VOZ SOBRE IP E QUALIDADE DE SERVIÇO EM REDES MULTISERVIÇOS – UMA ABORDAGEM PRÁTICA

EDNILSON GIMENES ROSA

Salvador – Bahia
2003

UNIVERSIDADE SALVADOR

MESTRADO EM REDES DE COMPUTADORES

VOZ SOBRE IP E QUALIDADE DE SERVIÇO EM REDES MULTISERVIÇOS – UMA ABORDAGEM PRÁTICA

Ednilson Gimenes Rosa

Dissertação apresentada à Universidade Salvador como parte das exigências do Curso de Mestrado Profissional em Redes de Computadores, áreas de concentração em Redes de Computadores, para obtenção do título de "Mestre".

Orientador
Prof. Dr. César Augusto Camillo Teixeira

Salvador – Bahia
Setembro – 2003

VOZ SOBRE IP E QUALIDADE DE SERVIÇO EM REDES MULTISERVIÇOS – UMA ABORDAGEM PRÁTICA

EDNILSON GIMENES ROSA

Dissertação apresentada à Universidade Salvador como parte das exigências do Curso de Mestrado Profissional em Redes de Computadores, áreas de concentração em Redes de Computadores, para obtenção do título de "Mestre".

APROVADA em 12 de setembro de 2003

Banca Examinadora:

Prof. Dr. Guido Lemos de Souza Filho (UFPB)	Membro
Prof. Dr. Joberto Sérgio Barbosa Martins (UNIFACS)	Membro
Prof. Dr. César Augusto Camillo Teixeira (UNIFACS)	Orientador

Salvador - Bahia
Setembro – 2003

Dedico este trabalho à minha filha, Vanessa.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram direta ou indiretamente na elaboração deste trabalho e na implementação do projeto, em especial a Patricia Rocha Loschiavo, Cláudio Laurentino da Silva, Marcelo Yamaguchi, Alexander da Silva Ferreira Segundo e Ana Carmen Deuerlein.

Ao orientador Professor Dr. César Augusto Camillo Teixeira e ao Professor Dr. José Augusto Suruagy Monteiro, pelo apoio e estímulo.

E às pessoas que me incentivaram e não me deixaram desistir quando a realização deste trabalho parecia distante demais, em especial a Iara Antônia de Oliveira Rosa, Juliette Gleide de Oliveira e Patrícia Lima Nogueira.

SUMÁRIO

LISTA DE FIGURAS VIII

LISTA DE TABELAS IX

LISTA DE SIGLAS X

RESUMO XIII

ABSTRACT XIV

1 INTRODUÇÃO 1

1.1 CONTEXTO 1
1.2 OBJETIVOS GERAIS 3
1.3 OBJETIVOS ESPECÍFICOS 4
1.4 ORGANIZAÇÃO DO TRABALHO 5
1.5 RESUMO DO CAPÍTULO 6

2 EVOLUÇÃO DAS REDES CORPORATIVAS 7

2.1 QUALIDADE DE SERVIÇO NAS REDES CORPORATIVAS 7
2.2 RESUMO DO CAPÍTULO 9

3 QUALIDADE DE SERVIÇO EM REDES IP 10

3.1 QUALIDADE DE SERVIÇO 10
3.2 MODELOS DE QUALIDADE DE SERVIÇO 11
3.2.1 O modelo Serviços Integrados (*IntServ*) 11
3.2.1.1 Limitações do modelo IntServ 12
3.2.2 O modelo *DiffServ* 13
3.2.2.1 Marcação dos pacotes 13
3.2.2.2 Per Hop Behaviors 15
3.2.2.2.1 PHB Padrão (*Default PHB*) 15
3.2.2.2.2 PHBs Class-Selector 16
3.2.2.2.3 PHB Expedited Forwarding (EF) 16
3.2.2.2.4 PHB Assured Forwarding (AF) 16
3.2.2.3 A arquitetura *DiffServ* 17
3.3 RECURSOS DE QUALIDADE DE SERVIÇO 18
3.3.1 Classificação e marcação 19
3.3.2 Controle de congestionamento 19
3.3.2.1 Técnicas de escalonamento 21
3.3.2.1.1 Fila *First-in, First-out (FIFO)* 21
3.3.2.1.2 Fila *Priority Queueing (PQ)* 22
3.3.2.1.3 Fila *Custom Queuing (CQ)* 23
3.3.2.1.4 Fila *Weighted Fair Queueing (WFQ)* 24
3.3.2.1.5 Fila *Class-Based WFQ (CB-WFQ)* 25
3.3.2.1.6 Fila *Priority Queue WFQ (PQ-WFQ)* 26
3.3.2.1.7 Fila *Low Latence Queueing (LLQ)* ou *Priority Queueing CBWFQ (PQ-CBWFQ)* 26
3.3.3 Condicionamento e policiamento de tráfego 27

3.3.3.1 CAR – *Commited Access Rate* 27
3.3.3.2 Suavização de tráfego 28
3.3.4 Mecanismos de eficiência de enlace 30
3.3.4.1 Compressão de cabeçalhos 30
3.3.4.2 Fragmentação e intercalação de quadros 31
3.3.5 Resumo dos recursos de *QoS* na plataforma *Cisco* 34
3.4 RESUMO DO CAPÍTULO 34

4 VOZ SOBRE IP 36

4.1 PROTOCOLOS DE VOZ SOBRE IP 36
4.2 BENEFÍCIOS DO PADRÃO VOZ SOBRE IP 37
4.3 PROCESSAMENTO DE UMA CHAMADA EM VOZ SOBRE IP 38
4.4 QUALIDADE DE SERVIÇO EM VOZ SOBRE IP 39
4.4.1 Atraso 40
4.4.2 Variação do atraso 40
4.4.3 Perda de pacotes 40
4.4.4 Consumo de banda 41
4.4.5 Efeitos da serialização 45
4.5 GATEKEEPER 45
4.6 VOZ SOBRE IP EM AMBIENTE CISCO 46
4.6.1 Recomendações de *QoS* da *Cisco* para *VoIP* 47
4.7 RESUMO DO CAPÍTULO 48

5 ROTEIRO PARA IMPLEMENTAÇÃO DE REDES MULTISERVIÇOS COM QUALIDADE DE SERVIÇO 49

5.1 CONHECENDO A REDE 49
5.2 DEFINIÇÃO DE EQUIPAMENTOS E *SOFTWARES* 49
5.3 DEFINIÇÃO DOS PROTOCOLOS DE ENLACE E DO ENDEREÇAMENTO 50
5.4 MONTAGEM DE UM LABORATÓRIO 51
5.5 REDE PILOTO 51
5.6 MONITORAÇÃO DOS RECURSOS E LOG'S 51
5.7 VALIDAÇÃO DOS RECURSOS PROJETADOS 52
5.8 FLUXO DE ATIVIDADES 53
5.9 RESUMO DO CAPÍTULO 54

6 IMPLEMENTANDO *QOS* EM UMA REDE COM EQUIPAMENTOS *CISCO* – ESTUDO DE CASO 55

6.1 A IMPLEMENTAÇÃO DA REDE 55
6.1.1 Requisitos da rede 57
6.2 QUALIDADE DE SERVIÇO 58
6.2.1 Classificação e marcação dos pacotes 59
6.2.2 Priorização do tráfego 63
6.2.3 Codificação das *policy-maps* 64
6.2.3.1 Ferramenta de configuração de *Policy-maps* 68
6.2.4 Condicionamento de tráfego 72
6.2.4.1 A arquitetura da família 7500 72
6.2.4.2 Configurações em *Frame Relay* 73
6.2.4.2.1 Configurações em roteadores sem placas VIP 73
6.2.4.2.2 Configurações em roteadores com placas VIP 75

6.2.4.3 Configurações em PPP 76
6.3 VERIFICAÇÃO DAS CONFIGURAÇÕES 78
6.3.1 Roteadores sem placas VIP 78
6.3.2 Roteadores com placas VIP 80
6.4 RESULTADOS OBTIDOS 82
6.5 RESUMO DO CAPÍTULO 83

7 IMPLEMENTANDO *VOIP* EM UMA REDE COM EQUIPAMENTOS *CISCO* – ESTUDO DE CASO 84

7.1 CONFIGURAÇÕES DE VOZ 84
7.1.1 Configuração via *Dial-Peers* 85
7.1.2 Configuração via *Gatekeeper* 85
7.2 VERIFICAÇÃO DAS CONFIGURAÇÕES 88
7.3 OS RESULTADOS OBTIDOS 90
7.4 RESUMO DO CAPÍTULO 90

8 PROBLEMAS E SOLUÇÕES NA IMPLEMENTAÇÃO DO PROJETO 91

8.1 PROBLEMAS DE *SOFTWARE* 91
8.1.1 Nomenclatura de versões de *software Cisco* 91
8.1.2 Problemas relacionados ao *software* (i.e. IOS®) *Cisco* 93
8.2 PROBLEMAS DE *HARDWARE* 95
8.3 OUTROS PROBLEMAS 96
8.4 RESUMO DO CAPÍTULO 97

9 CONSIDERAÇÕES FINAIS 99

10 REFERÊNCIAS BIBLIOGRÁFICAS 101

ANEXOS 107

ANEXO 01 – EQUIPAMENTOS UTILIZADOS NA IMPLEMENTAÇÃO DO PROJETO. 107
ANEXO 02 – CLASSIFICAÇÃO DE PROTOCOLOS E APLICAÇÕES. 114
ANEXO 03 – LISTAS DE ACESSO PARA MARCAÇÃO DOS PACOTES. 116
ANEXO 04 – RESULTADO DO COMANDO "*SHOW FRAME-RELAY PVC*" EM UM ROTEADOR SEM PLACA VIP 118
ANEXO 05 – RESULTADO DO COMANDO "*SHOW POLICY-MAP INTERFACE*" EM UM ROTEADOR COM PLACA VIP 120

LISTA DE FIGURAS

Figura 3.1: O *Byte ToS* Original no Ipv4..... 14
Figura 3.2: O Campo *DiffServ*..... 15
Figura 3.3: Arquitetura *DiffServ*..... 18
Figura 3.4: O Mecanismo *WRED*..... 21
Figura 3.5: Escalonamento *FIFO*..... 22
Figura 3.6: *Priority Queueing*..... 22
Figura 3.7: *Custom Queuing*..... 23
Figura 3.8: *Weighted Fair Queueing*..... 24
Figura 3.9: *Class Based WFQ*..... 25
Figura 3.10: *Priority Queue WFQ*..... 26
Figura 3.11: *Low Latency Queuing*..... 27
Figura 3.12: *Commited Access Rate*..... 28
Figura 3.13: *Traffic Shaping*..... 29
Figura 3.14: Parâmetros do *Frame Relay Traffic Shaping*..... 30
Figura 3.15: O *RTP Header Compression*..... 31
Figura 3.16: Fragmentação e Intercalação de Pacotes..... 33
Figura 4.1: O Ambiente de Voz sobre IP..... 39
Figura 5.1: Fases do projeto e implementação de uma rede..... 53
Figura 6.1: Topologia simplificada da rede..... 56
Figura 6.2: Ferramenta para configuração de *policy-map* de *QoS*..... 70
Figura 6.3: Ferramenta para configuração de *policy-map* de *QoS* – Versão 2..... 71

LISTA DE TABELAS

Tabela 3.1: Codificação *DiffServ* PHB AF..... 17
Tabela 3.2: Principais categorias e recursos de *QoS* do IOS® da C*isco*..... 34
Tabela 4.1: O Padrão *VoIP* e o modelo OSI..... 37
Tabela 4.2: Consumo de Banda por chamada *VoIP*..... 43
Tabela 6.1: Classes e Serviços definidos..... 61
Tabela 6.2: Classificação de protocolos e aplicações..... 61
Tabela A1: Relação de equipamentos..... 107
Tabela A2: Classificação de protocolos e aplicações..... 114

LISTA DE SIGLAS

ACL	*Access Control Lists*
AF	*Assured Forwarding*
ATM	*Asynchronous Transfer Mode*
B/W	*Bandwidth*
BA	*Behavior Aggregate*
BC	*Burst Committed*
BE	*Burst Excess*
BECN	*Backward Explicitly Congestion Notification*
CAR	*Committed Access Rate*
CB-WFQ	*Class-Based Weighted Fair Queuing*
CEF	*Cisco Express Forwarding*
CIR	*Committed Information Rate*
CPD	Centro de Processamento de Dados
CPU	*Central Processing Unit*
CQ	*Custom Queuing*
cRTP	*Compressed Real Time Protocol*
CTF	Concentrador de Transações Financeiras
DE	*Discard Eligibility*
DF	*Deferred*
DiffServ	*Differentiated Services*
DNS	*Domain Name Server*
DoD	*Department of Defense*
DRAM	*Dynamic Random Access Memory*
DS	*DiffServ*
DSCP	*Differentiated Services Code Points*
DSP	*Digital Signal Processors*
DTMF	*Dual Tone Multi Frequency*
DTS	*Distributed Traffic Shaping*
ED	*Early Deployment*
EF	*Expedited Forwarding*
ERP	*Enterprise Resource Planning*
FECN	*Forward Explicitly Congestion Notification*
FEP	*Front End Processor*
FIFO	*First-in, First-out*
FRTS	*Frame Relay Traffic Shaping*
FTP	*File Transfer Protocol*
FXS	*Foreign Exchange Station*
GD	*General Deployment*
GRTS	*Generic Traffic Shaping*
HTTP	*Hypertext Transfer Protocol*
I/O	*Input/Output*
IETF	*Internet Engineering Task Force*
INTSERV	*Integrated Services*
IP	*Internet Protocol*
ITU-T	*International Telecommunication Union*
KBPS	Kilo bits por segundo
LAN	Local Area Network

LD	*Limited Deployment*
LFI	*Link Fragmentation and Interleaving*
LLQ	*Low Latency Queuing*
MB	*Megabytes*
MGCP	*Media Gateway Control Protocol*
MinCIR	*Minimal Committed Information Rate*
MLPPP	*Multilink PPP*
MPLS	*Multiprotocol Label Switching*
MS	Milisegundos
MTU	*Maximum Transfer Unit*
NBAR	*Network-based Application Recognition*
OSI	*Open Source Initiative*
PABX	*Private Automatic Branch Exchange*
PC	*Personal Computer*
PHB	*Per Hop Behaviors*
POTS	*Plain Old Telephony System*
PPP	*Point to Point Protocol*
PQ	*Priority Queuing*
PSTN	*Public Switched Telephone Network*
PQ-WFQ	*Priority Queue Weighted Fair Queuing*
PVC	*Permanent Virtual Circuit*
QDM	*QoS Device Manager*
QoS	*Quality of Service*
QPM	*QoS Policy Manager*
RDP	*Remote Desktop Protocol*
RED	*Random Early Detect*
RENPAC	Rede Nacional de Pacotes
RFC	*Request for Comments*
RNP	Rede Nacional de Ensino e Pesquisa
RSH	*Remote Shell*
RSP	*Route Switching Processor*
RSVP	*Resource Reservation Protocol*
RTCP	*Real Time Conferencing Protocol*
RTP	*Real Time Protocol*
SAP	*Systems, Applications, and Products in Data Processing*
SDP	*Session Description Protocol*
SIP	*Session Initiation Protocol*
SLA	*Service-Level Agreements*
SNA	*System Network Architecture*
SNMP	*Simple Network Management Protocol*
SONET	*Synchronous Optical Network*
SQL	*Structured Query Language*
TAC	*Technical Assistance Center*
TC	*Time Committed*
TCP	*Transport Control Protocol*
TEF	Transferência Eletrônica de Fundos
TELNET	*Terminal Network Protocol*
ToS	*Type of Service*
UDP	*User Datagram Protocol*

URA	Unidade de Resposta Audível
VAD	*Voice Activity Detection*
VIP	*Versatile Interface Processors*
VNC	*Virtual Network Computing*
VoFR	*Voice Over Frame Relay*
VoIP	*Voice over Ip*
WAN	*Wide Area Network*
WFQ	*Weighted Fair Queuing*
WRED	*Weighted Random Early Detection*
WTS	*Web Transaction Security*
WWW	*World Wide Web*
XOT	*X.25 over TCP*

RESUMO

Rosa, G. Ednilson. **Voz sobre IP e Qualidade de Serviço em redes multiserviços – uma abordagem prática.** 2002. Dissertação (Mestrado em Redes de Computadores), Universidade Salvador, Salvador.

Palavras-chave: Voz sobre IP, Qualidade de Serviço, Serviços Diferenciados.

Nos últimos anos têm crescido a busca por implementações de redes que integrem serviços de diferentes naturezas, como dados, voz e imagem, buscando a racionalização de custos com telecomunicações e o aumento da produtividade que esta integração pode proporcionar. Estas implementações, no entanto, impõem um grande desafio no que tange à garantia da qualidade de determinados serviços de mídia contínua, como voz e vídeo, e de serviços de transmissão de dados prioritários, especialmente quando estão sendo utilizadas redes que não foram concebidas para a transmissão de mídia contínua com garantias de Qualidade de Serviço. Estes desafios são ainda maiores quando somados a inúmeros outros problemas técnicos que ocorrem durante uma implementação desse tipo, os quais, em geral, não são possíveis de se prever durante a fase de modelagem. Esta dissertação apresenta as soluções adotadas no projeto e implementação de uma rede de grande porte, envolvendo equipamentos *Cisco*, na qual foram utilizadas as mais recentes tecnologias de transmissão de Voz sobre IP e técnicas de garantia de Qualidade de Serviço, como as que são baseadas na padronização de Serviços Diferenciados. São ressaltados os problemas encontrados, as opções de soluções analisadas e as considerações realizadas que conduziram às soluções adotadas na busca de um coeficiente custo x benefício adequado. Este trabalho tem como objetivo contribuir com as tarefas de projeto, análise e implementação de redes de grande porte com serviços integrados de dados e de voz, servindo como guia de referência para implementações deste tipo e sugerindo um roteiro para desenvolvimento de projetos desta categoria.

ABSTRACT

Rosa, G. Ednilson. **Voice over IP and Quality of Service over multiservice networks – a practical approach.** 2002. Dissertation (Master on Computer Networks), Universidade Salvador, Salvador.

Keywords: Voice over IP, VoIP, Quality of Service, QoS, Differentiated Services, DiffServ.

In the last few years we have seen a growing demand for network solutions that integrate different kinds of services, like data, voice and image, reducing costs and increasing productivity. These implementations, however, may be a great challenge. The difficulty lies in assuring the quality of continuous media services, like voice and video, and in the transmission of priority data, especially when the used networks have not been designed for carrying real-time traffic with assured Quality of Service. Additional technical problems may occur in this kind of implementation. These problems are generally not easy to anticipate and will make this even a greater challenge. This dissertation presents the solutions adopted on the project and implementation of a large network using Cisco products. It uses the most recent developments for Voice over IP transmission and Quality of Service techniques, like those for Differentiated Services standard. This document points out the problems found during the project, the analyses carried out and the options that were considered in order to achieve the ideal cost x benefit relationship. This document is designed to help during all phases of a project lifecycle, from analysis to implementation of large networks with integrated services of data and voice. It can be used as a road map for a similar kind of project.

1 Introdução

1.1 Contexto

Com a disseminação da Internet, a maioria das empresas passou a adotar o TCP/IP[1] (i.e. *Transfer Control Protocol/Internet Protocol*) como seu principal conjunto protocolos, de forma a manter a homogeneidade e a compatibilidade em relação às suas próprias redes e às redes com as quais têm que se conectar. Dessa forma, a grande maioria das redes existentes hoje está baseada nos protocolos TCP/IP, enquanto que arquiteturas que tiveram grande destaque no passado, como a arquitetura SNA[2], acabaram perdendo espaço.

Nos últimos anos, com a evolução da qualidade, a redução dos custos e o aumento das taxas de transmissão dos meios físicos disponíveis, tem crescido nas empresas a tendência de integrar, em suas redes de dados, também serviços de tempo real com mídia contínua, como voz e vídeo. A principal razão para esta tendência é a busca da racionalização de custos com comunicação e transporte, que têm representado um fardo cada vez maior nos orçamentos das empresas em tempos de atuação globalizada. Assim, muitas empresas têm procurado, por exemplo, integrar serviços de telefonia e vídeo às suas redes de dados, de forma a cortar custos na utilização de chamadas telefônicas de longa distância.

A utilização de redes de pacotes, como as redes baseadas em protocolos IP[3], para transporte de tráfegos que tenham requisitos de tempo real, como as aplicações de voz e vídeo, esbarra no fato dessas redes não terem sido originariamente projetadas para esse fim e, portanto, não terem sido previstos mecanismos para garantia de qualidade desse tipo de serviço neste conjunto de protocolos. O tráfego de mídia contínua tem requisitos específicos em relação à garantia de banda, ao atraso máximo e à variação do atraso na transmissão dos pacotes, que não são preocupações do modelo original dos protocolos TCP/IP. Além disso, mesmo para a transmissão exclusivamente de dados, existe hoje uma demanda crescente por garantias de padrões mínimos de qualidade e priorização de determinadas aplicações consideradas de maior importância para as organizações.

[1] Conjunto de protocolos adotado pela Internet
[2] Arquitetura de redes proprietária da IBM.
[3] Redes baseadas no conjunto de protocolos TCP/IP

Todos estes requisitos de integração de serviços com garantias de padrões de qualidade e priorização demandam a adoção de técnicas avançadas de Qualidade de Serviço (i.e. *QoS*), de aplicação quase sempre complexa e, algumas vezes, até mesmo problemática.

É possível encontrar diversos estudos, trabalhos e documentos que abordem a teoria de implementações de *QoS* em redes IP. São poucos, no entanto, os que tratam o tema de uma forma global e que trazem uma abordagem prática aos conceitos associados a estes assuntos. Alguns deles dão uma ênfase mais teórica, enquanto que outros são mais específicos a determinados detalhes, sem uma abordagem mais ampla.

No *website* da *Cisco* (Cisco, 2003a) pode ser encontrada uma grande quantidade de informações práticas e teóricas sobre este assunto. O documento *Quality of Service Networking* (Cisco, 2002a) apresenta conceitos de Qualidade de Serviço e os recursos disponíveis para *QoS* na plataforma *Cisco*. Trata-se de um documento abrangente, porém essencialmente teórico, não entrando em detalhes quanto à implementação dos recursos expostos.

Em *Cisco* IOS® *QoS Technical Documents* (Cisco, 2002b) podem ser encontradas diversos *links* para documentos que tratam de aspectos diversos de Qualidade de Serviço. Em *Quality of Service for Voice over IP* (Cisco, 2003b) são abordados diversos aspectos técnicos de implementações de *QoS* relacionadas a *VoIP*[4] (i.e. Voz sobre IP). Em *Cisco IP Telephony / VoIP* (Cisco, 2003c) há *links* para uma grande quantidade de documentos da *Cisco* que tratam sobre o mesmo assunto. A partir de *Cisco QoS* (Cisco, 2003d) pode-se acessar também muitos documentos que tratam de tópicos relacionados a *QoS* de um modo geral.

Entre a documentação em português, pode-se destacar alguns artigos publicados na revista *News Generation* (RNP, 2003), da RNP. Em Santos (1999), a autora aborda alguns dos principais padrões de Qualidade de Serviço. Os artigos *Qualidade de Serviço em VoIP – Parte 1* (Silva, 2000a) e *Qualidade de Serviço em VoIP – Parte 2* (Silva, 2000b) trazem uma abordagem bastante prática e objetiva sobre obtenção de *QoS* em um ambiente *VoIP* com a utilização de equipamentos *Cisco*. Outro artigo bastante prático

[4] Padrão de transmissão de tráfego voz em redes IP

abordando *QoS* é Oyama & Lucena (2002). Este documento descreve a implementação das configurações de *QoS* na rede da RNP, que também utiliza roteadores *Cisco*.

Em Joberto Martins (1999), o autor apresenta uma visão geral sobre *QoS* e as ferramentas disponíveis para se obtê-la. Já Ferguson (1998) faz uma extensa exploração teórica sobre o assunto Qualidade de Serviço.

Apesar de todos estes documentos oferecerem uma grande quantidade de informações sobre Qualidade de Serviço e Voz sobre IP, todos padecem, em maior ou menor grau, de uma abordagem mais prática, que possa guiar de forma mais segura alguém que esteja interessado no projeto e, principalmente, na implementação de uma rede que ofereça estes recursos.

O objetivo deste trabalho é justamente suprir esta lacuna, buscando ilustrar e complementar, com experiências práticas e reais, o conteúdo teórico que envolve os temas Qualidade de Serviço e Voz sobre IP, de forma a servir como referência na construção de redes desta natureza. Para tanto, são descritos os problemas, as técnicas e as opções adotadas na construção de uma rede de grande porte com garantias de Qualidade de Serviço em um ambiente integrado de dados e voz.

Apesar da especificidade de alguns aspectos deste trabalho, o fato da implementação ter utilizado roteadores *Cisco*, um dos maiores fabricantes de equipamentos de redes a nível mundial, e ter feito uso de serviços de comunicação de dados com linhas dedicadas E1[5] e redes *Frame Relay*[6] da Embratel, uma das maiores prestadoras públicas de telecomunicações do Brasil, fez com que se tivesse um cenário bastante comum, tornando as conclusões do trabalho facilmente aplicáveis a uma grande quantidade de situações semelhantes.

1.2 Objetivos gerais

Este trabalho apresenta as soluções adotadas no projeto e implementação de uma rede de grande porte, na qual foram utilizadas algumas das mais recentes tecnologias de transmissão de voz e técnicas de garantia de Qualidade de Serviço, como as baseadas na

[5] Padrão de interface multiplexada com 30 canais formando um agregado de 2048 kbps.
[6] Padrão de rede de pacotes de nível 2 (camada de enlace do modelo OSI).

padronização de Serviços Diferençiados[7] (i.e. *DiffServ*) e Voz sobre IP. São ressaltados os problemas encontrados, as opções de soluções analisadas e as considerações realizadas que conduziram às soluções adotadas na busca de um coeficiente custo/benefício adequado. O trabalho tem ainda como objetivo servir como referência para implementações deste tipo, sugerindo um roteiro para sistematização de projetos desta categoria e de porte similar.

1.3 Objetivos específicos

Os objetivos específicos deste trabalho são:

- apresentar técnicas de garantia de Qualidade de Serviço e priorização de dados e como implementá-las em ambiente *Cisco*;

- apresentar as técnicas de implementação de Voz sobre IP e garantias de qualidade utilizando equipamentos e protocolos *Cisco*;

- abordar os problemas enfrentados durante a implementação de uma rede integrada, apresentando as soluções que podem ser adotadas para evitá-los;

- servir como guia prático na implementação de projetos de rede envolvendo Qualidade de Serviço e Voz sobre Ip utilizando equipamentos *Cisco*;

- sugerir um roteiro de trabalho para o projeto e implementação de redes com Qualidade de Serviço e Voz sobre Ip.

[7] Modelo de Qualidade de Serviço padronizado pelo *Internet Engineering Task Force* (IETF)

1.4 Organização do trabalho

Este trabalho encontra-se organizado da seguinte forma:

O presente capítulo (Introdução) aborda a evolução dos requisitos das redes corporativas modernas, o contexto no qual está inserido o cenário do trabalho e os objetivos gerais e específicos do mesmo, assim como sua organização. É feita também uma revisão bibliográfica envolvendo os temas abordados pelo trabalho.

No capítulo 2 (Evolução das Redes Corporativas) é feita uma explanação mais detalhada de como evoluíram as redes corporativas, a disseminação da suíte de protocolos TCP/IP e as limitações impostas por ela. São também abordados, nesse capítulo, algumas das novas aplicações das redes IP e os requisitos que elas trazem em termos de garantias de Qualidade de Serviço.

No capítulo 3 (Qualidade de Serviço em Redes IP) são apresentados os conceitos básicos de Qualidade de Serviço e algumas das técnicas mais comumente usadas para implementá-los. São abordados assuntos como suavização de tráfego (i.e *traffic-shaping*), fragmentação, técnicas de escalonamento, policiamento de tráfego e outros relacionados à Qualidade de Serviço. Também serão abordados os principais recursos presentes em roteadores que possibilitem a obtenção de Qualidade de Serviço, com ênfase especial aos encontrados na plataforma *Cisco*.

No capítulo 4 (Voz sobre IP) são apresentadas as técnicas de transmissão de Voz sobre IP, seus benefícios e requisitos e também os detalhes de sua implementação no ambiente de roteadores *Cisco*.

No capítulo 5 (Roteiro para Implementação de Redes Multiserviços com Qualidade de Serviço) é sugerido um roteiro para o projeto e a implementação de redes de grande porte com serviços integrados de dados e de voz.

No capítulo 6 (Implementando *QoS* em uma rede com equipamentos *Cisco* – estudo de caso) são apresentados os tópicos que devem ser levados em consideração no projeto de uma rede integrada com Qualidade de Serviço. São apresentados os aspectos que foram avaliados na escolha dos equipamentos e *softwares* que compõe a rede que

serviu como estudo de caso para este trabalho e os detalhes desta implementação em equipamentos Cisco

No capítulo 7 (Implementando *VoIP* em uma rede com equipamentos *Cisco* – estudo de caso) são apresentados os detalhes da implementação de Voz sobre IP em uma rede com equipamentos *Cisco* e Qualidade de Serviço.

No capítulo 8 (Problemas e Soluções na Implementação do Projeto) são enumerados os principais problemas enfrentados na implementação do projeto estudado e quais as soluções encontradas para os mesmos.

No capítulo 9 (Considerações finais) são sintetizadas as conclusões dos capítulos anteriores, apresentadas as considerações relativas aos resultados e objetivos do trabalho e sugeridos possíveis trabalhos futuros que possam complementar as contribuições deste estudo.

1.5 Resumo do capítulo

Neste capítulo são apresentados a motivação e o contexto deste trabalho, uma revisão bibliográfica sobre os temas Qualidade de Serviço e Voz sobre IP e também a forma como este documento encontra-se organizado.

No próximo capítulo é feita uma exposição a respeito da evolução das redes corporativas e os requisitos de qualidade que esta evolução propiciou.

2 Evolução das redes corporativas

Neste capítulo é abordada a evolução das redes corporativas e como esta evolução mudou os requisitos por Qualidade de Serviço que estas essas redes demandam.

2.1 Qualidade de serviço nas redes corporativas

Na última década cresceu muito a utilização de redes de computadores por organizações dos mais variados portes e ramos de atividade. Um grande impulsionador deste crescimento foi a disseminação da Internet, que propiciou novas aplicações para a comunicação em rede. Nas décadas de 70 e 80, apesar de as redes locais já terem começado a se difundir, ainda eram poucas as empresas que as utilizavam largamente e, menos ainda, as que utilizavam a comunicação em redes de longa distância, as redes WAN (i.e. *Wide Area Network*). Nessa época, as telecomunicações ainda eram um recurso muito caro e poucas organizações, como algumas grandes indústrias e instituições financeiras, tinham condições de investir em grandes redes de comunicação de dados. A plataforma de *hardware*[8] então dominante era a dos grandes *mainframes*[9] IBM e sua arquitetura proprietária de redes, a SNA (i.e. *System Network Architeture*).

Durante a Guerra Fria, o *Department of Defense* (i.e. *DoD*) dos Estados Unidos teve a iniciativa de construir uma infraestrutura de comunicações que fosse difícil de ser destruída por seus inimigos. Nascia assim o embrião da rede que viria se transformar na Internet e com ela foi concebida a arquitetura TCP[10]/IP[11]. Este conjunto de protocolos tinha como objetivo principal fornecer comunicação fim-a-fim de forma robusta e simplificada. Não havia grandes preocupações com garantias de entrega e integridade dos dados e, principalmente, não havia qualquer mecanismo que desse suporte a mídias de tempo real, como voz e vídeo.

Com o passar dos anos, a Internet disseminou-se fortemente nos meios acadêmicos com o apoio do *DoD*. No final da década de 80, a Internet já estava presente na grande maioria das principais universidades ao redor do mundo. Com essa

[8] Parte física de um computador.
[9] Computadores de grande porte.
[10] Protocolo de nível 4 (transporte) da arquitetura TCP/IP.

disseminação, foram se fortalecendo as padronizações em torno da arquitetura TCP/IP, que começava a despontar como o grande destaque nas redes do futuro.

Mas foi na década de 80 que a Internet ganhou caráter comercial e chegou de forma ampla, não só nas empresas, mas também nas residências de milhões de pessoas em todo o mundo. Nesta época, as corporações passavam também pelo fenômeno do *downsizing*[12], em que muitas delas trocavam seus grandes *mainframes* pela arquitetura cliente-servidor, tida como mais barata e fácil de manter e gerenciar. Esta conjunção de fatores contribuiu para que o TCP/IP acabasse sendo adotado quase como que um esperanto[13] para as redes de comunicação. Com a necessidade de as empresas se ligarem à Internet e o desejo de poder contar com uma arquitetura protocolar única e simplificada, o conjunto de protocolos TCP/IP tornou-se praticamente onipresente nas redes da maioria das empresas.

Finalmente, na década de 90, o mundo viu os custos com telecomunicações caírem bastante, tornando a adoção de redes privadas de longa distância algo possível até mesmo para empresas de pequeno porte. Mais ainda, surgiu no mundo o fenômeno da globalização. Com ele, as empresas passaram a ter cada vez mais necessidade de se comunicar com pessoas a distância, fossem elas clientes, fornecedores ou mesmo integrantes de filiais ou de empresas coligadas. Foi então que as corporações passaram a perceber que poderiam economizar muito com telecomunicações se utilizassem suas redes de dados para também transportar áudio, para comunicações de voz, e vídeo, para realização de reuniões virtuais a distância.

Toda esta demanda por novas aplicações para as redes IP, no entanto, tinham um obstáculo a ser vencido em relação às garantias de qualidade oferecidas pelo TCP/IP. Diferentemente das aplicações puramente de dados, as aplicações de mídia contínua têm necessidades específicas, sem as quais elas são inviáveis. Para que uma aplicação de transmissão de voz se realize com sucesso, por exemplo, a rede não deve inserir atrasos muito grandes na transmissão dos pacotes, pois isso pode tornar a conversação desconfortável para as pessoas que participam dela. Também não deve haver grande

[11] Protocolo de nível 3 (rede) da arquitetura TCP/IP.
[12] Tendência administrativa na área de Informática pela qual os grandes computadores foram substituídos por redes de computadores *desktop*.
[13] Idioma artificial criado em 1887 pelo médico e poliglota polonês Dr. Luís Lázaro Zamenhof, com o intuito de que pudesse servir como língua universal.

variação no atraso dos pacotes (i.e. *jitter*), pois isso pode fazer com que a voz saia distorcida para o receptor. Perdas de pacotes também não são desejáveis, já que elas também podem interferir negativamente na qualidade do áudio transmitido. Requisitos semelhantes também se aplicam a transmissões de vídeo, em especial para as realizadas ao vivo, como em videoconferências[14].

Além das aplicações de mídia contínua, as empresas também passaram a integrar, em suas redes, aplicações de missão crítica, diretamente relacionadas com a área fim da empresa, implicando na necessidade de se estabelecer prioridade sobre aplicações menos importantes compartilhando a mesma infra-estrutura.

Todas estas garantias, que se tornaram requisitos para aplicações de mídia contínua e de missão crítica, não faziam parte das preocupações do projeto inicial do protocolo TCP/IP. Como o TCP/IP tornou-se um padrão de fato nas redes de todo o mundo, não se podia esperar que as empresas resolvessem trocar suas estruturas de redes por outras que utilizassem protocolos mais indicados para aplicações dessa natureza, como a arquitetura ATM[15] (i.e. *Asynchronous Transfer Mode*), por exemplo. Assim, nos últimos anos foram surgindo diversos mecanismos buscando suprir as deficiências do TCP/IP para garantir a Qualidade de Serviço que as modernas redes demandam. Nos próximos capítulos são apresentados alguns desses mecanismos e como eles podem ser integrados de forma harmoniosa para se obter uma rede corporativa que permita a convergência de dados de diferentes naturezas e aplicações de mídia contínua, com todas as garantias de Qualidade de Serviço que se deseje.

2.2 Resumo do capítulo

Neste capítulo são abordados a evolução das redes corporativas e os requisitos de Qualidade de Serviço e novos recursos advindos dessa evolução.

No próximo capítulo são apresentados os conceitos e as técnicas relativas a Qualidade de Serviço, com destaque os recursos presentes em roteadores *Cisco*.

[14] Reuniões virtuais efetuadas com o uso de recursos de telecomunicações.
[15] Pilha de protocolos concebida para fornecer garantias de Qualidade de Serviço.

3 Qualidade de Serviço em redes IP

A evolução das redes IP levou a uma convergência de aplicações que demandou a criação de mecanismos que pudessem prover as garantias de níveis de serviço que eram necessárias para que estas aplicações tivessem êxito na arquitetura TCP/IP. Neste capítulo são discutidos os principais recursos e técnicas de Qualidade de Serviço e os modelos que podem ser seguidos para sua obtenção, com destaque especial aos recursos disponíveis na plataforma *Cisco*.

3.1 Qualidade de Serviço

Qualidade de Serviço pode ser definida como "a habilidade de uma rede em prover um melhor serviço para determinados tráfegos de rede em tecnologias que incluem *Frame Relay*, *Asyncrhonous Transfer Mode*, *Ethernet*, *SONET*[16] e outras redes com roteamento IP" (Cisco, 2003e). Em *Cisco* (1999) Qualidade de Serviço é definida como sendo "os mecanismos que dão aos administradores de redes a habilidade de controlar o *mix* de banda, atraso, variações no atraso (i.e. *jitter*), e perdas de pacotes em redes para oferecer serviços como Voz sobre IP, definir diferentes acordos de níveis de serviços (i.e. *Service-Level Agreements – SLA's*) para divisões, aplicações ou organizações; ou simplesmente priorizar tráfego em uma rede WAN (i.e. *Wide Area Network*)". Em resumo, Qualidade de Serviço pode ser definida como um conjunto de recursos ou ferramentas que permitem que se possa prover um melhor serviço a determinados fluxos de dados em detrimentos de outros. Isso pode ser feito tanto aumentando a prioridade de um ou mais fluxos como limitando a prioridade de outros.

Tradicionalmente, as redes IP sempre forneceram um serviço do tipo "melhor esforço" (i.e. *best effort*[17]). Neste tipo de serviço não existe qualquer garantia ou reserva de recursos para qualquer tipo de tráfego da rede. Existe apenas uma classe de serviços e os pacotes[18] são enfileirados conforme vão chegando para a transmissão. Os diferentes fluxos de dados, provenientes dos diferentes pontos da rede, compartilham entre si a largura de banda disponível para transmissão. Se houver congestionamentos, pacotes são descartados sem distinção. Para atender os requisitos de aplicações variadas como *video*

[16] Padrão de transmissão em rede ótica.
[17] Melhor Esforço: tipo de serviço no qual a rede não oferece quaisquer garantias quanto à qualidade.
[18] Unidade de dados de nível 3 do protocolo IP.

streams[19], Voz sobre IP, *e-commerce*[20], ERP (i.e. *Enterprise Resource Planning*) e outros, torna-se imperativa a implementação de Qualidade de Serviço (i.e. *Quality of Service - QoS*) nas redes modernas. Os mecanismos de Qualidade de Serviço fornecem ferramentas que permitem criar classes distintas de serviços, possibilitando oferecer serviços melhores para determinados fluxos de dados. Dessa forma, é possível que apenas os pacotes de aplicações menos prioritárias sejam descartados quando a rede se encontra congestionada. Pode-se, também, criar classes de serviços que tenham diferentes níveis de prioridade e garantia de banda dentro da rede, baseadas em critérios definíveis pelo usuário, como tipo da aplicação, endereços de origem e destino e muitos outros. Estes critérios podem variar muito em função dos serviços e protocolos a serem transportados pela rede. Recomenda-se que um fluxo de Voz sobre IP (i.e. *VoIP – Voice over IP*), por exemplo, tenha uma variação no atraso (i.e. *jitter*) bastante baixo, um atraso (i.e. *delay*[21]) de no máximo 100 ms e banda garantida na faixa de 8 a 64 kbps, a depender do *codec*[22] utilizado. Um certo nível de perda de pacotes é tolerável neste tipo de tráfego. Por outro lado, uma transmissão de arquivo baseada em FTP (i.e. *File Transfer Protocol*[23]), por exemplo, em geral não tem requisitos muito rigorosos relativos a atraso e a sua variação, mas perdas de pacotes podem afetar fortemente a aplicação e a vazão da rede.

3.2 Modelos de Qualidade de Serviço

Existe uma grande variedade de ferramentas e recursos para prover *QoS* em redes IP. O IETF[24] (i.e. *Internet Engineering Task Force*) padronizou dois modelos básicos para obtenção de Qualidade de Serviço: o modelo de Serviços Integrados (i.e. *IntServ*) e o modelo de Serviços Diferenciados (i.e. *DiffServ*).

3.2.1 O modelo Serviços Integrados (*IntServ*)

O modelo de Serviços Integrados (i.e. *IntServ*) é caracterizado pela reserva dos recursos. O protocolo RSVP (i.e. *Resource Reservation Protocol*) (IETF, 1997a) é o principal elemento deste modelo, em que os equipamentos da rede trocam mensagens

[19] Fluxo de dados gerados por uma transmissão de vídeo.
[20] Comércio Eletrônico – Qualquer forma de comercialização realizada eletronicamente por uma rede de computadores.
[21] Atraso fim-a-fim em uma transmissão de dados em uma rede.
[22] Algoritmo de codificação e decodificação usado na conversão de áudio e/ou vídeo analógico em informação digital, geralmente com a aplicação de técnicas de compressão.
[23] Protocolo de transmissão de arquivos da pilha TCP/IP

para a alocação dos recursos necessários para garantir a Qualidade de Serviço desejada para um determinado fluxo de dados. Cada fluxo na rede tem seus requerimentos de recursos sinalizados e reservados através do RSVP. Um fluxo pode ser identificado de forma individualizada por um conjunto de cinco características: endereço IP de origem, porta TCP/UDP[25] (i.e. *User Datagram Protocol*) de origem, endereço IP de destino, porta TCP/UDP de destino, e protocolo de transporte.

Dois tipos de serviços podem ser reservados via RSVP, assumindo-se que toda a rede, da origem ao destino, suporte este protocolo. O primeiro tipo é um serviço com garantias bastante rigorosas. Chamado de Serviço Garantido, ele é definido pela RFC[26] (i.e. *Request for Comments*) 2211 (IETF, 1997b) e provê limites rígidos relativos a atrasos fim-a-fim e reserva de banda. O segundo tipo, também definido pela RFC 2211 (IETF, 1997), é chamado de Serviço de Carga Controlada, e provê um serviço diferenciado em relação ao tradicional melhor esforço (i.e. *best effort*) em condições de carga de rede de leve a moderada. Dessa forma é possível prover a Qualidade de Serviço (i.e. *QoS*) requerida por cada fluxo em uma rede, desde que ele seja sinalizado pelo RSVP e que haja recursos na rede.

3.2.1.1 Limitações do modelo IntServ

O modelo *IntServ* apresenta algumas limitações que devem ser levadas em consideração ao se avaliar sua implementação:

- todos os dispositivos no caminho dos pacotes, incluindo-se aí os dispositivos finais, como servidores e PC's, devem suportar o protocolo RSVP e serem capazes de sinalizar seus requisitos de *QoS*;

- as reservas em cada dispositivo ao longo do caminho devem ser re-confirmadas periodicamente. Isto aumenta o tráfego na rede e cria a possibilidade de que a reserva expire se os pacotes de re-confirmação forem perdidos. Apesar de existirem alguns mecanismos que aliviem estes problemas, isto aumenta a complexidade da solução RSVP;

---

[24] Órgão regulador da Internet.
[25] Protocolo de nível 4 (transporte) em que não há garantias de entrega dos pacotes.
[26] Documento de padronização da IETF.

- a necessidade de manter as reservas em cada roteador da rede, aliado aos mecanismos de controle de admissão necessários em cada roteador, aumenta a complexidade de cada nó da rede e provoca maiores requisitos de memória e processador para que os mesmos possam suportar um grande número de reservas.

3.2.2 O modelo *DiffServ*

O modelo de Serviços Diferenciados (i.e.*DiffServ*) implementa *QoS* baseado na definição de tipos de serviços. Este modelo estabelece diferentes classes de serviços que têm tratamentos diferenciados nos nós que compõe a rede. O IETF publicou, no final de 1998, a RFC 2475 (IETF, 1998b), definindo este modelo com o objetivo de possibilitar um método relativamente simples e comum de se prover classes diferenciadas de serviços para o tráfego na Internet, que pudesse ser suportado com total interoperabilidade por domínios e fabricantes diferentes.

O funcionamento do modelo *DiffServ* está baseado em dois principais elementos: a marcação de pacotes, fazendo uso do byte de ToS (i.e. *Type of Service*) do IPv4 e os *Per Hop Behaviors* (i.e. *PHBs*).

3.2.2.1 Marcação dos pacotes

O Campo ToS foi definido originalmente como indicado na figura 3.1. Os três bits de precedência seriam usados primordialmente para a marcação de pacotes nas bordas das redes com uma das combinações mostradas na figura, conforme a RFC 1122 (IETF, 1989). A RFC 791 (IETF, 1981) definiu que cada pacote receberia um dos dois níveis de atraso, vazão e confiabilidade. A RFC 1349 (IETF, 1992), no entanto, redefiniu estes três bits e adicionou um sétimo bit no byte, desta forma designando um ToS ao pacote, em adição a sua prioridade.

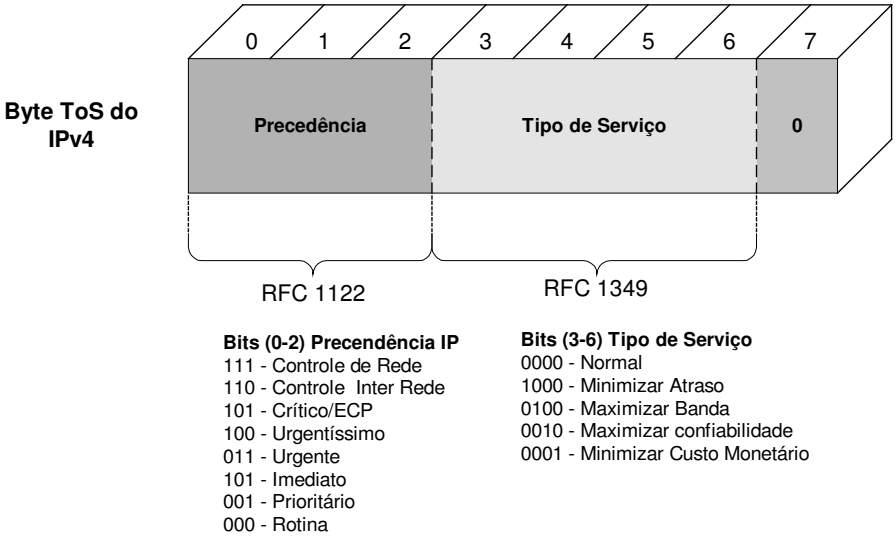

Figura 3.1 – O byte ToS original no IPv4 (fonte: IETF)

A utilização unicamente do campo ToS e de precedência IP (i.e. *IP Precedence*) nunca foi implementada de forma consistente por todos os fabricantes de equipamentos e aplicativos, impedindo a total interoperabilidade da solução. Além disso, a reduzida combinação desses bits limitava a quantidade de classes que se podia implementar com eles. Assim, a RFC 2474 (IETF, 1998a) redefiniu completamente o byte ToS de forma a criar o campo *DiffServ*. Seis bits são agora usados na marcação dos pacotes (figura 3.2) e dois bits ficaram reservados para utilização futura. Os seis bits substituem os três bits da Precedência IP e o ToS e são agora chamados de *Differentiated Services Codepoints* (i.e. *DSCP*) ou Codificação de Serviços Diferenciados. Dessa forma, 64 diferentes classes de serviços (i.e. 2^6) podem ser suportadas em um dado nó da rede permitindo uma granularidade muito maior na classificação dos pacotes. A padronização da codificação *DiffServ* foi estabelecida de forma a se manter a compatibilidade com o modelo de *IP Precedence*. Dessa forma, os três primeiros bits devem ser configurados como no modelo anterior e pacotes marcados apenas com *IP Precedence* são mapeados para o novo modelo, conforme veremos a seguir.

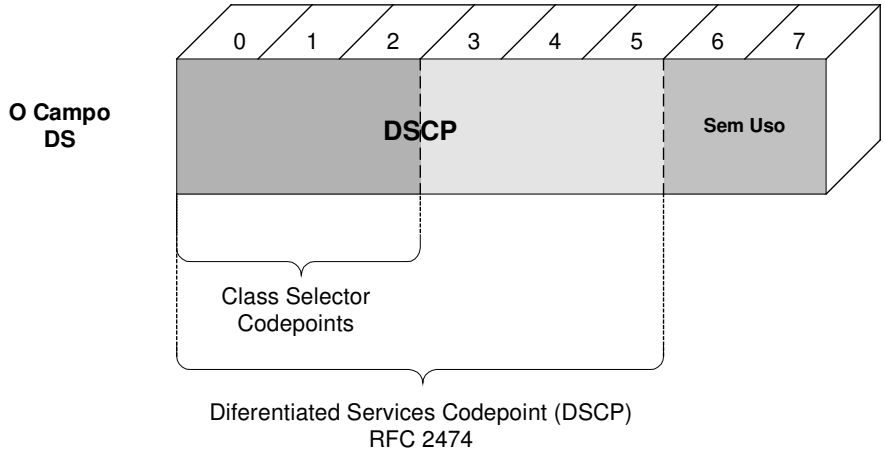

Figura 3.2 – O campo *DiffServ* (fonte: IETF)

3.2.2.2 *Per Hop Behaviors*

Uma vez que os pacotes tenham sido marcados através do campo DS, é necessário agora que tenhamos uma forma de processar os fluxos e prover a *QoS* que cada um deles requer. Uma coleção de pacotes, com um mesmo valor de DSCP, cruzando a rede em uma direção específica é chamada de *Behavior Aggregate* (i.e. *BA*) ou Agregado de Comportamento. Dessa forma, pacotes de múltiplas aplicações e origens podem fazer parte de um mesmo BA. Formalmente, a RFC 2475 (IETF, 1998b) define um PHB como sendo um comportamento (i.e. *Behavior*) aplicado em um nó *DiffServ* a um BA (i.e. *Behavior Aggregate*) *DiffServ*. Em termos mais concretos, um PHB refere-se ao escalonamento, enfileiramento, policiamento ou conformação de tráfego em um nó dado a um pacote pertencente a um BA na forma em que foi configurado. Atualmente quatro PHB padronizados estão disponíveis para se construir redes compatíveis com a especificação *DiffServ*.

3.2.2.2.1 *PHB* Padrão (*Default PHB*)

Definido na RFC 2474 (IETF, 1998a), o PHB padrão define que um pacote marcado com o valor DSCP ‘000000’ obtenha o tradicional serviço de melhor esforço. Adicionalmente é definido que se um pacote chega a um nó *DiffServ* sem nenhuma codificação PHB ele será mapeado para o PHB padrão.

3.2.2.2.2 *PHBs Class-Selector*

Também definido na RFC 2474 (IETF, 1998a), estes PHBs definem a compatibilidade com o modelo de Precedência IP. Dessa forma, valores de DSCP com o formato 'xxx000' (onde x pode ser 0 ou 1) tem seu comportamento definido da mesma forma que no modelo anterior de Precedência IP. Assim sendo, um pacote com DSCP '110000', por exemplo, (i.e. *IP Precedence* 110) tem prioridade sobre um pacote com DSCP '100000' (i.e. *IP Precedence* 100). Estes PHBs permitem a co-existência de nós que implementam DS e nós com somente Precedência IP.

3.2.2.2.3 *PHB Expedited Forwarding (EF)*

Assim como o RSVP, que no modelo *IntServ* provê um serviço com banda garantida, o PHB EF, definido na RFC 2598 (IETF, 1999c), permite, no modelo *DiffServ*, obter-se um serviço com baixa perda, baixa latência[27], baixa variação do atraso e banda garantida, ideal para aplicações como Voz sobre IP, vídeo e outras que necessitem este tipo de garantia. A codificação DS recomendada para este PHB é '101110'.

3.2.2.2.4 *PHB Assured Forwarding (AF)*

O equivalente, no *DiffServ*, ao Serviço de Carga Controlada do *IntServ*, é o PHB AF (IETF, 1999b). Ele define um método pelo qual BA's podem receber diferentes garantias de encaminhamento. Por exemplo, o tráfego pode ser dividido em classes que poderiam ser chamadas de ouro, prata, bronze e platina, em que a classe ouro poderia receber 40% da banda disponível no enlace, a classe prata 30%, a classe bronze 20% e a classe Platina 10%. O PHB AF define quatro classes padrão: AF1, AF2, AF3 e AF4. A cada uma delas é destinado uma certa quantidade de espaço em *buffer*[28] e banda na interface, de acordo com o SLA com o provedor de serviços ou a política aplicada. Além disso, são definidas três precedências de descarte (i.e. *drop precedence*) resultando na combinação de valores mostrada na tabela 3.1.

[27] Retardo, *delay.*
[28] Local de armazenamento temporário de dados a serem transmitidos em uma inteface.

Tabela 3.1: Codificação *DiffServ* PHB AF

Precedência de Descarte	Classe 1	Classe 2	Classe 3	Classe 4
Baixa Precedência de Descarte (DSCP)	AF11 001010 (10)	AF21 010010 (18)	AF31 011010 (26)	AF41 100010 (34)
Média Precedência de Descarte (DSCP)	AF12 001100 (12)	AF22 010100 (20)	AF32 011100 (28)	AF42 100100 (36)
Alta Precedência de Descarte (DSCP)	AF13 001110 (14)	AF23 010110 (22)	AF33 011110 (30)	AF43 100110 (38)

Fonte: Cisco Systems Inc.

3.2.2.3 A arquitetura *DiffServ*

Um domínio *DiffServ* é composto de Nós de Entrada DS (i.e. *DS Ingress Nodes*), nas bordas da rede, Nós Internos DS (i.e. *DS Interior nodes*) no núcleo e Nós de Saída DS (i.e. *DS Egress Nodes*), também nas bordas (figura 3.3).

Os Nós de Entrada e de Saída podem ser chamados de Nós de Fronteira (i.e. *Boundary Node*). Os Nós de Fronteira executam o condicionamento do tráfego, classificando os pacotes de entrada em agregados pré-definidos, medindo o tráfego para certificar-se de que ele está de acordo com os parâmetros determinados, marcando os pacotes através dos campos de DSCP e, finalmente, condicionando ou descartando os pacotes em caso de congestionamento. Um nó interno força um determinado PHB aplicando técnicas de policiamento ou de modelagem de tráfego, dependendo do SLA ou *policy-map* aplicado.

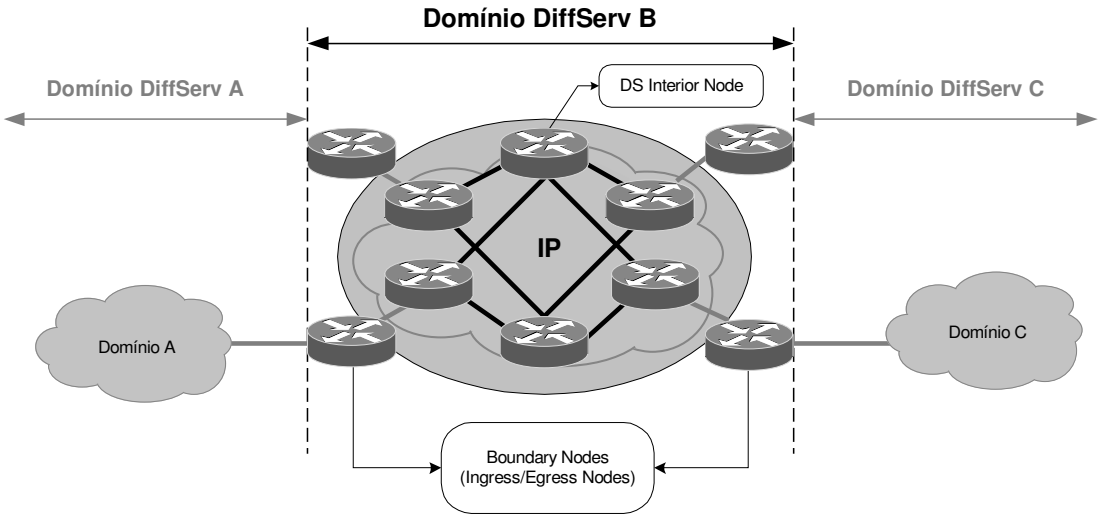

Figura 3.3 – A arquitetura *DiffServ*

3.3 Recursos de Qualidade de Serviço

Diversos são os recursos presentes nos equipamentos de rede (i.e. roteadores) que possibilitam a obtenção de Qualidade de Serviço. Alguns deles são mais genéricos e podem ser encontrados em praticamente todas as plataformas de roteadores. Outros já são mais específicos, tendo sido criados ou implementados de forma proprietária por alguns fabricantes. A seguir serão apresentados os recursos mais comuns e os que são específicos da plataforma *Cisco*, que foi utilizada no projeto abordado por este estudo.

Os recursos e ferramentas disponíveis para obtenção de *QoS* podem ser classificados em seis categorias principais, conforme abaixo (CISCO, 2002c):

1. Classificação e marcação;
2. Prevenção de congestionamento;
3. Controle de congestionamento;
4. Condicionamento e policiamento de tráfego;
5. Mecanismos de eficiência de enlace.

É importante que se note que nem todos estes mecanismos e ferramentas podem ser necessários em uma implementação que demande Qualidade de Serviço. Quais e quantos serão os recursos utilizados irá depender do perfil e das necessidades da rede e,

principalmente, de quais garantias se pretende oferecer para o tráfego que irá fluir por ela. A seguir são detalhados cada um desses recursos.

3.3.1 Classificação e marcação

A classificação de pacotes permite que o tráfego possa ser segregado em múltiplos níveis de prioridade ou classes de serviços. Os pacotes classificados podem ser marcados de diferentes formas, tanto no nível 2 como no nível 3 da rede. No nível 3 (i.e. IP) os pacotes podem ser marcados através do uso dos bits de *IP Precedence* e do DSCP, conforme já discutido anteriormente neste capítulo. Os métodos para marcação e classificação de pacotes em um roteador *Cisco* podem incluir a utilização de listas de controle de acesso (i.e. *access control lists*[29] ou ACLs), roteamento baseado em policiamento (i.e. *policy-based routing*[30]), taxa de acesso consolidado (i.e. *commited access rate*[31] - CAR) e reconhecimento de aplicação baseado em rede (i.e. NBAR – *network-based application recognition*[32]).

3.3.2 Controle de congestionamento

Algoritmos de prevenção de congestionamento fornecem uma forma de se tentar prevenir a ocorrência de situações de congestionamento, fazendo o descarte seletivo de pacotes à medida que aumentam os tamanhos das filas nos *buffers* de saída. Sem a utilização desses algoritmos, é comum acontecer o que se costuma chamar de ondas de congestionamento.

O protocolo de transporte TCP trabalha com um mecanismo de janela que faz com que a taxa de transmissão seja reduzida conforme deixem de ser confirmados pacotes que foram enviados, o que indicaria uma possível perda de pacotes devido a descarte gerado por congestionamento da rede. O que pode ocorrer, no entanto, é que várias fontes de tráfego sintam esta condição da rede e diminuam suas janelas de transmissão[33] ao mesmo tempo, o que faz com que o congestionamento seja

[29] Listas usadas em um roteador para controlar a admissão a um determinado serviço.
[30] Roteamento de pacotes tomando por base políticas configuradas no roteador. Em geral utilizadas para dar tratamento especial a determinados tipos de pacotes ou fluxos.
[31] Limitação da taxa de transmissão a um valor pré-determinado, condicionada a fatores e características associadas ao tráfego sendo transmitido.
[32] Recurso de reconhecimento automático de protocolos sendo transmitidos pela rede.
[33] Quantidade de dados que é transmitida antes que haja uma confirmação do recebimento pelo destinatário.

momentaneamente aliviado. Com isso, os transmissores voltam a aumentar suas janelas de transmissão, todos ao mesmo tempo, e um novo congestionamento ocorre.

Outro inconveniente da situação de congestionamento é que, quando as filas dos *buffers* de saída das interfaces ficam cheias, ocorre o descarte de pacotes pelo final da fila (i.e. *tail drop*). Dessa forma, um único fluxo pode ser mais severamente prejudicado, enquanto outros não são afetados. Para tentar evitar estes problemas foi criado o algoritmo RED (i.e. *Random Early Detect*). Este algoritmo monitora o tamanho da fila e passa a fazer descartes aleatórios de pacotes antes que a mesma fique cheia. Com isso, o congestionamento tem maiores chances de ser prematuramente evitado e os descartes afetam os fluxos de forma mais justa. O RED, no entanto, apresenta o inconveniente de descartar pacotes de forma indiscriminada, sem levar em consideração o nível de prioridade dos mesmos. Para se obter um descarte mais seletivo de pacotes em uma situação de congestionamento, criou-se o WRED (i.e. *Weighted Randon Early Detection*).

O WRED alia às funções do RED as funcionalidades do *IP Precedence*. Basicamente o que este algoritmo faz é dar pesos aos pacotes de acordo com a classificação de Precedência IP de cada um, de forma que eles tenham maior ou menor probabilidade de serem descartados em uma situação de congestionamento. Com isso, consegue-se fazer com que os fluxos menos prioritários tenham um descarte maior de pacotes em relação a fluxos mais prioritários. Uma outra variante deste algoritmo, criada pela *Cisco*, é o *Flow-based* WRED, ou WRED baseado em fluxos. Neste caso os pacotes são classificados em fluxos baseado nos endereços IP e portas TCP de origem e destino e, assim, pode-se fazer o descarte prioritário de pacotes de um fluxo que esteja gerando tráfego excessivo em relação a limites previamente estabelecidos. Dessa forma, aplicações mal comportadas podem ser mais fortemente afetadas no momento em que os pacotes precisem ser descartados, beneficiando as aplicações mais bem comportadas.

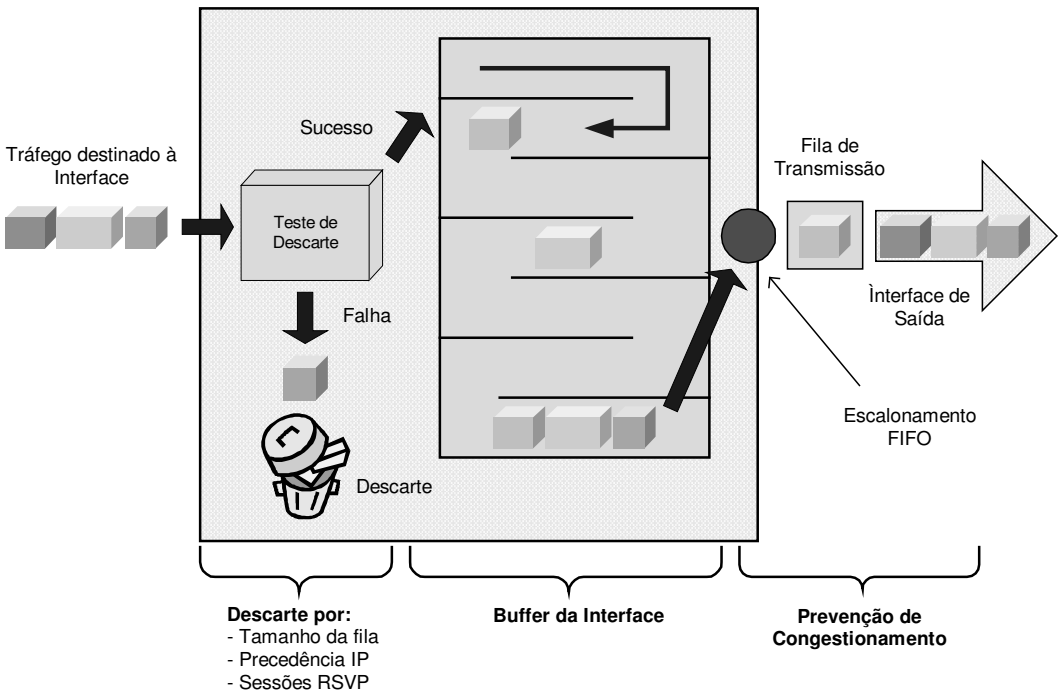

Figura 3.4 – O mecanismo WRED (fonte: *Cisco Systems Inc.*)

3.3.2.1 Técnicas de escalonamento

Ao chegar em uma interface de saída de um roteador para serem transmitidos, os pacotes de um fluxo de dados entram em uma fila que tem um algoritmo que define em que ordem estes pacotes serão encaminhados pela interface.

Diferentes técnicas de escalonamento podem ser utilizadas conforme o tipo de tráfego a ser transmitido, de forma a suprir a necessidades específicas de diferentes usuários. A seguir veremos as principais técnicas genéricas de escalonamento, e as que foram desenvolvidas especificamente pela *Cisco Systems* para uso em seus equipamentos:

3.3.2.1.1 Fila *First-in, First-out (FIFO)*

Neste tipo de fila os pacotes saem na mesma ordem que chegam na interface. Não há como se priorizar pacotes de maior importância ou urgência na rede, por isso mesmo este enfieliramento não é adequado para implementações de Qualidade de Serviço (figura 3.5).

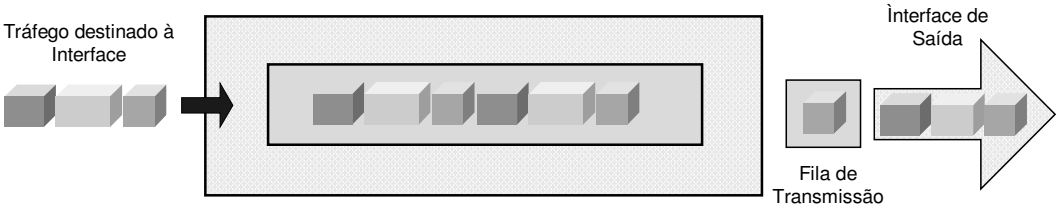

Figura 3.5 – Fila FIFO

3.3.2.1.2 Fila *Priority Queueing (PQ)*

No escalonamento *Priority Queueing* (i.e. *PQ*), os dados são colocados em vários níveis de prioridade, que poderiam ser, por exemplo, alta, média, normal e baixa. Pacotes que não são classificados em nenhum dos níveis de prioridade, são tratados pela fila normal. Neste tipo de fila, os pacotes de menor prioridade somente são transmitidos quando não há mais dados nas filas mais prioritárias (figura 3.6). Assim, apesar de se constituir uma boa opção para alguns tipos de perfil de tráfego, especialmente pela simplicidade de implementação, este escalonamento não é adequado a fluxos de mídias contínuas, como voz e vídeo, já que tráfegos menos prioritários poderiam sofrer muito fortemente ao competir com estes fluxos (i.e. *starvation*). O documento *Configuring Priority Queuing* (Cisco, 2002e) traz os detalhes de como se configurar este tipo de escalonamento em um roteador *Cisco*.

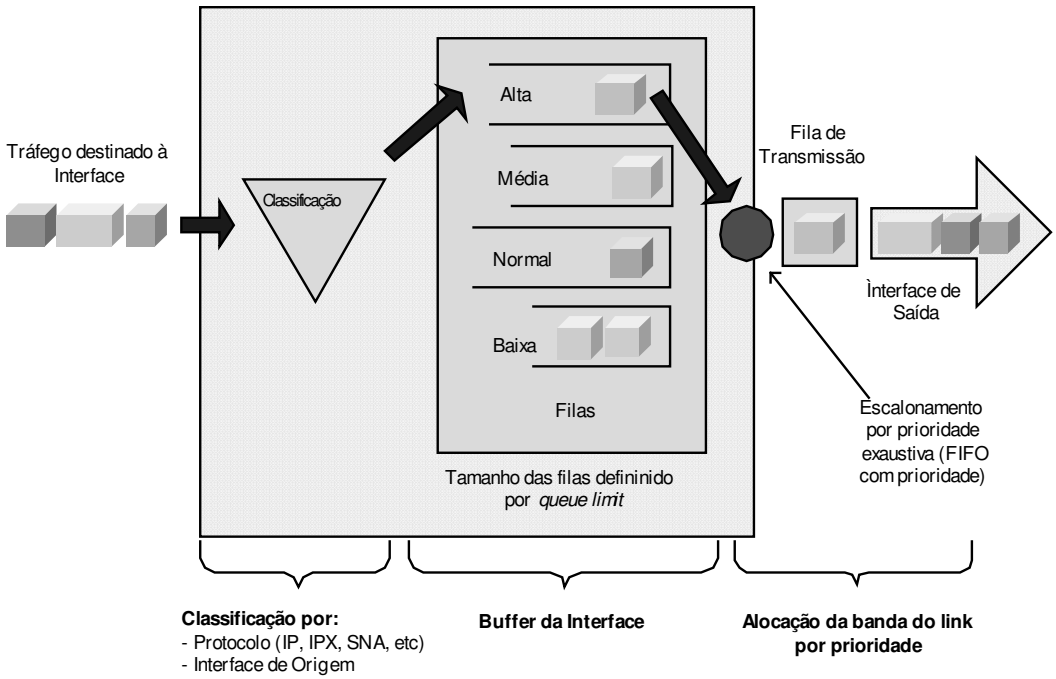

Figura 3.6 – *Priority Queueing* (fonte: *Cisco Systems Inc.*)

3.3.2.1.3 Fila *Custom Queuing (CQ)*

Neste algoritmo de escalonamento, criado pela *Cisco*, é possível garantir banda para um ou mais fluxos de dados. Isso é conseguido definindo-se um tamanho de fila para cada tipo de tráfego, até um máximo de 16 filas (figura 3.7). O roteador então serve as filas em *round-hobin*[34], transmitindo um percentual configurado de tráfego, antes de mudar para a fila seguinte. Dessa forma, garante-se o percentual desejado de banda para cada um dos fluxos, evitando-se a monopolização da banda que pode ocorrer na *Priority Queue*.

Este tipo de fila também não é adequado ao tráfego de voz e vídeo, pois, apesar de ser possível a garantia de banda para estas aplicações, não é possível se garantir níveis de atraso e variação do mesmo. Em *Configuring Custom Queuing* (Cisco, 2002f) pode-se ver como este tipo de fila pode ser implementado em roteadores *Cisco*.

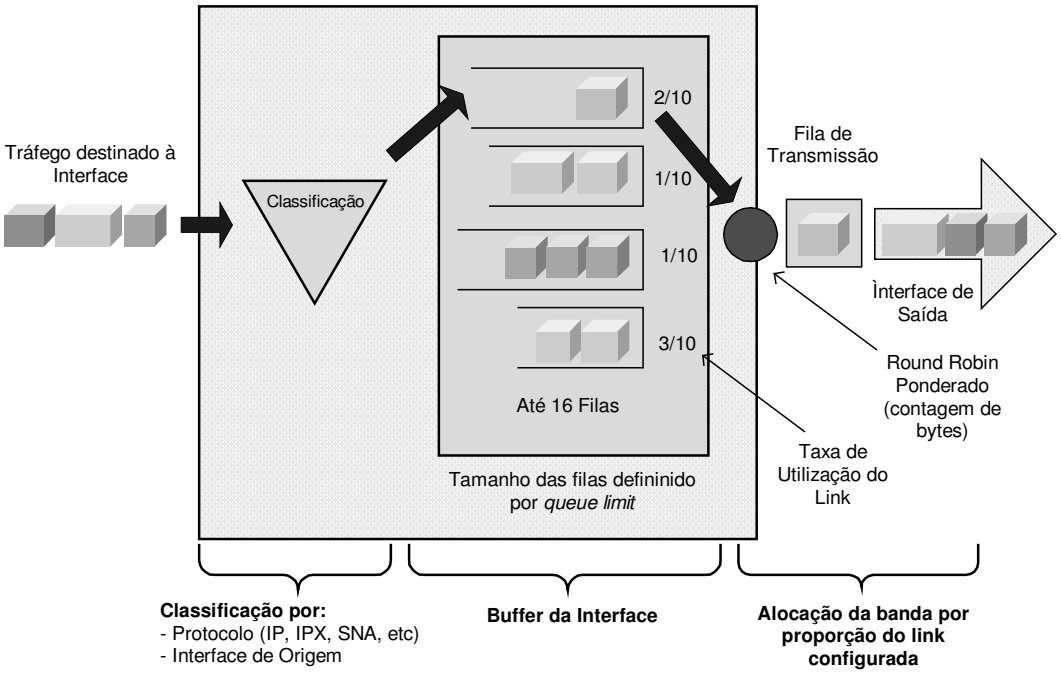

Figura 3.7 – *Custom Queuing* (fonte: *Cisco Systems Inc.*)

[34] Modo de organização de escalonamento em que a cada elemento é dada uma porção do tempo ou recurso de forma circular.

3.3.2.1.4 Fila *Weighted Fair Queueing (WFQ)*

Em roteadores *Cisco*, este é o tipo padrão de escalonamento para interfaces com velocidades menores que 2048 kbps (i.e. E1). Esta técnica de escalonamento proporciona uma distribuição mais justa da banda disponível entre os diversos fluxos de dados, identificados por seus endereços IP de origem e destino e portas TCP. Em roteadores *Cisco,* o algoritmo WFQ atribui um peso para cada fluxo, e serve estes fluxos a depender do peso de cada um deles (figura 3.8). Uma vantagem do WFQ é que seu algoritmo leva em conta a precedência IP dos fluxos, servindo de forma prioritária os pacotes com maior valor de precedência. Além disso, marcações feitas pelo protocolo RSVP e pelos indicadores de congestionamento *Frame Relay* DE, BECN e FECN também são levados em consideração no estabelecimento de pesos para os fluxos. Desta maneira é possível fazer com que fluxos que estejam enfrentando congestionamento, por exemplo, possam ser atendidos com uma menor freqüência em relação aos outros (Cisco, 2002g).

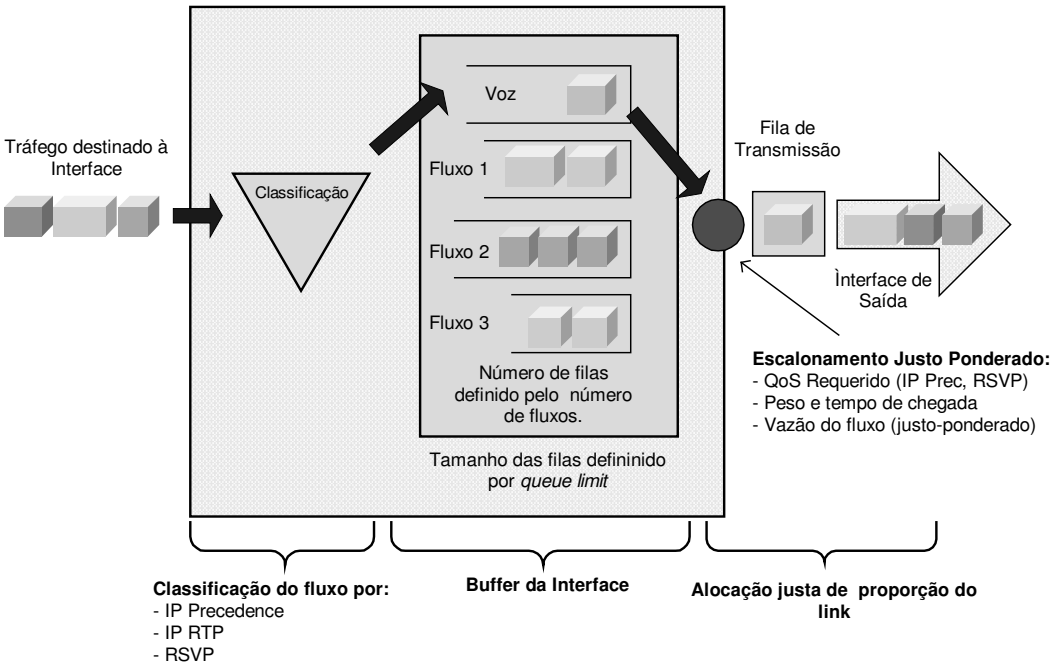

Figura 3.8 – ***Weighted Fair Queueing*** **(fonte:** ***Cisco Systems Inc.*****)**

Apesar de não ser a técnica de escalonamento mais adequada para o transporte de tráfego do tipo interativo, a WFQ pode ser usada com este objetivo quando nenhuma outra opção estiver disponível.

3.3.2.1.5 Fila *Class-Based WFQ (CB-WFQ)*

Neste tipo de fila o administrador da rede determina quanto da banda (em percentual ou em valores absolutos) será destinado para cada classe de tráfego. Os pacotes podem ser classificados por métodos que podem incluir o tipo de protocolo, listas de acesso, interface de origem, etc (figura 3.9).

Este é um dos tipos mais flexíveis de técnicas de escalonamento. Por não ser tão simples de implementar, no entanto, é recomendado apenas quando os requisitos de Qualidade de Serviço o exijam.

Apesar de prover garantia de banda, esta técnica não garante os parâmetros de atraso e variação do atraso e, portanto, não é adequada para tráfego de mídia contínua (e.g. voz e vídeo). Uma variação deste tipo de fila, o *Low Latence Queueing* (i.e. LLQ ou *Priority Queuening CBWFQ*), vista mais adiante, é a mais indicada para este tipo de fluxo. Maiores detalhes sobre a implentação deste tipo de escalonamento podem ser encontrados em *Class-Based Wheighted Fair Queuing* (Cisco, 2002h)

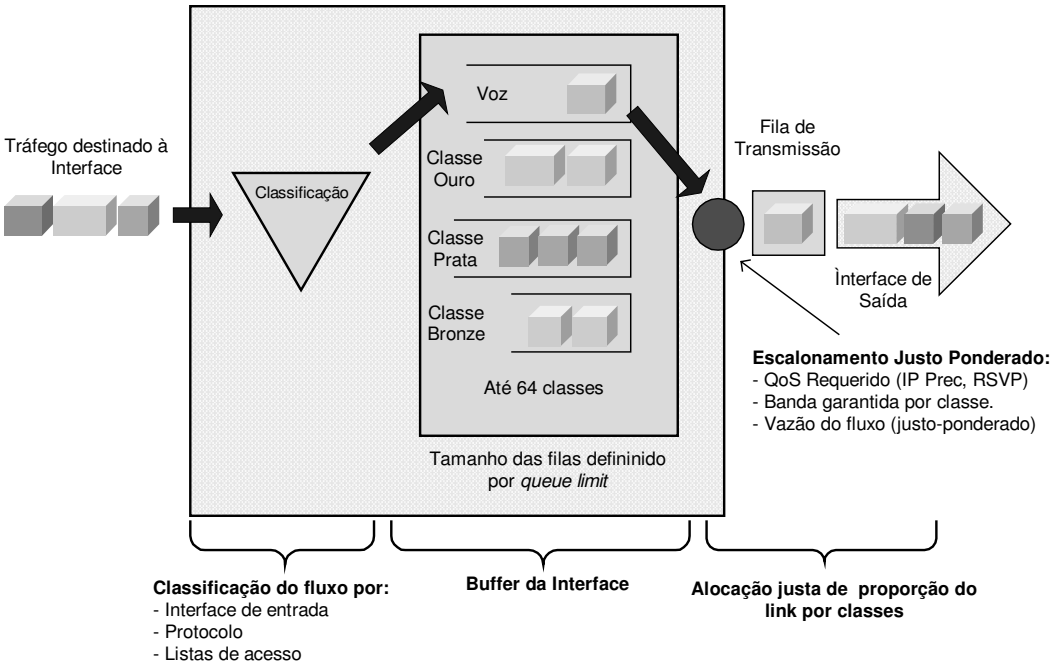

Figura 3.9 – *Class Based WFQ* (fonte: *Cisco Systems Inc.*)

3.3.2.1.6 Fila *Priority Queue WFQ (PQ-WFQ)*

Esta técnica é semelhante ao WFQ, porém adiciona a este uma fila de prioridade (i.e. *Priority Queueing*). O tráfego proveniente da fila prioritária é servido com prioridade exaustiva, enquanto que as demais filas são servidas da mesma forma que no WFQ. Como é possível se configurar um parâmetro de banda para a fila prioritária, evita-se que este fluxo sufoque os demais (Figura 3.10). Funciona bem com interfaces nas quais se tem tráfego interativo em conjunto com tráfego de dados. Apesar de não ser a técnica mais recomendada, pode ser usada para este tipo de tráfego quando não há a opção de se utilizar a LLQ. Este tipo de escalonamento pode ser obtido em um roteador *Cisco* através do comando *IP RTP Priority* (Cisco, 2002i)

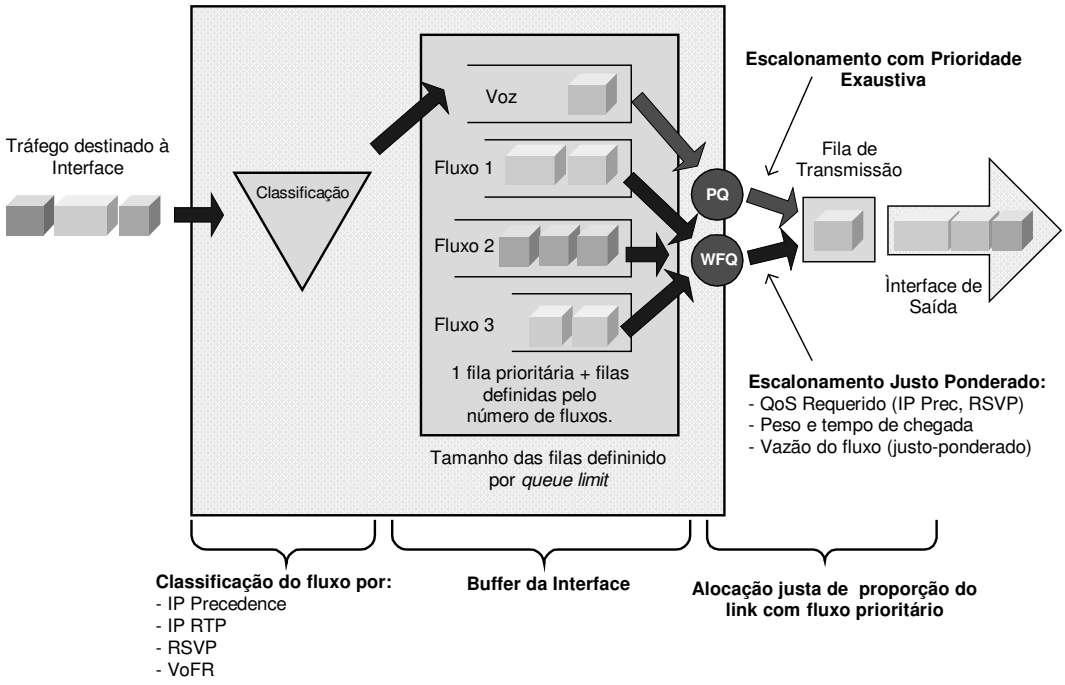

Figura 3.10 – *Priority Queue WFQ* (fonte: *Cisco Systems Inc.*)

3.3.2.1.7 Fila *Low Latence Queueing (LLQ)* ou *Priority Queueing CBWFQ (PQ-CBWFQ)*

Este é o tipo mais recomendado de escalonamento para interfaces que lidam com dados e tráfego interativo em roteadores Cisco. Ele implementa todos os recursos do CBWFQ, visto acima, e adiciona, ainda, uma fila prioritária (i.e. *Priority Queue*) que é tratada com prioridade estrita, garantindo, além de banda, os parâmetros de atraso e varioação do atraso (figura 3.11) (Cisco, 2002j).

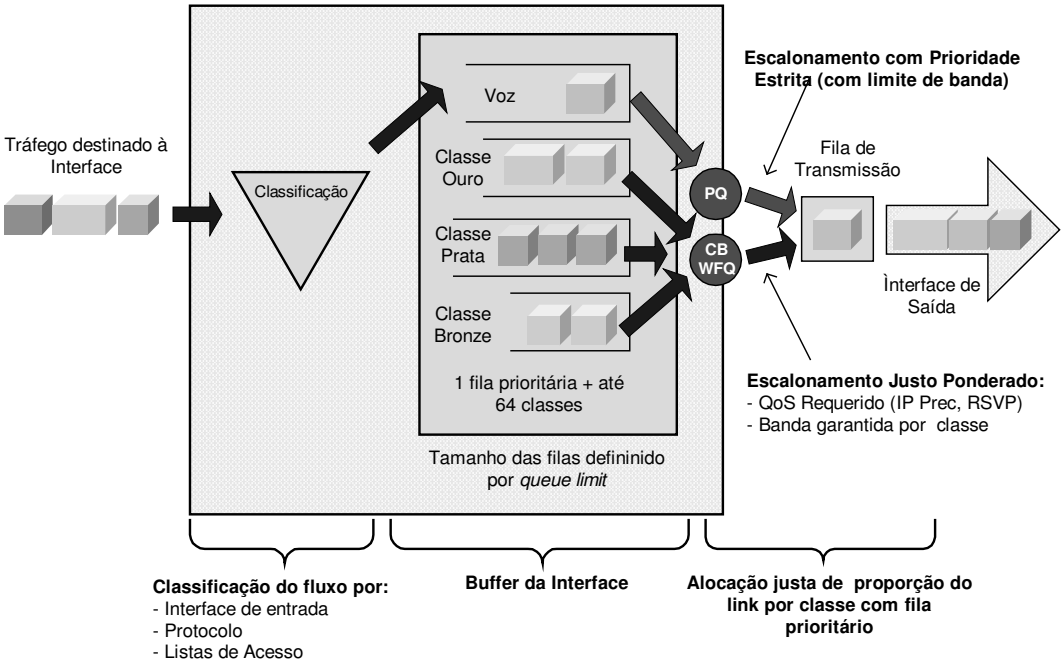

Figura 3.11 – ***Low Latency Queuing*** **(fonte:** ***Cisco Systems Inc.*****)**

3.3.3 Condicionamento e policiamento de tráfego

Mecanismos como *Traffic Shaping* (i.e. Suavização de Tráfego) e *Committed Access Rate* (i.e. *CAR*), podem ser utilizados para limitar e condicionar fluxos de tráfego entrando em uma rede, aumentando o controle e a eficiência na utilização dos enlaces.

3.3.3.1 CAR – *Commited Access Rate*

O recurso de CAR (i.e. *Commited Access Rate*), presente em roteadores *Cisco*, tem como função primária limitar a banda de um determinado fluxo de dados. No entanto, outras funções podem também ser executadas com este recurso. As ações que podem ser tomadas incluem a transmissão ou descarte do pacote, a marcação ou re-marcação do valor do campo *IP Precedence*, entre outras. Essas ações podem ocorrer de forma incondicional ou depender do comportamento de determinado fluxo de tráfego. Um fluxo de dados pode, por exemplo, ter seus pacotes remarcados com um valor de precedência mais baixo toda vez que um valor pré-estabelecido de consumo de banda for atingido. Com isso o CAR constitui-se em uma importante ferramenta para implementação de recursos de *QoS*, atuando como um "policiador".

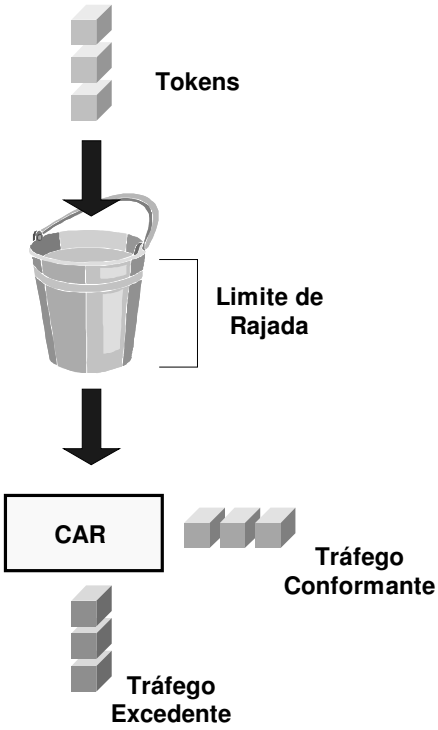

Figura 3.12 – ***Commited Access Rate***

3.3.3.2 Suavização de tráfego

Os recursos de suavização de tráfego (i.e. *Traffic Shaping*) permitem suavizar o fluxo de tráfego a uma taxa especificada com o uso dos *buffers* das interfaces. Os *buffers* são utilizados como um balde furado, que vai liberando o tráfego de forma uniforme, independente de como ele chega a interface (figura 3.13). Isso pode ser útil na transmissão de tráfego interativo, já que ajuda a reduzir variações no atraso e perdas de pacotes, uma vez que evita que o tráfego em rajadas seja descartado. Mecanismos de controle de congestionamento também podem estar disponíveis, no caso de redes *Frame Relay*[35]. Nessas redes, em que existe a possibilidade de congestionamento do meio físico compartilhado, sinalizações de congestionamento (i.e. FECN[36], BECN[37] e DE[38]) podem ser levadas em consideração pelo *Traffic Shaping* para adequar o volume de tráfego às condições da rede.

[35] Protocolo de rede de nível 2 (Enlace).
[36] Sinalização de congestionamento adiante na rede.
[37] Sinalização de congestionamento anterior na rede.
[38] Marcação indicando que o frame pode ser descartado, caso haja congestionamento na rede.

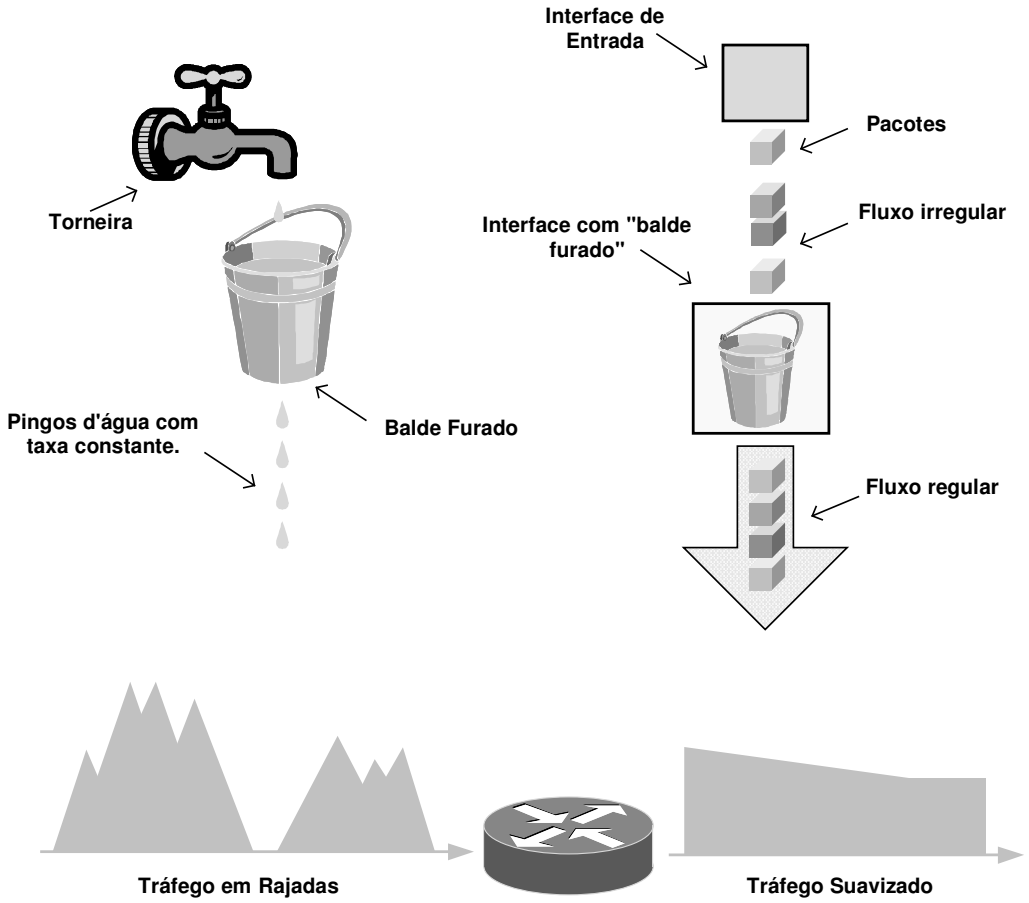

Figura 3.13 – ***Traffic Shaping***

Em uma rede *Frame Relay* alguns parâmetros são negociados entre o cliente e o provedor de serviços. São eles:

- CIR – *Committed Information Rate*: a taxa média de transmissão desejada em um enlace, em kbps. É igual a quantidade BC de dados enviada no intervalo TC de tempo;
- BC – *Burst Committed*: a quantidade de dados a ser enviada no enlace a cada intervalo de TC para satisfazer o limite de CIR;
- BE – *Burst Excess*: a quantidade de dados que é permitida ultrapassar o valor de BC dentro do intervalo de TC. Após esta taxa, os pacotes são marcados com DE (i.e. *Discard Eligibility*), significando que poderão ser descartados em caso de congestionamento da rede;
- TC – *Time Committed*: o intervalo de tempo no qual deve-se enviar BC para se obter a taxa média de CIR.

O gráfico da figura 3.14 ilustra o exemplo de um enlace com BC = 32 kbits, BE = 16 kbits e CIR = 32 kbps, resultando em TC = 1 segundo.

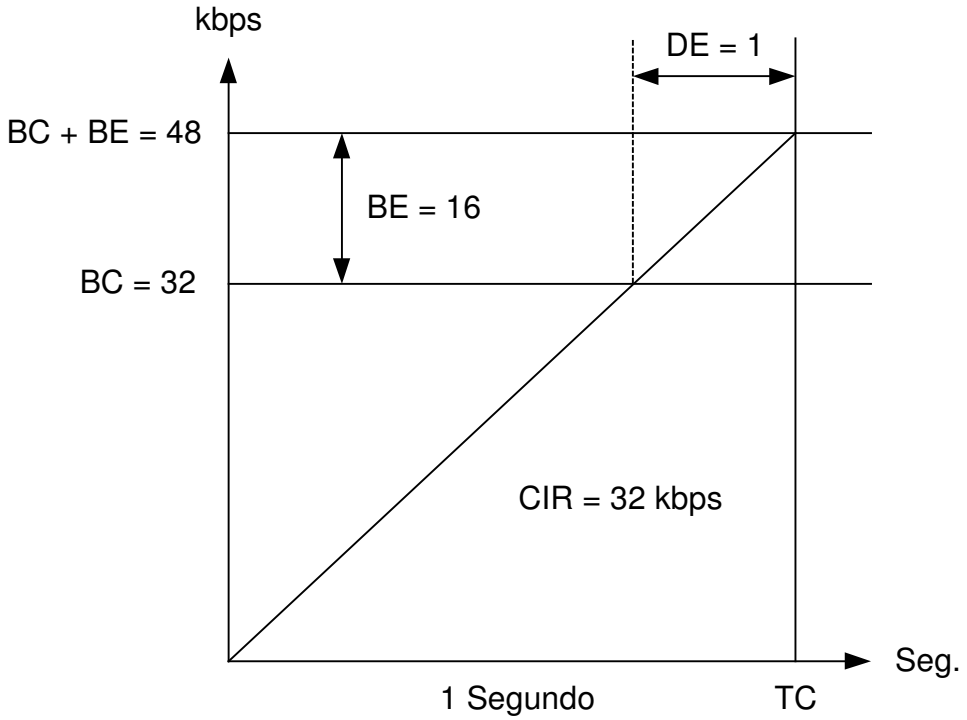

Figura 3.14 – Parâmetros do *Frame Relay Traffic Shaping*

3.3.4 Mecanismos de eficiência de enlace

Mecanismos de compressão de cabeçalhos e de fragmentação[39] e *interleaving*[40] permitem produzir uma grande economia no consumo de banda, mantendo baixos os índices de atraso e variação do atraso em fluxos de mídia contínua. Esses mecanismos incluem a compressão de cabeçalhos de IP, UDP e RTP[41] (i.e. *Real-Time Protocol*) a fragmentação e intercalação de quadros e a fragmentação *Frame Relay Forum 12* (i.e. FRF.12).

3.3.4.1 Compressão de cabeçalhos

Tráfegos de voz e vídeo contínuo utilizam-se do protocolo de tempo real (i.e. RTP). Os cabeçalhos dos pacotes IP, UDP e RTP podem ser compactados de

[39] Divisão de pacotes em tamanhos menores.
[40] Processo de intercalação de pacotes de maior prioridade.
[41] Protocolo de transmissão de tráfego de mídia contínua (voz e vídeo).

aproximadamente 40 bytes para 2 a 5 bytes (IETF, 1999a). Isso proporciona uma grande economia de largura de banda, o que é especialmente importante no caso de enlaces de baixa velocidade e no suporte a um grande número de fluxos de mídia. Esta compressão é classificada como *loss-less*, ou seja, não existe perda de informação no processo de compressão. A compressão é obtida simplesmente com a omissão de campos dos cabeçalhos que se repetem nos diversos pacotes que compõem um fluxo de dados e a utilização de uma codificação diferencial para reduzir o tamanho dos campos que se alteram.

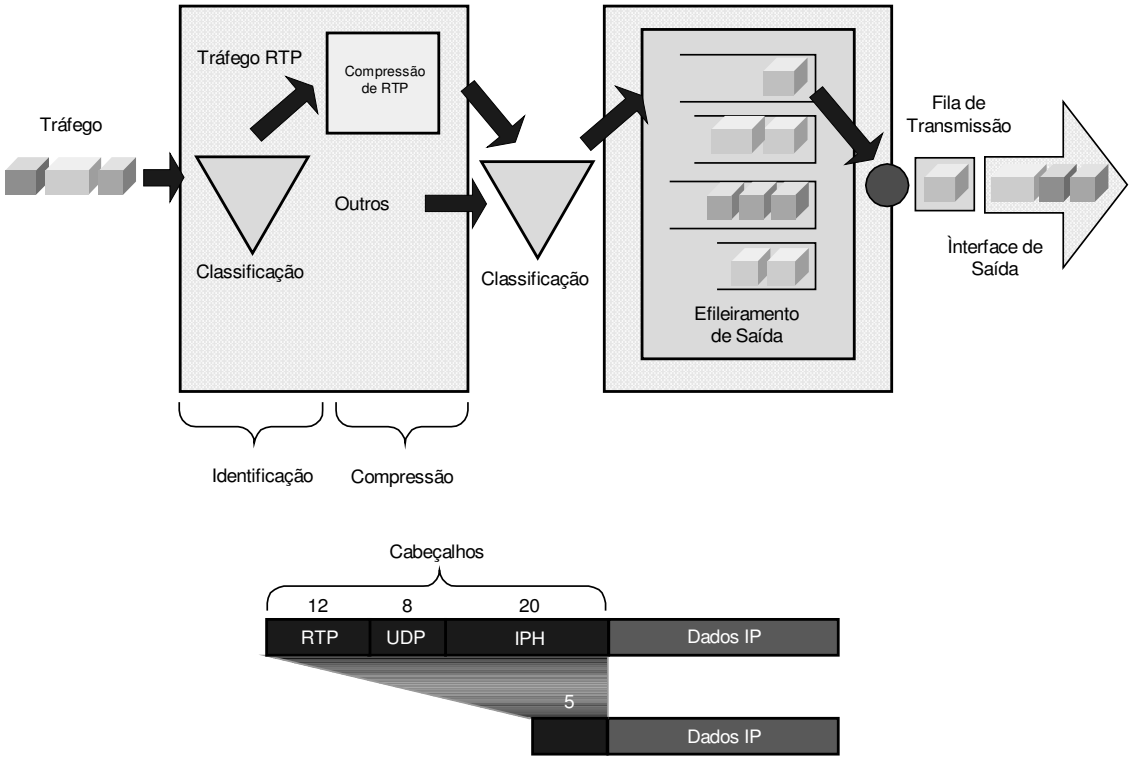

Figura 3.15 – O *RTP Header Compression* (fonte: *Cisco Systems Inc*.)

3.3.4.2 Fragmentação e intercalação de quadros

Tráfegos de mídia contínua exigem que pacotes sejam transmitidos em um fluxo constante, sem grandes variações no atraso entre os mesmos. Mas os tempos de serialização[42] em enlaces de baixa velocidade, associados à presença de pacotes de dados de tamanhos grandes, podem representar um grande problema para a cadência de

[42] Tempo que uma interface leva para transmitir, de forma serial, os dados que lhe são entregues pelo nível superior.

transmissão deste tipo de pacotes. Um pacote de 1500 bytes, por exemplo, leva 214 milisegundos para ser transmitido em um enlace de 56 kbps:

- Tamanho do Pacote: 1.500 bytes * 8 bits/byte = 12.000 bits;
- Taxa de transmissão: 56.000 bps;
- Tempo de transmissão: 12.000 bits / 56.000 bps = 0,214 segundos.

Para que tenha uma boa qualidade de voz em um tráfego de Voz sobre IP, por exemplo, o ITU-T[43] recomenda que um pacote de voz seja transmitido a cada 20 milisegundos, no máximo (ITU-T, 2003). Neste caso, se este pacote de voz entrar na fila após um pacote de dados de 1500 bytes, o tempo que o mesmo terá que esperar para ser transmitido (i.e. 214 milisegundos) poderia comprometer seriamente a qualidade da ligação, a não ser que outras medidas compensatórias fossem tomadas. Dentre estas medidas estaria, por exemplo, a utilização de uma bufferização[44] maior. Neste caso, no entanto, poderia se comprometer o atraso fim-a-fim da comunicação. Outra solução consistiria em se alterar o MTU[45] da rede, mas algumas aplicações IP não se comportam bem quando se reduz muito este parâmetro, além de se introduzir ineficiência e *overhead*[46] ao processador. Para resolver este problema, então, mecanismos de fragmentação e intercalação podem ser utilizados para quebrar os pacotes grandes em outros menores e intercalar os pacotes de tempo real entre os fragmentos dos pacotes maiores (figura 3.16). Além disso, por atuar abaixo da camada 3 do modelo OSI estes mecanismos podem fragmentar também outros tipos de tráfego além do IP, aumentando sua eficiência.

[43] *International Telecommunication Union* – Organização internacional de padronizações em telecomunicações.
[44] Armazenamento temporário de dados em filas de uma interface.
[45] Maior tamanho de pacote que a rede transmite sem fragmentação.
[46] Trabalho extra a ser executado.

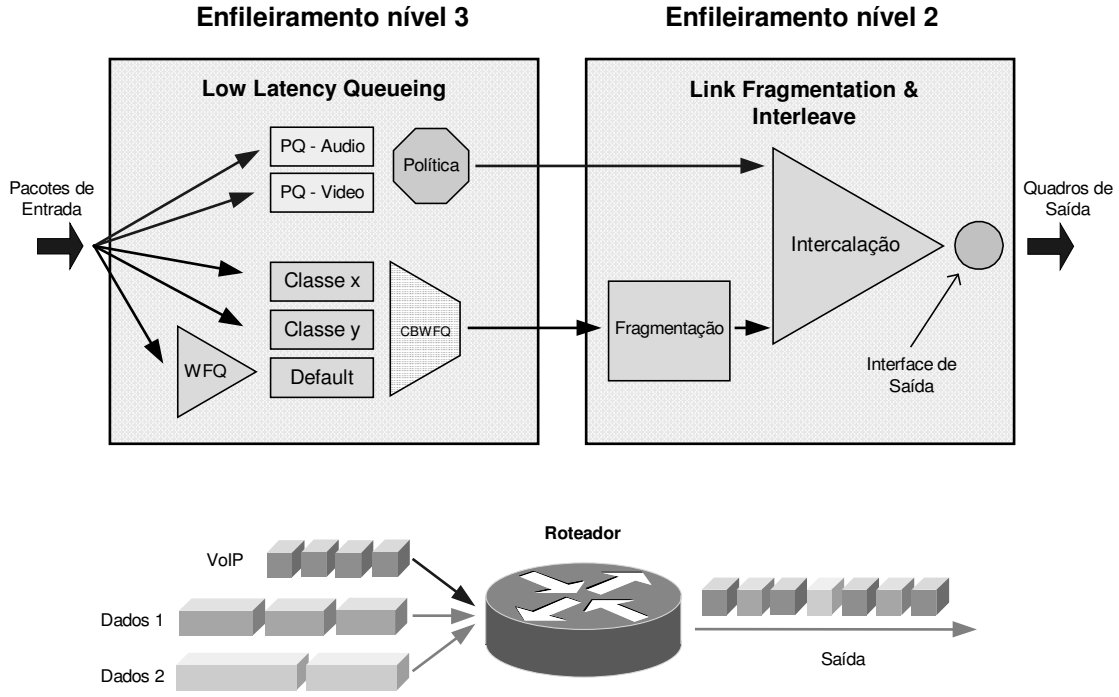

Figura 3.16 – Fragmentação e Intercalação de Pacotes (fonte: *Cisco Systems Inc.*)

Estas funções são exercidas pelo *interleaving* do MLPPP (IETF, 1994), no caso de enlaces utilizando o protocolo PPP[47], e pela Fragmentação *Frame Relay Forum 12* (i.e. FRF.12[48]), em enlaces *Frame Relay*. Em geral os parâmetros destes recursos são configurados de forma a se obter um tempo de serialização na ordem de 10 milisegundos por pacote. Independente do algoritmo de filas adotado no nível 3 do modelo OSI, os roteadores implementam outra fila no nível de interface (camada 2 do modelo OSI). Normalmente esta fila é do tipo FIFO, onde os pacotes são retirados da fila na mesma ordem em que chegam. Os recursos de MLPPP e FRF.12, no entanto, habilitam o uso de *Dual FIFO*[49] ao nível de interface em roteadores *Cisco* (Vegesna, 2000). Assim, após a fragmentação, os pacotes prioritários são colocados em uma fila prioritária, enquanto que outros pacotes (ou seus fragmentos) são colocados em uma fila FIFO comum. Dessa forma a interface pode intercalar os pacotes prioritários entre os fragmentos de um pacote não prioritário de tamanho grande que tenha sido fragmentado, permitindo que o tráfego interativo da fila prioritária seja transmitido com o menor atraso possível.

[47] *Point to point Protocol* – Protocolo de nível 2 na camada OSI.
[48] *FRF.12 Frame Relay Forum Implementation Agreement,* também conhecida como *FRF.11 Annex C.*
[49] Fila Dupla do tipo FIFO, sendo um fluxo prioritário e o outro normal.

3.3.5 Resumo dos recursos de *QoS* na plataforma *Cisco*

Como pode ser visto, são muitos os recursos disponíveis para obtenção de Qualidade de Serviço. A tabela a seguir traz um resumo dos recursos que são suportados pelo *software* IOS®, da *Cisco*, para prover *QoS* em ambientes que utilizem seus roteadores:

Tabela 3.2: Principais categorias e recursos de *QoS* do IOS® da *Cisco*

Categoria	**Recursos de *QoS* associados**
Classificação	CAR, CBWFQ, NBAR
Políticas de Escalonamento	WFQ, CBWFQ, LLQ, etc.
Prevenção de congestionamento	WRED, RED
Política e modelagem de tráfego	GTS, FRTS, CAR
Mecanismos de eficiência de enlace	LFI, cRTP[50]

Fonte: *Cisco Systems Inc.*

Em *Cisco IOS® Software Quality of Service* (Cisco, 2002c) são apresentados os recursos de *QoS* presentes no *software IOS®* da *Cisco*.

No capítulo 6 (Implementando *QoS* em uma rede com equipamentos *Cisco* – estudo de caso) são apresentados com detalhes alguns destes recursos e como eles são aplicados de forma a se obter níveis desejados de Qualidade de Serviço.

3.4 Resumo do capítulo

Neste capítulo são apresentados conceitos e mecanismos relacionados a Qualidade de Serviço. São expostos os modelos *IntServ* e *DiffServ* e as principais diferenças entre eles. Por fim são analisados os recursos para obtenção de Qualidade de Serviço, com especial destaque para os presentes na plataforma *Cisco*.

[50] Compressão de cabeçalhos RTP

No próximo capítulo são apresentadas as características do padrão Voz sobre IP, seus requisitos em relação à Qualidade de Serviço e detalhes de implementação em roteadores *Cisco*.

4 Voz sobre IP

Uma das principais aplicações que têm sido incorporadas nas atuais redes IP é a transmissão de voz. As empresas têm utilizado suas redes privadas de dados para transporte de tráfego de voz com o objetivo de racionalizar os custos com telecomunicações de longa distância e integrar serviços como telefonia sobre Internet e *voice-mail*[51]. Atualmente o mais versátil padrão de rede que permite este tipo de serviço em redes baseadas em IP é o que é conhecido como Voz sobre IP ou *VoIP* (i.e. *Voice over IP*). Neste capítulo são abordadas as características deste protocolo, seus requisitos em relação à Qualidade de Serviço e os detalhes e recomendações de implementação deste padrão em ambiente *Cisco*

4.1 Protocolos de Voz sobre IP

VoIP é uma aplicação de transmissão de voz através de redes IP que utiliza diversos protocolos ponto-a-ponto ou *link-layer* como PPP, *Frame Relay* ou ATM para seu transporte. O sinal de áudio é segmentado por processadores de sinal digital (i.e. *DSP – Digital Signal Processors*[52]) em quadros pequenos, que são armazenados em pacotes de voz, geralmente aplicando algum tipo de compressão, a depender do *codec* utilizado. Estes pacotes são transportados pelo IP de acordo com protocolos de comunicações ou padrões como o H.323[53], o *Media Gateway Control Protocol*[54] (i.e. MGCP) ou o *Session Initiation Protocol*[55] (i.e. SIP).

As aplicações de Voz sobre IP geralmente usam o RTP (i.e. *Real-time Transport Protocol*) para estabelecimento do *stream* de áudio, ou caminho de voz. O RTP usa o UDP (i.e. *User Datagram Protocol*) como seu protocolo de transporte. Já os pacotes de sinalização de voz geralmente utilizam o TCP (i.e. *Transmission Control Protocol*), uma vez que a garantia de entrega é fundamental neste caso. O IP provê roteamento e endereçamento de nível 3, enquanto que os protocolos de nível 2 controlam e direcionam a transmissão da informação através dos enlaces.

[51] Serviços de mensagens de voz através de e-mail.
[52] Processadores Digitais de Sinal – *Hardware* que processa sinal analógico transformando-o em informação digital.
[53] H.323 – Protocolo definido pela ITU-T para conferência interativa.
[54] MGCP – Protocolo de sessão para controle de *gateways* em redes de Voz sobre IP.
[55] SIP – Draft de padrão do IETF como alternativa ao H.323.

A tabela 4.1 mostra a relação entre o modelo de referência OSI e os protocolos e funções dos elementos de rede *VoIP*:

Tabela 4.1: O Padrão *VoIP* e o modelo OSI

Camada OSI	Nome da Camada	Protocolos e Funções do padrão *VoIP*
7	Aplicação	*NetMeeting*[56]/Outros
6	Apresentação	*Codecs* G.729/G.711/G.723/Etc.
5	Sessão	H.323/MGCP/SIP/SDP
4	Transporte	RTP/TCP/UDP/RSVP/RTCP
3	Rede	IP/LLQ/IP-*Precedence*
2	Data Link	*Frame Relay*, ATM, *Ethernet*, PPP, MLPPP, e outros.

Fonte: *Cisco Systems Inc*.

4.2 Benefícios do padrão Voz sobre IP

Alguns dos benefícios do padrão Voz sobre IP são:

- economia com tarifas de telefonia;
- possibilidade de presença remota de PABX através de uma rede WAN;
- serviços de *Voice-mail* e *Fax-mail* [57] acessíveis à distância;
- unificação das redes de voz e dados;
- *gateways*[58] entre telefonia tradicional e telefonia via Internet;
- suporte para utilização e integração de aplicações multimídia como *NetMeeting*.

[56] Aplicação de audio/video conferência da *Microsoft.*
[57] Serviços de fax através de e-mail.
[58] Interface de conexão entre duas redes distintas.

4.3 Processamento de uma chamada em Voz sobre IP

Para melhor compreensão do funcionamento do padrão Voz sobre IP, vejamos quais os eventos que ocorrem quando do estabelecimento de uma chamada de voz utilizando esta tecnologia:

1. O usuário pega o fone, sinalizando a condição de fora do gancho para o nível de aplicação Voz sobre IP;

2. A camada de sessão do padrão Voz sobre IP gera um tom de discar para que o usuário disque o número desejado;

3. Quando o usuário disca os números, a camada de sessão Voip acumula e armazena os dígitos coletados;

4. Assim que tiver sido coletada uma quantidade suficiente de dígitos que coincida com um padrão de destino configurado, o número de telefone é mapeado para um endereço IP pelo mapeador do plano de discagem. Este endereço IP será o host que terá conexão direta com o PABX ou telefone configurado como destino;

5. Na camada de sessão, um protocolo como o H.323, o MGCP ou o SIP, estabelece um canal de transmissão e recepção em cada direção através da rede IP. Se o protocolo de reserva de recurso (i.e. RSVP – *Resource Reservation Protocol*) tiver sido configurado, as reservas são colocadas em efeito para garantir a Qualidade de Serviço desejada na rede;

6. Os codificadores-decodificadores (i.e. *codecs*) são habilitados em ambas as pontas da conexão e a conversação prossegue utilizando o RTP/UDP/IP como pilha de protocolos. A voz é digitalizada, comprimida, colocada em pacotes IP e transportada através da rede;

7. Quaisquer indicadores de progresso de chamada ou outros sinais que possam ser transmitidos em banda, ou seja, em meio à transmissão de voz, são retirados do canal de voz assim que a comunicação é estabelecida. Sinais que são detectados após o

estabelecimento da chamada (como, por exemplo, tons DTMF[59] digitados durante a ligação) são capturados pela camada de sessão em cada ponta da conexão e transportados pela rede IP pelo protocolo RTCP (i.e. *Real Time Conferencing Protocol*[60]);

8. Quando ambas as pontas desligam, as reservas RSVP são desfeitas (se tiverem sido usadas) e cada ponta se torna disponível para a próxima chamada.

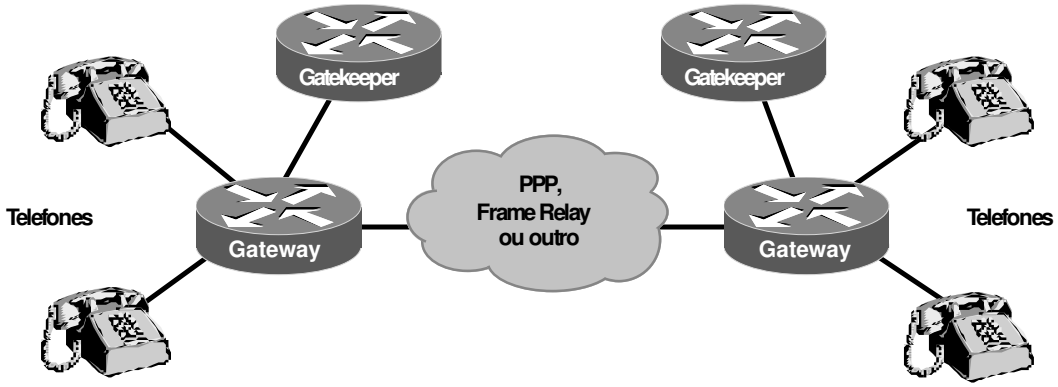

Figura 4.1 – O Ambiente de Voz sobre IP

4.4 Qualidade de Serviço em Voz sobre IP

Conforme visto no capítulo anterior, tráfegos de mídia continua, como o tráfego de voz, tem diversos requisitos específicos em relação à Qualidade de Serviço na rede. O tráfego de voz difere do tráfego de dados convencional da seguinte forma:

1. O tráfego de dados em geral é irregular e apresenta grandes variações, enquanto que o tráfego de voz é mais constante;

2. As aplicações de dados re-enviam os pacotes que se perdem na rede, enquanto que aplicações de voz desconsideram pacotes perdidos;

3. Aplicações de dados podem tolerar um certo atraso ou variação do mesmo, mas aplicações de voz devem minimizar estes problemas para que a voz seja inteligível para o ouvinte.

[59] Dual Tone Multi Frequence – Padrão de sinalização telefônica que utiliza tons em diferentes frequências para representar os números digitados.
[60] Protocolo de controle que atua em conjunto com o RTP em uma sessão de comunicação de mídia contínua (voz/vídeo).

Essas características fazem com que seja necessário que o tráfego de voz tenha prioridade absoluta na transmissão em uma rede IP, de forma a garantir uma entrega de pacotes confiável, com níveis de *delay* e *jitter* bastante reduzidos.

De uma forma geral, os requisitos de uma rede IP para transmissão de voz são as relacionadas a seguir.

4.4.1 Atraso

Atraso é o tempo que um pacote de voz leva de uma ponta a outra de uma conexão. Uma vez que os pacotes podem ter que atravessar uma enorme quantidade de equipamentos de rede como roteadores e *hubs*, uma certa quantidade de atraso é normal. No entanto, é preciso que se minimize ao máximo este atraso para não causar desconforto aos participantes de uma chamada de voz. O ser humano tolera até cerca de 150 ms de atraso sem perceber problemas. O padrão G.114, da ITU-T, recomenda justamente que não se tenha mais do que 150 ms de atraso em um sentido de voz (ITU-T, 2003). Entre 150 ms e 400 ms de atraso começa a haver desconforto aos ouvintes, e acima de 400 ms o atraso pode tornar a conversação bastante incômoda, devendo-se evitar ao máximo um atraso dessa magnitude.

4.4.2 Variação do atraso

Mais ainda do que o atraso em si, a variação do atraso, pode tornar a conversação simplesmente ininteligível. Este tipo de problema não existe na rede telefônica convencional, já que a banda de transmissão nestas redes é fixa e determinística[61]. Já em redes de pacotes, a coexistência de tráfego de voz e dados nos mesmos meios de transmissão, pode fazer com que os pacotes tenham atrasos variáveis a depender do volume de dados que está sendo transmitido. Por este motivo, recomenda-se que técnicas de condicionamento e policiamento de tráfego, como as vistas no capítulo anterior, sejam usadas para minimizar este efeito na rede.

4.4.3 Perda de pacotes

Perdas de pacotes podem ocorrer por motivos diversos, como problemas físicos no nível de enlace ou pelo descarte em um roteador ou switch da rede devido a excesso

de tráfego a ser transmitido. Mas, ao contrário de aplicações que carregam dados, onde a perda de uma parte da informação pode simplesmente inutilizar todo um arquivo ou documento sendo transmitido, em tráfego de mídia contínua é tolerada a perda de uma certa quantidade da informação. Isso se dá pelo próprio caráter de interatividade deste tipo de tráfego. Enquanto que em uma transmissão de arquivo pode-se requerer a retransmissão de uma parte da informação que eventualmente tenha se perdido, em transmissões de voz e vídeo essa retransmissão atrasaria a entrega da informação e inviabilizaria a comunicação. Por este motivo, ao invés de utilizar o TCP, que é um protocolo de transporte que garante a entrega da informação utilizando-se justamente do recurso de retransmissão da informação que não tiver seu recebimento confirmado pelo receptor, as aplicações de tempo real normalmente utilizam-se do UDP, que não provê garantias de entrega para as informações enviadas. Caso a quantidade de pacotes perdidos não seja muito grande, é provável que este fato, isoladamente, não cause grandes perdas na qualidade do áudio ou vídeo sendo transmitido, pois, neste tipo de tráfego, a redundância obtida com outros pacotes e o fato do significado poder ser preservado pelo ser humano na outra ponta fazem com que certos níveis de perda possam se tolerados.. A ITU-T recomenda que as perdas de pacotes em transmissões interativas situem-se abaixo de 5% (ITU-T, 2003). Obviamente a qualidade do sinal transmitido será inversamente proporcional à quantidade de pacotes que forem perdidos da origem ao destino.

4.4.4 Consumo de banda

Normalmente, uma chamada de voz, que não utilize compressão, consome cerca de 64 kbps de banda de uma rede. Em uma rede de Voz sobre IP, uma chamada deste tipo pode ser comprimida e digitalizada por um processador digital de sinal (i.e. DSP – *Digital Signal Processor*) de forma a reduzir este consumo de banda para até 5.3 kbps. Para o transporte na rede IP, no entanto, os cabeçalhos de IP, UDP e RTP devem ser adicionados. Esses cabeçalhos podem aumentar bastante o tamanho do pacote (cerca de 40 bytes por pacote). Tecnologias como compressão de cabeçalhos RTP, no entanto, podem reduzir esta sobrecarga para aproximadamente dois bytes. Além disso, recursos

[61] Com taxa de transmissão e banda fixos e garantidos.

como VAD (i.e. *Voice Activity Detection*[62]) permitem que não sejam enviados pacotes quando não há detecção de conversação, o que também proporciona uma grande economia no consumo de banda.

O consumo efetivo de banda de uma ligação em Voz sobre IP depende também do *codec* a ser utilizado. Vale salientar que a escolha por um ou outro *codec* depende não só da quantidade de banda que se deseja consumir com a transmissão, mas também da qualidade de áudio que é produzida e o quanto dos processadores de sinais (i.e. DSP's) cada *codec* necessita. Dentre os *codecs* que apresentam as melhores taxas de compressão, o G.729 é o mais usado, por apresentar boa qualidade de voz, além de não consumir muitos recursos dos DSP's, especialmente a versão G.729a, que usa 50% da quantidade de DSP's do *codec* G.729 padrão. A tabela 4.2 mostra as possíveis combinações de *codec*, tamanho de pacote de voz, compressão de cabeçalhos RTP e VAD (Cisco, 2003f).

[62] Algoritmo padronizado pela ITU-T que permite que se deixe de transmitir pacotes de voz quando se detecta silêncio na conversação.

Tabela 4.2: Consumo de Banda por chamada *VoIP*

Codec / (Taxa de bits do codec)	**Tamanho do Payload[63]**	**MLPPP ou FRF.12**	**cRTP[64] MLPPP ou FRF.12**	**VAD MLPPP ou FRF.12**	**cRTP & VAD MLPPP ou FRF.12**
kbps	Bytes	kbps	kbps	kbps	kbps
G.711 (64)	240	76	66	50	43
G.711 (64)	160 (Padrão)	83	68	54	44
G.726 (32)	120	44	34	29	22
G.726 (32)	80 (Padrão)	50	35	33	23
G.726 (24)	80	38	27	25	17
G.726 (24)	60 (Padrão)	42	27	27	18
G.728 (16)	80	25	18	17	12
G.728 (16)	40 (Padrão)	35	19	23	13
G.729 (8)	40	17.2	9.6	11.2	6.3
G.729 (8)	20 (Padrão)	26.4	11.2	17.2	7.3
G.723.1 (6.3)	48	12.3	7.4	8.0	4.8
G.723.1 (6.3)	24 (Padrão)	18.4	8.4	12.0	5.5
G.723.1 (5.3)	40	11.4	6.4	7.4	4.1
G.723.1 (5.3)	20 (Padrão)	17.5	7.4	11.4	4.8

Fonte: *Cisco Systems Inc.*

[63] Quantidade de bytes de informação (voz) a ser transmitido em um pacote.
[64] Compressão de cabeçalhos de RTP.

Os valores desta tabela foram obtidos a partir dos seguintes cálculos:

- Tamanho do pacote de voz = (cabeçalho nível 2 MLPPP ou FRF.12) + (cabeçalhos IP/UDP/RTP) + (*payload* de voz);
- Pacotes de voz por segundo (pps) = taxa de bits (*bit rate*) do *codec* / tamanho do *payload* de voz;
- Banda = tamanho do pacote de voz x pps.

Exemplo – uma ligação utilizando *codec* G.729 (*codec* com *bit rate* de 8 kbps) com cRTP (compressão de cabeçalho RTP), MLPP (*Multilink* PPP) e o tamanho padrão de *payload* de voz de 20 bytes:

- Tamanho do pacote de voz (bytes) = (cabeçalho MLPPP de 6 bytes) + (cabeçalho comprimido de IP/UDP/RTP de 2 bytes) + (*payload* de voz de 20 bytes) = 28 bytes;
- Tamanho do pacote de voz (bits) = (28 bytes) * 8 bits por byte = 224 bits;
- Pacotes de voz por segundo (pps) = (8 kbps *bit rate* do *codec*) / (160 bits[65]) = 50 pps;
- Banda por ligação = tamanho do pacote de voz (224 bits) * 50 pps = 11.2 kbps;

Deve-se atentar para o fato de que o recurso de VAD pode proporcionar uma economia considerável no consumo de banda, uma vez que o roteador deixa de enviar pacotes de voz quando nenhum dos interlocutores de uma conversação está falando. Esta economia pode chegar a 35% da banda (Cisco, 2003f). No entanto, não se deve levar esta economia muito em conta quando do dimensionamento de uma rede. Como esta economia não é constante, se ela for considerada em um enlace no qual trafegue somente um ou alguns poucos canais de voz, poderá haver uma sobrecarga nos momentos em que haja pouco silêncio nas ligações. Recursos como música em espera ou transmissão de fax, por exemplo, tornam nula a economia proporcionada pelo VAD, o que pode comprometer o dimensionamento feito. Por isso, a *Cisco* não recomenda levar em consideração, no dimensionamento da rede, a economia proporcionada pelo VAD em

[65] 160 bits = 20 bytes (*payload* de voz padrão) * 8 (bits por byte)

enlaces pelos quais trafeguem menos do que 24 ligações simultâneas de voz (Cisco, 2003f).

4.4.5 Efeitos da serialização

Em geral pacotes de voz são muito pequenos (de 80 a 256 bytes) enquanto que pacotes de dados podem ser bastante grandes (1.500 a 18.000 bytes). Em enlaces de velocidade reduzida, a transmissão de grandes pacotes de dados pode levar muito tempo, o que pode comprometer os requisitos de *delay* e *jitter*. Para evitar este problema, recursos de fragmentação e intercalação de dados (i.e. *interleaving*), que também foram vistos no capítulo anterior[66], podem ser aplicados de forma a se obter a cadência de transmissão ideal para uma boa qualidade de transmissão de voz.

4.5 Gatekeeper

Ao contrário de padrões de transmissão de voz de nível 2, como Voz sobre ATM (i.e. VoATM) ou Voz sobre *Frame Relay* (i.e. VoFR), nos quais é possível ter um processamento centralizado do plano de numeração, no padrão Voz sobre IP utilizando o protocolo H.323 todos os *hosts* de uma rede de voz, precisam saber o endereço de rede do destino final de suas chamadas. Em redes não muito grandes, com poucos pontos de voz, isto não chega a ser um grande problema. Mas em redes maiores, com muitas pontos, esta característica pode trazer grandes inconvenientes. Cada *host* precisa manter uma tabela com os endereços IP de cada um dos outros *hosts* com quem eventualmente precise se comunicar. Além do maior consumo de memória que este fato traz, há ainda a necessidade de todo um trabalho para se manter estas tabelas atualizadas e consistentes com as alterações que ocorram na rede.

Para resolver este e outros problemas, existe um componente, opcional em uma rede *VoIP*, que, entre outras coisas, funciona como um DNS[67] (i.e. *Domain Name Server*) para endereços de voz. Este componente é o *Gatekeeper*. Uma das funções deste componente é fazer a tradução de endereços de telefone (394-9087, por exemplo) para endereços IP (como 172.168.10.100). Ao executar uma chamada, o host de voz consulta o *Gatekeeper* e este lhe retorna o número IP correspondente ao telefone consultado. O

[66] Vide item 3.2.4.2
[67] Servidor que converte nomes em endereços de rede e vice-versa.

host de origem pode então completar a chamada sem que precise guardar uma imensa tabela com todos os endereços da rede.

Além de atuar como tradutor de endereços, o *Gatekeeper* pode ainda ter outras funcionalidades em uma rede de voz, tais como:

1. Controle de Chamadas: todas as chamadas efetuadas em uma rede são estabelecidas através do *Gatekeeper*;

2. Controle de Admissão: pode-se configurar o *Gatekeeper* para permitir ou restringir ligações de/para determinados números, permitindo maior controle do tráfego gerado pelas chamadas de voz;

3. Controle de Banda: em situações em que a banda disponível para transmissão de voz é inferior ao número possível de ligações na rede, pode-se configurar o *Gatekeeper* para limitar o número de ligações simultâneas, de forma a não exceder o limite de tráfego que poderia comprometer a qualidade das ligações;

4. Gerenciamento: o *Gatekeeper* pode gerar um log das ligações efetuadas, permitindo que se possa efetuar uma gerência do tráfego de voz que está sendo gerado na rede.

4.6 Voz sobre IP em ambiente Cisco

O sistema operacional dos roteadores *Cisco*, o IOS®, em sua versão 12.2 ou mais recente, suporta a maioria dos padrões e protocolos atuais para *VoIP*. Entre estes padrões podemos destacar:

- H.323: Padrão da ITU-T (i.e. *International Telecommunication Union-Telecommunications*) para transmissão de voz e vídeo em redes de dados;

- MGCP - *Media Gateway Control Protocol*: *dratf*[68] de padrão do IETF (i.e. *Internet Engineering Task Force*) para controle de *gateways* de voz em redes IP;

- SIP - *Session Initiation Protocol*: protocolo definido na RFC 2543 (IETF, 1999d) para telefonia, conferência e mensagens instantâneas;

- RSVP – *Resource Reservation Protocol*: protocolo de reserva de recursos na rede, usado para se obter garantia de banda e Qualidade de Serviço para tráfego multimídia;

Adicionalmente, o IOS® suporta também os principais mecanismos de *QoS*, já discutidos no capítulo 3, fundamentais para um bom desempenho na transmissão de voz sobre uma rede de dados.

4.6.1 Recomendações de *QoS* da *Cisco* para *VoIP*

De uma forma geral, a *Cisco* recomenda os seguintes procedimentos para uma implementação de Voz sobre IP (Cisco, 2000):

- usar IOS® versão 12.0.7T ou superior, para se obter os melhores recursos de escalonamento;

- não usar *VoIP* em um PVC[69] (i.e. *Permanent Virtual* Circuit) pelo qual também trafegue VoFR[70] (i.e. *Voice over Frame Relay*);

- configurar *IP Precedence* = 5 nos *dial-peers*[71];

- não usar WRED em filas de voz;

- em redes *Frame Relay*, não marcar pacotes de voz como DE;

- habilitar *DTMF-Relay*[72] para *codec*s com taxa de bits (i.e. *bit rate*) baixas (8k ou menores);

- medir o atraso de pacotes na rede, buscando entre 150 e 200 ms de atraso em um sentido;

- se os *delays* do TCP afetarem a performance da sinalização DTMF, usar "***cisco-rtp***" para "***dtmf-relay***";

- se possível, usar escalonamento LLQ, classificando voz como fila prioritária;

---

[68] Esboço. Padrão não definitivo.
[69] Circuito virtual em uma rede de pacotes, como a *Frame Relay*.
[70] Transmissão de voz sobre protocolo Frame Relay.
[71] Objeto de configuração que mapeia endereços de voz para endereços de rede ou interfaces físicas

- se LLQ não estiver disponível, usar "***IP RTP Priority***" (i.e. PQ-WFQ);

- configurar a banda de voz com o comando "***priority***" na LLQ ou no comando "***IP RTP Priority***";

- aplicar fragmentação para obter-se 10 ms de *delay*;

- configurar fragmentação de forma que os pacotes de voz não sejam fragmentados;

- para enlaces PPP, usar o comando "***ppp multilink fragment-delay***";

- para enlaces *Frame Relay*:

  - configurar "***frame-relay fragment***" no *map-class;*

  - fragmentar todos os PVC's que carreguem dados em uma interface que tenha no mínimo um PVC de voz;

  - habilitar *Frame Relay Traffic Shaping* na interface;

  - configurar BC para 10 ms (1/100 do CIR);

  - configurar MinCIR >= a banda de voz.

4.7 Resumo do capítulo

Neste capítulo são expostas as características do protocolo Voz sobre IP e seus requisitos em relação a Qualidade de Serviço. São também apresentadas recomendações da *Cisco* relativas a configuração deste recurso em roteadores de sua plataforma.

No próximo capítulo é sugerido um roteiro com os pontos a serem observados e os cuidados a serem tomados para o projeto e implementação de redes de natureza semelhante a que foi estudada neste trabalho.

[72] Transmissão de tons DTMF em separado do sinal de áudio.

5 Roteiro para implementação de redes multiserviços com Qualidade de Serviço

Neste capítulo é sugerido um roteiro para o projeto e implementação de uma rede que integre dados e voz com recursos de garantia de Qualidade de Serviço para voz e priorização e garantia de bandas para tráfego IP. São destacados os cuidados que se deve tomar buscando obter sucesso na implementação final do projeto.

5.1 Conhecendo a rede

Talvez a principal tarefa no projeto e implementação de uma rede complexa seja o levantamento inicial que se faz buscando conhecer as características que esta rede terá. Caso se trate de uma rede nova, partindo do zero, este trabalho pode ser bastante difícil e sujeito a muitos erros. No caso de uma rede que vá substituir uma rede já existente, este estudo pode ser tornar um pouco mais simples. Qualquer que seja o caso, no entanto, é preciso se ter uma base do volume de tráfego e dos recursos que a nova rede deverá suportar para que se possa dimensionar corretamente os equipamentos, meios físicos, protocolos e estrutura de endereçamento a serem utilizados.

5.2 Definição de equipamentos e *softwares*

Tendo-se definido os recursos que serão suportados pela rede, é preciso se verificar quais equipamentos atendem às necessidades de cada ponto da rede. No caso de roteadores, deve-se levar em consideração, nesta avaliação, diversos fatores, tais como:

1. Quantidade e tipo de interfaces a serem utilizadas;

2. Capacidade de processamento do equipamento;

3. Capacidade de memória do equipamento;

4. Suporte aos recursos desejados;

5. Facilidades de expansão do equipamento, quer seja em relação a quantidade de interfaces, quer seja em termos de processamento e memória;

6. Versão (e *feature set*[73]) do *software* que suporte as aplicações desejadas;

7. Disponibilidade de contingência e redundância de recursos tais como unidade de processamento e fontes de alimentação.

Alguns desses itens são de fácil definição e identificação. Itens como tipo e quantidades de interfaces e versões de *software* que suportem os recursos desejados podem ser identificados com as informações disponíveis na página da *Cisco* na Internet ou na sua documentação impressa. Já itens como capacidade de processamento e memória dos equipamentos podem ser um pouco mais complicados de se definir. Uma regra simples que pode ser seguida em relação à memória no caso de redes complexas é se dimensionar o equipamento com a quantidade de memória 50% superior a mínima exigida pela versão de *software* que for escolhida. Assim, se a versão de IOS® escolhida exige 32 MB de memória DRAM[74] (i.e. *Dynamic Random Access Memory*), por exemplo, sugere-se que o equipamento seja configurado com 48 MB deste tipo de memória. Com relação à capacidade de processamento, deve-se levar em conta a quantidade de pacotes por segundo (i.e. pps) que o modelo de roteador escolhido pode processar. Em ambos os casos, é interessante, ainda, que seja montado um laboratório onde seja testado máximo possível de configurações a serem empregadas na rede, de forma a se identificar possíveis erros de dimensionamento destes itens.

5.3 Definição dos protocolos de enlace e do endereçamento

Um ponto bastante importante no projeto de uma rede complexa diz respeito à definição dos protocolos que serão utilizados no nível de enlace e da topologia lógica e seu esquema de endereçamento. Protocolos de enlace, como o *Frame Relay*, permitem uma certa variação na topologia lógica e no esquema de endereçamento que podem ter conseqüências importantes se não forem corretamente levadas em consideração no momento do projeto. Da mesma forma, um bom esquema de endereçamento irá permitir a configuração de recursos de sumarização de rotas e a aplicação individualizada de *policy-maps* de conformação de tráfego, permitindo a construção de uma rede racional e com bom desempenho.

[73] Codificação usada pela Cisco para definir os recursos que determinada versão de software possui. Exemplos de *feature set* são IP, IP PLUS, ENTERPRISE, etc.
[74] Memória do tipo volátil, que perde seu conteúdo ao ser retirada sua alimentação.

5.4 Montagem de um laboratório

Sempre que forem projetados recursos para uma rede sobre os quais não se tem uma boa experiência e quantidade de conhecimentos, é interessante que seja montado um laboratório que possa conter, em escala reduzida, a maior quantidade de recursos iguais ao que a rede final terá, de forma a se poder testar e validar as configurações projetadas. Nesta fase costumam-se descobrir prematuramente problemas que trariam grandes dores de cabeça se fossem descobertos somente na fase de implementação final.

Ferramentas de avaliação podem ser utilizadas nesta fase para se tentar projetar o desempenho esperado para a rede final. Em casos em que a topologia é complexa demais para se montar um laboratório que consiga reproduzir uma porção significativa da rede, é possível se lançar mão ainda de recursos de simulação e/ou modelagem analítica, em especial quando muitos novos recursos estarão sendo implementados e não se tem ainda uma noção exata do impacto de cada um deles.

5.5 Rede Piloto

Mesmo tendo-se testado em laboratório as configurações projetadas para uma rede, é ainda possível (e até provável) que problemas ocorram na implementação final. Para evitar que estes problemas tragam grandes transtornos aos usuários da rede, é interessante se escolher um ou mais pontos pilotos para serem ativados e avaliados antes de se colocar diversos pontos da rede em produção. Nesta fase deve-se observar atentamente se os recursos dimensionados estão atendendo as necessidades da forma que se esperava no projeto. Caso ocorram problemas nesta fase, é ainda uma boa hora pra se fazer pequenas correções de rotas.

5.6 Monitoração dos recursos e log's

Conforme a rede for sendo implementada, é importante se ficar atento aos indicadores de performance e utilização de recursos disponíveis nos equipamentos. A cada ativação de um ponto remoto, recursos de processamento e memória vão sendo consumidos nos equipamentos. A rede pode se manter estável e com bom desempenho até o ponto em que algum desses recursos atinja um nível crítico, quando problemas sérios podem passar a ocorrer. Isto é especialmente importante em roteadores de maior

porte que utilizam placas VIP (i.e. *Versatile Interface Processor*). Estas placas possuem processadores e memórias próprios, independentes do processador e memória principal do roteador. Em muitos casos, faz-se a monitoração dos recursos do roteador e se esquece de monitorar as VIP's, que podem passar a apresentar *crashes*[75] quando a utilização de seu processador e, principalmente, de sua memória, ultrapassam um certo limite.

Da mesma forma, é bom se estar atento às mensagens que são gravadas nos log's dos roteadores. Mensagens que a princípio não indicam grandes problemas podem ser o indício de que algo maior está por acontecer. Em alguns casos, estas mensagens poderão apontar uma falha existente na versão de *software* que se está usando. Neste caso, convém que seja testada uma atualização do *software* em uma parte da rede em um dia e horário que sejam menos impactantes para o funcionamento da mesma.

5.7 Validação dos recursos projetados

Com a implementação da rede e a ativação progressiva das localidades remotas, é conveniente se colher dados que permitam avaliar se as opções adotadas no projeto foram realmente adequadas à situação real. Diversos comandos existentes nos roteadores permitem verificar a utilização dos enlaces e a aplicação das políticas de priorização dos dados e de garantia de Qualidade de Serviço

Outro indicador a ser observado é a satisfação do usuário final, quer seja em relação ao sentimento de agilidade da rede quanto ao tráfego de dados, quer seja em relação à qualidade de voz, percebida durante as ligações efetuadas pela rede.

Em redes com topologia complexa, com grande quantidade de alternativas de caminhos entre os diversos pontos, é importante também se observar se o fluxo de dados está seguindo sempre o melhor caminho dentro da rede. Problemas de configurações no protocolo de roteamento dinâmico, quando o mesmo é utilizado, podem fazer com que os pacotes utilizem rotas de menor capacidade enquanto que outras, melhores, acabam sem utilização. Este problema pode ser difícil de se detectar, principalmente no início da implementação, quando o volume de dados é ainda pequeno.

[75] Erro fatal no qual todo o processamento da placa é interrompido. Em alguns casos a recuperação de um erro deste tipo só se dá com a recarga da placa ou de todo o roteador.

5.8 Fluxo de atividades

As atividades apontadas nos itens anteriores podem ser resumidas e melhor compreendidas através do fluxo a seguir, que representa de forma gráfica as principais fases do projeto e implementação de uma rede:

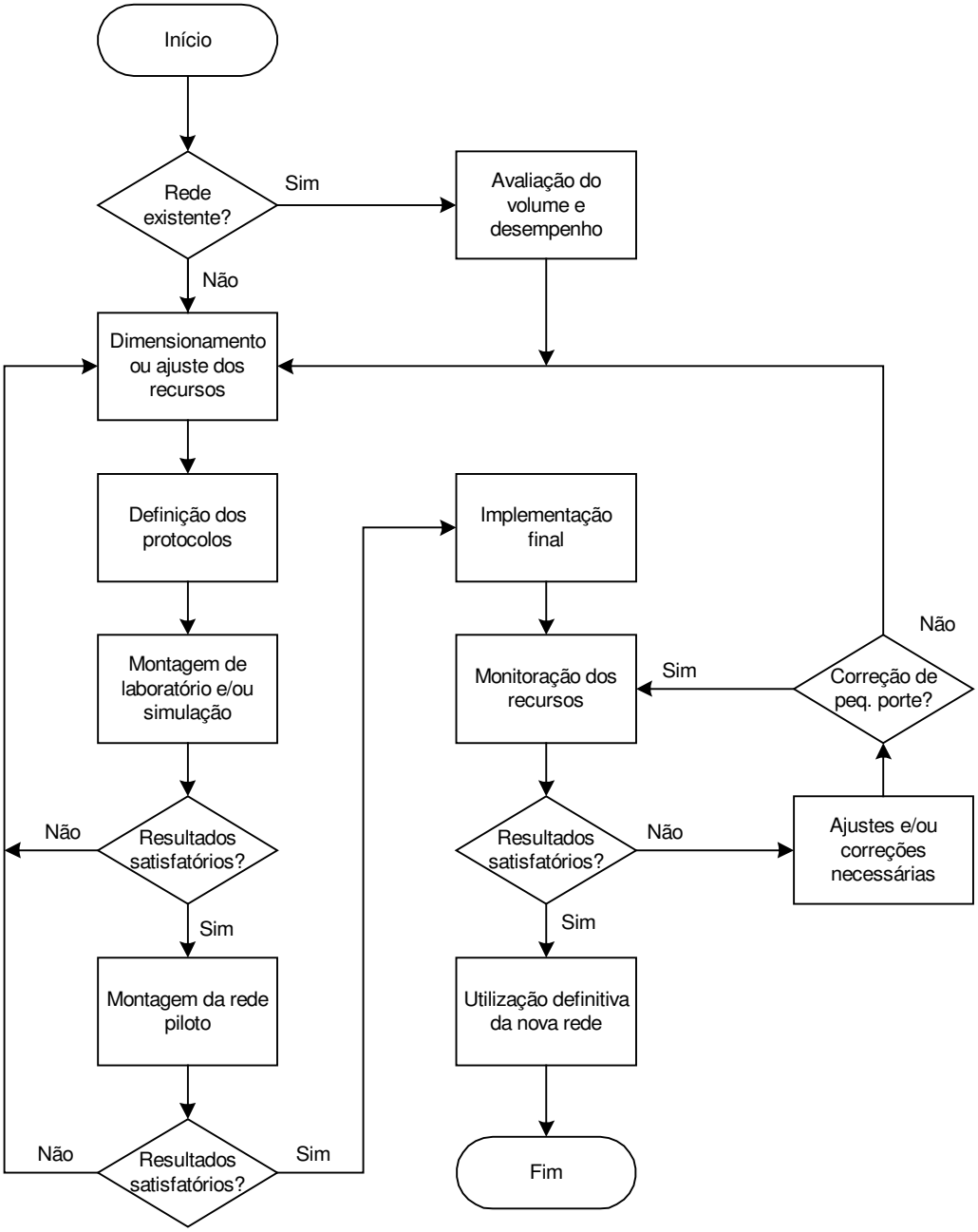

Figura 5.1 – Fases do projeto e implementação de uma rede

5.9 Resumo do capítulo

Neste capítulo é sugerido um roteiro para o projeto e a implementação de redes corporativas complexas envolvendo Qualidade de Serviço e Voz sobre Ip. São enumerados alguns fatores que devem ser observados para se obter êxito em um projeto deste tipo.

No próximo capítulo são apresentados detalhes do projeto e implementação de uma rede com *QoS* em um ambiente *Cisco*. São discutidos aspectos a serem analisados e fornecidas fontes para obtenção de informações importantes em uma implementação dessas.

6 Implementando *QoS* em uma rede com equipamentos *Cisco* – estudo de caso

Neste capítulo é feito o detalhamento da implementação de uma rede real nas quais foram aplicadas as técnicas de Qualidade de Serviço expostas nos capítulos anteriores. O objetivo aqui é mostrar, de forma prática e objetiva, como aplicar toda a teoria que envolve este assunto em uma rede que utiliza roteadores da *Cisco Systems*, atualmente os mais difundidos em redes privadas e públicas em todo o mundo. São mostrados exemplos, sintaxes de comandos e detalhes a serem observados em uma implementação como esta, assim como as soluções que foram adotadas para as situações que se apresentaram. Para preservar a segurança e a privacidade do cliente para qual a rede foi montada, não serão fornecidos nomes, configurações ou localidades reais.

6.1 A Implementação da rede

Na implementação desta rede, levou-se em consideração que o cliente tinha suas atividades baseadas uma capital brasileira, local onde se encontravam também cerca de 40% de suas lojas. Uma outra capital concentrava também outros 40% do total de lojas. Os 20% restantes eram distribuídos entre o interior destes dois estados e em alguns outros estados da federação. Dessa forma o projeto estabeleceu que haveria dois grandes pontos de concentração, dentro das dependências da Embratel nestas duas capitais, além de um ponto central, dentro do CPD do próprio cliente (figura 6.1).

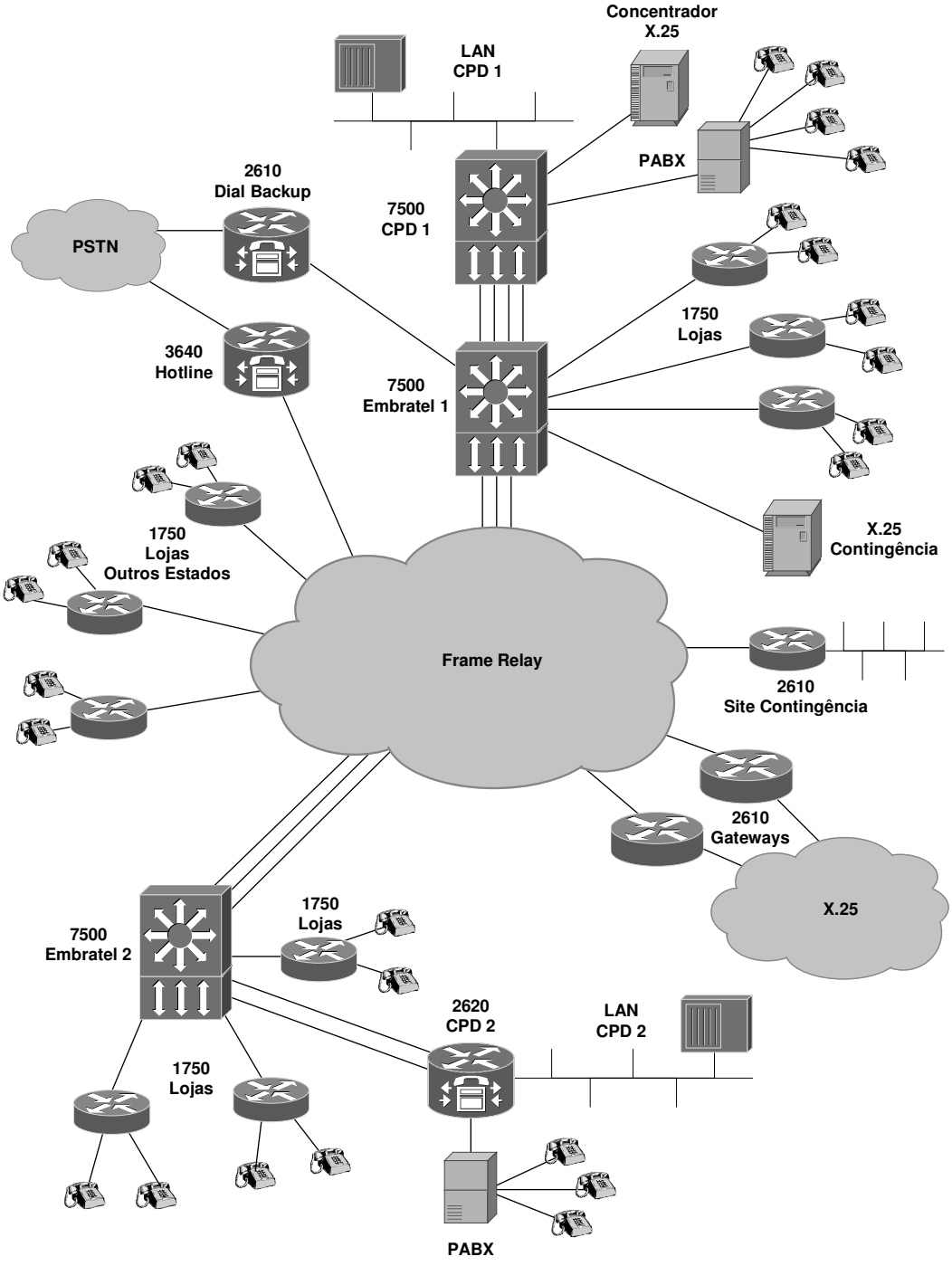

Figura 6.1 – Topologia simplificada da rede

6.1.1 Requisitos da rede

Desejava-se que a rede pudesse atender os seguintes requisitos:

1. Disponibilidade: desejava-se que houvesse o mínimo de paralisação na rede. Para tanto, o projeto estabeleceu que todos os equipamentos das lojas tivessem circuitos de dados duplicados, de forma que a loja não ficasse sem comunicação quando da parada de um circuito. Para aumentar a segurança, estabeleceu-se que os dois circuitos de cada loja passassem sempre por equipamentos e infra-estruturas separados na prestadora de comunicações, para evitar que houvesse pontos únicos de falha. Para os equipamentos de centralização, foram adotados roteadores com redundância automática em termos de fonte de alimentação e processadores (i.e. linha *Cisco* 7500), além da disponibilização de peças sobressalentes que pudessem ser trocadas com a maior brevidade em caso de falha em algum adaptador de portas;

2. Integração: a rede deveria integrar os serviços de dados em IP, dados em X.25 e voz. Estes serviços já existiam no ambiente do cliente, porém eram atendidos por redes independentes. Para os serviços de voz optou-se pela tecnologia de Voz sobre IP, pela flexibilidade em termos de implementação sobre diferentes infra-estruturas de rede em nível de enlace, assim como a possibilidade de integração futura com ambiente de *desktop*. Para os serviços de X.25, foram projetados dois *gateways*[76] centralizadores que teriam conexões únicas com a rede pública de pacotes RENPAC[77], de forma a se desativar os outros enlaces com a Renpac existentes em cada uma das lojas;

3. Qualidade de Serviço: a implementação de Voz sobre IP, por si só já demandava que fosse feito todo um trabalho de garantia de Qualidade de Serviço na rede, caso contrário não se atingiriam bons resultados com este serviço. No entanto, o cliente desejava implementar Qualidade de Serviço também para seu tráfego de dados. Havia uma demanda de priorização de tráfegos mais importantes para o cliente, enquanto que outros poderiam ter sua vazão limitada. Era desejado, por exemplo, que o tráfego X.25 tivesse prioridade máxima na rede, uma vez que o mesmo era relativo a transações de cartões de crédito, estando diretamente ligado ao faturamento da empresa.

[76] Interface entre redes de diferentes tipos.
[77] Rede de pacotes da Embratel utilizando o protocolo X.25.

Outros tipos de tráfego, como FTP e HTTP, poderiam ter suas prioridades limitadas de forma a não prejudicar os fluxos mais importantes;

4. Gerência e Recuperação de Falhas: era desejado também que a rede fosse permanentemente monitorada e que eventuais falhas fossem tratadas com a maior brevidade possível. Para tanto se estabeleceu que a Central de Gerência da prestadora de comunicações receberia tráfego SNMP[78] (i.e. *Simple Network Management Protocol*) da rede de forma a detectar de imediato qualquer falha ou queda nos circuitos ou equipamentos.

6.2 Qualidade de Serviço

A seguir veremos como foi feita a configuração dos principais parâmetros de *QoS* do projeto.

Optou-se pela implementação do modelo de Qualidade de Serviço *DiffServ*. Conforme visto no capítulo 3, neste modelo os pacotes são classificados e marcados nos roteadores das pontas e tem tratamentos diferenciados nas interfaces de saída desses roteadores, assim como nos roteadores que compões o núcleo da rede. A opção por este modelo se deu em face dos recursos proporcionados por ele e de suas vantagens em relação ao modelo *IntServ*, também discutidos no capítulo 3.

A técnica de escalonamento escolhida foi a *Low Latency Queueing* (i.e. LLQ ou PQ-CBWFQ) por sua melhor adequação à transmissão de tráfego interativo, conforme também visto no capítulo 3.

Além disso, foram aplicadas outras técnicas de obtenção de *QoS*, como a suavização de tráfego (i.e. *Traffic Shaping*) e a fragmentação e intercalação de quadros, de forma a proporcionar uma melhor qualidade ao tráfego de voz que iria passar pela rede.

Nos próximos tópicos serão detalhados cada um desses recursos e suas aplicações no projeto em questão.

[78] Protocolo de gerenciamento de rede.

6.2.1 Classificação e marcação dos pacotes

Para a classificação e marcação dos pacotes foram definidas cinco classes de serviços que receberam diferentes prioridades e garantias na rede. O cliente forneceu uma planilha na qual detalhou os protocolos e endereços para os quais desejava dar tratamento diferenciado, após um estudo realizado em sua rede onde foram identificados suas principais aplicações e requisitos de banda para as mesmas. A partir dessa planilha estabeleceram-se as seguintes classes de serviços, resumidas na tabela 6.1:

1. Classe Voz: pacotes de voz. Estes pacotes foram marcados com *IP precedence* 5, tendo esta marcação ocorrido nos *dial-peers.* A marcação exclusivamente da precedência IP, no entanto, não é suficiente para manter a conformidade com o modelo *DiffServ*, já que neste caso este tráfego deveria receber a marcação referente ao tipo de serviço EF (i.e. *Expedited Forwarding*). Como não era possível se executar esta marcação diretamente nos *dial-peers* este trabalho teve de ser efetuado, excepcionalmente, pela *policy-map* de priorização, que será vista mais adiante[79];

2. Classe Altíssima: dados provenientes do tráfego X.25. O trafego X.25 é transportado pela rede IP através do protocolo XOT (i.e. *X.25 over TCP*). Este protocolo encapsula o X.25 em pacotes IP e os encaminha pela rede segundo rotas definidas nos roteadores. A identificação desses pacotes para a classificação se dá pela porta TCP que é utilizada por este protocolo (i.e. porta 1998). Dessa forma, através de uma lista de acesso[80] (i.e. *access-list*) todos os pacotes que tenham a porta 1998 como origem ou destino são identificados como pertencentes a esta classe. Também neste caso, por não originar de uma interface do tipo IP, não foi possível fazer a marcação *DiffServ* adequada para este tráfego, que foi definido como AF41 (i.e. DSCP 34)[81], correspondente ao *IP Precedence* 4 com descarte baixo[82]. Essa marcação também foi deixada, em caráter excepcional, para a *policy-map* de priorização, a ser vista mais adiante;

3. Classe Alta: dados provenientes das aplicações IP que o cliente considera de maior prioridade. Nesta classe foram enquadradas as aplicações IP de maior importância

[79] Em versões mais recentes do IOS®, esta marcação passou a ser possível através do comando ***"ip qos dscp".***
[80] Recurso que permite controle de acesso e filtragem de pacotes.
[81] Vide capítulo 3.
[82] Vide tabela 6.1.

para o cliente. Os pacotes referentes a estas aplicações foram identificados através das portas TCP e UDP e endereços IP utilizados por cada um deles, por meio de listas de acesso. Estes pacotes foram marcados com o DSCP AF42, correspondente ao *IP Precedence* 4 com descarte médio (i.e. DSCP 36);

4. Classe Média: dados provenientes das aplicações IP que o cliente considera de média prioridade. Nesta classe foram classificados os protocolos e aplicações com importância média para o cliente. Os pacotes referentes a estas aplicações também foram identificados através de suas portas TCP e UDP e endereços IP. Estes pacotes são marcados com IP DSCP AF32, que corresponde ao *IP Precedence* 3 e descarte médio (i.e. DSCP 28);

5. Classe Regular: nesta classe foram incluídos os pacotes referentes ao tráfego de *Lotus Notes*[83]. Como esta aplicação tem um tráfego bastante intenso na rede, principalmente devido à transmissão de mensagens de e-mail com anexos, o cliente solicitou que fosse criada uma classe exclusivamente para ela, de forma a dar-lhe uma prioridade diferenciada, ao mesmo tempo em que se limita o consumo de banda que ela proporciona. Os dados referentes a esta classe foram identificados através da porta TCP 1352, que é a porta utilizada por esta aplicação. Estes pacotes são marcados com IP DSCP AF22, correspondente ao *IP Precedence* 2 com descarte médio (i.e. DSCP 20). Nesta classe foram incluídos ainda os pacotes com *IP Precedence* 6 e 7. Estes pacotes correspondem aos pacotes de controle da rede, como os pacotes de *keepalive*[84] e controle do protocolo de roteamento. Esta inclusão teve como objetivo dar uma maior garantia de banda a estes pacotes, que de outra forma iriam disputar banda com os pacotes de menor prioridade na classe padrão (i.e. *class default*);

6. Classe baixa (i.e. *class default*): dados das demais aplicações IP. Estes pacotes são marcados com IP AF13, correspondente ao *IP Precedence* 1 e descarte alto (i.e. DSCP 14).

[83] Aplicação de correio eletrônico e colaboração da *Lotus Corp*.
[84] Troca de informações entre duas extremidades de um *enlace* ou rede com o objetivo de manter uma a outra informada de seu estado operacional.

Tabela 6.1: Classes e Serviços definidos

Classe	% da Banda	Serviço	Precedência	Descarte
Voz	Variável	EF	5	-
Altíssima	5,0%	AF41	4	Baixo
Alta	20,0%	AF42	4	Médio
Média	25,0%	AF32	3	Médio
Regular	40,0%	AF22	2	Médio
Baixa	10,0%	AF13	1	Alto

A marcação dos pacotes foi feita através de uma *policy-map* aplicada às configurações das interfaces *Fast Ethernet*[85] dos roteadores das bordas da rede (i.e. lojas). O primeiro passo consistiu na definição das listas de acesso. As mesmas foram codificadas a partir de uma planilha com a relação dos protocolos e prioridades desejadas pelo cliente. A tabela 6.2 reproduz parte desta planilha. A relação completa dos protocolos que foram priorizados encontra-se no anexo 2.

Tabela 6.2: Classificação de protocolos e aplicações

Porta	Descrição	Classe
any	Tráfego não classificado	BAIXA
ftp-data	Dados de FTP	BAIXA
ftp	Controle de Dados de FTP	BAIXA
cmd	Remote Copy	BAIXA
1352	Notes	REGULAR
8080	HTTP via Proxy	MÉDIA
3600-3602	SAPR3	MÉDIA
3200 3202	SAPR3	MÉDIA
9401	Distribuição de profiles	MÉDIA
9494-9495	Conexão Gateway-Endpoint/Conexão Endpoint-Gateway	ALTA
telnet	Telnet	ALTA
3389	RDP/WTS	ALTA
3500	FEP Autorização	ALTA
xot	XOT	ALTÍSSIMA

[85] Interface de rede local com taxa de transmissão de 100 Mbps.

A partir desta tabela, as listas de acesso foram configuradas como no exemplo a seguir:

```
access-list 117 remark prioridade baixa (FTP, RSH, OUTROS)
access-list 117 permit tcp any any eq ftp-data
access-list 117 permit tcp any eq ftp-data any

access-list 118 remark prioridade media (SQL, SAP, HTTP, OUTROS)
access-list 118 permit tcp any any eq 8080
access-list 118 permit tcp any eq 8080 any

access-list 119 remark prioridade alta (TELNET, VNC, SNMP, OUTROS)
access-list 119 permit tcp any any range 9494 9495
access-list 119 permit tcp any range 9494 9495 any

access-list 120 remark prioridade altissima (X25 over IP)
access-list 120 permit tcp any any eq 1998
access-list 120 permit tcp any eq 1998 any

access-list 121 remark prioridade regular (NOTES)
access-list 121 permit tcp any any eq 1352
access-list 121 permit tcp any eq 1352 any
```

A listagem completa das listas de acesso que foram codificadas encontra-se no anexo 3.

Deve-se observar que, em alguns casos, foi utilizada a porta TCP, enquanto que em outros a porta UDP, a depender da aplicação sendo classificada. Outro ponto que deve ser notado é que foram incluídas duas linhas para cada aplicação ou protocolo classificado, cada uma delas correspondendo a um sentido do tráfego. Dessa forma são marcados tanto os pacotes destinados a estas portas TCP/UDP, quanto as que forem originadas dessas mesmas portas.

Tendo sido definidas as listas de acesso, o passo seguinte foi o mapeamento dessas listas para as classes a serem utilizadas pela *policy-map* de marcação de pacotes. Isto foi feito através de comandos "***class-map***", que fazem referência às listas de acesso configuradas. Este comando pode ser observado na sintaxe abaixo. As palavras à direita das exclamações são apenas comentários, que não são considerados pelo roteador:

```
class-map match-all tag-alta
  match access-group 119     ! Pacotes de Tivoli, RDP, Telnet, etc
class-map match-all tag-media
  match access-group 118     ! Pacotes de SAP, HTTP, etc
class-map match-all tag-regular
  match access-group 121     ! Somente Pacotes NOTES
class-map match-all tag-baixa
  match access-group 117     ! Pacotes de FTP, RSH, outros
```

Definiu-se, então, a *policy-map* que iria marcar os pacotes conforme sua classificação:

```
policy-map tag-dscp
  class tag-alta
   set ip dscp af42    ! IP Precedence = 4, Medium Drop (dscp 36)
  class tag-media
   set ip dscp af32    ! IP Precedence = 3, Medium Drop (dscp 28)
  class tag-regular
   set ip dscp af22    ! IP Precedence = 2, Medium Drop (dscp 20)
  class tag-baixa
   set ip dscp af13    ! IP Precedence = 1, High Drop (dscp 14)
```

Finalmente aplicou-se esta *policy-map* na interface *Fast Ethernet* do roteador:

```
interface FastEthernet0
   service-policy input tag-dscp
```

Com isso, obteve-se a classificação e a marcação dos pacotes. O passo seguinte foi a configuração da *policy-map* de priorização do tráfego.

6.2.2 Priorização do tráfego

Foi definido, em conjunto com o cliente, que a cada classe de serviço fosse proporcionada uma garantia de banda e priorização, conforme a tabela 6.1.

Para o tratamento e garantia de bandas das diversas classes de serviço estipuladas, foram estabelecidas *policy-maps* de *QoS* a serem aplicadas nas interfaces de saída dos roteadores das pontas e nas interfaces de ligação dos roteadores no núcleo da rede. Para estas *policy-maps* foram aplicadas as seguintes técnicas:

1. Para classe de voz estipulou-se uma fila prioritária com reserva de banda suficiente para passagem do número de canais de voz correspondentes a cada *site*. O valor da banda reservada levou em consideração o *codec* utilizado. Neste caso, foi utilizado o *codec* G.729a. Conforme visto no capítulo 4, este *codec*, quando utilizado em conjunto com técnicas de compressão de cabeçalhos e de fragmentação de nível 2, produz um consumo de banda de 11.2 kbps por canal de voz. Dessa forma, utilizamos o valor de 12 kbps por canal como valor base para voz nas configurações das *policy-maps*;

2. Para a classe altíssima, correspondente ao tráfego X.25, foi efetuada uma reserva de banda equivalente à quantidade de dados estimada para este protocolo em cada *site*. Esta quantidade foi estimada pelo cliente em cerca de 5%, em média, do total da banda após a reserva para voz. Neste caso, teve que ser observado, ainda, o limite mínimo de 4 kbps, que é a banda mínima exigida pelo protocolo na aplicação do cliente;

3. Para a classe alta, foi efetuada uma reserva de banda equivalente cerca de 20%, em média, do total da banda após a reserva para voz;

4. Para a classe média, foi efetuada uma reserva de banda equivalente à quantidade de dados estimada pelo cliente para esta classe, cerca de 25% do total da banda após a reserva para voz;

5. Para a classe regular, foi efetuada uma reserva de banda equivalente à quantidade de dados estimada para o protocolo Notes em cada site, por volta de 40% em média do total da banda após a reserva para voz. Adicionalmente foi aplicada a técnica de WRED (i.e. *Weighted Random Early Detection*) que visa efetuar descarte seletivo de pacotes, a depender da precedência dos mesmos, de forma a prevenir a ocorrência de congestionamentos na rede. Isso se deve ao fato de que nesta classe foram também incluídos os pacotes com precedência 6 e 7, correspondentes aos pacotes de controle da rede. Essa inclusão visou dar uma maior garantia para estes pacotes e permitir que se fizesse a reserva de banda de um valor maior que os 75% recomendados para não comprometimento deste tipo de tráfego. Com isso, em caso de congestionamento, os pacotes com precedência menor têm preferência no descarte, preservando os protocolos de controle da rede;

6. Para a classe baixa, ficou destinada a banda restante do enlace, cerca de 10% em média do total da banda após a reserva para voz. Adicionalmente, foi também aplicada a técnica de WRED (i.e. *Weighted Random Early Detection*) visando efetuar o descarte seletivo de pacotes, dependendo da precedência dos mesmos.

6.2.3 Codificação das *policy-maps*

A sintaxe para a configuração das *policy-maps*, levando-se em consideração as classes desejadas, é a seguinte:

```
policy-map nome
  class voz
       priority banda
  class altissima
   bandwidth percent percetual
  class alta
   bandwidth percent percentual
  class media
   bandwidth percent percentual
  class regular
   bandwidth percent percentual
   random-detect
  class class-default
   fair-queue
   random-detect
```

Para que esta *policy-map* possa ser configurada é preciso que se configure, antes, os "*map-classes*" abaixo, de forma a se mapear as classes de acordo com a marcação feita antes nos pacotes:

```
class-map match-all voz
  match ip precedence 5      ! Pacotes de voz
class-map match-all altissima
  match access-group 120     ! Pacotes de XOT
class-map match-all alta
  match ip dscp AF42         ! Telnet, etc. (DSCP 36)
class-map match-all media
  match ip dscp AF32         ! SAP, HTTP, etc (DSCP 28)
class-map match-all regular
  match ip precedence 2 6 7  ! Notes e Network Control
```

Dessa forma parece ser simples a configuração das *policy-maps* necessárias para se obter os níveis de *QoS* constantes na tabela 6.1. A sintaxe faz parecer que bastaria substituir os parâmetros banda pelo valor de 12 kbps x número de canais e os parâmetros de percentual pelos valores de 5, 20, 25 e 40, respectivamente. No entanto, a sintaxe dos comandos de *policy-map* esconde um detalhe que torna esta configuração bem mais difícil do que parece à primeira vista. Os valores que são configurados nos parâmetros *percent* de cada classe, referem-se ao percentual da banda total do enlace, e não à banda remanescente após a reserva para voz feita pelo comando *priority*. Com isso, todos os valores têm que ser recalculados para refletir os percentuais reais desejados.

Para um melhor entendimento deste mecanismo, consideremos o exemplo de uma *policy-map* que seria aplicada em um enlace de 96 kbps de CIR e 2 canais de voz. Para a classe voz, o valor a ser configurado corresponde ao número de canais de voz (i.e.

2) multiplicado pela banda considerada para cada canal (i.e. 12 kbps). Assim, a classe voz seria configurada desta forma:

```
policy-map qos-exemplo
  class voz
    priority 24
```

Com a alocação de 24 kbps para voz, restam, do enlace de 96 kbps, 72 kbps para distribuição entre as outras classes. Para a classe altíssima, deseja-se um percentual de 5% da banda remanescente do enlace, que é igual a 3,6 kbps. Mas, conforme comentado anteriormente, a aplicação de X.25, que faz uso da classe altíssima, requer uma banda de 4 kbps, no mínimo. Assim sendo, através de uma regra de três simples, constatamos que 4 kbps é igual a 4,16% de 96 kbps. Assim, o valor a ser configurado para esta classe seria de 4,16. No entanto, a sintaxe do comando somente aceita números inteiros. Dessa forma, temos que considerar o valor inteiro imediatamente acima, ou seja, 5%. Com isso, a classe altíssima fica com a seguinte sintaxe:

```
class altissima
  bandwidth percent 5
```

Repare que, neste caso, o valor configurado acabou sendo igual aos 5% desejados inicialmente, mas tratou-se apenas de uma coincidência gerada pelos limites e valores considerados. Com esta configuração, a classe altíssima obteve uma garantia real de 4 kbps, já que os valores reservados pelo roteador também são arredondados, neste caso sempre para baixo. Essa banda corresponde a 5,6% da banda remanescente do enlace (i.e. 72 kbps). Dessa forma a banda real obtida para esta classe ficou sendo igual a 5,6% da banda disponível do enlace.

Cálculo semelhante deve ser aplicado às demais classes. Para classe alta, por exemplo, deseja-se 20% da banda de 72 kbps. Isso corresponde a 14,4 kbps. Por regra de três, verifica-se que este valor corresponde a 15% de 96 kbps. Com o arredondamento feito pelo roteador na reserva, a garantia real é de 14 kbps, correspondente a 19,4% da banda. Veja que, desta vez, não houve coincidência de valores e que, para uma reserva desejada de 20% da banda, o valor a ser configurado é de 15%. Assim, esta classe deve ser configurada da seguinte forma na *policy-map*:

```
class alta
  bandwidth percent 15
```

Repare que, devido aos arredondamentos envolvidos tanto na sintaxe quanto na aplicação da reserva pelo roteador, os percentuais atingidos dificilmente coincidirão exatamente com os que se deseja, porém valores bastante próximos podem ser obtidos, como nos dois exemplos acima.

Aplicando-se os mesmos cálculos para as demais classes, ficamos com a *policy-map* configurada da seguinte forma:

```
policy-map qos-exemplo
class voz
   priority 24          ! Banda garantida para 2 canais de voz
  set ip dscp EF        ! Precedence = 5 (DSCP 46)
class altissima
  bandwidth percent 5   ! 5% de 96K = 5,26% de 72K (4K)
  set ip dscp AF41      ! Precedence = 4, baixo descarte (DSCP 34)
class alta
  bandwidth percent 15 ! 15% de 96K = 19,4% de 72K (14K)
class media
  bandwidth percent 19 ! 19% de 96K = 25% de 72K (18K)
class regular
  bandwidth percent 30 ! 30% de 96K = 40% de 72K (28K)
  random-detect         ! Weighted Random Early Detection (WRED)
class class-default
  fair-queue            ! Restante = 11,1% de 72K (8K)
  random-detect         ! Weighted Random Early Detection (WRED)
```

Note-se que, conforme mencionado anteriormente, para as classes voz e altíssima, além de fazer a priorização dos pacotes, esta *policy-map* está também efetuando a marcação dos mesmos, já que não havia outra forma de fazê-lo em conjunto com as demais classes. Com isso, esta *policy-map* deve ser diferente nos roteadores de borda e do núcleo. Nestes últimos, os comandos "***set ip dscp***" devem ser retirados, já que não deve ser função dos roteadores centrais efetuar a marcação de pacotes.

É importante se observar, também, qual é a referência utilizada pelo roteador como base para os valores a serem reservados. Para o cálculo desses valores, o roteador utiliza-se do que for configurado como CIR no *map-class* associado ao PVC em questão (no caso de enlace *Frame Relay*). Caso não seja configurado um valor para CIR, o valor considerado será o que for configurado pelo comando "***bandwidth***" da interface. Em enlaces PPP, o valor utilizado também é o do "***bandwidth***".

Deve-se notar, ainda, que, apesar de ser possível se configurar o parâmetro *bandwidth* nas sub-interfaces de uma interface *Frame Relay*, o valor que o roteador utiliza é sempre o que está configurado na interface principal. Isso pode causar grandes problemas no caso de interfaces com muitas sub-interfaces. Caso seja configurado o *bandwidth* total (i.e. agregado) na interface principal, ao se tentar reservar um percentual da banda para as classes de um PVC, os valores calculados serão relativos ao total do enlace e não à banda do circuito virtual. Se, por outro lado, for configurado um *bandwidth* na interface principal igual ao *bandwidth* de cada PVC, não será possível reservar-se banda para mais de uma sub-interface, já que o roteador irá informar que não há mais banda disponível a partir da configuração do segundo enlace. Por este motivo, é muito importante a configuração de *map-classes* com parâmetros corretos de CIR e MinCIR em PVCs *Frame Relay*, conforme será explicado mais adiante no tópico "Condicionamento de Tráfego".

Outro detalhe interessante, que pode causar bastante confusão, é que não existe correlação entre o nome da codificação DSCP e seu valor em decimal ou binário. Assim, o DSCP AF41, por exemplo, corresponde ao valor de DSCP 34. A tabela 3.1, contida no capítulo 3, traz os valores em binário e decimal para os DSCP dos PHB padronizados para o *DiffServ*. A depender do modelo de roteador que se está usando e da versão de IOS® utilizada pelo mesmo, a sintaxe da configuração exibida por comandos de *show* pode indicar o nome da classe AF ou seu valor decimal equivalente. Para os comandos de configuração, no entanto, ambas as formas são aceitas.

6.2.3.1 Ferramenta de configuração de *Policy-maps*

Conforme pôde ser observado pelo exemplo acima, a configuração da *policy-map* de priorização não é tão simples como pode parecer à primeira vista. Em uma rede como a deste projeto, em que havia um grande número de perfis diferentes de lojas, com diferentes valores de velocidade de enlaces e números de canais de voz, o trabalho despendido na configuração dessas *policy-maps* pode ser bastante grande e sujeito a diversos erros. Para facilitar este trabalho e minimizar a incidência de configurações erradas, foi desenvolvida uma ferramenta que monta a *policy-map* desejada a partir das informações de banda (i.e. CIR) do circuito, do número de canais de voz a serem

atendidos e dos percentuais desejados para cada classe. Esta ferramenta efetua todos os cálculos e arredondamentos e fornece a *policy-map* pronta para ser colada na configuração do roteador.

Para utilização desta ferramenta, cuja aparência pode ser vista na figura 6.2, deve-se preencher os valores das células em itálico. O texto dentro da área quadriculada pode, então, ser copiado e colado diretamente no *prompt* de configuração do roteador. Os valores na coluna "QoS Real" representam os percentuais reais de *QoS* obtidos pela aplicação da *policy-map*.

Esta ferramenta foi desenvolvida para atender especificamente ao projeto descrito neste trabalho, e gera a *policy-map* com as classes que foram requisitadas pelo cliente. No entanto, ela pode ser facilmente adaptada para outras necessidades.

Um ponto a ser observado é que a sintaxe do comando ***"bandwidth"*** admite a omissão do parâmetro *percent* sendo que, neste caso, o valor seria configurado diretamente em kbps, ao invés de um percentual da banda do enlace. O inconveniente, neste caso, é que o comando nesta sintaxe aceita como mínimo o valor de 8 kbps. Neste caso, ficaríamos impossibilitados de configurar nossa *policy-map* como no exemplo anterior, onde pudemos reservar um valor de apenas 4 kbps para uma de nossas classes.

PRIORIDADE	*QoS* Cliente	*QoS* Desejado	Banda (kbps)	*QoS* Real	Banda Real
Altíssima (Xot)	5,0%	*5,0%*	3,6	5,6%	4
Alta (Telnet, Vnc)	20,0%	*20,0%*	14,4	19,4%	14
Média (Sap,Http)	25,0%	*25,0%*	18,0	25,0%	18
Regular (Notes)	40,0%	*40,0%*	28,8	38,9%	28
Baixa (Ftp, Default)	10,0%	10,0%	7,2	11,1%	8
Total Global	100,0%	100,0%	72,0	100,0%	72

Banda do Link (kbps): *128*
CIR do Link (kbps): *96*
Canais de voz (qtde): *2*
Banda de Voz (kbps): 24
Banda de Voz (%): 25
Banda Restante (kbps): 72
Banda Restante (%): 75

```
policy-map qos-exemplo
 class voz
  priority 24
  set ip dscp ef
 class altissima
  bandwidth percent 5
  set ip dscp af41
 class alta
  bandwidth percent 15
 class media
  bandwidth percent 19
 class regular
  bandwidth percent 30
  random-detect
class class-default
  fair-queue
  random-detect
```

Figura 6.2 – Ferramenta para configuração de *policy-map* de *QoS*

Deve-se notar que esta não é a forma mais comum de implementação de *Policies* de *QoS* em roteadores *Cisco*. Existe uma recomendação da *Cisco* de que não mais do que 75% da banda do enlace sejam utilizados na reserva de banda pelas classes. Dessa forma, pelo menos 25% da banda total deveria ser alocada para a classe *default*. Esta recomendação visa garantir que os pacotes de controle da rede possam fluir livremente, evitando que ocorram problemas nos protocolos de roteamento e nos pacotes de *keepalive.* No caso específico desta implementação, os pacotes deste tipo, que têm valores de precedência IP iguais a 6 e 7, foram mapeados para a classe "Regular" lhes

garantindo uma reserva de banda igual a 40%. Dessa forma pôde-se reservar menos de 25% para a classe *default*. Para uma implementação mais "clássica", no entanto, também foi desenvolvida uma segunda versão desta ferramenta (figura 6.3). Neste caso, além da reserva de 25% para a classe *default*, utilizou-se, o comando ***"bandwidth"*** na forma de valores absolutos, ao invés de valores percentuais.

PRIORIDADE	QoS Cliente	Banda (kbps)	QoS Total	QoS Relativo	QoS s/ X.25
Voz (Voip)	-	12,0	18,8%	-	-
Altíssima (Xot)	-	8,0	12,5%	15,4%	-
Alta (Telnet, Vnc)	20,0%	*8,0*	12,5%	15,4%	18,2%
Média (Sap,Http)	25,0%	*9,0*	14,1%	17,3%	20,5%
Regular (Notes)	40,0%	*11,0*	17,2%	21,2%	25,0%
Baixa (Ftp, Default)	10,0%	16,0	25,0%	30,8%	36,4%
Total Global	95,0%	64,0	100,0%	100,0%	100,0%

Banda do Link (kbps): *64*
MinCIR do Link (kbps): *64*
Canais de voz (qtde): *1*
Banda Reservável (75%): 48
Banda de Voz (kbps): 12
Banda Restante (kbps): 36
Banda QoS (kbps): 52
Banda QoS s/ X.25 (kbps): 44

```
policy-map qos-exemplo
 class voz
  priority 12
 set ip dscp ef
class altissima
  bandwidth 8
 class alta
  bandwidth 8
class media
  bandwidth 9
class regular
  bandwidth 11
class class-default
  fair-queue
random-detect
```

Figura 6.3 – Ferramenta para configuração de *policy-map* de *QoS* – Versão 2

6.2.4 Condicionamento de tráfego

Conforme visto nos capítulos 3 e 4, técnicas de condicionamento de tráfego se fazem necessárias para se moldar o padrão de transmissão em enlaces de baixa velocidade de forma a torna-lo adequado aos requisitos de tráfego multimídia, como é o caso de Voz sobre IP. No caso de enlaces *Frame Relay*, pode-se se utilizar técnicas de *Traffic Shaping* (i.e. Suavização de Tráfego) para impedir que a ocorrência de rajadas de tráfego produza variações no atraso e perdas de pacotes que impossibilitem uma transmissão eficaz de voz. Além disso, é interessante se aplicar fragmentação de quadros *Frame Relay*, para impedir que o efeito da serialização interfira negativamente na qualidade do fluxo transmitido. Em enlaces que utilizam protocolo PPP, pode-se aplicar a fragmentação e o *interleaving* dos pacotes de dados, através do *Multilink PPP*.

As configurações que foram apresentadas até agora tinham uma sintaxe única, quer seja para roteadores de pequeno porte, como os da linha 1700 utilizados nas lojas em nosso projeto, quer seja em roteadores de grande porte, como os 7507 que utilizados no núcleo da rede. Já as técnicas que iremos ver a seguir, são configuradas de forma distinta a depender do porte do roteador e serão apresentados separadamente.

6.2.4.1 A arquitetura da família 7500

Os roteadores de grande porte da *Cisco*, como os da linha 7500, trabalham com uma arquitetura distribuída. Todo o *hardware* do equipamento é distribuído por placas que possuem processadores independentes. A placa RSP (i.e. *Route Switchig Processor*) constitui-se no coração do roteador. Esta placa, a princípio, processa todas as funções de processamento e roteamento do equipamento. Neste modelo de roteador, no entanto, as placas adaptadoras de interfaces (i.e. *interface adapters*), ao invés de serem instaladas em *slots* simples, como em roteadores de menor porte, são instaladas em placas chamadas VIP – *Versatile Inteface Processors*. Estas placas possuem inteligência própria e, desde que corretamente configuradas, tomam pra si parte do processamento que seria feito pela placa RSP. Com isso tem-se um equipamento bem mais escalável e versátil, que pode aumentar à medida que seja necessário, bastando que sejam adicionadas novas VIPs com os cartões de interfaces.

Por outro lado, a presença das placas VIP faz com que alguns recursos tenham sua forma de configuração totalmente distinta do modo que são configurados em equipamentos de menor porte, o que pode confundir quem precise efetuar estas programações e não tenha experiência com este tipo de equipamento. Uma dessas diferenças, por exemplo, reside na forma de se configurar o *Frame Relay Traffic Shaping*. Diversos dos comandos que são usados em equipamentos menores não são aceitos em um modelo 7500 com placas VIP. O próprio roteador informa que deve ser configurado o recurso de DTS, ou seja, *Distributed Traffic Shaping*, (i.e. ou Suavização de Tráfego Distribuída). A funcionalidade oferecida pelo DTS é exatamente a mesma do *Traffic Shaping* executado pelos roteadores menores. A diferença é que, ao invés de ser processado pela RSP, o DTS é processado pela CPU da própria placa VIP.

Nos tópicos a seguir são mostradas as configurações com as sintaxes referentes aos roteadores de menor porte e, onde for aplicável, também as diferenças para roteadores baseados em RSP e VIPs.

6.2.4.2 Configurações em *Frame Relay*

Para enlaces *Frame Relay*, foram aplicadas as técnicas de *Frame Relay Traffic Shaping* e a fragmentação *Frame Relay Forum 12* (i.e. FRF.12).

6.2.4.2.1 Configurações em roteadores sem placas VIP

Para moldagem do tráfego e a fragmentação de quadros de nível 2 através de *Frame Relay Traffic Shaping* em roteadores de menor porte, deve-se, primeiramente, habilitar-se o *Traffic Shaping* na interface com o comando "***frame-relay traffic-shaping***". Este comando deve figurar na interface principal (i.e. interface cheia) do enlaces, como a seguir:

```
interface Serial0
 bandwidth 128
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
```

Em seguida deve-se criar um *map-class* e aplicá-lo ao PVC na sub-interface correspondente:

```
map-class frame-relay map-class-exemplo
 frame-relay cir 96000
 frame-relay bc 960
 frame-relay be 0
 frame-relay mincir 96000
 no frame-relay adaptive-shaping
 service-policy output qos-exemplo
 frame-relay fragment 160

interface Serial0.1 point-to-point
 bandwidth 128
 ip address 10.6.18.142 255.255.255.252
 ip ospf network point-to-point
 frame-relay interface-dlci 597
  class map-class-exemplo
 frame-relay ip tcp header-compression
 frame-relay ip rtp header-compression
```

Repare no *map-class* acima, em negrito, a presença do comando "***service-policy output***". Este comando faz a aplicação da *policy-map* de *QoS* vista no tópicos anteriores. Repare, também, nos comandos de *header-compression* de TCP e RTP. Eles executam a compressão dos cabeçalhos de TCP e de RTP de forma a se obter uma melhor eficiência no enlace, necessária para otimização do consumo de banda.

Os comandos do *map-class* aplicados ao PVC devem seguir a seguintes regras (Cisco, 2003g):

1. *CIR*: Para enlace pelos quais trafegarão somente dados, sem tráfego interativo, este parâmetro deve ser configurado com a velocidade nominal do circuito. Já no caso de enlaces que transportem voz, este comando deve ser configurado com o CIR contratado com a prestadora de serviço *Frame Relay*. Do contrário, o tráfego acima desta taxa seria reduzido para o valor de MinCIR em caso de congestionamento da rede, o que poderia causar variações no *delay* e no *jitter* . No nosso exemplo, este parâmetro foi configurado com 96000, que é o CIR de nosso circuito de 128 kbps;

2. *BC*: Para enlaces de dados, este comando normalmente é configurado com o valor do CIR/8, de forma a se obter TC = 125 ms. Já para enlaces que transportem voz, configura-se este valor para CIR/100, assim teremos TC = 10 ms, o que minimiza o tempo de delay para pacotes de voz;

3. *BE*: Configurar sempre como 0 (zero). Dessa forma o roteador não irá enviar tráfego em rajada acima do valor de BC, assegurando a melhor condição para garantia dos parâmetros de qualidade para a transmissão de voz;

4. *MinCIR*: Configura-se com o valor do CIR do circuito. Este é o menor valor para o qual o roteador irá baixar sua taxa de transmissão em caso de congestionamento na rede. Caso o valor de CIR e MinCIR sejam iguais, a taxa de transmissão se manterá constante, situação ideal para transmissão de tráfego interativo;

5. *Adaptive-shaping*: deve ser habilitado para enlaces de dados e desabilitado para enlaces que transportem voz. Dessa forma a taxa de transmissão não será alterada em caso de congestionamento na rede. A habilitação deste parâmetro só faz sentido em casos em que os valores de CIR e de MinCIR sejam diferentes;

6. *Fragment*: deve ser de 80 bytes para cada 64 kbps de velocidade do circuito. Isso garante que o tempo de serialização dos pacotes seja inferior a 10 ms, garantindo o envio de pacotes de voz com o mínimo de delay no circuito. No nosso exemplo, o enlace é de 128 kbps, portanto o fragmento deve ser configurado como 160 bytes.

6.2.4.2.2 Configurações em roteadores com placas VIP

Conforme visto antes, no caso de roteadores com placas VIP, deve ser configurado o recurso de DTS (i.e. *Distributed Traffic Shaping*), ao invés do *Frame Relay Traffic Shaping* convencional. A primeira diferença está na interface principal do enlace *Frame Relay*. Ao contrário do que ocorre em roteadores menores, neste tipo de roteador, não se deve configurar o comando "***frame-relay traffic-shaping***" nesta interface. Assim sendo, as configurações da interface principal, e de uma sub-interface, em um roteador com placa VIP ficam assim:

```
interface Serial1/1/0:17
 bandwidth 128
 no ip address
 encapsulation frame-relay

interface Serial1/1/0:17.1 point-to-point
 bandwidth 128
 ip address 10.6.18.137 255.255.255.252
 frame-relay interface-dlci 597
  class map-class-exemplo
 frame-relay ip tcp header-compression
 frame-relay ip rtp header-compression
```

Como se vê, exceto pela ausência do comando de *traffic-shaping*, a sintaxe, neste caso, é bastante semelhante. As maiores diferenças começam a surgir na configuração do *map-class*:

```
map-class frame-relay map-class-exemplo
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 service-policy output shape-exemplo
 frame-relay fragment 160
```

A fragmentação FRF.12 é configurada de forma idêntica ao que é feito com roteadores menores (i.e. através do comando "***frame-relay fragment***") mas, neste caso, não são configurados aqui os parâmetros de *traffic shaping*. Ao invés disso, este *map-class* deve chamar uma *policy-map* onde são configurados estes parâmetros da seguinte forma:

```
Policy-map shape-exemplo
  class class-default
    shape average 96000 384 384
  service-policy output qos-exemplo
```

Os parâmetros do comando "***shape average***" são CIR, BC e BE. No entanto, a *Cisco* recomenda não configurar os parâmetros BC e BE neste caso, que são calculados automaticamente pelo algoritmo da placa VIP e são completados com os valores considerados ótimos para o funcionamento do *traffic shaping*. No caso de enlaces de voz, como no nosso exemplo, os valores de CIR e MinCIR são idênticos, e este último não precisa ser configurado, pois o roteador assume o mesmo valor para ambos. Já para enlaces de dados o valor de MinCIR pode ser configurado pelo comando "***shape adaptive***", que tem como argumento o valor de MinCIR.

Repare, ainda, que a *policy-map* ***"shape-exemplo"*** acima, chama a *policy-map* **"*qos-exemplo*"**, que é nossa *policy-map* de priorização de dados.

6.2.4.3 Configurações em PPP

No caso de enlaces PPP, é necessário se configurar a fragmentação dos quadros, para se evitar o efeito da serialização na qualidade do áudio transmitido. Isto é obtido através do recurso de *Multilink PPP*. Este recurso foi criado para se agrupar dois ou mais enlaces PPP como se fossem um só, de forma a otimizar a utilização de banda em

um feixe de enlaces. No caso de transmissão de voz, no entanto, devemos usar o *Multilink PPP* mesmo quando temos um único enlace ponto a ponto. Isso porque precisamos dos comandos de "***fragment-delay***" e "***interleave***", que não existem no PPP original. A sintaxe, neste caso, é a seguinte:

```
interface Serial0
 bandwidth 128
 no ip address
 encapsulation ppp
 no ip route-cache
 no ip mroute cache
 ppp multilink
 multilink-group 1
!
interface Multilink1
 ip address 10.6.17.153 255.255.255.252
 no ip route-cache cef
 no cdp enable
 ppp multilink
 ppp multilink-fragment delay 10
 ppp multilink interleave
 multilink-group 1
 service-policy output qos-exemplo
```

Neste caso a configuração é mais simples que no *Frame Relay*. Não há necessidade de *traffic-shapping*, uma vez que o enlace PPP é uma conexão física totalmente privativa e não está sujeita às variações de uma rede compartilhada como a *Frame Relay*. O valor de fragmento é automaticamente calculado de acordo com o valor de *bandwidth* e de *delay* configurados. Também a *policy-map* de priorização é diretamente configurada sob a interface *multilink*, não existindo *map-class*. Estas configurações são idênticas tanto para o 7500 como para os roteadores menores.

Para maiores detalhes sobre a sintaxe dos comandos apresentados neste tópico, consulte *Cisco IOS Software Releases 12.2 Mainline CS3: Part 3: Quality of Service Solutions* (Cisco, 2003h).

6.3 Verificação das configurações

Uma série de comandos pode ser utilizada para a verificação do funcionamento das configurações que foram expostas. Com estes comandos é possível se verificar se as configurações foram efetuadas corretamente e como estão se comportando os recursos configurados. Pode-se, por exemplo, verificar se estão ocorrendo descartes de pacotes IP em alguma das classes de *QoS* estabelecidas ou descarte de fragmentos de *frames* em enlaces *Frame Relay*.

Para verificação do funcionamento das configurações de *traffic shaping* (i.e. Suavização de Tráfego), pode-se utilizar os comandos "***show frame-relay pvc***" e "***show policy-map interface***". A sintaxe é a mesma para qualquer modelo de roteador. As informações exibidas, no entanto, podem variar a depender do modelo e da versão de IOS® presente em cada equipamento.

6.3.1 Roteadores sem placas VIP

A seguir é exibido o resultado, de forma reduzida, do comando "***show frame-relay pvc***" em um roteador sem placas VIP. O resultado completo deste comando pode ser visualizado no anexo 4.

```
ROUTER-7206#sh frame-relay pvc 515

PVC Statistics for interface Serial1/1:15 (Frame Relay DCE)

DLCI = 515, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1/1:15.1

  input pkts 983827        output pkts 1180489   in bytes 58929519
  out bytes 185628468      dropped pkts 1472     in pkts dropped 1472
  out pkts dropped 0       out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 61979     out bcast bytes 12762566
  pvc create time 3d21h, last time pvc status changed 3d21h
  service policy QoS-Super
  Serial1/1:15.1: DLCI 515

  Service-policy output: QoS-Super

    Class-map: voz (match-all)
      688532 packets, 44043040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 24
        Bandwidth 24 (kbps) Burst 600 (Bytes)
        (pkts matched/bytes matched) 688532/44043040
        (total drops/bytes drops) 0/0

    Class-map: class-default (match-any)
      133246 packets, 25564621 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Weighted Fair Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 16
        (total queued/total drops/no-buffer drops) 0/0/0
         exponential weight: 9

class  Transmitted  Random drop   Tail drop   Minimum  Maximum  Mark
       pkts/bytes   pkts/bytes    pkts/bytes  thresh   thresh   prob
0     53710/10779604   0/0          0/0          64      128   1/10
1     17826/2986466    0/0          0/0          71      128   1/10
2         0/0          0/0          0/0          78      128   1/10
3         0/0          0/0          0/0          85      128   1/10
4         0/0          0/0          0/0          92      128   1/10
5         0/0          0/0          0/0          99      128   1/10
6         0/0          0/0          0/0         106      128   1/10
7         0/0          0/0          0/0         113      128   1/10
rsvp      0/0          0/0          0/0         120      128   1/10

  Output queue size 0/max total 600/drops 0
  fragment type end-to-end         fragment size 80
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 64000     byte increment 80    BECN response no
  frags 2510585   bytes 152510075 frags delayed 1520830   bytes
  delayed 123292325
  shaping active
```

Pela saída exibida pelo roteador no comando anterior, é possível se verificar os parâmetros de *traffic-shaping* (i.e. CIR, MinCIR, BC, Be) e de fragmentação (em negrito). É possível se verificar, também, quais os percentuais de banda configurados em cada classe (neste caso, por ter sido resumido, o comando exibe apenas os valores para a classe "voz"), qual o tráfego constatado no roteador para cada uma delas, e se houve *drops* (i.e. descartes) de pacotes em alguma das filas. Estas informações são bastante úteis na checagem da adequação das configurações aplicadas. Descartes na classe de voz, por exemplo, podem indicar que o tráfego para esta classe foi incorretamente estimado, podendo ter sido considerado um número incorreto de canais de voz. Da mesma forma, descartes excessivos em algumas das outras classes, podem indicar erro na estimativa de tráfego para as configurações ou outros tipos de problemas no perfil de tráfego.

Pode-se observar, ainda, que na classe *class-default*, o roteador indica qual o tráfego constatado para cada uma das precedências IP (*class*). Isso se deve ao fato de ter sido configurado, nesta classe, o recurso de detecção WRED, que promove o descarte seletivo de pacotes em caso de congestionamento na rede (vide capítulo 3).

6.3.2 Roteadores com placas VIP

Abaixo se pode observar que o comando "***show frame-relay pvc***" produz uma saída totalmente diferente no roteador modelo 7507, que possui placas VIP.

```
ROUTER-7507#sh frame-relay pvc 515

PVC Statistics for interface Serial1/1/0:15 (Frame Relay DCE)

DLCI = 515, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1/1/0:15.1

  input pkts 90786          output pkts 529064        in bytes 14409044
  out bytes 62141701        dropped pkts 1738         in pkts dropped 0
  out pkts dropped 1738     out bytes dropped 1586354
  late-dropped out pkts 1738         late-dropped out bytes 1586354
  in FECN pkts 0            in BECN pkts 0            out FECN pkts 0
  out BECN pkts 0           in DE pkts 0              out DE pkts 0
  out bcast pkts 62003      out bcast bytes 12857496
  pvc create time 3d22h, last time pvc status changed 3d22h
  fragment type end-to-end          fragment size 80
```

Neste caso, para se obter as mesmas informações do exemplo anterior, deve-se utilizar o comando "***show policy-map interface***", que apresenta uma saída semelhante a

do comando "***show frame-relay pvc***" em um roteador menor. O resultado completo deste comando pode ser visto no anexo 4:

```
ROUTER-7507#show policy-map interface Ser 1/1/0:15.1

 Serial1/1/0:15.1: DLCI 515 -

  Service-policy output: Shape-Super

    queue stats for all priority classes:
      queue size 0, queue limit 6
      packets output 186334, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0

    Class-map: class-default (match-any)
      525137 packets, 62075582 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      queue size 0, queue limit 16
      packets output 529012, packet drops 1738
      tail/random drops 1738, no buffer drops 0, other drops 0
      Shape: cir 64000,  Bc 256,  Be 256
        lower bound cir 0,  adapt to fecn 0
        output bytes 54699253, shape rate 0 bps

      Service-policy : QoS-Super

        Class-map: voz (match-all)
          186334 packets, 11905141 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 5
          Priority: kbps 24, burst bytes 1500, b/w exceed drops: 0

        Class-map: class-default (match-any)
          22274 packets, 2714984 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          queue size 0, queue limit 1
          packets output 27661, packet drops 225
          tail/random drops 225, no buffer drops 0, other drops 0
          Fair-queue: per-flow queue limit 2
          Random-detect:
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0
       Class Random   Tail Minimum   Maximum    Mark       Output
             drop   drop threshold threshold  probabity  packets
       0          0      0         0         1     1/10      22093
       1          0      0         0         1     1/10       5568
       2          0      0         0         1     1/10          0
       3          0      0         0         1     1/10          0
       4          0      0         0         1     1/10          0
       5          0      0         0         1     1/10          0
       6          0      0         0         1     1/10          0
       7          0      0         0         1     1/10          0
```

É possível se perceber que, apesar de algumas diferenças na apresentação dos resultados, as informações obtidas pelos dois comandos nas duas plataformas diferentes

são basicamente as mesmas. Um detalhe para o qual deve-se atentar é que, no caso de roteadores com a placa VIP, os valores de *traffic-shaping* são exibidos sob a classe *shape*, logo no início da saída do comando "***show policy-map interface***". Isto se deve a configuração de DTS (i.e. *Distributed Traffic Shaping*) que é feita neste tipo de equipamento, conforme explicado anteriormente neste capítulo.

Para maiores detalhes e outros comandos para verificação de *QoS*, consulte *Cisco IOS Software Releases 12.2 Mainline CS3: Part 3: Quality of Service Solutions* (Cisco, 2003h).

6.4 Resultados obtidos

O ideal na implementação de um projeto como este é que se possa fazer avaliações qualitativas e quantitativas relativas ao desempenho da rede antes e após as alterações que são implementadas. Isso, no entanto, nem sempre é possível. Estas avaliações podem ser feitas, por exemplo, através da medição de tempos de resposta de aplicações ou da vazão da rede medida em aplicativos de transferência de arquivos ou ainda no índice de chamadas completadas e de quedas de ligações, no caso de transporte de voz. Em alguns casos, como quando se trata de uma rede nova, por exemplo, não há uma situação inicial com a qual se comparar os resultados obtidos. Em outros, as alterações inseridas são tão grandes que não é possível este tipo de comparação.

No caso do projeto analisado neste trabalho, as avaliações que se pôde obter foram mais subjetivas do que objetivas. Por restrições do cliente, não foi possível fazer um estudo relativo ao desempenho da rede anterior. A análise que teve que se restringir à observação dos indicadores tratados no tópico anterior e na resposta dos usuários quanto ao sentimento de qualidade da rede.

Através dos comandos apresentados, foi possível se perceber que a rede foi dimensionada de forma adequada, uma vez que não se notaram descartes freqüentes devido a congestionamento nos circuitos. Os recursos físicos dos roteadores (memória e processadores) também se mostraram adequados, após alguns ajustes que precisaram ser feitos e que serão tratados no capitulo 8.

Alguns indicativos mais objetivos em relação à melhora do desempenho da rede sentida pelos usuários referem-se a problemas que existiam antes das alterações e que

deixaram de ocorrer, como lentidão em momentos em que ocorriam transferências de FTP e baixa qualidade em ligações de voz.

6.5 Resumo do capítulo

Neste capítulo são apresentados os detalhes que foram observados na implementação de uma rede com recursos de *QoS* em um ambiente com roteadores *Cisco*. São focados os detalhes importantes a serem analisados em projetos desta natureza e as soluções que foram adotadas para as situações que foram enfrentadas. São também discutidos os resultados que foram obtidos com a execução deste trabalho.

No capítulo seguinte são detalhadas as configurações específicas a implementação de Voz sobre IP nesta mesma rede. Da mesma forma que neste capítulo, são enfatisados os detalhes importantes de serem observados em um trabalho desta natureza.

7 Implementando *VoIP* em uma rede com equipamentos *Cisco* – estudo de caso

Neste capítulo são detalhadas as configurações referentes a Voz sobre IP na rede onde foi efetuado o estude de caso deste trabalho. Assim como no capítulo anterior, são mostrados, na prática, os comandos e ajustes que devem ser feitos para se obter sucesso na implementação desse recurso na rede

7.1 Configurações de voz

Uma vez que se tenha definido e aplicado todas as configurações de *QoS* e condicionamento de tráfego, as configurações de voz não trazem grandes segredos. O primeiro passo consiste em configurar o *hardware* que fará a interface do roteador com um dispositivo de voz, que pode ser um PABX ou aparelho telefônico. Este *hardware* é o *voice-port.* Existem diversos tipos de *voice-ports*. Eles podem ser analógicos ou digitais e suportar os mais diferentes tipos de sinalização utilizados pelos fabricantes de PABX. As configurações irão variar a depender do tipo de placa usada e da sinalização escolhida. Abaixo segue o exemplo de um *voice-port* utilizando uma placa do tipo FXS[86] (i.e. *Foreign Exchange Station*), um dos tipos mais comuns de *voice-port* analógicos. Para maiores informações sobre outros tipos de *voice-port*, consulte *Voice Interface Cards* (Cisco, 2003i) e *Voice Hardware Compatibility Matrix* (Cisco, 2003j).

```
voice-port 1/0
 vad
 cptone BR
!
dial-peer voice 1 pots
 destination-pattern 11111
 port 1/0
```

As três primeiras linhas acima definem as opções do *voice-port*. Neste caso foi habilitada a detecção de voz (i.e. VAD) e configurados os tons de chamada e de discagem para o padrão brasileiro.

As linhas seguintes compõem o *dial-peer. Dial-peer* é o objeto de configuração que define um mapeamento de discagem. Neste caso, o *dial-peer* 1 define que chamadas para o número 11111 devem ser destinadas ao *voice-port* 1/0. Configurações adicionais,

[86] Interface que permite a ligação de equipamentos de telefone e PABX.

como manipulação de dígitos, podem ser também feitas diretamente no *dial-peer*. Repare que este *dial-peer* é do tipo POTS[87] (i.e. *Plain Old Telephony System*), o que significa que ele refere-se a uma conexão telefônica local.

Configurados o *voice-port* e o *dial-peer pots*, o passo seguinte é o mapeamento do plano de numeração da rede. Esse mapeamento pode ser feito de duas formas: através de *dial-peers* do tipo *voip* ou com a utilização de um *gatekeeper*.

7.1.1 Configuração via *Dial-Peers*

Conforme mencionado no capítulo anterior, em uma rede *VoIP* utilizando o protocolo H.323, todos os roteadores devem conhecer o endereço IP de destino para os quais irão encaminhar chamadas telefônicas. Isto pode ser obtido com a configuração de um *dial-peer voip* para cada destino da rede. Assim, por exemplo, um roteador que se estabeleça chamadas telefônicas com outros dois roteadores, poderia ter uma configuração de *dial-peers* desta forma:

```
dial-peer voice 200 voip
 destination-pattern 22222
 session target ipv4:10.2.2.2
 ip precedence 5
!
dial-peer voice 300 voip
 destination-pattern 33333
 session target ipv4:10.3.3.3
 ip precedence 5
```

Este tipo de configuração pode ser bastante simples e prático em redes com poucos pontos. Em topologias maiores, no entanto, a configuração de um *dial-peer voip* para cada ponto da rede em cada um dos roteadores que a compõem, pode trazer inconvenientes enormes aos seus administradores. A alternativa técnica a esta situação é a utilização de um *gatekeeper*.

7.1.2 Configuração via *Gatekeeper*

Por ser um elemento padronizado da arquitetura *VoIP*, a função de *gatekeeper* pode ser exercida por diversos tipos de *hardware* diferentes, incluindo um roteador que

[87] Sistema telefônico convencional

possua o *software* adequado para tanto. A *Cisco* oferece, em algumas de suas versões de IOS®, a disponibilidade da funcionalidade de *gatekeeper*, de forma a permitir se montar uma solução *VoIP* completa com a utilização apenas de seus equipamentos. Segue abaixo um exemplo de configuração de Voz sobre IP utilizando um roteador 3640 como *gatekeeper* da rede.

A funcionalidade de *gatekeeper* é habilitada através do comando "***gatekeeper***". Define-se um nome para a zona local da topologia e um domínio no qual os outros roteadores (i.e. os *gateways*) irão se registrar:

```
gatekeeper
 zone local gatekeeper-abc empresa 10.7.0.110
 no shutdown
```

Com esta configuração, o *gatekeeper* está já pronto para receber os registros dos *gateways* da rede. Foi definida uma zona local chamada *gatekeeper-abc* e um domínio chamado *empresa.*

Caso se tenha mais de um *gatekeeper* na rede, pode-se fazer com que eles formem um *cluster*[88], de forma a um assumir as funções do outro em caso de falha em um deles. Assim são definidas duas zonas para os gatekeepers, uma local e outra remota. Neste caso, as configurações em um dos *gatekeepers* ficariam assim:

```
gatekeeper
 zone local gatekeeper-abc empresa 10.7.101.100
 zone remote gatekeeper-xyz empresa 10.7.0.100
 no shutdown
!
zone cluster local gatekeeper gatekeeper-abc
element gatekeeper-xyz 10.7.0.100 1719
```

Nos demais roteadores (os *gateways*) a configuração a ser feita é da seguinte forma:

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id gatekeeper-abc ipaddr 10.7.0.110
 h323-gateway voip h323-id A123@empresa
 h323-gateway voip bind srcaddr 10.1.1.1
!
dial-peer voice 1 pots
```

[88] Grupo de equipamentos em que um ou mais deles pode assumir as funções de outros que deixem de funcionar.

```
 destination-pattern 11111
 port 1/0
!
dial-peer voice 1001 voip
 destination-pattern .T
 session target ras
 ip precedence 5
!
gateway
```

Deve-se escolher uma interface do roteador para atuar como interface do *gatekeeper*. Esta interface não precisa ser a interface pela qual irão ser encaminhados os pacotes de voz, podendo ser inclusive uma interface virtual (i.e. *Loopback*[89]), como no nosso exemplo. É preciso, no entanto, que o roteamento da rede esteja configurado de forma que todos os outros *gateways* da rede saibam como chegar até esta interface. Sob ela são, então, configuradas as informações a respeito do *gatekeeper* com o qual o *gateway* irá se registrar. O Comando ***"h323-gateway voip bind srcaddr"*** faz com que todas as ligações *VoIP* deste roteador utilizem este endereço como seus endereços de origem.

O *dial-peer 1001 voip*, acima, informa ao roteador que qualquer ligação deve ser estabelecida através do *gatekeeper*.

O comando ***"gateway"*** habilita o roteador a se registrar no *gatekeeper* da rede. Neste caso, os endereços 11111, configurado no *dial-peer pots*, e o nome *A123@empresa* serão registrados no *gatekeeper* e estarão disponíveis para os demais *gateways* da rede para estabelecimento de chamadas.

Um detalhe a ser observado é que roteadores com interfaces do tipo FXS registram automaticamente seus números no *gatekeeper*. Já equipamentos com interfaces digitais, como *voice-ports* com interfaces E1, precisam ter seus endereços manualmente configurados no *gatekeeper* para que eles estejam disponíveis para os outros *gateways*. Neste caso, este mapeamento pode ser efetuado através do comando ***"gw-type-prefix"***, como mostrado abaixo:

```
gatekeeper
 zone local gatekeeper-abc empresa 10.7.101.100
 zone remote gatekeeper-xyz empresa 10.7.0.100 1719
 gw-type-prefix 7* gw ipaddr 10.7.200.200 1720
 gw-type-prefix 20* gw ipaddr 10.7.105.100 1720
```

[89] Interface virtual do roteador.

```
gw-type-prefix 2055* gw ipaddr 10.7.115.200 1720
```

Neste exemplo, todas as ligações para números que iniciem com o digito 7 serão encaminhadas para o *gateway* com endereço IP 10.7.200.200. Já as chamadas iniciando com os dígitos 20 serão encaminhadas para o *gateway* 10.7.105.100, exceto as ligações para o número 2055, que, por possuírem uma entrada específica na tabela, serão encaminhadas para o endereço 10.7.115.200.

7.2 Verificação das configurações

Alguns comandos podem ser utilizados nas verificações do funcionamento das configurações de voz e do *gatekeeper*. Nos *gateways*, pode-se utilizar os comandos "***show voice-port***" e "***show dial-peer voice***" para se verificar o status dos *voice-ports* e *dial-peers*. Ambos os comandos aceitam o argumento *summary* no final, que ajuda a obter-se uma visão mais geral dos *voice-ports* e *dial-peers*.

```
Router-1750#show voice port summary
                                    IN      OUT
PORT   CH SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
====== == ========== ===== ==== ======== ======== ==
1/0    -- fxs-ls     up    dorm on-hook  idle     y
1/1    -- fxs-ls     up    dorm on-hook  idle     y

Super-515-1#sh dial-peer voice summary
dial-peer hunt 0
          AD                                PRE PASS
TAG  TYPE MIN OPER PREFIX DEST-PATTERN   FER THRU  SESS-TARGET  PORT
1    pots up   up            11111              0               1/0
1001 voip up   up            .T                 0  syst ras
```

Também o comando "***sh gateway***" é bastante útil pra se verificar se o *gateway* foi corretamente registrado no *gatekeeper*:

```
Super-515-1#sh gateway
Gateway  A123@empresa is registered to Gatekeeper gatekeeper-abc

Alias list (CLI configured)
 E164-ID 11111
 H323-ID A123@empresa
Alias list (last RCF)
 E164-ID 11111
 H323-ID A123@empresa

 H323 resource thresholding is Disabled
```

No caso do *gatekeeper*, alguns comandos podem ser bastante úteis na verificação de funcionamento e na pesquisa de problemas. O comando ***"show gatekeeper endpoints"***, por exemplo, mostra todos os *gateways* registrados no *gatekeeper*, juntamente com seus números associados (para *gateways* com interfaces FXS):

```
GateKeeper#show gatekeeper endpoints
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr  Port   Zone Name          Type
--------------- ----- -------------- -----  ---------          ----
10.1.1.1        1720  10.1.1.1        51290 gatekeeper-abc    VOIP-GW
    H323-ID: A123@empresa
    E164-ID: 11111
10.2.2.2        1720  10.2.2.2        51967 gatekeeper-abc    VOIP-GW
    H323-ID: B123@empresa
    E164-ID: 22222
10.3.3.3        1720  10.3.3.3        55613 gatekeeper-abc    VOIP-GW
    H323-ID: C123@empresa
    E164-ID: 33333
```

O comando "***show gatekeeper calls***" mostra todas as chamadas estabelecidas pelo *gatekeeper*:

```
GateKeeper#show gatekeeper calls
Total number of active calls = 2.
                          GATEKEEPER CALL INFO
                          ====================
LocalCallID             Age(secs)     BW
811-1206                77            12(Kbps)
Endpt(s): Alias         E.164Addr     CallSignalAddr  Port
src EP: A123@empresa    11111         10.1.1.1        1720
dst EP: B123@empresa    22222         10.2.2.2        1720


LocalCallID             Age(secs)     BW
811-1263                346           12(Kbps)
Endpt(s): Alias         E.164Addr     CallSignalAddr  Port
src EP: C123@empresa    33333         10.3.3.3        1720
dst EP: A123@empresa    11111         10.1.1.1        1720
```

E o comando "***show gatekeeper status***" mostra o status do *gatekeeper*:

```
  GateKeeper#show gatekeeper status
    Gatekeeper State: UP
    Zone Name:        gatekeeper-rce
    Accounting:       DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:
```

Para maiores informações sobre comandos para verificação de voz e *gatekeeper*, consulte *Cisco IOS Software Releases 12.2 Mainline CS3: Part 4: Voice, Video, and Fax* (Cisco, 2003k).

7.3 Os Resultados obtidos

Para avaliação das configurações de *VoIP* que foram aplicadas na rede estudada, foram verificados os resultados dos comandos apresentados no tópico anterior e no capítulo 6 e ainda colhidas impressões de usuários da rede quanto à qualidade percebida pelos mesmos nas ligações de voz.

Os indicativos colhidos mostraram que não ocorreram perdas de pacotes ou descartes relativos a *QoS*, indicando acerto nas estimativas de tráfego gerado pelo transporte de voz.

Também os usuários em geral, salvo em casos de problemas específicos que foram tratados e resolvidos[90] pela equipe de suporte, fizeram avaliações positivas quanto aos resultados obtidos, informando não ocorrerem cortes no sinal de áudio nem degradação da qualidade de voz transmitida.

7.4 Resumo do capítulo

Neste capítulo são apresentados os detalhes de implementação de *VoIP* em uma rede com roteadores *Cisco*. São apresentadas as opções de configurações através da utilização de um *gatekeeper* e sem a utilização deste elemento opcional. São discutidos também os resultados obtidos e as formas que podem ser usadas para avaliá-los.

No capítulo seguinte serão abordados os principais problemas que foram enfrentados durante a implementação do projeto. Serão apresentados principalmente os problemas que demandaram mais tempo no diagnóstico e solução, e que os causaram maiores impactos à operação da rede. Pretende-se, desta forma, contribuir com a identificação e solução de problemas semelhantes, e ao mesmo tempo chamar a atenção para aspectos a serem observados de modo a evitá-los.

[90] Vide capítulo 8

8 Problemas e soluções na implementação do projeto

Durante a implementação do projeto abordado por este trabalho, foram enfrentados problemas de diversas naturezas, que exigiram um grande esforço e tempo na sua identificação e solução. Neste capítulo são descritas as soluções que foram encontradas para os problemas mais significativos que se apresentaram. Alguns destes problemas foram solucionados simplesmente com a análise e a aplicação de técnicas de determinação de problemas. Outros precisaram do suporte dos Analistas do TAC (i.e. *Cisco Tecnical Assistence Center*), o centro de suporte da *Cisco*.

Os problemas apresentados foram divididos em problemas de *software*, problemas de *hardware* e outros tipos de problemas. A seguir serão analisados cada um deles.

8.1 Problemas de *Software*

Alguns dos problemas aqui descritos referem-se a falhas no *software* IOS® da *Cisco*. Antes de abordar estas falhas, vejamos alguns detalhes referentes às versões de *software* da *Cisco*.

8.1.1 Nomenclatura de versões de *software Cisco*

A *Cisco* adota uma nomenclatura para identificar o estágio de maturação e testes de suas versões de IOS®. As versões são divididas em "*Major Release Updates"*, "*Early Deployment Updates"* e "*Deferred Releases"*. As "*Major Release Updates*" são as versões nas quais são efetuadas apenas correções de falhas em relação às chamadas versões "*mainline"*, ou seja, as versões principais. Já as versões "*Early Deployment Updates*" trazem suporte a novas características, interfaces ou plataformas introduzidas após a liberação da última versão *"mainline"*. Por exemplo, a versão 12.2(13), que é uma versão *"major*" contém apenas correções de *bugs* em relação à versão "*mainline*" 12.2. Já a versão 12.2(13)T, que é uma versão "*early*", possui suporte a novas características que só estarão disponíveis na versão *"mainline"* 12.3. Por este motivo, as versões *"major*" costumam ser mais estáveis que as versões *"early"* já que nestas últimas a quantidade de mudanças introduzidas é bem maior.

As versões *"Major Release Updates"*, por sua vez, são ainda divididas em *"General Deployment"* (i.e. GD) e *"Limited Deployment"* (i.e. LD), a depender do quanto estas versões tenham sido testadas o suficiente para serem consideradas estáveis.

Existem, ainda, as versões chamadas de *"Deferred"*, versões que são retiradas de disponibilidade por apresentarem problemas graves. A lista a seguir exibe, em resumo, o significado destas nomenclaturas *How to Choose a Cisco IOS Software Release* (Cisco, 2003l):

1. ***Major Releases*****:** versões nas quais são efetuadas apenas correções de falhas em relação à versão principal. São divididas em:

1.1. ***General Deployment*** **(i.e. GD):** Uma versão de IOS® recebe esta denominação quando a *Cisco* considera que a mesma encontra-se testada o suficiente para poder ser aplicada em qualquer parte de uma rede de um cliente em que os recursos e funcionalidades da versão se façam necessários. Os critérios para uma versão alcançar este status incluem a reposta de clientes que utilizaram a versão em redes de teste e de produção e relatos de pessoal de suporte quanto à existência de falhas;

1.2. ***Limited Deployment*** **(i.e. LD):** Uma versão recebe esta denominação entre o período de seu lançamento e a obtenção do status de GD. Este status significa que a versão não contém nenhum grande falha ou problema conhecido, mas que mesma deve ser aplicada com cautela em redes de produção por não ter sido ainda exaustivamente testada;

2. ***Early Deployment*** **(i.e. ED):** São versões que trazem, além de correção de falhas, suporte a novas plataformas, equipamentos e características a serem incorporados à próxima versão *"mainline";*

3. ***Deferred*** **(i.e. DF):** Uma versão de *software* recebe esta designação quando a mesma é retirada de disponibilidade por parte da *Cisco*. Esta remoção pode ocorrer por um ou mais dos seguintes motivos:

- falhas graves detectadas depois da versão do *software* ter sido publicada;
- defeito que possa desabilitar a funcionalidade de um recurso importante;

- falhas causadas por comandos de configurações, linhas de comandos e comando de exibição (i.e. *show*);

- corrupção de dados, falhas de memória, comprometimento de tabelas de roteamento ou erros de fragmentação;

- outros defeitos considerados graves o suficiente para justificar a indisponibilidade da versão.

Recomenda-se, sempre que possível, que se utilize versões do tipo *"major"* e que estejam com status de GD, especialmente em redes de produção. Isto, no entanto, nem sempre é possível, uma vez que pode ser necessário o suporte a um determinado recurso ou novo modelo de *hardware* que só possa ser encontrado em uma versão ED ou LD. Outras vezes, a solução para um determinado problema que se tenha que resolver pode ser possível somente através de uma versão recém-lançada, em ED ou LD. Em hipótese alguma, no entanto, deve-se utilizar versões que estejam com status de *"deferred",* pois as mesmas podem possuir alguma falha grave de segurança ou funcionalidade que podem por em risco a operação da rede.

8.1.2 Problemas relacionados ao *software* (i.e. IOS®) *Cisco*

Durante a implementação do projeto, alguns problemas relacionados a falhas ou limitações das versões de *software* utilizadas foram encontrados. Normalmente a solução para problemas desta natureza se dá com a atualização da versão do IOS®. Alguns dos problemas enfrentados, no entanto, não tinham ainda solução em nenhuma versão disponível de *software* e tiveram que ser contornados de alguma outra forma. Todos as falhas relatados aqui foram corrigidos em versões posteriores do IOS®, assim a descrição dos mesmos e suas soluções se dará de forma bastante sucinta:

1. Voz "picotando": o projeto iniciou-se com a versão de IOS® 12.1(5)T, tendo a mesma sido escolhida na fase do projeto por suportar todos os recursos que eram requeridos pelo cliente. Esta versão, no entanto, apresentava problemas na qualidade de voz. A voz às vezes se apresentava com cortes (i.e. picotes), especialmente em localidades onde havia mais de um caminho para o roteador de destino (i.e. rotas paralelas). Este problema foi eliminado com a simples troca do *software* para a versão 12.2(3);

2. Falha no encaminhamento de pacotes: pacotes deixavam de ser encaminhados entre interfaces virtuais (como interfaces *multilink PPP*) quando era habilitado o método de encaminhamento CEF (i.e. *Cisco Express Forwarding*). O método CEF se fazia necessário para configuração dos recursos de *QoS*, como a aplicação de *policy-maps* nas interfaces. No entanto, ao habilitá-lo, pacotes deixavam de ser encaminhados entre algumas interfaces do roteador que utlizavam interfaces virtuais. As configurações de voz exigiam a configuração de *multilink PPP* por causa do *interleaving* e, na época, não havia correção para este *bug* em nenhuma versão disponível de *software*. A solução foi utilizar, como protocolo de nível 2, o *Frame Relay* entre as lojas e o concentrador, ao invés do protocolo PPP que havia sido estabelecido no projeto. Para tanto foi habilitado o recurso de *Frame Relay Switching* permitindo que o roteador central atuasse como *switch* de *Frame Relay* nos links E1 utilizados. Este problema está documentado pelo *Bug ID* CSCdu57004 e foi corrigido na versão 12.2(6);

3. *Crashes* e *reloads* nas VIPs: outro problema que afetou o início da operação da rede foram *crashes*[91] e *reloads*[92] que algumas vezes afetaram as placas VIP. Conforme exposto no capítulo 6, as placas VIP possuem processadores próprios que se encarregam de parte das tarefas que seriam executadas pelo processador central. Em algumas situações especiais, falhas no IOS® forçaram *crashes* e *reloads* nas placas VIP, interrompendo todo o tráfego que circulava pelas interfaces instaladas nelas. Dois *bugs* foram identificados como causadores desses problemas: a falha CSCdt88568 está relacionada à aplicação de uma *service-policy* a uma interface que esteja com tráfego de dados. Neste caso, na época, a única solução para se evitar o problema era suspender todo o tráfego na interface no momento da aplicação da *policy-map.* Já a falha CSCdw07967 fazia com que um *router* ou placa VIP que tivesse interfaces configuradas com CBWFQ e WRED configurados em um circuito *Frame Relay* com compressão cabeçalhos de RTP habilitada pudesse vir a sofrer um *reload* em certas circunstâncias. Também não havia solução para este problema na época, tendo sido recomendada a não utilização do recurso WRED para evitar que o problema ocorresse. Estas falhas foram corrigidas em versões posteriores do IOS®. Outra falha de IOS® relacionado ao protocolo RTP era o CSCdy48848, que fazia com que uma placa VIP pudesse sofrer um *reload* quando a compressão de RTP era removida em uma interface *Frame Relay*. Este *bug*

[91] Erro de programa que força sua interrupção

também já foi corrigido nas versões atuais e a solução para evitá-lo nas versões anteriores é também suspender o tráfego na interface ao se efetuar esta alteração.

Alguns outros problemas relacionados a falhas de IOS® foram encontrados durante a implementação do projeto, mas foram problemas de menor impacto para a rede e o cliente e não serão comentados aqui.

8.2 Problemas de *hardware*

Alguns dos problemas enfrentados estavam relacionados ao *hardware* utilizado ou ao dimensionamento do mesmo. Alguns deles foram:

1. Memória insuficiente nas placas VIP: as configurações de *QoS* e Voz sobre IP acabaram consumindo mais memória nas placas VIP do que se tinha previsto no projeto. Na verdade, este tipo de dimensionamento é bem difícil de se fazer devido a detalhes que só surgem durante a implementação. A falta de memória causou *crashes* de VIP que só foram solucionados com a ampliação da memória nas placas. Como estávamos no limite de expansão de memória (128 MB) para o modelo de placa VIP utilizado (VIP2-40), tivemos que também substituir estas placas por outras do tipo VIP4-80, que nos permitiram instalar os 256 MB necessários para suportar toda a configuração e o processamento do cliente;

2. Memória insuficiente nos roteadores 1750: outro problema relacionado a *hardware* foi a insuficiência de memória que foi apresentada pelos roteadores 1750 de algumas lojas. Neste caso, ao invés de substituir ou expandir a memória, utilizou-se o recurso de se alterar o particionamento da mesma. Os roteadores *Cisco* reservam, por padrão, 25% de sua memória para os *buffers* de interfaces. Este valor é reservado levando-se em conta as velocidades máximas que podem ser suportadas pelo equipamento. Em nosso projeto, no entanto, os enlaces para as lojas tinham velocidades que podiam ser classificadas como baixas (de 128 kbps, no máximo). Com isso, a maior parte da memória de I/O[93] (i.e. *Input/Output*) ficava ociosa. Para que mais memória pudesse ser liberada para o processamento das configurações do roteador, foi utilizado o comando "***memory-size iomem***", cujo parâmetro indica quantos por cento da memória

[92] Reinicialização do sistema
[93] Entrada e saída.

deve ser reservada para os *buffers*. A alteração deste valor para 15% foi suficiente para a liberação de memória que se fazia necessária para as configurações desejadas;

3. Falta de suporte a recursos de *QoS*: um outro problema não exatamente relacionado a *hardware* mas sim a um modelo específico de equipamento, foi a falta de suporte a alguns comandos relativos a *QoS* no modelo MC3810. Este modelo de roteador, que está sendo descontinuado pela *Cisco*, foi empregado em alguns das localidades da rede devido à necessidade de utilização de interfaces analógicas de voz do tipo E&M. Neste modelo, no entanto, não foi possível utilizar-se os comandos ***"service-policy input"*** e ***"set ip dscp"***, ambos necessários na marcação dos pacotes nos roteadores de borda, conforme foi visto no capítulo 5. Para se contornar este problema, foi feita apenas a classificação e priorização dos pacotes, utilizando-se as *access-lists* e o comando ***"service-policy output"***, ficando a marcação a cargo do roteador central, no caso destas localidades.

8.3 Outros problemas

Alguns outros problemas enfrentados foram resolvidos com comandos específicos ou alterações nas configurações. Entre eles pode-se destacar:

1. *One-way-audio*: Em lojas em que tinhamos mais de um caminho possível para o tráfego de voz (i.e. caminhos paralelos) em alguns casos ocorriam o chamado "*one-way-audio*" ou seja, áudio somente em um sentido. Este problema é descrito no documento *Voice Quality Troubleshooting One Way Voice Issues* (Cisco, 2003m). Entre as soluções apontadas neste documento, encontram-se o comando "***h323-gateway voip bind srcaddr*"**, já descrito nas configurações de *gatekeeper* no capítulo 5, e o comando "***voice rtp send-recv***". Este último abre os canais para a transmissão de pacotes de RTP imediatamente ao se iniciar uma chamada. Sem este comando, o roteador só abre o canal de transmissão ao receber a mensagem de conexão do lado remoto. Em casos em que esta mensagem não chega com a temporização devida, pode ocorrer o problema de apenas um dos lados da ligação ouvir o outro;

2. Demora nos estabelecimento de chamadas em localidades com interface de voz E1: Nas localidades em que o tipo de interface de voz utilizado foi o E1 digital, ocorria uma demora excessiva (de 8 a 10 segundos) para o estabelecimento da chamada.

Após extensa pesquisa, foi-nos informado pelo TAC da *Cisco*, que esta demora era "normal" e inerente ao tipo de sinalização que se estava usando (r2-digital compelido.) Para solucionar este problema foi alterada a configuração para r2-digital dtmf;

3. Persistência em conexões X.25: no início da operação da rede também ocorreram alguns problemas relativos às configurações de XOT (i.e. X.25 over TCP). Em casos em que ambos os circuitos para uma determinada loja caiam, ou que o roteador da loja era desligado de forma abrupta (por uma falta de energia, por exemplo) havia dificuldade para re-conexão das lojas aos *hosts* x.25 no CPD central. Ao receber a chamada, estes *hosts* respondiam com uma mensagem de erro informando diagnóstico 131. Este diagnóstico significava que, para o *host* central, a loja já estava conectada e que ele não poderia aceitar a chamada por não permitir duas conexões para um mesmo endereço de origem. O problema ocorria porque, por padrão, o roteador somente derruba uma conexão XOT ao receber um *disconnect* de algum dos lados da comunicação, o que não ocorria nas situações acima. Para resolver este problema, foi configurado o recurso de *XOT Keepalive*. Com este recurso, os roteadores ficam trocando mensagens de *keepalive* a cada intervalo de tempo pré-determinado. Caso uma das pontas deixe de receber estas mensagens por um número configurável de vezes, a ligação é derrubada através de um *disconnect* forçado. A sintaxe para implementação deste recurso pode ser vista na descrição do comando "***x25 route***" no documento *X.25 and LAPB Commands (x25 remote-red through x29 profile)* (Cisco, 2003n). No caso deste projeto, as opções foram configuradas para que as conexões caíssem após a ausência de três mensagens de *keepalive* que deveriam ser transmitidas a cada 10 segundos.

8.4 Resumo do capítulo

Neste capítulo são abordados os problemas que foram enfrentados na implementação de um projeto de rede utilizando recursos de *QoS* e *VoIP*. São expostas as principais falhas e dificuldades que se apresentaram em relação a *hardware, software* e outros tipos de problemas que se apresentaram no decorrer do projeto. Para cada um desses problemas é apresentada a solução encontrada, de forma a permitir ao leitor evitar que os mesmos erros sejam cometidos em projetos semelhantes, assim como servir como base na solução de problemas da mesma natureza. Além disso, são descritas as

convenções utilizadas pela *Cisco* na nomenclatura de suas versões de *software*, facilitando a identificação e a escolha da melhor versão a ser empregada.

No próximo capítulo é apresentada a conclusão deste trabalho, onde são ressaltados os principais resultados obtidos e as contribuições oferecidas pelo mesmo.

9 Considerações finais

As redes múltiplas baseadas na tecnologia de transmissão de pacotes, mais especificamente, as redes IP, tendem a continuar a se expandir e a se tornar mais complexas, com a integração de tráfegos de mídia contínua e a necessidade de se dar diferentes prioridades aos diferentes tipos de tráfegos de dados.

O projeto e implementação de redes desta natureza exige uma metodologia e conhecimentos específicos. Apesar das informações sobre estes assuntos estarem amplamente disponíveis em meios como a Internet, juntar todas as peças de forma correta pode ser uma tarefa bastante difícil e muitos problemas podem ocorrer no meio do caminho. Decisões mal pensadas na fase de projeto, problemas inesperados com falhas de *hardware* ou *software* ou erros na implementação podem comprometer a qualidade e o resultado esperado da rede como um todo.

O principal objetivo deste trabalho é contribuir com estudos e indicação de soluções que possam ser aproveitados na implementação de redes heterogêneas e de integração de serviços de considerável grau de complexidade e sofisticação. As soluções e configurações apresentadas não pretendem esgotar o assunto, até porque existem diversas formas diferentes de se alcançar um mesmo objetivo. O que se apresentou foram as soluções que foram consideradas mais adequadas diante das situações vivenciadas. Para tanto foram descritos desde os fatores que foram levados em conta nas decisões iniciais do projeto até detalhes de implementação que podem causar muita dificuldade e confusão a pessoas que enfrentem esta tarefa pela primeira vez. Além disso, foram apontadas fontes para a obtenção de informações importantes para a complementação dos conhecimentos aqui apresentados.

Através deste trabalho é também possível se ter uma idéia de adequação dos equipamentos da *Cisco* ao modelo de Qualidade de Serviço *DiffServ*, principalmente função dos resultados positivos que foram obtidos no projeto como um todo.

Com tudo isso pretende-se que este trabalho possa servir como um guia na implementação de redes complexas que incluam recursos de Voz sobre IP e Qualidade de Serviço utilizando equipamentos Cisco, de forma a facilitar o trabalho de pessoas que

tenham que lidar com tais implementações, através do aproveitamento das experiências e conclusões nele relatadas.

Outra contribuição deste trabalho reside nas ferramentas que foram desenvolvidas para a codificação de *policy-maps* de *QoS* em roteadores *Cisco*. Estas ferramentas podem facilitar bastante a tarefa de configuração de roteadores em projetos onde exista um grande número de perfis diferentes tráfego já que, conforme visto no capítulo 6, esta configuração não é nada trivial estando sujeita a muitos erros e confusões.

Alguns experimentos e estudos adicionais podem ser sugeridos como complemento a este trabalho:

- proposição de uma metodologia de avaliação objetiva da melhoria do desempenho obtido com configurações de *QoS*;

- proposição de uma metodologia detalhada de processos listando as fases de projeto e implementação de redes;

- estudo da integração do modelo *DiffServ* com *MPLS* (i.e. *Multiprotocol Label Switching*) e o mapeamento entre estas duas tecnologias;

- estudo sobre o impacto de configurações de *QoS* em termos de *overhead* de processador e memória nos roteadores onde as mesmas são aplicadas;

- estudo da utilização de ferramentas de configuração e gerenciamento de *QoS*, como o *QDM – QoS Device Manager* e o *QPM – QoS Policy Manager*, ambos da *Cisco*;

- estudo da utilização do recurso *Netflow*, da *Cisco*, como ferramenta de medição de *QoS.*

10 Referências bibliográficas

CISCO SYSTEMS INC., **End-to-end Quality of Service**, EUA, 1999. Disponível em: <http://www.cisco.com/warp/customer/784/packet/apr99/3.html>. Acesso em 17 Nov. 2002.

CISCO SYSTEMS INC., **Cisco Voice over *Frame Relay*, ATM and IP Student Guide – Volume 2**, EUA, 2000.

CISCO SYSTEMS INC., **Quality of Service Networking**, EUA, 2002a. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm>. Acesso em 17 nov. 2002.

CISCO SYSTEMS INC., **Cisco IOS *QoS* Technical Documents**, EUA, 2002b. Disponível em: <http://www.cisco.com/warp/public/732/Tech/qos/qos_techdoc.shtml>. Acesso em 17 nov. 2002.

CISCO SYSTEMS INC., **Cisco IOS Software: Quality of Service**, EUA, 2002c. Disponível em: <http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosq_ds.htm>. Acesso em 20 nov. 2002.

CISCO SYSTEMS INC., **Voice Over IP Overview**, EUA, 2002d. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfvoip.htm>. Acesso em 20 nov. 2002.

CISCO SYSTEMS INC., **Configuring Priority Queuing**, EUA, 2002e. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qcpq.htm> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **Configuring Custom Queuing**, EUA, 2002f. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qccq.htm> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **Configuring Weighted Fair Queuing**, EUA, 2002g. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qcwfq.htm> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **Class-Based Weighted Fair Queuing**, EUA, 2002h. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart2/qcwfq.htm> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **IP RTP Priority**, EUA, 2002i. Disponível em: <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iprtp.htm> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **Low Latency Queuing**, EUA, 2002j. Disponível em: <http://www.cisco.com/warp/public/121/latencyqueueing.html> Acesso em 07 dez. 2002.

CISCO SYSTEMS INC., **Cisco Systems Homepage**, EUA, 2003a. Disponível em: <http://www.cisco.com>. Último acesso em 15 ago. 2003.

CISCO SYSTEMS INC., **Quality of Service for Voice over IP**, EUA, 2003b. Disponível em: <http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800d6b73.shtml>. Acesso em 10 jan. 2003.

CISCO SYSTEMS INC., **IP Telephony / *VoIP***, EUA, 2003c. Disponível em: <http://www.cisco.com/en/US/tech/tk652/tk701/tech_protocol_family_home.html>. Acesso em 30 abr. 2003.

CISCO SYSTEMS INC., ***Cisco QoS***, EUA, 2003d. Disponível em: <http://www.cisco.com/en/US/tech/tk543/tech_topology_and_network_serv_and_protocol_suite_home.html>. Acesso em 30 abr. 2003.

CISCO SYSTEMS INC., ***QoS* Frequently Asked Questions**, EUA, 2003e. Disponível em: <http://www.cisco.com/warp/customer/105/qos_faq.html>. Acesso em 30 mar. 2003.

CISCO SYSTEMS INC., **Voice Over IP - Per Call Bandwidth Consumption**, EUA, 2003f. Disponível em: <http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html>. Acesso em 10 jan. 2003.

CISCO SYSTEMS INC., **Configuring *Frame Relay* Traffic Shaping**, EUA, 2003g. Disponível em:<http://www.cisco.com/warp/public/125/traffic_shaping_6151.html>. Acesso em 07 mai. 2003.

CISCO SYSTEMS INC., **Cisco IOS Software Releases 12.2 Mainline CS3: Part 3: Quality of Service Solutions**, EUA, 2003h. Disponível em: <http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summary_book09186a008008713f.html>. Acesso em 30 abr. 2003.

CISCO SYSTEMS INC., **Voice Interface Cards**, EUA, 2003i. Disponível em: <http://www.cisco.com/en/US/products/hw/modules/ps2641/ps3111/index.html> Acesso em 20 mai. 2003.

CISCO SYSTEMS INC., **Voice Hardware Compatibility Matrix**, EUA, 2003j. Disponível em: <http://www.cisco.com/warp/public/788/products/voice_comp_matrix.html>. Acesso em 30 abr. 2003.

CISCO SYSTEMS INC., **Cisco IOS Software Releases 12.2 Mainline CS3: Part 4: Voice, Video, and Fax**, EUA, 2003k. Disponível em: <http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_summary_book09186a0080087488.html>. Acesso em 15 jun. 2003.

CISCO SYSTEMS INC., **How to Choose a Cisco IOS Software Release**, EUA, 2003l. Disponível em: <http://www.cisco.com/warp/customer/130/choosing_ios.shtml>. Acesso em 05 mai. 2003.

CISCO SYSTEMS INC., **Voice Quality Troubleshooting One Way Voice Issues**, EUA, 2003m. Disponível em: <http://www.cisco.com/en/US/partner/tech/tk652/tk698/technologies_tech_note09186a008009484b.shtml>. Acesso em 07 mai. 2003.

CISCO SYSTEMS, INC., **X.25 and LAPB Commands (x25 remote-red through x29 profile)**, EUA, 2003n. Disponível em: <http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7f7.html#33836>. Acesso em 07 mai. 2003.

FERGUSON, P; HUSTON, G. **Quality of Service: Delivering *QoS* on the Internet and in Corporate Networks**, EUA, 1998, Paperback, 288p.

IETF - THE INTERNET SOCIETY, **Request For Comments 791, Internet Protocol**, set. 1981, Disponível em: <http://www.ietf.org/rfc/rfc791.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 1122, Requirements for Internet Hosts - Communication Layers**, out. 1989, Disponível em: <http://www.ietf.org/rfc/rfc1349.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 1349, Type of Service in the Internet Protocol Suite**, jul. 1992, Disponível em: <http://www.ietf.org/rfc/rfc1349.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 1717, The PPP Multilink Protocol (MP)**, nov. 1994, Disponível em: <http://www.ietf.org/rfc/rfc1717.txt>. Acesso em 10 mai. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2205, Resource ReSerVation Protocol (RSVP),** set. 1997, Disponível em: <http://www.ietf.org/rfc/rfc2205.txt>. Acesso em 10 jul. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2211, Specification of the Controlled-Load Network Element Service**, set. 1997, Disponível em: <http://www.ietf.org/rfc/rfc2211.txt>. Acesso em 10 jul. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers**, dez. 1998a, Disponível em: <http://www.ietf.org/rfc/rfc2474.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2475, An Architecture for Differentiated Services**, dez. 1998b, Disponível em:<http://www.ietf.org/rfc/rfc2475.txt>. Acesso em 22 mar. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links**, fev. 1999a, Disponível em: <http://www.ietf.org/rfc/rfc2508.txt>. Acesso em 22 mar. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2597, Assured Forwarding PHB Group**, jun. 1999b, Disponível em: <http://www.ietf.org/rfc/rfc2597.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2598, An Expedited Forwarding PHB**, jun. 1999c, Disponível em: <http://www.ietf.org/rfc/rfc2598.txt>. Acesso em 30 abr. 2003.

IETF - THE INTERNET SOCIETY, **Request For Comments 2543, SIP: Session Initiation Protocol**, mar. 1999d, Disponível em: <http://www.ietf.org/rfc/rfc2543.txt>. Acesso em 22 mar. 2003.

ITU-T - INTERNATIONAL TELECOMMUNICATION UNION, **ITU-T Website**, ago. 2003, Disponível em: <http://www.itu.int/home/index.html>. Acesso em 08 ago. 2003.

MARTINS, JOBERTO SÉRGIO BARBOSA, Qualidade de Serviço (*QoS*) em Redes IP Princípios Básicos, Parâmetros e Mecanismos, **Network Designers**, set. 1999. Disponível em: <http://networkdesigners.com.br/Artigos/qos/qos.html>. Acesso em 15 fev. 2003.

OYAMA, CYBELLE SUEMI ODA; LUCENA, SIDNEY CUNHA DE, Considerações acerca do estabelecimento de *QoS* no RNP2, **RNP NewsGeneration,** v. 6, n. 3, Rio de Janeiro, mai. 2002. Disponível em: <http://www.rnp.br/newsgen/0205/qos_rnp.shtml>. Acesso em 15 fev. 2003.

RNP, **RNP NewsGeneration**. Revista Eletrônica, Rio de Janeiro, 2003. Disponível em: <http://www.rnp.br/newsgen/>. Acesso em 15 fev. 2003.

SANTOS, ANA PAULO SILVA DOS, Qualidade de Serviço na Internet, **RNP NewsGeneration,** v. 3, n. 6, Rio de Janeiro, nov. 1999. Disponível em: <http://www.rnp.br/newsgen/9911/qos.shtml>. Acesso em 15 fev. 2003.

SILVA, ADAILTON J. S., Qualidade de Serviço em *VoIP* – Parte 1, **RNP NewsGeneration,** v. 4, n. 3, Rio de Janeiro, mai. 2000a. Disponível em: <http://www.rnp.br/newsgen/0005/qos_voip1.shtml>. Acesso em 15 fev. 2003.

SILVA, ADAILTON J. S., Qualidade de Serviço em *VoIP* – Parte 2, **RNP NewsGeneration,** v. 4, n. 6, Rio de Janeiro, set. 2000b. Disponível em: <http://www.rnp.br/newsgen/0009/qos_voip2.shtml>. Acesso em 15 fev. 2003.

VEGESNA, SRINIVAS. **IP Quality of Service**. Indianapolis, EUA, 2000, Cisco Press, 343p.

ANEXOS

ANEXO 01 – Equipamentos utilizados na implementação do projeto.

Tabela A1 – Relação de Equipamentos

Tipo de Loja:	Concentrador – Cidade 1	
Equipamento	CISCO 7507/4X2	
Quantidade	**Part Number**	**Descrição**
1	CISCO7507/4X2	Cisco 7507 7-Slot, 2 CyBus, 2 RSP4, Dual Power Supply
2	RSP4+	Cisco 7500 Series Route Switch Processor 4+
2	MEM-RSP4-FLC20M	RSP4 Flash Card: 20 MB Option
2	MEM-RSP4-128M	RSP4/RSP4+ 128MB DRAM Option
3	VIP2-40	Versatile Interface Processor-2, model 40
3	MEM-VIP240-32M	32 MB DRAM Option for VIP2-40 (Default)
4	PA-4E1G/75	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PA-4E1G/75=	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PWR-7507/4X2-DC	Cisco 7507/4x2 Dual DC Power Supply Option
2	CAB-7KAC=	Cisco 7500 Series AC Power Cord, US
1	FR-WPP75	Cisco IOS RSPx Series WAN Packet Protocols/Netflow License
1	S75BS-12105T	Cisco RSPx Series IOS DESKTOP/IBM
1	PA-8T-V35	8-Port Serial, V.35 Port Adapter
1	PA-8T-V35=	8-Port Serial, V.35 Port Adapter
1	PA-FE-TX	1-Port Fast Ethernet 100BaseTx Port Adapter
16	CAB-E1-BNC	E1 Cable BNC 75ohm/Unbal 5m
1	CAB-OCT-V35-MT=	8 Lead Octal Cable and 8 Male V35 DTE Connectors

Tipo de Loja:	Concentrador – Cidade 2	
Equipamento	CISCO 7507/4X2	
Quantidade	**Part Number**	**Descrição**
1	CISCO7507/4X2	Cisco 7507 7-Slot, 2 CyBus, 2 RSP4, Dual Power Supply
2	RSP4+	Cisco 7500 Series Route Switch Processor 4+
2	MEM-RSP4-FLC20M	RSP4 Flash Card: 20 MB Option
2	MEM-RSP4-128M	RSP4/RSP4+ 128MB DRAM Option
2	VIP2-40	Versatile Interface Processor-2, model 40
2	MEM-VIP240-32M	32 MB DRAM Option for VIP2-40 (Default)
2	PA-4E1G/75	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PA-4E1G/75=	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PWR-7507/4X2-DC	Cisco 7507/4x2 Dual DC Power Supply Option
2	CAB-7KAC=	Cisco 7500 Series AC Power Cord, US
1	FR-WPP75	Cisco IOS RSPx Series WAN Packet Protocols/Netflow License
1	S75BS-12105T	Cisco RSPx Series IOS DESKTOP/IBM
1	PA-4T+	4 Port Serial Port Adapter, Enhanced
1	PA-4T+=	4-Port Serial Port Adapter, Enhanced
4	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
8	CAB-E1-BNC	E1 Cable BNC 75ohm/Unbal 5m

Tabela A1(continuação)

Tipo de Loja:	Transportadora	
Equipamento	CISCO 2610	
Quantidade	**Part Number**	**Descrição**
1	CAB-ADPT-75-120	Adapter cable-converts 75 ohm to 120 ohm
1	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
2	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
1	NM-HDV-1E1-30	Single-Port 30 Channel E1 Voice/Fax Network Module
1	WIC-1T	1-Port Serial WAN Interface Card
1	WIC-2T	2-Port Serial WAN Interface Card
1	CISCO2610	Ethernet Modular Router w/ Cisco IOS IP Software
1	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
1	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
1	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
1	CAB-AC	Power Cord,110V

Tipo de Loja:	CPD – Cidade 2	
Equipamento	CISCO 2610	
Quantidade	**Part Number**	**Descrição**
1	CAB-ADPT-75-120	Adapter cable-converts 75 ohm to 120 ohm
1	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
2	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
1	NM-HDV-1E1-30	Single-Port 30 Channel E1 Voice/Fax Network Module
1	WIC-1T	1-Port Serial WAN Interface Card
1	WIC-2T	2-Port Serial WAN Interface Card
1	CISCO2610	Ethernet Modular Router w/ Cisco IOS IP Software
1	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
1	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
1	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
1	CAB-AC	Power Cord,110V

Tipo de Loja:	CPD – Cidade 3	
Equipamento	CISCO 2610	
Quantidade	**Part Number**	**Descrição**
1	CAB-ADPT-75-120	Adapter cable-converts 75 ohm to 120 ohm
1	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
2	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
1	NM-HDV-1E1-12	Single-Port 12 Channel E1 Voice/Fax Network Module
1	WIC-1T	1-Port Serial WAN Interface Card
1	WIC-2T	2-Port Serial WAN Interface Card
1	CISCO2610	Ethernet Modular Router w/ Cisco IOS IP Software
1	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
1	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
1	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
1	CAB-AC	Power Cord,110V

Tabela A1(continuação)

Tipo de Loja:	Depósito
Equipamento:	CISCO 1750-2V
Quantidade:	2

Quantidade	Part Number	Descrição
4	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	VIC-2FXS	Two-port Voice Interface Card - FXS
2	WIC-2T	2-Port Serial WAN Interface Card
2	CISCO1750-2V	10/100 Modular Router w/2 Voice channels, IOS IP/VOICE + SW
2	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
2	CAB-AC	Power Cord,110V

Tipo de Loja:	Diretoria
Equipamento:	CISCO MC3810-V3-AC
Quantidade:	1

Quantidade	Part Number	Descrição
2	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
1	MC3810-V3-AC	MC3810-V3 Chassis w/ 100-220 VAC Power Supply
1	MC3810-AVM6	6 port Analog Voice Interface
6	MC3810-APM-FXS	FXS Analog Personality Module
1	MC3810-HCM2	2 DSP High Density Voice Compression Module
1	S38CP-12103T	Cisco 3800 Series IOS IP PLUS
1	CAB-AC	Power Cord,110V

Tipo de Loja:	Gateway X.25
Equipamento:	CISCO 2610
Quantidade:	2

Quantidade	Part Number	Descrição
8	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
4	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
2	NM-4A/S	4-Port Async/Sync Serial Network Module
2	WIC-2A/S	2-Port Async/Sync Serial WAN Interface Card
2	CISCO2610	Ethernet Modular Router w/ Cisco IOS IP Software
2	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
2	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
2	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
2	CAB-AC	Power Cord,110V

Tipo de Loja:	Loja Grande - Tipo 1
Equipamento:	CISCO 1750-4V
Quantidade:	16

Quantidade	Part Number	Descrição
32	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
32	VIC-2FXS	Two-port Voice Interface Card - FXS
16	WIC-2T	2-Port Serial WAN Interface Card
16	CISCO1750-4V	10/100 Modular Router w/4 Voice channels, IOS IP/VOICE + SW
16	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
16	CAB-AC	Power Cord,110V

Tabela A1(continuação)

Tipo de Loja:	Loja Grande – Tipo 2
Equipamento:	CISCO 1720
Quantidade:	16

Quantidade	Part Number	Descrição
16	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
16	CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet
16	WIC-1T	1-Port Serial WAN Interface Card
16	WIC-2T	2-Port Serial WAN Interface Card
16	CAB-232FC	RS-232 Cable, DCE, Female, 10 Feet
16	CISCO1720	10/100BaseT Modular Router w/2 WAN slots, 8M Flash/32M DRAM
16	S17CP-12103T	Cisco 1700 IOS IP PLUS
16	CAB-AC	Power Cord,110V

Tipo de Loja:	Loja Grande – Tipo 1
Equipamento:	CISCO 1750-4V
Quantidade:	5

Quantidade	Part Number	Descrição
5	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
5	CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet
10	VIC-2FXS	Two-port Voice Interface Card - FXS
5	WIC-2T	2-Port Serial WAN Interface Card
5	CISCO1750-4V	10/100 Modular Router w/4 Voice channels, IOS IP/VOICE + SW
5	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
5	CAB-AC	Power Cord,110V

Tipo de Loja:	Loja Grande – Tipo 2
Equipamento:	CISCO 1750-2V
Quantidade:	5

Quantidade	Part Number	Descrição
5	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
5	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
5	CAB-SS-232FC	RS-232 Cable, DCE Female to Smart Serial, 10 Feet
5	VIC-2FXS	Two-port Voice Interface Card - FXS
5	WIC-1T	1-Port Serial WAN Interface Card
5	WIC-2T	2-Port Serial WAN Interface Card
5	CISCO1750-2V	10/100 Modular Router w/2 Voice channels, IOS IP/VOICE + SW
5	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
5	CAB-AC	Power Cord,110V

Tipo de Loja:	Loja Média – Tipo 1
Equipamento:	CISCO 1750-4V
Quantidade:	3

Quantidade	Part Number	Descrição
6	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
6	VIC-2FXS	Two-port Voice Interface Card - FXS
3	WIC-2T	2-Port Serial WAN Interface Card
3	CISCO1750-4V	10/100 Modular Router w/4 Voice channels, IOS IP/VOICE + SW
3	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
3	CAB-AC	Power Cord,110V

Tabela A1(continuação)

Tipo de Loja:	Loja Média - Tipo 2
Equipamento:	CISCO 1720
Quantidade:	3

Quantidade	Part Number	Descrição
3	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
3	CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet
3	WIC-1T	1-Port Serial WAN Interface Card
3	WIC-2T	2-Port Serial WAN Interface Card
3	CAB-232FC	RS-232 Cable, DCE, Female, 10 Feet
3	CISCO1720	10/100BaseT Modular Router w/2 WAN slots, 8M Flash/32M DRAM
3	S17CP-12103T	Cisco 1700 IOS IP PLUS
3	CAB-AC	Power Cord,110V

Tipo de Loja:	Loja Pequena
Equipamento:	10 x CISCO 1720 + Módulos
Quantidade:	19

Quantidade	Part Number	Descrição
19	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
19	CAB-SS-232FC	RS-232 Cable, DCE Female to Smart Serial, 10 Feet
10	WIC-1B-S/T	1-Port ISDN WAN Interface Card(dial and leased line)
19	WIC-2A/S	2-Port Async/Sync Serial WAN Interface Card
19	CAB-S/T-RJ45	Orange Color Cable for ISDN BRI S/T, RJ-45, 6 feet
10	CISCO1720	10/100BaseT Modular Router w/2 WAN slots, 8M Flash/32M DRAM
19	S17CP-12103T	Cisco 1700 IOS IP PLUS
10	CAB-AC	Power Cord,110V

Tipo de Loja:	Centro de Distrinuição
Equipamento:	CISCO 2610
Quantidade:	1

Quantidade	Part Number	Descrição
1	CAB-ADPT-75-120	Adapter cable-converts 75 ohm to 120 ohm
1	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
2	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
1	NM-HDV-1E1-12	Single-Port 12 Channel E1 Voice/Fax Network Module
1	WIC-1T	1-Port Serial WAN Interface Card
1	WIC-2T	2-Port Serial WAN Interface Card
1	CISCO2610	Ethernet Modular Router w/ Cisco IOS IP Software
1	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
1	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
1	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
1	CAB-AC	Power Cord,110V

Tabela A1(continuação)

Tipo de Loja:	CPD – Cidade 1
Equipamento:	CISCO 7507/4X2
Quantidade:	1

Quantidade	Part Number	Descrição
1	CISCO7507/4X2	Cisco 7507 7-Slot, 2 CyBus, 2 RSP4, Dual Power Supply
2	RSP4+	Cisco 7500 Series Route Switch Processor 4+
2	MEM-RSP4-FLC20M	RSP4 Flash Card: 20 MB Option
2	MEM-RSP4-128M	RSP4/RSP4+ 128MB DRAM Option
3	VIP2-40	Versatile Interface Processor-2, model 40
3	MEM-VIP240-32M	32 MB DRAM Option for VIP2-40 (Default)
2	PA-4E1G/75	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PA-4E1G/75=	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
1	PWR-7507/4X2	Cisco 7507/4x2 Dual AC Power Supply Option (Default)
2	CAB-7KAC=	Cisco 7500 Series AC Power Cord, US
1	FR-WPP75	Cisco IOS RSPx Series WAN Packet Protocols/Netflow License
1	S75BS-12105T	Cisco RSPx Series IOS DESKTOP/IBM
1	PA-4T+	4 Port Serial Port Adapter, Enhanced
1	PA-4T+=	4-Port Serial Port Adapter, Enhanced
2	PA-VXC-2TE1+	2 port TE1 hi-capacity enhanced voice PA
1	PA-VXC-2TE1+=	2 port TE1 hi-capacity enhanced voice PA
1	PA-FE-TX	1-Port Fast Ethernet 100BaseTx Port Adapter
1	PA-FE-TX=	1-Port Fast Ethernet 100BaseTx Port Adapter
4	CAB-E1-RJ45BNC	E1 Cable RJ45 to Dual BNC (Unbalanced)
1	CAB-E1-RJ45BNC=	E1 Cable RJ45 to dual BNC (unbalanced), Spare
8	CAB-E1-BNC	E1 Cable BNC 75ohm/Unbal 5m
1	CAB-E1-BNC=	FSIP and MIP-CE1: BNC 75ohm/Unbal 5 meters
4	CAB-V35FC	V.35 Cable, DCE, Female, 10 Feet

Tipo de Loja:	Loja Normal
Equipamento:	CISCO 1750-2V
Quantidade:	63

Quantidade	Part Number	Descrição
63	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
63	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
63	CAB-SS-232FC	RS-232 Cable, DCE Female to Smart Serial, 10 Feet
63	VIC-2FXS	Two-port Voice Interface Card - FXS
63	WIC-1T	1-Port Serial WAN Interface Card
63	WIC-2T	2-Port Serial WAN Interface Card
63	CISCO1750-2V	10/100 Modular Router w/2 Voice channels, IOS IP/VOICE + SW
63	S17CVP-12103T	Cisco 1700 IOS IP/VOICE PLUS
63	CAB-AC	Power Cord,110V

Tabela A1(continuação)

Tipo de Loja:	Backup Discado
Equipamento:	CISCO 2620
Quantidade:	1

Quantidade	Part Number	Descrição
1	CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet
1	CAB-SS-V35FC	V.35 Cable, DCE Female to Smart Serial, 10 Feet
1	NM-8B-S/T	8-Port ISDN-BRI Network Module
1	WIC-2T	2-Port Serial WAN Interface Card
1	CISCO2620	10/100 Ethernet Router w/2 WIC Slots & 1 Network Module Slot
8	CAB-S/T-RJ45	Orange Color Cable for ISDN BRI S/T, RJ-45, 6 feet
1	S26CP-12103T	Cisco 2600 Series IOS IP PLUS
1	MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
1	MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
1	CAB-AC	Power Cord,110V

Tipo de Loja:	Hotline
Equipamento:	CISCO 3640
Quantidade:	1

Quantidade	Part Number	Descrição
2	CAB-ADPT-75-120	Adapter cable-converts 75 ohm to 120 ohm
1	CAB-V35MT	V.35 Cable, DTE, Male, 10 Feet
2	CAB-RPSY-2218	RPS 22/18 Two-to-one DC Power Cable
1	CISCO3640-RPS	Cisco 3600 4-slot modular router, use w/ AC RPS with IP
1	NM-1E2W	1 Ethernet 2 WAN Card Slot Network Module
1	WIC-1T	1-Port Serial WAN Interface Card
1	MEM3600-8U16FS	8-to-16MB Flash Factory Upgrade for the Cisco 3600
1	MEM3640-32U64D	32-to-64 MB DRAM Factory Upgrade for the Cisco 3640
1	PWR600-AC-RPS-NCAB	600W Redundant AC Power System W/O DC Power Cables
1	ACS-3600ASYN	Auxiliary/Console Port Cable Kit for the Cisco 3600 Series
1	S364CP-12103T	Cisco 3640 Series IOS IP PLUS
1	NM-HDV-2E1-60	Dual-Port 60 Channel E1 Voice/Fax Network Module
2	CAB-RPSAC	AC Power Cord North America for RPS

ANEXO 02 – Classificação de Protocolos e Aplicações.

Tabela A2: Classificação de protocolos e aplicações

Porta	Descrição	Classe
any	Tráfego não classificado	BAIXA
ftp-data	Dados de FTP	BAIXA
ftp	Controle de Dados de FTP	BAIXA
cmd	Remote Copy	BAIXA
524	Netware File Service	BAIXA
900-1099	CIUX RSH	BAIXA
1352	Notes	REGULAR
8080	HTTP via Proxy	MÉDIA
3600-3602	SAPR3	MÉDIA
3200 3202	SAPR3	MÉDIA
9401	Distribuição de profiles	MÉDIA
2502	Remote file transfer Controll	MÉDIA
512	Remote Exec	MÉDIA
514	Remote Shell	MÉDIA
2967	Antivirus	MÉDIA
80	HTTP	MÉDIA
139	NETBIOS Session Service	MÉDIA
1433	Microsoft SQL	MÉDIA
1320	ARS	MÉDIA
37992	Universal RH	MÉDIA
37994	Universal RH	MÉDIA
2725	infosql	MÉDIA
515	spooler	MÉDIA
1521	nCube License Manager (oracle)	MÉDIA
9494-9495	Conexão Gateway-Endpoint/Conexão Endpoint-Gateway	ALTA
telnet	Telnet	ALTA
3389	RDP/WTS	ALTA
5529	Envio de eventos para a TEC	ALTA
2501	Remote control (tela teclado e mouse)	ALTA
2503	remote control chat	ALTA
5900	VNC	ALTA
31111	Workload Scheduler	ALTA
161	SNMP	ALTA
4000	URA/FEP	ALTA
94	Tivoli Object Dispatcher	ALTA
9006	URA/Autorização	ALTA

Tabela A2(continuação)

53	Domain Name Server	ALTA
3000	FEP Autorização	ALTA
137	NETBIOS Name Service	ALTA
9005	URA Autorização	ALTA
1365	Gateway DIMEP	ALTA
15665	Cartão de fidelidade	ALTA
15664	Cartão de fidelidade	ALTA
15666	Cartão de fidelidade	ALTA
19655	CTF/NX	ALTA
3500	FEP Autorização	ALTA
135	Location Service	ALTA
445	Microsoft-DS	ALTA
113	Authentication Service	ALTA
xot	XOT	ALTÍSSIMA

ANEXO 03 – Listas de acesso para marcação dos pacotes.

```
access-list 117 remark prioridade baixa (FTP, RSH, OUTROS)
access-list 117 permit tcp any any eq ftp-data
access-list 117 permit tcp any eq ftp-data any
access-list 117 permit tcp any any eq ftp
access-list 117 permit tcp any eq ftp any
access-list 117 permit tcp any any eq 524
access-list 117 permit tcp any eq 524 any
access-list 117 permit tcp any any range 900 1099
access-list 117 permit tcp any range 900 1099 any
access-list 117 permit udp any any eq 524
access-list 117 permit udp any eq 524 any
access-list 117 permit udp any any range 900 1099
access-list 117 permit udp any range 900 1099 any

access-list 118 remark prioridade media (SQL, SAP, HTTP, OUTROS)
access-list 118 permit tcp any any eq 8080
access-list 118 permit tcp any eq 8080 any
access-list 118 permit tcp any any eq www
access-list 118 permit tcp any eq www any
access-list 118 permit tcp any any range 3600 3602
access-list 118 permit tcp any range 3600 3602 any
access-list 118 permit tcp any any range 3200 3202
access-list 118 permit tcp any range 3200 3202 any
access-list 118 permit tcp any any eq 9401
access-list 118 permit tcp any eq 9401 any
access-list 118 permit tcp any any eq 2502
access-list 118 permit tcp any eq 2502 any
access-list 118 permit tcp any any eq exec
access-list 118 permit tcp any eq exec any
access-list 118 permit tcp any any eq cmd
access-list 118 permit tcp any eq cmd any
access-list 118 permit tcp any any eq 2697
access-list 118 permit tcp any eq 2697 any
access-list 118 permit tcp any any eq 139
access-list 118 permit tcp any eq 139 any
access-list 118 permit tcp any any eq 1433
access-list 118 permit tcp any eq 1433 any
access-list 118 permit tcp any any eq 1320
access-list 118 permit tcp any eq 1320 any
access-list 118 permit tcp any any eq 37992
access-list 118 permit tcp any eq 37992 any
access-list 118 permit tcp any any eq 37994
access-list 118 permit tcp any eq 37994 any
access-list 118 permit tcp any any eq 2725
access-list 118 permit tcp any eq 2725 any
access-list 118 permit tcp any any eq lpd
access-list 118 permit tcp any eq lpd any
access-list 118 permit tcp any any eq 1521
access-list 118 permit tcp any eq 1521 any
access-list 118 permit udp any any eq 9401
access-list 118 permit udp any eq 9401 any

access-list 119 remark prioridade alta (TELNET, VNC, SNMP, OUTROS)
access-list 119 permit tcp any any range 9494 9495
access-list 119 permit tcp any range 9494 9495 any
access-list 119 permit tcp any any eq telnet
access-list 119 permit tcp any eq telnet any
access-list 119 permit tcp any any eq 3389
access-list 119 permit tcp any eq 3389 any
access-list 119 permit tcp any any eq 5529
access-list 119 permit tcp any eq 5529 any
```

```
access-list 119 permit tcp any any eq 2501
access-list 119 permit tcp any eq 2501 any
access-list 119 permit tcp any any eq 2503
access-list 119 permit tcp any eq 2503 any
access-list 119 permit tcp any any eq 5900
access-list 119 permit tcp any eq 5900 any
access-list 119 permit tcp any any eq 31111
access-list 119 permit tcp any eq 31111 any
access-list 119 permit tcp any any eq 4000
access-list 119 permit tcp any eq 4000 any
access-list 119 permit tcp any any eq 94
access-list 119 permit tcp any eq 94 any
access-list 119 permit tcp any any eq 9006
access-list 119 permit tcp any eq 9006 any
access-list 119 permit tcp any any eq domain
access-list 119 permit tcp any eq domain any
access-list 119 permit tcp any any eq 3000
access-list 119 permit tcp any eq 3000 any
access-list 119 permit tcp any any eq 9005
access-list 119 permit tcp any eq 9005 any
access-list 119 permit tcp any any eq 1365
access-list 119 permit tcp any eq 1365 any
access-list 119 permit tcp any any range 1564 1566
access-list 119 permit tcp any range 1564 1566 any
access-list 119 permit tcp any any eq 19655
access-list 119 permit tcp any eq 19655 any
access-list 119 permit tcp any any eq 3500
access-list 119 permit tcp any eq 3500 any
access-list 119 permit tcp any any eq 135
access-list 119 permit tcp any eq 135 any
access-list 119 permit tcp any any eq 445
access-list 119 permit tcp any eq 445 any
access-list 119 permit tcp any any eq ident
access-list 119 permit tcp any eq ident any
access-list 119 permit udp any any eq snmp
access-list 119 permit udp any eq snmp any
access-list 119 permit udp any any eq snmptrap
access-list 119 permit udp any eq snmptrap any
access-list 119 permit udp any any range 9494 9495
access-list 119 permit udp any range 9494 9495 any
access-list 119 permit udp any any eq 3389
access-list 119 permit udp any eq 3389 any
access-list 119 permit udp any any eq 5529
access-list 119 permit udp any eq 5529 any
access-list 119 permit udp any any eq domain
access-list 119 permit udp any eq domain any
access-list 119 permit udp any any eq netbios-ns
access-list 119 permit udp any eq netbios-ns any
access-list 119 permit udp any any eq 19655
access-list 119 permit udp any eq 19655 any

access-list 120 remark prioridade altissima (X25 over IP)
access-list 120 permit tcp any any eq 1998
access-list 120 permit tcp any eq 1998 any

access-list 121 remark prioridade regular (NOTES)
access-list 121 permit tcp any any eq 1352
access-list 121 permit tcp any eq 1352 any
```

ANEXO 04 – Resultado do comando "*show frame-relay pvc*" em um roteador sem placa VIP

```
ROUTER-7206#sh frame-relay pvc 515

PVC Statistics for interface Serial1/1:15 (Frame Relay DCE)

DLCI = 515, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial1/1:15.1

  input pkts 983827        output pkts 1180489   in bytes 58929519
  out bytes 185628468      dropped pkts 1472     in pkts dropped 1472
  out pkts dropped 0       out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 61979     out bcast bytes 12762566
  pvc create time 3d21h, last time pvc status changed 3d21h
  service policy QoS-Super
 Serial1/1:15.1: DLCI 515 -

  Service-policy output: QoS-Super

    Class-map: voz (match-all)
      688532 packets, 44043040 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 24
        Bandwidth 24 (kbps) Burst 600 (Bytes)
        (pkts matched/bytes matched) 688532/44043040
        (total drops/bytes drops) 0/0

    Class-map: altissima (match-all)
      209402 packets, 10997882 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 120
      Weighted Fair Queueing
        Output Queue: Conversation 25
        Bandwidth 7 (%) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 209402/10997882
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: alta (match-all)
      62004 packets, 13192145 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 4
      Weighted Fair Queueing
        Output Queue: Conversation 26
        Bandwidth 13 (%) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 62004/13192145
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: media (match-all)
      35756 packets, 27559785 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 3
      Weighted Fair Queueing
        Output Queue: Conversation 27
        Bandwidth 16 (%) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 35756/27559785
        (depth/total drops/no-buffer drops) 0/0/0
```

```
    Class-map: regular (match-all)
      51569 packets, 55650050 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Match: ip precedence 2  6  7
      Weighted Fair Queueing
        Output Queue: Conversation 28
        Bandwidth 22 (%)
        (pkts matched/bytes matched) 51569/55650050
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0

class  Transmitted  Random drop   Tail drop   Minimum  Maximum  Mark
       pkts/bytes   pkts/bytes    pkts/bytes  thresh   thresh   prob
0         0/0          0/0           0/0          64     128   1/10
1         0/0          0/0           0/0          71     128   1/10
2     51569/54135136   0/0           0/0          78     128   1/10
3         0/0          0/0           0/0          85     128   1/10
4         0/0          0/0           0/0          92     128   1/10
5         0/0          0/0           0/0          99     128   1/10
6     61710/11242667   0/0           0/0         106     128   1/10
7         0/0          0/0           0/0         113     128   1/10
rsvp      0/0          0/0           0/0         120     128   1/10


    Class-map: class-default (match-any)
      133246 packets, 25564621 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Weighted Fair Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 16
        (total queued/total drops/no-buffer drops) 0/0/0
         exponential weight: 9

class  Transmitted  Random drop   Tail drop   Minimum  Maximum  Mark
       pkts/bytes   pkts/bytes    pkts/bytes  thresh   thresh   prob
0     53710/10779604   0/0           0/0          64     128   1/10
1     17826/2986466    0/0           0/0          71     128   1/10
2         0/0          0/0           0/0          78     128   1/10
3         0/0          0/0           0/0          85     128   1/10
4         0/0          0/0           0/0          92     128   1/10
5         0/0          0/0           0/0          99     128   1/10
6         0/0          0/0           0/0         106     128   1/10
7         0/0          0/0           0/0         113     128   1/10
rsvp      0/0          0/0           0/0         120     128   1/10

  Output queue size 0/max total 600/drops 0
  fragment type end-to-end         fragment size 80
  cir 64000     bc   640       be 0         limit 80     interval 10
  mincir 64000     byte increment 80    BECN response no
  frags 2510585   bytes 152510075 frags delayed 1520830
```

ANEXO 05 – Resultado do comando "*show policy-map interface*" em um roteador com placa VIP

```
ROUTER-7507#show policy-map interface Ser 1/1/0:15.1

 Serial1/1/0:15.1: DLCI 515 -

  Service-policy output: Shape-Super

    queue stats for all priority classes:
      queue size 0, queue limit 6
      packets output 186334, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0

    Class-map: class-default (match-any)
      525137 packets, 62075582 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      queue size 0, queue limit 16
      packets output 529012, packet drops 1738
      tail/random drops 1738, no buffer drops 0, other drops 0
      Shape: cir 64000,  Bc 256,  Be 256
        lower bound cir 0,  adapt to fecn 0
        output bytes 54699253, shape rate 0 bps

      Service-policy : QoS-Super

        Class-map: voz (match-all)
          186334 packets, 11905141 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 5
          Priority: kbps 24, burst bytes 1500, b/w exceed drops: 0

        Class-map: altissima (match-all)
          216015 packets, 11216347 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: access-group 120
          queue size 0, queue limit 1
          packets output 215585, packet drops 430
          tail/random drops 430, no buffer drops 0, other drops 0
          Bandwidth: 7%, kbps 4

        Class-map: alta (match-all)
          23597 packets, 4395956 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 4
          queue size 0, queue limit 2
          packets output 23496, packet drops 101
          tail/random drops 101, no buffer drops 0, other drops 0
          Bandwidth: 13%, kbps 8

        Class-map: media (match-all)
          7033 packets, 6085132 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 3
          queue size 0, queue limit 2
          packets output 6701, packet drops 332
          tail/random drops 332, no buffer drops 0, other drops 0
          Bandwidth: 16%, kbps 10
```

```
Class-map: regular (match-all)
  69884 packets, 25758022 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 2  6  7
  queue size 0, queue limit 3
  packets output 69235, packet drops 650
  tail/random drops 650, no buffer drops 0, other drops 0
  Bandwidth: 22%, kbps 14
  Random-detect:
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 0
 Class Random   Tail Minimum   Maximum    Mark       Output
         drop   drop threshold threshold  probabity  packets
 0          0      0         0         1     1/10          0
 1          0      0         0         1     1/10          0
 2          0      0         0         1     1/10      12146
 3          0      0         0         1     1/10          0
 4          0      0         0         1     1/10          0
 5          0      0         0         1     1/10          0
 6          0      0         0         1     1/10      23417
 7          0      0         0         1     1/10          0

Class-map: class-default (match-any)
  22274 packets, 2714984 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  queue size 0, queue limit 1
  packets output 27661, packet drops 225
  tail/random drops 225, no buffer drops 0, other drops 0
  Fair-queue: per-flow queue limit 2
  Random-detect:
    Exp-weight-constant: 9 (1/512)
    Mean queue depth: 0
 Class Random   Tail Minimum   Maximum    Mark       Output
         drop   drop threshold threshold  probabity  packets
 0          0      0         0         1     1/10      22093
 1          0      0         0         1     1/10       5568
 2          0      0         0         1     1/10          0
 3          0      0         0         1     1/10          0
 4          0      0         0         1     1/10          0
 5          0      0         0         1     1/10          0
 6          0      0         0         1     1/10          0
 7          0      0         0         1     1/10          0
```