60445 | 13,05865 |
| N | 215 | 213 | 72 |

Tabela 7-18 - Jitter médio para os cenários a1, b1 e b2

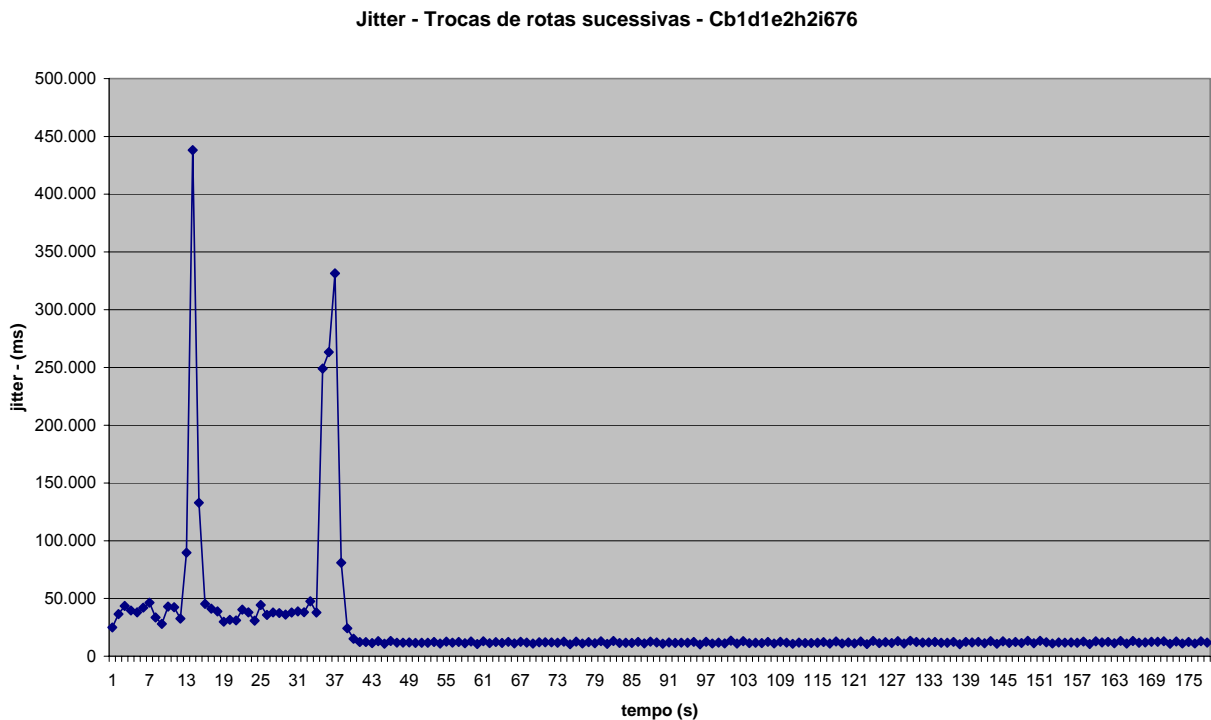


Figura 7-25 - trocas sucessivas de rotas

Na Figura 7-25 está plotado o comportamento de uma amostragem deste ambiente, para o cenário b1 (Dijkstra com métrica no *jitter*), pacotes do fluxo de voz de 126 bytes, pacotes dos fluxos de medição de 66 bytes, tratamento de filas RED e destino para PC 6, tendo como fluxo competidor j76 (origem no PC 7 e destino no PC 6).

Pelo gráfico percebem-se claramente as duas situações de troca de rota executadas pelo plano de controle, demarcadas pelos picos nos valores do *jitter*. Essas trocas sucessivas comprovam a característica dinâmica do plano de controle. Ao mesmo tempo, deve-se observar que os valores elevados do *jitter* devem alterar a média para maior, mesmo que o resultado final tenha sido satisfatório também em termos estatísticos.

As influências dos demais fatores estão demonstradas no Apêndice I, uma vez que já foram discutidas para o ambiente de 26,4 kbps.

7.3.2. Árvore de eventos para o *jitter* médio no ambiente 1 pps

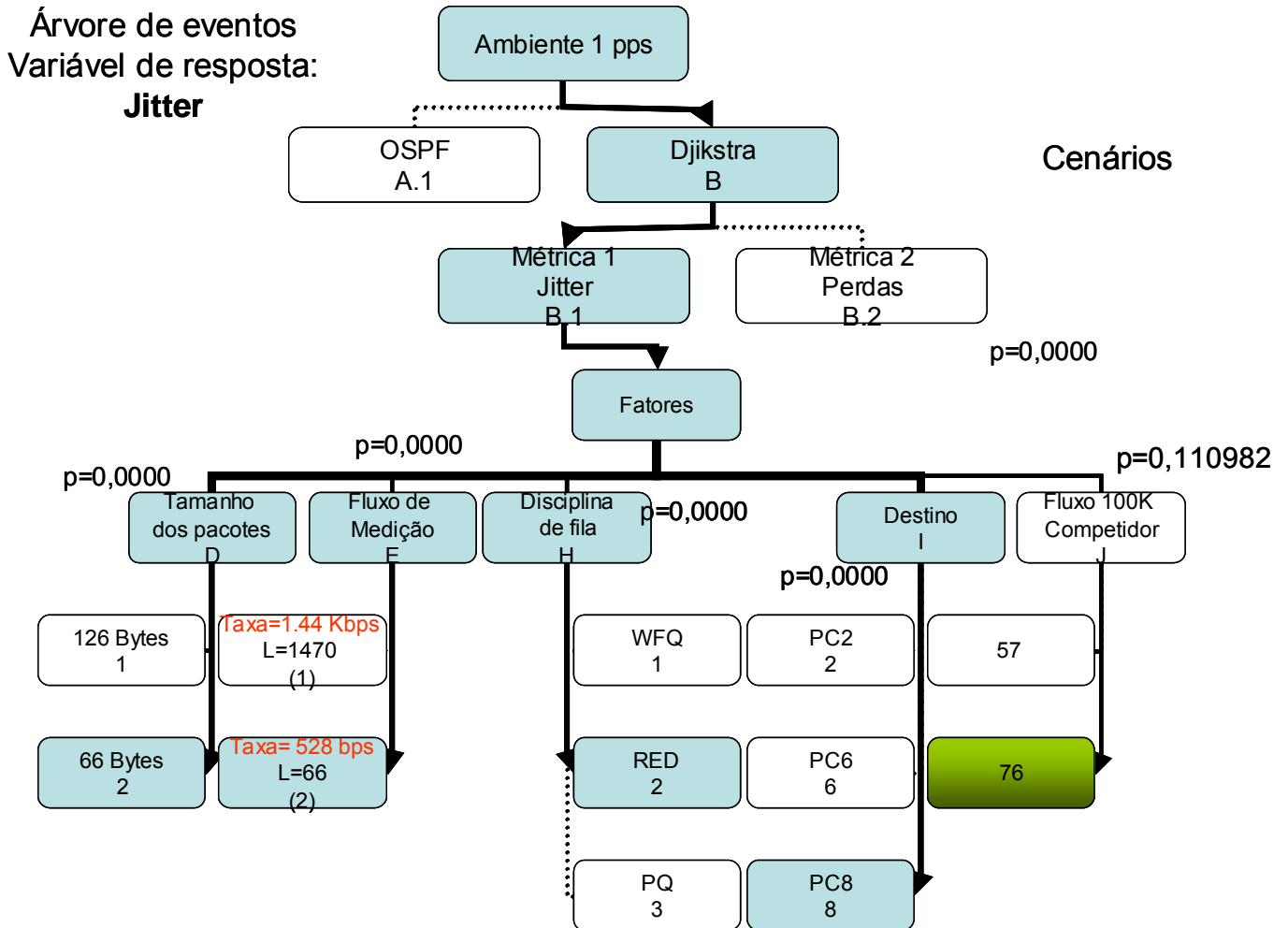


Figura 7-26 - Arvore de eventos para variável jitter - ambiente 1 pps

Acompanhando-se os valores de p para a variável *jitter* no ambiente de 1 pps, pode-se concluir que as melhores médias são obtidas nas seguintes condições:

O melhor cenário é o B1, com uma média de 16,246 ms e valor de $p=0,0000$. Este cenário, combinado com os níveis a seguir deve levar aos melhores desempenhos com relação as médias para o *jitter*.

- Fluxos de voz constituídos por pacotes de 66 bytes;
- Fluxos de medição com pacotes de 66 bytes;

- os roteadores com uma disciplina de filas RED;
- um destino com poucos saltos e caminhos não utilizados normalmente pelos fluxos competidores.

Estes eventos estão em concordância com a “equação do *jitter*” e são semelhantes aos obtidos no ambiente de 26,4 kbps.

7.4. Ambiente 1 pps - média de perdas Perdas

Neste ambiente, como no ambiente de 26,4 kbps, todos os fatores foram influentes nas variações da médias de perdas, considerando-se um nível de significância de 5%.

| | df | F | p |
|---------------------------|-----------|----------|----------|
| Cenário | 2 | 107,7902 | 0,000000 |
| Tam pacote de voz | 1 | 46,4595 | 0,000000 |
| Fluxo de medição | 1 | 7,2429 | 0,007362 |
| Disciplina de fila | 2 | 93,5611 | 0,000000 |
| Destino | 2 | 13,8473 | 0,000001 |
| fluxo competidor | 1 | 23,9416 | 0,000001 |

Tabela 7-19 - Efeitos dos fatores nas médias de perdas - Ambiente 1 pps

7.4.1. Perdas em relação aos cenários

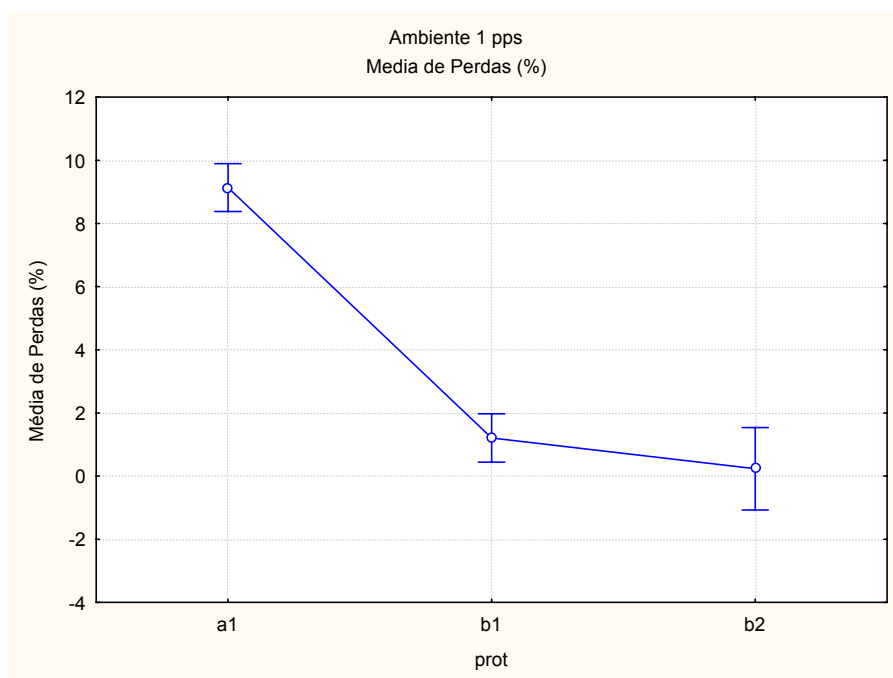


Figura 7-27 - Média de perdas em relação aos cenários

| Perdas (%) | Cenário | | |
|---------------|-----------|----------------------|----------------------|
| | OSPF (a1) | Dijkstra/jitter (b1) | Dijkstra/perdas (b2) |
| Média | 9,137484 | 1,206029 | 0,231231 |
| Desvio Padrão | 10,33707 | 2,99226 | 1,56314 |
| N | 215 | 213 | 72 |

Tabela 7-20 – Média de perdas em relação aos cenários

Pela análise da Tabela 7-17 e da Figura 7-27 pode-se constatar que os cenários (protocolos) foram efetivos na formação das médias de perdas ($p=0,0000$). Percebe-se que o plano de controle conseguiu reduzir as perdas (tendo como base o desempenho do cenário OSPF) mesmo quando acionado para reduzir o *jitter* (cenário b1). Como não existem amostras nas condições de filas RED e PQ para o cenário b2, não se pode concluir que o plano de controle foi efetivo no valor das perdas para este ambiente. Devido a essa diferença no número de amostras do cenário b2, optou-se por não elaborar a árvore de eventos para essa variável no ambiente 1 pps.

As influências dos demais fatores estão demonstradas no Apêndice I, uma vez que já foram discutidas para o ambiente de 26,4 kbps.

7.5. Árvore de eventos para o Jitter média de perdas nos dois ambientes

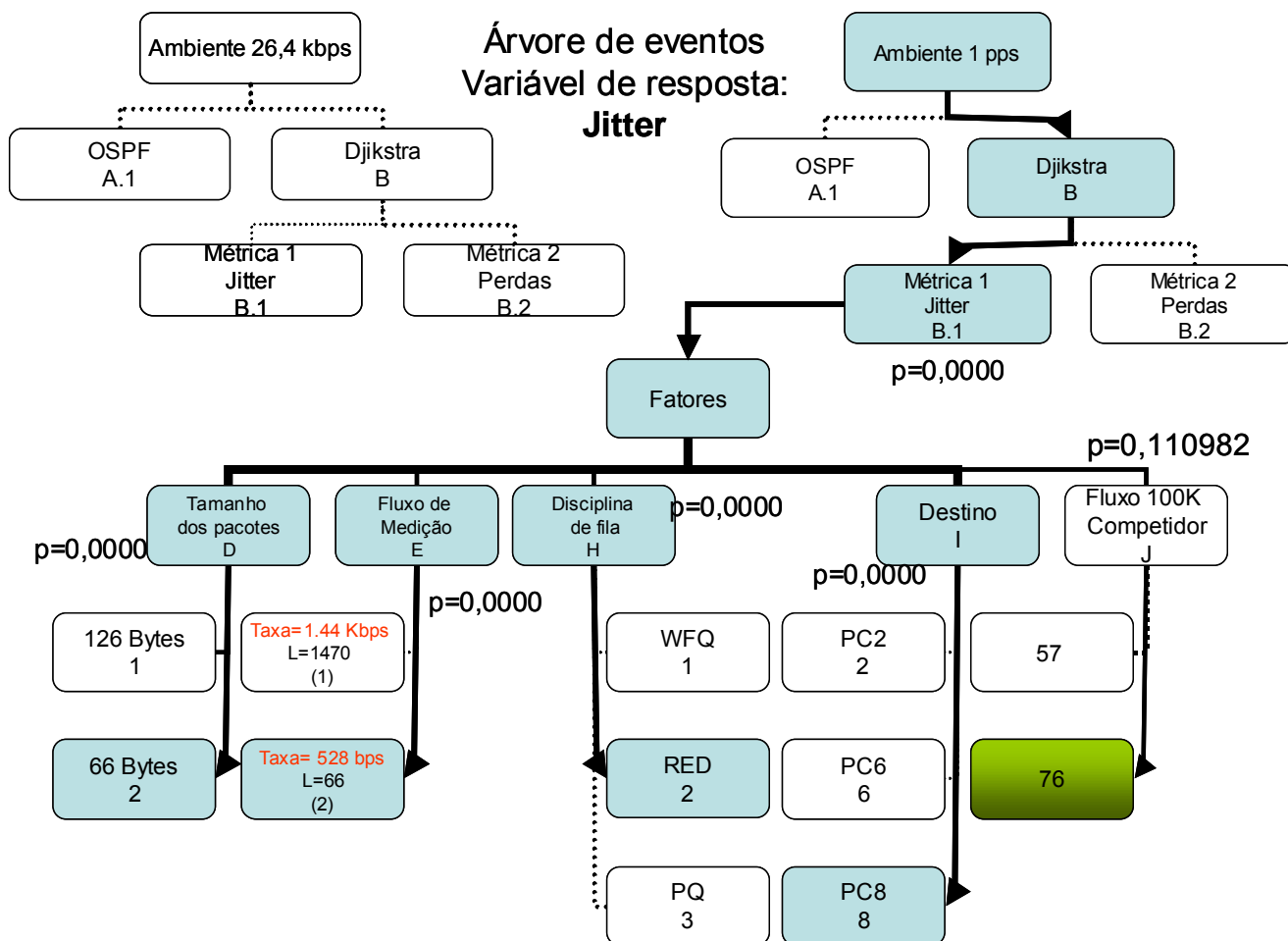


Figura 7-28 - Árvore de eventos - Jitter para os dois ambientes

A redução das médias de *jitter* foi mais eficiente no ambiente 1 pps, usando-se como cenário o plano de controle com métrica *jitter*. No ambiente de 26,4 kbps essa condição de melhoria foi mostrada como uma tendência apenas. Considerando-se que as médias mesmo assim ficaram abaixo do limiar estabelecido, pode-se afirmar que o plano de controle reduz eficientemente as médias do *jitter* ao escolher os melhores caminhos com base nos valores dos enlaces.

7.6. Árvore de eventos para as médias de perdas nos dois ambientes

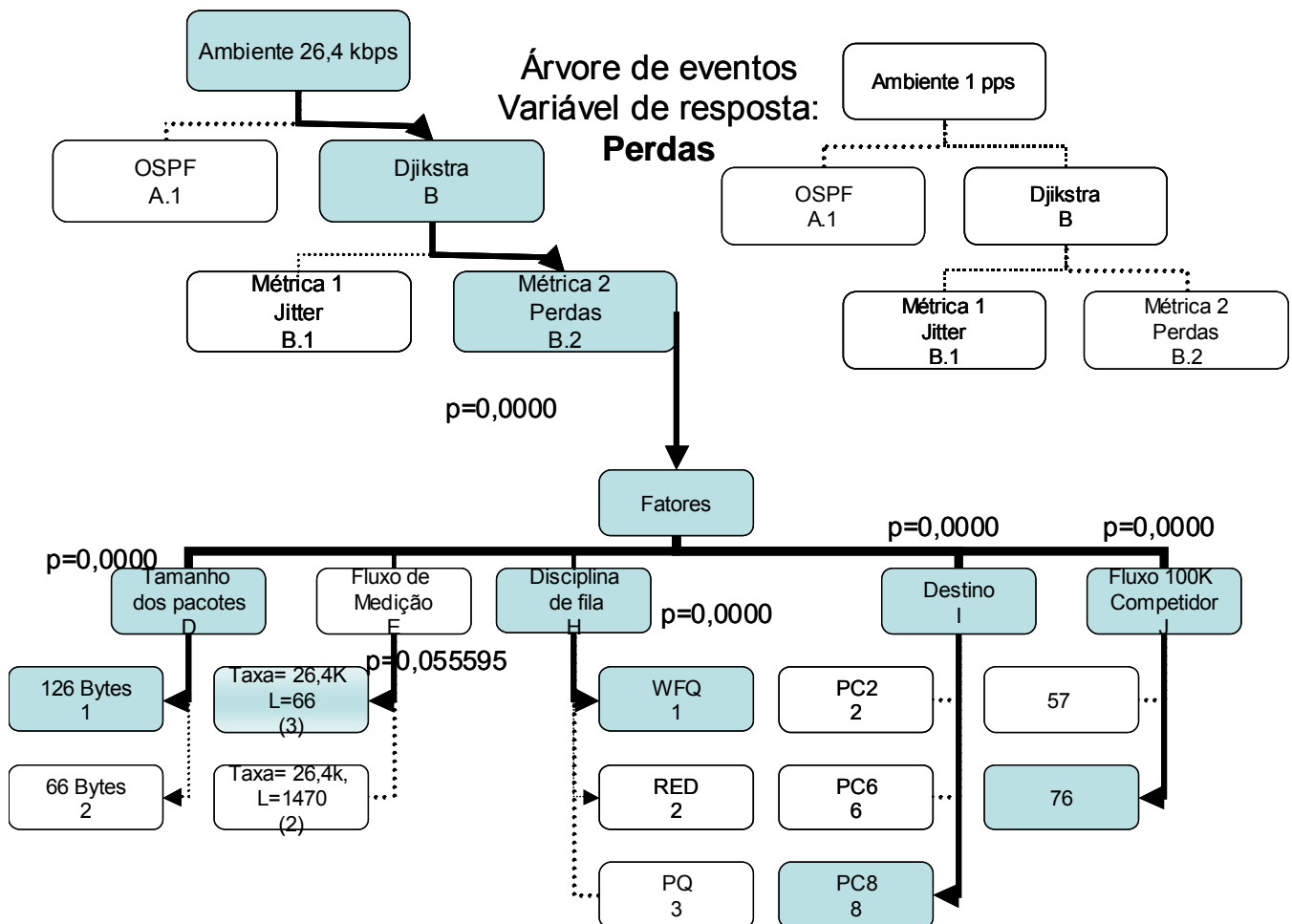


Figura 7-29 - Árvore de eventos - Perdas para os dois ambientes

O ambiente de 26,4 kbps se mostrou mais favorável para a redução das perdas, embora a comparação não possa ser considerada completamente, em virtude da falta de amostras para o cenário b2 no ambiente 1 pps. O plano de controle foi eficiente na redução das médias de perdas, quando usou-se essa métrica para disparar o gatilho de escolha de caminhos melhores.

7.7. Conclusões do capítulo

Este capítulo mostrou a análise dos dados obtidos com os experimentos projetados para amostragem do ambiente de estudos. Os experimentos foram divididos em dois blocos, ou ambientes, uma vez que no primeiro experimento a influência do plano de controle na redução do *jitter* não ficou bem determinada.

Após a análise das 1144 amostras de 180 segundos, dentro dos dois ambientes estudados, pode-se afirmar que:

- O plano de controle é eficiente para redução do *jitter*, especialmente quando os *probs* de medição utilizam poucos recursos da rede. Este foi o caso do cenário 1 pps, onde o plano de controle reduziu o *jitter* de uma média de 28,159 ms com o OSPF para uma média de 16,246 ms com o plano de controle com a métrica *jitter*. Além de estar bem abaixo do limiar de 27 ms, esta média representa uma redução de 42% na média do *jitter* (Figura 7-24 e Tabela 7-18).
- Para a variável *jitter*, a utilização de pacotes pequenos (menores que 100 bytes) nos fluxos de medição é recomendada, a uma taxa de 1 pacote por segundo, a exemplo das implementações do utilitário *ping*. Quando os pacotes menores foram utilizados (66 bytes, 20,51 ms), os valores do *jitter* médio baixaram aproximadamente 14%, em relação aos pacotes de 1470 bytes (23,75 ms).
- Pacotes menores nos fluxos de voz, em conformidade com a equação do *jitter*, sofrem menos *jitter*. Os pacotes de 66 bytes tiveram média de 18,55 ms, 28% menor que os pacotes de 126 bytes (25,72 ms) no ambiente de 1 pps.
- Pacotes menores nos fluxos de voz representam mais perdas em situações de degradação dos enlaces. No ambiente 26,4 kbps, os pacotes de 66 bytes tiveram média de perdas de 6,4%, contra 4,7% dos pacotes de 126 bytes. Isso representa um aumento de 36%.
- O uso de mais recursos da rede pelos *probs* de medição acarreta em alterações nas medidas de *jitter*, mascarando os resultados das análises.
- O plano de controle é eficiente para encontrar melhores caminhos quando usa a métrica de perdas percentuais. No ambiente de 26,4 kbps, as perdas passaram de 10,45 % sem a ação do plano de controle para 2,16%, representando uma redução de 79%.
- O plano de controle mostrou-se dinâmico o suficiente para alterar os caminhos de formas sucessivas, até a situação de estabilidade.

- O plano de controle reduz a média de *jitter* mesmo quando a métrica usada para disparar o gatilho é o percentual de perdas. No ambiente de 1 pps, essa redução foi de 23%, passando de uma média de 28,16 ms para 21,71 ms.
- O plano de controle reduz o percentual de perdas mesmo quando a métrica utilizada para disparar o gatilho é o *jitter*. No ambiente de 26,4 kbps, essa redução foi de 62%, passando de uma média de 10,45% com o OSPF para 4,02% quando o plano de controle baseou-se no *jitter* para encontrar um caminho melhor.
- A disciplina de filas WFQ é a que mostrou-se mais eficiente para o controle de perdas nos ambientes estudados. No ambiente de 26,4 kbps, essa disciplina apresentou perdas de 0,03%, contra mais de 8% nas demais disciplinas (RED e PQ).
- A política de controle de congestionamento RED mostrou-se mais eficiente que WFQ e PQ para as médias de *jitter* nos ambientes estudados. No ambiente 1 pps, esta disciplina obteve médias de 19,64 ms, ficando 11% abaixo das médias da disciplina WFQ (21,89 ms) e 21,4% abaixo da disciplina PQ (24,98 ms).
- As amostras devem ser maiores que os 180 segundos utilizados, pois em algumas situações o plano de controle efetua mais de uma troca de rotas até encontrar um caminho que suporte o fluxo de voz e continue com as métricas abaixo dos limiares estabelecidos.
- Existe uma degradação momentânea das métricas no momento das trocas de rotas. Obviamente, estes valores influenciam nas médias.
- A quantidade de interfaces (*hop count*) no percurso afeta a média do *jitter* e de perdas, em uma relação inversa.

7.8. Evidências das limitações dos experimentos

Uma análise das variações das medições -Figura 7-30 – demonstra que alguns casos, embora possam ter sido resolvidos pelo plano de controle, tiveram suas médias de *jitter* bastante elevadas. Uma média elevada pode significar que o tempo de amostragem não foi representativo da situação obtida com os novos caminhos, como demonstram os gráficos da Figura 7-13 e Figura 7-25.

As médias podem ser elevadas também devido aos picos dos valores sempre que os caminhos são alterados. Estes casos devem ser investigados com maior atenção.

Durante as amostragens se observou ainda que o tempo entre o início de cada acesso ao roteador e a saída (logout) foi computado em 1250 ms. Este tempo poderia ser melhorado usando-se outro protocolo, como o SNMP, ao invés do Telnet.

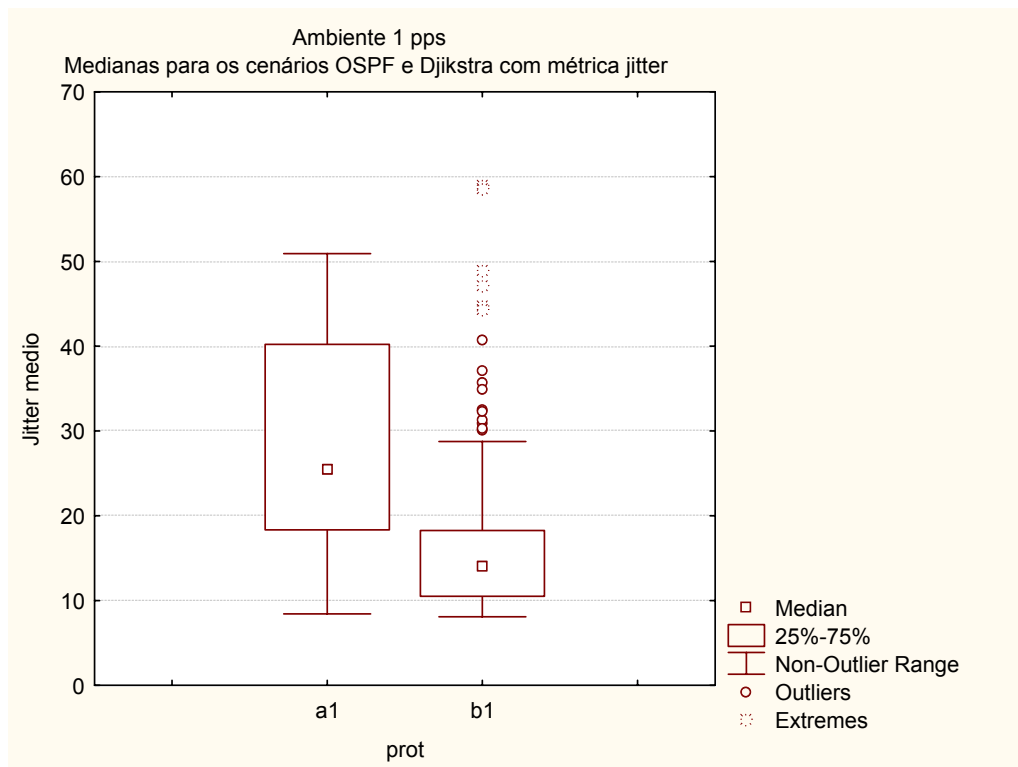


Figura 7-30 - Medianas para o jitter em relação aos cenários a1-OSPF e b1-Dijkstra com métrica jitter

8. Conclusões

Existe uma infinidade de iniciativas dos pesquisadores na direção da preservação das métricas de desempenho das redes IP para garantir qualidade nos serviços. Este fato ficou mais evidente após a convergência dos tráfegos elásticos e inelásticos para um rede única. O problema maior parece ser o de adaptar as redes baseadas no IP ao novo paradigma de transportar tráfegos inelásticos em conjunto com os dados tradicionais, notadamente HTTP, SMTP, FTP.

Embora esta evidência aponte para um fato irreversível, até o momento nenhuma iniciativa parece satisfazer a todos os requisitos dos tráfegos exigentes de recursos, como voz e vídeo, ao mesmo tempo que mantém com eficácia as condições para os tráfegos de menor exigência.

Com base nessa discussão, pode-se concluir que não existe uma proposta abrangente para contemplar todas as necessidades das demandas cada vez mais diversificadas na Internet.

São muitos os problemas que precisam ser resolvidos ou otimizados: Garantir recursos para os tráfegos sensíveis, e não exaurir os recursos disponíveis para os tráfegos de dados. Reduzir os consumos de banda, através de codificações eficientes. A determinação das métricas de qualidade de serviço, e as maneiras de executar as medições.

Os próprios órgãos de padronização (ITU-T, ETSI, IETF) possuem soluções nem sempre convergentes, o que contribui para uma carência de soluções unificadas, ou pelo menos homogêneas.

Três grandes vertentes podem ser destacadas como modelos de manutenção da QoS, cada qual com muitas variantes de implementação:

- A reserva antecipada de recursos da rede;
- A marcação e classificação dos pacotes;
- O re-roteamento como técnica de engenharia de tráfego.

As definições de serviços e as necessidades de cada tipo de tráfego também possuem divergências. Sabe-se que para as aplicações de voz as perdas devem ser inferiores a 1% com o CODEC G.729, mas não está documentado o percentual aceitável para os demais tipos de CODEC.

Uma abordagem de manutenção de QoS passa pela análise da disciplina de fila utilizada pelo roteadores e comutadores. São várias as disciplinas de filas, e o tratamento utilizado para o descarte dos pacotes excedentes também é variado. Muitas implementações são dependentes de fabricantes, inclusive para as definições das filas utilizadas como padrão para determinadas interfaces.

Dentre as soluções propostas para a manutenção das métricas estão as técnicas de roteamento baseadas em QoS. Também nessa área não existe consenso sobre o tratamento dos principais problemas (quando se devem anunciar as novas rotas, quais as métricas que devem ser utilizadas, qual o melhor algoritmo). Não existe conclusão sobre as formas de manter as tabelas de rotas (centralizadas em um servidor, ou distribuídas?). Deve-se pré-computar os caminhos, mantendo em cache ou esse cálculo deve ser dinâmico?

Sabe-se também que a utilização de duas ou mais métricas independentes para o cálculo de um caminho é um problema que demanda tempos exponenciais, mas são poucos os estudos em relação ao uso de aproximações ou heurísticas para se encontrar caminhos próximos do melhor caminho. Este trabalho comprovou que usando-se uma métrica (*jitter* ou perdas) pode-se melhorar os caminhos sem que os valores das métricas sejam realmente restritivos, mas sirvam como base para o disparo do gatilho de mudança, que deve ser disparado sempre que este limiar seja ultrapassado.

Neste trabalho de pesquisa foi apresentada uma proposta para manter os fluxos de voz dentro de limiares de qualidade pré estabelecidos, escolhendo dinamicamente melhores caminhos sempre que as rotas convencionais se degradarem.

Tal proposta fundamenta-se na monitoração do fluxos de voz e dos enlaces em relação a uma métrica. As métricas escolhidas para manutenção da qualidade dos fluxos de voz foram perdas de pacotes (RFC 2680) e variação do atraso (RFC 3393). A proposta inclui uma estação servidora de QoS (QNS), que recebe os valores das medições e calcula os melhores caminhos com base no algoritmo de Dijkstra. Uma métrica somente é utilizada para estabelecer os novos caminhos, para se evitar a

complexidade do algoritmo de menor caminho baseado em restrições. Os caminhos são alterados através de scripts ExpectJ integrados ao protótipo QoS-Path, na QNS.

A proposta se mostrou eficiente para o controle das variáveis dentro dos ambientes estudados, considerando-se que *jitter* e perdas não devem restringir em conjunto a escolha do melhor caminho. Essa abordagem parte do princípio que os fluxos a preservar podem ter restrições de perda ou de *jitter*, contemplando uma delas apenas.

Foi criado um protótipo para a monitoração e reconfiguração da rede, que serviu de base para o QNS, servidor de QoS da rede. Esse protótipo mesclou a linguagem Java com scripts ExpectJ, e mostrou-se eficiente, embora a carência de uma interface amigável para a configuração.

Os resultados mostraram que a alteração das rotas com base em uma das métricas (principal) pode ser suficiente para melhorar o desempenho também com relação a outra métrica (secundária), embora os valores fiquem mais distantes dos limiares estabelecidos para a métrica secundária. Obviamente essa situação fica mais fácil de se estabelecer nos ambientes estudados, uma vez que eram poucos os fluxos competidores em relação às possibilidades de caminhos alternativos. Assim, era de se prever que, ao escolher um caminho com menor *jitter*, por exemplo, esse mesmo caminho apresentasse as melhores condições em relação às perdas, pois provavelmente teria mais banda disponível.

O comportamento da variável *Jitter* frente aos diversos fatores utilizados nos experimentos deste trabalho, seguiu o esperado quando se verifica a “equação do *jitter*” utilizada por alguns autores (Ma, Q. & Steenkiste, P., 1997): Aumenta com o tamanho dos pacotes, com o número de saltos e o tamanho dos buffers. Segundo a equação, o *jitter* deve diminuir com o aumento da taxa de transmissão das interfaces (considerando que essa variável possibilite banda disponível). Esse resultado também foi encontrado neste trabalho de pesquisa.

As disciplinas de filas tiveram uma influência no *jitter* semelhante aos resultados encontrados por (Ali, R. B.; Pierre, S. & Lemieux, Y., 2005): A disciplina WFQ é mais eficiente para o *jitter* que a disciplina PQ. Ao contrário deste trabalho de pesquisa, aqueles autores não utilizaram o tratamento RED, tendo preferido as filas do tipo FIFO como terceira técnica de enfileiramento.

Para a variável média de perdas, as disciplinas de filas não seguiram o comportamento esperado, uma vez que as filas PQ deveriam reduzir as taxas de perdas para os pacotes menores que 100 bytes. O desempenho melhor para as perdas foi obtido com a política WFQ. Este comportamento deve ser melhor analisado.

Os roteadores têm conseguido reduzir o tempo de ruptura na comunicação de vários segundos para menos de um segundo, o que ainda não é suficiente para os serviços emergentes na Internet, que necessitam de períodos com ordens de magnitude menores que isso. Um plano de controle dinâmico como o proposto neste trabalho poderá evitar as rupturas causadas pela degradação dos caminhos bem antes que elas aconteçam, bastando para isso determinar-se os limiares de tais métricas.

Analisando-se a ferramenta de medição, ficam claros alguns aspectos no uso desses recursos:

A atividade da ferramenta é responsável por uma parcela dos resultados, fato que pode não ser um problema, quando os probs forem calibrados com os critérios corretos, o que vai depender dos objetivos das medições e dos ambientes utilizados.

A variável perdas sofre influência menor que o *jitter* pelos probs de medição. Essa menor sensibilidade da variável pode representar um problema quando se quer detectar um nível muito baixo de perdas, por exemplo. O *jitter*, por sua vez, pode não responder muito bem quando a intensidade da variação for mais elevada.

É necessária uma investigação do comportamento das medições comparando-se com medições internas (buffers dos roteadores, protocolo SNMP para verificação de perdas), para poder-se analisar com mais segurança as condições de erro. Sabe-se, através do trabalho de Barford e Sommers que existem diferenças entre as medidas de perdas através de probs quando comparadas com os dados obtidos através das leituras das MIBs SNMP nos roteadores (Barford, P. & Sommers, J., 2004).

Existe uma indefinição na literatura sobre os limiares de *jitter* e perdas com os quais se deve trabalhar para considerar um caminho degradado ou não para fluxos de voz. Embora bem estabelecido para os atrasos, os padrões são vagos para *jitter* e perdas (alguns autores citam o site de um fabricante para recomendar taxas de perdas para determinado CODEC). Tal situação acaba deixando a solução dessa questão para ser resolvida pelas implementações nos sistemas finais. Assim, o usuário deverá ter o

poder de ajustar seus equipamentos de forma a aumentar ou diminuir os *buffers* de recepção até que a qualidade “percebida” esteja dentro de níveis aceitáveis.

As definições das métricas e formas de medição também não são homogêneas dentro dos padrões do IETF em relação a telefonia (ETSI-TIPHON, ITU-T, 3GPP).

8.1. Sugestões de continuidade

É de se esperar que ainda demore algum tempo até que seja especificado um padrão para manutenção dos tráfegos inelásticos dentro das métricas exigidas. Essa expectativa deve-se às inúmeras situações e variáveis que devem ser consideradas para uma solução genérica. Com este panorama estabelecido, pode-se progredir na proposta de uma estação QNS, elaborando-se políticas para as métricas e sistemas de distribuição dessas políticas, para solucionar outros problemas, como o tráfego de vídeo ou mesmo rajadas de dados por períodos prolongados.

Um plano de controle completo pode ser obtido através da integração com gerência SNMP, o protocolo de gerência de enlaces LMP (RFC 4204 - Lang, J. Ed., 2005) e controle de sinalização pelo RSVP.

A monitoração de outras métricas pode ser facilmente implementada (atrasos one-way e round-trip, banda utilizável).

A aplicação de medições passivas, através do SNMP pode auxiliar na utilização do plano de controle em ambientes reais, uma vez que os fluxos monitorados foram todos através de probs artificiais introduzidos na rede.

A análise dos cabeçalhos dos pacotes também pode ser implantada, e com isso a estação servidora de políticas poderia estabelecer restrições, ao estabelecer comunicação com um serviço de diretórios. A análise dos cabeçalhos pode auxiliar as políticas de filtros e detecção de comportamentos anômalos ou indesejados.

Testar a influência dos protocolos em separado (sinalização dos protocolos de roteamento, SIP, H.323).

Testar o desempenho do plano de controle em relação a convergência, na presença de quedas nos enlaces.

Comparar o desempenho do plano de controle com recursos clássicos de QoS, como RSVP e DiffServ.

Integração com mensagens de reserva do RSVP. O servidor de QoS poderá ser integrado ao protocolo RSVP, recebendo requisições de largura de banda, por exemplo.

Utilizar outros tipos de filas como parâmetros, com diferentes tamanhos de *buffers*, e acompanhar a situação dos pacotes nas interfaces dos roteadores.

Durante a calibração da ferramenta de medição, percebeu-se que a quantidade de fluxos nas interfaces utilizadas pode ser um fator de interferência nos valores. Essa possibilidade precisa ser investigada.

Usar calibração dos *buffers* das placas de redes das estações, e também nas interfaces dos roteadores.

No plano de controle proposto, a restrição do valor da métrica é utilizada somente para o disparo do gatilho de busca de um caminho melhor que o atual. Eventualmente, um enlace com valores maiores que as restrições podem ser utilizados, desde que componham o melhor caminho. Essa restrição também deve ser testada, forçando-se um caminho com a métrica sempre menor que o limiar pretendido.

Uma possibilidade de melhoria seria o cálculo do melhor caminho com base na métrica escolhida e com o menor número de saltos possível, o que também não está sendo utilizado no plano de controle atual.

A ferramenta de medição Iperf, por possuir código aberto e uma versão de interface escrita na linguagem Java, possibilita uma integração com o protótipo QoS-Path, proposto neste trabalho. Estas medidas devem ser implantadas na continuidade deste trabalho.

Uso do SNMP para verificação das rotas atuais e da alteração das rotas nos roteadores, uma vez que o ExpectJ acrescenta um retardo de 1250 ms entre o telnet e o logout da CLI do roteador. Pode-se esperar um desempenho melhor com o uso do SNMP, uma vez que este protocolo é baseado no UDP. As possíveis restrições ao uso do SNMP podem se dar em função da vulnerabilidade do protocolo nas primeiras versões, e a dificuldade de homogeneizar as variáveis, uma vez que encontrar as MIBs específicas dos fabricantes em ambientes heterogêneos pode não ser uma tarefa trivial.

Referências Bibliográficas

- Ali, R. B.; Pierre, S. & Lemieux, Y., 2005: UMTS-to-IP QoS Mapping for Voice and Video Telephony Services – IEEE Networks, Mar/Apr (2005)
- Ali, M.; Chirivalu, G. & Ge, A., 2005: Traffic Engineering in Metro Ethernet – IEEE Network, Mar/Apr 2005.
- Almes, G.; Kalidindi, S. & Zekauskas, 1999: A One-way Delay Metric for IPPM RFC 2679 – IETF – disponível em <http://www.ietf.org/rfc/rfc2679.txt>
- Almes, G.; Kalidindi, S. & Zekauskas, 1999: A one-way Packet Loss Metric for IPPM – RFC 2680 – IETF – disponível em <http://www.ietf.org/rfc/rfc2680.txt>
- Alwayn, V. , 2002: Advanced MPLS Design and Implementaion. Cisco Press, Indianapolis.
- Apostolopoulos, G. et al, 1999: QoS Routing Mechanisms and OSPF Extensions– IETF- RFC 2676 disponível em <http://www.ietf.org/rfc/rfc2676.txt>
- Apostolopoulos, G.; Guerin, R.; Kamat, S. & Tripathi, S., 1998: “Quality of service based routing: A performance perspective,” in Proc. ACM SIGCOMM , Vancouver, Canada, Sept. 1998, pp. 17–28.
- Armitage, G., 2000-a: MPLS: The Magic Behind the Myths - IEEE Communications Magazine • January 2000
- Armitage, G., 2000-b: Quality of Service in IP Networks: Foundations for a Multi-Service Internet - New Riders Publishing
- Armitage, G. J., 2003: Revisiting IP QoS: Why do we care, what have we learned? - ACM SIGCOMM 2003 RIPQOS Workshop Report
- Awduche, D.; Chiu, A.; Elwalid, A.; Widjaja, I.; Xiao, X., 2002: Overview and Principles of Internet Traffic Engineering - IETF - RFC 3272 disponível em <http://www.ietf.org/rfc/rfc3272.txt>
- Awduche, D.; Malcolm, J.; Agogbua, J.; O'Dell, M. & McManus, J., 1999: Requirements for Traffic Engineering Over MPLS, IETF- RFC 2702 - disponível em <http://www.ietf.org/rfc/rfc2702.txt>
- Banerjee, A.; Drake, J.; Lang, J.; Turner, B.; Awduche, D.; Berger, L.; Kompella, K. & Rekhter, Y., 2001: Generalized Multiprotocol Label Switching: An Overview of Signaling Enhancements and Recovery Techniques - IEEE Communications Magazine • July 2001
- Barford, P. & Sommers, J., 2004: Comparing Probe and Router-Based Packet-Loss Measurement - IEEE INTERNET COMPUTING- Sep-Oct 2004
- Blum, R., 2003: Network Performance Open Source Toolkit Using Netperf, Tcptrace, NIST Net, and SSFNet . Wiley Publishing, Inc., Indianapolis, Indiana
- Bolot, J., 1993: End-to-End Packet Delay and Loss Behavior in the Internet - Proc.ACM Special Interest Group on Data Communications (SIGCOMM '93), ACM Press
- Braden, R. et al., 1997: Resource ReSerVation Protocol (RSVP) —Version 1 Functional Specification, - IETF - RFC 2205 – disponível em <http://www.ietf.org/rfc/rfc2205.txt>
- Braden, R.; Clark, D. & Shenker, S., 1994: Integrated Services in the Internet Architecture: An Overview. IETF – Network Working Group – RFC 1633 - disponível em <http://www.ietf.org/rfc/rfc1633.txt>
- C. Fraleigh et al, 2003: Packet-Level Traffic Measurements from the Sprint IP Backbone - IEEE Network, vol. 17, no. 6,2003, pp. 6–16.
- Campbell, A. T., 1996: A Quality of Service Architecture. PhD thesis, Lancaster University, England.

- Caputo, R., 2000:** *Cisco™ Packetized voice and data integration* – Ed. McGraw-Hill
- Chan, K. et al, 2001:** *COPS Usage for Policy Provisioning (COPS-PR)*. RFC 3084
- Chen, S. & Nahrstedt, K., 1998:** *An Overview of Quality of Service Routing for Next-Generation High-Speed Networks: Problems and Solutions* - IEEE Network, pp. 64–79, Nov./Dec 1998
- Chen, X. et al, 2003:** *Survey on QoS Management of VoIP* - Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (ICCNMC'03)
- Choudhury, D., 2001:** *Unified IP Internetworking*. Springer-Verlag, New York
- Clark, D., 1995:** *Adding service discrimination to the Internet*. MIT Laboratory for Computer Science technical Report, sep 1995. Disponível em <http://ana-www.lcs.mit.edu/anaWeb/papers.html>
- Comer, D., 1998:** *Interligacao em Redes TCP/IP*. Vol. 1. 3a. Edicao. Editora Campus, Ltda.
- Cox, R. V., 1997:** *Three New Speech Coders from the ITU Cover a Range of Applications* - IEEE Communications Magazine, Sep - 1997.
- Crawley, E.; Nair, R.; Rajagopalan, B. & Sandick, H., 1998:** *A framework for QoS-based Routing in the Internet* – RFC 2386, IETF - <http://www.ietf.org/rfc/rfc3272.txt>
- Dijkstra, E. W., 1959:** *A Note on Two Problems in Connections with Graphs*. – Numer. Math. 1:269-271
- Dixit, S. (ed), 2003:** *IP over WDM: Building the Next-Generation Optical Internet*, John Wiley & Sons, Inc.
- Demichelis, C.; Chimento, P., 2002:** *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)* - RFC 3393 - IETF - <http://www.ietf.org/rfc/rfc3393.txt>
- Doyle, J., 1998:** *Routing TCP/IP – Vol I* – Ed. Macmillan Technical Publishing
- Dubrovsky, A.; Guerla, M.; Lee, S. S. & Cavendish, D., 2000:** *Internet QoS Routing with IP Telephony and TCP Traffic* – ICC 2000 - Disponível em citeseer.ist.psu.edu/dubrovsky00internet.html
- Duffield, N. G., 2004:** *Network Tomography From Measured End-to-End Delay Covariance* - IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 6,.
- Durham, D.; Boyle, J.; Cohen, R.; Herzog, S.; Rajan, R.; & Sastry, A., 2000:** *The COPS (Common Open Policy Service) Protocol*. RFC 2748, January 2000.
- Eder, M. & Nag, S., 2001:** *Service Management Architectures Issues and Review* – RFC 3052 -IETF - <http://www.ietf.org/rfc/rfc3052.txt>
- El-Sayed, M. & Jaffe, J., 2002:** *A View of Telecommunications Network Evolution* - IEEE Communications Magazine - Dec 2002.
- Ferguson, P. & Huston, G., 1998:** *Quality of Service – Delivering QoS on the Internet and in Corporate Networks*- John Wiley & Sons.
- Finenberg, V., 2002:** *A Practical Architecture for Implementing End-to-End QoS in an IP Network* - IEEE Communications Magazine • January 2002
- Flanagan, M. E. (ed), 2001:** *Administering Cisco QoS for IP Networks* – Syngress Publishing, Inc, Rockland, MA.
- Guérin, R., 2002:** *Computing Shortest Paths for any number of Hops*- IEEE/ACM Trans. Netwks– oct 2002
- Hall, E., 2000:** *Internet Core Protocols: The Definitive Guide* – Ed. O'Reilly.
- Hardy, W. C., 2001:** *QoS: Measurement and Evaluation of Telecommunications Quality of Service* - John Wiley & Sons, Ltd

- Hassan, M. & Jain, R., 2004:** *High Performance TCP/IP Networks – Concepts, Issues and Solutions* – Pearson Education, Inc.
- Hersent, O.; Gurle, D. & Petit, J. P., 2000:** *IP Telephony* – Ed Pearson Education Limited.
- Holland, G. :** *The Role of Signaling in MPLS* – Riverstone Networks White Paper
- Iovana, P.; Sabela, R. & Settembre, M., 2003:** *A traffic Engineering System form Multilayer Networks Based on the GMPLS paradigm.* – IEEE Network, march/april 2003
- ITU-T, 1999:** *Internet Protocol Data Communication Service: IP Packet Transfer and Availability Performance Parameters* - ITU-T recommendation I.380.
- Iwata, A. & Fujita, N., 2000:** *A Hierarchical Multilayer QoS routing system with dynamic SLA Management.* IEEE Journal on Selected Areas in Communications, Vol 18, No. 12.
- Jain, R., 1991:** *The Art of Computer Systems Performance Analysis.* - John Wiley and Sons, NY.
- Jajszczyk, A. & Rozycki, P., 2006:** *Recovery of the Control Plane after Failures in ASON/GMPLS Networks* - IEEE Network – Jan/Feb-2005
- Jamoussi, et al., 2002:** *Constraint-Based LSP Setup using LDP* - Internet RFC 3212 January 2002.
- Jha, S. & Hassan, M., 2003:** *Java implementation of policy-based bandwidth Management* - Int. J. Network Mgmt 2003; 13: 249–258 (DOI: 10.1002/nem.473)
- Jha, S.; Hassan, M., 2002:** *Engineering Internet QoS* – Ed. Artech House.
- Katz, D.; Kompella, K. & Yeung, D., 2003:** *Traffic Engineering (TE) Extensions to OSPF Version 2* – RFC 3630
- Kodialam, M. S.; Lakshman, T. V.; Sengupta S., 2000:** *Online multicast routing with bandwidth guarantees: a new approach using multicast network flow* - ACM SIGMETRICS Perf. Eval. Rev., Proc.2000 Int. Conf. Meas. Mod. Comp. Sys., Vol 28 - 1.
- Kosiur, D., 2001:** *Understanding Policy-Based Networking* - John Wiley & Sons, Inc.,
- Kowalik, K. & Collier, M., 2003:** *Should QoS routing algorithms prefer shortest paths?* Research Institute for Networks and Communications Engineering (RINCE) - Dublin City University, Ireland.
- Kuo, G. & Ko, P., 2003:** *Dynamic RSVP Protocol* - IEEE Communications Magazine • May 2003
- Kurose, J. F.; Ross, K. W., 2003:** *Computer Networking - A top-down aproach featuring the Internet* 3rd Ed. - Addison-Wesley Pub Co
- Lakshmi-Ratan, R., 1999:** *The Lucent Technologies Softswitch - Realizing the Promise of Convergence* - Bell Labs Tech. J., April–June 1999, pp. 174–195
- Lang, J. Ed., 2005:** *Link Management Protocol* – IETF – RFC 4204 – Disponível em <http://www.ietf.org/rfc/rfc4204.txt>
- Lemma, H. G., 2003:** *Enhanced Fast Rerouting Mechanisms for Protected Traffic in MPLS Networks* – Ph. D. Thesis – Universitat Politècnica de Catalunya-UPC – Dept Arquitectura de Computadores – TDX 0323104-125205
- Liu, H.; Pendarakis, D.; Komae, N. & Tellium, D. S., 2002:** *GMPLS-Based Control Plane for Optical Networks: Early Implementation Experience* -SPIE ITCOM 2002, Oceanport, NJ
- Ma, Q. & Steenkiste, P., 1997:** *On path selection for traffic with bandwidth quarantees* - In Proceedings of IEEE International Conference on Network Protocols, Atlanta, GA, October 1997. Disponível em citeseer.ist.psu.edu/ma97path.html

- Ma, Q. & Steenkiste, P., 1997:** *Routing Traffic with Quality of Service Guarantees in Integrated Services Networks* - Proc. IFIP International Workshop on Quality of Service, Columbia University, New York, May 1997, pp. 115–126.
- Ma, Q., 1998:** *Quality of Service Routing in Integrated Services Networks* – PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh – CMU-CS-98-138
- Marsh, M. G., 2002:** *Policy Routing Using Linux*. Ed. SAMS
- Menascé, D. A., 2003:** *Automatic QoS control*- IEEE Internet Computing – Jan – Feb 2003.
- Mieghem, P. V. & Kuipers, F. A., 2004:** *Concepts of Exact QoS Routing Algorithms* - IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 12, NO. 5, OCTOBER 2004 851
- Nagle, J., 1984:** *Ford Aerospace and Communications Corporation Congestion Control in IP/TCP Internetworks* - RFC 896 – IETF. Disponível em: <http://www.ietf.org/rfc/rfc896.txt>
- Nahrstedt, K.; Wichadakul, D. & Xu, D., 2000:** *Distributed QoS compilation and runtime instantiation*. In *Proceedings of the IEEE/IFIP International Workshop on QoS (IWQoS'2000)*, Pittsburgh, June 2000.
- Nelakuditi, S. Zhang, Z.; Tsang, R. P. & Du, D. H. C., 2002:** *Adaptive Proportional Routing: A Localized QoS Routing Approach* -IEEE/ACM Transactions On Networking, Vol. 10, No. 6, Dec 2002
- Nichols, K.; Blake, S. ; Baker, F. & Black, D., 1998:** *Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers*. IETF- RFC 2747 disponível em <http://www.ietf.org/rfc/rfc2747.txt>
- Nichols, K.; Jacobson, V. & Zhang, L., 1999:** *A two-bit differentiated services architecture for the Internet*. IETF-RFC 2638 disponível em <http://www.ietf.org/rfc/rfc2638.txt>
- Norden, S., 2002:** *Improving network performance using QoS routing and deferred reservations*. PhD thesis, dep of computer science, Washington University.
- Osborne, E. & Simha, A., 2003:** *Traffic Engineering with MPLS* – Ed Cisco Press.
- Park, K. I., 2005:** *QoS in Packet Networks* - Springer Science + Business Media, Inc.
- Pawlikowski, K., 1990:** *Steady state simulation of queueing processes: A survey of basic problems and solutions*. ACM Computing Surveys, June 1990, 22(2): 123-170
- Paxson, V. et. al, 1998:** *Framework for IP Desempenho Metrics* – RFC 2330 - <http://www.ietf.org/rfc/rfc2330.txt>
- Peterson, L. L. & Davie, B. S., 1999:** *Computer Networks: A Systems Approach* - 2nd ed - Morgan Kaufmann
- Peyravian, M. & Kshemkalyani, 1997:** *Network path caching: Issues, algorithms and a simulation study* – Computer Communications (vol 20).
- Raisanen, V., 2003:** *Implementing Service Quality in IP Networks* - John Wiley & Sons, Ltd.
- Raisanen, V. ; Grotefeld, G. & Morton, A., 2002:** *Network performance measurement with periodic streams* – RFC 3432 – IETF. Disponível em: <http://www.ietf.org/rfc/rfc3432.txt>
- Reisslein, M.; Ross, K. W. & Rajagopal, S., 2002:** *A Framework for Guaranteeing Statistical QoS*- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 10, NO. 1, FEBRUARY 2002
- Rosen, E.; Viswanathan, A. & Callon, R., 2001:** *Multiprotocol Label Switching Architecture* – IETF- RFC 3031 disponível em <http://www.ietf.org/rfc/rfc3031.txt>
- Roy, A., 2001:** *End-To-End Quality Of Service For High-End Applications* – Ph. D. Thesis - The University Of Chicago - The Faculty of the Division of the Physical Sciences

- Schulzrinne, H.; Casner, S.; Frederick, R. & Jacobson, V., 1996:** *RTP: A Transport Protocol for Real-Time Applications* – RFC 1889 – IETF. Disponível em: <http://www.ietf.org/rfc/rfc1889.txt>
- Sedgewick, R., 1983:** *Algorithms* – Ed. Addison-Wesley
- Shaikh, A.; Rexford, J. & Shin, K. G., 2001:** *Evaluating the impact of stalelink state on quality-of-service routing* - IEEE/ACM Transactions on Networking (TON), vol. 9, no. 2, pp. 162–176, 2001.
- Shand, M. & Bryant, S., 2006:** *IP Fast Reroute Framework* – IETF – draft-ietf-rtgwg-ipfrr-framework-05.txt
- Sharma, V. & Hellstrand, F., 2003:** *Framework for multi-protocol label switchinfg (MPLS)-based Recovery* - RFC 3469 – IETF. Disponível em: <http://www.ietf.org/rfc/rfc3469.txt>
- Shin, J.; Daniel C. Lee, D.C. & Kuo, C.C.J., 2003:** *Quality of service for internet multimedia* – Prentice Hall PTR
- Sprenkels, R.; Waaij, B.; Beijnum, B.; Pras, A., 1998:** *Management of Networks that Provides QoS Guarantees*. CTIT, University of Twente, the Netherlands. <http://www.snmip.cs.utwente.nl/nm/>
- Stallings, W., 2002:** *High Speed Networks and Internets*. 2nd ed., Prentice Hall, New Jersey
- Sun, W. & Shin, K. G., 2005:** *End-to-End Delay Bounds for Traffic Agregates Under Guaranteed-Rate Scheduling Algorithms* – IEEE/ACM Transactions on Networking – Vol 13 – No. 5
- Swallow, G., 1999:** *MPLS Advantages for Traffic Engineering* - IEEE Com Mag Dec 1999.
- Tanenbaum, A., 2003:** *Computer Networks* - Prentice Hall PTR - 4th. Ed.
- TIPHON, 2002:** *End-to-end Quality of Service in TIPHON systems; Part 5: Quality of Service (QoS) measurement methodologies* - Telecommunications and Internet Protocol Harmonization Over Networks - Release 3; ETSI TS 101 329-5 V1.1.2
- TIPHON, 2002-1:** *End-to-end Quality of Service in TIPHON systems; Part 3: Signalling and control of end-to-end Quality of Service (QoS)* Telecommunications and Internet Protocol Harmonization Over Networks - Release 3; ETSI TS 101 329-3 V2.1.2
- Tsuchiya, P. F., 1991:** *Efficient and Robust Policy Routing Using Multiple Hierarchical Addrestes* - ACM 0.89791 .44~-9/91
- Vegesna, S., 2001:** *IP Quality of Service* – Ed. Cisco Press, Indianapolis.
- Verma, D., 2000:** *Policy-Based Networking: Architecture and Algorithms* - New Riders Publishing
- Vogt, C., 2002:** *Admission Control and Resource Reservation on the Internet* - ACM SIGSOFT Software Engineering Notes vol 27 no 3 May 2002 Page 80
- Wang, J.; Nahrstedt, K. & Zhou, Y., 2000:** *Design and Implementation of DiffServ Routers in OPNET*, in Proc. of OPNETWORK'00, Washington D.C., August-September, 2000.
- Weiser, M., 2001:** *Whatever happened to the next-generation Internet?* – COMM. ACM – Sep. 2001/Vol. 44, No. 9
- Wisely, D.; Eardley, P. & Burness, L., 2002:** *IP for 3G: Networking Technologies for Mobile Communications* – Ed. John Wiley & Sons, Ltd.
- Xiao, X., 2000:** *Providing Quality Of Service In The Internet* – Ph. D. Dissertation - Michigan State University, Department of Computer Science and Engineering
- Xiao, X.; Ni, L., 1999:** *Internet QoS: A Big Picture* - IEEE Network Magazine, March/April, pp. 8-18.

- Yuan, X. & Zheng, W., 2004:** *A Comparative Study of Quality of Service Routing Schemes That Tolerate Imprecise State Information* - Florida State University Computer Science Department, Technical Report. Disponível na URL: <http://websrv.cs.fsu.edu/research/reports/TR-010704.pdf>
- Zhang, H., 1990:** *Service disciplines for guaranteed desempenho service in packet switching networks.* Proceedings of the IEEE, (10)83.

Apêndice 1

Resultados adicionais para o ambiente 1pps e fatores

a) – Análise da variável de resposta jitter médio

1. Jitter em relação ao tamanho do pacote do fluxo de voz

A Figura A1 - 1 e a Tabela A1 - 1 mostram as diferenças significativas (nível de 95%) das médias obtidas pelos fluxos de voz com pacotes de 126 bytes (25,716 ms). Para os pacotes de 66 bytes, essa média cai para 18,549 ms.

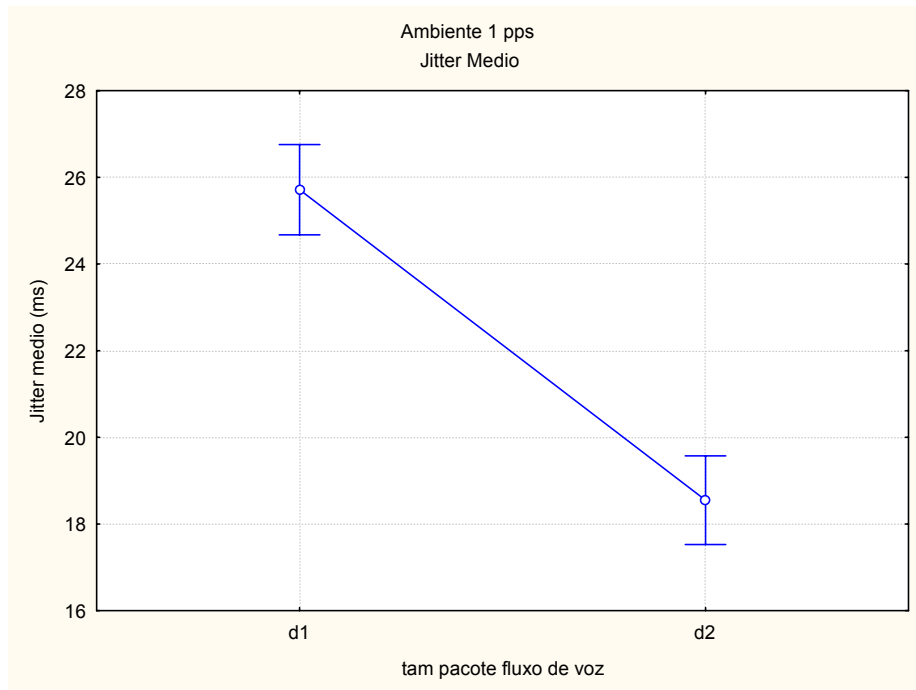


Figura A1 - 1 Jitter médio em relação ao tamanho dos pacotes dos fluxos de voz - d1=1470 bytes - d2=66 bytes

| <i>Jitter (ms)</i> | Tamanho do pacote do fluxo de voz | |
|----------------------|-----------------------------------|---------------|
| | 126 bytes (d1) | 66 bytes (d2) |
| Media | 25,71550 | 18,54846 |
| Desvio Padrão | 12,41038 | 10,60971 |
| N | 248 | 252 |

Tabela A1 - 1 Jitter médio em relação aos tamanhos dos pacotes dos fluxos de voz

2. Jitter em relação ao fluxo de medição

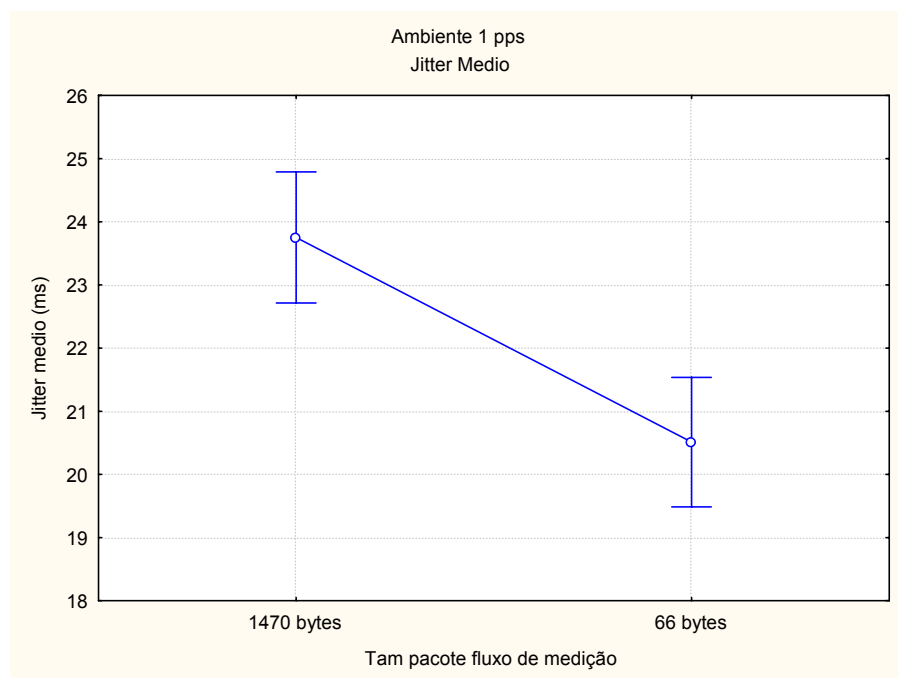


Figura A1 - 2-Jitter médio em relação aos fluxos de medição (1 pps)

| <i>Jitter (ms)</i> | Tamanho do pacote do fluxo de medição | |
|----------------------|---------------------------------------|---------------|
| | 1470 bytes (e1) | 66 bytes (e2) |
| Media | 23,75231 | 20,51166 |
| Desvio Padrão | 12,36146 | 11,55752 |
| N | 249 | 251 |

Tabela A1 - 2-Jitter médio em relação aos fluxos de medição

3. Jitter em relação a disciplina de filas

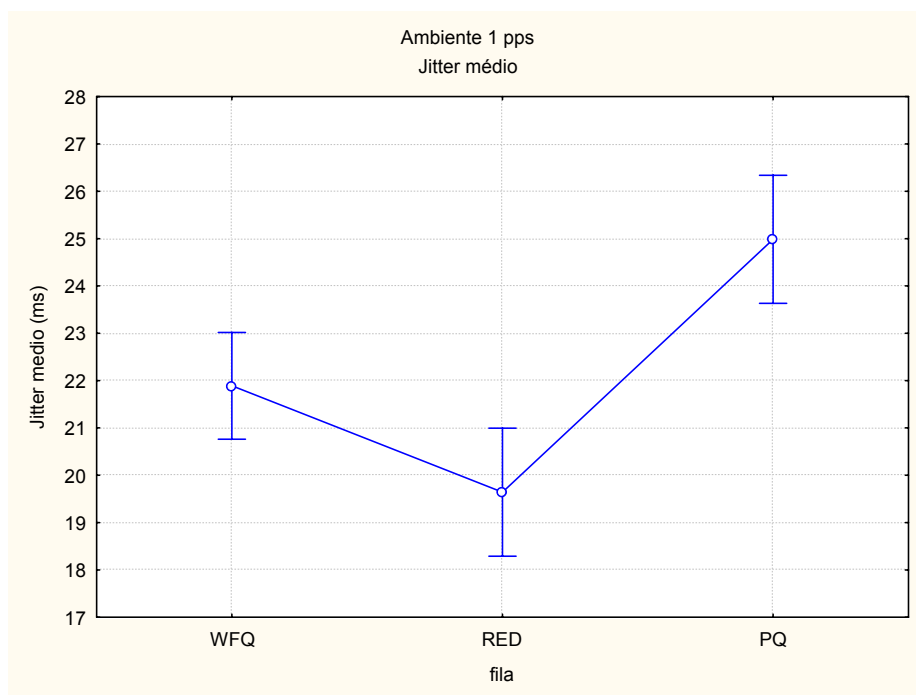


Figura A1 - 3-Jitter médio em relação às disciplinas de filas – ambiente 1 pps

| Jitter (ms) | Fila | | |
|---------------|----------|----------|------------------|
| | WFQ (h1) | RED (h2) | PQ (LT 100) (h3) |
| Media | 21,89026 | 19,64150 | 24,98505 |
| Desvio Padrão | 12,46790 | 8,90596 | 13,60586 |
| N | 212 | 144 | 144 |

Tabela A1 - 3-Jitter médio em relação às disciplinas de filas

1. Jitter em relação ao destino do fluxo de voz

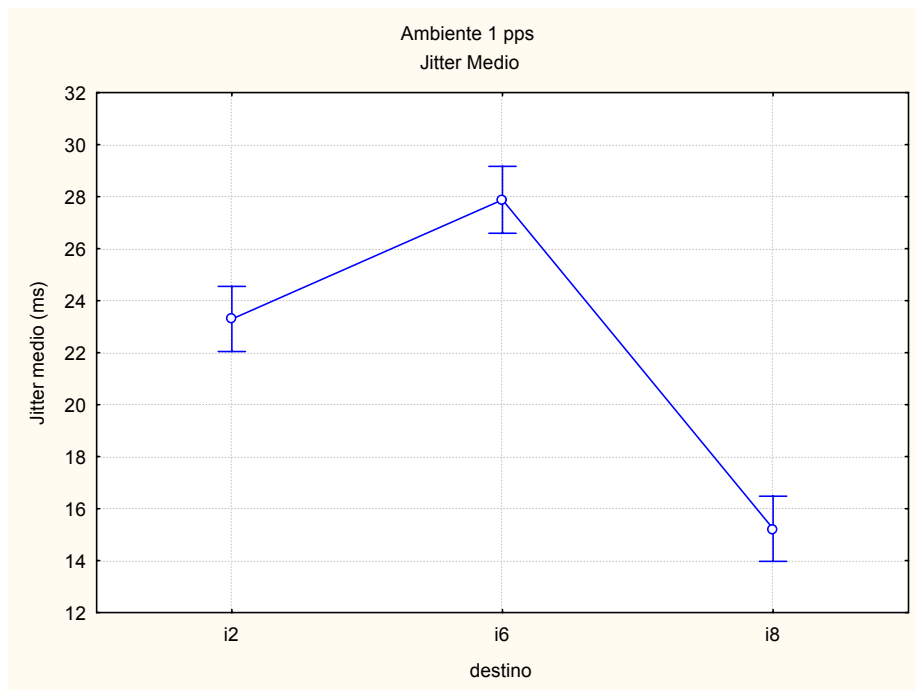


Figura A1 - 4-Jitter médio em relação ao destino dos fluxos de voz

| Jitter (ms) | destino | | |
|---------------|----------|----------|----------|
| | PC2 (i2) | PC6 (i6) | PC8 (i8) |
| Media | 23,29371 | 27,87661 | 15,22562 |
| Desvio Padrão | 11,59367 | 11,71645 | 9,20561 |
| N | 168 | 164 | 168 |

Tabela A1 - 4-Jitter médio em relação aos destinos dos fluxos de voz

2. Jitter em relação ao fluxo competidor

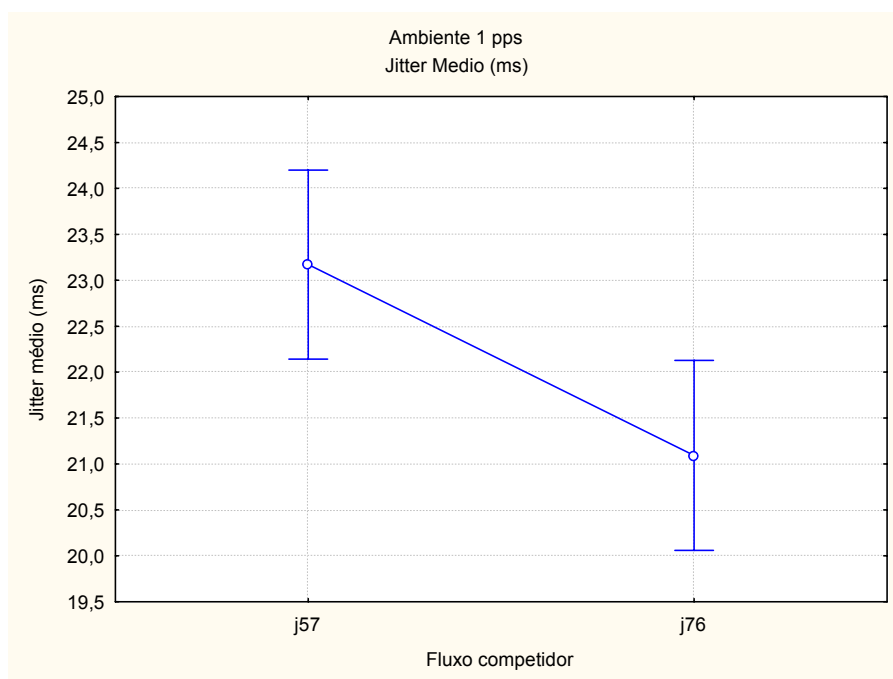


Figura A1 - 5-Jitter médio em relação aos fluxos competidores

| Jitter (ms) | Fluxo competidor | |
|---------------|------------------|----------|
| | J57 | J76 |
| Media | 23,17066 | 21,09331 |
| Desvio Padrão | 11,43692 | 12,61404 |
| N | 250 | 250 |

Tabela A1 - 5- Jitter medio em relação aos fluxos competidores

b- Análise da variável de resposta média de perdas

3. Média de Perdas em relação ao fluxo competidor

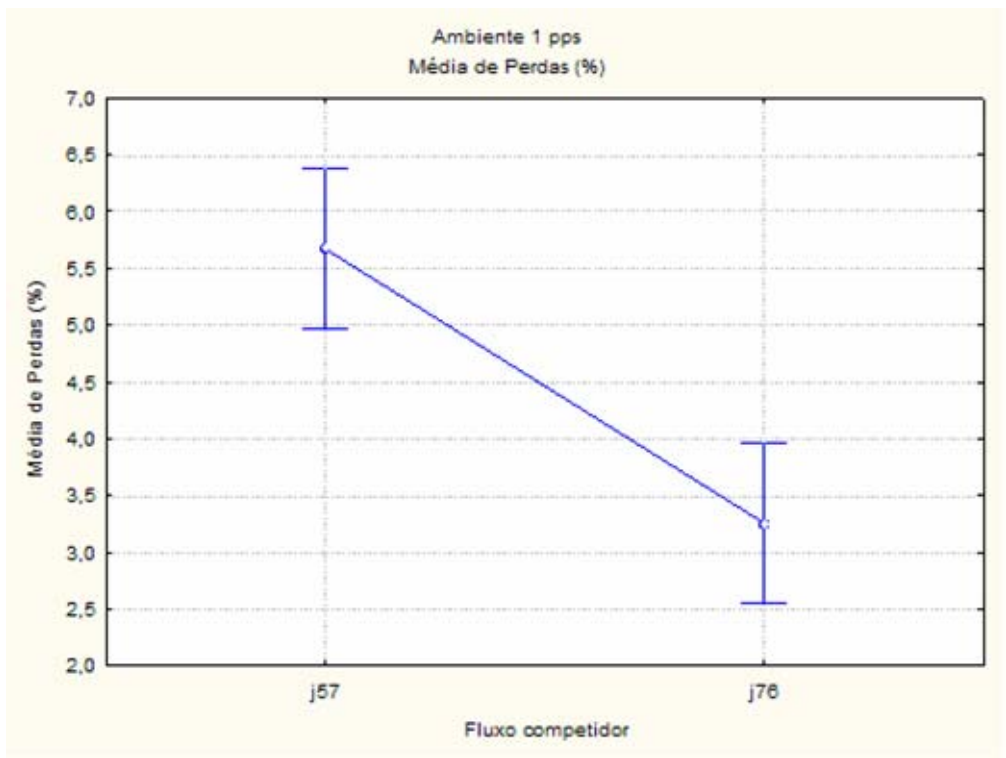


Figura A1 - 6- Média de perdas em relação ao fluxo competidor

| Perdas (%) | Fluxo competidor | |
|---------------|------------------|----------|
| | J57 | J76 |
| média | 5,676960 | 3,254974 |
| Desvio Padrão | 9,036760 | 6,991458 |
| N | 250 | 250 |

Tabela A1 - 6 – Média de perdas em relação aos fluxos competidores pelos recursos

4. Média de Perdas em relação ao tamanho dos pacotes do fluxo de voz

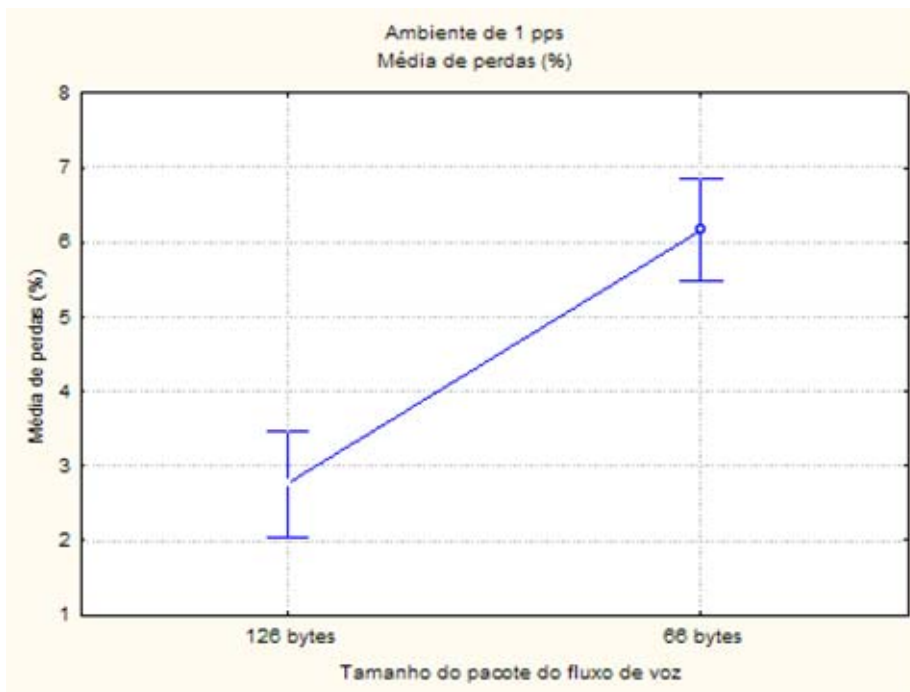


Figura A1 - 7- Média de perdas em relação ao tamanho dos pacotes do fluxo de voz

| Perdas (%) | Fluxo de voz | |
|---------------|----------------|---------------|
| | 126 bytes - d1 | 66 bytes - d2 |
| média | 2,763244 | 6,168690 |
| Desvio Padrão | 5,20869 | 10,00719 |
| N | 248 | 252 |

Tabela A1 - 7- Média de perdas em relação aos tamanhos dos pacotes dos fluxos de voz

5. Média de Perdas em relação ao fluxo de medição

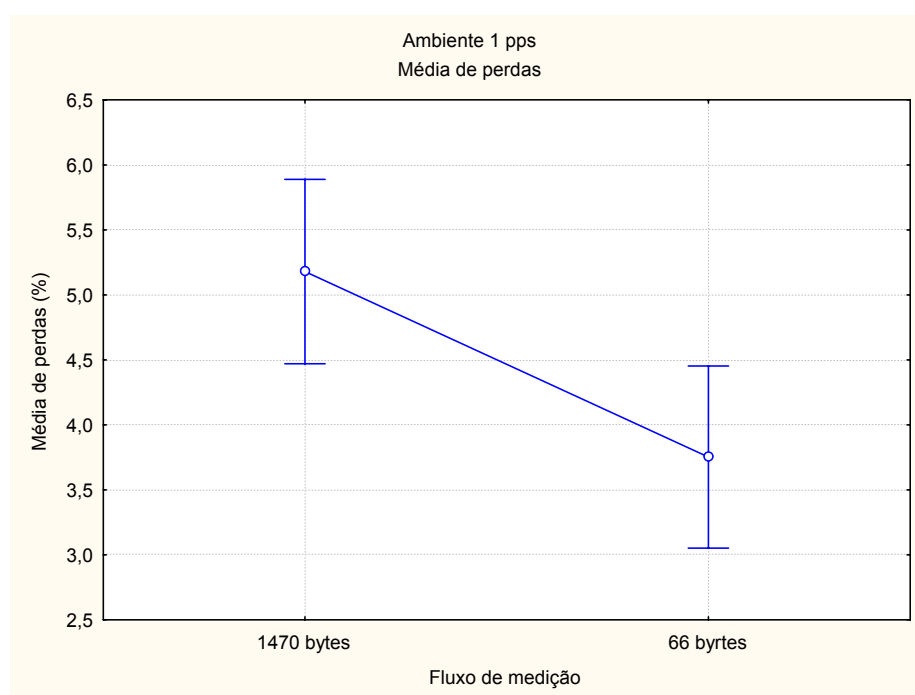


Figura A1 - 8 - Média de perdas em relação ao fluxo de medição

| Perdas (%) | Fluxo de medição | |
|---------------|--------------------------------|----------------------------|
| | 1470 bytes (1.44 Kbps) – e1 | 66 bytes – 528 bps – e2 |
| média | 5,179694 | 3,752240 |
| Desvio Padrão | 8,841616 | 7,373883 |
| N | 249 | 251 |

Tabela A1 - 8- Média de perdas em relação ao fluxo de medição

6. Média de Perdas em relação a disciplina de filas

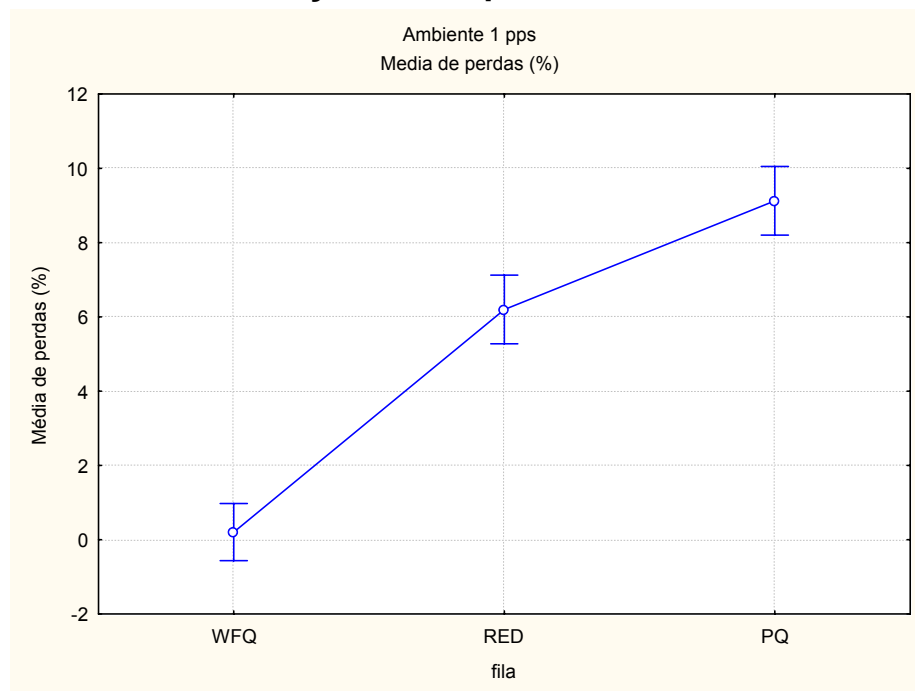


Figura A1 - 9-Média de perdas em relação às filas

| Perdas (%) | Fila | | |
|---------------|----------|----------|----------|
| | WFQ (h1) | RED (h2) | PQ (h3) |
| média | 0,204437 | 6,199721 | 9,124508 |
| Desvio Padrão | 1,50219 | 6,38607 | 11,68861 |
| N | 212 | 144 | 144 |

Tabela A1 - 9 – Média de perdas em relação às disciplinas de filas

7. Média de Perdas em relação ao destino dos fluxos de voz

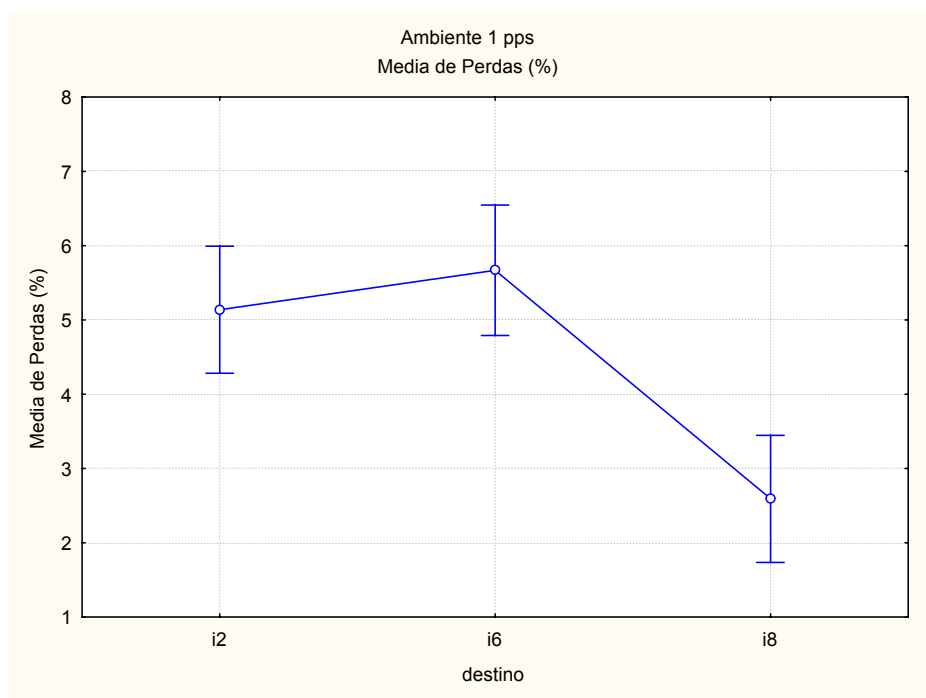


Figura A1 - 10- Média de perdas em relação ao destino

| Perdas (%) | Destino | | |
|---------------|----------|----------|----------|
| | PC2 | PC6 | PC8 |
| média | 5,137640 | 5,668904 | 2,591357 |
| Desvio Padrão | 8,189536 | 8,833538 | 7,080950 |
| N | 168 | 164 | 168 |

Tabela A1 - 10- Média de perdas em relação aos destinos dos fluxos

Apêndice 2

Codificação da fonte e codificação do canal

1. Codificação da fonte

a) Waveform coding

É sem dúvida o método mais simples, no qual as ondas analógicas são amostradas em pontos de tempo discretos, e cada amostra é representada por bits binários. A base matemática da codificação Waveform é o teorema de Nyquist. De acordo com este teorema, as ondas analógicas podem ser amostradas numa taxa igual a duas vezes a largura de banda (B) e a partir dessas amplitudes discretas amostradas, reconstroem-se “perfeitamente” as ondas originais. A Figura A2 - 1 mostra uma onda analógica sendo amostrada em diferentes taxas.

| |
|--|
| <i>Taxa de amostragem de Nyquist = 2 x largura de banda da fonte do sinal analógico</i> |
|--|

Pulse Code Modulation – PCM. A técnica de codificação PCM e a PCM adaptativa diferencial (ADPCM) são os tipos clássicos de codificação Waveform. O PCM foi o primeiro método de codificação, introduzida originalmente pelos laboratórios Bell da AT&T e depois padronizada pelo ITU-T (G.711) em 1988.

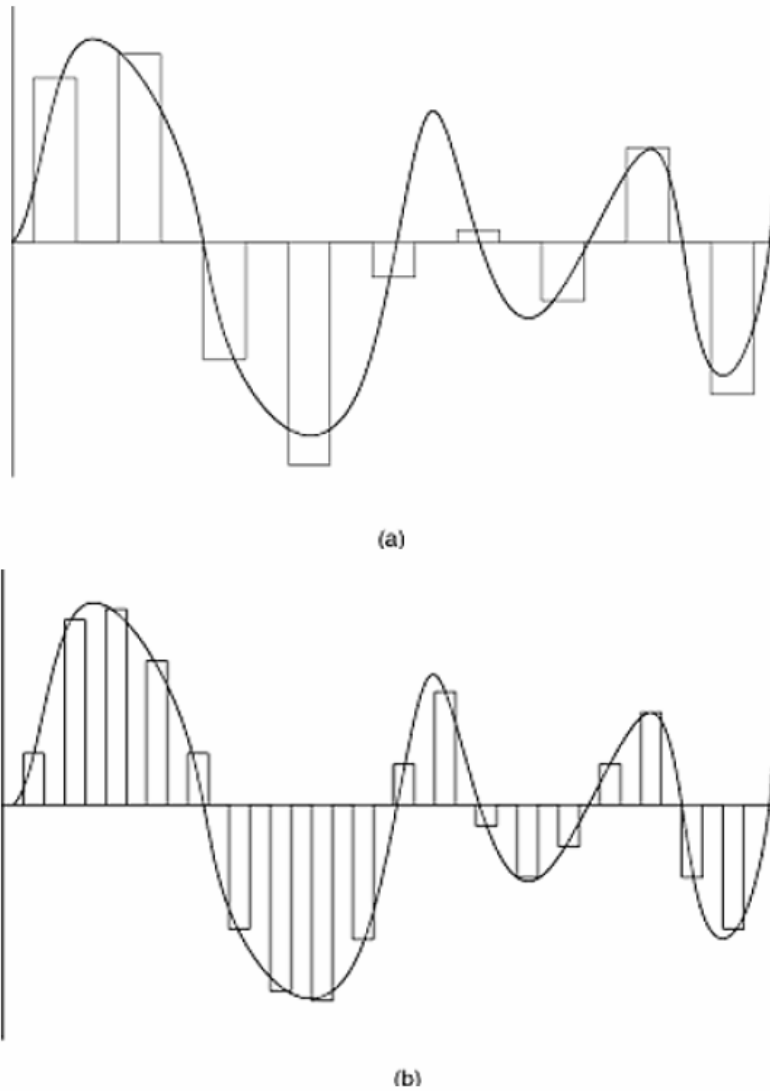


Figura A2 - 1 - Aproximação amostral do formato original da onda analógica. (a) frequência de amostragem muito baixa e (b) frequência duas vezes maior que em (a) – Fonte: Caputo, R., 2000

A voz humana utiliza frequências de até 4kHz, o que, segundo o teorema, sugere que o sinal de voz da fonte seja amostrado a $2 \times 4\text{kHz} = 8\text{ kHz}$, ou 8000 amostras por segundo. Cada amostra discreta é codificada em 8 bits. Como resultado, a codificação PCM produz uma stream digital de 64 kbps., representando a voz da fonte original:

$$(8000 \text{ amostra/s}) \times 8 \text{ bits/amostra} = 64 \text{ kbps}$$

Como o tamanho da amostra é de 8 bits, ou um byte, a duração do quadro na codificação PCM é de 0,125 ms.

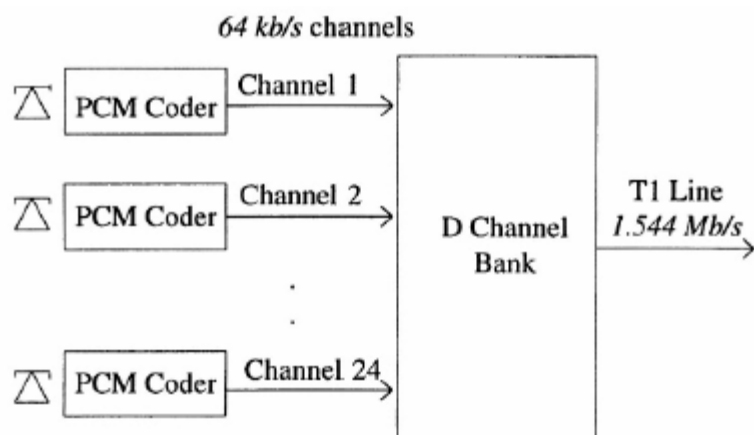


Figura A2 - 2- Banco de canais "D" , taxa DS-1 e linha T-1 – Fonte: Park, K. I., 2005

A taxa de 64 kbps do PCM serve de base para a hierarquia digital baseada no TDM -Time Division Multiplexing. Por exemplo, na América do Norte os bancos de canais "D" multiplexam 24 canais de voz-Figura A2 - 2, cada um operando na taxa de 64 kbps, nos frames DS-1 (Digital Signal-1). Um adicional de 8 kbps serve de sinalização dos quadros. Como resultado, o banco de canais D tem uma saída com taxa DS-1, ou 1544 Mbps:

$$(64 \text{ kbps} \times 24 \text{ canais}) + 8 \text{ kbps} = 1544 \text{ Mbps}$$

O sistema de transmissão operando com essas taxas é comumente conhecido como linhas "T1". Na Europa, são usados 30 canais de voz no multiplexador. A taxa resultante é conhecida como "E1". Portanto, na codificação Waveform é conveniente se utilizarem taxas multiplas de 64 kbps (ou submultiplas, como 32 ou 16 kbps).

ADPCM - Adaptive Differential Pulse Code Modulation. Desde a introdução do PCM, existe uma busca contínua para se reduzir a taxa de bits, o que economiza banda do sistema de transmissão. Merece destaque a técnica ADPCM, que utiliza uma previsão da próxima amostra com base nas amostras anteriores. A cada momento amostral, (tN), as últimas (N-1) amostras são utilizadas para prever a amostra N. Quando a amostra é tomada, a diferença entre o previsto e o obtido é computado.

Uma vez que as amostras adjacentes tendem a ser similares, e a variação na amplitude não é grande, a diferença entre a previsão e a amostra real tende a ser bem menor que a amplitude absoluta da própria amostra real. Uma vez que um número menor requer menos bits para representá-lo, a técnica adaptativa reduz a taxa de bits necessária no canal de voz. A taxa de amostragem contínua 8000/s, mas cada amostra é codificada em 4 bits, formando um fluxo de 32 kbps. Este ganho no uso da banda é obtido com o aumento da complexidade do CODEC.

b) LPC - linear predictive coding

A abordagem da codificação LPC é bastante diferente [Cox, R. V., 1997] . Ao invés de amostrar o formato da ondas e reconstruir a fala original a partir das amplitudes amostradas, a técnica LPC emprega modelos do trato vocal humano. A LPC aprende os padrões individuais do trato vocal, baseado em amostras e estima parâmetros para um modelo. Depois, transmite estes parâmetros para o decodificador, no lado do receptor da voz. O decodificador usa os parâmetros e sintetiza a voz do emissor da fala. A fala resultante não é uma reconstrução das ondas analógicas originais, mas sim uma fala construída localmente, baseada no modelo original. Essa técnica é análoga ao reconhecimento de voz por computador e a voz computadorizada. A LPC permitiu uma taxa de bits muito menor, como 13 kbps e 8 kbps(Park, K. I., 2005).

2. Codificação do canal

Após os processos de codificação da fonte e de empacotamento, o fluxo binário precisa ainda de uma codificação do canal de transmissão (channel coding), processo relacionado basicamente com proteção e correção de erros. A codificação do canal torna o fluxo de bits mais robusto, na presença de problemas na transmissão. Dois processos estão envolvidos na codificação do canal:

- a) Entrelaçamento (Interleaving);
- b) Correção de erros.

O entrelaçamento não exige bits adicionais, mas insere retardo adicional. A correção erros insere bits extras e aumenta o retardo [Park, K. I., 2005].

a. Entrelaçamento

O entrelaçamento é uma das maiores técnicas utilizadas para prover robustez aos sinais digitalizados. A correção de erros normalmente é usada para erros de 1 bit, randômicos [Kurose, J. F.; Ross, K. W., 2003]. Tal concepção torna as funções de correção menos aptas aos problemas de erros consecutivos, em rajadas. O entrelaçamento está demonstrado na Figura A2 - 3, onde blocos de 5 bits são entrelaçados no lado do emissor do sinal. A ordem natural dos bits está representada pelos bits de 1 a 25. O entrelaçador toma os primeiros bits de cada bloco de 5 e constrói o primeiro bloco de saída no canal de transmissão. O segundo bit de cada bloco é usado para construir o segundo bloco. O ciclo total necessita, neste exemplo, de um buffer de 5 blocos de 5 bits. No extremo receptor, o de-entrelaçador precisa de um buffer do mesmo tamanho para recuperar a sequência original. Generalizando, para prover entrelaçamento em blocos de N bits, N blocos de N bits precisam ser armazenados no buffer do entrelaçador:

$$\text{Tamanho do } \textit{buffer} \text{ do entrelaçador} = N^2$$

A Figura A2 - 4 mostra o de-entrelaçamento dos bits no extremo receptor do fluxo binário. O de-entrelaçador reorganiza os bits na sequência original. Supondo-se que os 5 bits do primeiro bloco em trânsito sejam alterados por uma rajada de erros ("x" na figura). Embora estivessem ordenados seqüencialmente durante a transmissão, ao se re-ordenarem os 5 bits errados ficam isolados, permitindo que os algoritmos de correção atuem com eficiência.

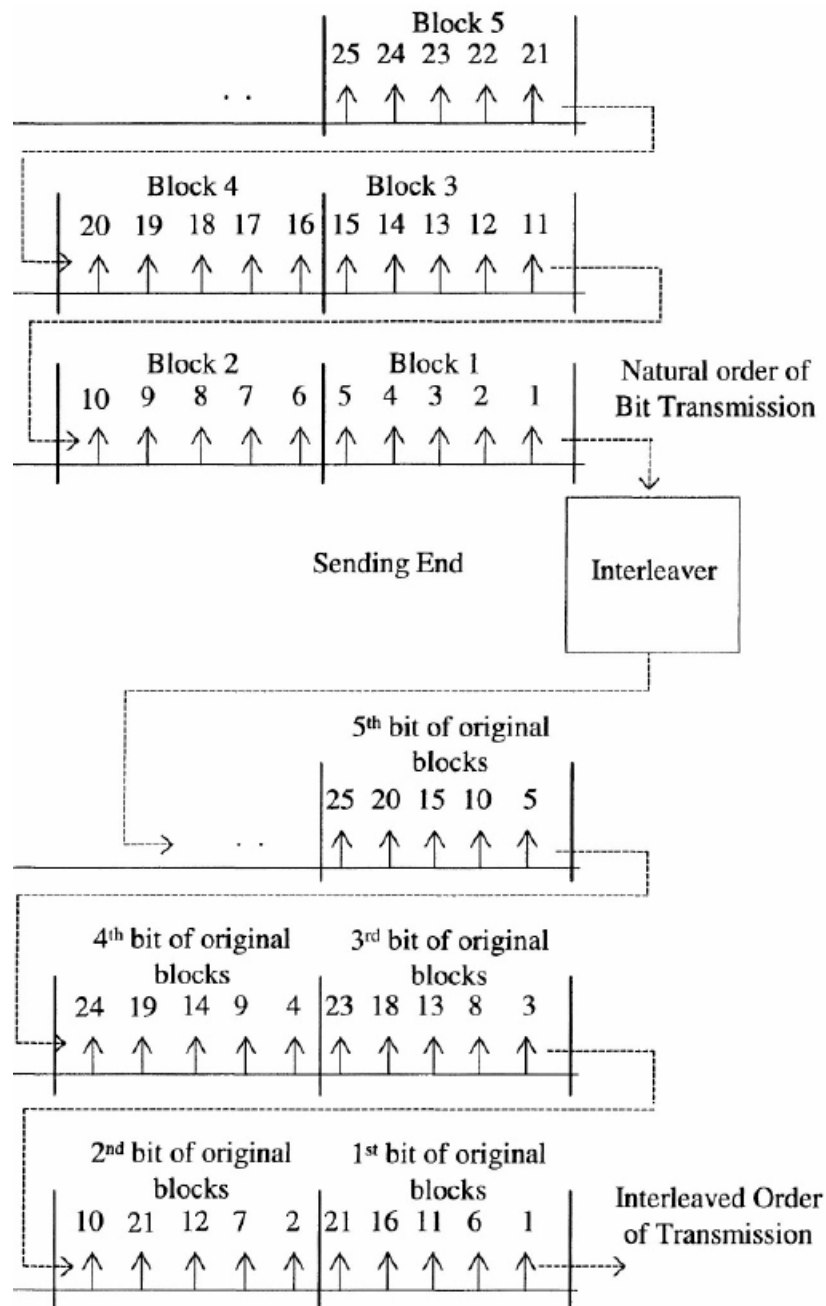


Figura A2 - 3- Entrelaçamento do sinal no emissor – Fonte: Park, K. I., 2005.

b. Correção de erros

Existem várias metodologias para correção de erros, e todas acrescentam atrasos, seja pelo aumento do processamento ou pelo acréscimo de sobrecarga, ao enviar bits redundantes. Uma forma simples de corrigir erros é pelo envio de quatro bits adicionais para cada bit gerado pela fonte, num total de cinco bits. No extremo receptor os bits são processados em blocos de 5 bits, sendo interpretados como um ou zero

dependendo do número maior de zeros ou uns do bloco. O compromisso dessa técnica fica entre a precisão e a banda utilizada.

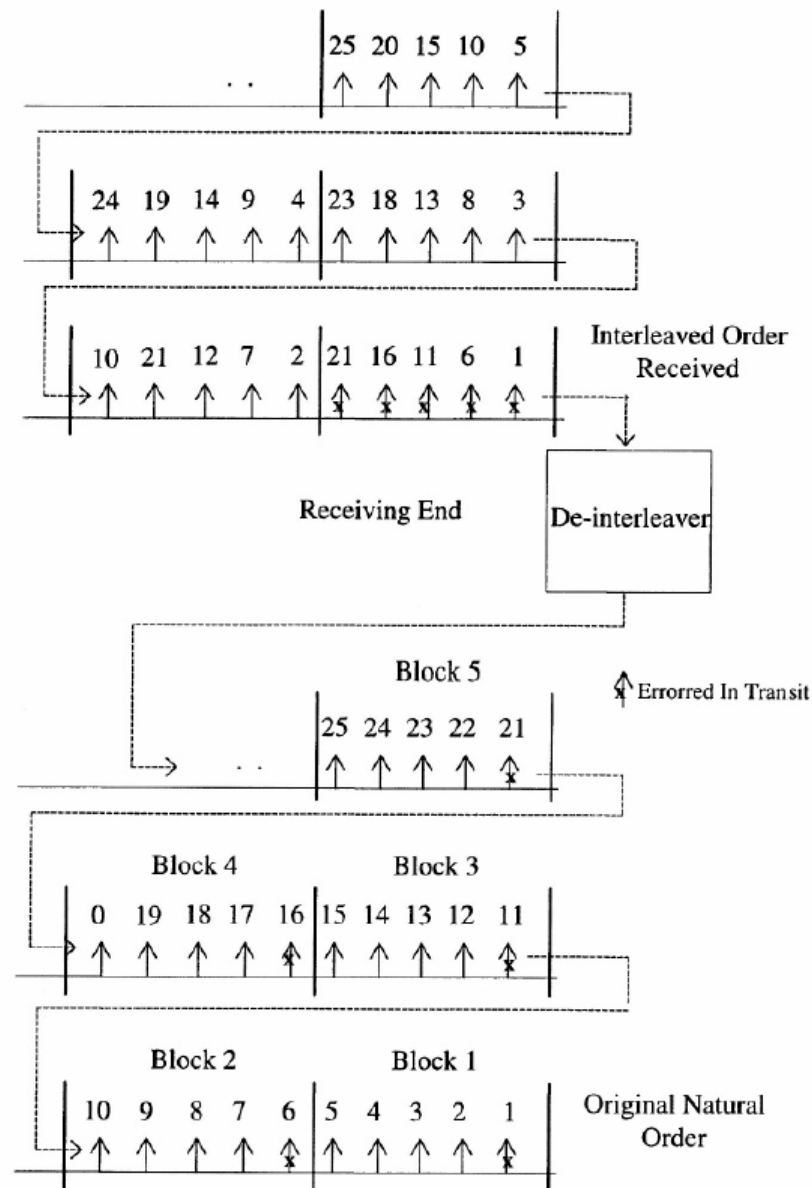


Figura A2 - 4-De-entrelaçamento no extremo do receptor dos fluxos digitais - Fonte: Park, K. I., 2005.

a) MODULAÇÃO

A modulação é o último passo antes da transmissão do sinal digital no meio físico. A informação é comunicada pela variação da portadora, que é uma onda "sinusoidal". O processo de alterar a portadora é denominado modulação.

Apêndice 3

Conceitos de Engenharia de Tráfego

Essa seção fornece os termos que definem os processos de engenharia de tráfego, segundo a RFC 3272 (Awduche, D.; Chiu, A.; Elwalid, A; Widjaja, I.; Xiao, X., 2002).

- Análise da linha de base (Baseline Analysis):
 - Um trabalho de pesquisa conduzido para servir de base para comparação com o comportamento atual da rede.

- Hora ocupada (Busy hour):
 - Um período de uma hora dentro de um intervalo de tempo especificado (tipicamente 24 horas) no qual a carga de tráfego na rede – ou sub-rede – é o maior.

- Gargalo (Bottleneck):
 - Um elemento da rede cuja taxa de tráfego de entrada tende a ser maior que a taxa de saída.

- Congestionamento (Congestion):
 - Um estado de um recurso de rede no qual o tráfego incidente no recurso excede sua capacidade de saída por um intervalo de tempo.

- Prevenção de congestionamento (Congestion avoidance):
 - Uma abordagem da gerência de congestionamento que tenta evitar a ocorrência de congestionamento.

- Controle de congestionamento (Congestion control):
 - Uma abordagem da gerência de congestionamento que tenta remediar os problemas de congestionamento que efetivamente já ocorreram.

- Roteamento baseado em restrições (Constraint-based routing):
 - Uma classe de protocolos de roteamento que considera, ao tomar decisões de roteamento, atributos específicos do tráfego, restrições da

rede e restrições de política. O termo é aplicável a agregações de tráfego e a fluxos específicos. É uma generalização o roteamento de QoS.

- Gerência de congestionamento no lado da demanda (Demand side congestion management):
 - Um esquema de gerência de congestionamento que aborda os problemas de congestionamento pela regulação ou congestionamento da carga oferecida.
- Largura de banda efetiva (Effective bandwidth):
 - A banda mínima que pode ser disponibilizada a um fluxo ou tráfego agregado para fornecer 'QoS aceitável' ao fluxo ou tráfego.
- Tráfego Egresso (Egress traffic):
 - Tráfego que está deixando a rede ou um elemento da rede
- Ponto Quente (Hot-spot):
 - Um elemento da rede ou sub-sistema que está em estado de congestionamento.
- Tráfego Ingresso (Ingress traffic):
 - Tráfego que está entrando na rede ou em um elemento da rede.
- Tráfego Inter-domínio (Inter-domain traffic):
 - Tráfego que tem origem em um Sistema Autônomo e termina em outro.
- Rede de perdas (Loss network):
 - Uma rede que não propicia buferização adequada para o tráfego, de forma que o tráfego entrando em um recurso ocupado dentro dessa rede será descartado ao invés de enfileirado.
- Métrica (Metric):
 - Um parâmetro definido em termos de unidades de medida padrão.

- Metodologia de medição (Measurement Methodology):
 - Uma técnica de medição reproduzível usada para obter uma ou mais métricas de interesse.
- Capacidade de Sobrevivência da rede (Network Survivability):
 - A capacidade da rede em prover o nível prescrito de QoS para os serviços existentes depois de um dado número de falhas terem ocorrido dentro da rede.
- Engenharia de tráfego externa (Offline traffic engineering):
 - Um sistema de engenharia de tráfego que existe fora dos limites da rede.
- Engenharia de tráfego interna (Online traffic engineering):
 - Um sistema de engenharia de tráfego que existe dentro dos limites da rede, tipicamente implementado em um elemento da rede ou adjunto a este elemento.
- Medidas de desempenho (Desempenho measures):
 - Métricas que fornecem medidas quali ou quantitativas do desempenho dos sistemas ou subsistemas de interesse.
- Gerência de desempenho (Desempenho management):
 - Uma abordagem sistemática para melhorar a efetividade em se atingirem metas específicas da rede, relacionadas com o desempenho.
- Métrica de desempenho (Performance Metric):
 - Um parâmetro de desempenho definido em termos de unidades de medida padrão.
- Provisionamento (Provisioning):
 - O processo de designar ou configurar os recursos da rede para atingir certas requisições.
- Roteamento de QoS
 - Classe de sistemas de roteamento que seleciona os caminhos a serem utilizados por um fluxo, baseado nas requisições de QoS deste fluxo.
- Acordo de Nível de Serviço (Service Level Agreement):

- Um contrato entre um provedor e o cliente que garante níveis de desempenho específicos e confiabilidade a um custo determinado.
- Estabilidade (Stability):
 - Um estado operacional no qual a rede não oscila de forma disruptiva de um modo para outro.
- Gerência de congestionamento no lado fornecedor (Supply side congestion management):
 - Um esquema de gerência de congestionamento que fornece recursos adicionais a rede para resolver e/ou antecipar-se aos problemas de congestionamento.
- Tráfego transitório (Transit traffic):
 - Tráfego cuja origem e destino estão ambos fora da rede em consideração.
- Características do tráfego (Traffic characteristic):
 - Uma descrição do comportamento temporal ou uma descrição dos atributos de um dado fluxo de tráfego ou de um agregado de tráfego.
- Sistema de engenharia de tráfego (Traffic engineering system):
 - Uma coleção de objetos, mecanismos e protocolos que são utilizados em conjunto para atingir os objetivos da engenharia de tráfego.
- Fluxo de tráfego (Traffic flow):
 - Uma seqüência de pacotes entre dois sistemas finais que pode ser caracterizada de determinada maneira. Um micro fluxo tem uma definição mais específica: É uma seqüência de pacotes com os mesmos endereços de origem e destino, com as mesmas portas de origem e destino e o mesmo identificador de protocolo.
- Intensidade de tráfego (Traffic intensity):
 - Uma medida da carga de um tráfego com respeito a capacidade de um recurso durante um período de tempo especificado. Nos sistemas de telefonia clássicos, a intensidade do tráfego é medida em unidades de Erlang.
- Matriz de tráfego (Traffic matrix):

- Uma representação da demanda de tráfego entre um conjunto de origem e destino de nós abstratos. Um nó abstrato pode consistir de um ou mais elementos de rede.
- Monitoração de tráfego (Traffic monitoring):
 - O processo de observação das características do tráfego em um dado ponto na rede, coletando as informações de tráfego para análise e ações futuras.
- Tronco de tráfego (Traffic trunk):
 - Uma agregação de fluxos de tráfego pertencentes a uma mesma classe, que são encaminhados através de um mesmo caminho. Um tronco de tráfego pode ser caracterizado por um nó de ingresso e outro de saída, e um conjunto de atributos que determinam suas características e requerimentos da rede.