Universidade do Minho
Escola de Engenharia

Nuno Gonçalves Rodrigues

Qualidade de Serviço na implementação de serviços VoIP – Avaliação a partir de um modelo de simulação

Tese de Mestrado em Informática

Trabalho efectuado sob a orientação do Professor Doutor Alexandre Júlio Teixeira Santos

Fevereiro de 2009

À memória de meu pai

Agradecimentos

Gostaria de começar por agradecer ao Professor Doutor Alexandre Júlio Teixeira Santos, meu orientador, pela sua inesgotável paciência e compreensão ao longo de todos estes anos de acompanhamento.

Uma palavra de apreço muito especial também para a minha futura esposa, Katy, pela paciência, incentivo e decisivo empurrão que me levou à conclusão deste trabalho e para a minha família, pelo inesgotável apoio ao longo de todos estes anos.

Por último, gostaria também de deixar uma palavra de agradecimento para todos aqueles que, de alguma forma, contribuíram com palavras de incentivo para a conclusão deste trabalho.

Resumo

A Internet teve a sua origem há aproximadamente três décadas, em meios militares e de investigação Americanos, tendo por base um princípio que fez sucesso nas comunicações por computador: a comutação de pacotes. Teve desde então um crescimento verdadeiramente notável como meio de comunicação, de partilha de informação e mais recentemente de entretenimento à escala global, sustentada por um conjunto de protocolos muito bem sucedidos e pelos contínuos desenvolvimentos de meios de transmissão e de tecnologias cada vez mais eficientes, fiáveis e avançadas.

Por outro lado, a rede pública telefónica comutada (PSTN) é a infra-estrutura que suporta as comunicações de voz há mais de 100 anos. Tendo apresentado também significativos avanços desde as primeiras centrais de comutação manual desenvolvidas por *Alexander Graham Bell*, baseia no entanto o seu modo básico de funcionamento no mesmo princípio dessa altura: a comutação de circuítos.

Sendo duas infra-estruturas de comunicação (Internet e PSTN) desde o início baseadas em princípios de operação opostos, mantiveram durante muitos anos desenvolvimentos completamente independentes.

No entanto, apesar destas características opostas, nos últimos anos tem-se assistido a uma convergência crescente (e mesmo acelerada mais recentemente) entre as tradicionais redes de voz e as redes de dados, com especial "intromissão" das tecnologias do mundo Internet na transmissão de voz. O conjunto destas tecnologias deram origem aos termos Voz sobre IP (VoIP) e, com um significado mais abrangente, à Telefonia IP.

Apesar de os protocolos desenvolvidos permitirem a implementação destes serviços de voz sobre as redes de dados actuais, há ainda questões fundamentais a resolver, como a qualidade de serviço (QoS) das conversações em ambientes onde a voz partilha a infra-estrutura com diversas outras fontes de tráfego com características completamente diferentes.

Neste contexto, o presente trabalho pretende: apresentar um projecto de implementação de serviços VoIP numa instituição de ensino superior – projecto VoIP@IPB; identificar os requisitos de qualidade de serviço fundamentais para o seu correcto funcionamento e, por último, avaliar, em ambiente de simulação, o impacto do recurso a mecanismos de QoS baseados na *framework DiffServ* para assegurar a QoS adequada ao funcionamento do serviço.

Abstract

Internet had its origin nearly three decades ago, in American military and investigation groups, based on one principle that made success in computer communications: packet switching.

It had, since that time, a notable growth as a communication system, to share information and, more recently, to entertain at a global scale, based on a set of very sucessful protocols and by the continuous developments of transmission systems and technologies each time more efficient and advanced.

On the other hand, the Public Switched Telephone Network (PSTN) is the infrastructure that supports the voice communications for more than 100 years.

Having presented great advances since the first switchboards developed by *Alexander Graham Bell*, PSTN basic operation is, nevertheless, based on the same principle of that time: circuit switching.

Internet and PSTN are two communication infrastructures based on antagonic principles, independently developed for many years.

Nevertheless, and despite these antagonic characteristics, in the last few years we have been assisting to an increasing convergence (and almost accelerated more recently) between traditional voice networks and data networks, with special "invasion" of Internet technologies in the voice transmission world. The set of these technologies gave origin to the terms Voice over IP (VoIP) and IP Telephony.

Although developed protocols allow the implementation of these voice services under the actual data networks, basic questions still need to be solved, like the quality of service (QoS) of the conversations in environments where the voice shares the infrastructure with other sources of traffic with completely different characteristics.

In this context, the present work intends to: describe a project for implementation of VoIP services in a higher education institution – VoIP@IPB project; identify the basic requirements of quality of service for its normal operation and, finally, to evaluate, in simulation environment, the impact of the QoS mechanisms used, based in the *DiffServ* framework, to assure the adequate QoS for the correct operation of the service.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

À medida que a Internet vai crescendo, em número de utilizadores, *hosts* ligados e conteúdos disponibilizados, com mais intensidade se vão verificando algumas das suas debilidades. Uma das que ultimamente mais tem ocupado os investigadores prende-se com a Qualidade de Serviço.

O surgimendo de novos serviços e aplicações, associados a diferentes tipos de tráfego, com necessidades distintas (vídeo, áudio, tempo-real, etc), é um dos motores dos desenvolvimentos recentes nesta área.

O funcionamento da Internet caracteriza-se, desde o seu surgimento, pelo paradigma do *best effort* associado ao protocolo IP[1]. Significa isto que cada nodo da rede vai realizar o melhor esforço possível para tratar os pacotes IP, dando-lhes no entanto o mesmo tratamento, em função das condições de rede existentes em cada momento.

Ora, muitas das novas aplicações têm diferentes graus de exigência no tráfego que geram, nomeadamente ao nível do atraso do transporte dos dados, perdas e largura de banda disponível.

São estes factores que não são compatíveis com o paradigma tradicional do *best effort*, e que motivam a procura de novas soluções que garantam uma qualidade de serviço diferenciada.

Entre os desenvolvimentos mais recentes nesta área, destacam-se dois modelos que têm vindo a ser desenvolvidos no âmbito do IETF: *Integrated Services* - IntServ [4] e *Differentiated Services* - DiffServ [5].

O primeiro [30, 31] define um conjunto de métodos de especificação de qualidade de serviço e que permitem reservar recursos, que são alocados para fluxos de dados individuais. Este modelo tem apresentado no entanto algumas limitações que têm vindo a colocar em causa a sua aplicabilidade em escala alargada.

Como tentativa de ultrapassar estas limitações, surgiu o modelo DiffServ [32, 33], que classifica o tráfego em diferentes classes de serviço (CoS), com base num conjunto de bits específicos nos cabeçalhos dos pacotes IP (sejam eles pacotes IPv4, sejam pacotes IPv6).

O objectivo é fornecer um tratamento particular a diferentes classes de tráfego, identificadas em cada pacote IPv4 ou IPv6 pelo campo DS[2] [32], por parte dos

[1] *Internet Protocol*

[2] *differentiated services field*

sistemas de comunicação, com base na classe de serviço definida para esse mesmo pacote.

Um dos factores que tem induzido esta procura de mecanismos mais eficientes de QoS é a crescente convergência entre as redes de Voz e Dados. As redes tradicionais de voz sempre funcionaram com base numa abordagem de comutação de circuitos, que se traduz numa garantia de reserva de recursos durante todo o tempo de uma comunicação. Por outro lado, as redes de dados desenvolveram-se, nas últimas décadas, em redor do paradigma da comutação de pacotes, onde por norma não são usados mecanismos de reserva ou prioritização de recursos (princípio *best effort* referido anteriormente).

Na sequência deste movimento de convergência, começou a equacionar-se, há três anos atrás, a migração progressiva da antiga e tecnicamente desactualizada rede de Voz do Instituto Politécnico de Bragança (IPB), para o mundo IP, através da implementação de serviços VoIP[3] sobre a Rede de Dados da Instituição. Esta abordagem traduziu-se na criação do projecto VoIP@IPB, que será descrito no capítulo 4 desta dissertação.

Entretanto, mais recentemente, a FCCN[4] decidiu avançar com um projecto a nível nacional para criação de uma Rede de VoIP sobre a infra-estrutura da RCTS - projecto VoIP@RCTS [68]. O IPB, à semelhança da generalidade das Instituições de Ensino Superior Portuguesas, aderiu a este projecto, sendo o mesmo visto internamente como um projecto complementar ao projecto VoIP@IPB atrás referido.

1.1 Objectivos

Pretende-se com esta dissertação, descrever sumariamente os trabalhos desenvolvidos para implementação do projecto VoIP@IPB e avaliar, através de um ambiente de simulação, a efectiva capacidade do modelo *DiffServ* para tratar de forma diferenciada o tráfego VoIP relativamente ao restante tráfego na Rede do IPB.

O tráfego de tempo real em geral, e o VoIP em particular, é bastante sensível ao atraso fim-a-fim e à variação desse mesmo atraso. Assim, um dos objectivos deste trabalho passa por identificar os pontos críticos onde o efeito destes factores se possa fazer sentir de forma mais acentuada. Para esses pontos, pretende-se de seguida fazer uma avaliação dos requisitos de QoS necessários para a sua respectiva minimização, recorrendo para tal à implementação de políticas de QoS baseadas no modelo DiffServ. Esta avaliação será efectuada com uma ferramenta de simulação amplamente testada neste domínio - NCTUns [77], desenvolvida no Departmento de Ciências da Computação da *National Chiao Tung University* (NCTU), Taiwan.

Importa analisar o comportamento que o tráfego normal produz nos fluxos de tráfego VoIP ao passar por esses pontos, em igualdade de condições e em condições de tratamento diferenciado para estes últimos fluxos.

Pretende-se assim analisar o comportamento, em termos de Qualidade de Serviço (atrasos, variação dos atrasos, taxas efectivas de transmissão, pacotes perdidos), dos

[3]Voz sobre o protocolo IP

[4]Fundação para a Computação Científica Nacional: entidade que gere a RCTS - Rede Ciência Tecnologia e Sociedade

sistemas intermediários e da rede na sua generalidade, quando submetidos a classes de tráfego diferenciado, em concorrência com tráfego *best effort*.

1.2 Organização da Tese

No capítulo *Das Redes de Computadores à Voz sobre IP* começam por ser analisadas as principais tecnologias e protocolos usados nas redes da actualidade, com especial ênfase no modelo TCP/IP e respectivo protocolo de rede (IP). Segue-se uma breve descrição do Serviço VoIP, ao nível das suas características, princípio de funcionamento e principais protocolos e tecnologias usadas.

No capítulo *Qualidade de Serviço em Redes IP*, começa por ser feita uma breve resenha sobre as principais motivações para a necessidade de introdução de mecanismos de qualidade de serviço nas redes da actualidade, a que se segue uma pequena análise sobre o que se entende por qualidade de serviço em redes informáticas.

Analisam-se a seguir os principais mecanismos de controlo de tráfego disponíveis em redes IP, nomeadamente ao nível dos algoritmos de gestão das filas de espera dos encaminhadores e dos mecanismos de controlo e prevenção de congestão. Por último, são analisados os principais modelos de implementação de qualidade de serviço em redes IP, com especial ênfase no modelo de Serviços Diferenciados – *DiffServ*, dada a sua importância para o trabalho desenvolvido.

O capítulo *Implementação de Serviços VoIP numa Rede de Campus: O caso do Instituto Politécnico de Bragança - IPB* começa com uma apresentação da Instituição IPB e respectivas rede telefónica e de dados. Segue-se uma descrição do projecto VoIP@IPB, ao nível dos seus objectivos, arquitectura, pormenores de implementação e estado actual. Conclui-se o capítulo com uma breve descrição do projecto VoIP@RCTS e a sua interação/integração com o projecto VoIP@IPB.

No capítulo *Implementação de QoS para suporte de Serviços VoIP* serão analisados os principais factores que condicionam o normal funcionamento de um serviço VoIP e procurar-se-á definir os requisitos que permitam assegurar esse mesmo normal funcionamento.

Conclui-se este capítulo com uma breve descrição da ferramenta *NCTUns* e, mais especificamente, dos seus mecanismos de suporte à simulação do modelo *DiffServ*.

O capítulo *Experiências e resultados* começa com uma descrição do modelo de simulação a implementar para cumprir os objectivos traçados para o presente trabalho. De seguida, detalham-se os testes realizados para avaliação do comportamento do tráfego VoIP quando em competição com os fluxos de tráfego tradicional pelos recursos da rede. Apresentam-se assim os testes realizados em dois cenários diferentes: num ambiente *best effort* e num ambiente com diferenciação de serviços, em que o tráfego VoIP recebe tratamento privilegiado relativamente ao tráfego tradicional.

No capítulo *Conclusões e trabalho futuro* são apresentadas algumas conclusões retiradas do trabalho realizado, bem como a indicação de possíveis caminhos futuros de desenvolvimento deste mesmo trabalho.

Capítulo 2

Das Redes de Computadores à Voz sobre IP

2.1 Arquitecturas Protocolares

As redes de computadores são uma peça fundamental da vasta área das tecnologias de informação da actualidade e, por arrastamento, dos sistemas de informação e, em última instância, da própria sociedade, dita "da Informação".

Tendo surgido à algumas décadas atrás, primeiro ao serviço dos militares e passando a seguir para as grandes organizações, atravessaram um longo caminho até à realidade actual.

No início, cada fabricante desenvolvia as suas próprias tecnologias de rede de forma completamente independente, e por conseguinte incompatíveis com os produtos dos outros fabricantes.

Assim, vários organismos internacionais têm-se dedicado a tarefas de normalização nesta área, com o objectivo de criar padrões ou modelos de referência que, desde que seguidos pelos fabricantes, garantirão a inter-operacionalidade dos diferentes equipamentos. Entre os organismos mais conhecidos nesta matéria destacam-se a *International Standards Organization* – ISO, o *Institute of Electrical and Electronics Engineers* – IEEE, *Internet Society* – ISOC, *Internet Engineering Task Force* – IETF, *International Telecommunications Union* – ITU e o *American National Standards Institute* – ANSI, entre outros. Embora o ANSI seja um instituto americano, desempenha um papel de normalização importante a nível internacional, devido ao peso da própria economia americana em todo o mundo.

O resultado dos trabalhos de normalização destas organizações normalmente traduz-se em **modelos ou arquitecturas abertas**, já que podem (e devem) ser livremente implementados pelos fabricantes dos equipamentos.

Por outro lado, vários fabricantes de equipamentos desenvolveram também os seus próprios modelos de comunicação, ditos **modelos proprietários**, já que são propriedade de quem os desenvolve (e normalmente apenas implementados nos equipamentos destes).

Os modelos ou arquitecturas referidos atrás constituem um conjunto coerente de especificações ou **protocolos**, que definem os diferentes aspectos a ter em conta na interligação de equipamentos em rede.

Pode-se definir protocolo como sendo um conjunto de convenções ou regras, mutuamente aceites por duas entidades/sistemas e que regem a comunicação entre ambos, definindo aspectos como a sintaxe, a semântica e a temporização das trocas de dados.

Para se chegar a um conjunto coerente de protocolos, os modelos são estruturados em camadas ou níveis protocolares, traduzindo uma individualização, tanto quanto possível, das diversas tarefas envolvidas no processo de comunicação.

Uma arquitectura de comunicações por computador pode também ser vista como uma pilha de protocolos, em que cada protocolo se enquadra num determinado nível dessa arquitectura.

A utilização de arquitecturas abertas no desenvolvimento e implementação de sistemas de comunicação por computador apresenta algumas vantagens [47]:

- independência dos utilizadores relativamente a um único fabricante;
- integração de equipamentos de diferentes fabricantes num mesmo sistema, com inter-operacionalidade entre eles.

Por outro lado existem também algumas desvantagens [47]:

- maior complexidade nos equipamentos, para garantir a compatibilidade entre equipamentos diferentes, que se traduz normalmente em menor desempenho e maiores custos;
- necessidade de verificação de conformidade de funcionamento entre diferentes equipamentos.

De seguida será feita uma breve apresentação dos modelos e arquitecturas de comunicação por computador mais relevantes, nomeadamente as arquitecturas abertas **TCP/IP** e **modelo de referência OSI**.

2.1.1 O Modelo de Referência OSI

O modelo de referência OSI (*Open Systems Interconnection*) foi proposto pela ISO[1], com o objectivo de promover a definição de um conjunto de normas para a interligação em rede de sistemas abertos. Com início de desenvolvimento na década de 70, acabaria por ser publicado como standard ISO 7498 em 1984.

Apesar dos objectivos iniciais, bastante ambiciosos na criação de um modelo de adopção universal, na prática tal não veio a acontecer. Por várias razões, entre as quais a complexidade, razões de mercado e de desenvolvimento tecnológico, este modelo não teve uma adopção generalizada por parte dos fabricantes.

Ficou, no entanto, um trabalho de base muito importante para os desenvolvimentos dos últimos anos nesta área, já que este modelo passou a ser uma referência para a generalidade das arquitecturas de comunicação da actualidade.

A especificação deste modelo contempla uma divisão em sete camadas, correspondentes a diferentes níveis de abstração identificados num processo de comunicação entre dois sistemas informáticos:

[1] *International Standards Organization*

- Camada física: lida com a transmissão não estruturada da sequência de bits sobre o meio físico; em suma, lida com os detalhes mecânicos, eléctricos, funcionais e procedimentais de acesso ao meio físico; por exemplo: tipo de comunicação (*simplex*, etc.), quantos volts para representar um bit 1 ou 0, qual a duração de cada bit, qual a configuração dos pinos de um conector, etc;

- Camada de ligação de dados: fornece a transferência estruturada e fiável de dados sobre a ligação física; envia blocos de dados (*frames*) tendo em atenção aspectos como a sincronização, tratamento de erros (e.g., retransmissões) e controlo de fluxo;

- Camada de rede: fornece às camadas superiores independência das tecnologias de transmissão e comutação usadas na conexão física dos sistemas; encaminha as mensagens (pacotes) desde o sistema originador, através de sistemas intermediários, até ao sistema de destino; efectua controlo de congestão;

- Camada de transporte: oferece transmissão fiável de dados entre sistemas finais; providencia gestão de fluxo e recuperação de erros fim-a-fim; efectua sequenciação e fragmentação;

- Camada de sessão: fornece a estrutura de controlo da comunicação entre duas aplicações; estabelece, gere e termina conexões (sessões) entre aplicações; efectua gestão de *tokens* (que permite, a duas aplicações, intercalarem as suas mensagens/actividades) e sincronização da transferência de dados (que permitem a recuperação de uma transferência interrompida, pela análise de *check-points*);

- Camada de apresentação: fornece às aplicações independência de diferenças na representação (sintaxe) dos dados; codifica os dados em "representações de rede", independentes do código de caracteres (ASCII vs Unicode) e do byte ordering (*big-endian vs little-endian*) do sistema;

- Camada de aplicação: fornece aos utilizadores acesso ao ambiente OSI, bem como serviços de informação distribuídos; contém todas as aplicações de nível utilizador que, de alguma forma, necessitam da rede.

2.1.2 A Arquitectura TCP/IP

A Arquitectura Protocolar TCP/IP, também conhecida por pilha protocolar Internet, herda o nome dos seus dois protocolos mais importantes: TCP – *Transmission Control Protocol* e IP – *Internet Protocol*, sendo no entanto constituída por um número bastante mais alargado de protocolos.

Esta arquitectura tem vindo a ser progressivamente desenvolvida durante os últimos quase 40 anos, tendo como origem, no final dos anos 60, uma investigação levada a cabo no âmbito do desenvolvimento da rede de comutação de pacotes ARPANET, financiada pela agência governamental americana DARPA - *Defense Advanced Research Projects Agency.*

É uma arquitectura directamente associada à rede mundial de cumputadores **Internet**, no seio da qual surgiu, foi testada e é actualmente o seu suporte fundamental.

A Internet surgiu a partir da evolução da ARPANET, e da sua interligação a outras redes, no início dos anos 80, nomeadamente à rede de investigação americana CSNet[2].

Tal como outras arquitecturas de rede, a pilha TCP/IP está modelada em níveis, ou camadas, sendo normalmente usada uma representação em quatro camadas:

- Camada física: na prática, o modelo TCP/IP pouco concretiza em relação a esta camada, para além do facto de ter de suportar o transporte de pacotes IP;

- Camada de rede: opera em modo não orientado à conexão; o protocolo que a materializa é designado por IP – *Internet Protocol*. Este nível é responsável por fornecer a ilusão de uma única rede global. Torna transparente, para os níveis superiores, as tecnologias utilizadas ao nível físico entre as redes interligadas;

- Camada de transporte: fornece a transferência de dados fim-a-fim. É corporizada por dois protocolos: o TCP – *Transmission Control Protocol* (orientado à conexão; efectua, se necessário fragmentação e controlo de fluxo) e o UDP – *User Datagram Protocol* (não orientado à conexão; sem garantias de sequenciação);

- Camada de aplicação: oferece aplicações/protocolos de terminal virtual (telnet), transferência de ficheiros (ftp), correio electrónico (smtp), resolução de nomes (dns), hipertexto (http), fóruns de discussão (nntp), etc...

O Protocolo IP

O IP [6, 7, 8, 9] é o protocolo base de toda a arquitectura, operando ao nível da camada de rede. Esconde aos níveis superiores os detalhes da ligação física da rede, criando a ilusão de uma rede virtual única.

Trata-se de um protocolo de transmissão de pacotes não orientado à conexão (*connectionless* - CL), não fiável e que aplica a princípio do fornecimento de um serviço baseado no melhor esforço (*best-effort*).

Este princípio significa que, aplicando igual tratamento aos pacotes que a rede lhe confia, o protocolo IP tenta efectuar o seu encaminhamento até ao destino, com base no melhor aproveitamento possível dos recursos disponíveis no momento. Significa ainda que os pacotes enviados pelo IP podem ser perdidos, recebidos fora de ordem, ou eventualmente duplicados, sem que este se preocupe; é problema dos protocolos dos níveis superiores resolver essas situações.

A unidade de transferência de pacotes de dados em redes TCP/IP designa-se por Datagrama IP. Este é constituído por um cabeçalho, com informação relevante para o IP, e por dados, que são apenas relevantes para os protocolos de nível superior.

[2] *Computer Science Network*

Um endereço IP [12] identifica univocamente um interface de rede, em ambiente TCP/IP, sendo representado por um conjunto de 32 bits. Habitualmente é representado no formato de notação decimal pontuada, ou seja, agrupam-se os 32 bits em conjuntos de 8 (formando 4 bytes) e representa-se assim o equivalente decimal de cada um dos bytes, concatenados pelo sinal ponto final ".".

O endereço IP é constituído por duas partes: <número de rede> <número do nodo>. O número de rede é administrado centralmente pelo InterNIC[3] e tem de ser único em toda a Internet. O número do nodo é administrado localmente a cada rede, onde tem de ser único.

De uma forma genérica, um endereço IP identifica um nodo, numa rede TCP/IP, no entanto, de uma forma mais exacta, identifica um interface que tem capacidade de enviar e receber datagramas IP. Isto significa que um nodo pode ter mais que um interface de rede, logo poderá ter mais do que um endereço IP atribuído.

Para enviar um datagrama IP para determinado endereço IP de destino, é necessário mapear esse endereço para o respectivo endereço físico; esta tarefa é realizada, nas LAN's, pelo protocolo ARP[4].

Historicamente, os primeiros bits do endereço IP especificam como é que o resto do endereço deve ser separado na parte da rede e na parte do nodo. Esta separação conduz à noção de classes de endereços IP, sendo o conjunto do espaço de endereçamento IP (na versão 4 deste protocolo – IPv4) dividido em 5 classes:

- Classe A (primeiro bit toma o valor zero (0)): utiliza 7 bits para identificar a <rede> e 24 bits para a parte <nodo> do endereço IP; Isto permite $2^7 - 2$ (126) redes com $2^{24} - 2$ (16777214) nodos cada; no total perfaz mais de 2 biliões de endereços.

- Classe B (primeiros dois bits tomam os valores um e zero (10), respectivamente): usa 14 bits para identificar a <rede> e 16 bits para identificar o <nodo>; permite $2^{14} - 2$ (16382) redes com $2^{16} - 2$ (65534) nodos cada; dá um total superior a um bilião de endereços.

- Classe C (primeiros dois bits tomam o valor um e o terceiro bit toma o valor zero (110)): utiliza 21 bits para a <rede> e 8 bits para o <nodo>; disponibiliza $2^{21} - 2$ (2097150) redes com $2^8 - 2$ (254) nodos cada; no total cerca de meio bilião de endereços.

- Classe D (primeiros três bits tomam o valor um e o quarto bit toma o valor zero (1110)): gama de endereços reservada para comunicação multicast.

- Classe E (primeiros quatro bits tomam o valor um e o quinto bit toma o valor zero (11110)): gama reservada para uso futuro.

Independentemente desta divisão, qualquer componente de um endereço IP em que todos os bits contém o valor zero ou todos os bits contém o valor um têm um significado especial:

[3] *Internet Network Information Center*
[4] *Address Resolution Protocol*

- todos os bits zero (0): significa *'para este'*. Este nodo (endereço IP com <nodo number>=0) ou esta rede (endereço IP com <rede>=0);

- todos os bits a um (1): significa *'para todos'*; todas as redes ou todos os nodos. Por exemplo, o endereço 128.2.255.255 identifica todos os nodos na rede de Classe B 128.2, designando-se nestes casos Endereço de Broadcast directo;

- *Loopback*: a rede de Classe A 127.0.0.0 está definida como rede de *loopback*; os endereços desta rede são atribuídos a interfaces virtuais que processam dados dentro do sistema local, sem nunca aceder a um interface físico.

Com o crescimento explosivo da Internet, o princípio de definição/divisão dos endereços IP mostrou-se relativamente ineficiente, para permitir pequenas alterações nas configurações locais das redes, nomeadamente quando: a) se instala um novo tipo de rede física; b) o crescimento do número de nodos requer a separação de uma rede local em duas ou mais redes separadas; c) o crescimento das distâncias requer a separação de uma rede local em redes mais pequenas, interligadas entre si por *Gateways*.

Para ser possível a atribuição de mais endereços IP nestes casos, introduziu-se o conceito de Sub-Rede. Esta definição pode ser apenas local, continuando a aparecer perante o exterior como uma única rede IP.

Com este conceito, a parte <host number> do endereço IP é sub-dividida em <subnet number> e <host number>. O endereço IP passa assim a ser interpretado da seguinte forma:

<network number><subnet number><host number>

O conjunto *subnet number* e *host number* formam o *endereço local*, podendo este processo de divisão de uma rede (*subnetting*) ser implementado de forma transparente para as redes remotas.

A divisão da parte local do endereço IP pode ser feita livremente pelo administrador local da rede. Qualquer conjunto de bits na parte local pode ser usado para formar a sub-rede. Esta divisão é feita usando uma máscara de sub-rede (*subnet mask*), que é um número de 32 bits, normalmente também representado em notação decimal pontuada.

Os bits com valor zero (0) na máscara de rede correspondem a bits no endereço IP que identificam a parte *host number*. Os bits com valor um (1) na máscara de rede identificam os bits no endereço IP que representam a parte da rede.

Embora seja possível associar qualquer parte do endereço local à parte da sub-rede e à parte do nodo, o mais normal e aconselhável é usar um bloco contínuo de bits do início da parte local para a sub-rede e os restantes bits para o nodo.

A divisão de uma rede em duas ou mais partes pode ser feita de uma forma estática ou variável.

Com *subnetting* estático todas as sub-redes utilizam a mesma máscara de rede. Tem como principal vantagem a simplicidade de implementação e de manutenção, implicando, no entanto, o desperdício de espaço de endereçamento para pequenas redes. Por exemplo, uma rede de quatro nodos que utiliza uma máscara de rede 255.255.255.0 desperdiça 250 endereços IP.

Com *subnetting* variável, as sub-redes de uma rede maior podem ter diferentes máscaras, logo diferentes dimensões. Este tipo de divisão permite adequar a dimensão das sub-redes às reais necessidades, sem muitos desperdícios de endereços IP.

A maior parte dos endereços IP identificam recipientes simples, referidos como endereços *Unicast*, que permitem o estabelecimento de ligações ponto-a-ponto.

Adicionalmente, existem três tipos especiais, que são usados para identificar múltiplos recipientes:

- endereços de *Broadcast* identificam todos os nodos de uma rede;
- endereços de *Multicast* identificam grupos de nodos e
- endereços de *Anycast* identificam um de vários nodos possíveis.

Qualquer protocolo não orientado à conexão pode enviar mensagens para endereços de *Broadcast*, *Multicast* ou *Anycast*, bem como *Unicast*. Os protocolos orientados à conexão podem apenas usar endereços *Unicast*, já que a ligação é estabelecida entre um par específico de nodos.

Desde a segunda metade da década de 90, a Internet experimentou um crescimento exponencial, que se traduziu na manifestação de um conjunto de problemas. O primeiro deles teve orígem no grande crescimento das tabelas de encaminhamento e do tráfego de encaminhamento trocado pelos encaminhadores, motivado pelo enorme incremento no número de redes utilizadas.

O segundo grande problema traduziu-se num progressivo esgotamento do espaço de endereçamento IP.

A versão 4 do protocolo IP (IPv4) define endereços de 32 bits, o que permite um máximo teórico de 2^{32} (4.294.967.296). Apesar de aparentemente parecer um valor grande, na realidade, devido a limitações já referidas atrás (nomeadamente a divisão do espaço de endereçamento em Classes, que não permite a sua gestão de um modo verdadeiramente eficiente, e a existência de endereços especiais que não identificam nodos) o valor real disponível desce consideravelmente. Tendo em conta o crescimento da sua procura na última década e meia, prevê-se para breve um esgotamento de todo o espaço de endereçamento usado pelo IPv4.

Durante bastante tempo, a gestão da atribuição de redes não foi efectuada com as devidas precauções, nomeadamente em relação à adequação do tamanho das redes atribuídas às reais necessidades de máquinas a interligar. Durante a década de noventa tentou-se minorar este problema, com a definição de um conjunto de regras mais restritivas para a alocação de espaço do endereçamento IPv4 [10, 11].

Para além desta tentativa de melhor gerir e controlar a alocação do espaço de endereçamento disponível, foi criado um outro conjunto de medidas com o mesmo objectivo: a) definição de redes IP para utilização privada; b) definição do mecanismo *Classless Inter-Domain Routing* – CIDR.

O RFC 1918 [50] define um conjunto de gamas de endereços que não podem ser utilizados para ligação de nodos directamente à Internet, ficando assim disponíveis para utilização em organizações que pretendem interligar apenas internamente computadores, através da arquitectura TCP/IP. Foram alocadas três gamas

de endereços para este efeito: a) a rede de Classe A 10/8; b) 16 redes contínuas de Classe B 172.16/16 até 172.31/16; c) 256 redes contínuas de Classe C 192.168.0/24 até 192.168.255/24.

Qualquer organização pode utilizar este espaço de endereçamento privado sem dar satisfações a ninguém. Dado que estes endereços poderão ser utilizados por várias organizações ao mesmo tempo, não podem ser utilizados em encaminhadores que interligam diferentes redes. Espera-se que os encaminhadores de fronteira de uma rede que utiliza endereçamento privado descartem toda a informação de encaminhamento referente a esses endereços, devendo limitar essas referências ao interior da rede.

Nodos que têm apenas um endereço IP privado não devem ter conectividade no nível de Rede com a Internet. Neste caso, toda a conectividade com nodos fora da rede privada deve ser fornecida por *Application Gateways*.

O mecanismo *Classless Inter-Domain Routing* – CIDR [13, 14, 15, 16], veio disponibilizar duas funcionalidades que, em conjunto, permitiram uma redução substancial do tamanho das tabelas de encaminhamento da Internet e um melhor aproveitamento do espaço de endereçamento do IPv4.

A primeira funcionalidade consistiu na eliminação da tradicional divisão em classes dos endereços IP, introduzindo o conceito de prefixo de rede. Este prefixo especifica o número de bits contíguos mais à esquerda que identificam a parte da rede, num endereço IP.

Os encaminhadores passaram assim a determinar o ponto de separação entre a parte *network number* e *host number* destes endereços recorrendo a este prefixo, em vez de analisar os seus primeiros bits. Esta alteração veio permitir a utilização de redes com tamanhos arbitrários (ajustados às reais necessidades), em vez dos tradicionais tamanhos fixos, resultantes da definição das classes (8, 16 ou 24 bits).

A segunda grande funcionalidade do CIDR está no suporte à agregação de rotas, onde uma única entrada numa tabela de encaminhamento pode representar o espaço de endereçamento que antes correspondia a centenas ou milhares de rotas tradicionais, baseadas em classes. Neste caso, cada entrada de uma rede numa tabela de encaminhamento conterá, para além dos campos habituais, também o prefixo associado a essa rede, que definirá o seu tamanho.

A agregação de rotas traduz-se no conceito de Super-Rede (*supernetting*), em oposição ao conceito de divisão de redes, conhecido por *subnetting*.

A par do endereçamento universal dos nodos, outra das principais funções da camada de rede do TCP/IP é realizar o encaminhamento dos pacotes IP. Esta tarefa é realizada por encaminhadores, que são nodos com capacidade de interligar diferentes redes físicas ao nível da camada de rede, recorrendo para essa função a tabelas de encaminhamento que indicam qual o próximo salto para onde cada pacote deve ser transmitido.

As tabelas de encaminhamento podem ser construídas manual ou dinamicamente. No primeiro caso, a sua construção é feita a partir de informação introduzida pelos administradores de cada rede.

No segundo caso, os encaminhadores recorrem a Protocolos de Encaminhamento (que por sua vez utilizam algoritmos de encaminhamento) para trocar informação entre si sobre as rotas que cada um conhece, com a qual vão construir dinâmica e

automaticamente estas tabelas.

Directamente associado ao encaminhamento IP na Internet está o conceito de Sistema Autónomo [17], que se pode definir como o conjunto de redes IP sob administração de uma única autoridade administrativa. Por exemplo, o conjunto de redes IP alocadas a um ISP constituirá, em condições normais, o seu Sistema Autónomo.

Com base no conceito de Sistema Autónomo, os protocolos de encaminhamento são divididos em duas categorias: a) *Interior Gateway Protocols* – IGP; b) *Exterior Gateway Protocols* – EGP.

Os protocolos IGP são usados para trocar informação de encaminhamento no interior dos Sistemas Autónomos. Entre os mais utilizados destacam-se: a) o *Routing Information Protocol* – RIP [18] e RIPv2 [19], baseados num algoritmo de encaminhamento do tipo vector/distância; b) o protocolo *Open Shortest Path First* – OSPF [20], baseado num algoritmo de encaminhamento do tipo *link state*.

Os protocolos EGP permitem a troca de informação de encaminhamento inter-Sistemas Autónomos, através dos encaminhadores de fronteira. Destaca-se nestas funções o *Border Gateway Protocol* – BGP que, a partir da versão quatro (BGP-4) [21], passou a suportar a agregação de redes de acordo com o mecanismo CIDR, tornando assim mais eficiente o seu anúncio entre diferentes Sistemas Autónomos.

Protocolo IP, versão 6 – IPv6

Como foi referido anteriormente, um dos problemas do protocolo IP identificados no início da década de 90 era o previsível esgotamento do espaço de endereçamento.

Para resolver este problema, para além das medidas de curto prazo já abordadas anteriormente, foi decidido, a médio/longo prazo, desenvolver um novo protocolo de Rede, que eliminasse essa e outras limitações da versão actual (4) do referido protocolo (IPv4). Assim, após alguns anos de especificações e testes, surgiu o novo protocolo IP, conhecido por **Protocolo IP de Próxima Geração** (*IP Next Generation*) ou **Protocolo IP versão 6 - IPv6**.

O protocolo IPv6 [22, 23] é actualmente a nova especificação do protocolo IP, recomendada pelo grupo de trabalho IPng da IETF[5] em Julho de 1994, tendo sido aprovada pela IESG[6] em Novembro desse ano e tornada Standard em Dezembro de 1995.

Comparativamente ao IPv4, este novo protocolo apresenta as seguintes características principais [24]:

- Expansão da capacidade de endereçamento (endereços de 128 bits), em conjunto com uma estrutura hierarquizável dos endereços;
- Expansão e simplificação das capacidades de encaminhamento, com a eliminação da noção anterior de classes e recorrendo ao endereçamento hierárquico;
- Simplificação do protocolo, que veio permitir um processamento mais rápido dos pacotes;

[5]Internet Engineering Task Force
[6]Internet Engineering Steering Group

- Suporte alargado e mais flexível para opções, recorrendo para tal à utilização de cabeçalhos adicionais, sem necessidade de alteração do formato genérico dos pacotes;

- Suporte de diferentes níveis de Qualidade de Serviço (QoS) e de reserva de recursos;

- Autenticação e Privacidade, através da inclusão de mecanismos de segurança no nível de rede, recorrendo nomeadamente a cabeçalhos de autenticação e cabeçalhos para dados encriptados;

- Novos tipos de endereços. Além dos tipos já suportados na versão 4 *unicast* (informação dirigida a um destinatário) e *multicast* (uma única cópia dos pacotes para todos os elementos de um grupo), é acrescentado um novo tipo *anycast* (os pacotes deverão ser entregues a apenas um membro de um grupo de destino). Foi ainda eliminado o tipo de endereços *broadcast* (informação enviada a todos os destinatários);

- Introdução de mecanismos de auto-configuração dos endereços.

O datagrama IPv6 começa com um cabeçalho genérico, cuja estrutura é consideravelmente mais simplificada que a da versão 4.

Quando se torna necessário transportar opções adicionais não previstas neste cabeçalho genérico, utilizam-se os chamados cabeçalhos de extensão, posicionados imediatamente a seguir ao inicial.

Com um tamanho variável (no entanto, sempre múltiplo de 8 bytes), estão actualmente definidas as seguintes extensões: para Opções Salto-a-Salto, Encaminhamento, Fragmentação, Autenticação (*Autentication Header* – AH), Encriptação (*Encapsulating Security Payload* – ESP) e extensão para Opções no Destinatário.

Como referido anteriormente, esta nova versão do protocolo IP passou o tamanho dos endereços de 32 bits para 128 bits. Embora em termos lineares o aumento seja verdadeiramente extraordinário (de 2^{32} (4.294.967.296) para 2^{128} (340.282.366.920.-938.463.363.374.607.431.768.211.456), na prática não é exactamente assim, devido nomeadamente à estrutura hierárquica e ao esquema de alocação de endereços. No entanto, ainda assim, o aumento real é verdadeiramente notável, esperando-se que este seja um problema resolvido por muito tempo.

Tal como com IPv4, em IPv6 um endereço identifica um interface de uma máquina ligada a determinada sub-rede, podendo ainda cada interface possuir mais do que um endereço (habitualmente tem no mínimo um endereço local e um endereço global).

Os endereços IPv6 são constituídos, como já se disse, por um total de 128 bits, sendo representados por oito conjuntos de inteiros de 16 bits, separados pelo sinal de pontuação ":".

Para além desta forma de representação, existem ainda mais algumas alternativas: a) substituição de uma sequência inicial de zeros por um único zero; b) substituição de múltiplos de 16 bits totalmente preenchidos com zeros pela sequência "::"(esta representação só pode ser usada uma vez em cada endereço); c) 8 grupos

de valores hexadecimais separados por ":" seguidos de quatro valores decimais separados pelo sinal ponto final ".", correspondendo estes últimos 4 valores decimais a endereços IPv4, para os quais se usa a sua notação convencional.

Abstraíndo estes diferentes esquemas de representação, que têm como objectivo principal facilitar o manuseamento dos endereços, um endereço IPv6 apresenta sempre um formato genérico, que o divide em duas partes: um *prefixo* e um *token*. Assim, uma representação textual completa conterá os 8 conjuntos de inteiros de 16 bits, numa das formas apresentadas atrás, seguido de uma barra ("/") e de um valor n, que identifica o número de bits mais significativos reservados ao prefixo.

A utilização deste prefixo permite a criação de uma estrutura hierárquica de endereçamento, através da qual se definem vários tipos de endereços, classificados quanto ao seu nível de validade/visibilidade.

De uma forma genérica, os endereços IPv6 podem ser do tipo *unicast*, *multicast* ou *anycast*.

Os endereços *unicast* são por sua vez estruturados em várias categorias, tendo em conta o seu nível de validade/visibilidade: *Global*, *Link-Local*, *Site-Local*, *Embedded IPv4* e endereço de *Loopback*

Com o objectivo de facilitar a implementação de uma estrutura hierárquica de endereçamento a nível mundial, e com isso diminuir o tamanho das tabelas de encaminhamento, os endereços do tipo *unicast global* apresentam-se divididos em diferentes níveis identificadores de agregação.

O encaminhamento IPv6 é idêntico ao encaminhamento com CIDR do IPv4. Com as extensões necessárias para o suporte do IPv6, é possível a utilização de diversos protocolos de encaminhamento, entre os quais *Open Shortest Path First* – OSPF, *Routing Information Protocol, Next Generation* – RIPng, *Intermediate System to Intermediate System Routing Protocol* – ISIS e *Border Gateway Protocol* – BGP4+.

O IPv6 inclui ainda algumas extensões ao nível do encaminhamento bastante poderosas e úteis, nomeadamente encaminhamento com selecção de fornecedor de serviço, encaminhamento adaptado à mobilidade dos nodos e reendereçamento automático.

Um dos passos típicos para os utilizadores e administradores de redes IPv4 é a fase de atribuição/definição de um endereço IP para uma nova máquina a ligar à rede, e a sua configuração manual. Principalmente estando esta tarefa a cargo dos utilizadores, torna-se evidente a vulnerabilidade a erros/conflitos de endereços a que a rede fica sujeita.

Por forma a minimizar estes problemas, e ainda com o objectivo de tornar mais fácil e rápida a instalação de novas estações numa sub-rede IPv6, a especificação deste protocolo prevê um mecanismo de auto-configuração, o qual atribui automaticamente um endereço IP a cada interface que se liga à sub-rede, sem intervenção humana.

Apesar de parecerem evidentes os benefícios do IPv6 para o funcionamento futuro da Internet, é também claro que não é possível migrar da noite para o dia da actual Internet sobre IPv4 para uma rede completamente nova, a correr apenas IPv6.

Embora os problemas referidos anteriormente com o IPv4 sejam reais, prevê-se ainda uma vida relativamente longa a esta versão do protocolo IP, até se conseguir

realizar uma completa migração para o protocolo de nova geração.

Dado que não é algo que possa ser feito de um momento para o outro, definiram-se mecanismos que permitam estabelecer uma migração faseada e gradual, sem pôr em causa em algum momento o funcionamento actual da Rede [25, 26]:

- Sistemas de *Dual-Stack*: Este mecanismo baseia-se na existência em simultâneo de uma infraestrutura IPv4 e IPv6, onde os nodos terão de suportar simultaneamente uma pilha protocolar dupla.

  Um componente fundamental deste mecanismo é o sistema de DNS[7], já que é com base neste serviço que os nodos vão identificar qual das duas pilhas protocolares vão usar para comunicar com outro nodo. Em redes IPv4, o registo "A" do DNS associa um endereço IP a um nome. Um nodo com um endereço IPv6 terá um registo no DNS do tipo "AAAA" em vez do tradicional "A", o que permite assim aos sistemas identificar o tipo de pilha protocolar usada pelo nodo de destino.

- Túneis IPv6 sobre IPv4: Dado que não existe ainda uma rede nativa a correr IPv6 à escala mundial, uma alternativa para garantir conectividade entre nós IPv6 fisicamente afastados passa pelo estabelecimento de túneis IPv6 sobre a infraestrutura IPv4 instalada.

  Para o estabelecimento de um túnel IPv6 sobre IPv4 encapsula-se o pacote IPv6 num pacote IPv4, ou seja, coloca-se o primeiro no campo de dados do segundo, sem ser sujeito a análise intermédia, entre a origem IPv4 e o destino IPv4. É necessário, como é evidente, que a origem e o destino desse mesmo túnel sejam sistemas *Dual-Stack*. Assim, quando o pacote IPv4 atinge o destino, é analisado o campo de dados, "desencapsulado" o pacote IPv6 e processado de acordo com a sua pilha IPv6.

  Este tipo de túneis poderá ser estabelecido quer entre dois sistemas terminais, como entre um sistema terminal e um sistema intermediário, ou ainda entre dois sistemas intermediários.

A par de outros motivos referidos anteriormente, a falta de garantias de qualidade de serviço na versão quatro do protocolo IP foi um dos factores que motivaram o desenvolvimento de um novo protocolo de rede.

Neste sentido, foram definidos dois campos no cabeçalho inicial do pacote IPv6, com o objectivo de introduzir, no nível de rede, capacidade de controlar e fornecer diferentes níveis de Qualidade de Serviço (QoS), à medida da exigência de diferentes aplicações.

O primeiro campo (*Class Field*) permite definir classes de prioridade para os pacotes transmitidos. Este campo foi redefinido posteriormente à especificação do IPv6, tendo actualmente a designação de *Differentiated Services Field* (Campo DS) [32]. Esta alteração teve por objectivo adaptar o protocolo IPv6 (bem como o protocolo IPv4) ao suporte do modelo de Serviços Diferenciados (*DiffServ*).

O DiffServ é um modelo de fornecimento de Qualidade de Serviço em redes IP, que será abordado com mais detalhe em próximos capítulos deste trabalho.

[7] *Domain Name System*

O segundo campo do pacote IPv6 que tem funções relacionadas com a qualidade de serviço é o *Flow Label*. Este campo permite efectuar controlo de fluxo ao longo dos nós intermédios do percurso de um datagrama, facilitando nomeadamente o trabalho dos encaminhadores, através da aplicação simplificada do mesmo tratamento a todos os pacotes de um mesmo fluxo de dados.

A camada de Transporte

Como referido anteriormente, a camada de transporte da arquitectura TCP/IP tem por função principal a disponibilização de mecanismos de transferência de dados fim-a-fim.

Para o estabelecimento de uma ligação fim-a-fim entre duas aplicações, é necessário identificar de forma unívoca cada um dos processos associados. Quando essa comunicação se realiza em modo um-para-um na mesma máquina, este processo de identificação pode ser feito recorrendo aos identificadores de processos[8] implementados pelos Sistemas Operativos. No entanto, como esta forma de identificação não é uniforme (nomeadamente entre diferentes sistemas operativos), foi necessário desenvolver outro mecanismo padrão, a que se deu o nome de **porto**.

Assim, um porto identifica de maneira uniforme e única uma conexão entre programas e respectivos nodos associados, de forma independente dos PID's locais. Um porto é um número de 16 bits, usado pelos protocolos *host-to-host* para identificar que protocolo de nível superior ou que aplicação pretende estabelecer comunicação com outra.

Os dois protocolos que materializam esta camada são o UDP [48] e o TCP [49].

O protocolo UDP é basicamente uma interface de aplicação do IP, não adicionando fiabilidade, controlo de fluxo ou recuperação de erros a este. Simplesmente serve como um multiplexador/desmultiplexador para envio e recepção de datagramas, usando portos para os guiar.

O nível de actuação deste protocolo pode ser visto como extremamente leve, introduzindo pouco *overhead*. Em contrapartida, exige às aplicações a responsabilidade pela recuperação de erros, verificação da sequenciação, etc. Cada segmento UDP é enviado em simples datagramas IP, que podem ser fragmentados pelo nível IP, e posteriormente reassemblados no destino, antes de ser apresentados novamente ao nível UDP.

O TCP fornece às aplicações bastante mais facilidades que o UDP, nomeadamente recuperação de erros, controlo de fluxo e fiabilidade. É um protocolo orientado à conexão, ao contrário do UDP, que é não orientado à conexão.

O objectivo principal do protocolo TCP é fornecer um canal de comunicação lógico e fiável entre pares de processos. Isto é, não assume fiabilidade de comunicação nos protocolos de nível inferior (p. e. IP), procurando garanti-la ele próprio. É caracterizado pelas seguintes facilidades, que fornece às aplicações que o usam:

- Transferência de Sequências de Dados: do ponto de vista das aplicações, o TCP transfere sequências contínuas de bytes através da rede.

[8] vulgarmente conhecidos pela sigla PID, de *Process Identificator*

A aplicação não tem de se preocupar em agrupar os dados em blocos ou datagramas, já que o TCP realiza esta tarefa, agrupando os bytes a transferir em segmentos TCP, que são passados de seguida ao IP para serem transmitidos.

- Sequenciação: o TCP atribui um número de sequência a cada byte transmitido e espera uma confirmação positiva (*positive acknowledgement* - ACK) do nodo de destino.

  Se o ACK não é recebido durante um intervalo de *timeout*, os dados são retransmitidos. Se os dados forem transmitidos em blocos (segmentos TCP), é enviado apenas o número de sequência do primeiro byte de dados.

  O TCP de destino usa os números de sequência para reagrupar os segmentos, quando estes chegam fora de ordem, bem como para eliminar segmentos duplicados.

- Controlo de Fluxo: o TCP de destino, quando envia um ACK para a origem, indica também qual o número de bytes que pode receber a seguir, sem causar congestionamento dos seus *buffers*.

  A informação de controlo de fluxo é enviada no ACK, na forma do maior número de sequência que pode receber sem problemas. Este mecanismo é também conhecido como o princípio de Janela Deslizante.

- Multiplexagem: é fornecida recorrendo ao uso dos portos, da mesma forma que no UDP.

- Conexões lógicas: A sequenciação e o controlo de fluxo necessitam que o TCP inicialize e mantenha determinada informação de estado para cada sequência de dados.

  O conjunto desta informação, que inclui os *sockets* usados, números de sequência e tamanho das "janelas" é denominado conexão lógica. Cada conexão é identificada de forma unívoca por um par de sockets.

- *Full Duplex*: o TCP fornece transferência de sequências de dados, de forma concorrente, em ambas as direcções.

A camada de Aplicação

Na camada de aplicação da pilha TCP/IP estão definidos os protocolos de aplicação, que comunicam com outras aplicações em outros sistemas/nodos. Estes protocolos são, para os utilizadores, a face visível de toda a arquitectura.

Os protocolos de aplicação estão, na maior parte dos casos, directamente associados a aplicações, com as quais os utilizadores interagem directamente. Utilizam, normalmente, na camada de transporte, o protocolo TCP – *Transport Control Protocol* ou o protocolo UDP – *User Datagram Protocol*.

Entre os mais conhecidos destacam-se:

- TELNET: para acesso interactivo a terminais remotos;

- FTP – *File Transfer Protocol*: para transferência de ficheiros entre sistemas;
- SMTP – *Simple Mail Transfer Protocol*: sistema de transferência de mensagens de correio electrónico, através da Internet;
- POP3 – *Post Office Protocol, version 3* e IMAP4 – *Internet Message Access Protocol, version 4*: protocolos que permitem o acesso à caixa de correio electrónico de um utilizador.
- HTTP – *Hipertext Transfer Protocol*: sistema de transferência de páginas hipertexto;

2.2 Tecnologias de Comunicações

As redes de computadores são classificadas de acordo com vários critérios, que definem conjuntos comuns de características, de acordo com determinados parâmetros. Entre os critérios mais utilizados, encontram-se a topologia física e a área de cobertura.

A topologia física de uma rede define a forma de interligação física dos diferentes equipamentos. Entre as mais comuns temos:

- Topologia em Barramento: caracterizada pela existência de um único canal físico partilhado, que interliga todos os computadores de cada segmento de rede;
- Topologia em Estrela: constituída por um ponto central, ao qual cada nodo da rede é interligado, em ligações ponto-a-ponto;
- Topologia em Anel: os nodos da rede são interligados entre si por repetidores, em ligações unidireccionais ponto-a-ponto, num circuíto fechado;
- Topologia em Malha: o meio de transmissão é constituído por ligações arbitrárias ponto-a-ponto, entre os diferentes nodos da rede.

A classificação baseada no critério da área de cobertura diferencia as redes de computadores de acordo com a sua abrangência geográfica, recorrendo normalmente a três categorias: Redes de Área Local (LAN[9]), Redes de Área Metropolitana (MAN[10])e Redes de Área Alargada (WAN[11]).

Nas secções seguintes será feita uma breve apresentação de algumas das principais tecnologias de comunicações por computador usadas na actualidade e que estão pode detrás de alguns dos serviços descritos e implementados no âmbito do presente trabalho.

[9]Local Area Network
[10]Metropolitan Area Network
[11]Wide Area Network

2.2.1 Redes de Área Local

Uma rede de área local pode ser definida como sendo uma rede que cobre uma área geográfica limitada, com uma velocidade de transferência de dados relativamente alta (maior ou igual a 1 Mbps, de acordo com especificação do IEEE), com baixa taxa de erros e com administração privada.

Os meios físicos de transmissão mais comuns neste tipo de redes baseiam-se em sistemas de cablagem – cabos de cobre (cabo coaxial, cabo de pares entrançados – *unshielded twisted pair* - UTP, *shielded twisted pair* - STP) e cabos ópticos – e, mais recentemente, em meios de transmissão sem fios.

O controlo do meio físico de transmissão, embora variando de acordo com a tecnologia utilizada, baseia-se em duas técnicas principais [47]: *CSMA/CD*[12] e *passagem de testemunho* (*token*).

Tratando-se de uma técnica utilizada em redes com meio físico partilhado, o CSMA/CD tem o seguinte princípio de funcionamento:

1. Cada nodo ausculta continuamente o meio físico, para determinar, em tempo real, se está ou não ocupado;

2. quando um nodo pretende transmitir, se o meio está livre, transmite imediatamente, senão

3. se o meio físico está ocupado, continua a auscultá-lo até que este fique livre, e então transmite imediatamente;

4. se for detectada um colisão durante a transmissão, é emitido um breve sinal de interferência, reforçando essa mesma colisão, com o objectivo de todas as restantes estações se aperceberem da situação e cessarem as transmissões;

5. após a situação anterior, cada estação espera um intervalo de tempo aleatório, voltando de seguida ao ponto 1.

Apesar de, com técnicas deste tipo, a eficiência da rede ser negativamente influenciada pela ocorrência de colisões, o algoritmo CSMA/CD limita a capacidade desperdiçada ao tempo que demora a ser detectada uma colisão.

A técnica de passagem de testemunho resolve o problema das colisões com a introdução do conceito de *testemunho*. Apenas quem possuir este testemunho – trama de controlo, que circula circularmente de nodo em nodo – pode colocar dados no canal de comunicação, libertando-o de seguida para o nodo seguinte.

Este princípio de funcionamento implica uma topologia lógica em anel, podendo funcionar sobre topologias físicas do mesmo tipo ou, em alternativa, sobre topologias físicas em barramento (sendo criado o conceito de anel virtual, sobre o qual circula o testemunho).

Apesar de esta técnica assegurar uma eficiência superior relativamente ao CSMA/CD, introduz também um maior nível de complexidade nos nodos para, por um lado, estabelecer e manter em funcionamento o anel lógico e, por outro lado, permitir a admissão e retirada de novas estações na rede.

[12] *Carrier Sense Multiple Access with Collision Detection*

As principais tecnologias de área local têm vindo a ser normalizadas, ao longo dos tempos, pelo IEEE[13] e pela ISO[14].

Entre as mais importantes, destacam-se as tecnologias da família IEEE 802.3 (também conhecida por *Ethernet*) e variantes (IEEE 802.3u, IEEE 802.3z e IEEE 802.3ae). Nas últimas décadas tiveram também alguma divulgação as normas IEEE 802.4 –*Token Bus*, IEEE 802.5 –*Token Ring* e ISO 9314 – *FDDI*[15], mas entretanto foram caindo sucessivamente em desuso em detrimento das normas da família Ethernet.

IEEE 802.3 – Ethernet

A tecnologia de rede Ethernet foi desenvolvida inicialmente pela *Xerox*, durante a década de 70, com tradução posterior na norma IEEE 802.3, pelo IEEE.

A especificação original (IEEE 802.3) utiliza a técnica CSMA/CD como mecanismo de acesso ao meio. As redes iniciais desta categoria usavam topologia física em barramento com cabo coaxial (normas 10Base5 e 10Base2). tendo evoluído entretanto para topologias físicas em estrela com cabo de par entrançado UTP[16] (10BaseT) ou fibra óptica (10BaseFP, 10BaseFL e 10BaseFB).

A tecnologia de rede Ethernet atingiu uma enorme divulgação no mercado das redes locais, fruto da grande simplicidade de funcionamento (herdada do algoritmo de acesso ao meio CSMA/CD) e dos baixos custos de instalação e manutenção, comparativamente a outras tecnologias similares. Permite um débito de 10 Mbps em cada segmento de rede, o que era considerado suficiente para a grande maioria das necessidades das redes locais de à duas décadas atrás.

Entretanto, como estas necessidades foram aumentando, a própria Ethernet foi evoluindo, dando orígem a novas especificações com débitos superiores: 100 Mbps com a norma IEEE 802.3u, 1 Gbps com a norma IEEE 802.3z e mais recentemente 10 Gbps, com a norma IEEE 802.3ae.

IEEE 802.3u – Fast Ethernet

A norma IEEE 802.3u define uma tecnologia de rede local com um débito de 100 Mbps e compatível com as redes Ethernet de 10 Mbps, logo implementando o algoritmo CSMA/CD. Inclui ainda a possibilidade de auto-negociação do débito, entre 10 ou 100 Mbps, para além da capacidade de funcionamento em *full-duplex* [47].

Tal como as variantes Ethernet sobre cablagem 10BaseT e 10BaseF, pode funcionar sobre infra-estruturas comutadas. Um comutador trata a ligação de cada nodo como se se tratasse de um segmento Ethernet, garantindo assim um débito individual de 10 (Ethernet) ou 100 Mbps (Fast-Ethernet), através do encaminhamento das tramas apenas para a porta de saída respectiva.

Em oposição, com repetidores ou concentradores Ethernet, cada trama que chega a uma porta é enviada automaticamente para todas as restantes portas, obrigando

[13] *Institute of Electrical and Electronic Engineers*
[14] *International Standards Organization*
[15] *Fiber Distributed Data Interface*
[16] UTP: *Unshielded Twisted Pair*

assim à partilha da totalidade do débito fornecido pela globalidade dos nodos ligados a esse segmento.

Ao contrário da Ethernet, esta tecnologia não funciona sobre topologias físicas em barramento, limitando-se a topologias em estrela ou árvore. Utiliza para tal 3 tipos de cablagem:

- *100BaseTX*: cabos UTP, de categoria 5, dos quais utiliza dois pares, com conectores RJ45. Suporta o modo de funcionamento full-duplex.

- *100BaseT4*: cabos UTP de categoria 3 ou superior, utilizando 4 pares com conectores RJ45. Ao contrário do anterior, não suporta o modo full-duplex.

- *100BaseFX*: cabos de fibra óptica multimodo, com conectores ST ou SC nas extremidades. Suporta o funcionamento em full-duplex.

IEEE 802.3z – Gigabit Ethernet

A Gigabit Ethernet é, na prática, uma extensão do standard Ethernet IEEE 802.3.

Permite atingir débitos até 1000 Mbps, enquanto mantém compatibilidade com os dispositivos Ethernet e Fast Ethernet.

Com o mesmo formato de tramas que o usado nas redes IEEE 802.3, permite modos de operação *full-duplex* em ligações Comutador-Comutador e Comutador-Estação e modo *half-duplex* em ligações partilhadas com repetidores e CSMA/CD.

Embora inicialmente o objectivo fosse a utilização de apenas fibra óptica, actualmente pode ser implementada também sobre cablagem UTP Categoria 5 e Cabo coaxial [27]. Existem quatro tipos de meios físicos que podem ser utilizados com esta tecnologia:

- *1000Base-LX* (*Long Wavelength*): fibra óptica multimodo ou monomodo, utilizada tipicamente em ligações de *backbone* de *Campus* (*Switch-to-Switch*), até 5 Kms de distância (com fibra monomodo).

- *1000Base-SX* (*Short Wavelength*): fibra óptica multimodo normalmente utilizada em ligações de *backbone* de *Campus* e de edifícios (*Switch-to-Switch*). Permite distâncias até 220 metros, com fibra multimodo de 62,5 microns ou 550 metros com fibra multimodo de 50 microns.

- *1000Base-CX* (*Short Haul Copper*): cabo coaxial do tipo STP (*shielded twisted pair*), normalmente utilizado em ligações de alto débito em *clusters* de servidores e entre comutadores. Está limitado a um comprimento máximo de 25 metros por segmento.

- *1000Base-T* (*Long Haul Copper*): Cabo UTP de categoria 5e (ou superior), utilizado para ligações de alto débito entre estações e servidores a comutadores (comprimento máximo de cada segmento limitado a 100 metros). Esta variante permite o aproveitamento da vasta base instalada de cablagem estruturada utilizada nas redes Ethernet e Fast Ethernet.

A actualização das LAN's para a Gigabit Ethernet tem vindo a ser feita de forma gradual ao longo dos últimos 10 anos. Actualmente a principal utilização é feita a nível do backbone das redes e nas ligações dos servidores, sendo usada ainda em pequena escala nas ligações dos postos de trabalho.

IEEE 802.3ae - 10 Gigabit Ethernet

Em 2002 foi aprovada a variante mais recente da família de normas IEEE 802.3: IEEE 802.3ae, também conhecida por 10 Gigabit Ethernet (10GbE). Tal como o nome indicia, esta norma suporta débitos até 10 Gbps.

Foi originamente desenvolvida em torno de cablagem de fibra óptica, para a qual existem diversas variantes que diferem entre si no tipo de fibra óptica usada e nas distâncias máximas alcançadas: 10GBASE-LR (*Long Range*), 10GBASE-ER (*Extended Range*), 10GBASE-ZR e 10GBASE-SR (*Short Rage*).

Para ligações com base em cablagem de cobre, foram desenvolvidas duas variantes: 10GBASE-CX4 (cabo coaxial) e 10GBASE-T (802.3an), que usa cabo de par entrançado de categoria 6 (até 55 metros) ou categoria 6a (até 100 metros). Têm também vindo a ser normalizados interfaces específicos para interoperar com tecnologias de área alargada SDH/SONET.

Em função do custo actual dos componentes, a utilização desta norma nas redes de área local está actualmente ainda muito limitada ao backbone das redes de grande dimensão.

Se ao nível das redes locais a implantação do 10GbE ainda é insipiente, onde esta tecnologia tem vindo a assumir progressivamente um papel importante é nas redes de área metropolitana e alargada. Enquanto a Ethernet original permitia distâncias máximas até aos 2 Kms, a norma 10GbE suporta já distâncias que vão até aos 80 Kms, com a variante 10GBASE-ZR. Com estas características, esta norma está assim a entrar progressivamente em territórios que anteriormente eram dominados por tecnologias significativamente mais caras e complexas, como por exemplo o SDH/Sonet, assumindo hoje em dia boa parte do papel que se previa há alguns anos atrás para o ATM (uma mesma tecnologia para a LAN e a WAN).

Redes locais "sem fios"

As redes de área local sem fios (WLAN – *Wireless LAN's*) podem definir-se como redes com um alcance local, que utilizam o ar como meio de transmissão.

Por rede sem fios entendemos uma rede que utiliza ondas electromagnéticas como meio de transmissão da informação, através de uma canal que interliga os diferentes equipamentos móveis presentes na mesma. Estas ligações são normalmente implementadas através de tecnologias de microondas ou de infravermelhos.

Uma rede local sem fios é um sistema flexível de comunicações, que pode ser implementado como uma extensão ou directamente como uma alternativa a uma rede de cablagem guiada.

Este tipo de infraestruturas proporciona grande mobilidade aos utilizadores, sem perder conectividade. Outras vantagens encontram-se ao nível da facilidade de instalação e na economia associada à supressão dos meios de transmissão guiados.

As redes locais sem fios começaram a ser utilizadas há aproximadamente duas décadas, inicialmente em ambientes experimentais e de investigação.

Em março de 1985, a Comissão Federal de Comunicações Americana – FCC, (organismo com competências na área da regulação das telecomunicações nos Estados Unidos), atribuiu aos sistemas WLAN as gamas de frequência 902-928 Mhz, 2.400-2.4835 Ghz e 5.725-5.850 Ghz. Estas gamas de frequências, que ficaram conhecidas como bandas ISM – *Industrial, Científica e Médica*, podem ser utilizadas sem necessidade de licenciamento prévio por parte das entidades reguladoras.

As redes WLAN são suportadas por duas categorias base de tecnologias:

- Tecnologias de Rádio *Spread Spectrum*: a energia dos sinais é repartida de igual forma ao longo de toda a largura de banda disponível, em vez de a concentrar à volta de uma portadora concreta.

  Existem dois tipos de tecnologias de *Spread Spectrum*:

  - *Direct Sequence Spread Spectrum* – DSSS: distribui o sinal ao longo de toda a gama de frequência disponível, reorganizando posteriormente os pacotes no receptor.
  - *Frequency Hopping Spread Spectrum* – FHSS: envia segmentos curtos de dados que são transmitidos através de frequências específicas, controlando o fluxo com o receptor. Este negoceia velocidades menores, comparativamente às velocidades oferecidas pela técnica DSSS mas menos susceptíveis a interferências.

- Tecnologia de Infravermelhos: os sistemas de infravermelhos posicionam-se em altas frequências, imediatamente abaixo da faixa de frequências da luz visível.

  Assim, as propriedades dos infravermelhos são as mesmas da luz visível, o que faz com que estes não possam passar através de objectos opacos. Podem no entanto reflectir-se em determinadas superfícies.

  Esta tecnologia aplica-se tipicamente em ambientes interiores, para a criação de ligações ponto-a-ponto de curto alcance.

O grau de complexidade de uma rede local sem fios é variável, dependendo das necessidades a satisfazer. O equivalente sem fios a um segmento de rede guiada é a célula. Estas células são designadas por BSA – *Basic Service Area*, dependendo o seu tamanho das características do ambiente e da potência dos transmissores/receptores usados nas estações.

Entre as topologias mais comuns, destacam-se as seguintes:

- Redes sem infra-estrutura (*ad-hoc*): correspondem à topologia mais simples, sendo constituídas por um conjunto de equipamentos terminais móveis, equipados com uma placa adaptadora sem fios.

  Para a comunicação ser possível, é necessário que todas as estações estejam no raio de cobertura radioeléctrica umas das outras. Trata-se de redes muito simples de implementar e que não requerem grandes recursos de administração.

- Extensão das células básicas: Para aumentar o alcance de uma rede do tipo anterior, torna-se necessário instalar um Ponto de Acesso – AP (*Access Point*).

  Os Pontos de Acesso são estações especiais, responsáveis pela captura das transmissões realizadas pelas estações da sua célula, destinadas a estações localizadas em outras células, e retransmitindo-as através de um sistema de distribuição. Com este novo elemento a distância máxima permitida deixa de ser entre estações, passando a ser a distância entre cada estação e o AP.

  Ao mesmo tempo, os pontos de acesso podem ser interligados a outras redes, nomeadamente a redes fixas, às quais o utilizador móvel passa a poder ter acesso.

  Para fornecer cobertura a zonas maiores, torna-se necessário instalar mais pontos de acesso. A ligeira sobreposição das diferentes células de cobertura vai permitir também o deslocamento dos utilizadores móveis ao longo de toda essa área sem perder conectividade.

- Interligação entre duas ou mais LAN: Esta opção permite a interligação de diferentes LAN's (por exemplo de edifícios separados, etc) usando redes sem fios.

  Neste caso, as soluções mais simples passam pela instalação de uma antena direccional em cada extremo, apontando-se mutuamente. Ao mesmo tempo, cada uma destas antenas está ligada à rede local do seu lado, através de um AP.

  Em situações mais complexas, são utilizadas, hoje em dia, antenas omnidireccionais ligadas a encaminhadores (que substituem os AP), que por sua vez se ligam às respectivas redes locais. Desta forma é possível extender o conceito de Redes Locais Sem Fios para Redes Metropolitanas Sem Fios, que interligam redes locais à escala de uma cidade, por exemplo.

Durante a década de 90, o IETF iniciou um processo de normalização deste tipo de tecnologias, que se têm traduzido, ao longo da última década, numa sucessão de normas da família IEEE 802.11.

A primeira surgiu em 1997, quando o IEEE rectificou a norma **IEEE 802.11** [51]. Esta norma veio estabelecer um ponto de referência para a implementação deste tipo de redes ao nível da arquitectura dos níveis físico e de ligação de dados.

Tal como os restantes protocolos IEEE 802x, também esta norma intervém ao nível das camadas mais baixas do Modelo OSI, com especificações para os níveis Físico e de *Medium Access Control* - MAC (figura 2.1).

As restantes camadas mantém-se semelhantes às definidas para as LAN's da família IEEE 802, nomeadamente a sub-camada superior do nível lógico (*IEEE 802.2 Logical Link Control - LLC*), a estrutura de endereçamento de 48 bits e todos os níveis superiores até à camada de aplicação.

No nível físico são tratadas apenas as transmissões com radiofrequência (RF) e por infravermelho (IR). Na prática, apenas as transmissões por radiofrequência são utilizadas, com recurso às técnicas DSSS ou FHSS.

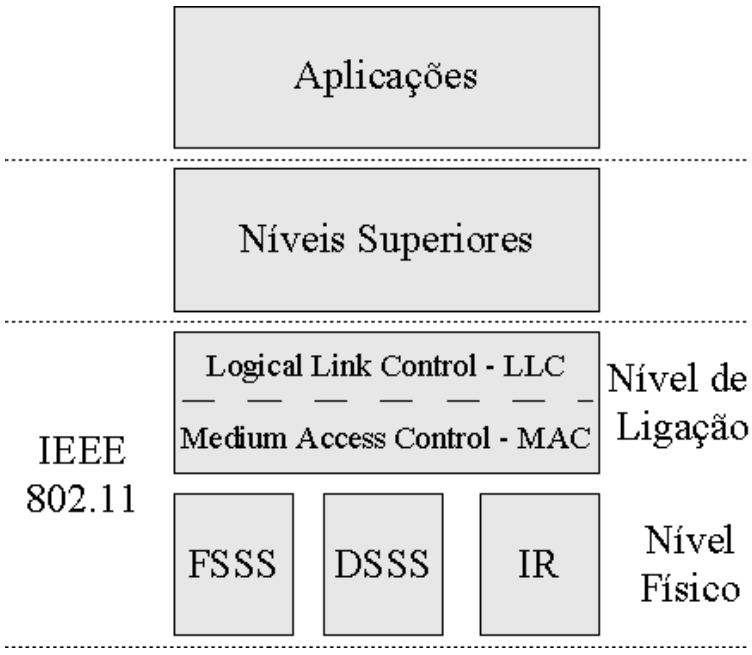

Figura 2.1: Arquitectura protocolar 802.11

O algoritmo básico de acesso ao nível MAC é semelhante ao CSMA/CD implementado na norma IEEE 802.3, sendo aqui designado por CSMA/CA - *Carrier Sense Multiple Access with Collision Avoidance*.

O IEEE 802.11 especifica uma taxa de transmissão entre 1 e 2 Mbps. Opera na banda de frequências 2.400-2.4835 GHz, podendo funcionar com FHSS ou DSSS. Numa rede IEEE 802.11 típica, as estações sem fios (designadas STA) associam-se a Pontos de Acesso (AP), que por sua vez actuam como uma espécie de pontes para a rede de cabos. A combinação de um AP com as STA's associadas designa-se por *Basic Service Set* - BSS. Cada rede sem fios é identificada univocamente por um *Service Set Identifier* - SSID. O SSID é um número de 32 bits que é adicionado ao cabeçalho dos pacotes que circulam na WLAN, funcionando também como método básico de autenticação dos clientes perante um Ponto de Acesso.

Em 1999, o IEEE apresentou uma versão melhorada da norma IEEE 802.11, que designou **IEEE 802.11b**. Esta versão, que especifica taxas de transmissão de 1 Mbps, 2 Mbps, 5.5 Mbps e 11 Mbps, trouxe um novo fôlego a este tipo de redes, traduzido numa crescente aceitação do mercado. Uma parte significativa das WLAN usadas actualmente ainda são baseadas nesta norma.

Funciona na mesma banda de frequências do IEEE 802.11 (2.400-2.4835 GHz), usando neste caso apenas DSSS, já que a técnica FHSS não suporta velocidades acima dos 2 Mbps sem violar as disposições da FCC. Neste sentido, o IEEE 802.11b apenas mantém compatibilidade com sistemas da norma IEEE 802.11 que utilizam DSSS.

O intervalo de frequências referido é dividido em canais (13 nos países que adoptam as especificações do ETSI), apenas se podendo utilizar 3 num mesmo espaço físico, com um intervalo de 5 canais entre cada um.

Em espaço aberto, é possível estabelecer ligações a 11 Mbps até 300 a 400 metros

de distância, sem antenas de ganho adicionais. Em espaço fechado, esta distância diminui para 30 a 50 metros, dependendo das condições do local. Para suportar distâncias superiores ou ambientes com maior influência de ruído, esta norma utiliza degradação dinâmica do débito. Quando um terminal se afasta do alcance óptimo do Ponto de Acesso, a norma degrada a transmissão para velocidades inferiores, primeiro para 5.5 Mbps, 2 Mbps e por último 1 Mbps. Quando o terminal se aproxima, verifica-se o processo inverso.

A norma **IEEE 802.11a** foi aprovada aproximadamente na mesma altura da norma IEEE 802.11b, em Dezembro de 1999. Trata-se de mais uma evolução da norma IEEE 802.11 mas com uma diferença fundamental em relação a esta: opera na banda de frequências dos 5 GHz. Suporta débitos até 54 Mbps para distâncias até 50 metros, com valores intermédios para 6, 12, 18, 24, 36 e 48 Mbps.

Ao nível físico, esta norma usa *Orthogonal Frequency Division Multiplexing* - OFDM, já abordado anteriormente.

A banda de frequências dos 5 GHz é, na generalidade, actualmente ainda muito menos utilizada que a banda dos 2.4 GHz. Por um lado este aspecto apresenta-se como uma vantagem para o IEEE 802.11a, já que a probabilidade de ocorrência de interferências com outros equipamentos a operar na mesma gama de frequências diminui substancialmente. No entanto, por outro lado acaba por se traduzir também numa desvantagem, dada a falta de regulamentação que ainda existe em muitos países para a utilização deste espaço do espectro electromagnético.

Enquanto na banda de frequências dos 2.4 GHz apenas podemos ter 3 canais sobrepostos, o IEEE 802.11a suporta até 12 canais simultâneos, permitindo assim o aumento da largura de banda disponível para os utilizadores, através do incremento de Pontos de Acesso com células sobrepostas. O número real de canais disponíveis para utilização varia de país para país.

Os equipamentos IEEE802.11a não são directamente compatíveis com equipamentos das normas antecessoras (IEEE 802.11 e IEEE 802.11b), por dois motivos: a)funcionamento em bandas de frequências diferentes; b) utilizam diferentes tecnologias de *spread spectrum*. O IEEE 802.11a funciona com OFDM enquanto as outras duas normas funcionam com FHSS ou DSSS.

Apesar destas condicionantes, existe interoperabilidade entre os equipamentos das três normas ao nível MAC, já que todas utilizam, a este nível, o algoritmo CSMA/CA da especificação original do IEEE 802.11.

A norma **IEEE 802.11g** foi rectificada em 2003, tendo este desfecho sido aguardado com imensa expectativa pelo mercado. Percebe-se facilmente porquê: O IEEE 802.11g prometia uma performance comparável ao IEEE 802.11a, com débitos de até 54 Mbps, enquanto mantém compatibilidade retroactiva com a norma IEEE 802.11b. Há quem compare esta combinação de performance e compatibilidade retroactiva com a evolução da Ethernet de 10 Mbps para os 100 Mbps da norma Fast-Ethernet, nas Redes Locais.

Esta norma opera na mesma banda de frequências do IEEE 802.11b (2.4 GHz), estando igualmente limitada ao máximo de três canais sobrepostos.

Um dos requisitos obrigatórios nesta norma é a total compatibilidade com o IEEE 802.11b, sendo visto como um importante factor de protecção de investimento para a base instalada. Por outro lado, tal como o IEEE 802.11a, utiliza OFDM

para a transmissão de dados a débitos mais elevados. Quando entra em modo de compatibilidade com a norma IEEE 802.11b, passa automaticamente a utilizar DSSS.

A maior parte das WLAN actuais são baseadas nesta norma. Entretanto, encontra-se actualmente em processo de normalização a próxima evolução desta família de tecnologias, denominada *IEEE 802.11n*. Espera-se para breve a sua aprovação definitiva, prometendo débitos numa primeira fase de até 100 Mbps.

2.2.2 Redes de Área Alargada

As redes de área alargada (WAN) fornecem serviços de interligação à escala de uma região, país ou do próprio planeta.

Fornecem tipicamente débitos inferiores aos das tecnologias utilizadas nas redes de área local e metropolitana. Em muitos casos, as WAN são usadas para ligar diferentes LAN e MAN entre si.

Circuitos Alugados

Dada a sua cobertura, a Rede Pública Telefónica Comutada (*Public Switched Telephonic Network – PSTN*) tem um grande peso nas comunicações de dados, a nível mundial.

Tratando-se de uma tecnologia pensada para o suporte de comunicações de voz, apresenta uma limitação fundamental na transmissão de dados: a largura de banda máxima está limitada a 3400 Hz. Sendo suficiente para a transmissão de sinais de voz, impõe um limite de aproximadamente 56000 bps na transmissão de dados [47].

A utilização da PSTN na transmissão de sinais digitais obriga ao recurso de modems (moduladores/desmoduladores), para a conversão dos sinais analógicos em sinais digitais e vice-versa.

Esta rede funciona de acordo com a técnica de multiplexagem de circuitos, onde um novo circuito é estabelecido no início de cada chamada, e explicitamente terminado no final da mesma.

Para além deste tipo de funcionamento, é também possível a utilização da infraestrutura da PSTN para suporte de circuitos permanentes entre dois pontos, também conhecidos por Circuitos Alugados. Estes circuitos têm a vantagem de não precisarem de uma fase prévia de estabelecimento da ligação, já que esta está permanentemente estabelecida.

Podem ainda ser retirados os dispositivos de limitação da largura de banda existentes nos circuitos telefónicos comutados, permitindo assim o suporte de débitos superiores.

Com a digitalização da PSTN, é actualmente possível o aluguer de circuitos digitais baseados nesta infraestrutura. Estes permitem débitos superiores aos circuitos analógicos, tipicamente em valores múltiplos de 64 Kbps, ao mesmo tempo que apresentam taxas de erros mais baixas.

Circuitos de Multiplexagem Plesiócrona

A multiplexagem plesiócrona – ou seja, parcialmente síncrona – corresponde à aplicação da técnica TDM – *Time Division Multiplexing* na multiplexagem de sinais digitais. Esta tecnologia é tambem conhecida por PDH – *Plesiochronous Digital Hierarchy*.

A operação de multiplexagem plesiócrona permite um melhor aproveitamento dos meios de transmissão, através da agregação de canais de comunicação em diferentes níveis.

Existem actualmente duas grandes hierarquias de agrupamento dos canais que diferem, quer no débito de cada canal, quer no número de canais agrupados em cada nível [47]:

- Hierarquia de multiplexagem Europeia:

Nível	Nº de canais de 64 Kbps	Débito binário
E1 fraccional	n < 30	n x 64 Kbps
E1	30	2.048 Mbps
E2	120	8.448 Mbps
E3	480	34.368 Mbps
E4	1920	139.264 Mbps
E5	7680	564.148 Mbps

- Hierarquia de multiplexagem Americana:

Nível	Nº de canais de 56 Kbps	Débito binário
T1 fraccional	n < 24	n x 56 Kbps
T1	24	1.544 Mbps
T2	96	6.312 Mbps
T3	672	44.736 Mbps
T4	4032	274.16 Mbps

X.25

O X.25 corresponde a uma recomendação da ITU-T, sendo utilizado como meio de comunicação de dados através de redes telefónicas com infraestruturas analógicas, tipicamente caracterizadas pela baixa qualidade dos meios de transmissão e pela alta taxa de erros. Permite a criação de redes de comutação de pacotes, tipicamente utilizadas em ambiente WAN.

A recomendação X.25 é, na realidade, um conjunto de protocolos, enquadrados nos três primeiros níveis protocolares do modelo OSI.

No nível mais baixo – camada física – a norma X.21 define a interface entre o DTE e o DCE fornecido pelo operador de telecomunicações. O DCE tem um papel semelhante a um modem síncrono, uma vez que a sua função é disponibilizar um caminho de transmissão síncrono, série, *full-duplex* entre o DTE e o PSE[17]. Pode operar a velocidades entre 600 bps e os 64 kbps.

[17]PSE – *Packet-Switching Exchange*

A camada de ligação de dados utiliza uma variante simplificada (modo ABM) do protocolo HDLC[18] conhecida por LAPB – *Link Access Protocol – Balanced*. Tem como função disponibilizar um mecanismo fiável (sem erros e sem pacotes repetidos) de transporte através da ligação física entre o DTE e o PSE.

Esta camada não tem qualquer conhecimento do canal lógico a que determinado pacote pertence – esta é uma das responsabilidades da camada superior. Os procedimentos de controlo de fluxo e de processamento de erros aplicam-se, portanto, a todos os pacotes independentemente do canal lógico.

A camada de rede (também conhecida por camada de pacote) tem a responsabilidade de transportar o TPDU e multiplexar um ou mais canais virtuais (ligações) numa única ligação física controlada pela camada de ligação. Fornece transferência fiável de pacotes X.25, fim-a-fim.

A tecnologia X.25 teve uma grande implantação até aos anos noventa, fruto das características herdadas das técnicas de comutação de pacotes.

Entretanto, com o desenvolvimento do *Frame Relay*, o X.25 entrou em decréscimo de utilização, limitando-se actualmente a alguns tipos de ligações mais específicas. Um dos factores deste decréscimo tem a ver com a elevada sobrecarga introduzida na rede, pelas múltiplas funções de controlo das diferentes camadas protocolares, traduzida em limitações no débito disponível.

Frame Relay

O Frame Relay surgiu a partir de um movimento do mesmo grupo de normalização que deu lugar ao X.25 – a ITU. Como referido anteriormente, o X.25 apresenta limitações importantes, originadas pela sobrecarga introduzida pelos mecanismos de controlo de erros e de fluxo, em todos os saltos da rede.

Um dos objectivos iniciais do Frame Relay foi eliminar estas limitações do X.25, reduzindo comparativamente de forma significativa os mecanismos de controlo, nos comutadores intermédios da rede.

Enquanto o X.25 foi "desenhado" para funcionar sobre infraestruturas analógicas, o Frame Relay, pelo contrário foi desenvolvido tendo em vista a sua utilização em meios de cumunicação digitais.

Neste sentido, enquanto no primeiro se justificavam os complexos mecanismos de controlo de erros e de fluxo entre cada dois nodos da rede, dadas as características da infraestrutura, o Frame Relay já podia abdicar de boa parte dos mesmos, dada a maior qualidade (tecnologia digital) dos meios de transmissão.

O Frame Relay é definido como um serviço portador RDIS[19] de banda estreita, em modo de pacotes, tendo sido especialmente adaptado para velocidades de 64 Kbps até 2,048 Mbps (embora nada impeça que estas sejam superadas).

Proporciona conexões entre utilizadores através de uma rede pública. O uso de conexões implica que os nodos da rede sejam comutadores, por onde as tramas são transmitidas, de forma ordenada (já que todas seguem o mesmo caminho), até ao destino.

[18] HDLC – *High-Level Data Link Control*
[19] Rede Digital com Integração de Serviços

No caso do X.25, a multiplexagem de circuitos virtuais é efectuada na camada de pacote (rede) enquanto que a camada de trama (ligação) efectua apenas o tratamento de erros e controlo de fluxo local. Este facto leva a que o processamento de tramas no comutador público seja efectuado ao nível da camada de pacote, o que introduz mais sobrecarga no processamento.

No Frame Relay, as funções de encaminhamento e de multiplexagem são efectuadas ao nível da camada de ligação (trama). Este facto tem como consequência uma taxa útil de transmissão superior, o que levou este protocolo, apesar de ser desenvolvido no âmbito da tecnologia RDIS, a descobrir um mercado próprio.

As redes Frame Relay são constituídas por dois tipos de equipamentos:

- FRAD – *Frame Relay Assembler/Disassembler*: equipamento do utilizador, que empacota as tramas dos protocolos de nível superior em tramas Frame Relay;
- FRND – *Frame Relay Network Device*: faz a comutação das tramas Frame Relay, em função do identificador de conexão, através da rota estabelecida.

O FRAD é também responsável pelo controlo de fluxo e de erros, em modo fim-a-fim.

A rede encarrega-se apenas da transmissão e comutação dos dados, bem como de indicar qual o estado dos recursos. Em caso de erros ou saturação dos nodos intermédios da rede, os equipamentos do utilizador – FRAD – solicitam o reenvio (ao outro extremo) das tramas incorrectas e, se necessário, reduzirão a velocidade de transmissão, para evitar congestão.

Ao nível da camada de ligação de dados, o Frame Relay utiliza uma variante do protocolo HDLC, designada LAPF – *Link Access Procedure for Frame-Mode*.

As redes Frame Relay são orientadas à conexão, sendo cada conexão identificada pelo identificador DLCI – *Data Link Connection Identifier*.

Para além do DLCI, existem outros três campos com especial relevância, no cabeçalho das tramas deste protocolo:

- DE – *Discard Elegibility*: este bit é usado para identificar tramas que podem ser descartadas pela rede, em caso de congestão;
- FECN – *Forward Explicit Congestion Notification*: é usado para enviar uma notificação de congestão dirigida ao destino;
- BECN – *Backward Explicit Congestion Notification*: usado para enviar uma notificação de congestão dirigida à origem.

Rede Digital com Integração de Serviços - RDIS

A Rede Digital com Integração de Serviços surgiu como uma evolução das redes telefónicas tradicionais.

Originalmente, todo o sistema telefónico se baseava em comunicação analógica. Com o desenvolvimento das centrais digitais, a comunicação entre estas passou a usar tecnologia digital.

A RDIS surgiu assim como o elemento que faltava para o fornecimento de comunicação telefónica digital extremo-a-extremo, acrescentando, simultaneamente, um conjunto alargado de serviços adicionais.

O processo de padronização foi iniciado pelo CCITT[20] (actualmente ITU) em 1984, com a Recomendação I.120.

Esta tecnologia oferece um grande número de vantagens quando comparada com a rede telefónica tradicional, nomeadamente:

- Velocidade: O débito de dados teórico actual obtido com uma linha telefónica analógica situa-se nos 56 Kbps (norma V.90), embora a velocidade real seja normalmente inferior, em função das condições da linha. A RDIS oferece múltiplos canais digitais, que podem operar simultaneamente através da mesma conexão telefónica entre a central e o utilizador. Assim, com um Acesso Básico RDIS (serviço mais comum para os utilizadores finais) é possível agregar dois canais, obtendo um débito máximo de 128 Kbps.

  Adicionalmente, o tempo de estabelecimento de uma chamada é bastante mais reduzido em linhas RDIS do que em linhas com sinal analógico.

- Ligação de múltiplos dispositivos: As linhas telefónicas analógicas só podem ser utilizadas por um único dispositivo de cada vez. Por outro lado, cada tipo de equipamento, normalmente tem a si associado um tipo de interface de ligação à rede especifico.

  Com a RDIS é possível combinar diferentes fontes de dados digitais simultaneamente, ao mesmo tempo que as próprias normas desta tecnologia especificam um conjunto de serviços, fornecidos através de interfaces normalizados.

- Sinalização: Nas linhas telefónicas analógicas, a sinalização é efectuada no mesmo canal em que circulam os dados. Isto faz com que o período de estabelecimento de uma chamada seja relativamente longo.

  Numa ligação RDIS, a sinalização é efectuada por um canal independente dos canais de dados (canal D), tornando o processo de estabelecimento de uma chamada extremamente rápido.

- Serviços: A RDIS não se limita a oferecer comunicações de voz. Oferece muitos outros serviços, como transmissão de dados, fax, videoconferência, acesso à Internet, além de opções como chamada em espera, identificação da origem, etc.

A RDIS dispõe de três tipos distintos de canais de transmissão:

- Canal B: transmitem informação a uma velocidade de 64 Kbps, utilizados para transportar tanto dados de voz como dados informáticos. De acordo com [28], a velocidade de 64 Kbps, permite enviar dados de voz sobre linhas digitais, com qualidade telefónica. Estes canais não transportam informação de controlo da RDIS. Servem também como base para qualquer outro tipo de canais de dados de maior capacidade, que se obtêm por combinação de canais do tipo B.

[20]CCITT – *Telefone and Telegraph Consultative Committee*

- Canal D: utilizados para envio de informação de controlo, podendo também transportar dados, em situações especiais em que não são usados na primeira função. Funcionam a 16 Kbps ou 64 Kbps, dependendo do tipo de serviço contratado.

- Canais H: são obtidos através da agregação de vários canais B, transportando dados do utilizador. Os mais usados são os seguintes:

  - Canais H0: funcionam a 384 Kbps, com a agregação de 6 canais B;
  - Canais H10: funcionam a 1472 Kbps, com a agregação de 23 canais B;
  - Canais H11: funcionam a 1536 Kbps, com a agregação de 24 canais B;
  - Canais H12: funcionam a 1920 Kbps, com a agregação de 30 canais B;

A tecnologia RDIS é disponibilizada em dois tipos de serviços:

- Acesso Básico (BRI – *Basic Rate Interface*): disponibiliza dois canais B e um canal D de 16 Kbps. Tem como principais alvos os utilizadores individuais e o mercado SOHO[21].

- Acesso Primário (PRI – *Primary Rate Interface*): disponibiliza 23 canais B e um canal D de 64 Kbps (o que dá um débito total de 1536 Kbps), nos Estados Unidos da América. Na Europa, é constituído por 30 canais B e um canal D de 64 Kbps, disponibilizando um débito total de 1984 Kbps. Destina-se tipicamente a utilizadores empresariais e institucionais.

O nível físico da RDIS está especificado nas normas I.420 e I.431 da ITU.

Este nível fornece os serviços de transmissão dos canais B, D e H, bem como um sistema de sinalização e temporização para acesso ao canal D. Especificam-se ainda nestas normas os interfaces eléctricos utilizados nas linhas RDIS.

Ao nível de ligação de dados, a tecnologia RDIS utiliza um subconjunto do protocolo HDLC, designado por protocolo LAPD – *Link Access Protocol - D Channel*. A sua principal função é transmitir as mensagens de nível superior, entre os equipamentos do utilizador e a central telefónica, necessárias ao estabelecimento de uma chamada. Com esta chamada estabelece-se também um circuito virtual através da rede, entre o utilizador de origem e o de destino.

Fruto das vantagens referidas, comparativamente às linhas telefónicas analógicas, a RDIS tem vindo a traçar um percurso de lenta, mas segura afirmação, fundamentalmente junto dos consumidores empresariais.

Hierarquia Digital Síncrona – SDH e Rede Óptica Síncrona – SONET

Com as tecnologias de multiplexagem plesiócronas (PDH), o acesso directo a sinais de um nível inferior não é possível, a partir de um qualquer nível superior da hierarquia, já que cada nível transporta os inferiores de forma transparente. A partir

[21]SOHO: *Small Office, Home Office*

de um determinado nível, não é possível distinguir, nos níveis inferiores, os bits de sincronização dos bits de carga.

Assim, o acesso aos sinais de determinado nível só é possível após a desmultiplexagem sucessiva até esse mesmo nível.

A tecnologia SDH, sendo considerada uma evolução da tecnologia PDH, permite o acesso directo a todos os níveis da hierarquia sem necessidade de desmultiplexagem, já que torna visível, para qualquer nível, a informação de controlo e de carga dos inferiores.

Nesta tecnologia, os canais são transportados em quadros síncronos com uma duração fixa de 125 μs, cada um deles com uma parte de informação de controlo e outra de carga.

A SDH é uma tecnologia normalizada pelo ITU-T, encontrando-se definida nas recomendações G.707, G.708 e G.709. Teve a sua origem na tecnologia SONET – *Synchronous Optical Network*, desenvolvida inicialmente pela *Bellcore* e posteriormente normalizada pela ANSI.

Trata-se de duas tecnologias de transmissão (posicionando-se ao nível físico) que fornecem mecanismos para comunicação a longas distâncias, em alta velocidade.

Tal como com os Circuitos de multiplexagem plesiócrona, também as tecnologias SONET/SDH se estruturam numa hierarquia baseada em níveis.

Na tecnologia SDH, os níveis são designados STM-n – *Synchronous Transport Module* (o n identifica o nível). Na SONET, os níveis são designados OC-n (*Optical Carrier* de nível n).

SONET OC-n	SDH STM-n	Débito binário (Mbps)
OC-1	–	51.48
OC-3	STM-1	155.52
OC-9	–	466.56
OC-12	STM-4	622.08
OC-18	–	933.12
OC-24	–	1244.16
OC-36	–	1866.24
OC-48	STM-16	2488.32
OC-192	STM-64	9953.28
OC-768	STM-256	39813.12
OC-3072	STM-1024	159252.24

A utilização destas tecnologias tem actualmente especial relevo no transporte de grandes volumes de tráfego, nos *backbones* dos operadores de telecomunicações. Efectuam assim o transporte de uma grande variedade de sinais tributários, incluindo tráfego das hierarquias plesiócronas, ATM, canais de vídeo, etc.

Com a evolução da Ethernet para a variante 10GbE e o consequente aumento da área de abrangência deste tipo de tecnologias no sentido das redes WAN, têm vindo a ser desenvolvidos esforços no sentido de fomentar a interoperabilidade entre as duas tecnologias.

A iniciativa *Ethernet over SDH* (EoS) visa definir um conjunto de normas para transporte de tráfego Ethernet sobre infra-estruturas SDH (ou SONET). A norma

ITU-T G.7041 define a técnica de multiplexagem *Generic Framing Procedure* (GFP), que pode ser usada para este objectivo.

Wavelength Division Multiplexing – WDM

A transmissão de dados sobre fibras ópticas usa, tradicionalmente, técnicas de multiplexagem por divisão de tempo (TDM), com a transmissão a ser feita num determinado comprimento de onda. As tecnologias mais recentes desta área permitem a obtenção de débitos até 159,252 Gbps (OC-3072).

Recentemente tem vindo a ser desenvolvida uma nova tecnologia baseada em multiplexagem por divisão de frequência, denominada *Wavelength Division Multiplexing* – WDM.

O WDM permite a transmissão de informação em múltiplos comprimentos de onda (logo múltiplos canais separados), numa mesma fibra, o que permite uma grande expansão na capacidade das redes ópticas existentes. Enquanto os primeiros sistemas WDM usavam apenas dois comprimentos de onda (1310 nm e 1550 nm) os últimos desenvolvimentos tecnológicos em amplificadores ópticos e de lasers permitem a instalação de sistemas com 16, 32 ou 40 comprimentos de onda numa mesma fibra. Estes últimos são conhecidos por sistemas DWDM – *Dense Wavelength Division Multiplexing*, dada a densidade de canais que se conseguem estabelecer em cada fibra.

A combinação das técnicas TDM e DWDM permite a obtenção de débitos da ordem dos 400 Gbps por fibra óptica.

Modo de Transferência Assíncrono – ATM

Até alguns anos atrás, as redes eram planeadas e instaladas com o objectivo de transportar tipos específicos de tráfego. As redes telefónicas destinavam-se, primariamente, ao transporte de tráfego de voz. As redes de televisão efectuavam apenas o transporte do sinal de televisão. Os operadores de redes de dados instalavam redes com suporte para apenas este tipo de tráfego.

Assim, se um operador actuasse simultaneamente em mais do que uma destas áreas, teria de planear e gerir paralelamente várias infraestruturas de rede distintas.

Deste problema surgiu um esforço conjunto de várias entidades internacionais ligadas às telecomunicações e às redes de computadores, com o objectivo de criar uma nova tecnologia que suportasse simultaneamente o transporte de diferentes tipos de tráfego (voz, vídeo, dados, etc).

O resultado deste esforço ficou traduzido no desenvolvimento da tecnologia ATM, caracterizada pela capacidade de suportar todos os tipos de tráfego e pela capacidade de aplicação indistinta em ambientes de rede de área local, metropolitana ou alargada.

A tecnologia ATM é semelhante, em termos de conceitos, ao Frame Relay. Tal como este, também o ATM teve origem nos trabalhos de desenvolvimento da RDIS (neste caso da RDIS de Banda Larga – B-ISDN). As suas principais especificações foram desenvolvidas pelo ITU-T, ATM Forum e pelo IETF.

O ATM permite, tal como o X.25 e o Frame Relay, o suporte de múltiplas ligações lógicas, sobre a mesma ligação física.

A informação que circula em cada ligação lógica é organizada em pacotes de dimensão fixa (53 octetos: 5 octetos com informação de controlo e 48 octetos para transporte dos dados) denominados **células**.

A dimensão fixa da célula permite simplificar os mecanismos de comutação. Ao mesmo tempo, o facto de a célula ter um tamanho reduzido permite garantir um atraso aceitável para a transmissão de voz ou vídeo em movimento. Por outras palavras, significa que pode ser emulado um circuito.

Ao nível físico, o ATM é independente do meio de transmissão utilizado, podendo as células ser transportadas sobre os mais variados meios, entre os quais redes SDH/SONET.

A arquitectura desta tecnologia identifica duas camadas relacionadas com funções ATM:

- Camada ATM: define o formato da célula e a metodologia seguida na transmissão de células sobre a rede;
- Camada de Adaptação – AAL: especifica como as células são usadas por forma a criar ligações adequadas ao tipo de serviço (transporte de voz, transmissão de dados, fluxo contínuo de dados, etc.). Divide-se em cinco níveis distintos:
  - AAL 1: Bit Rate Constante; Orientado à Conexão;
  - AAL 2: Bit Rate Variável; Orientado à Conexão;
  - AAL 3/4: Bit Rate Variável; Orientado (ou Não-orientado) à Conexão;
  - AAL 5: Bit Rate Variável; Orientado à Conexão.

O endereço dos intervenientes na comunicação é definido apenas quando a ligação é efectuada. As ligações numa rede ATM são criadas como caminhos virtuais (VP – *Virtual Path*). Estes, por sua vez, são decompostos em secções denominadas ligações de canal virtual (VC – *Virtual Circuit*). Os vários canais e caminhos definidos no início da ligação são identificados por números no cabeçalho das células de ligações activas. Cada número é denominado identificador de canal virtual (VCI – *Virtual Channel Identifier*) e identificador de caminho virtual (VPI – *Virtual Path Identifier*).

Uma das vantagens do ATM, comparativamente a outras tecnologias de transmissão, está nos mecanismos de qualidade de serviço que suporta.

A implementação de diferentes níveis de qualidade de serviço é feita com recurso a quatro classes de serviço de utilizador: Classe A, B, C e D. Estas resultam da combinação de diversas possibilidades para parâmetros [47], como sejam o atraso na transferência de células (CTD – *Cell Transfer Delay*), taxa de perda de células (CLR – *Cell Loss Ratio*), taxa de erro de células (CER – *Cell Error Ratio*) e variação no atraso de células (CDV – *Cell Delay Variation*).

As classes de serviço de utilizador têm suporte em níveis específicos da camada AAL do ATM. Assim, a classe A é suportada pelo AAL1, a classe B pelo AAL2 e as classes C e D pelos AAL3/4 ou AAL5.

Dado que a camada AAL existe apenas nos sistemas terminais, as especificações do ATM definem um conjunto de categorias de serviço, na camada ATM, para

assegurar uma distribuição adequada dos recursos de rede pelos diferentes fluxos de tráfego.

As categorias de serviço são caracterizadas em termos de padrões de tráfego, dos requisitos de QoS e dos mecanismos de controlo.

Categorias de Serviço do ATM, definidas pelo *ATM Forum*:

- *Constant Bit Rate* – CBR: categoria de serviço para tráfego de débito constante, com requisitos de qualidade de serviço bastante rígidos;

  Destinada a aplicações de voz, vídeo de débito constante e serviços de emulação de circuitos.

- *Real-time Variable Bit Rate* – rt-VBR: para tráfego de tempo real e débito variável, como, por exemplo, tráfego de vídeo codificado.

- *Non-real-time Variable Bit Rate* – nrt-VBR: para tráfego de débito variável sem requisitos temporais.

- *Available Bit Rate* – ABR: para suporte de aplicações não sensíveis a variações da largura de banda disponível.

- *Unspecified Bit Rate* – UBR: para suporte de aplicações não críticas, funcionando em modo de *best effort*; Não são dadas quaisquer garantias em termos de qualidade de serviço.

O ATM foi desenvolvido com o objectivo de se tornar, a prazo, um tecnologia universal, usada nas LAN's, MAN's e WAN's. Com o decorrer do tempo, tem-se vindo a constatar que, em parte, este objectivo inicial não foi cumprido. Se ao nível das redes WAN dos operadores o ATM se tornou a tecnologia de eleição, ao nível das redes locais foram as sucessivas evoluções da Ethernet que vingaram e dominam hoje em dia este tipo de redes.

Um dos factores que contribuiu para esta realidade foi a complexidade da tecnologia ATM, quando comparada com a Ethernet. Enquanto esta funciona em modo não orientado à conexão, o ATM é uma tecnologia orientada à conexão, o que levou à necessidade de desenvolvimento de mecanismos complementares, como o stantard LANE (*LAN Emulation*), para ser possível a emulação de um ambiente LAN típico (Ethernet ou Token Ring, p.e.), sobre uma rede ATM.

Também o transporte de pacotes IP em redes ATM não é directo, dados os seus modos de operação opostos. Foram desenvolvidas duas formas básicas de transportar IP sobre ATM:

- Encapsulamento: é adicionado um cabeçalho de nível de ligação de dados (com 8 bytes de comprimento) aos pacotes IP, sendo o conjunto transportado em unidades de serviço de dados AAL 5.

- Resolução de Endereços: utiliza o modelo clássico das redes IP, baseado nos conceitos de sub-rede e de servidores ARP, a que se dá o nome *Classical IP over ATM* – CLIP, definido no RFC 1577.

De acordo com o CLIP, os nodos IP são agrupados em sub-redes lógicas IP (*Logical IP Subnets* – LIS). A comunicação entre LIS é efectuada através de encaminhadores.

Cada LIS tem o seu servidor ARP, designado servidor ATMARP, que faz o mapeamento entre endereços IP e endereços ATM.

2.3 A Voz sobre IP - *VoIP*

2.3.1 Da telefonia tradicional à Voz sobre IP

Durante muitas décadas, as infra-estruturas de comunicação de voz e as infra-estruturas de comunicação de dados foram consideradas dois mundos opostos. Com a evolução das tecnologias de comunicação e dos protocolos de suporte da Internet, considera-se actualmente que já é possível aquilo que há 15 anos atrás não passava de uma miragem: transportar voz em tempo real através das infra-estruturas que suportam esta rede.

Após uma fase inicial de alguma indiferença, os fabricantes tradicionais de equipamentos para redes de voz têm vindo progressivamente a acompanhar a tendência, incluindo, no seu portfólio actual, ofertas completas de soluções de voz baseadas em protocolos da família TCP/IP.

O termo **Voz sobre IP** [67] refere-se a serviços de comunicações - voz ou fax - que são transportados através de redes baseadas na arquitectura TCP/IP, em vez do transporte através da rede PSTN. Os passos básicos envolvidos neste processo passam pela conversão da voz analógica para sinais digitais, com subsequente compressão e colocação desses sinais em datagramas IP, para poderem ser transportados através da rede até ao outro extremo da comunicação. Neste, efectua-se o processo inverso, obtendo-se como resultado novamente a voz analógica.

O termo Telefonia IP é normalmente utilizado quando se adicionam novos serviços ao transporte da voz, como voicemail integrado com o e-mail, chamadas em espera, conferência, vídeo-conferência, música para clientes em espera, etc.

O serviço de Telefonia IP é baseado num conjunto de componentes, que interagem entre si:

- Terminal: componente de terminação de uma comunicação. Pode ser um componente de software (soft-phone) que funciona num computador ou de hardware (hard-phone), podendo funcionar neste caso autonomamente.

- Servidor: Um servidor actua como um agente intermédio, com o objectivo de facilitar o processo de estabelecimento de uma comunicação entre dois terminais. Tipicamente, quando um terminal se liga à rede, regista-se junto de um servidor. Desta forma, torna-se mais fácil o processo de comunicação com outros terminais, já que o servidor mantém a informação da localização de todos os terminais ligados à rede. Este componente desempenha normalmente também funções de autenticação, autorização e contabilização.

- Gateway: componente que permite a comunicação entre terminais que usam tecnologias diferentes entre si. Permite, por exemplo, a comunicação de um

terminal SIP para H.323 ou PSTN, e/ou vice-versa.

Entre os protocolos mais importantes para o suporte deste serviço sobre redes de dados destacam-se: o RTP - *Real Time Protocol* [1], que permite a sequenciação, identificação de payloads e sincronização de streams; a norma H.323 da ITU e o protocolo de sinalização SIP - *Session Initialization Protocol* [62], do IETF.

2.3.2 Compressão e codificação digital da voz

O processo de digitalização dos sinais de voz analógica implementado nas redes TDM tradicionais é baseado na técnica *Pulse Code Modulation* (PCM), que produz um output digital de 64 Kbps. Trata-se de um débito relativamente baixo para a generalidade das redes de área local actuais, não podendo ser já hoje em dia também considerado elevado para algumas redes de acesso (ADSL, Cabo) e de área alargada. Apesar de tudo, para este tipo de serviços de tempo real, mais importante que o débito em si, são aspectos como o atraso e a variação do atraso entre os sistemas finais da comunicação, a taxa de perdas, etc.

Apesar de a Voz sobre IP poder ser transmitida sem compressão (taxa de 64 Kbps), têm vindo a ser desenvolvidos um conjunto de algoritmos que minimizam a largura de banda necessária, através da compressão dos sinais, supressão dos períodos de silêncio, etc. Estes algoritmos têm também como objectivo codificar os sinais de voz num determinado formato, pelo que são conhecidos por *codecs*. Trata-se de uma área em continuo desenvolvimento, apresentando-se de seguida, a título de exemplo, alguns dos codecs actualmente em uso em serviços VoIP:

- G723.1: oferece um nível relativamente elevado de compressão, com um bit rate de saída entre os 5,3 e os 6,4 Kbps e um atraso fim-a-fim de aproximadamente 135 ms. Cada pacote transporta 30 ms de sinal de voz, com um tamanho entre os 20 e os 24 bytes. A sua utilização está dependente de licenciamento prévio, em determinadas situações de utilização;

- G.729 e G.729a: apresenta um bit rate resultante da compressão de 8 Kbps, com 10 ms de voz em cada pacote. Cada um destes ocupa 10 bytes, fornecendo um atraso fim-a-fim de aproximadamente 50 ms. Também a utilização deste codec necessita de licenciamento;

- G.711 (PCM): protocolo de codificação de voz sem compressão, que produz um bit rate de 64 Kbps, com a transmissão de 50 ou 33 pacotes por segundo e intervalos de 20 ou 30 ms de voz em cada um. Existem actualmente duas variantes: *ulaw* usada nos Estados Unidos da América e *alaw*, usada na Europa.

- iLBC (*Internet Low Bitrate Codec*): codec de utilização livre que fornece um bit rate relativamente baixo, ideal para funcionamento em situações de escassez de largura de banda. Trata-se de um codec com boa capacidade de adaptação a situações de perdas de pacotes. Fornece um bit rate de 13,33 ou 15,2 Kbps, em função do tamanho do pacote de dados (50 bytes ou 38 bytes).

De salientar que a contabilização dos requisitos de largura de banda para estes codecs tem de incluir, para além do bit rate definido para cada um deles, os *overheads* de todos os encapsulamentos sofridos pelos dados aplicacionais, nomeadamente, cabeçalhos dos pacotes RTP, UDP e IP e do PDU da camada de ligação de dados.

2.3.3 A Norma H.323

Em 1996, a ITU aprovou o conjunto de normas H.323, que definem o modo como o tráfego de voz, vídeo e dados em tempo real podem ser transportados através de redes baseadas no protocolo IP. Esta recomendação recorre, para o trasporte dos sinais de áudio e vídeo, aos protocolos *Real Time Protocol* - RTP e *Real Time Control Protocol* - RCTP.

O H.323 é usado para o estabelecimento de chamadas e negociação de capacidade. Um outro elemento que faz parte da norma - Q.931 - faz a sinalização de chamada entre os elementos do serviço. O mecanismo RAS H.323 (*Registration, Admission, Status*), materializado na norma H.225.0, disponibiliza funcionalidades de resolução dinâmica de endereços IP.

Os componentes fundamentais de uma rede H.323 são:

- Terminais de Rede Corporativa: terminais para utilização em LAN's, com suporte de som de alta qualidade e múltiplas funções;
- Terminais Internet: optimizados para funcionamento num ambiente de largura de banda mínima;
- Gateways: fornecem interligação entre terminais H.323 ligados a redes IP e outros dispositivos de áudio (por exemplo telefones normais) ligados a outras redes;
- Gatekeepers: implementam funções de servidores de directório e de controlo;
- MCU - Multipoint Control Unit's: fornecem serviços de gestão de conferências multiponto.

  As normas H.323 disponibilizam um conjunto exaustivo de especificações detalhadas, que permitem uma implementação completa de serviços de comunicação multimédia. Fruto deste nível de detalhe, é actualmente considerada uma alternativa "pesada", para a implementação de serviços de Telefonia IP. Em consequência, o protocolo SIP, abordado a seguir, tem vindo a conquistar uma fatia importante deste mercado, reposicionando-se actualmente o H.323 como melhor opção mais ao nível específico dos serviços de vídeo-conferência.

2.3.4 O Protocolo SIP

O protocolo SIP (*Session Initiation Protocol*) [62] foi desenvolvido no seio do IETF, com o objectivo de permitir o estabelecimento, alteração e terminação de sessões multimédia com um ou mais participantes.

Trata-se de um protocolo de sinalização fim-a-fim, que é usado apenas para tornar o processo de comunicação possível. A comunicação em si mesma, depois

de estabelecida, terá de usar outro(s) protocolo(s) para efectuar o transporte da informação entre a origem e o destino. Entre os mais importantes, destacam-se:

- RTP (*Real Time Protocol*): usado para transportar a informação multimédia através da rede IP;
- SDP (*Session Description Protocol*): usado para descrever as capacidades, ao nível dos codecs usados e outros parâmetros, dos participantes na comunicação.

Ao contrário do H.323, o SIP é um protocolo desenhado à imagem da generalidade dos protocolos da Internet, sendo caracterizado pela simplicidade, facilidade de implementação, boa escalabilidade e flexibilidade. Apresenta assim um princípio de funcionamento semelhante ao do protocolo HTTP, usado pelo serviço da *World Wide Web*. Entre outras semelhanças, destaca-se o formato das mensagens (de texto, baseadas no RFC 822), trocadas entre os agentes intervenientes na comunicação. Também a identificação dos extremos da comunicação é baseada num *Uniform Resource Identifier* (SIP URI), neste caso com um formato do tipo *username@domínio* (semelhante a um endereço de correio electrónico).

Uma rede SIP simples pode ser constituída por apenas dois agentes terminais, com a troca de mensagens directa entre eles. No entanto, na maior parte dos casos, uma rede SIP é constituída por um número mais alargado de elementos, dos quais se destacam:

- *User Agent*, residente em cada terminal SIP:
  - *User Agent Client* - UAC: responsável por despoletar pedidos SIP;
  - *User Agent Server* - UAS: responsável por receber e responder a pedidos SIP.
- *Network Server*: disponibiliza funções avançadas, como registo (função de *Registrar*), autenticação, autorização e contabilização. Pode actuar também como servidor *Proxy*, para o encaminhamento de pedidos de estabelecimento de sessões para um determinado destinatário. Um Servidor Proxy pode actuar em modo *stateless*, onde funciona como simples reencaminhador de mensagens, ou em modo *stateful*, mantendo neste caso a informação de estado ao longo de toda uma comunicação.

À semelhança do protocolo HTTP, também as mensagens SIP trocadas entre dois agentes são baseadas na invocação de funções denominadas **métodos** (neste caso métodos SIP). Apresentam-se de seguida os principais métodos definidos na especificação do protocolo:

- REGISTER: Utilizado no login para registar o cliente no servidor;
- INVITE: Mensagem enviada para iniciar uma chamada;
- ACK: Confirmação de um INVITE pelo receptor final da mensagem;
- CANCEL: Aborta o inicio de uma chamada;

- BYE: Termina uma chamada;
- OPTIONS: interroga o servidor por opções neste;
- REFER: Usado para transferência de chamadas;
- MESSAGE: Permite a implementação de mecanismos de comunicação de *Instant Messaging*;
- SUBSCRIBE / NOTIFY: Implementa um mecanismo de presença.

Em jeito de conclusão, podemos afirmar que o H.323 representa o "Mundo Antigo" das redes telefónicas TDM, por ser complexo, determinístico e vertical. Ao ser focalizado em aplicações multimédia, preocupa-se em especificar todos os parâmetros da comunicação, centralizando a complexidade no servidor.

Ao contrário, o SIP representa o "Novo Mundo" das telecomunicações sobre redes IP. Trata-se de um protocolo da família dos protocolos Internet, simples, aberto e horizontal.

Actualmente nota-se um crescente movimento de adesão ao protocolo SIP, por parte de fabricantes, "novos" operadores de VoIP, mundo académico, etc. Prevê-se assim que este protocolo venha a adquirir, durante os próximos anos, um estatuto no mundo da Telefonia IP semelhante ao que actualmente usufrui o protocolo HTTP ao nível do serviço WWW.

2.3.5 Considerações de segurança

A integração de um serviço de voz na rede de dados de uma instituição levanta questões de segurança importantes, que importa analisar atentamente. Entre os aspectos mais relevantes, segundo [3], destacam-se:

- desenvolvimento de uma arquitectura de rede adequada, com separação lógica das redes de voz e dados, quer a nível dois, com utilização de diferentes VLAN, quer a nível três, com a utilização de diferentes sub-redes IP.
- assegurar que a instituição analisou e consegue gerir os riscos para a informação que circula na rede e para os sistemas e consegue manter a continuidade das operações essenciais em situações de ataque. Deve ser dada especial atenção à disponibilidade dos serviços de emergência (número 112).
- se as comunicações de voz não utilizarem cifragem no transporte da informação, o acesso ao meio físico pode ser crítico em termos de escuta das conversações. Igualmente importante é a segurança dos sistemas de suporte ao serviço, como gateways, proxys, etc.
- deve-se proceder a uma avaliação das necessidades de dispositivos de alimentação eléctrica de backup, que assegurem a continuidade do serviço durante quebras de energia.
- deve ser disponibilizado um cuidado especial à implementação/configuração de firewalls e outros mecanismos de protecção específicos para o tráfego VOIP.

- deve ser dada uma especial atenção à regulamentação nacional relacionada com as comunicações de voz.

Por forma a minimizar o impacto das questões da segurança na operacionalidade de uma rede VoIP, o planeamento actual destas infra-estruturas contempla normalmente um componente denominado *Session Border Controller* (SBC). Trata-se de um equipamento que actua na fronteira da rede VoIP, controlando todos os pedidos de comunicação entre essa mesma rede VoIP interna e o exterior e vice-versa.

Capítulo 3

Qualidade de Serviço em Redes de IP

3.1 A necessidade de Qualidade de Serviço

O protocolo IP permitiu a criação de uma rede global de comunicações, baseada numa grande variedade de sistemas e meios de transmissão.

À volta do mundo a troca de correio electrónico e a navegação na *World Wide Web* são actualmente parte do dia-a-dia, no trabalho, estudo e entretenimento.

De acordo com as tendências mais recentes, outras redes - telefone (fixo e móvel), rádio e televisão - estão também a convergir para o protocolo IP, por forma a tirar partido da sua enorme capacidade e flexibilidade.

Com estas novas redes, chegam novas aplicações e novos utilizadores, não existindo sinais de abrandamento, nos tempos mais próximos, do incrível crescimento da mais importante rede baseada neste protocolo - a Internet.

Uma razão para o tremendo sucesso do protocolo IP é a sua simplicidade. O princípio fundamental que esteve na base do seu desenvolvimetno derivou do "argumento fim-a-fim"[1] [40], segundo o qual a complexidade fica do lado dos sistemas finais, mantendo-se a rede relativamente simples.

No entanto, os encaminhadores que se situam nos pontos de interligação das redes têm de fazer algo mais do que simplesmente analisar o endereço IP de destino nas tabelas de encaminhamento, para determinar o próximo salto de um datagrama IP. Se a fila para o próximo salto é longa, os datagramas podem ser atrasados. Se esta está cheia ou indisponível, um encaminhador IP é "autorizado" a descartar datagramas.

O resultado é traduzido no fornecimento de um serviço, por parte do IP, baseado no "melhor esforço"[2], que está sujeito a atrasos imprevisíveis e perda de dados.

Com o contínuo crescimento da Internet, o IP tem vindo gradualmente a denunciar as suas principais fraquezas.

Aumentar a largura de banda disponível para evitar o congestionamento das ligações da Internet é a solução mais óbvia. No entanto, o problema é mais complexo

[1] *end-to-end argument*
[2] Princípio do *best-effort*

do que uma mera questão de capacidade. A questão é que o tráfego não cresceu apenas em volume, mas também se alterou na sua natureza.

Existem actualmente várias novas aplicações baseadas no IP, com grandes diferenças de requisitos operacionais.

Alguns dos novos tipos de aplicações da Internet são multimédia, que requerem quantidades significativas de largura de banda. Outras têm necessidades específicas de sincronismo, funções de um-para-muitos ou muitos-para-muitos (*multicast*). Estas requerem serviços de rede para além do simples serviço baseado no "melhor esforço" que oferece o protocolo IP.

Na prática, estas novas aplicações precisam que as actuais redes IP ganhem alguma "inteligência". Um exemplo concreto é a Voz sobre IP - VoIP[3], que é actualmente considerada uma "*killer application*". Mais do que qualquer outra, o desejo de oferecer serviço telefónico através da Internet guia a convergência entre as indústrias do Telefone e da Internet.

Embora parecendo interessante à partida, os princípios de funcionamento do telefone são exactamente opostos dos que estão por detrás das redes IP. Enquanto o IP usa comutação de pacotes e oferece serviços com base no "melhor esforço", as redes telefónicas usam comutação de circuitos (comunicação orientada à conexão), para fornecer os serviços previstos.

Diferentes aplicações de rede têm diferentes requisitos operacionais, que por sua vez requerem diferentes serviços de rede.

Incrementos no tráfego da rede requerem incrementos na largura de banda, mas novas aplicações, como a Voz sobre IP, têm também outros requisitos, para os quais o aumento da capacidade da rede não é a única resposta. É assim necessário identificar esses requisitos e desenvolver mecanismos que assegurem a sua conformidade, dentro de parâmetros aceitáveis.

3.2 A Convergência para o Protocolo IP

Nas redes de dados, a convergência para o IP é hoje em dia um "facto consumado". Para as redes de rádio e televisão, a convergência com o IP já começou, mas ainda com um longo caminho a percorrer. Em primeiro lugar, precisam de mais largura de banda.

Os meios de difusão actuais servem milhões de clientes simultaneamente, podendo encaixar-se no modelo do *IP multicast*, com comunicação um–para–muitos. Só assim será possível trazer estas redes de massas para a Internet, já que aqui a comunicação *unicast* nunca poderá escalar a estes níveis.

Chega-se assim à conclusão de que é necessário mais desenvolvimento na tecnologia *multicast*, para ser possível a convergência destas redes para o mundo IP.

O valor acrescentado que estas redes podem oferecer às aplicações de áudio/vídeo é enorme, abrindo novas dimensões aos conteúdos multimédia. Podem incluir hiperligações web, ou simultaneamente enviar ficheiros, slides ou outros conteúdos, durante a transmissão, para enriquecer a emissão.

[3]do inglês *Voice over IP*

As redes IP vão permitir que estas comunicações se estabeleçam nos dois sentidos, onde os destinatários dos conteúdos podem interagir e dialogar com os fornecedores.

Como o *multicast* permite aos receptores comunicar com outros receptores (isto é, muitos-para-muitos) abre-se a porta para um conjunto de novas possibilidades de aplicação (grupos de discussão, ensino à distância interactivo, jogos em grupo, etc).

No entanto, antes deste tremendo potencial poder ser completamente utilizado, existem outros requisitos dos serviços de rede a serem satisfeitos, em adição ao *multicast*.

Como referido anteriormente, a Voz sobre IP (VoIP) é actualmente uma das principais "*Killer Applications*".

A pressão do mercado para desenvolver tecnologias de VoIP fez muito para expôr as deficiências do serviço IP, tendo empurrado para a frente a definição de normas e o desenvolvimento de mecanismos de gestão de largura de banda.

Apesar de se tratar de uma aplicação multimédia (áudio), os seus requisitos de largura de banda são relativamente modestos (abaixo de 8 Kbps com alguns codecs), logo a largura de banda não é a questão. No entanto a latência já é uma questão a resolver. Para o VoIP – e outras aplicações de tempo real ou *two–way* – os requisitos de tempo são muito mais importantes que os requisitos de largura de banda.

Neste serviço, há uma pessoa de cada lado da conversação que têm evidência imediata e óbvia da qualidade da chamada – ou falta dela. Atrasos médios acima dos 300 milisegundos podem tornar o serviço inutilizável.

O consumidor actual padrão para este tipo de serviço é a telefonia móvel. Qualquer pessoa que tenha usado este serviço, sabe que não é perfeito. Ruído e chamadas perdidas não são totalmente incomuns. Por outro lado, a latência nunca foi um problema limitativo do desenvolvimento deste serviço.

Assim, apesar destes defeitos, o serviço de telefonia móvel é considerado bastante melhor do que o que é possível utilizando o serviço "best–effort" do IP, através da Internet. Esta comparação ilustra o impacto na usuabilidade que os atrasos no tráfego representam.

A indústria das telecomunicações começou com uma aplicação específica (telefonia) e construiu uma rede para a suportar. A Internet, por outro lado, começou exactamente da forma oposta: começou com uma nova tecnologia de rede e explorou, com sucesso, novas aplicações que têm capacidade para usar um serviço indiferenciado ("*best–effort*").

Aumentar a largura de banda melhorará o serviço prestado pelo protocolo IP, portanto este é um primeiro passo, essencial para resolver a questão da latência. No entanto não é suficiente para satisfazer os requisitos das novas aplicações multimédia e de tempo real que emergem actualmente na Internet.

3.3 Diferentes alternativas

A largura de banda é a capacidade de transportar dados pela rede, sendo o recurso através do qual mais comodamente se medem as capacidades das redes.

Trata-se de uma medida de quantos bits elementares de informação a rede pode transportar de um nodo para outro, em unidades de tempo (segundos) e em

condições ideais. Infelizmente, muitas redes operam em condições distantes do ideal.

Em termos de capacidade consistente de largura de banda entre dois nodos, a Internet também está longe de uma situação ideal, sendo considerada a rede das redes, formada por uma mistura de vários meios de transmissão com grandes diferenças de largura de banda e de latência.

O estado de uma ligação entre dois nodos através da Internet pode variar muito de um milisegundo para o próximo. O tráfego das aplicações da rede é caracterizado por um comportamento "*bursty*" onde, com muitas aplicações a partilhar as mesmas ligações ao mesmo tempo, o resultado traduz-se em congestão. Esta causa atrasos na entrega ou perda de dados.

Este comportamento não é problema crítico para aplicações tolerantes ao atraso (isto é, "elásticas"), como é o caso do correio electrónico ou mesmo da transferência de ficheiros e a navegação web.

No entanto, os atrasos podem ser fatais para aplicações *mission–critical*, ou limitam de forma significativa a utilização de aplicações de tempo real.

O crescimento da Internet significa mais nodos, redes, utilizadores e aplicações. Ao mesmo tempo, as necessidades de largura de banda da Internet estão sempre a crescer.

Aumentar de forma drástica a capacidade das redes é uma necessidade, não um luxo. Afortunadamente, as Leis de Moore ajudam neste objectivo, promovendo (indirectamente) novas e cada vez mais rápidas tecnologias de largura de banda para WAN's, MAN's e LAN's.

A propósito disto, Andrew S. Grove, *Chairman* da Intel afirmou: "*se está espantado com a rápida descida do custo do poder de computação ao longo da última década, espere até ver o que vai acontecer ao custo da largura de banda*".

A questão não é que largura de banda estará disponível, mas que tecnologias estarão. Existem várias em vários estágios de desenvolvimento, sendo as mais excitantes de todas as ligadas à transmissão óptica.

Os protocolos actuais de grande largura de banda incluem ATM, 10-Gigabit Ethernet, SDH/SONET, DWDM e xDSL. O objectivo está na disponibilização e na comercialização destas tecnologias junto das empresas e dos consumidores particulares, algo que acontece lentamente.

Desde que o mundo da comunicações se começou a mover cada vez mais em direcção ao protocolo IP, a interoperabilidade entre este e as tecnologias de comunicações de alta velocidade é ainda mais necessária.

O IP é independente dos meios de transmissão, logo tipicamente isso não é um problema. De qualquer modo, as características operacionais de alguns meios não se encaixam bem nos mecanismos do IP.

Por exemplo, as comunicações por satélite são frequentemente "*one-way*" e alguns protocolos – como o TCP – funcionam de forma "*two-way*". Mesmo quando o satélite tem um canal de retorno, pode ser assimétrico.

O facto dos satélites proporcionarem largura de banda muito elevada, em conjunto com alta latência, levanta questões a serem tratadas. Por outro lado, uma vantagem significativa das comunicações por satélite é o perfeito suporte para o multicast IP.

Outra tecnologia que teve significativa importância nas últimas duas décadas

foi o ATM (*Asynchronous Transfer Mode*). O ATM desempenha ainda um papel importante na espinha dorsal das redes telefónicas, devido aos seus mecanismos de qualidade de serviço (QoS). Alocando recursos para o circuito virtual aquando da inicialização de uma ligação, que se vão manter reservados enquanto esta durar, o ATM pode satisfazer os requisitos de tempo real de uma conversação telefónica.

A arquitectura de circuito virtual do ATM está em perfeito contraste com o desenho "*packet-switched*" do IP.

Em adição às células ATM de 53 bytes, o facto deste protocolo se posicionar ao nível da ligação de dados enquanto o IP é um protocolo de rede, acentua as questões relacionadas com a compatibilidade entre ambos.

Afortunadamente, o trabalho para assegurar que o IP possa operar sobre redes ATM está feito, tendo provado funcionar bem. O serviço ABR (*Available Bit Rate*) do ATM é actualmente considerado para fornecer um serviço similar ao "melhor esforço" do IP.

Uma popular *t-shirt* de engenheiros do IETF[4] dizia: "*IP: necessary and sufficient*". A implicação óbvia é que outros protocolos de rede são supérfluos, e o serviço de melhor esforço do IP pode satisfazer todos os requisitos aplicacionais.

Isto é verdade se assumirmos que a largura de banda da rede é suficiente para evitar atrasos ou datagramas descartados. Mas como os utilizadores habituais da Internet sabem, os atrasos na rede são ocorrências comuns.

O tráfego Internet cresce porporcionalmente à largura de banda disponível, logo os atrasos são inevitáveis. Adicionalmente, há alturas em que o tráfego cresce temporariamente para posições extraordinárias e imprevisíveis, por vários motivos, normalmente imprevistos. Nestes instantes ocorre congestão, que afecta drasticamente partes da Internet. Quando isto acontece, o melhor esforço do IP fornece níveis de serviço uniformes a todos os utilizadores – níveis de serviço uniformemente maus.

A solução óbvia para ultrapassar estes períodos de pico é o sobre-dimensionamento das redes. Isto permitiria fornecer largura de banda "de sobra", em antecipação às taxas de pico, durante períodos de grande procura. Igualmente óbvio, no entanto, é o facto desta solução não ser economicamente viável – pelo menos com as tecnologias e infra-estruturas actuais. Mesmo que as taxas de pico e as regiões onde estes picos de congestão podem ocorrer sejam possíveis de ser determinadas, esta não é uma alternativa realista.

O IP e a largura de banda são necessários, mas ambos não são suficientes para todas as necessidades aplicacionais, em todas as condições. São assim necessários mecanismos adicionais, que permitam disponibilizar serviços de rede às aplicações com diferentes níveis de Qualidade de Serviço.

3.4 Definição de Qualidade de Serviço (QoS)

De acordo com [41], Qualidade de Serviço (QoS) "*é a capacidade que um elemento de rede (uma aplicação, nodo final ou encaminhador) tem para fornecer algum nível de garantia de que os requisitos de tráfego e de serviço são satisfeitos*".

[4] *Internet Engineering Task Force*

Disponibilizar QoS basicamente significa proporcionar garantias de transmissão para certos fluxos de dados. De acordo com [42], estas garantias de transmissão podem ser expressas através da combinação de diferentes parâmetros, nomeadamente:

- Atraso: é o tempo necessário para um pacote ser transportado, do emissor, através da rede, até ao receptor. Quanto maior for o atraso, maiores são os problemas causados ao bom funcionamento dos protocolos de transporte, como o TCP.
- Variação do Atraso (*jitter*): é a variação do atraso fim-a-fim. Mesmo com níveis de atraso dentro de limites aceitáveis, variações acentuadas deste podem ter efeitos negativos na qualidade do serviço disponibilizado a algumas aplicações.
- Largura de Banda: é a taxa de transmissão de dados máxima que pode ser sustentada entre dois pontos finais. Para além dos limites físicos (dependentes da tecnologia utilizada), a largura de banda é também limitada pela quantidade de fluxos que partilham a utilização de determinados componentes da rede.
- Confiabilidade: tratando-se de uma propriedade dos sistemas de transmissão, pode ser vista como a taxa de erros do meio físico.

Embora seja um conceito muito relativo, um serviço com qualidade pode ser visto genericamente como aquele que garante baixo atraso e variação de atraso, grande quantidade de largura de banda e elevada confiabilidade.

3.5 Mecanismos de condicionamento e controlo de tráfego

O melhor esforço do IP não consegue fornecer continuamente um bom serviço, nem mesmo um serviço aceitável para sempre. Mesmo numa rede IP relativamente folgada, os atrasos podem ter uma variação suficiente para afectar de forma adversa aplicações com requisitos de tempo real.

Para fornecer garantias de serviço – algum nível de garantia quantificável – os serviços IP têm de ser complementados. Isto requer a adição de algumas funcionalidades à rede, para poder **diferenciar** tráfego e activar diferentes níveis de serviço para diferentes utilizadores e aplicações.

Por outras palavras, as redes IP precisam de mecanismos de gestão activa da largura de banda. Significa isto que é necessário encontrar formas adequadas de repartição dos recursos de um canal de transmissão, quando a quantidade de informação a transmitir excede a capacidade máxima desse canal.

Na prática, é necessário interferir na gestão dos *buffers* que armazenam temporariamente os pacotes de informação, antes destes serem transmitidos pelo interface determinado, nos encaminhadores da rede.

A gestão destes dispositivos de armazenamento temporário pode ser feita recorrendo a mecanismos de gestão de filas de espera onde, no caso mais simples, um *buffer* corresponde a uma única fila.

Nas redes IP baseadas no serviço *best-effort*, a gestão destes *buffers* é efectuada de acordo com a técnica FIFO[5]. Tal como o nome sugere, os primeiros pacotes a chegar à fila são os primeiros a ser transmitidos pelo canal de saída, logo que exista disponibilidade de recursos para tal (figura 3.1).

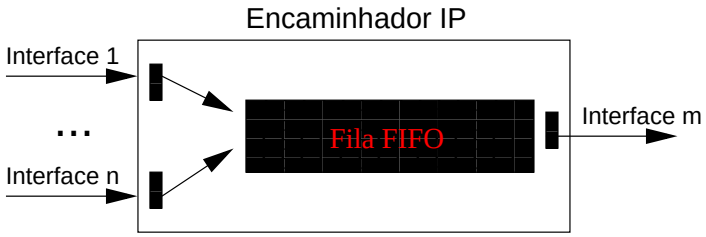

Figura 3.1: Gestão de Filas com a técnica FIFO

Dado que, como vimos anteriormente, o modelo *best-effort* não serve as necessidades actuais de fornecimento de qualidade de serviço em redes IP, torna-se necessário alterar a forma de tratamento dos pacotes, nas filas dos interfaces de rede dos encaminhadores. A figura 3.2 apresenta graficamente as alterações necessárias, nos encaminhadores, para ser possível uma evolução do tradicional paradigma *best-effort*, para novos paradigmas que suportem qualidade de serviço.

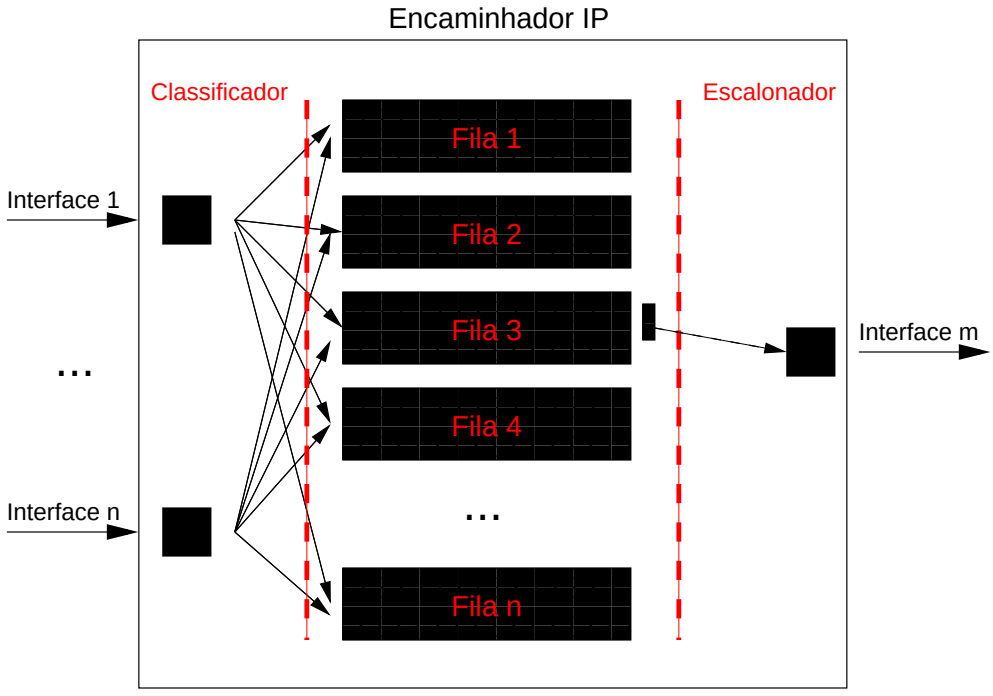

Figura 3.2: Classificação, Enfileiramento e Escalonamento, nos encaminhadores IP

Para que estas alterações sejam possíveis, é necessário substituir a tradicional fila única de cada interface por um conjunto de filas, que possam receber tráfego com diferentes necessidades de qualidade de serviço.

[5] *First In First Out* – primeiro a chegar, primeiro a sair

Mais de uma fila por interface só será útil se tiver existido uma **classificação** prévia do tráfego, por forma a distribui-lo pelas diferentes filas.

Por fim, é necessário um mecanismo próprio de **escalonamento** dos pacotes, que, em função dos parâmetros de QoS definidos, os retira das filas e transmite-os pelo interface de saída.

3.5.1 Gestão das Filas de Espera

As técnicas de gestão de filas de espera têm por objectivo genérico definir métodos para gerir a forma como os pacotes são tratados nos *buffers* dos interfaces de rede, enquanto aguardam para ser transmitidos. Permitem, por exemplo, alterar a ordem de envio de um pacote, com base na prioridade que lhe foi atribuída a si (pacote) ou à fila onde foi colocado.

Os diferentes critérios usados pelas técnicas de gestão de filas de espera têm influência na latência sofrida por cada pacote, ao determinar quanto tempo este vai esperar até ser transmitido. Apresentam-se de seguida algumas das abordagens mais divulgadas para tratar esta questão.

First In, First Out – **FIFO**

De entre as diferentes técnicas existentas, a FIFO é considerada a mais simples. Os pacotes são enfileirados numa base de "primeiro a chegar, primeiro a sair".

Esta técnica ignora as características dos pacotes, nomeadamente ao nível da informação de precedência no cabeçalho de um datagrama IP.

Na forma de funcionamento mais simples, um pacote que é aceite na fila FIFO será sempre transmitido. Um pacote só será descartado quando a fila estiver completamente cheia. Neste caso, o pacote não chega a entrar na fila, sendo automaticamente eliminado.

A técnica FIFO funciona bem em ligações de grande capacidade, não congestionadas e que apresentam atrasos mínimos. É também aceitável quando não se torna necessário diferenciar serviços, assegurados por pacotes que atravessam um determinado interface.

Uma das desvantagens desta técnica está no facto de uma única estação poder monopolizar a utilização de uma determinada ligação por tempos longos de tempo.

Por exemplo, quando uma estação começa uma transferência de ficheiros, pode consumir toda a largura de banda de uma determinada ligação, em detrimento de sessões interactivas que também estejam estabelecidas. Este fenómeno é conhecido por "trem de pacotes", porque uma determinada fonte envia uma grande número de pacotes seguidos para um destinatário e os pacotes das restantes estações apenas seguirão no final destes.

Priority Queuing – **PQ**

O *Priority Queuing* é um esquema bastante rígido de prioritização de tráfego. O princípio de funcionamento é o seguinte: se o pacote A tem um nível de prioridade mais elevado que o pacote B, então o pacote A será sempre enviado primeiro que o pacote B.

Com este mecanismo, o *buffer* do interface é dividido em uma ou mais filas. Os pacotes são distribuídos por estas filas de acordo com a sua classificação prévia, com base nas políticas de prioridades definidas para o interface.

Normalmente, existe uma fila com prioridade normal, que irá receber todos os pacotes que não foram classificados.

A grande desvantagem deste mecanismo está no facto da fila de maior prioridade obter absoluta preferência sobre as filas de menor prioridade. Por exemplo, os pacotes da fila de prioridade menor só serão enviados quando todas as filas com prioridade superior estiverem completamente vazias. Se a fila de maior prioridade estiver sempre cheia, nenhuma das restantes será servida, com os pacotes aí colocados a serem perdidos.

Por outro lado, se bem aproveitada, esta técnica pode permitir por exemplo a utilização de uma fila de maior prioridade para transmitir tráfego que tem baixos requisitos de largura de banda, mas onde o atraso mínimo é fundamental. Isto assegurará que o tráfego é transmitido imediatamente mas, como precisa de pouca largura de banda, as filas de menor prioridade não serão afectadas.

Custom Queuing – **CQ**

A técnica de *Custom Queuing* permite a implementação de um esquema de prioritização de tráfego que aloca um valor de largura de banda mínimo para os tipos de tráfego especificados.

As filas são servidas num princípio de *round-robin*, enviando pacotes de uma fila até o seu contador atingir o limite. Nessa altura, é passada a vez à próxima fila. Este princípio assegura que nenhuma fila ocupará a totalidade da ligação durante um longo período de tempo, ao contrário da técnica *Priority Queuing*.

Para utilizar este mecanismo é necessário definir políticas de classificação do tráfego, e a seguir implementá-las, antes de cada pacote ser colocado numa determinada fila.

Weighted Fair Queuing – **WFQ**

A técnica *Weighted Fair Queuing* permite a prioritização de pacotes sem penalizar, de forma irreversível, os pacotes de mais baixa prioridade.

Trata-se de um mecanismo baseado num algoritmo de *Fair Queuing* – FQ. Este algoritmo (FQ) mantém filas separadas para os diferentes fluxos que atravessam os encaminhadores. As diferentes filas são então servidas de acordo com um princípio de *round-robin*. Evita-se assim que uma única fonte monopolize a totalidade de uma ligação partilhada, à custa de outros fluxos.

Na realidade o algoritmo de *Fair Queuing* é mais complexo que esta abordagem simplista do serviço *round-robin*. Desde logo, devido ao tamanho dos pacotes. Se este aspecto não fosse tido em conta, um fluxo com pacotes de 1000 bytes tería o dobro da largura de banda de um fluxo com pacotes de 500 bytes. O que acontece na prática é uma aproximação a um serviço *round-robin* bit-a-bit, mais justo na partilha da ligação de saída entre diferentes fluxos.

Com FQ, qualquer largura de banda que não seja usada por um fluxo, é automaticamente disponibilizada aos outros fluxos.

Por exemplo, se temos quatro fluxos a enviar pacotes através de uma ligação, cada um vai receber um quarto da largura de banda. Se um dos fluxos deixa de gerar pacotes durante tempo suficiente para esvaziar a sua fila, então a largura de banda da ligação passa a ser partilhada de forma igual pelos três fluxos restantes.

Pode-se assim afirmar que o mecanismo FQ fornece uma partilha mínima garantida da largura de banda para cada fluxo, com a possibilidade de obtenção de um valor acima do garantido, se outros fluxos não usarem a sua parte.

O *Weighted Fair Queuing* é uma variante do *Fair Queuing*, que permite a atribuição de um peso específico a cada fila. Este peso especifica quantos bits são transmitidos de cada vez que o encaminhador serve determinada fila, sendo assim controlada a percentagem da largura de banda utilizada por cada uma.

Um encaminhador que implementa WFQ tem de obter o peso associado a cada fluxo, seja através de configuração manual, seja através de um mecanismo de sinalização a partir da fonte.

Class-Based Queuing – **CBQ**

O *Class-Based Queuing* [57] baseia-se num modelo de classificação do tráfego em classes agregadoras, de acordo com determinados princípios, dependentes do modelo de serviço a utilizar.

Um destes princípios pode ser baseado no tipo de aplicações, sendo o tráfego classificado de acordo com as aplicações a que diz respeito. Por exemplo, é criada uma classe para tráfego FTP, outra para tráfego HTTP, etc.

Desta forma, os utilizadores são agrupados de acordo com as aplicações que utilizam. Significa que um utilizador pode obter melhor serviço quando usa a aplicação x do que quando usa a aplicação y.

A ideia fundamental é evitar que um determinado grupo de utilizadores de uma aplicação consuma a totalidade da capacidade de uma ligação, mesmo se a aplicação que estão a usar requer maior qualidade de serviço que outra aplicação.

Esta abordagem traduz-se num grau de importância relativo de cada pacote individual, que vai depender do nível de carga agregada da classe a que pertence. Quanto mais utilizadores uma classe tiver, menos importantes são os pacotes individuais e vice-versa.

Dado que a importância relativa dos pacotes de diferentes classes depende do nível de carga de cada classe e do seu peso, é praticamente impossível prever antecipadamente qual será a qualidade de serviço associada a cada fluxo individual.

3.5.2 Mecanismos de Controlo e Prevenção de Congestão

Ao nível da pilha protocolar TCP/IP, o controlo de uma ligação fim-a-fim está enquadrado no âmbito das funções da camada de transporte. Nesta camada, o protocolo TCP implementa um conjunto de mecanismos de controlo de congestão fim-a-fim.

A estratégia fundamental do TCP passa por enviar segmentos para a rede e ir reagindo a eventos observáveis que entretanto ocorrem. Este protocolo assume

gestão de filas FIFO nos encaminhadores da rede, podendo no entanto funcionar também com *fair queuing*.

Para efectuar este controlo de congestão, o TCP recorre aos mecanismos *Slow Start*, *Fast Retransmit* e *Fast Recovery*.

É importante perceber que a estratégia do TCP passa pelo controlo da congestão apenas quando ela ocorre, em vez de tentar evitar a sua ocorrência. Este protocolo vai incrementando sucessivamente o débito da transmissão (*slow start*) até encontrar um ponto em qua a congestão ocorre, controlando então o fluxo a partir desse ponto. Por outras palavras, precisa de criar perdas para saber qual a largura de banda disponível da ligação.

Uma alternativa interessante, embora ainda não usada em larga escala, passa por prevêr situações de congestão antes da sua efectiva ocorrência, por forma a ser possível diminuir o fluxo de dados antes de começarem a ser descartados pacotes.

Existem actualmente diferentes mecanismos que permitem implementar o princípio da detecção atempada de congestão, em redes TCP/IP. Nos próximos pontos serão apresentados alguns dos mais importantes.

DECbit

O mecanismo DECbit foi originalmente desenvolvido para utilização com a arquitectura *Digital Network Architecture* – DNA. Pode no entanto ser tambem aplicado com os protocolos TCP e IP.

Como foi referido anteriormente, o objectivo é partilhar a responsabilidade pelo controlo da congestão entre os encaminhadores e os sistemas finais.

Os encaminhadores efectuam monitorização contínua da carga, notificando explicitamente os nodos finais quando está prestes a ocorrer congestão.

A notificação é implementada através da activação de um *bit de congestão* nos pacotes que atravessam o encaminhador. Os nodos de destino copiam a seguir este bit para os pacotes de ACK, enviando-os de volta à orígem. Finalmente, a orígem ajusta a taxa de envio por forma a evitar a congestão.

Random Early Detection – RED

O mecanismo RED [37] permite, à semelhança do DECbit, detectar quando está eminente a ocorrência de congestão, notificando nessa altura a fonte para que esta proceda ao ajustamento da taxa de envio de pacotes.

Enquanto o mecanismo DECbit notifica explicitamente os sistemas finais, o RED notifica implicitamente a fonte que se aproxima uma situação de congestão, através da descartagem de um dos seus pacotes. A fonte será então efectivamente notificada pela consequente ocorrência de um *timeout* ou pela recepção de um pacote de ACK duplicado. Este sinal de ocorrência de congestão com base num *timeout* ou em pacotes duplicados é implementado pelos mecanismos de controlo de congestão do TCP, para o qual o RED foi desenhado.

Como uma parte do nome *early*[6] do RED sugere, um encaminhador descarta o pacote antes da altura em que devería faze-lo, por forma a notificar a fonte que

[6] *Early* = Cedo

deverá começar a diminuir a janela de congestão mais cedo do que normalmente o faría.

Por outras palavras, o encaminhador descarta um pequeno número de pacotes antes de ter esgotado completamente os seus *buffers*, para forçar a fonte a abrandar o ritmo de envio, na esperança de não ter de descartar uma quantidade de pacotes muito maior passado pouco tempo.

Dois aspectos fundamentais da implementação do algoritmo RED estão na forma como decide quando descartar um pacote e, após essa decisão, que pacote descartar.

Em vez de aguardar que a fila fique completamente cheia, sendo nessa altura forçado a descartar os pacotes que entretanto estão a chegar (aplicando uma política de descartagem do tipo *drop tail*[7]), o RED decide que pode descartar qualquer pacote que chega, com uma determinada *probabilidade de descartagem*, sempre que o tamanho da fila exceda determinado *nível de descartagem*. Este princípio tem o nome de *Descartagem Aleatória Antecipada*[8].

O RED usa o valor da taxa de ocupação média da fila como parâmetro para uma função aleatória, que decide quando os mecanismos de prevenção de congestão devem ser activados.

Quando a taxa de ocupação média sobe, a probabilidade de se iniciar uma acção de descarte de um pacote aumenta.

Uma fila de um encaminhador RED pode-se encontrar numa de três fases distintas:

1. Fase Normal: para uma taxa de ocupação entre zero e um determinado *threshold* mínimo, os pacotes são enfileirados sem qualquer problema (probabilidade de descarte é zero);

2. Fase de Prevenção de Congestão: acima do *threshold mínimo*, a probabilidade de um pacote ser descartado sobe linearmente até uma probabilidade máxima (Max_p), delimitada pelo *threshold* máximo;

3. Fase de Controlo de Congestão: com uma taxa de ocupação da fila acima do *threshold* máximo, o descarte dos pacotes é garantido.

A taxa média de ocupação é normalmente recalculada de cada vez que um novo pacote chega à fila, de acordo com a fórmula 3.1:

$$Tam_{med} = (1 - Peso) * Tam_{med} + Peso * Tam_{inst} \tag{3.1}$$

Onde:

- Tam_{med} é a taxa média de ocupação da fila;
- Tam_{inst} define a ocupação instantânea (no momento de realização da amostra);
- $Peso$ controla a "importância" relativa (varia entre zero e um) da taxa média de ocupação relativamente à taxa da ocupação instantânea.

[7]São descartados os últimos pacotes da fila
[8]Do inglês *early random drop*

Valores de *Peso* mais elevados traduzem uma postura mais "agressiva", no sentido de uma reacção mais rápida a uma possível aproximação de congestão. No campo oposto, valores da variável *Peso* mais baixos traduzem-se numa postura mais conservadora.

Devido à natureza *bursty* do tráfego Internet, as filas podem ficar cheias muito rapidamente e a seguir ficar vazias de novo. Assim, a utilização do tamanho médio da fila em vez do seu tamanho instantâneo permite uma captura mais precisa da noção de congestão.

Os encaminhadores que implementam RED suportam diferentes valores de *thresholds* mínimos e máximos para filas diferentes. Pode ainda ser definido um *Peso* diferente para cada fila.

As estratégias estatísticas de descarte de pacotes apresentam um conjunto útil de características:

- originam um mecanismo de notificação negativa para o TCP, cuja intensidade aumenta em função do nível de congestão no encaminhador;
- os fluxos que consomem maior quantidade de recursos de uma fila são sujeitos a notificações mais intensas;
- a sincronização é minimizada entre os esforços de prevenção da congestão de sessões de transporte independentes que partilham uma fila particular.

Começando atempadamente com descarte aleatório de pacotes (antes da fila ter esgotado o seu espaço), é aumentada a probabilidade de controlar uma congestão eminente, antes da ocupação da fila ficar demasiado elevada. Tornando aleatória a distribuição do descarte na fase de prevenção de congestão, reduzem-se as possibilidades de sujeitar simultaneamente múltiplos fluxos à perda de pacotes.

Weighted Random Early Detection – **WRED**

Os mecanismos de gestão de filas não estão limitados ao fornecimento de apenas um tipo simples de comportamento, perante uma determinada fila. A informação adicional dependente do contexto permite seleccionar uma de múltiplas funções de descarte.

Por exemplo, um pacote marcado num qualquer ponto anterior do seu percurso por exceder determinado perfil, pode ser sujeito a uma política de descarte mais agressiva do que outros pacotes colocados na mesma fila.

Neste contexto, o WRED é uma extensão do RED que permite a definição de diferentes perfis de descarte RED para diferentes tipos de tráfego, colocados numa mesma fila. Na prática, significa que poderão existir dois ou mais *thresholds* mínimos e máximos aplicáveis a uma determinada fila. Assim, a probabilidade de descarte passa a ser função da taxa de ocupação da fila e da classe de tráfego em que o pacote é enquadrado.

O processo de alteração da função de probabilidade com base no contexto do pacote é normalmente referenciado como *Pesagem*[9], donde resulta o nome deste mecanismo.

[9]do inglês: *weighting*

Random Early Detection with In and Out – **RIO**

O RIO usa o mesmo mecanismo do RED, sendo no entanto configurado com dois conjuntos de parâmetros. O primeiro conjunto aplica-se aos pacotes *In* (*in* = dentro do perfil RED) e o segundo aos pacotes marcados como *Out* (*out* = fora do perfil RED).

Este mecanismo utiliza assim um bit adicional de *In*/*Out*, usado numa base de marcação pacote-a-pacote. Assume ainda que os pacotes passaram anteriormente por um marcador, que marcará cada pacote (recorrendo ao bit in/out) como estando dentro (*In*) ou fora (*Out*) do perfil RED definido.

Quando cada pacote chega ao encaminhador, este verifica se o pacote está marcado como *In* ou como *Out*. Se for um pacote *In*, o encaminhador calcula o tamanho médio da fila para este tipo de pacotes ($Tam_{med}In$). Ao mesmo tempo, é calculado o tamanho médio da fila total (Tam_{med}), considerando todos os pacotes (*In* e *Out*) que chegam.

Tipicamente, os *thresholds* mínimo e máximo são menores para os pacotes *Out* que para os pacotes *In*.

A probabilidade de descartar um pacote *In* depende apenas do valor de $Tam_{med}In$, enquanto a probabilidade de descartar um pacote *Out* depende da ocupação média total da fila (Tam_{med}). Este princípio faz com que a curva de probabilidade de descarte dos pacotes *Out* seja mais agressiva. Por outro lado, os pacotes *Out* que passam pela fila não afectam a probabilidade de descarte dos pacotes *In*.

Em resumo, o RIO descarta primeiro os pacotes *Out*, quando é detectado o início de uma situação de congestão e passa a descartar todos os pacotes deste tipo se a congestão persiste. Apenas em último recurso, quando o encaminhador está a ser inundado por pacotes *In*, estes pacotes também são descartados, na esperança de se controlar a congestão.

Apesar de, à primeira vista parecer igual, o RIO difere do WRED na implementação da função de cálculo de taxa média de ocupação de cada fila, fazendo-o com base na marcação pacote-a-pacote prévia.

Adaptive Random Early Detection – **ARED**

O mecanismo RED requer um ajustamento cuidadoso dos seus parâmetros para funcionar correctamente. Infelizmente, a correcta definição destes parâmetros depende da natureza e da taxa de variabilidade do tráfego que passa através da fila RED.

Por exemplo o efeito do parâmetro $Peso$ sobre o cálculo do Tam_{med} varia significativamente com o número de fluxos TCP simultâneos. Na presença de poucos fluxos simultâneos, é provável que uma situação de congestão se vá criando relativamente devagar, pelo que o valor de $Peso$ deverá ser baixo. No entanto, usando o mesmo valor de $Peso$ na presença de muitos fluxos TCP pode resultar numa reacção atrasada a uma possível situação de congestão eminente.

Inversamente, definindo $Peso$ para que o RED possa reagir suficientemente rápido em situação de muitos fluxos TCP, pode resultar num comportamento de descarte demasiado agressivo, quando poucos fluxos atravessam a fila.

O *Adaptive* RED [38] surgiu assim como uma resposta a esta limitação do RED, permitindo que exista um ajustamento dinâmico dos parâmetros, com base no

histórico de congestão recente.

Com a abordagem do ARED, se existirem N ligações a partilhar uma fila, o efeito do descarte de um pacote induzido pelo RED traduz-se na redução da carga num factor de $(N - 1/(2 * N))$. Significa que quando o N cresce, o RED precisa de se tornar mais agressivo, para manter constante a sua eficácia.

Para resolver esta questão, o mecanismo ARED ajusta dinamicamente o valor de Max_p, com base nos valores recentes do tamanho médio da fila (Tam_{med}). Se o valor de Tam_{med} se mantém próximo do *threshold* mínimo, é calculado um valor de Max_p mais conservador (mais baixo). Se Tam_{med} se mantém mais próximo do *threshold* máximo, é definido um valor de Max_p mais agressivo (mais elevado).

À medida que o valor de Tam_{med} se vai deslocando mais num ou noutro sentido, o valor de Max_p também vai sendo ajustado, permitindo a rápida adaptação da resposta do mecanismo de controlo de congestão à variação do número de fluxos que atravessam a fila.

Flow Random Early Detection – **FRED**

O mecanismo FRED [39] pode ser considerado como mais um refinamento ao algoritmo RED. O RED pode-se transformar num mecanismo menos justo, quando a fila por ele gerida é partilhada por fluxos que reagem de forma diferente a notificações de congestão antecipadas.

De acordo com [39], os fluxos de tráfego podem ser divididos em três categorias diferentes, tendo em atenção a forma como reagem a situações de congestão:

- Fluxos não adaptativos: protocolos de transporte que ignoram perda de pacotes;
- Fluxos robustos: ligações TCP com curtos *round trip times* (RTTs) que, consequentemente, recuperam rapidamente de situações de perda de pacotes;
- Fluxos frágeis: ligações TCP com RTTs longos que, consequentemente, recuperam lentamente da perda de pacotes.

Quando uma mistura destes fluxos passa através de uma fila RED, o comportamento dos fluxos não adaptativos pode "arrastar" o parâmetro Tam_{med} para valores superiores aos do *threshold* mínimo, provocando probalidade de perda de pacotes superior a zero para todos os restantes fluxos, mesmo que estes não apresentem um "mau" comportamento.

Ao mesmo tempo, fluxos robustos são menos afectados por pequenas perdas de pacotes individuais que os fluxos frágeis, já que a taxa de recuperação do TCP depende do RTT dos fluxos.

Neste sentido, pode-se concluir que a notificação de congestão afecta de forma desiquilibrada os diferentes tipos de fluxos.

O mecanismo FRED resolve esta questão ajustando o comportamento de descarte de cada pacote, na base do estado de curto prazo do fluxo (apenas para fluxos que mentém pacotes na fila num dado instante).

Assim, são associadas a cada fluxo as variáveis Min_q e Max_q, que representam respectivamente o menor e maior número de pacotes que esse fluxo "pode" ter na

fila, num determinado instante. A variável Med_{cq} representa uma estimativa do número médio de pacotes que cada fluxo tem na fila.

Quando Tam_{med} é menor que o *threshold* máximo, o FRED aceita sempre pacotes de fluxos que tenham menos de Min_q pacotes na fila. Se o fluxo tem mais de Max_q pacotes actualmente na fila, o FRED descarta o pacote, independentemente do valor de Tam_{med}. Desta forma, este mecanismo consegue controlar os fluxos não adaptativos.

Quando um fluxo tem um valor de pacotes na fila que se situa entre Min_q e Max_q, o FRED usa o algoritmo do RED para determinar se cada novo pacote é aceite ou descartado.

Apesar deste mecanismo não necessitar de gestão de filas com base nos fluxos, requer que o encaminhador mantenha, de alguma forma, informação de contexto dos fluxos. Tal traduz-se na introdução de alguma complexidade na classificação, relativamente a variantes do RED referidas anteriormente.

3.6 Implementação de Qualidade de Serviço

A QoS não cria largura de banda. Não é possível à rede dar aquilo que não tem, logo a disponibilidade de largura de banda é o primeiro ponto a ter em conta, para resolver alguns dos problemas que se colocam ao funcionamento dos serviços de rede.

Os mecanismos de QoS apenas gerem a largura de banda, de acordo com os pedidos das aplicações e as definições da administração da rede. Assim, QoS com níveis de garantia de serviço requer alocação de recursos para sequências de dados individuais.

A largura de banda alocada para uma aplicação com base em determinada "reserva de recursos" deixa de estar disponível para utilização por aplicações "*best–effort*". Considerando que a largura de banda é um recurso finito, um aspecto a ter em atenção pelos administradores de rede é a garantia de que a totalidade das reservas de recursos deixam ainda alguma margem de tráfego *best–effort*. Aplicações com a mais alta prioridade de tráfego não podem impedir o funcionamento das aplicações de mais baixa prioridade. O que deve acontecer é que estas aplicações de mais baixa prioridade simplesmente têm um serviço pior (mais lento), mas continuam a funcionar.

Existem duas formas básicas de estabelecimento de medidas de QoS em redes IP [41]:

- **Reserva de Recursos**: os recursos de rede são repartidos, de acordo com pedidos prévios (reservas) de QoS das aplicações, e em conformidade com a política de gestão da largura de banda;
- **Prioritização de Tráfego**: o tráfego é classificado em fluxos agregados e os recursos da rede são repartidos de acordo com critérios da política de gestão da largura de banda.

Na sequência da importância crescente que esta área tem vindo a adquirir, o IETF tem vindo a desenvolver vários modelos e mecanismos para implementação de QoS nas redes informáticas, donde se destacam os seguintes [52]:

- **Modelo de Serviços Integrados** – *IntServ*[10] [29, 30, 31], define um conjunto de métodos de especificação de qualidade de serviço, que permitem reservar recursos a ser alocados para fluxos de tráfego individuais;

- **Multiprotocol Label Switching** – MPLS [53], recorre a uma etiqueta de tamanho fixo, a partir da qual os encaminhadores tomam a decisão de envio dos pacotes.

- **Engenharia de Tráfego** [55]. Preocupa-se com a optimização do desempenho das redes de dados.

- **Encaminhamento com Qualidade de Serviço** [56]. Disponilibiza mecanismos de selecção de rotas, para o envio de pacotes, com base em requisitos de qualidade de serviço.

- **Modelo de Serviços Diferenciados** – *DiffServ*[11] [32, 33], baseado num princípio de prioritização do tráfego, classifica-o em diferentes Classes de Serviço (CoS), com base num conjunto de bits específicos no cabeçalho dos pacotes IP (sejam pacotes IPv4 ou IPv6). O seu objectivo é fornecer um tratamento particular a diferentes classes de tráfego, identificadas em cada pacote IP pelo campo DS[12], por parte dos sistemas de comunicação.

Nos próximos pontos será feita uma breve descrição de cada um destes mecanismos.

Dada a importância do modelo *DiffServ* para o presente trabalho, será efectuada uma análise mais detalhada deste.

3.6.1 O Modelo de Serviços Integrados – *IntServ*

Como referido anteriormente, os atrasos no transporte dos pacotes e as perdas por congestão fazem com que as aplicações de tempo real não funcionem bem com tráfego *best–effort*. Estas aplicações precisam assim de largura de banda garantida.

O modelo *IntServ* foi desenvolvido com o objectivo de optimizar a utilização dos recursos de rede por novas aplicações (multimédia, de tempo real), que requerem garantias de QoS. Fornece assim garantias de disponibilização de recursos fim-a-fim, para fluxos individuais. Um encaminhador que o suporte tem de ser capaz de fornecer uma QoS apropriada para cada fluxo, de acordo com o modelo de serviço.

O fornecimento de diferentes níveis de qualidade de serviço é efectuado, nestes encaminhadores, por uma função de controlo de tráfego, constituída pelos seguintes componentes:

- **Classificador de pacotes**: Identifica os pacotes de um fluxo IP nos nodos, mapeando-os para um classe específica. Todos os pacotes que são classificados aqui com a mesma classe, recebem o mesmo tratamento no Escalonador de Pacotes.

[10] de *Integrated Services*
[11] de *Differentiated Services*
[12] *differentiated services field*

- **Escalonador de pacotes**: Faz a gestão do envio das sequências de dados nos nodos, de acordo com a sua classe de serviço. Utiliza mecanismos de gestão de filas, além de vários algoritmos de escalonamento. Este componente é implementado no ponto onde os pacotes são "enfileirados".

- **Função de Controlo de admissão**: Contém o algoritmo que o encaminhador usa para determinar a existência de recursos suficientes para aceitar a QoS requisitada para determinado fluxo.

O RFC 2215 [30] define um conjunto de parâmetros de caracterização e controlo, usados no modelo de Serviços Integrados. Entre os mais importantes, destacam-se parâmetros relativos à gestão do tráfego, cujo parâmetro-chave é $TOKEN\_BUCKET\_TSPEC$, abreviadamente designado por $TSPEC$.

Fruto do trabalho desenvolvido pelo *Integrated Services Working Group* do IETF, foram definidas duas classes de serviço específicas, que se juntam ao tradicional Serviço *Best–effort*:

- *Guaranteed Service* [44]: trata-se de um serviço semelhante à emulação de um circuito dedicado virtual. Fornece fronteiras rígidas em atrasos nas filas fim-a-fim, através da combinação de parâmetros de vários elementos da rede ao longo do caminho. Assegura ainda disponibilidade de largura de banda, de acordo com parâmetros TSpec.

- *Controlled Load Service* [43]: classe de serviço equivalente ao serviço best–effort em condições controladas. Na prática, trata-se de um serviço melhor que o *best-effort*, mas sem o controlo rígido do *Guaranteed Service*.

Resource Reservation Protocol - RSVP

O modelo de Serviços Integrados pressupõe que os recursos (principalmente os dos encaminhadores), devam ser explicitamente reservados para atender às necessidades das aplicações, partindo do princípio que os utilizadores podem "requisitar" uma qualidade de serviço específica para cada transmissão, superior à oferecida pelo serviço *best-effort*.

Este pressuposto traduz-se na necessidade da realização prévia de reserva de recursos e controlo de admissão, tal como acontece no sistema telefónico.

A reserva de recursos pode ser efectuada de forma estática ou dinâmica. No modelo IntServ, a sinalização das especificações do serviço solicitado e consequente reserva dinâmica de recursos através dos elementos da rede é efectuada pelo Protocolo RSVP - *Resource Reservation Protocol* [45, 46].

As instâncias IntServ comunicam entre si através do protocolo RSVP, para criar e manter estados de fluxos específicos nos diferentes nodos (encaminhadores e sistemas finais) ao longo do caminho de um fluxo.

Apresenta-se de seguida, de forma simplificada, o processo de reserva de recursos baseado na sinalização do RSVP:

- O Emissor define os requisitos do tráfego de saída de acordo com os limites máximo e mínimo de largura de banda, atrasos e perdas. De seguida, o RSVP envia uma *PATH message*, que transporta a informação TSpec até ao receptor;

- Para efectuar a reserva dos recursos, o(os) receptor(es) envia(m) uma *RESV message* (mensagem de reserva) pelo caminho definido pela *PATH message*, até ao emissor. Adicionalmente à TSpec, a *RESV message* inclui a *Request specification* – Rspec, que indica o tipo de serviços integrados requeridos (*Controlled Load* ou *Guaranteed*) e a *filter specification* (filter spec), que caracteriza a forma como os pacotes vão ser reservados (por exemplo pelo protocolo de transporte e número do respectivo porto); Em conjunto, o RSpec e o filter spec definem o descritor de fluxo que os encaminhadores usam para identificar cada reserva.

- Quando cada encaminhador RSVP ao longo do caminho recebe a *RESV message*, vai utilizar um processo de controlo de admissão para autenticar o pedido e alocar os recursos necessários. Se o pedido não pode ser satisfeito (por falta de recursos ou falha na autenticação) o encaminhador envia um erro de volta até ao receptor. Se o pedido for aceite, o encaminhador envia a mensagem para o próximo encaminhador no caminho até ao emissor;

- Quando o último encaminhador recebe a *RESV message* e aceita o pedido, envia uma mensagem de confirmação de volta para o receptor do fluxo que se está a reservar;

- No final de uma sessão RSVP tem de haver uma terminação explicita da mesma.

Apesar de representar uma significativa alteração no actual paradigma de funcionamento da Internet, o modelo *IntServ* apresenta um conjunto de limitações importantes, que limitam a sua escalabilidade para funcionamento em larga escala [52]:

- a quantidade de informação de estado cresce proporcionalmente com o número de fluxos individuais, o que se traduz numa elevada carga de processamento e armazenamento adicional, nos encaminhadores. Por esse motivo, esta arquitectura não consegue escalar bem ao nível das grandes redes centrais da Internet.

- São exigídos elevados recursos aos encaminhadores. Todos têm de implementar o protocolo RSVP, realizar controlo de admissão, classificação *multi-field* e escalonamento de pacotes.

3.6.2 MultiProtocol Label Switching – MPLS

Nas redes IP, quando um encaminhador recebe um pacote, obtém o seu endereço de destino e efectua uma busca na sua tabela de encaminhamento à procura do interface de saída correspondente à rota para esse endereço. Esta busca pode levar bastante tempo, dependendo do tamanho da tabela de cada encaminhador.

O MPLS [52, 53] rompe com este paradigma, usando uma etiqueta de tamanho fixo a partir da qual o encaminhador decide por onde enviar os pacotes.

Este protocolo é o resultado da padronização de várias implementações proprietárias da técnica de encaminhamento baseado em etiquetas (*label switching*), posicionando-se entre a camada de Ligação de Dados e a camada de Rede do Modelo OSI.

Cada pacote MPLS possui um cabeçalho de 32 bits, constituído por: uma Etiqueta de 20 bits, um campo *Classe de Serviço* (COS) com 3 bits, um *Label Stack Indicator* de 1 bit e um campo *Time-to-Live* de 8 bits.

O cabeçalho MPLS é encapsulado entre o cabeçalho da camada de Ligação de Dados e o cabeçalho da camada de Rede.

Os encaminhadores que suportam este protocolo são designados por *Label Switching Routers* (LSR), tomando estes a decisão de encaminhamento apenas com base na etiqueta de cada pacote.

A designação de *MultiProtocol Label Switching* surge do seu suporte para múltiplos protocolos de Ligação de Dados e de Rede.

Para funcionar, o MPLS precisa de um protocolo que efectue a distribuição das Etiquetas entre os encaminhadores, por forma a definir os caminhos a percorrer pelos pacotes (*Label Switched Paths* – LSP). Normalmente, é usado nestas funções o *Label Distribution Protocol* (LDP) [54], podendo no entanto também ser usado RSVP, com extensões apropriadas para este efeito.

O encaminhamento baseado em MPLS proporciona algumas vantagens relativamente ao encaminhamento tradicional, nomeadamente:

- melhor desempenho no encaminhamento de pacotes;
- a criação dos caminhos LSP's entre encaminhadores torna-se útil para a engenharia de tráfego;
- possibilidade de associar requisitos de qualidade de serviço com base na etiqueta dos pacotes.

3.6.3 Engenharia de Tráfego

Mecanismos de QoS como os modelos de Serviços Integrados e de Serviços Diferenciados garantem que a degradação do desempenho das redes seja mais suave, quando o carga de tráfego é pesada. Quando a carga de tráfego é pequena, a diferença entre estes mecanismos e o serviço *best-effort* não é muito significativa.

Partindo deste princípio, a principal motivação da Engenharia de Tráfego [52, 55] passa por evitar que as situações de congestão venham efectivamente a ocorrer.

A congestão da rede pode ocorrer por falta de recursos ou por distribuição desigual do tráfego. No primeiro caso, todos os encaminhadores e ligações estão com sobrecarga, passando a solução pela disponibilização de mais recursos. No segundo caso, algumas partes da rede podem estar com sobrecarga enquanto outras se mantém sub-ocupadas.

Esta distribuição desigual do tráfego pode ser causada pelos protocolos de encaminhamento dinâmico usados actualmente, já que estes baseiam sempre a sua decisão de encaminhamento na escolha do menor caminho (de acordo com as métricas definidas) para cada pacote. Como resultado, encaminhadores e ligações ao longo do

menor caminho entre dois nodos tenderão a ficar congestionadas, enquanto outros encaminhadores e ligações de caminhos mais longos tendem a ter pouca ocupação.

Neste sentido, a Engenharia de Tráfego engloba a aplicação de princípios tecnológicos e científicos para medir, modelar, caracterizar e controlar os fluxos de tráfego ao longo das redes, por forma a que a congestão causada por utilização desigual de recursos possa ser evitada.

3.6.4 Encaminhamento com Qualidade de Serviço

As tabelas de encaminhamento dos encaminhadores podem ser mantidas estática (através de administração manual) ou dinamicamente. A sua manutenção dinâmica é efectuada através de protocolos de encaminhamento, como o RIP[13], OSPF[14] ou BGP[15].

Estes protocolos escolhem as melhores rotas com base no caminho mais curto, sendo normalmente optimizados para a utilização de apenas uma métrica que pode ser, por exemplo, a quantidade de encaminhadores a ser percorrida ou o peso administrativo de cada ligação.

Recorrendo a Encaminhamento com Qualidade de Serviço [56], as rotas utilizadas para o envio dos pacotes podem ser determinadas com base em algum tipo de conhecimento da disponibilidade de recursos da rede e nos requisitos de QoS de cada fluxo (por exemplo, largura de banda, atraso, etc).

Os principais objectivos do Encaminhamento com QoS são:

- Determinação dinâmica dos caminhos possíveis: o encaminhamento com QoS pode determinar um rota para um fluxo, a partir de múltiplas escolhas, que terá boas possibilidades de assegurar a QoS requerida para esse fluxo. A selecção dos caminhos possíveis pode ser sujeita à aplicação prévia de mecanismos de policiamento, como sejam a definição dos custos dos caminhos ou a indicação do ISP a atravessar, por exemplo.

- Optimização da utilização dos recursos: um mecanismo deste tipo pode ajudar, de forma efectiva, na utilização eficiente dos recursos de rede.

- Degradação suave do desempenho: encaminhamento dependente do estado dos recursos pode fornecer melhor desempenho e uma maior suavização na degradação do serviço do que o encaminhamento tradicional, quando a rede se aproxima de uma situação de congestão.

Encaminhamento com Qualidade de Serviço pode ser utilizado para descobrir as rotas que a seguir serão utilizadas por encaminhadores que implementam MPLS, *IntServ*/RSVP ou *DiffServ*, por exemplo.

[13] *Routing Information Protocol*
[14] *Open Shortest Path First*
[15] *Border Gateway Protocol*

3.6.5 O Modelo de Serviços Diferenciados – *DiffServ*

Entre as várias alternativas para implementação de QoS nas redes IP, o modelo de Serviços Diferenciados [5, 32] tem vindo a conquistar algum destaque por, entre outros factores, oferecer uma característica fundamental: escalabilidade. Esta escalabilidade é obtida através da agregação de fluxos e pela separação das funções entre os encaminhadores de fronteira e os encaminhadores do núcleo das redes.

As redes que implementam serviços diferenciados de acordo com uma política de QoS comum são denominadas Domínios DS[16].

Diferentes Domínios DS podem negociar entre si acordos (SLA – *Service Level Agreements*) para fornecimento de garantias mínimas de QoS às aplicações dos utilizadores.

Todos os pacotes que circulam de um domínio para outro são fiscalizados nos encaminhadores de fronteira desses domínios, para verificar a sua conformidade com os acordos estabelecidos.

No centro da rede, os encaminhadores simplesmente encaminham os pacotes para os seus destinos, oferecendo algumas garantias de QoS a determinados pacotes.

Pacotes distintos podem ter tratamentos distintos, nos encaminhadores, de acordo com determinados requisitos de QoS. Este tratamento específico de encaminhamento é traduzido no Comportamento dos Nodos – PHB (*Per-Hop Behavior*).

A combinação dos PHB no centro da rede com as regras de policiamento na fronteira permitem a criação de várias classes de serviço (CoS), numa rede *DiffServ*.

O campo DS

Uma das formas de introduzir diferenciação no tratamento dos pacotes por parte dos encaminhadores, passa pela análise de alguns campos do seu cabeçalho, para posterior aplicação de políticas associadas.

Como parte do desenvolvimento de uma arquitectura de Serviços Diferenciados, o IETF propôs a alteração do formato do cabeçalho dos pacotes IP. Os octetos *Tipo de Serviço* do cabeçalho IPv4 e *Classe de Tráfego* do cabeçalho IPv6 foram redefinidos, dando origem ao campo DS[17] [32].

Este foi por sua vez dividido em dois sub-campos:

- DSCP – *Differentiated Services CodePoint*: primeiros seis bits do campo DS, que armazenam o valor que permite seleccionar determinado PHB para o pacote;
- CU – *Currently Unused*: últimos dois bits do campo DS, reservados para utilização futura, sendo ignorados pelos nodos compatíveis com o modelo *DiffServ*.

O DSCP permite definir até 64 *codepoints* diferentes. Este espaço foi dividido pela IANA[18] em três *pools* distintas, para efeitos de atribuição e administração de *codepoints*:

[16] DS = *Differentiated Services*
[17] *Differentiated Services field*
[18] IANA: *Internet Assigned Numbers Authority*

- *Pool* 1 (32 *codepoints*): reservada para *codepoints* normalizados, tomando o bit menos significativo o valor zero ($xxxxx0$);
- *Pool* 2 (16 *codepoints*): reservada para experimentação e utilização local. Neste caso, os dois bits menos significativos tomam o valor um ($xxxx11$);
- *Pool* 3 (16 *codepoints*): inicialmente reservada para experimentação e utilização local, mas podendo ser preferencialmente utilizada para normalização, no futuro, se a *Pool* 1 ficar esgotada. Os *codepoints* desta *Pool* têm os dois bits menos significativos com os valores zero e um, respectivamente ($xxxx01$).

A Arquitectura de Serviços Diferenciados

O *Working Group DiffServ* do IETF [5] produziu, no âmbito das suas atribuições, um modelo arquitectural para a implementação de Serviços Diferenciados em larga escala [33].

Esta arquitectura baseia-se num modelo onde o tráfego que chega a uma rede é classificado e possivelmente condicionado na sua fronteira, sendo associado, de acordo com a classificação, um determinado tipo de comportamento agregado (*behaviour aggregate*).

Cada tipo de comportamento agregado é identificado por um DS *codepoint*. Nos encaminhadores interiores da rede, os pacotes são reenviados de acordo com o comportamento do nodo (*per-hop behaviour*) associado ao *codepoint*.

Domínios e Regiões DS

Um domínio DS é um conjunto contíguo de nodos DS, que operam sob serviços de policiamento e grupos de PHB's comuns, implementados em cada nodo [33]. Normalmente consiste numa ou mais redes sob a mesma administração (por exemplo, a rede de um ISP[19]).

Cada domínio deste tipo é limitado por uma fronteira, constituída por encaminhadores DS de fronteira.

Os encaminhadores DS de fronteira interligam diferentes domínios DS e domínios DS com domínios não DS. Estes classificam e possivelmente condicionam o tráfego de entrada, para assegurar que os pacotes que chegam ao domínio são apropriadamente marcados com *codepoints* correspondentes a PHB's de grupo aqui suportados.

Os encaminhadores DS do interior do domínio interligam-se a outros encaminhadores do mesmo tipo e a encaminhadores DS de fronteira. Seleccionam o comportamento de reenvio dos pacotes com base no seu *codepoint* DS, mapeando este valor para um dos PHB's suportados.

Tanto os encaminhadores de fronteira como os interiores têm de ser capazes de aplicar o PHB apropriado aos pacotes que os atravessam, de acordo com o seu *codepoint* DS.

O conjunto de um ou mais Domínios DS constituí uma Região DS. Os domínios de uma região DS podem suportar internamente diferentes grupos de PHB's e diferentes mapeamentos *codepoint* $\rightarrow$ PHB. Para ser possível que determinados serviços

[19] *Internet Service Provider*

atravessem diferentes domínios de uma mesma região DS, é necessário o estabelecimento de Acordos de Serviço (SLA's) entre estes domínios, que definem as regras de condicionamento do tráfego (TCA – *Traffic Conditioning Agreement*) que os atravessa.

É também possível que diferentes domínios de uma mesma região DS adoptem políticas de fornecimento de serviços comuns, suportando simultaneamente os mesmos grupos de PHB's e mapeamentos de *codepoints*, que eliminam a necessidade da reclassificação de tráfego entre estes domínios.

Classificação e Condicionamento do Tráfego

Os SLA estabelecidos entre diferentes domínios DS devem especificar as regras de classificação e remarcação de pacotes. Podem ainda especificar adicionalmente diferentes perfis de tráfego e respectivas acções a desencadear, consoante os pacotes se enquadram dentro ou fora desses perfis.

Os acordos de condicionamento de tráfego (TCA) são determinados (implicita ou explicitamente) a partir dos SLA.

Estes acordos são implementados por mecanismos de condicionamento, que podem incluir funções de classificação, medição, policiamento, marcação, *shaping* e descarte, para garantir que o tráfego entra num domínio DS em conformidade com as regras especificadas no TCA.

As políticas de classificação de pacotes identificam o sub-conjunto de tráfego que deve receber serviço diferenciado, através de condicionamento e/ou mapeamento para um ou mais tipos de comportamento agregado (através de remarcação do respectivo *codepoint*) existentes no interior do domínio DS.

Os **Classificadores** seleccionam os pacotes com base no conteúdo de um ou mais campos do cabeçalho.

Em [33] são definidos dois tipos de classificadores que podem ser usados para implementação de Serviços Diferenciados:

- Classificadores BA (*Behavior Aggregate*): classificam os pacotes com base no conteúdo do *codepoint* DS;
- Classificadores MF (*Multi-field*): seleccionam pacotes com base numa combinação dos valores de um ou mais campos do cabeçalho, nomeadamente endereços de orígem e destino, campo DS, *Protocol ID*, portos de orígem e destino, etc.

As funções de medição do tráfego são implementadas por **Medidores**, que controlam se o reenvio dos pacotes seleccionados pelo Classificador se enquadra dentro do perfil de tráfego acordado no SLA. Estes mecanismos passam informação de estado a outras funções de condicionamento, para que estas possam despoletar acções particulares para cada pacote, em função da conformidade ou não com os requisitos de QoS definidos.

Os **Marcadores** de pacotes preechem o campo DS de cada pacote com um *codepoint* específico, associando o pacote marcado a um determinado perfil de tráfego

agregado DS. Esta marcação é influenciada pela classificação e medição realizadas anteriormente.

Os **Shapers** e **Droppers** asseguram a conformidade do tráfego com os perfis de tráfego acordados, através do atraso no envio de pacotes durante algum tempo (*Shapers*), ou do seu descarte (*Droppers*).

Comportamento dos Nodos (*Per-Hop Behaviors* – PHB's)

Os pacotes IP atingem os nodos de destino sendo reenviados por encaminhadores intermédios ao longo do percurso. Quando, após uma decisão de encaminhamento, são reenviados para outros encaminhadores, os pacotes que requerem serviço similar são agrupados em função do seu *Per-Hop Behavior* (PHB).

De acordo com [33], o PHB traduz o comportamento externamente observável do envio de pacotes por parte de um determinado nodo DS, aplicado a um comportamento agregado DS particular.

Um comportamento agregado (*behavior aggregate* – BA) DS representa uma colecção de pacotes com o mesmo *codepoint* a atravessar uma ligação numa determinada direcção.

Os PHB's podem ser especificados com base na prioridade relativa dos seus recursos relativamente a outros PHB's (por exemplo, alocação de *buffers* e largura de banda), ou em função das suas características relativas observáveis do tráfego (por exemplo, atraso e perdas).

Um PHB de grupo é um conjunto de um ou mais PHB's especificados e implementados simultaneamente, de uma forma consistente e inter-relacionada.

Os PHB's são seleccionados, em cada nodo, através de um mapeamento do *codepoint* definido no campo DS de cada pacote. Os PHB's normalizados têm um *codepoint* associado.

Nos nodos DS, todos os *codepoints* têm de ter um mapeamento para um determinado PHB. Quando tal não existe explicitamente, o *codepoint* é mapeado para o PHB por defeito (*Default PHB*).

Para além da definição do *Default PHB*, o *DiffServ Working Group* do IETF manteve a compatibilidade com a utilização histórica do campo *IP Precedence* do cabeçalho do pacote IP. Para tal, foram reservados os *codepoints* utilizados por este campo para mapeamento em PHB's que asseguram os requisitos históricos estabelecidos (*Class Selector PHB*) [32].

Até ao momento, o IETF propôs ainda, para normalização, mais dois grupos de PHB's: o PHB EF – *Expedited Forwarding* e o PHB AF – *Assured Forwarding*.

Default PHB

Todos os nodos que suportem o modelo *DiffServ* terão de disponibilizar um *Default PHB* [32], que corresponderá ao tradicional serviço de melhor esforço fornecido pelo protocolo IP. O tráfego que não recebe uma classificação que lhe permita receber outro PHB específico, será tratado de acordo com este PHB.

É importante que cada nodo DS reserve alguns recursos mínimos para este tipo de tráfego agregado, por forma a assegurar a utilização da rede por parte de nodos não-DS.

De acordo com [32], é recomendado um *codepoint* com o valor '000000' para este PHB.

Pacotes marcados inicialmente para o *Default PHB* podem ser remarcados com outros *codepoints* na fronteira de domínios DS, de acordo com os SLA estabelecidos.

Class Selector PHB Group (CS PHB)

Como referido anteriormente, o grande objectivo do *Class Selector PHB Group* é manter compatibilidade com a utilização actual dos bits 0 a 2, do octeto TOS[20] do cabeçalho dos pacotes IPv4.

Como o princípio de uso destes bits é similar ao dos PHBs, faz sentido adaptar a sua utilização no contexto da arquitectura *DiffServ*. No entanto, a perspectiva de utilização deste PHB é especial: enquanto os outros PHB's são usados para construir novos serviços, a definição do grupo CS-PHB tenta abranger variados, em alguns casos contraditórios, usos do campo TOS, nas redes actuais.

De acordo com [32], valores do campo DSCP no formato ´xxx000' são reservados para o grupo CS-PHB. Os PHB's que são mapeados por estes *codepoints* têm de satisfazer os requisitos do CS-PHB, preservando adicionalmente os requisitos do *Default PHB*, mapeado pelo *codepoint* ´000000'.

Em [32] são definidos os requisitos genéricos deste grupo de PHB's:

- Cada CS-PHB deve fornecer uma probabilidade de transmissão aos seus pacotes que não seja menor que a probabilidade de transmissão disponibilizada a pacotes marcados com um CS-PHB de valor mais baixo, em condições de operação e ocupação normais.

- Os PHB's seleccionados pelos *codepoints* ´11x000' têm de fornecer aos seus pacotes um tratamento de transmissão preferencial, comparativamente com o *Default PHB*, por forma a preservar a actual utilização dos valores ´110' e ´111' do campo *IP Precedence* para tráfego de encaminhamento.

- Cada CS-PHB recebe um tratamento de transmissão independente dos restantes CS-PHB's. Os nodos da rede podem estabelecer limites na quantidade de recursos utilizados por cada um destes PHB's.

Um nodo DS-compatível pode suportar um ou mais CS-PHB's. Tal significa que é possivel mapear múltiplos CS-*codepoints* para um mesmo CS-PHB, desde que sejam garantidos os requisitos enunciados atrás. Não é condição obrigatória a existência de um CS-PHB diferente por cada um dos *codepoints* inseridos no conjunto ´xxx000'.

Expedited Forwarding PHB (PHB EF)

O PHB EF [35] permite criar um serviço fim-a-fim, com baixa taxa de perdas, baixa latência, baixo *jitter* e largura de banda assegurada (características importantes por exemplo para um serviço de VoIP). É visto nas extremidades como uma ligação

[20] *Tipe of Service*

ponto-a-ponto ou um circuito virtual dedicado, sendo também conhecido como *Premium Service*.

Esta abordagem divide os pacotes em duas classes. A primeira engloba uma pequena parte do tráfego, a ser marcado com um *codepoint* especial, que lhe permite receber o tratamento definido para tráfego EF, com as características descritas anteriormente.

A segunda classe engloba o restante tráfego (a maior parte dos pacotes), que é transmitido de acordo com o princípio do melhor esforço.

Em [35] é recomendado um *codepoint* com o valor '101110' para o PHB EF.

Os nodos DS que suportam tráfego EF têm de garantir um débito agregado mínimo para este tipo de tráfego sempre igual ou superior ao configurado.

Por outro lado, se este PHB for implementado por mecanismos que permitam uma ocupação ilimitada das ligações por determinados tipos de tráfego (por exemplo usando *Priority Queuing*), deve ser incluído um limite máximo de ocupação para tráfego EF. Este mecanismo de limitação pode ser implementado com recurso a um sistema do tipo *token bucket*. Neste caso, o tráfego deste tipo que excede o limite máximo terá de ser descartado.

Pacotes marcados para o PHB EF podem ser remarcados, na fronteira de domínios DS, apenas para outros *codepoints* que também satisfaçam as condições do EF. Não podem assim ser remarcados para outros PHB's.

Da mesma forma, quando pacotes marcados com este PHB são encapsulados em outros pacotes para transporte através de túneis, estes últimos pacotes também têm de ser marcados com o mesmo PHB EF.

O PHB EF pode coexistir em redes que utilizam outros esquemas de PHB's, desde que estes não interfiram com os seus requisitos pré-definidos.

Assured Forwarding PHB Group (PHB AF)

O PHB de Grupo *Assured Forwarding* (PHB AF) [34] fornece entrega de pacotes IP em quatro classes de transmissão independentes. Em cada uma destas classes, os pacotes são divididos em três níveis distintos de precedência de descarte.

É objectivo deste PHB disponibilizar uma forma de "assegurar" diferentes níveis de transmissão de pacotes IP, entre dois domínios DS.

Cada uma das quatro classes será contemplada com determinado conjunto de recursos de transmissão, nomeadamente espaço nos *buffers* e largura de banda.

No RFC 2597 [34] recomenda-se um conjunto de *codepoints* (ver tabela 3.1), escolhidos de modo a não se sobreporem, quer com outros PHB's previamente definidos, quer com as regras gerais de normalização destes identificadores, definidas em [32].

	Classe 1	Classe 2	Classe 3	Classe 4
Baixa Precedência de Descarte	001010	010010	011010	100010
Média Precedência de Descarte	001100	010100	011100	100100
Alta Precedência de Descarte	001110	010110	011110	100110

Tabela 3.1: *Codepoints* do PHB AF

Os pacotes IP que usam os serviços deste PHB serão associados em primeiro lugar a uma das classes. De seguida serão marcados com um nível de precedência da classe a que pertencem, de acordo com o serviço previamente acordado.

Em caso de congestão, o valor de precedência de descarte determina a importância relativa do pacote dentro da classe AF. Os pacotes com valores de precedência de descarte mais elevados terão maior probabilidade de ser descartados que os pacotes com valores de precedência mais baixos.

O nível de garantia de transmissão dos pacotes IP que usam serviços do PHB AF depende:

1. de quantos recursos de transmissão foram alocados à classe AF a que o pacote pertence;

2. de qual é a carga actual dessa classe AF e

3. em caso de congestão dentro da classe, qual é a precedência de descarte do pacote.

Cada classe AF assegura aos seus pacotes um tratamento independente do que é dado aos pacotes das outras classes AF. Tal significa que um nodo DS não pode agregar duas ou mais classes AF.

Por outro lado, uma classe AF pode ser configurada para receber mais recursos de transmissão, quando existem recursos em excesso disponíveis, quer de outras classes AF, quer de outros PHB's.

Service Level Agreements – **SLA**

A gestão de serviços (*Service Level Management* – SLM) envolve a administração integrada de redes, sistemas e aplicações, com o objectivo de estabelecer e cumprir políticas especificadas em acordos de serviços [59]. Estas políticas definem regras e restrições no controlo e alocação dos recursos da rede para os serviços suportados, sendo expressas sob a forma de contratos, ou SLA (*Service Level Agreements*).

Os SLA [60] determinam a qualidade dos serviços oferecidos em função de parâmetros relacionados com a disponibilidade, segurança, tempo de resposta, atraso, etc.

Estes acordos podem ser definidos estática ou dinamicamente. Os primeiros são negociados entre o fornecedor e o cliente do serviço, podendo sofrer modificações periódicas.

Os SLA dinâmicos adaptam-se automaticamente às mudanças das condições da rede, no sentido de manter a QoS negociada com o utilizador.

Quando dois domínios DS pretendem trocar tráfego diferenciado entre si, estabelecem previamente um SLA, onde são definidas as regras de tratamento do tráfego que os atravessa. Todos os pacotes são assim policiados nos encaminhadores de fronteira, para verificar a sua conformidade com os SLA estabelecidos.

O *DiffServ Working Group* do IETF limita-se a definir apenas os componentes básicos da arquitectura de serviços diferenciados, não abrangendo assim as questões relacionadas com as políticas de gestão de serviços implementadas sobre este modelo.

Em [59] é proposto um modelo de gestão de serviços, estruturado em quatro planos inter-relacionados e representando os diferentes graus de abstracção sobre os serviços disponibilizados pelas redes de computadores:

- **Plano de Negócio:**

  O Plano de Negócio define e avalia os serviços através de informações menos técnicas, que podem ser compreendidas pelos utilizadores da rede. Os utilizadores deste plano devem ter capacidade para monitorizar e actuar sobre os serviços que utilizam, sem necessidade de conhecer os seus detalhes de implementação.

  Os acordos estabelecidos ao nível destes planos integram cláusulas relacionadas com a finalidade do serviço, custos de operação e manutenção, rapidez na recuperação de falhas, equipa de suporte técnico, horário de fornecimento do serviço, prioridade do serviço na rede, duração do contrato, penalizações por falta de cumprimento do contrato, etc.

  Neste plano, os contratos têm valor jurídico, sendo denominados CLA (*Customer Level Agreements*).

- **Plano de Serviço:**

  Este plano define os serviços em termos mais técnicos, de acordo com parâmetros de QoS como o atraso, largura de banda, *jitter*, prioridade no encaminhamento, políticas de condicionamento do tráfego, etc.

  Apesar dos acordos deste plano serem definidos a partir dos acordos individuais de cada cliente, envolvem na realidade a especificação de acordos que atendem aos requisitos exigidos pelo tráfego agregado de cada classe de serviço.

  Os acordos deste plano são os denominados SLA (*Service Level Agreements*). O controlo dos requisitos aí especificados é efectuado por um Gestor de Serviços, que tem a responsabilidade de definir, monitorizar e alterar (quando necessário) as políticas de serviço subjacentes ao acordo.

  Um SLA agrupa vários CLA, desde que estes sejam do mesmo tipo do primeiro.

- **Plano de Rede:**

  O Plano de Rede constrói acordos que definem como a infra-estrutura de rede deverá suportar os serviços comercializados através dos CLA e especificados nos SLA.

  Neste plano, o acordo denomina-se TCA (*Traffic Conditioning Agreement*). A sua função é definir parâmetros para os mecanismos de gestão das filas e para os algoritmos de encaminhamento dos pacotes que circulam na rede que suporta o serviço.

- **Plano de Administração:**

  Este plano define as actividades de gestão que permitem a coordenação dos outros três planos do modelo.

A coordenação entre todos os planos é de extrema importância, pois só assim será possível assegurar que as alterações ao contrato CLA se reflectem em todos os níveis.

Bandwidth Broker

Do ponto de vista de um encaminhador *DiffServ*, a implementação de funções de tratamento diferenciado depende de três acções base: definição das classes que vão receber os pacotes, associação dos recursos a cada uma das classes e associação dos pacotes às mesmas. O modelo *DiffServ* define a forma de implementação da primeira e da terceira acção. Para tratar da segunda componente (associação dos recursos a cada uma das classes), o RFC 2638 [36] define um mecanismo denominado *Bandwidth Broker*.

Um *Bandwidth Broker* é assim um elemento que conhece as políticas de QoS definidas para uma determinada rede *DiffServ* e, com base nesse conhecimento, faz a gestão da alocação de recursos às aplicações. Trata-se de um componente que pode actuar na fronteira de um domínio *DiffServ*, estabelecendo relações de vizinhança com pares de domínios adjacentes. Desta forma é possível manter coerência na alocação de recursos entre diferentes domínios e fornecer serviços com QoS fim-a-fim.

Uma das funções básicas implementadas por estes componentes é o controlo de admissão. Com esta função, o *Bandwidth Broker* garante que só são admitidos novos fluxos de tráfego na rede se os mesmos não influenciarem negativamente o desempenho dos fluxos existentes.

A utilização de *Bandwidth Brokers* não está restrita a domínios *DiffServ*, existindo actualmente inúmeros projectos em desenvolvimento em torno deste conceito.

Considerações adicionais

Apesar de ser escalável, o *DiffServ* não oferece garantia rígida de recursos para todos os fluxos, como o modelo *IntServ*.

As reservas de recursos são feitas para agregações, ou seja, grandes conjuntos de fluxos, não existindo simultaneamente um mecanismo de controlo de admisão explícito. Este facto leva a que um fluxo individual possa não atingir as suas necessidades mínimas em termos de parâmetros de QoS, como largura de banda disponível ou atraso, por exemplo.

Por outro lado, o modelo *IntServ* fornece garantia de reserva de recursos para fluxos individuais, mas não é facilmente escalável, como foi referido anteriormente.

Neste sentido, existe actualmente a tendência para a construção de uma arquitectura de QoS fim-a-fim, com base no melhor de cada um destes dois modelos [61].

Pode-se assim usar o modelo *IntServ*, com um mecanismo de reserva de recursos e controlo de admissão (por exemplo o protocolo RSVP), nos extremos de uma ou mais regiões *DiffServ*. No núcleo dessas Regiões usar-se-ão mecanismos *DiffServ*, como meio agregador (em classes) dos fluxos individuais de tráfego gerados pelas aplicações.

Capítulo 4

Implementação de Serviços VoIP numa Rede de Campus: O caso do Instituto Politécnico de Bragança

4.1 O Instituto Politécnico de Bragança

O Instituto Politécnico de Bragança (IPB) é uma instituição portuguesa de ensino superior politécnico que conta, no ano lectivo de 2008/09, com aproximadamente 6700 alunos e mais de 300 docentes. É actualmente constituído por cinco escolas, distribuídas por três pólos:

- Campus de Santa Apolónia em Bragança, onde se localizam as três maiores escolas: Escola Superior Agrária (ESA), Escola Superior de Educação (ESE) e Escola Superior de Tecnologia e de Gestão (ESTiG). Encontram-se ainda neste campus os Serviços Centrais, Serviços de Acção Social e três residências de estudantes.
- Instalações da Escola Superior de Saúde (ESSA), em Bragança, localizada a aproximadamente 1 Km do Campus de Santa Apolónia.
- Instalações da Escola Superior de Tecnologia e Gestão de Mirandela (ESTGM), em Mirandela.

4.2 A Rede de Dados do IPB

A rede de dados do IPB é baseada numa infra-estrutura recente, com equipamentos activos actuais, permitindo assim a implementação de novos serviços aos utilizadores.

Entre as principais características desta rede destacam-se:

- backbone do Campus (figura 4.1) e Rede de distribuição baseados inteiramente na norma Gigabit Ethernet em fibra óptica, com suporte de IEEE 802.1Q (VLANs) e IEEE 802.1p (Qualidade de Serviço ao nível dois do modelo OSI);
- sistema horizontal maioritariamente constituído por ligações comutadas Fast-Ethernet, com suporte de IEEE 802.1Q e 802.1p em boa parte dos pontos;

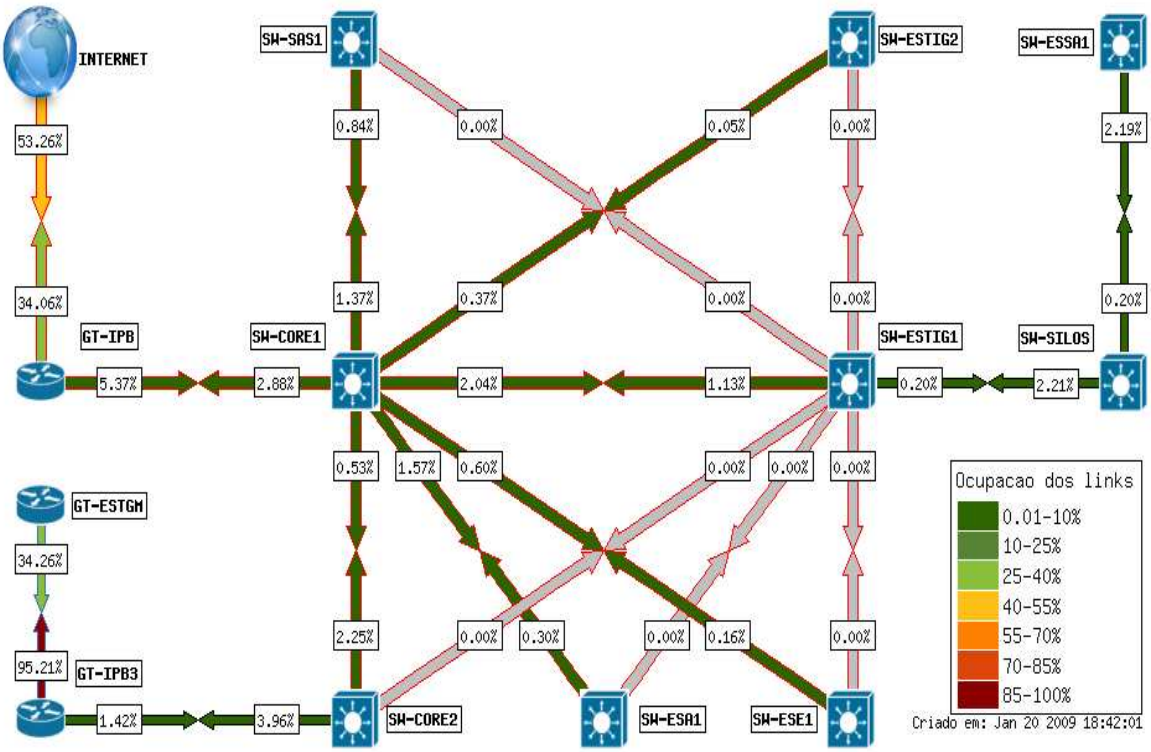

Figura 4.1: Topologia do Backbone da Rede de Dados do IPB

- Rede Wi-Fi com cobertura generalizada dos edifícios do IPB (130 pontos de acesso), incluindo residências de estudantes. Trata-se de uma rede inteiramente baseada na norma 802.11g (54 Mbps), sendo actualmente usada regularmente por mais de 50% da comunidade académica desta instituição;

- rede WAN: o acesso à Internet é efectuado através da RCTS - Rede Ciência, Tecnologia e Sociedade, com um débito actual de 100 Mbps. A ligação de dados entre o Campus de Santa Apolónia e a ESTGM é garantida por um circuito dedicado de 4 Mbps. A ligação do Campus para a ESSA é baseada numa ligação laser FSO, com um débito de 100 Mbps.

4.3 A Rede Telefónica do IPB

Um dos motivos que levou ao desenvolvimento do projecto VoIP@IPB, descrito adiante, foram as limitações identificadas na rede actual de voz do IPB, em conjunto com a identificação das potencialidades oferecidas pela actual rede de dados desta Instituição.

O Campus de Santa Apolónia é servido por duas centrais telefónicas (PBX[1]) de marca Matra, interligadas entre si através de um acesso Primário RDIS com suporte de 30 canais simultâneos. Esta rede disponibiliza 542 extensões telefónicas

[1]Private Branch Exchange

com acesso directo ao exterior e 50 extensões sem acesso directo ao exterior. O acesso ao exterior é assegurado por três acessos primários RDIS (90 canais de voz simultâneos): 2 no PBX da ESTiG e 1 no PBX da ESA. Nos pólos remotos (ESSA e ESTGM) existem pequenas centrais RDIS, com um limitado número de extensões internas. Em cada um destes locais, o acesso ao exterior é assegurado por um acesso básico RDIS (2 canais de voz simultâneos).

Entre as principais limitações do actual sistema de comunicação de voz do IPB destaca-se:

- PBX com idade bastante significativa e tecnologicamente ultrapassados;
- capacidade de expansão (novas extensões) praticamente esgotada;
- impossível a adição de novas cartas para acesso directo a partir do interior às redes GSM (para implementação de um mecanismo baseado na rota de menor custo). Esta limitação implica actualmente elevados custos para estas redes GSM;
- taxação detalhada por extensão não implementada;
- não é possível identificar a origem de eventuais abusos de utilização a partir da rede interna;
- gestão corrente das funcionalidades dos PBX dependente de empresa externa;
- serviços ao utilizador muito limitados. O sistema apenas permite o estabelecimento e recepção de chamadas e pouco mais...
- ligação dos pólos remotos (ESTGM e ESSA) é feita pelas linhas externas.

A figura 4.2 sintetiza as infra-estruturas de voz nos três pólos.

4.4 O Projecto VoIP@IPB

A evolução verificada durante a última década, ao nível das tecnologias, meios de comunicação e protocolos aplicacionais, a par da progressiva desactualização tecnológica da infra-estrutura de voz do IPB levou-nos a considerar o desenvolvimento de um projecto piloto para implementação e teste de serviços VoIP nesta Instituição.

O projecto VoIP@IPB [67] surgiu assim com o objectivo de efectuar experimentação com serviços de Telefonia IP sobre a rede de dados do IPB, para avaliar do seu potencial interesse futuro para a Instituição.

Os objectivos concretos definidos para o Serviço VoIP@IPB são os seguintes:

1. Disponibilizar um serviço de Telefonia IP à comunidade do IPB, tirando partido da rede de dados existente, com as seguintes características:
   - 1 endereço SIP para cada aluno e funcionário
   - serviço de voicemail, integrado com e-mail

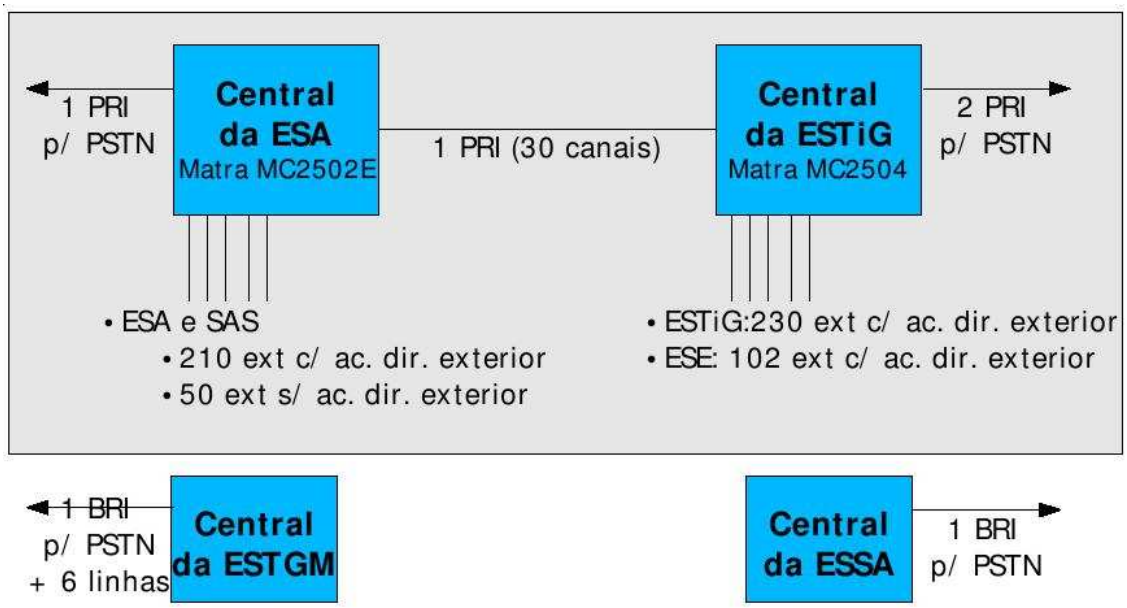

Figura 4.2: A Rede telefónica interna do IPB

- funcionalidades de gestão de chamadas em espera
- funcionalidades de música para as chamadas em espera
- suporte de conferência (áudio e vídeo)
- mecanismo de notificação de chamadas perdidas, etc

2. Interligação desta infra-estrutura com a rede telefónica interna e com a Rede Telefónica Pública

3. Interligação dos pólos remotos (ESTGM e ESSA) com a rede telefónica do Campus, usando tecnologia VoIP sobre os circuitos de dados existentes

4. Avaliar a viabilidade (financeira e técnica) de substituição da infra-estrutura telefónica actual (PBX e cablagem independentes) por uma alternativa *full-VoIP*.

4.4.1 Arquitectura do Sistema

O piloto de VoIP em implementação no IPB é baseado em plataformas e ferramentas opensource, ao nível dos elementos da componente servidor. O núcleo do sistema é constituído por dois Servidores:

- Proxy SIP, com funções de *registrar server*, *location server* e router/proxy;
- Media Gateway (PBX IP) para interligação da rede SIP com outras redes, como a PSTN[2], Rede telefónica interna e Redes GSM.

A figura 4.3 apresenta a arquitectura geral do projecto VoIP@IPB.

[2]Rede Telefónica Pública Comutada

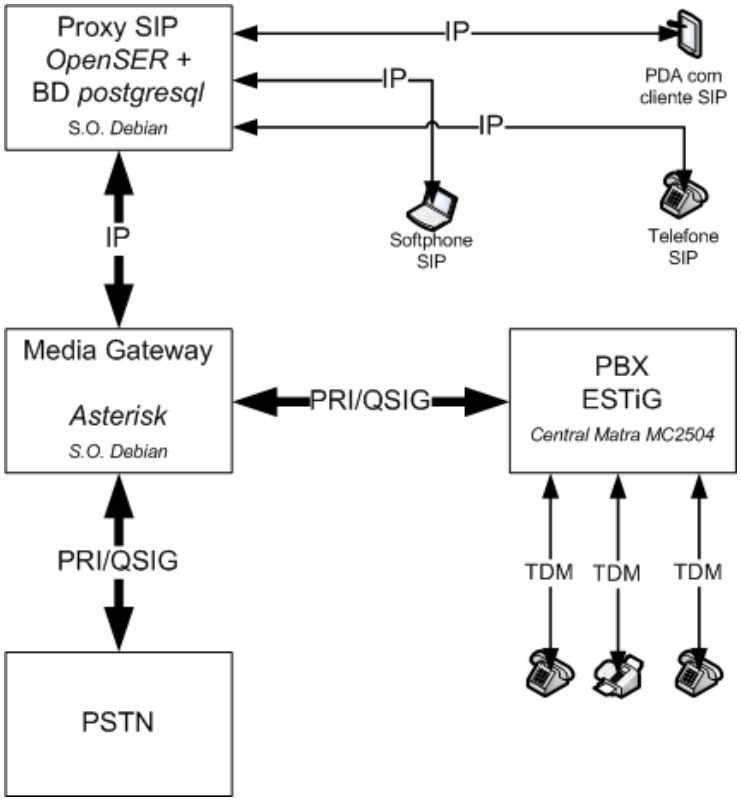

Figura 4.3: Arquitectura do projecto VoIP@IPB

Proxy SIP

De entre as diferentes alternativas actuais de Servidores SIP opensource, o *OpenSER* (*Open SIP Express Router*) [63] tem vindo a ganhar grande popularidade, fundamentalmente devido à sua elevada performance, modularidade e flexibilidade de configuração.

Entre as suas principais características destacam-se:

- implementação bastante completa do protocolo SIP, com suporte de SIP sobre TCP ou UDP, em conformidade com o RFC3261 [62];
- suporte de ENUM [66]. Este mecanismo utiliza o sistema de DNS para estabelecer uma relação entre o sistema de numeração telefónico (E.164) e os mecanismos de identificação da Internet, como um URI SIP, por exemplo;
- suporte de diversos mecanismos de atravessamento de redes com NAT;
- suporte de lookups de DNS SRV;
- suporte de múltiplos domínios DNS de utilizador em paralelo;
- sendo modular, são facilmente adicionáveis novos módulos para extensão das funcionalidades.

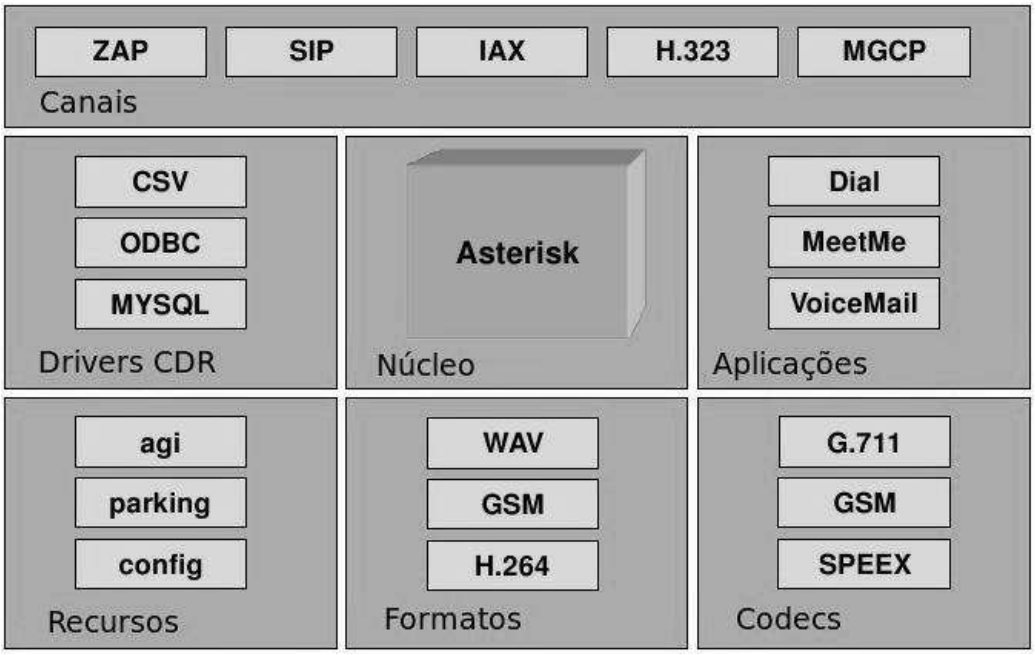

Figura 4.4: Arquitectura do *Asterisk*

As funções de registo de utilizadores, autenticação e contabilização são asseguradas pelo Proxy SIP, sedo esta informação armazenada permanentemente num Servidor de base de dados relacional (*postgresql*).

O serviço VoIP tem dificuldades especiais de funcionamento quando um ou os dois extremos da comunicação estão por detrás de diferentes mecanismos de NAT. O *OpenSER* resolve em boa medida este problema, através de um módulo *nathelper*, que recorre a um programa externo de proxy RTP (*rtpproxy ou mediaproxy*), através do qual passam todos os pacotes de uma comunicação entre dois terminais VoIP que se encontram na mesma situação.

Media Gateway

O *OpenSER* é um excelente servidor de SIP, com uma implementação bastante completa da generalidade dos métodos e funcionalidades deste protocolo, mas não passa disso. Sempre que é necessário garantir comunicação da rede SIP com outras redes, como por exemplo a PSTN, é necessário recorrer a outro componente, normalmente denominado de *Media Gateway*. Neste domínio, o software *Asterisk* [64] tem-se apresentado como a solução mais interessante, no campo dos PBX IP baseados em software opensource.

Trata-se de uma plataforma que suporta interacção com os mais variados tipos de protocolos e equipamentos de VoIP. Suporta, entre outros, os protocolos SIP, H323 e IAX, bem como a implementação de diversos serviços complementares, como voicemail integrado com o e-mail, gestão de conferências, mecanismos de *Interactive Voice Response* (IVR), etc. A figura 4.4 apresenta graficamente a arquitectura do *Asterisk*.

Em resumo, e justificando a opção da escolha do *Asterisk* para a função de *Media*

Gateway do projecto VoIP@IPB, trata-se de um Servidor que permite a interligação da rede SIP com a PSTN e rede telefónica interna e ainda disponibilizar um conjunto alargado de serviços adicionais aos utilizadores, como o voicemail, gestão de chamadas em espera, música para utilizadores em espera, etc.

A interligação do *Asterisk* com a rede TDM (Rede telefónica interna e PSTN) é normalmente efectuada através de canais Zaptel[3]. Estes canais são fornecidos pela API Zaptel, criada originalmente por Jim Dixon e entretanto desenvolvida pela empresa *Digium* [65], actuando como mecanismo de interface entre o hardware TDM (cartas BRI ou PRI) e o sistema operativo de um computador.

Existem actualmente no mercado diversos módulos de hardware, a preços bastante acessíveis, que funcionam com base nos drivers Zaptel e suportam diversos tipos de interfaces TDM, nomeadamente interfaces de acesso básico RDIS (BRI) e de acesso primário RDIS (PRI). A sua interligação pode ser feita directamente com as linhas do operador de comunicações tradicional ou com o PBX da rede telefónica da instituição, desde que este tenha um interface do mesmo tipo disponível. Ao nível protocolar, a interligação do *Asterisk* com o PBX utiliza o protocolo QSIG, que terá de ser suportado de ambos os lados da comunicação. O QSIG é protocolo de sinalização entre PBX, baseado no protocolo Q.932 da norma RDIS.

No caso específico do projecto VoIP@IPB, foi usada uma carta TDM *Digium Wildcard TE210P*, com dois interfaces de acesso primário RDIS. O primeiro interface interliga o Servidor *Asterisk* com o PBX da ESTiG, permitindo assim a comunicação da rede VoIP com a rede telefónica interna. O segundo interface interliga o mesmo servidor à rede PSTN, permitindo desta forma o acesso à rede telefónica pública fixa e móvel.

4.4.2 Níveis de Serviço

A coexistência de tráfego VoIP com outros tipos de tráfego IP, ao nível de uma rede local tão heterogénea como a de uma Instituição de Ensino Superior, requer particular atenção a dois níveis: qualidade de serviço e segurança. Esta questão será abordada de forma mais detalhada no próximo capítulo.

Tendo em atenção estes dois factores, a implementação do projecto VoIP@IPB implicou a definição de dois tipos de serviço, com implicações ao nível da criação de uma VLAN específica sobre a infra-estrutura de rede local (figura 4.5):

- *Serviço Premium*: implementado sobre uma VLAN própria, com activação de mecanismos de QoS de nível 2 ao longo de toda a infra-estrutura de suporte a este serviço. Estará disponível em locais do campus cuja infra-estrutura de rede suporte estes mecanismos, incluindo a rede Wi-Fi.

  Trata-se de um serviço a que só terão acesso terminais exclusivamente VoIP (*hard-phones* SIP ligados à rede cablada ou à rede Wi-Fi), depois de devidamente autenticados. Este serviço inclui a possibilidade de comunicação com outros terminais SIP, comunicação de e para a rede telefónica interna e para o exterior (PSTN), em função do perfil do utilizador autenticado.

[3]abreviatura de *Zapata Telephony*

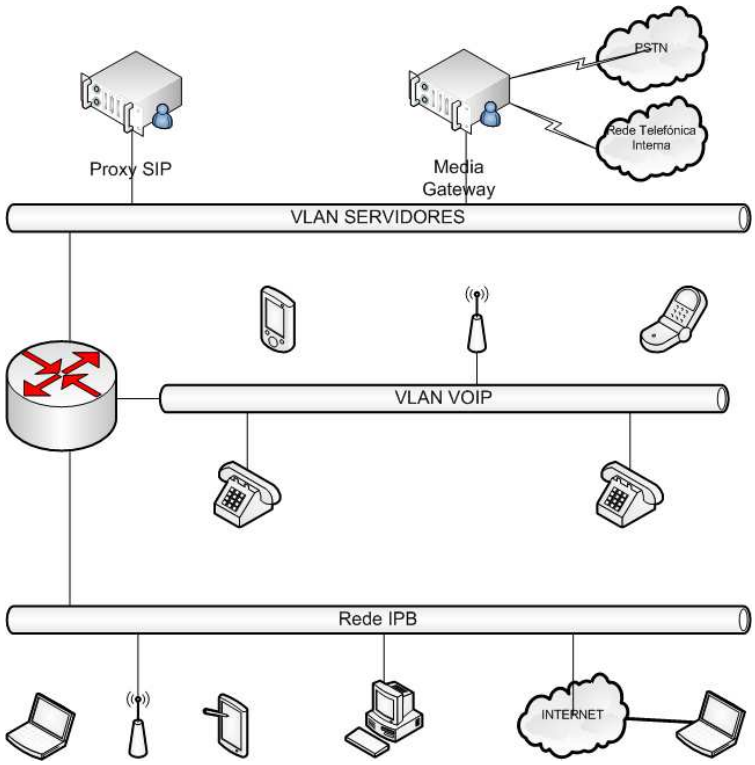

Figura 4.5: Topologia de Rede usada pelo projecto VoIP@IPB

- *Serviço Standard*: acessível a partir de qualquer ponto da rede de dados do IPB, podendo ser utilizado com *hard-phones* ou com *soft-phones* instalados em computadores. Permite a comunicação com outros terminais SIP, com a rede telefónica interna do IPB e com a PSTN, em função do perfil do utilizador.

  Funcionando sobre as VLAN de dados normais da instituição, o utilizador deste serviço não deve esperar um tratamento diferenciado do tráfego VoIP, pelo que o grau de disponibilidade e qualidade de serviço serão inferiores ao serviço *Premium*.

4.4.3 Plano de endereçamento VoIP

Um URI SIP, definido em [62], permite a identificação de utilizador deste serviço através de um endereço com um formato conhecido e de uso generalizado na Internet (idêntico a um endereço de e-mail): *sip:utilizador@dominio*. No entanto, a interação do serviço SIP com outras redes não SIP não pode ser baseado neste endereço, já que, nomeadamente a rede TDM convencional sempre baseou a identificação dos extremos de comunicação apenas num conjunto de dígitos, de acordo com a norma internacional E.164. Num telefone convencional apenas temos, na maior parte dos casos, a possibilidade de marcar os dígitos de zero a nove e alguns caracteres especiais (+, * e #), não sendo possível introduzir um endereço SIP para identificar um utilizador baseado neste protocolo.

Para ultrapassar a limitação atrás descrita, torna-se necessário associar um endereço alternativo, baseado unicamente nos dígitos 0 a 9, a cada utilizador SIP. No projecto VoIP@IPB, cada utilizador é primariamente identificado por um URI SIP, no formato *sip:utilizador@ipb.pt* ou *sip:utilizador@alunos.ipb.pt*, em função do tipo de utilizador. Complementarmente, é associado a cada utilizador um *alias* SIP inteiramente numérico.

A definição deste *alias* SIP é baseada, para os funcionários do IPB, na extensão telefónica interna TDM que já lhes está atribuída. Neste sentido, importa apresentar o plano de endereçamento telefónico TDM do IPB:

- Prefixo externo: 27330
  - Extensões Internas: 3000 a 3199: alocadas à ESTiG
  - Extensões Internas: 3200 a 3399: alocadas à ESA e Serviços de Acção Social
- Prefixo externo: 27333
  - Extensões Internas: 3600 a 3710: alocadas à ESE (do exterior o 3 é substituído por 0)

Com base nesta informação, a obtenção dos URI e *alias* SIP é determinada pelas seguintes regras:

- URI SIP:
  - Funcionários: *login@ipb.pt* (ex: maria@ipb.pt)
  - Alunos: *login@alunos.ipb.pt* (ex: a12345@alunos.ipb.pt)
- Alias SIP:
  - Funcionários (Campus Sta Apolónia): *5x3yyy*, onde
    - *x*: um dígito, entre 0 e 9 (começando em 0), para desempate entre vários utilizadores com a mesma extensão interna TDM
    - *3yyy*: tem correspondência directa com a Extensão Interna TDM actual
  - Funcionários (ESTGM): *504zzz*, onde *z* é um valor incremental, começando em 0
  - Funcionários (ESSA): *505zzz*, onde *z* é um valor incremental, começando em 0
  - Alunos do IPB: *4zzzzz*, onde *zzzzz* corresponde ao número mecanográfico do aluno

Figura 4.6: Interface de activação e configuração do serviço VoIP@IPB

4.4.4 Estado actual do Projecto

O projecto VoIP@IPB foi iniciado em Maio de 2005. Encontram-se actualmente em operação os servidores previstos e anteriormente referidos:

- Servidor SIP, com software *OpenSER* (versão 1.0.1), actua como *registrar*, *location* e proxy entre terminais SIP. O registo, autenticação e contabilização da utilização está a ser efectuado no Servidor de base de dados *postgresql*, instalado fisicamente na mesma máquina. Ao nível do hardware, destacam-se os seguintes parâmetros: 1 Processador Intel Xeon a 3 GHz; 2 GB de memória RAM, 2 discos SCSI de 40 GB cada.

- *Media Gateway*, com software *Asterisk* (versão 1.4.18) e uma placa *Digium Wildcard TE210P* para interligação com o mundo TDM. Esta equipamento está instalado numa plataforma de hardware com as mesmas características do servidor SIP.

Complementarmente à instalação e parametrização das plataformas descritas, foi desenvolvido um novo módulo para o portal interno de gestão dos serviços de rede

Figura 4.7: Agenda telefónica com indicação dos utilizadores online

(http://myconfig.ipb.pt), onde os utilizadores do IPB podem efectuar a activação do serviço e configurar opções adicionais (figura 4.6).

Tirando partido do armazenamento em base de dados da informação de *accounting* e das funcionalidades de *Application Server* do *Asterisk*, foram desenvolvidos um conjunto de serviços complementares, dos quais se destacam os seguintes:

- Agenda telefónica online - http://voip.ipb.pt - (figura 4.7), com os contactos dos utilizadores aderentes ao serviço e indicação daqueles que se encontram no momento online. É ainda possível nesta página associar uma aplicação por defeito para o serviço SIP, o que permite que, um click em cima de um endereço do tipo sip:utilizador@dominio, execute automaticamente a aplicação associada e inicie uma chamada para esse endereço;

- Notificação de chamadas perdidas (figura 4.8): foi desenvolvida uma *script* que analisa em tempo real os registos produzidos pelo servidor SIP e guardados na base de dados, despoletando automaticamente o envio de um e-mail para um utilizador que foi objecto de uma chamada perdida. Este serviço pode ser activado/desactivado por cada utilizador, no portal interno de gestão dos serviços de rede referido anteriormente.

- Voicemail, integrado com email (figura 4.9). Esta funcionalidade pode ser activada pelo utilizador no portal *myconfig.ipb.pt* e permite, tal como o próprio

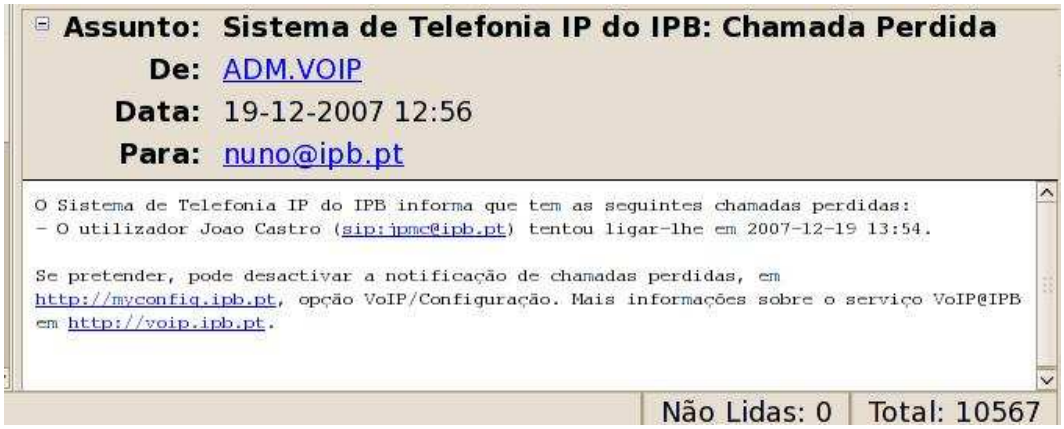

Figura 4.8: Exemplo de email com alerta de chamada perdida

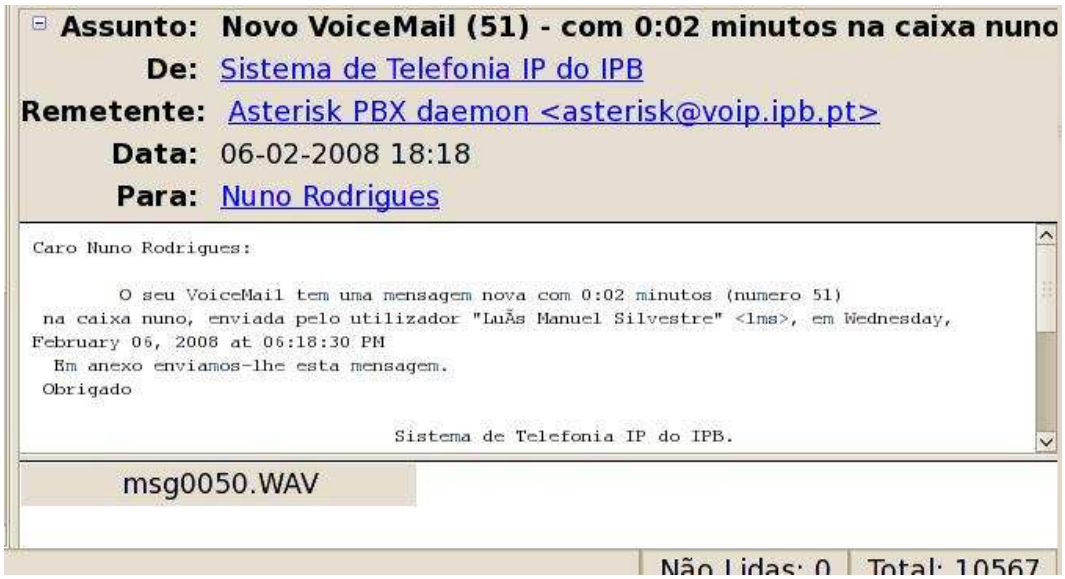

Figura 4.9: Exemplo de email com mensagem de voicemail

nome indica, que o utilizador receba uma mensagem de voz na sua caixa de correio electrónico, caso não atenda a chamada telefónica VoIP.

À data de 23 de Janeiro de 2009, existiam 819 utilizadores aderentes ao Serviço, dos quais 169 são funcionários (docentes e não docentes) e os restantes 650 são alunos.

A política de utilização do serviço define níveis de acesso, em função do tipo de utilizador. Assim, os funcionários podem efectuar chamadas telefónicas através deste serviço com base nas mesmas regras que se aplicam à sua extensão telefónica interna TDM. Ou seja, se um utilizador pode efectuar chamadas telefónicas internas, locais, nacionais e para redes móveis na extensão interna TDM, pode usar a extensão VoIP exactamente com as mesmas condições/restrições.

Já aos alunos é aplicado um perfil padrão, que define a possibilidade de efectuar chamadas telefónicas para outros utilizadores SIP e para a rede telefónica interna TDM do IPB.

4.5 O projecto VoIP@RCTS

Em Dezembro de 2006, a FCCN[4] decidiu avançar com um projecto a nível nacional para criação de uma Rede de VoIP sobre a infra-estrutura da RCTS. Entre os objectivos deste projecto, está a migração do tráfego de voz entre as instituições ligadas à RCTS e a PSTN para a rede RCTS. Desta forma, todas as chamadas telefónicas entre instituições ligadas à RCTS terão custo zero, já que as mesmas serão transportadas através da infra-estrutura da RCTS já existente. Todo o tráfego de Voz para fora da RCTS será encaminhado por esta rede através de trunks SIP, estabelecidos sobre túneis L2TP[5] até aos operadores de telecomunicações contratados. É possível, desta forma, a contratualização de tráfego de forma agregada, permitindo assim a obtenção de preços por segundo mais baixos, por efeito de contratação destes serviços em larga escala (um único concurso de serviços de voz para todas as instituições aderentes ao projecto).

Da página de apresentação do projecto [68], pode retirar-se a seguinte descrição, que clarifica os seus objectivos:

"O projecto VoIP@RCTS resulta de um contrato de finaciamento do POSC Programa Operacional para Sociedade do Conhecimento e tem como objectivo dotar as instituições de ensino superior público com ligação à RCTS das infra-estruturas necessárias ao transporte do tráfego de voz dentro desta rede e num ambiente convergente, integrado e seguro. Este projecto foi homolgado em Setembro de 2006 e tem a duração prevista de 2 anos.

A VoIP@RCTS será uma rede que interligará todos os sistemas telefónicos de todas as instituições aderentes mediante utilização do backbone de alto desempenho da RCTS, promovendo desta forma a agregação da procura e entrega centralizada e segura de tráfego em operadores de telecomunicações.

Estima-se que a implementação deste projecto conduza a uma redução de custos na ordem dos 30% nas componentes de locação de infra-estruturas (lacetes locais e centrais telefónicas) e tráfego (tarifário de chamadas). Com efeito imediato, o tráfego telefónico entre instituições aderentes e outras redes VoIP existentes no mundo académico, passa a ser gratuito."

Vendo este projecto da FCCN como uma excelente oportunidade de extender o alcance e objectivos anteriormente definidos para o projecto VoIP@IPB, o IPB aderiu ao mesmo, desde o início, com o maior dos entusiasmos. Se o projecto do IPB visava fundamentalmente a implementação de serviços VoIP voltados para o interior da Instituição, o projecto da FCCN vem complementar o primeiro, permitindo a extensão destes serviços ao exterior.

Na sequência dos objectivos traçados pela FCCN e em função do levantamento de requisitos efectuado em conjunto pelas equipas da FCCN e do IPB, foi elaborado, pela primeira entidade, um projecto de implementação que define a arquitectura final a implementar e sumariamente apresentada na figura 4.10[6].

[4]Fundação para a Computação Científica Nacional: entidade que gere a RCTS - Rede Ciência Tecnologia e Sociedade

[5]L2TP: *Layer 2 tunneling protocol*

[6]Figura retirada do documento *Guião de Instalação do projecto VoIP@RCTS - Instituto Politécnico de Bragança*, elaborado pela FCCN em Abril de 2008

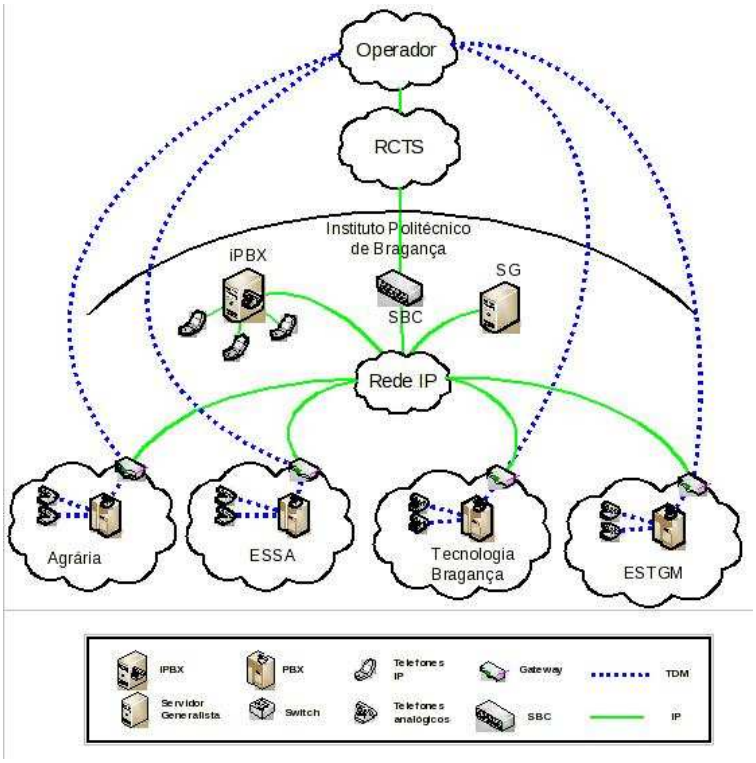

Figura 4.10: Arquitectura do projecto VoIP@RCTS a implementar no IPB

Da arquitectura proposta fazem parte os seguintes componentes:

- *Media Gateway*: equipamentos responsáveis pela interligação entre a rede TDM e a rede IP. Permitem a ligação dos PBX convencionais à Rede VoIP e asseguram as linhas de backup para a PSTN, em caso de falha dos trunks SIP estabelecidos com os operadores telefónicos a quem é contratado o serviço telefónico para fora da RCTS.

- SBC - *Session Border Controller*: equipamento colocado na fronteira da rede de cada instituição, que possibilita a interligação entre as diferentes redes de Voz e por onde passará toda a sinalização e tráfego de voz. É utilizado como elemento fundamental de protecção da rede interna SIP da instituição.

- Servidor Generalista (SG): equipamento de suporte aos serviços de *accounting*, *billing* e monitorização.

- iPBX - Central telefónica IP: equipamento responsável pelo fornecimento de serviços de telefonia IP complementares ao serviço oferecido pelas centrais telefónicas convencionais, nomeadamente para suporte a terminais SIP. No caso do projecto do IPB, este equipamento será integrado com o Servidor SIP já instalado no âmbito do Projecto VoIP@IPB.

- PBX: Centrais telefónicas existentes na rede telefónica da instituição, responsáveis pela sinalização, plano de numeração, encaminhamento e confi-

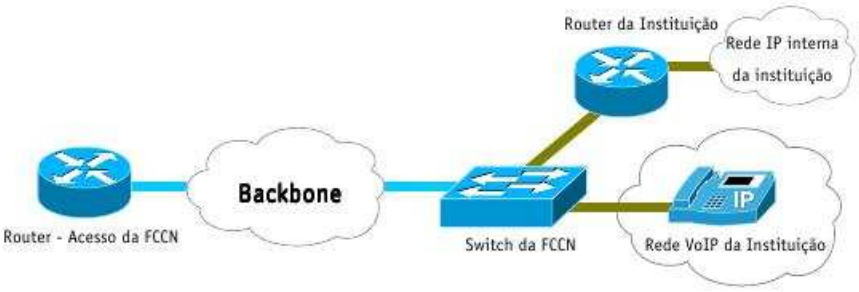

Figura 4.11: Arquitectura WAN de suporte ao projecto VoIP@RCTS a implementar no IPB

guração de chamadas que permitem a gestão das extensões telefónicas convencionais.

Em Janeiro de 2009, o projecto encontra-se numa fase decisiva de implementação, prevendo-se para muito curto prazo o estabelecimento dos trunks SIP com os operadores vencedores do concurso de voz e a consequente entrada em produção de toda a infra-estrutura.

4.5.1 Modelo de QoS

Um dos objectivos fundamentais deste projecto é passar a encaminhar o tráfego de voz das instituições pela mesma rede de dados que é usada para o acesso à Internet. É reconhecido que estas ligações das redes locais das Instituições de Ensino Superior à Internet são pontos que sofrem habitualmente de congestionamento, desde que não sejam implementadas medidas específicas de condicionamento e controlo do tráfego que por aí circula. Trata-se portanto de pontos especialmente sensíveis para se garantir um funcionamento adequado deste projecto.

Com o objectivo de minimizar o impacto destas fragilidades, a FCCN definiu um Modelo de QoS, cuja topologia física se apresenta na figura 4.11 e cujos aspectos mais importantes se descrevem de seguida:

- o tráfego VoIP sofrerá uma marcação *DiffServ*, com o DSCP **EF** (valor 46).
- o switch representado na figura 4.11 tem como principal função o policiamento do tráfego de saída da Instituição, garantindo que o tráfego VoIP não é afectado pelo restante tráfego.
- o tráfego VoIP que chega a este switch é colocado numa fila configurada em modo *priority queue*. Desta forma, todo o tráfego que chega a esta fila é sempre tratado em primeiro lugar.

Não tendo entrado este projecto ainda em fase de produção, é praticamente impossível neste momento fazer uma análise detalhada acerca da adequabilidade deste modelo em funcionamento real.

Com base nestas conclusões, é objectivo do trabalho desenvolvido no âmbito da presente dissertação proceder a um conjunto de testes, em ambiente de simulação,

para determinar a adequabilidade da aplicação de um modelo de QoS baseado na *framework DiffServ* a esta situação.

Neste sentido, no Capítulo 5 serão definidos os requisitos de QoS necessários a um correcto funcionamento de um Serviço VoIP e, no Capítulo 6, proceder-se-á à realização de um conjunto de experiências e consequente análise dos resultados obtidos.

Capítulo 5

Implementação de QoS para suporte de Serviços VoIP

5.1 Requisitos de QoS para serviços VoIP

A implementação de Serviços de Voz usando a infra-estrutura de comunicação de dados das organizações começa, hoje em dia, a ser uma realidade cada vez mais presente.

Tradicionalmente, os serviços de voz foram implementados, desde há mais de um século, sobre infra-estruturas dedicadas e desenhadas especificamente para este fim, operadas pelos tradicionais operadores de telecomunicações. Entre as principais características destes sistemas tradicionais está a percepção, generalizadamente assumida pelos utilizadores, de que este serviço apresenta uma elevada taxa de disponibilidade. É comum os operadores e fabricantes de equipamentos de telefonia tradicional terem como objectivo, os chamados *cinco noves*: 99,999% de disponibilidade do serviço. Este valor significa um tempo de indisponibilidade média inferior a 5,3 minutos por ano. Trata-se de um valor difícil de ser atingido em muitas das redes de dados actuais, já que esta disponibilidade é influenciada por vários factores, que vão desde as questões da alimentação eléctrica da infra-estrutura até ao nível aplicacional.

A obtenção destes níveis de disponibilidade numa rede de dados só se consegue através da implementação de infra-estruturas altamente redundantes, em conjunto com boas práticas de planeamento, desenho, implementação e operação.

Entre os factores que contribuem para a elevada disponibilidade da Rede Telefónica Comutada Pública (PSTN[1]) está o facto de ser baseada numa arquitectura TDM[2], que oferece um serviço de comutação de circuitos com características especialmente adequadas ao transporte de voz.

Por outro lado, as redes de dados da actualidade são maioritariamente baseadas no protocolo IP, que funciona com base num princípio de comutação de pacotes e oferece um serviço do tipo *best-effort*. Por outras palavras, este protocolo IP não oferece qualquer garantia de entrega ou sequer limites no atraso dos pacotes

[1]PSTN: *Public Switched Telephone Network*
[2]TDM: *Time Division Multiplexiing*

MOS	Qualidade	Efeito
1	Mau	Distorção irritante e desagradável
2	Pobre	Distorção irritante mas não desagradável
3	Razoável	Distorção perceptível e um pouco irritante
4	Bom	Pequeno nível de distorção, não irritante
5	Excelente	Nível de distorção imperceptível

Tabela 5.1: Escala usada pelo MOS

entregues. Estas condições, sendo o oposto dos princípios subjadentes à rede PSTN, são desde logo um obstáculo à implementação de serviços de voz.

Têm vindo a ser desenvolvidos, ao longo dos últimos anos, um conjunto de mecanismos que permitem contrariar o princípio *best-effort* do protocolo IP (já anteriormente abordados no capítulo 3). Ao longo do presente trabalho, pretende-se avaliar a utilização de um destes mecanismos (*framework DiffServ*), para suporte de serviços VoIP em condições aceitáveis. Importa assim, nesta fase, clarificar quais os parâmetros que podem influenciar a qualidade de um serviço de voz e quais os limites aceitáveis para esses mesmos parâmetros.

5.1.1 Métodos de avaliação da Qualidade de Voz

A determinação da qualidade de uma conversação de voz não é um processo inteiramente objectivo, já que pode depender, entre outros parâmetros, da sensibilidade do utilizador que participa na conversação. Têm vindo a ser desenvolvidos, ao longo dos anos, diversos métodos de aferição da qualidade de uma comunicação de voz.

Uma das primeiras abordagens desenvolvidas para determinar a qualidade de uma convesação de voz foi o chamado teste MOS – *Mean Opinion Score*. Trata-se de um método subjectivo, baseado na opinião de um conjunto de avaliadores sobre a qualidade de uma conversação. Estes avaliadores participam numa conversção ou ouvem uma amostra de voz e atribuem uma pontuação, de acordo com a escala apresentada na tabela 5.1.

Assim, o MOS de uma determinada amostra é obtido através do cálculo da média das opiniões formuladas pelos avaliadores.

Trata-se de um método simples e relativamente eficiente de avaliação. Não é no entanto escalável para avaliação, em tempo real, de grandes quantidades de conversações telefónicas. Por este motivo, têm vindo a ser desenvolvidas novas abordagens, baseadas em software, que permitem estimar e quantificar, em tempo real, a qualidade de comunicação de um serviço de VoIP.

Entre os métodos desta categoria, destacam-se:

- PSQM - *Perceptual Speech Quality Measure* (recomendação ITU-T P.861 [70]): Algoritmo baseado num modelo matemático para determinar a degradação de qualidade dos sinais de voz, usando uma escala entre 0 (sem degradação) e 6,5 (total degradação).

Este mecanismo não foi originalmente desenvolvido para ter em conta as perturbações típicas das redes de dados, usadas pelos serviços de VoIP. Para ultrapassar esta limitação, foi desenvolvida a variante PSQM+ e, mais recentemente, o algoritmo PESQ.

- PAMS - *Perceptual Analysis Measurement System*: Método desenvolvido pela *British Telecom*. Usa um algoritmo diferente do PSQM e uma escala de medição de qualidade da voz entre 1 e 5, o que permite estabelecer alguma relação com a escala MOS.

- PESQ - *Perceptual Evaluation of Speech Quality* (recomendação ITU-T P.862 [71]): Mecanismo desenvolvido a partir da combinação de dois mecanismos anteriores (PSQM+ e PAMS) para medir a qualidade fim-a-fim de uma comunicação voz, em condições de rede reais. Pode ser usado sobre diversas tecnologias, como VoIP, ISDN, PSTN, GSM, etc.

5.1.2 Factores de degradação do serviço VoIP

Nas redes TDM, a infra-estrutura aloca um circuito dedicado entre os dois extremos de cada comunicação de voz. Esta abordagem tem a vantagem de oferecer garantias de serviço, já que os recursos alocados na fase de estabelecimento da chamada se mantém por todo o tempo que dura a comunicação. Apresenta no entanto o inconveniente de não suportar a partilha por outros utilizadores dos recursos alocados a uma comunicação mas não usados.

Por outro lado, o protocolo IP permite que o serviço VoIP partilhe os recursos com as restantes aplicações que usam a mesma infra-estrutura de rede mas, em contrapartida, não oferece garantias de serviço. Esta partilha dos recursos pode-se traduzir na degradação das condições oferecidas pela rede para o serviço VoIP operar.

Há um conjunto de factores que contribuem para a degradação do serviço VoIP, desde que se manifestem na rede acima de determinados intervalos limite. Entre os que interferem decisivamente na qualidade de um serviço VoIP destacam-se três: Perda de pacotes, Atraso e *Jitter*.

Perda de Pacotes

Do ponto de vista da infra-estrutura de comunicação, a perda de um pacote ocorre quando o mesmo não atinge o seu destino. Um pacote pode perder-se por vários motivos, nomeadamente sobrecarga de tráfego na rede ou nos *buffers* dos nodos intermédios, falha de um link na rede, avaria nos equipamentos, erros no canal de comunicação, pacotes mal formados, etc.

Na arquitectura protocolar TCP/IP, o protocolo TCP fornece um mecanismo de transmissão fiável fim-a-fim. Tal significa que, no caso de um segmento TCP se perder, o próprio protocolo vai-se encarregar de promover a sua retransmissão. Este mecanismo de retransmissão é fundamental para o normal funcionamento da generalidade dos serviços aplicacionais usados na Internet actual. No entanto, porque se baseia na retransmissão dos segmentos apenas após a detecção da sua falta pelo

destino ou após a ocorrência de um *timeout*, este mecanismo tende a ser demasiado lento para os chamados serviços de tempo real, como o caso do VoIP. Tal significa que, se usarmos TCP, enquanto se processa a recuperação de um segmento perdido a conversação vai avançando. Portanto, quando o segmento recuperado estiver em condições de ser entregue à aplicação, já não fará sentido a reprodução do respectivo conteúdo, visto que contém informação que entretanto está já desactualizada. Neste caso o segmento será considerado osbsoleto e será descartado.

Por este motivo, a generalidade dos serviços de tempo real recorrem ao protocolo de transporte UDP. Trata-se de um protocolo que não fornece qualquer mecanismo de recuperação de pacotes perdidos mas, em contrapartida é mais rápido que o TCP, porque tem uma estrutura mais leve que este. Assume-se assim, com este princípio, que é mais importante assegurar a chegada constante e rápida dos pacotes do que a eventual ocorrência de algumas perdas (desde que dentro de limites toleráveis).

Apesar da generalidade dos *codecs* usados em serviços VoIP suportarem algum nível de perdas, o serviço degrada-se significativa e rapidamente se este valor crescer para lá dos limites toleráveis. Não existem tabelas padronizadas para definição do limite máximo de perdas tolerável por cada *codec*. Por exemplo, os equipamentos do fabricante Cisco requerem um nível de perdas inferior a 1%, quando em uso o codec G.729 [72]. Em [74] refere-se também que um dos requisitos para um serviço VoIP funcionar de acordo com o previsto é a existência de uma **taxa de perdas inferior a 1%**.

Atraso

A latência, ou atraso fim-a-fim, é o tempo total desde que uma unidade de dados é transmitida até que chega ao destino. É normalmente considerado um dos factores críticos para o bom funcionamento de um serviço VoIP. Operando este serviço em tempo real, facilmente se compreende porquê. Se a latência ultrapassar determinados limites, então a conversação deixa de ocorrer em tempo real, o que na prática inviabiliza o funcionamento do serviço.

A norma G.114 da ITU-T [73], define que, para mantermos uma conversação de voz perceptível entre dois interlocutores, o atraso não deve ultrapassar os **150 ms em cada sentido**. Desta forma, os 150 ms são normalmente considerados o valor máximo de referência para o atraso num sentido, neste tipo de serviços.

Este valor de atraso é normalmente influenciado por dois factores:

- processamento protocolar: inclui o tempo necessário à digitalização e eventual compressão dos sinais de voz (e vice-versa), nos extremos da comunicação. Este tempo depende normalmente do *codec* em uso.

- propagação dos sinais no meio de comunicação: este componente inclui igualmente os tempos consumidos nas filas e no processamento dos pacotes de voz pelos equipamentos intermédios.

Jitter

O *jitter* mede, numa rede de dados, a variação do atraso fim-a-fim. Ou seja, dá-nos uma medida da variação ao longo do tempo do parâmetro atraso. Numa conversação

de voz, os fluxos de pacotes devem chegar ao receptor numa cadência constante e, de preferência, ao mesmo ritmo com que foram gerados no emissor.

Se este valor for demasiado grande, mesmo que o atraso se mantenha sempre dentro de limites aceitáveis, a qualidade da comunicação vai decrescer até se tornar inaceitável. Uma das formas de minimizar o efeito do *jitter* passa pela utilização de *buffers* nos sistemas de destino, por forma a harmonizar o mais possível a cadência de reprodução dos sinais de voz.

De acordo com [74], a qualidade de um serviço VoIP fica irremediavelmente afectada com valores de *jitter* **superiores a 30 ms**.

5.1.3 Nível de Serviço do Projecto VoIP@RCTS

Como referido na secção anterior, há três factores que influenciam decisivamente a funcionalidade de um serviço VoIP: perda de pacotes, atraso e *jitter*. Sempre que se planeia a disponibilização de um serviço deste tipo torna-se pois importante analisar pormenorizadamente os factores que influenciam estes parâmetros e tomar as medidas necessárias para os controlar.

O fornecimento de serviços deste tipo entre diferentes entidades é normalmente protocolado tendo por base um Acordo de Nível de Serviço - SLA (*Service Level Agreement*). Neste acordo são definidos, entre outros, os intervalos aceitáveis para os parâmetros referidos.

O projecto VoIP@RCTS, apresentado no capítulo 4, visa implementar serviços VoIP entre diversas instituições, utilizando a rede RCTS como infra-estrutura de trânsito. Assim, a FCCN, como entidade gestora da rede RCTS e promotora deste projecto, definiu um SLA para o mesmo. Este aplica-se, quer à infra-estrutura sob gestão desta entidade, quer às infra-estruturas de cada instituição envolvida no projecto.

Assim, no âmbito deste SLA, a FCCN responsabiliza-se por garantir a entrega do tráfego VoIP com as seguintes métricas [75]:

- **Latência**:

  a) Desde o ponto de saída da instituição A até ao ponto de entrada na instituição B, utilizando a RCTS como meio de transporte de tráfego VoIP o valor da latência não ultrapassa os 60 ms.

  b) Desde o ponto de saída de uma instituição até ao ponto de entrada no operador o valor da latência não ultrapassa os 30 ms.

- *Jitter*:

  a) Desde o ponto de saída da instituição A até ao ponto de entrada na instituição B, utilizando a RCTS como meio de transporte de tráfego VoIP o valor do jitter não ultrapassa os 10 ms.

  b) Desde o ponto de saída de uma instituição até ao ponto de entrada no operador valor do *jitter* não ultrapassa os 10 ms.

- **Perda de pacotes**:

a) Desde o ponto de saída da instituição A até ao ponto de entrada na instituição B, utilizando a RCTS como meio de transporte de tráfego VoIP a percentagem de perda de pacotes não ultrapassa os 0,5%.

b) Desde o ponto de saída de uma instituição até ao ponto de entrada no operador a percentagem de perda de pacotes não ultrapassa os 0,5%.

Ainda no âmbito do mesmo SLA, cada instituição participante no projecto VoIP@RCTS deve assegurar a entrega de tráfego VoIP com as seguintes métricas:

- **Latência**:

  Desde o terminal de telefonia (telefone) da instituição até ao seu ponto de saída, o valor da latência não ultrapassa os 45 ms.

- *Jitter*:

  Desde o terminal de telefonia (telefone) da instituição até ao seu ponto de saída, o valor do *jitter* não ultrapassa os 10 ms.

- **Perda de pacotes**:

  Desde o terminal de telefonia (telefone) da instituição até ao seu ponto de saída, a percentagem da perda de pacotes não ultrapassa o 0,5%.

A figura 5.1 representa graficamente a latência máxima aceite no âmbito do projecto RCTS, an nível dos diversos intervenientes.

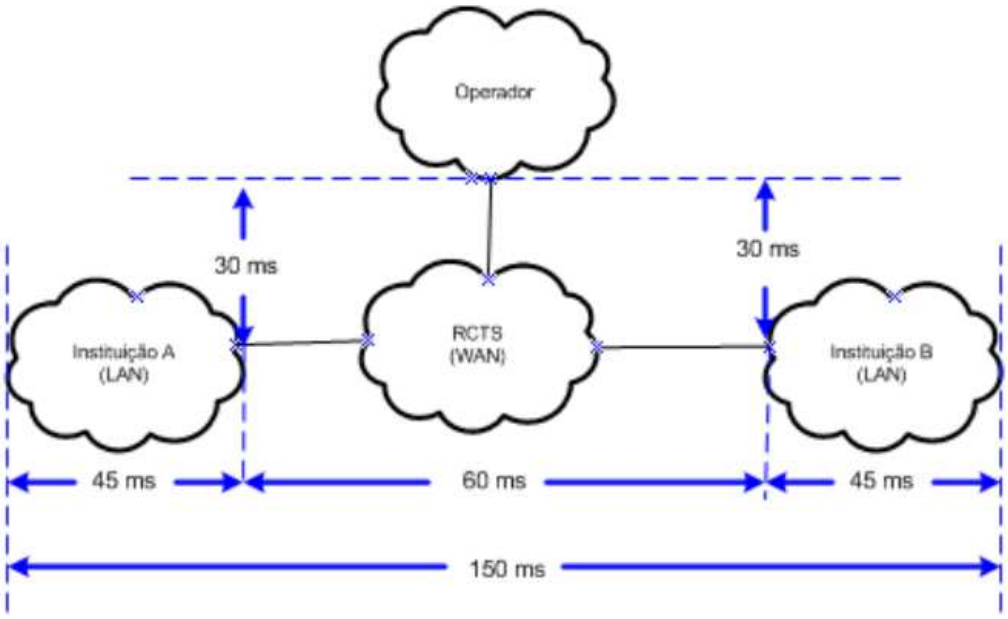

Figura 5.1: SLA do projecto VoIP@RCTS: Latência na rede RCTS [75]

5.2 A ferramenta de simulação e emulação de tráfego *NCTUns*

A utilização de ferramentas de modelação e simulação de tecnologias e protocolos de rede é uma prática corrente, desde há longos anos, nos meios académicos e empresariais. O desenvolvimento e teste de novas tecnologias e protocolos é um processo moroso, complexo e muitas vezes dispendioso. Por estes motivos, a realização destes testes com recursos reais é muitas vezes dificultada e até, às vezes impraticável. É aqui que entram então as ferramentas de simulação, permitindo avaliar num ambiente simulado o comportamento dos protocolos em desenvolvimento, muitas vezes antes de estes protocolos serem mesmo implementados em ambiente real.

De entre as principais ferramentas de simulação disponíveis para a área das redes de computadores, o *ns-2* (*Network Simulator 2*) [58] é o mais reconhecido e usado pela comunidade académica e científica.

Trata-se de um simulador implementado em linguagem *C++* e disponível em formato de código aberto. As *scripts* com as simulações dos utilizadores são desenvolvidas em linguagem TCL[3]. Utiliza um princípio de funcionamento baseado em eventos discretos, suportando a simulação de diversos tipos de redes (*Ethernet, Wireless, ATM, Frame Relay, MPLS*, etc) e protocolos dos diversos níveis protocolares (IP, UDP, TCP, RTP, RTCP, FTP, HTTP, etc).

O *ns-2* é actualmente considerado um standard de facto na área dos simuladores de rede, sendo a sua validação comprovada e aceite por diversos organismos americanos de relevância internacional, como o NIST[4] ou a agência DARPA[5].

Para além do *ns-2*, vários outros simuladores de rede são usados para este fim. Entre eles, encontra-se o OPNET [76]. Trata-se de um simulador comercial bastante divulgado nos meios empresariais, que apresenta como principais vantagens o interface gráfico com o utilizador e uma rápida curva de aprendizagem, quando comparado com o *ns-2*.

Entretanto, no início desta década, o Professor S.Y. Wang coordenou o desenvolvimento da primeira versão do simulador *NCTUns* [77], aproveitando os trabalhos realizados no âmbito do doutoramento, conluído na Universidade de Harvard em 1999. Nestes trabalhos foi desenvolvida uma metodologia inovadora de reentrância do kernel [78], que foi então aproveitada, já na *National Chiao Tung University (NCTU)* de Taiwan, para a criação deste novo simulador de rede.

Graças a esta nova metodologia, defendem os seus autores que se trata de um simulador e emulador de rede altamente preciso e extensível, capaz de simular vários protocolos usados em redes cabladas e sem fios com várias vantagens sobre os simuladores tradicionais, como o *ns-2* ou o OPNET.

Na primeira versão, este simulador funcionava apenas sobre o sistema operativo FreeBSD. Entretanto, foi portado para o sistema Linux, plataforma sobre a qual correm as versões mais recentes.

Entre as principais vantagens identificadas pelos autores desta ferramenta, des-

[3]TCL: *Tool Command Language*
[4]NIST: *National Institute of Standards and Technology*
[5]DARPA: *Defense Advanced Research Projects Agency*

tacam-se as seguintes [80]:

- pode ser facilmente usado como simulador ou emulador, podendo ser adicionados hosts e aplicações reais a uma simulação. Dois nodos externos podem também trocar pacotes entre si através de uma rede simulada no NCTUns.

- utilizando as funcionalidades referidas de reentrância do kernel, recorre à pilha protocolar TCP/IP real de um sistema Linux para gerar simulações com resultados de elevada precisão.

- pode correr qualquer aplicação UNIX real num nodo simulado, sem qualquer modificação.

- pode usar, numa rede simulada, aplicações UNIX reais de configuração e monitorização de rede, como por exemplo as ferramentas *route, ifconfig, netstat, tcpdump, traceroute, etc.*

- a configuração e utilização das redes e aplicações simuladas é feita da mesma forma que nas redes reais, tornando mais simples e rápido o processo de aprendizagem e operação com o simulador.

- permite a simulação das tecnologias e protocolos mais divulgados. Entre outras tecnologias, inclui suporte para redes Ethernet, IEEE 802.11b, GPRS, ópticas, IEEE 802.11e, IEEE 802.16 (Wimax), DVB-RCS, etc.

- suporta também a simulação de vários dos protocolos mais importantes das redes actuais, entre os quais: *IEEE 802.3 CSMA/CD MAC, IEEE 802.11b CSMA/CA MAC, IEEE 802.11e QoS MAC, IEEE 802.16d WiMAX wireless MAC e PHY, DVB-RCS satelite MAC e PHY, learning bridge protocol, spanning tree protocol, IP, Mobile IP, Diffserv (QoS), RIP, OSPF, UDP, TCP, RTP/RTCP/SDP, HTTP, FTP, Telnet*, etc.

- processa uma simulação de rede de forma mais rápida que a generalidade dos simuladores concorrentes, graças à metodologia de reentrância do kernel baseada em eventos discretos.

- suporta simulações paralelas em máquinas *multi-core*.

- disponibiliza um interface gráfico (GUI[6]) (figura 5.2) altamente integrado e profissional, onde o utilizador pode, de forma rápida e fácil, desenhar uma topologia, configurar os protocolos a usar nos nodos, especificar os percursos e movimentos para nodos móveis, desenhar gráficos de performance da rede ou rever a animação de uma simulação realizada.

- o motor de simulação é baseado numa arquitectura e código abertos. O utilizador pode desenvolver os seus próprios protocolos e adicioná-los ao motor da simulação, de forma facilitada.

[6]GUI: *graphical user interface*

- através de uma arquitectura distribuída, suporta simulações remotas e concorrentes.

  O GUI e o motor de simulação são implementados separadamente, usando o modelo cliente-servidor para operar. Desta forma, um utilizador pode submeter, através do GUI, a sua simulação a um servidor remoto a correr o motor de simulação. Este servidor executa a simulação e devolve mais tarde os resultados de volta ao primeiro, para análise.

- está permanentemente em actualização, com novas funções e protocolos a serem continuamente adicionados.

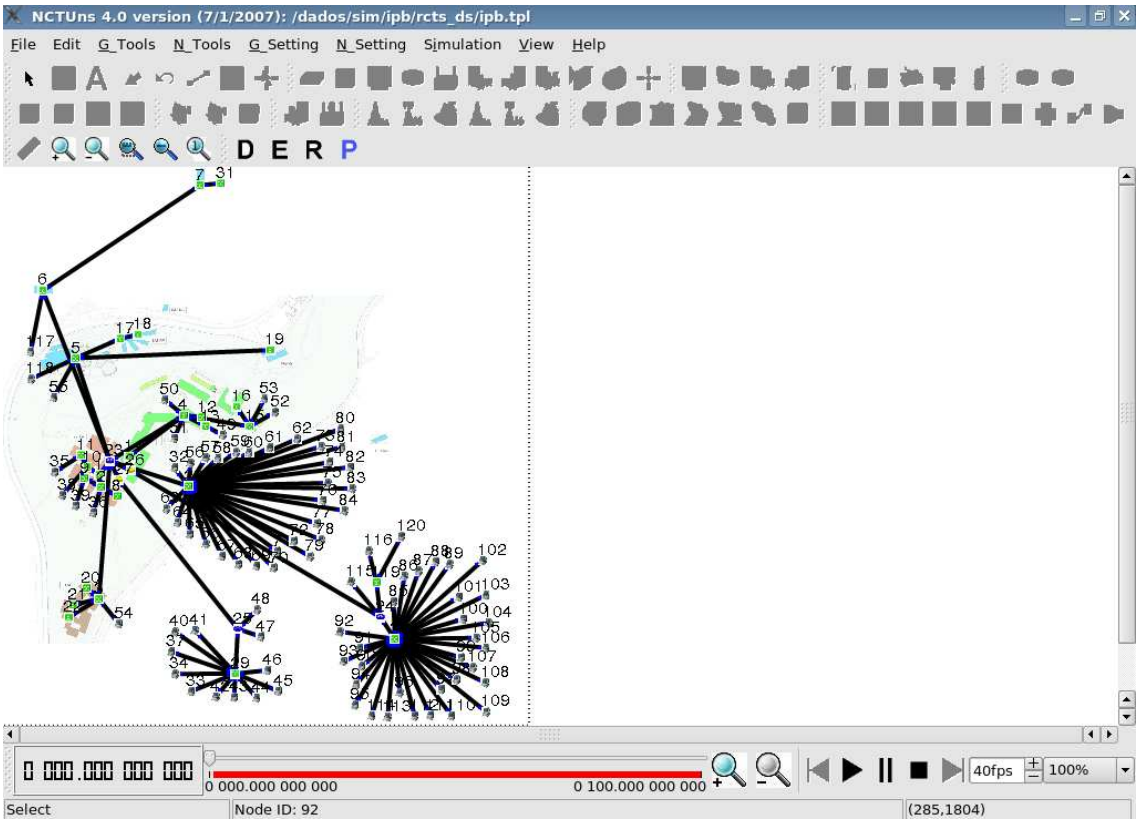

Figura 5.2: Interface gráfico do simulador *NCTUns*

Como referido, o simulador *NCTUns* é baseado numa arquitectura distribuída (figura 5.3), sendo esta constituída por oito componentes fundamentais [79]:

1. interface gráfico com o utilizador (GUI);

2. **motor de simulação**, que fornece os os serviços básicos da simulação aos módulos protocolares, como o escalonamento de eventos, manuseamento do tempo e dos pacotes, etc.

   A máquina onde este componente corre é denominada **servidor de simulação**;

3. módulos protocolares, que implementam os diferentes protocolos e funções suportadas no simulador;

4. **expedidor** (*dispatcher*) dos trabalhos de simulação submetidos, que pode controlar simultaneamente múltiplos servidores de simulação, aumentando desta forma a performance da infra-estrutura de simulação;

5. programa **coordenador** (*coordinator*). Corre um em cada servidor de simulação, registando-se junto do expedidor definido e passando a este componente informações sobre o estado do referido servidor (disponível ou ocupado). Desta forma, o expedidor pode escolher em qualquer altura um servidor de simulação livre pode submeter um trabalho. É também este coordenador que vai passando informações de estado do trabalho submetido para simulação ao GUI (por exemplo, o tempo actual da simulação);

6. *patches* ao kernel do sistema operativo Linux onde o servidor de simulação vai correr;

7. aplicações, que correm em ambiente real, usadas pelo simulador para gerar tráfego de rede;

8. vários *daemons* executados automaticamente em cada simulação para executar diversas funções intermédias (por exemplo *daemons* para criação de tabelas de encaminhamento com base nos protocolos RIP ou OSPF).

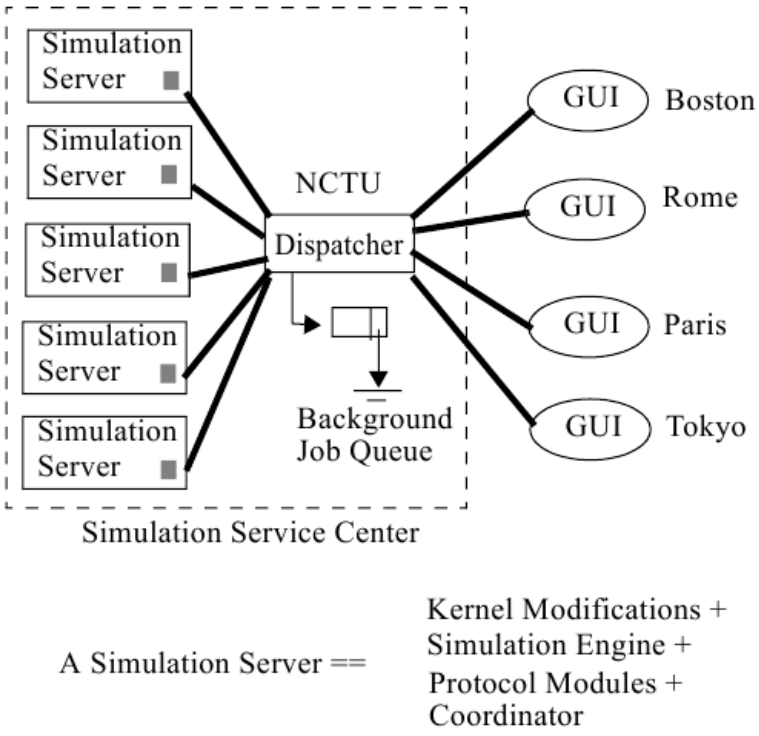

Figura 5.3: Arquitectura distribuída do *NCTUns* [79]

Em resultado das simulações realizadas, o *NCTUns* produz um ficheiro de *trace* com os registos de todos os eventos relacionados com os pacotes gerados no decorrer

da simulação. Este ficheiro pode ser posteriormente analisado detalhadamente, para se avaliar o comportamento da simulação testada.

Adicionalmente, é possível a activação de registos para protocolos e/ou nodos específicos, que aumentam o nível de informação produzida para situações concretas. É possível, por exemplo, seleccionar a geração automática de um ficheiro de texto com o *throughtput* de entrada e/ou saída de um qualquer interface de um host.

Tirando partido da ferramenta integrada de geração de gráficos, podemos na fase de análise usar as informações destes ficheiros para, por exemplo, produzir gráficos com o *throughtput* ou o número de pacotes descartados num interface de rede.

Embora seja possível usar qualquer aplicação de rede que corra num sistema Linux, o *NCTUns* disponibiliza um conjunto de aplicações padrão, para geração e teste de diversos tipos de tráfego, nomeadamente UDP, TCP, fontes CBR ou On-Off, RTP/RTCP, etc. De referir que estas aplicações podem funcionar também num sistema Linux de forma independente do simulador.

5.2.1 Justificação da escolha do *NCTUns* para o presente trabalho

Entre os objectivos do presente trabalho está a realização de um conjunto de testes, em ambiente de simulação, para avaliar a implementação de políticas de tratamento diferenciado de tráfego VoIP. Assim, foi necessário proceder à escolha de uma ferramenta de simulação adequada aos objectivos pretendidos.

Em face da análise das diferentes alternativas referidas na secção anterior e das características apresentadas pela ferramenta *NCTUns*, a escolha recaiu sobre esta opção. Entre os principais factores contretos que justificam esta escolha, destacam-se os seguintes:

- disponibilização de aplicações específicas para geração de tráfego VoIP, com suporte de vários dos principais *codecs* usados hoje em dia;
- suporte integrado para simulação de redes com tráfego *DiffServ*;
- funcionamento de um ambiente de simulação integrado com a emulação de tráfego real e hosts externos. Embora esta funcionalidade tenha sido inicialmente considerada relevante, não chegou a ser utilizada no presente trabalho.

No próximo capítulo serão descritos e analisados os diversos testes realizados com esta ferramenta.

Capítulo 6

Experiências e resultados

Pretende-se, com o presente trabalho, avaliar sobre os requisitos de qualidade de serviço necessários à implementação de serviços de VoIP numa rede de dados, usando como exemplo de aplicação o caso da Rede do Instituto Politécnico de Bragança.

Nos capítulos anteriores foram apresentados os projectos VoIP@IPB e VoIP@RCTS e definidos os requisitos de qualidade de serviço para um adequado funcionamento de um serviço de VoIP. Neste sentido, pretende-se neste capítulo descrever um conjunto de experiências realizadas e comentar os resultados obtidos, com o objectivo de avaliar o impacto da implementação de políticas de QoS baseadas no modelo *DiffServ* para o cumprimento dos requisitos referidos atrás.

6.1 Descrição do modelo de simulação

Tendo em atenção os requisitos especiais do tráfego VoIP quanto aos parâmetros de pacotes perdidos, atraso e *jitter* (cuja caracterização foi efectuada na secção 5.1), existem dois pontos na rede especialmente sensíveis, para os quais se vai avaliar o comportamento no tratamento deste tipo de tráfego em situações de congestão:

- Ligação entre a Rede do Campus de Sta Apolónia e a rede da ESTGM (circuito MPLS de 4 Mbps, alugado a um operador de telecomunicações)
- Ligação entre a Rede do IPB e a Internet (circuito de 100 Mbps, gerido pela FCCN - Fundação para a Computação Científica Nacional)

Assim, os testes a realizar dividir-se-ão em duas fases (uma para cada ponto identificado atrás). Em cada uma das fases, pretende-se avaliar o comportamento do tráfego VoIP, em concorrência com outro tráfego de rede, em duas situações:

- a) sem aplicação de políticas de QoS, ou seja, todo o tráfego tratado em modo *best-effort*;
- b) aplicando um tratamento diferenciado ao tráfego VoIP relativamente ao restante tráfego. Serão avaliadas duas alternativas de tratamento diferenciado:
  - i) *DiffServ* com marcação e PHB AF para tráfego VoIP e marcação BE para restante tráfego;

– ii) *DiffServ* com marcação e PHB EF para tráfego VoIP e marcação BE para restante tráfego.

Os testes realizados, em ambiente de simulação, serão efectuados com recurso à ferramenta *NCTUns*, descrita na secção 5.2 e usando a topologia apresentada na figura 6.1.

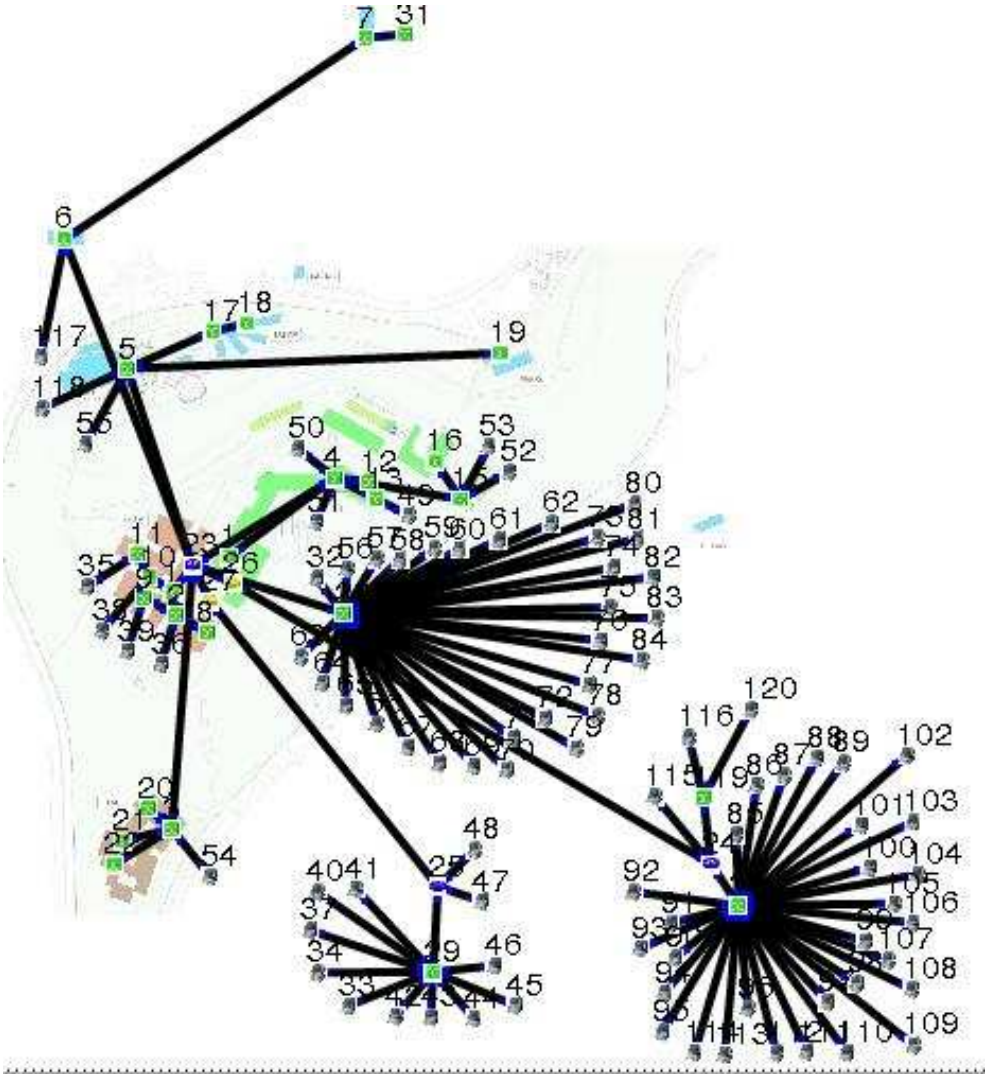

Figura 6.1: Topologia da rede de testes implementada no *NCTUns*

6.1.1 Simulação de Tráfego

Para efeitos de simulação, definiram-se três tipos de aplicações: tráfego VoIP que se pretende proteger, tráfego TCP genérico e tráfego UDP genérico.

Pretende-se com o tráfego TCP genérico (cujos fluxos são adiante identificados com o prefixo *tcpxx*) simular o comportamento de uma aplicação cliente-servidor tradicional (p.e. serviço FTP). Neste caso, os mecanismos de controlo de fluxo do protocolo TCP ajustam automaticamente a taxa de envio às condições da rede,

minimizando por este motivo a percentagem de pacotes perdidos em condições de congestão. Os pacotes perdidos são recuperados pelo TCP, pelo que esta situação se traduzirá na prática na necessidade de transmitir mais pacotes (retransmitidos para recuperar os perdidos). O efeito mais notório do ajuste da taxa de envio às condições da rede será uma menor taxa de transferência, traduzida numa menor quantidade de bytes por segundo do que numa situação normal (sem sobrecarga da rede).

Para a simulação do tráfego TCP, o *NCTUns* disponibiliza duas aplicações: *rtcp*, servidor TCP e *stcp*, cliente TCP, que funcionam em modo *greedy* (tal significa que o emissor tenta enviar o máximo de pacotes que lhe for possível).

Pretende-se com o tráfego UDP genérico (cujos fluxos são adiante identificados com o prefixo *udpxx*) sobrecarregar a rede até ao ponto de congestão, para desta forma se poder avaliar o comportamento das restantes aplicações nestas circunstâncias. Sendo tráfego transportado pelo protocolo UDP, não é utilizado qualquer mecanismo de controlo de fluxo, produzindo-se na prática um efeito de ocupação da totalidade da largura de banda disponível.

A geração do tráfego UDP foi baseada na aplicação *stg* [69] do *NCTUns*, a funcionar também em modo *greedy*. Para as simulações realizadas no trabalho, os clientes e servidores UDP foram configurados para operar com esta função em modo *greedy* e com pacotes de tamanho fixo de 1400 bytes.

Para efeitos de avaliação da viabilidade de implementação de mecanismos de QoS para protecção do tráfego VoIP entre as redes referidas, considera-se suficiente basear a simulação deste tráfego apenas no codec G.711 (variante *allaw*). A utilização de outros codecs irá apenas influenciar o número de canais protegidos, em função da largura de banda requerida para cada canal (que é dependente do tipo de codec usado). O *bit rate* fornecido pelo G.711 é de 64 Kbps, a que acresce o *overhead* dos protocolos RTP, UDP, IP e do PDU[1] da camada de ligação de dados. Em função destes factores, considera-se, para efeitos de simulação, que a largura de banda consumida por cada chamada VoIP nestas condições é de 88 Kbps.

A simulação do tráfego VoIP foi efectuada com recurso à aplicação *rtpsendrecv*, disponibilizada pelo simulador usado. Trata-se de uma aplicação que gera e recebe pacotes RTP e RTCP. Usa uma taxa fixa para enviar pacotes RTP, com base num conjunto de parâmetros definidos num ficheiro SDP[2]. Para activação de cada um dos fluxos VoIP nas simulações realizadas (identificados com o prefixo *voipxx*), foi criado um ficheiro SDP com a descrição de cada sessão, contendo parâmetros como: data de início e fim de sessão, codec usado, taxa de amostragem, bits por amostragem, e taxa de amostragem (*ms* de voz por pacote). Apresenta-se de seguida como exemplo o ficheiro com a descrição da sessão RTP para o host 80:

e=80@ipb 3
b=AS:1600
t=26 200
m=audio 5004 RTP/AVP 8
a=rtpmap:8 PCMA/8000/8

[1]PDU:*Protocol Data Unit*
[2]SDP: *Session Description Protocol*

a=ptime:20
c=IN IP4 1.0.10.27

A definição destes parâmetros é efectuada na interface gráfica do *NCTUns* (figura 6.2).

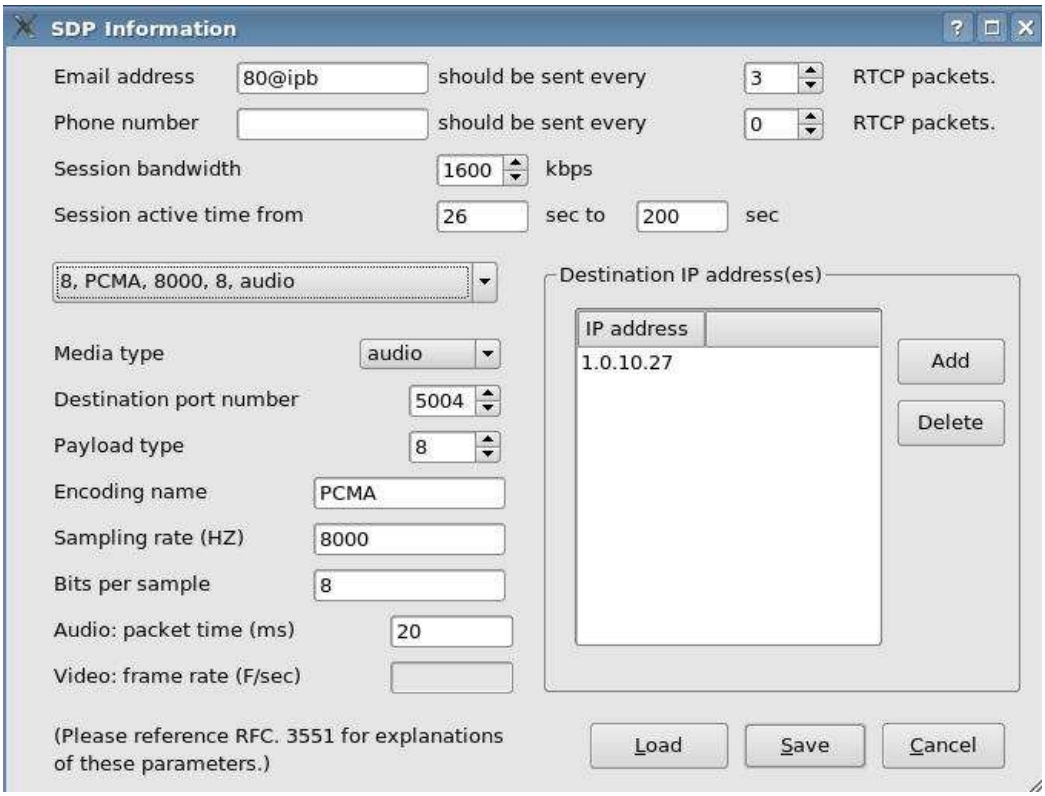

Figura 6.2: Definição dos parâmetros SDP para os fluxos VoIP

6.1.2 Tratamento dos resultados das simulações

Os resultados obtidos nas simulações realizadas são analisados na perspectiva dos *pacotes perdidos e/ou retransmitidos*, *atraso* e *jitter* de cada fluxo testado.

Os valores obtidos para estes parâmetros são calculados, com recurso a um conjunto de *scripts* em linguagem de *scripting BASH*[3], desenvolvidas no âmbito do presente trabalho para este efeito. As *scripts* desenvolvidas actuam sobre o ficheiro de *trace* gerado pelo simulador *NCTUns*. Este ficheiro contém os registos de todos os eventos relacionados com os pacotes gerados durante uma simulação, apresentando um *output* baseado no conjunto dos seguintes campos:

Protocolo; Tipo de evento; Início de transmissão; duração do evento; Tipo de pacote; Origem–destino (IP); Origem–destino (Phy); ID do pacote; Tamanho do pacote; Nº de retransmissões; Razão de descarte

[3]BASH: acrónimo de *Bourne-again shell*

Apresenta-se de seguida o exemplo de um excerto do *output* de um ficheiro de trace do *NCTUns*, onde se podem visualizar os campos referidos:

...
802.3 BTX 1000011838 5211 DATA <0 0> <23 26> 6 64 0 NONE
802.3 BRX 1000012838 5211 DATA <0 0> <23 26> 6 64 0 NONE
802.3 TX 1000018049 5241 DATA <0 0> <26 23> 7 64 0 NONE
802.3 RX 1000019049 5241 DATA <0 0> <26 23> 7 64 0 NONE
802.3 TX 1000024290 18518 DATA <32 85> <23 26> 5 218 0 NONE
802.3 RX 1000025290 18518 DATA <32 85> <23 26> 5 218 0 NONE
...

O valor dos pacotes perdidos para cada fluxo VoIP e UDP é calculado da seguinte forma:

- (1) contagem dos pacotes transmitidos pelo nodo de origem
- (2) contagem dos pacotes recebidos pelo nodo de destino correspondente
- (3) Pacotes perdidos = (1) – (2)

Considerando os mecanismos de controlo de fluxo e sequenciação do protocolo TCP, assume-se que todos os segmentos são entregues no destino. Neste sentido, quando existe um menor número de pacotes recebidos pelo destino do que pacotes enviados pelo sistema de origem, pode concluir-se que a diferença entre estes dois valores corresponde a segmentos perdidos ao longo do percurso e, portanto, retransmitidos pelo TCP. Desta forma, o cálculo dos pacotes retransmitidos nos fluxos TCP baseia-se no seguinte princípio:

- (1) contagem dos pacotes transmitidos pelo nodo de origem
- (2) contagem dos pacotes recebidos pelo nodo de destino correspondente
- (3) Pacotes perdidos, posteriormente retransmitidos = (1) – (2)

O cálculo do atraso de cada pacote VoIP foi efectuado da seguinte forma:

- (1) obtenção do instante temporal do evento que marca o início de transmissão (TX), no sistema de origem do fluxo (terceiro campo do ficheiro de *trace*)
- (2) obtenção do instante temporal de início do último evento ocorrido com o pacote (evento RX no sistema de destino)
- (3) obtenção do valor da duração do evento referido em (2) (quarto campo do ficheiro de *trace*)
- (4) Atraso do pacote = (2) – (1) + (3)

A determinação da média do atraso para os pacotes VoIP transmitidos em cada segundo é feita do seguinte modo:

- (1) soma do atraso de todos os pacotes recebidos nesse segundo
- (2) determinação da quantidade de pacotes recebidos nesse segundo
- (3) Atraso médio, para um dado segundo = (1) / (2)

A determinação da média do atraso para cada fluxo VoIP é feita da seguinte forma:

- (1) soma do atraso de todos os pacotes do fluxo, recebidos no sistema de destino
- (2) determinação da quantidade de pacotes do fluxo recebidos no sistema de destino
- (3) Atraso médio, por fluxo = (1) / (2)

O cálculo do valor do *jitter* para cada pacote VoIP é efectuado da seguinte forma:

- (1) obtenção do valor do atraso do pacote actual (N), de acordo com procedimento descrito atrás
- (2) obtenção do valor do atraso do pacote anterior ($N - 1$)
- (3) *Jitter* do pacote N = (1) – (2)

A determinação da média do *jitter* para os pacotes VoIP transmitidos em cada segundo é feita do seguinte modo:

- (1) soma do *jitter* de todos os pacotes recebidos nesse segundo
- (2) determinação da quantidade de pacotes recebidos nesse segundo
- (3) *Jitter* médio, para um dado segundo = (1) / (2)

A determinação da média do *jitter* para cada fluxo VoIP é feita da seguinte forma:

- (1) soma do *jitter* de todos os pacotes do fluxo, recebidos no sistema de destino
- (2) determinação da quantidade de pacotes do fluxo recebidos no sistema de destino
- (3) *Jitter* médio, por fluxo = (1) / (2)

6.1.3 Algumas limitações do *NCTUns* e suas implicações

O *NCTUns* não guarda, no ficheiro de *trace*, qualquer marcação unívoca dos pacotes gerados. Tal significa que não é possível seguir, com base num marcador específico, o percurso de um pacote gerado, desde o sistema de origem até ao sistema de destino. Por este motivo, todos os cálculos dos valores relacionados com os parâmetros *atraso* e *jitter* descritos atrás estão sujeitos às seguintes limitações/condições:

- só são possíveis quando o atraso de cada pacote é inferior ao *inter-arrival time* dos pacotes.

  Nos testes realizados, o *inter-arrival time* dos pacotes VoIP gerados é de 20 ms. Este valor decorre dos parâmetros definidos para cada sessão VoIP, baseada neste caso em pacotes RTP com codec G.711. Também se verificou que o pior caso de atraso máximo ocorrido não ultrapassou os 12 ms pelo que, para os testes realizados neste trabalho, esta limitação não influencia os resultados obtidos.

- o cálculo do atraso e do *jitter* pode conduzir a resultados incorrectos (temporizações incorrectas) quando é efectuado para o pacote que se segue a um pacote perdido. Para minimizar o impacto destes desvios nos cálculos efectuados, optou-se por não contabilizar os valores obtidos nestas circunstâncias. Tal significa que para o pior dos casos, nos fluxos em que se obtém perdas de pacotes próximas de 1%, os valores de atraso e *jitter* médio do fluxo foram calculados com base em pouco mais de 98% dos pacotes em vez da totalidade dos pacotes.

Concluído o enquadramento do modelo de simulação a implementar, descrevem-se de seguida os testes realizados para cada uma das fases identificadas anteriormente.

6.2 Testes realizados na ligação entre a Rede do Campus de Sta Apolónia e a rede da ESTGM

Como referido no capítulo 4, a ligação de dados entre o Campus de Santa Apolónia, em Bragança, e a ESTGM, em Mirandela, é garantida por um circuito MPLS de 4 Mbps, alugado a um operador de telecomunicações.

Trata-se de uma ligação com um débito limitado, que se encontra próximo da capacidade máxima de utilização durante boa parte do horário normal de funcionamento da Instituição (ver gráfico da figura 6.3). Por este motivo, é de fundamental importância o estabelecimento de políticas de tratamento diferenciado do tráfego de voz que se pretende transportar sobre a mesma.

Pretendendo-se partilhar este canal de comunicação pelos serviços de Voz (VoIP), e dados (acesso a aplicações internas - Intranet do IPB - e Internet), nenhuma destas duas categorias deve canibalizar a ligação. Neste sentido, o conjunto de testes apresentados a seguir pretende ajudar a determinar uma configuração para

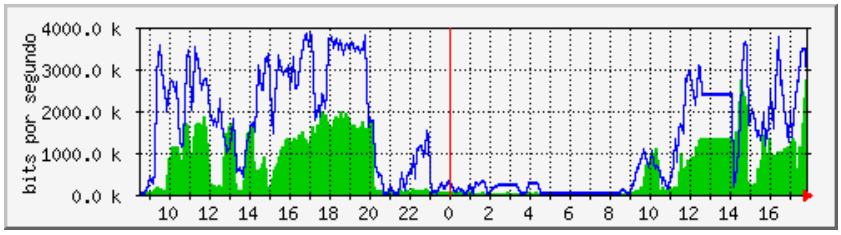

Figura 6.3: Amostra da taxa de ocupação da linha de dados entre o Campus de Santa Apolónia e a ESTGM, por um período de 24 horas

implementação de um serviço de transporte de tráfego VoIP entre os dois locais, com um nível de qualidade de serviço adequado.

A ligação da rede telefónica da ESTGM à rede pública é assegurada por um acesso básico RDIS (2 canais de voz simultâneos). Aproveitando a mudança do acesso de voz ao exterior para um trunk VoIP, pretende-se aumentar o número de chamadas simultâneas possíveis, das duas referidas para até um máximo de seis.

Considerando que se pretende garantir até um máximo de seis chamadas VoIP simultâneas e que cada fluxo requer 88 Kbps, então os requisitos de largura de banda para este conjunto agregado de fluxos são de 528 Kbps.

Com base nos pressupostos anteriores, procedeu-se à realização de um conjunto de testes no simulador *NCTUns*, com o objectivo de avaliar sobre a possibilidade de garantir a realização das chamadas simultâneas referidas, sem interferência do restante tráfego de dados. Para este efeito, foi usada a topologia representada na figura 6.4.

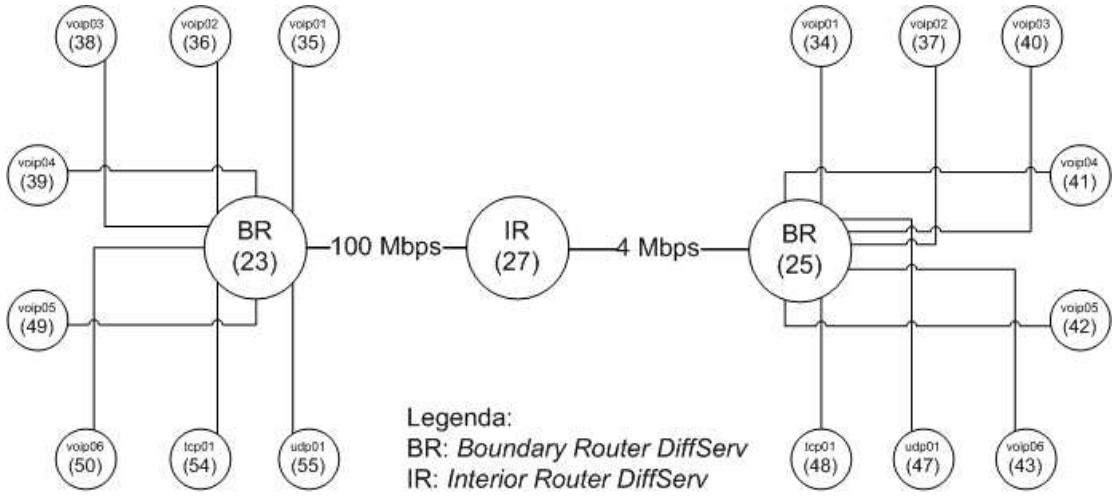

Figura 6.4: Topologia de rede usada nos testes entre a Rede do Campus de Santa Apolónia e a ESTGM

Foram definidos 8 fluxos de dados entre as duas redes, configurados de acordo com as informações constantes na tabela 6.1.

Todas as simulações realizadas tiveram uma duração de 100 segundos, sendo o início dos fluxos faseado, entre o segundo 4 e o segundo 40.

Fluxo	Host Origem	Local	Serviço	Host Destino	Local	Tráfego
voip01	35	IPB.ESTIG	VoIP	34	ESTGM	VoIP
voip02	36	IPB.ESTIG	VoIP	37	ESTGM	VoIP
voip03	38	IPB.ESTIG	VoIP	40	ESTGM	VoIP
voip04	39	IPB.ESTIG	VoIP	41	ESTGM	VoIP
voip05	49	IPB.ESA	VoIP	42	ESTGM	VoIP
voip06	50	IPB.ESA	VoIP	43	ESTGM	VoIP
tcp01	54	IPB.ESE	TCP	47	ESTGM	TCP
udp01	55	IPB.SAS	UDP	48	ESTGM	UDP

Tabela 6.1: Identificação dos fluxos estabelecidos entre a rede do Campus de Santa Apolónia e a ESTGM

Considerando que a saturação da ligação em análise se dá normalmente no sentido *Campus de Santa Apolónia – ESTGM*, os valores obtidos e as análises efectuadas nas secções seguintes são baseadas nas informações recolhidas no encaminhador de fronteira da rede da ESTGM (host 25).

6.2.1 Testes sem prioritização de tráfego

Numa primeira fase, procedeu-se à simulação dos fluxos descritos na tabela 6.1 sem qualquer tipo de prioritização (todos os fluxos tratados num princípio *best-effort*).

Na tabela 6.2 são apresentados os resultados desta primeira simulação, em termos de valores de pacotes enviados, recebidos e perdidos (em valor e percentagem). De notar que, relativamente aos fluxos TCP, pretende-se identificar os segmentos retransmitidos.

Como se pode constatar pela análise destes resultados, a taxa de pacotes perdidos nos fluxos VoIP é muito significativa (sempre acima dos 50%), o que, na prática, impede um correcto funcionamento deste serviço. Os fluxos VoIP iniciados mais tarde (mais próximo do instante em que é activado o fluxo de tráfego UDP) são os que apresentam percentagem de perdas maior, visto o período de tempo em que estiveram activos sem congestionamento do canal ter sido menor.

Apesar do tráfego TCP também ter sido severamente afectado pelo congestionamento provocado pelo tráfego UDP (em termos de taxa de transmissão), o número de pacotes retransmitidos mantém-se extremamente baixo. Tal deve-se à actuação dos mecanismos de controlo de congestão do TCP referidos atrás, que ajustam a taxa de envio às capacidades do canal em cada momento.

A figura 6.5 apresenta o comportamento do tráfego VoIP de entrada e saída, no encaminhador de fronteira (host 25) da Rede da ESTGM.

Tal como já foi referido anteriormente, cada fluxo VoIP simulado ocupa 88 Kbps (11 KBps) em cada sentido. Assim, os seis fluxos simultâneos devem gerar uma taxa constante de 528 Kbps (66 KBps) em cada sentido.

Como se pode verificar na figura 6.5, o tráfego VoIP que sai da rede da ESTGM mantém essa taxa constante (linha azul) ao longo de toda a simulação (até ao segundo 40 a linha azul não é visível no gráfico porque é sobreposta pela linha que

Fluxo	Pacotes enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4819	2353	2466	51.172%
voip02	4718	1750	2968	62.908%
voip03	4618	1668	2950	63.880%
voip04	4517	1541	2976	65.884%
voip05	4417	1448	2969	67.217%
voip06	4317	1379	2938	68.056%
tcp01	1675	1630	45*	2.686%*
udp01	49407	19640	29767	60.248%

Tabela 6.2: Pacotes perdidos/retransmitidos, apenas com tráfego *best-effort*

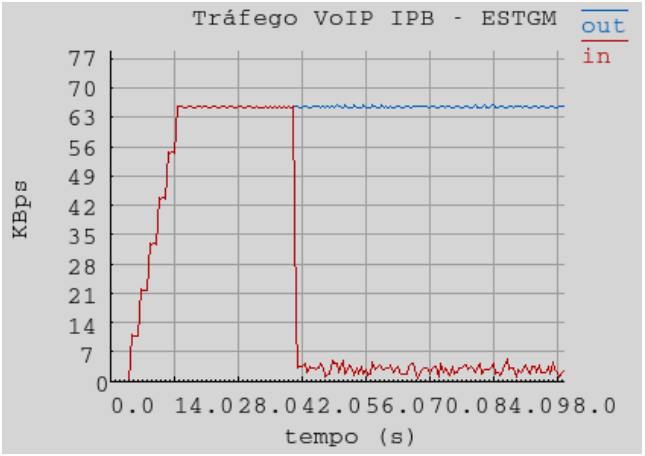

Figura 6.5: Comportamento dos fluxos de tráfego VoIP entre IPB e ESTGM, sem prioritização

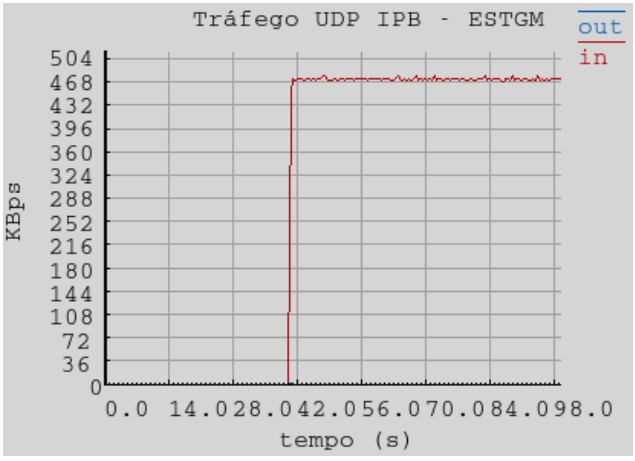

Figura 6.6: Comportamento dos fluxos de tráfego UDP entre IPB e ESTGM, sem prioritização

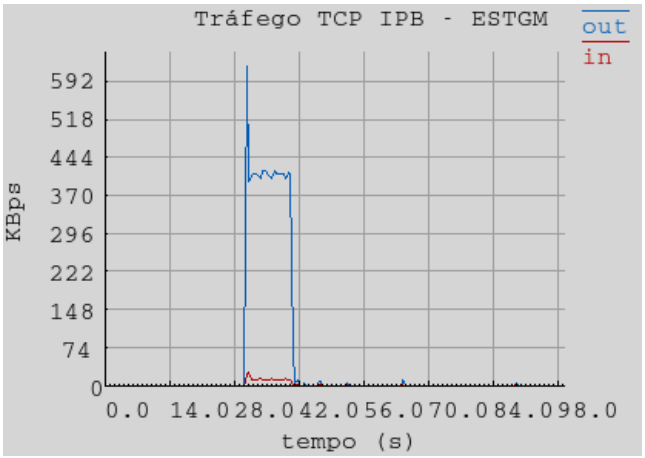

Figura 6.7: Comportamento dos fluxos de tráfego TCP entre IPB e ESTGM, sem prioritização

representa o tráfego de entrada - linha vermelha). O tráfego VoIP que chega à entrada da rede ESTGM mantém-se constante nos valores previstos apenas até ao instante *40 seg*, altura em que se iniciou o fluxo de tráfego UDP entre as duas redes. A partir deste momento, o tráfego UDP vai saturar a ligação, no sentido IPB - ESTGM (figura 6.6), afectando automaticamente os fluxos VoIP (figura 6.5) e TCP activos (figura 6.7).

Concluíndo, sem utilização de um mecanismo de QoS, não é possível assegurar o funcionamento do serviço VoIP nos termos descritos anteriormente.

6.2.2 Testes com prioritização do tráfego VoIP

Repetiram-se de seguida os testes realizados na secção anterior, mantendo as mesmas características de tráfego dessa simulação mas introduzindo prioritização *DiffServ*.

Foram neste âmbito realizadas duas simulações distintas, baseadas na topologia da figura 6.4:

- a) *DiffServ* com marcações, e respectivos PHBs, AF e BE (adiante designada apenas por simulação AF).

  Nesta simulação, o tráfego VoIP foi marcado com o *codepoint* **001010** (*PHB AF11*), sendo portanto colocado na fila da classe AF1 e recebendo o tratamento associado a essa classe, nos encaminhadores *DiffServ* do domínio. O restante tráfego TCP e UDP foi marcado com o *codepoint* **000000** (*PHB BE*), recebendo portanto um tratamento *best-effort*. A tabela 6.3 sintetiza as configurações *DiffServ* aplicadas no simulador para tratamento das classes usadas. Pode ver-se na referida tabela que é alocado 1/6 do canal de comunicação para a classe AF1, ficando os restantes 5/6 para o tráfego BE.

- b) *DiffServ* com marcações, e respectivos PHBs, EF e BE (adiante designada apenas por simulação EF).

Classe DiffServ	% do canal alocado	largura de banda alocada	Tipo de Tráfego
AF1	1/6	666 Kbps	VoIP
BE	5/6	3334 Kbps	TCP e UDP

Tabela 6.3: Classificação DiffServ implementada no link IPB–ESTGM, simulação AF

Classe DiffServ	% do canal alocado	largura de banda alocada	Tipo de Tráfego
EF	1/6	666 Kbps	VoIP
BE	5/6	3334 Kbps	TCP e UDP

Tabela 6.4: Classificação DiffServ implementada no link IPB–ESTGM, simulação EF

Neste caso, o tráfego VoIP foi marcado com o *codepoint* **101110** (*PHB EF*), sendo portanto colocado na fila da classe EF e recebendo em consequência o tratamento associado a essa classe. O restante tráfego TCP e UDP foi marcado com o *codepoint* **000000** (*PHB BE*), recebendo portanto um tratamento *best-effort*. Na tabela 6.4 apresenta-se um sintese das configurações usadas pelos encaminhadores *DiffServ* do domínio para tratamento do tráfego EF e BE.

A tabela 6.5 evidencia os resultados da simulação AF, em termos de valores de pacotes enviados, recebidos e perdidos (retransmitidos no caso do fluxo TCP), enquanto a tabela 6.6 apresenta os mesmos dados para a simulação EF.

De acordo com o descrito na secção 5.1, considera-se que a qualidade de uma conversação VoIP é irremediavelmente afectada com taxas de perdas acima de 1%.

Como se pode constatar nas tabelas 6.5 e 6.6, o valor das perdas para o tráfego VoIP é sempre inferior a 0,5%. Neste sentido, podemos afirmar que, quanto ao factor **perda de pacotes**, a aplicação das medidas de prioritização descritas foram eficazes para assegurar a qualidade do serviço VoIP, quer para a simulação AF, quer para a simulação EF.

	Pacotes			
Fluxo	enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4819	4810	9	0.186%
voip02	4718	4703	15	0.317%
voip03	4618	4601	17	0.368%
voip04	4517	4503	14	0.309%
voip05	4417	4399	18	0.407%
voip06	4317	4298	19	0.440%
tcp01	1665	1637	28*	1.681%*
udp01	49396	17052	32344	65.478%

Tabela 6.5: Simulação AF: análise dos pacotes perdidos

Fluxo	Pacotes enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4819	4819	0	0%
voip02	4718	4718	0	0%
voip03	4618	4618	0	0%
voip04	4517	4517	0	0%
voip05	4417	4417	0	0%
voip06	4317	4317	0	0%
tcp01	1692	1660	32*	1.891%*
udp01	49389	17032	32357	65.514%

Tabela 6.6: Simulação EF: análise dos pacotes perdidos

Verifica-se também que, apesar de, com prioritização AF, o tráfego VoIP receber um tratamento adequado ao funcionamento do serviço, é com prioritização EF que este tráfego recebe o melhor tratamento, não se registando neste caso qualquer perda de pacotes para todos os fluxos VoIP testados.

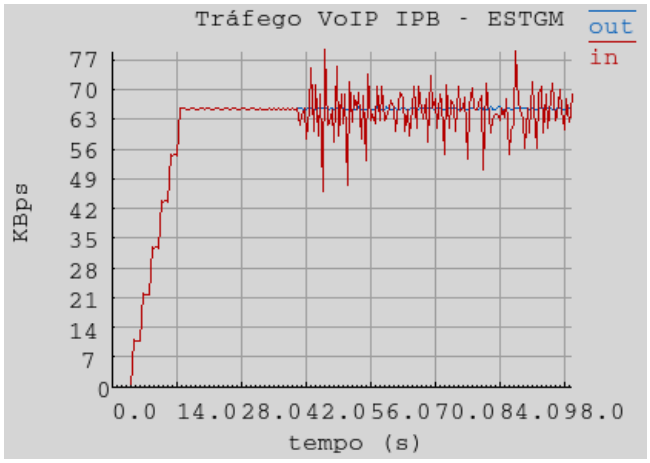

Figura 6.8: Simulação AF: tráfego VoIP entre IPB e ESTGM

Nestas simulações, o tráfego UDP deixa de canibalizar completamente a ligação. Verifica-se que o tráfego VoIP mantém um débito médio à volta dos 528 Kbps (66 KBps), como se pode visualizar nas figuras 6.8 (simulação AF) e 6.9 (simulação EF).Nesta última figura optou-se por apresentar os valores de entrada e saída em gráficos separados, para evitar a ocultação de uma das linhas por sobreposição da outra, caso se usasse um único gráfico. É também visível, na simulação AF, o efeito que a activação do fluxo UDP (aos 40 segundos) tem no tráfego VoIP de entrada, provocando uma maior variabilidade da taxa de transmissão deste último, mas sempre à volta do valor 66 KBps.

Já na simulação EF verifica-se que o tráfego VoIP não sofre qualquer impacto com a activação do tráfego UDP.

Simultaneamente, o fluxo de tráfego TCP continua a sofrer degradação significativa de serviço, após activação do fluxo UDP, nas duas simulações. Isto acontece

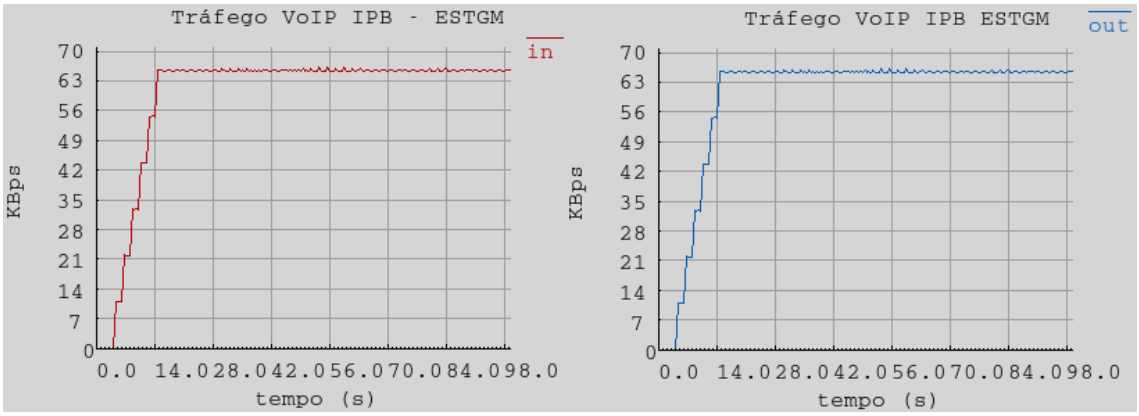

Figura 6.9: Simulação EF: tráfego VoIP entre IPB e ESTGM

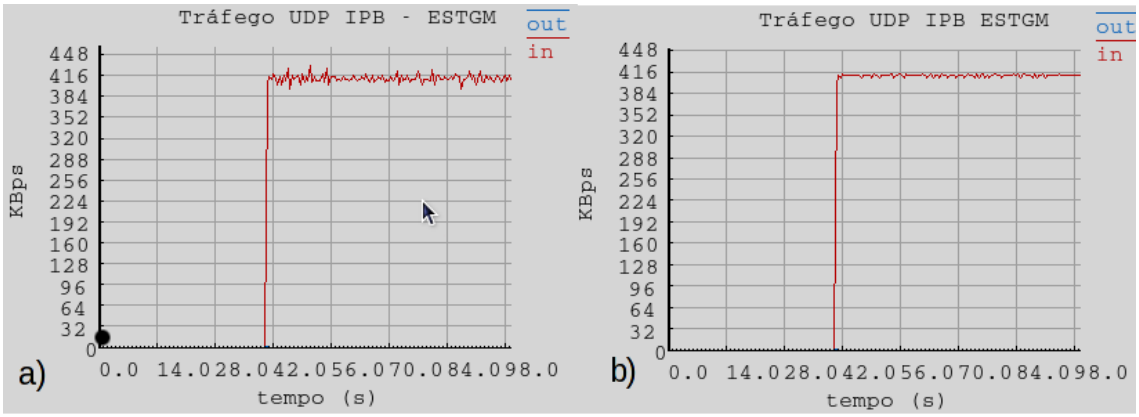

Figura 6.10: Tráfego UDP entre IPB e ESTGM: a) simulação AF; b) simulação EF

porque este tráfego recebe a mesma classificação que o tráfego UDP. Esta degradação nota-se fundamentalmente ao nível da taxa de transmissão (figura 6.11), já que, como descrito anteriormente, o TCP ajusta o fluxo em função dos recursos disponíveis, o que faz com que a taxa de pacotes perdidos, e consequentemente retransmitidos, se mantenha em valores significativamente baixos.

Comprovada a adequabilidade da taxa de perda de pacotes na operação dos fluxos VoIP descritos, procederemos de seguida à análise dos outros dois factores relevantes para assegurar uma QoS adequada a este serviço: atraso e *jitter*.

Os gráficos das figuras 6.12 e 6.13 apresentam o comportamento do atraso e do *jitter* nos fluxos VoIP para as duas simulações em análise.

As tabelas 6.7 e 6.8 apresentam uma sintese dos valores médios finais de percentagem de pacotes perdidos, atraso e *jitter* para cada um dos seis fluxos VoIP.

Com base na análise destas tabelas, podemos verificar o seguinte:

- simulação AF: o atraso apresenta valores médios entre os 8 e os 10 milisegundos. Se analisarmos o comportamento deste parâmetro para os diversos fluxos ao longo do tempo (figura 6.12, a)), verificamos que, até ao instante 40 segundos, o intervalo de valores se situa entre os cinco e os oito milisegundos. A partir deste instante (quando se inicia o fluxo UDP), o atraso médio passa

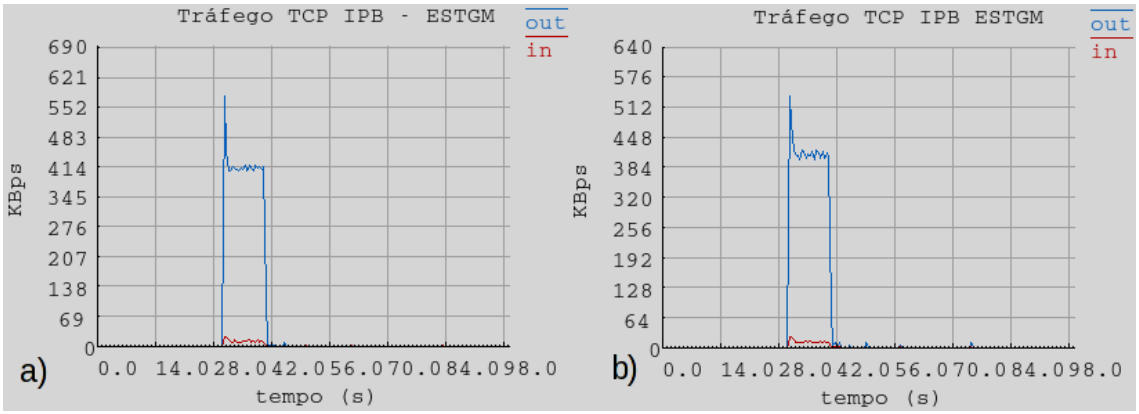

Figura 6.11: Tráfego TCP entre IPB e ESTGM: a) simulação AF; b) simulação EF

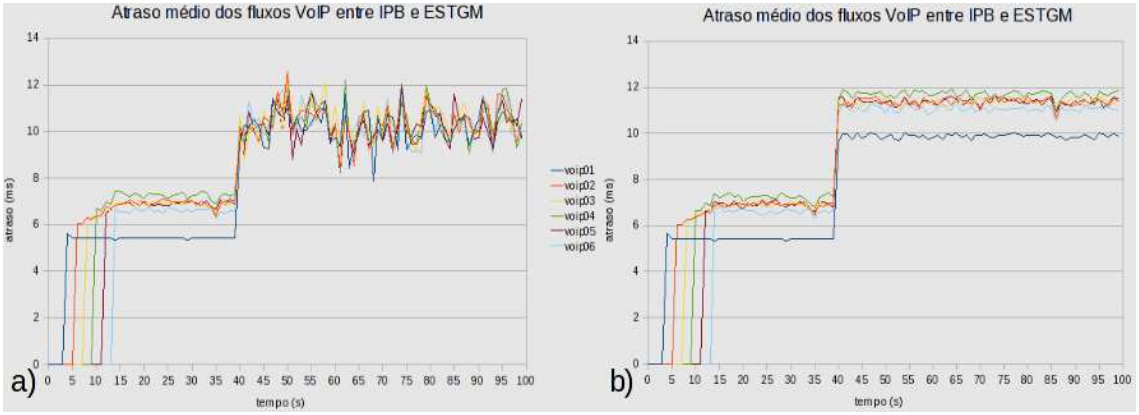

Figura 6.12: Atraso dos fluxos VoIP entre IPB e ESTGM: a) simulação AF; b) simulação EF

para um intervalo de valores entre os oito e os doze milisegundos, mas com alguma variabilidade ao longo do tempo.

- simulação EF: o atraso apresenta valores médios entre os 8 e os 10,4 milisegundos. Analisando o comportamento deste parâmetro para os diversos fluxos ao longo do tempo (figura 6.12, b)), verificamos que, até ao instante 40 segundos, o comportamento é similar ao da simulação AF (intervalo de valores entre os cinco e os oito milisegundos). A partir deste instante (quando se inicia o fluxo UDP), o atraso médio passa para um intervalo de valores entre os dez e os doze milisegundos, mas com uma variabilidade mínima ao longo do tempo.

Na sequência do descrito na secção 5.1, considera-se que uma conversação VoIP deixa de ser perceptível a partir de valores de atraso superiores a 150 ms em cada sentido. Assim, podemos afirmar que, quanto ao factor **atraso**, a aplicação das medidas de prioritização descritas em cada uma das simulações foram eficazes para assegurar a qualidade do serviço VoIP.

Por último, constata-se que a variação média do *jitter* nos seis fluxos em apreciação se situa entre os três e os cinco milisegundos, para a simulação AF e entre os

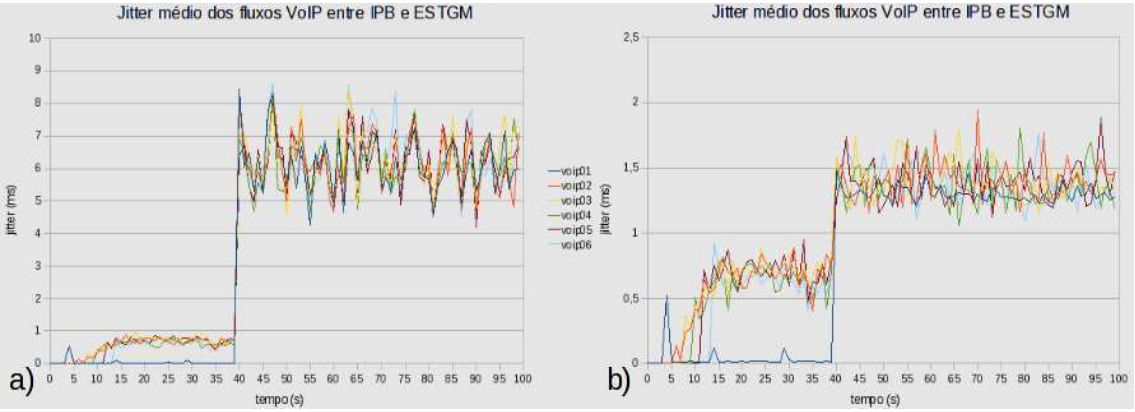

Figura 6.13: *Jitter* dos fluxos VoIP entre IPB e ESTGM: a) simulação AF; b) simulação EF

Fluxo	% Pac. perdidos	Atraso médio	Jitter médio
voip01	0.186%	8.574	3.918
voip02	0.317%	9.267	4.274
voip03	0.368%	9.396	4.426
voip04	0.309%	9.491	4.369
voip05	0.407%	9.401	4.523
voip06	0.440%	9.403	4.655

Tabela 6.7: Simulação AF: perda de pacotes, atraso e *jitter* do tráfego VoIP entre IPB e ESTGM

0,8 milisegundos e os 1,2 milisegundos, para a simulação EF. Analisando o comportamento deste parâmetro ao longo do tempo (figura 6.13), verificamos que:

- para a simulação AF, até ao instante em que o fluxo UDP se inicia (40 segundos), o valor médio de *jitter* se situa entre os zero e 1 milisegundos. A partir deste instante, e por efeito do referido fluxo UDP, o *jitter* médio cresce para valores entre os 4 e os 9 milisegundos.

- para a simulação EF, o valor médio de *jitter* situa-se entre os 0 e 1 milisegundos até ao instante em que o fluxo UDP se inicia (40 segundos). Após esse instante, este valor médio cresce ligeiramente, para valores entre os 1 e os 2 milisegundos. Continuam no entanto a ser valores muito baixos, quando comparados com os valores obtidos com a simulação AF.

Na secção 5.1 referiu-se que, a partir de um *jitter* de 30 ms, a qualidade da voz sofre uma degradação significativa. Desta forma, podemos concluir que, também para este parâmetro, com a implementação das políticas de prioritização descritas e testadas nas duas simulações *DiffServ* realizadas, conseguimos assegurar a qualidade de serviço necessária à realização das seis chamadas de voz com qualidade aceitável.

Pode também concluir-se que, embora com a classificação AF do tráfego VoIP se consiga assegurar as condições mínimas para manter um serviço adequado, é com

Fluxo	% Pac. perdidos	Atraso médio	Jitter médio
voip01	0%	8.374	.843
voip02	0%	9.893	1.138
voip03	0%	9.973	1.175
voip04	0%	10.384	1.150
voip05	0%	10.142	1.194
voip06	0%	9.906	1.184

Tabela 6.8: Simulação EF: perda de pacotes, atraso e *jitter* do tráfego VoIP entre IPB e ESTGM

a classificação EF e correspondente tratamento diferenciado dado aos pacotes VoIP que se consegue o mais elevado nível de qualidade de serviço para estes fluxos.

6.3 Testes realizados na ligação entre a Rede do IPB e a RCTS/Internet

A ligação de dados entre a Rede do IPB e a Internet, via RCTS - Rede Ciência, Tecnologia e Sociedade, é garantida por um circuito dedicado de 100 Mbps, entregue ao IPB com terminação física *Fast-Ethernet*.

Trata-se de uma ligação com um débito limitado, que se encontra próximo da capacidade máxima de utilização durante uma boa parte do tempo (ver gráfico da figura 6.14). Por este motivo, à semelhança da ligação *Campus de Santa Apolónia – ESTGM*, também nesta é de fundamental importância o estabelecimento de políticas de tratamento diferenciado do tráfego de voz que se pretende transportar sobre a mesma.

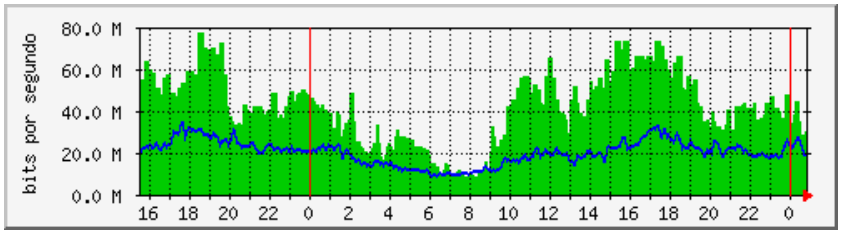

Figura 6.14: Ocupação da linha de dados entre o IPB e a RCTS/Internet

O conjunto de testes apresentados a seguir pretende ajudar a determinar uma configuração para implementação de um serviço de transporte de tráfego VoIP entre os dois extremos desta ligação, com um nível de qualidade de serviço adequado.

A ligação da rede telefónica do Campus de Santa Apolónia à rede pública é assegurada por três acessos primários RDIS (90 canais de voz simultâneos). Considerando que os requisitos de QoS são idênticos para os 90 canais, assumir-se-á, para efeitos de simulação, a utilização simultânea de trinta canais (um acesso primário RDIS). Depois de encontrados os valores adequados para garantir QoS a estes trinta

canais, podem facilmente extrapolar-se esses valores para assegurar QoS aos noventa canais referidos.

Com base nos pressupostos enunciados, procedeu-se à realização de um conjunto de testes no simulador *NCTUns*, com o objectivo de avaliar sobre a possibilidade de garantir a realização das chamadas simultâneas referidas, sem interferência do restante tráfego de dados. Para este efeito, foi usada a topologia representada na figura 6.15.

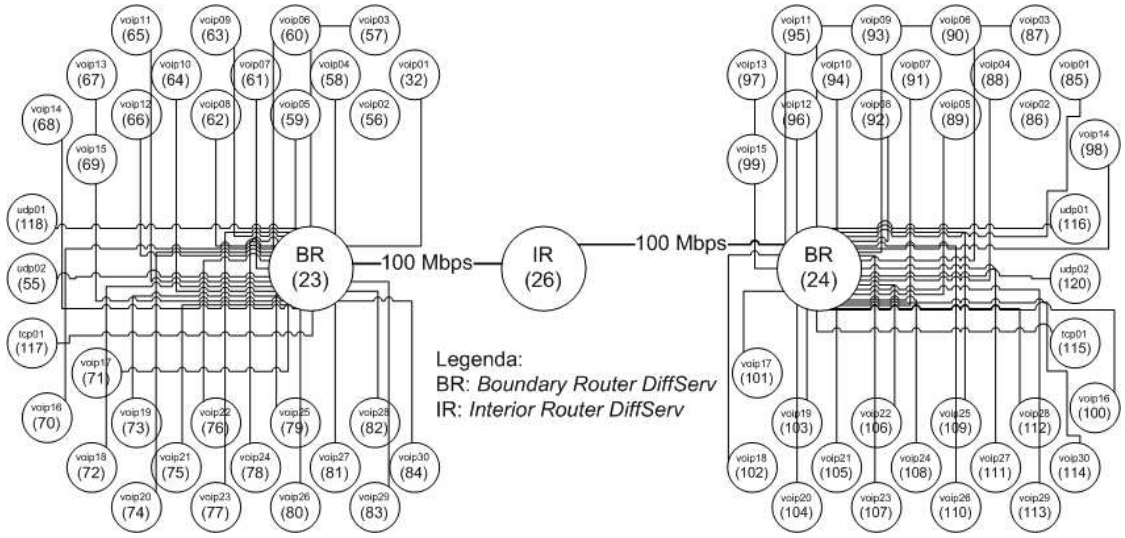

Figura 6.15: Topologia de rede usada nos testes entre a Rede do Campus de Santa Apolónia e a RCTS

Os tipos de aplicações usados na simulação e as respectivas características são idênticas às usadas na simulação da secção anterior e descritas na secção 6.1, variando apenas o número de fluxos activados (tabela 6.9). Tendo o link em teste um débito de 100 Mbps, optou-se nesta simulação por activar dois fluxos de tráfego UDP, para garantir uma saturação da ligação por este tipo de tráfego.

Todas as simulações realizadas tiveram uma duração de 100 segundos, sendo o início dos fluxos faseado, entre o segundo 1 (1º fluxo VoIP) e o segundo 40 (fluxos UDP).

Considerando que a saturação da ligação em análise se dá habitualmente no sentido *RCTS – IPB*, os valores obtidos e as análises efectuadas nas secções seguintes são baseadas nas informações recolhidas no encaminhador de fronteira da rede do Campus de Santa Apolónia (host 23).

6.3.1 Testes sem prioritização de tráfego

Numa primeira fase, procedeu-se à simulação dos fluxos descritos na tabela 6.9 sem qualquer tipo de prioritização (todos os fluxos tratados num princípio *best-effort*).

Na tabela 6.10 são apresentados os resultados desta primeira simulação, em termos de valores de pacotes enviados, recebidos e perdidos (em valor e percentagem).

Como se pode constatar pela análise destes resultados, a taxa de pacotes perdidos nos fluxos VoIP é muito significativa (sempre acima dos 52%), o que, na prática,

Fluxo	Host Origem	Local	Serviço	Host Destino	Local	Tráfego
voip01	85	Internet	VoIP	32	IPB	VoIP
voip02	86	Internet	VoIP	56	IPB	VoIP
voip03	87	Internet	VoIP	57	IPB	VoIP
voip04	88	Internet	VoIP	58	IPB	VoIP
voip05	89	Internet	VoIP	59	IPB	VoIP
voip06	90	Internet	VoIP	60	IPB	VoIP
voip07	91	Internet	VoIP	61	IPB	VoIP
voip08	92	Internet	VoIP	62	IPB	VoIP
voip09	93	Internet	VoIP	63	IPB	VoIP
voip10	94	Internet	VoIP	64	IPB	VoIP
voip11	95	Internet	VoIP	65	IPB	VoIP
voip12	96	Internet	VoIP	66	IPB	VoIP
voip13	97	Internet	VoIP	67	IPB	VoIP
voip14	98	Internet	VoIP	68	IPB	VoIP
voip15	99	Internet	VoIP	69	IPB	VoIP
voip16	100	Internet	VoIP	70	IPB	VoIP
voip17	101	Internet	VoIP	71	IPB	VoIP
voip18	102	Internet	VoIP	72	IPB	VoIP
voip19	103	Internet	VoIP	73	IPB	VoIP
voip20	104	Internet	VoIP	74	IPB	VoIP
voip21	105	Internet	VoIP	75	IPB	VoIP
voip22	106	Internet	VoIP	76	IPB	VoIP
voip23	107	Internet	VoIP	77	IPB	VoIP
voip24	108	Internet	VoIP	78	IPB	VoIP
voip25	109	Internet	VoIP	79	IPB	VoIP
voip26	110	Internet	VoIP	80	IPB	VoIP
voip27	111	Internet	VoIP	81	IPB	VoIP
voip28	112	Internet	VoIP	82	IPB	VoIP
voip29	113	Internet	VoIP	83	IPB	VoIP
voip30	114	Internet	VoIP	84	IPB	VoIP
tcp01	115	Internet	TCP	117	IPB	TCP
udp01	116	Internet	UDP	118	IPB	UDP
udp02	120	Internet	UDP	55	IPB	UDP

Tabela 6.9: Identificação dos fluxos estabelecidos entre a rede do IPB e a Internet

Fluxo	Pacotes enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4969	2337	2632	52.968%
voip02	4919	2355	2564	52.124%
voip03	4869	2254	2615	53.707%
voip04	4819	2227	2592	53.787%
voip05	4768	2186	2582	54.152%
voip06	4718	2074	2644	56.040%
voip07	4668	2099	2569	55.034%
voip08	4618	2009	2609	56.496%
voip09	4568	1952	2616	57.267%
voip10	4517	1967	2550	56.453%
voip11	4467	1873	2594	58.070%
voip12	4417	1803	2614	59.180%
voip13	4367	1751	2616	59.903%
voip14	4317	1691	2626	60.829%
voip15	4267	1643	2624	61.495%
voip16	4216	1631	2585	61.314%
voip17	4166	1562	2604	62.506%
voip18	4116	1512	2604	63.265%
voip19	4066	1454	2612	64.240%
voip20	4016	1431	2585	64.367%
voip21	3965	1368	2597	65.498%
voip22	3915	1329	2586	66.053%
voip23	3865	1254	2611	67.554%
voip24	3815	1218	2597	68.073%
voip25	3764	1168	2596	68.969%
voip26	3714	1107	2607	70.193%
voip27	3664	1068	2596	70.851%
voip28	3614	1012	2602	71.997%
voip29	3564	941	2623	73.597%
voip30	3514	897	2617	74.473%
tcp01	21687	20005	1682*	7.755%*
udp01	493898	242612	251286	50.878%
udp02	493903	249367	244536	49.510%

Tabela 6.10: Resultado da primeira simulação, apenas com tráfego *best-effort*

impede um correcto funcionamento deste serviço. Os fluxos VoIP iniciados mais tarde (mais próximo do instante em que são activados os fluxos de tráfego UDP) são os que apresentam percentagem de perdas maior, visto o período de tempo em que estiveram activos sem congestionamento do canal ter sido menor.

Apesar do tráfego TCP também ter sido severamente afectado pelo congestionamento provocado pelo tráfego UDP (em termos de taxa de transmissão), o número de pacotes retransmitidos mantém-se relativamente baixo. Tal deve-se à actuação dos mecanismos de controlo de congestão do TCP referidos atrás, que ajustam a taxa de envio às capacidades do canal em cada momento.

A figura 6.16 apresenta o tráfego VoIP de entrada e saída, no encaminhador de fronteira (host 23) da Rede do Campus de Santa Apolónia.

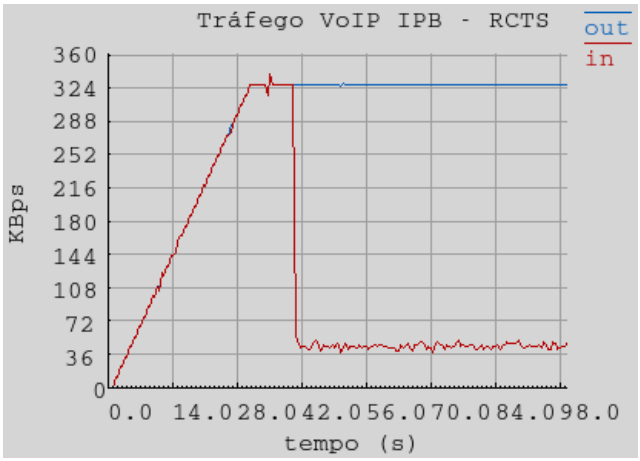

Figura 6.16: Tráfego dos fluxos VoIP entre a Rede do IPB e a Internet, sem priorização

Tal como já foi referido anteriormente, cada fluxo VoIP simulado ocupa 88 Kbps (11 KBps) em cada sentido. Assim, os trinta fluxos simultâneos devem gerar uma taxa constante de 2640 Kbps (330 KBps) em cada sentido.

Como se pode verificar na figura 6.16, o tráfego VoIP que sai da rede do IPB mantém essa taxa constante (linha azul) ao longo de toda a simulação (até ao segundo 40 a linha azul não é visível no gráfico porque é sobreposta pela linha que representa o tráfego de entrada - linha vermelha). O tráfego VoIP que chega à entrada da Rede do IPB mantém-se constante nos valores previstos apenas até ao instante *40 seg*, altura em que se iniciaram os fluxos de tráfego UDP entre as duas redes. A partir deste momento, o tráfego UDP vai saturar a ligação, no sentido Internet - IPB (figura 6.17), afectando automaticamente os fluxos VoIP (figura 6.16) e TCP activos (figura 6.18).

Concluíndo esta análise, pode-se afirmar que, sem utilização de um mecanismo de QoS adequado, não é possível assegurar o funcionamento do serviço VoIP nos termos descritos anteriormente.

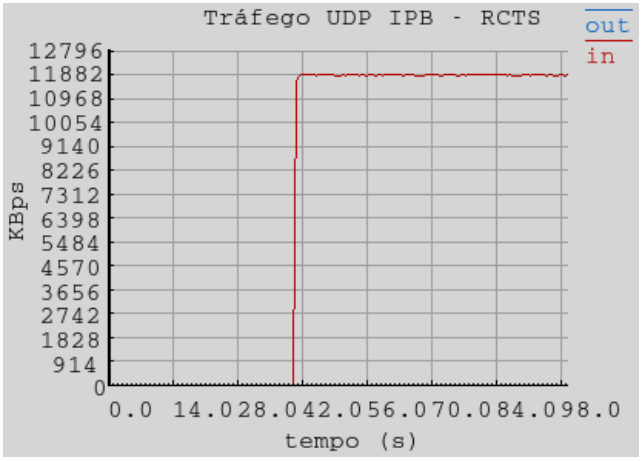

Figura 6.17: Tráfego UDP entre a Rede do IPB e a Internet, sem prioritização

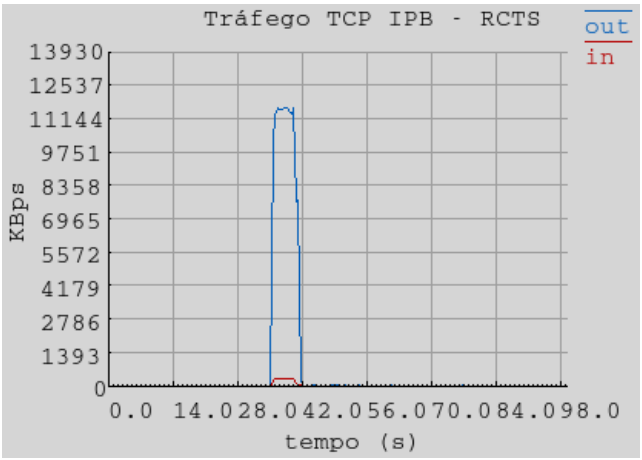

Figura 6.18: Tráfego TCP entre a Rede do IPB e a Internet, sem prioritização

6.3.2 Testes com prioritização do tráfego VoIP

Tal como para a ligação *Campus de Santa Apolónia – ESTGM*, também neste caso se repetiram os testes realizados na secção anterior, mantendo as mesmas características de tráfego da simulação anterior mas introduzindo prioritização *DiffServ*.

Procedeu-se assim à realização de duas simulações distintas, baseadas na topologia da figura 6.15 e com as seguintes características:

- a) *DiffServ* com marcações, e respectivos PHBs, AF e BE (adiante designada apenas por simulação AF).

  Nesta simulação, o tráfego VoIP foi marcado com o *codepoint* **001010** (*PHB AF11*), sendo portanto colocado na fila da classe AF1 e recebendo o tratamento associado a essa classe, nos encaminhadores *DiffServ* do domínio. O restante tráfego TCP e UDP foi marcado com o *codepoint* **000000** (*PHB BE*), recebendo portanto um tratamento *best-effort*. A tabela 6.11 sintetiza as configurações *DiffServ* aplicadas no simulador para tratamento das classes usadas.

Classe DiffServ	% do canal alocado	largura de banda alocada	Tipo de Tráfego
AF11	1/33	3 Mbps	VoIP
BE	32/33	97 Mbps	TCP e UDP

Tabela 6.11: Classificação DiffServ implementada no link IPB–Internet: simulação AF

Classe DiffServ	% do canal alocado	largura de banda alocada	Tipo de Tráfego
EF	1/33	3 Mbps	VoIP
BE	32/33	97 Mbps	TCP e UDP

Tabela 6.12: Classificação DiffServ implementada no link IPB–Internet: simulação EF

Pode ver-se na referida tabela que é alocado 1/33 do canal de comunicação para a classe AF1, ficando os restantes 32/33 para o tráfego BE.

- b) *DiffServ* com marcações, e respectivos PHBs, EF e BE (adiante designada apenas por simulação EF).

  Neste caso, o tráfego VoIP foi marcado com o *codepoint* **101110** (*PHB EF*), sendo portanto colocado na fila da classe EF e recebendo em consequência o tratamento associado a essa classe. O restante tráfego TCP e UDP foi marcado com o *codepoint* **000000** (*PHB BE*), recebendo portanto um tratamento *best-effort*. Na tabela 6.4 apresenta-se um sintese das configurações usadas pelos encaminhadores *DiffServ* do domínio para tratamento do tráfego EF e BE.

A tabela 6.13 evidencia os resultados da simulação AF, em termos de valores de pacotes enviados, recebidos e perdidos (retransmitidos no caso do fluxo TCP), enquanto a tabela 6.14 apresenta os dados equivalentes para a simulação EF.

Em resultado da implementação das políticas de prioritização referidas, constata-se que,

- na simulação AF, a percentagem de pacotes perdidos nos fluxos VoIP desce para valores abaixo de 1%.

- na simulação EF não existem pacotes VoIP perdidos.

De acordo com o descrito na secção 5.1, considera-se que a qualidade de uma conversação VoIP é irremediavelmente afectada com taxas de perdas acima de 1%. Neste sentido, podemos afirmar que, quanto ao factor **perda de pacotes**, a aplicação das medidas de prioritização descritas foi eficaz para assegurar os requisitos mínimos de qualidade do serviço VoIP. No caso da simulação AF, este requisitos situam-se próximo do limite aceitável, mas ainda assim, dentro desse limite. As políticas implementadas na simulação EF foram completamente eficazes para garantir uma condição de zero pacotes perdidos.

Fluxo	Pacotes enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4969	4942	27	.543%
voip02	4919	4891	28	.569%
voip03	4869	4846	23	.472%
voip04	4819	4795	24	.498%
voip05	4768	4740	28	.587%
voip06	4718	4689	29	.614%
voip07	4668	4639	29	.621%
voip08	4618	4600	18	.389%
voip09	4568	4552	16	.350%
voip10	4517	4496	21	.464%
voip11	4467	4442	25	.559%
voip12	4417	4393	24	.543%
voip13	4367	4342	25	.572%
voip14	4317	4286	31	.718%
voip15	4267	4246	21	.492%
voip16	4216	4194	22	.521%
voip17	4166	4143	23	.552%
voip18	4116	4093	23	.558%
voip19	4066	4044	22	.541%
voip20	4016	3990	26	.647%
voip21	3965	3946	19	.479%
voip22	3915	3892	23	.587%
voip23	3865	3847	18	.465%
voip24	3815	3790	25	.655%
voip25	3764	3743	21	.557%
voip26	3714	3694	20	.538%
voip27	3664	3628	36	.982%
voip28	3614	3579	35	.968%
voip29	3564	3541	23	.645%
voip30	3514	3478	36	1.024%
tcp01	32448	23772	8676*	26.738%*
udp01	493944	242659	251285	50.873%
udp02	493952	237496	256456	51.919%

Tabela 6.13: Simulação AF: análise dos pacotes perdidos

	Pacotes			
Fluxo	enviados	recebidos	perdidos (retransm.*)	% perdidos (retransm.*)
voip01	4969	4969	0	0%
voip02	4919	4919	0	0%
voip03	4869	4869	0	0%
voip04	4819	4819	0	0%
voip05	4768	4768	0	0%
voip06	4718	4718	0	0%
voip07	4668	4668	0	0%
voip08	4618	4618	0	0%
voip09	4568	4568	0	0%
voip10	4517	4517	0	0%
voip11	4467	4467	0	0%
voip12	4417	4417	0	0%
voip13	4367	4367	0	0%
voip14	4317	4317	0	0%
voip15	4267	4267	0	0%
voip16	4216	4216	0	0%
voip17	4166	4166	0	0%
voip18	4116	4116	0	0%
voip19	4066	4066	0	0%
voip20	4016	4016	0	0%
voip21	3965	3965	0	0%
voip22	3915	3915	0	0%
voip23	3865	3865	0	0%
voip24	3815	3815	0	0%
voip25	3764	3764	0	0%
voip26	3714	3714	0	0%
voip27	3664	3664	0	0%
voip28	3614	3614	0	0%
voip29	3564	3564	0	0%
voip30	3514	3514	0	0%
tcp01	23763	20752	3011*	12.670%*
udp01	493927	240100	253827	51.389%
udp02	493940	240098	253842	51.391%

Tabela 6.14: Simulação EF: análise dos pacotes perdidos

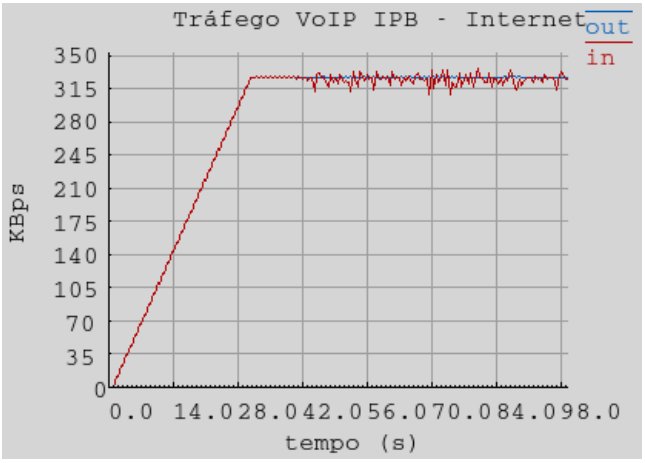

Figura 6.19: Simulação AF: tráfego VoIP entre IPB e a Internet

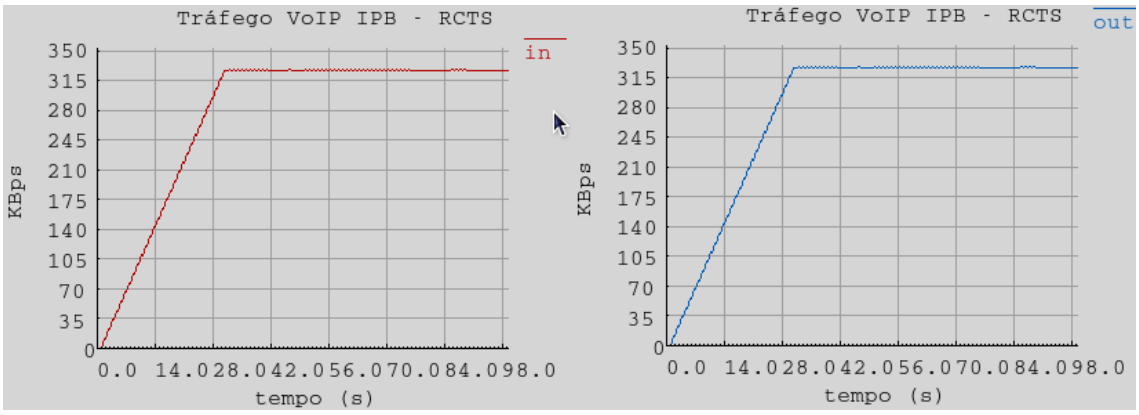

Figura 6.20: Simulação EF: tráfego VoIP entre IPB e a Internet

Nestas simulações, o tráfego UDP deixa de saturar por completo a totalidade do canal de comunicação. Verifica-se que o tráfego VoIP mantém um débito médio à volta dos 2640 Kbps (330 KBps), como se pode comprovar nos gráficos das figuras 6.19 (simulação AF) e 6.20 (simulação EF). É também visível, na simulação AF (6.19, o efeito que a activação do fluxo UDP (aos 40 segundos) tem no tráfego VoIP de entrada, provocando uma maior variabilidade da taxa de transmissão deste último, mas sempre à volta do valor 2640 KBps. Já na simulação EF verifica-se que o tráfego VoIP não sofre qualquer impacto com a activação do tráfego UDP.

Simultaneamente, o fluxo de tráfego TCP continua a sofrer degradação significativa de serviço, após activação dos fluxos UDP, nas duas simulações. Isto acontece porque este tráfego recebe a mesma classificação que o tráfego UDP. Esta degradação nota-se fundamentalmente ao nível da taxa de transmissão (figura 6.22), já que, como descrito anteriormente, o TCP ajusta o fluxo em função dos recursos disponíveis, o que faz com que a taxa de pacotes retransmitidos se mantenha em valores relativamente baixos.

Comprovada a adequabilidade da taxa de perda de pacotes na operação dos fluxos VoIP descritos, procederemos de seguida à análise do atraso e do *jitter*, considerados igualmente factores relevantes para assegurar uma QoS adequada a este serviço.

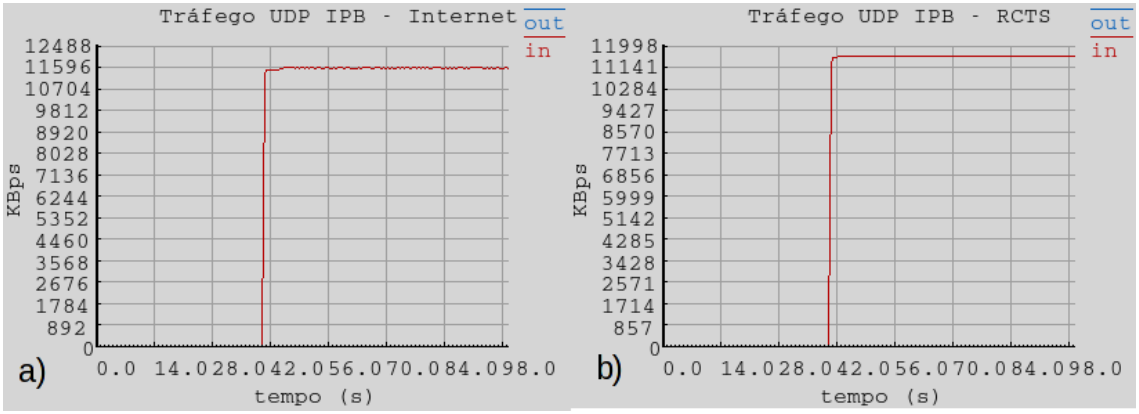

Figura 6.21: Tráfego UDP entre IPB e a Internet: a) simulação AF; b) simulação EF

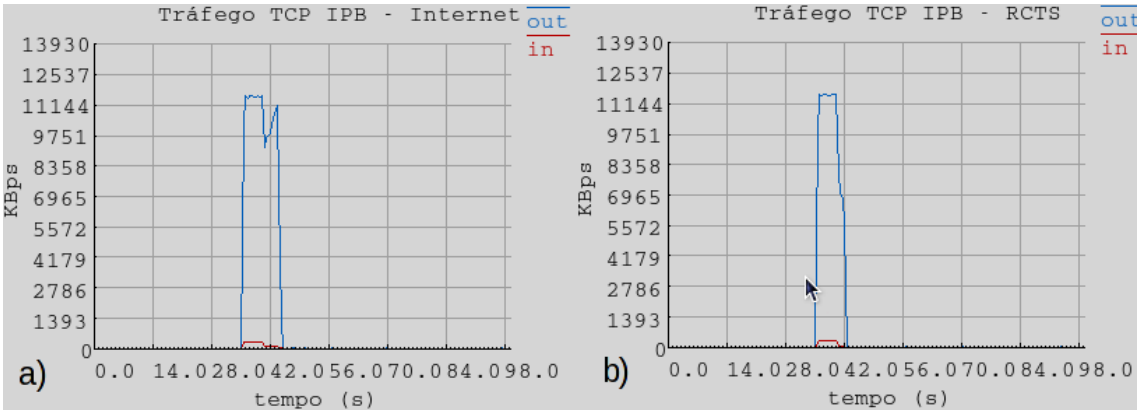

Figura 6.22: Tráfego TCP entre IPB e a Internet: a) simulação AF; b) simulação EF

Os gráficos das figuras 6.23 e 6.24 evidenciam o comportamento do atraso e do *jitter* de uma amostra de fluxos VoIP (fluxos *voip01, voip05, voip10, voip15, voip20, voip25 e voip30*), para as duas simulações em análise. Optou-se por representar graficamente os dados relativos a apenas este conjunto de fluxos para manter o gráfico mais legível. Como todos os fluxos VoIP recebem idêntico tratamento da rede, o comportamento dos restantes é similar ao destes.

As tabelas 6.15 e 6.16 apresentam uma sintese dos valores médios finais de percentagem de pacotes perdidos, atraso e *jitter* para cada um dos trinta fluxos VoIP.

Com base na análise destas tabelas, podemos verificar o seguinte:

- simulação AF: o atraso apresenta valores médios entre os 7 e os 10 milisegundos. Se analisarmos o comportamento deste parâmetro para os diversos fluxos ao longo do tempo (figura 6.23, a)), verificamos que, até ao instante 40 segundos, o intervalo de valores se situa entre os 3 e os 4 milisegundos. A partir deste instante (quando se inicia o fluxo UDP), o atraso médio passa para um intervalo de valores entre os 8 e os 12 milisegundos, mas com uma variabilidade significativa ao longo do tempo, dentro deste intervalo referido.

Fluxo	% Pac. perdidos	Atraso médio	Jitter médio
voip01	.54%	7.586	3.239
voip02	.56%	7.814	3.205
voip03	.47%	7.845	3.260
voip04	.49%	7.944	3.365
voip05	.58%	7.909	3.356
voip06	.61%	7.946	3.311
voip07	.62%	8.010	3.470
voip08	.38%	8.119	3.588
voip09	.35%	8.082	3.533
voip10	.46%	8.178	3.600
voip11	.55%	8.286	3.735
voip12	.54%	8.308	3.705
voip13	.57%	8.373	3.640
voip14	.71%	8.406	3.761
voip15	.49%	8.596	3.718
voip16	.52%	8.578	3.831
voip17	.55%	8.576	3.847
voip18	.55%	8.699	3.906
voip19	.54%	8.751	3.948
voip20	.64%	8.752	4.012
voip21	.47%	8.855	4.127
voip22	.58%	8.993	4.077
voip23	.46%	8.988	4.247
voip24	.65%	9.090	4.295
voip25	.55%	9.072	4.257
voip26	.53%	9.237	4.430
voip27	.98%	9.308	4.367
voip28	.96%	9.370	4.369
voip29	.64%	9.467	4.516
voip30	1.02%	9.440	4.631

Tabela 6.15: Simulação AF: perda de pacotes, atraso e *jitter* do tráfego VoIP entre IPB e a Internet

Fluxo	% Pac. perdidos	Atraso médio	Jitter médio
voip01	0%	3.674	.160
voip02	0%	3.859	.158
voip03	0%	3.862	.160
voip04	0%	3.865	.168
voip05	0%	3.871	.165
voip06	0%	3.879	.169
voip07	0%	3.885	.170
voip08	0%	3.888	.174
voip09	0%	3.894	.172
voip10	0%	3.895	.172
voip11	0%	3.899	.172
voip12	0%	3.905	.179
voip13	0%	3.910	.179
voip14	0%	3.914	.178
voip15	0%	3.920	.177
voip16	0%	3.925	.186
voip17	0%	3.926	.184
voip18	0%	3.930	.185
voip19	0%	3.935	.184
voip20	0%	3.949	.186
voip21	0%	3.943	.189
voip22	0%	3.953	.187
voip23	0%	3.951	.188
voip24	0%	3.957	.189
voip25	0%	3.961	.185
voip26	0%	3.965	.184
voip27	0%	3.966	.181
voip28	0%	3.975	.186
voip29	0%	3.976	.188
voip30	0%	3.976	.184

Tabela 6.16: Simulação EF: perda de pacotes, atraso e *jitter* do tráfego VoIP entre IPB e a Internet

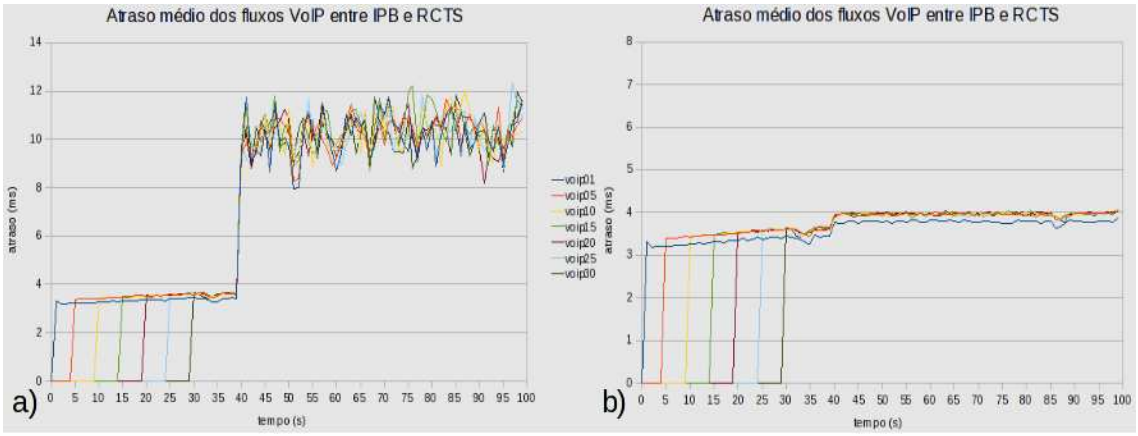

Figura 6.23: Atraso dos fluxos VoIP entre IPB e a Internet: a) simulação AF; b) simulação EF

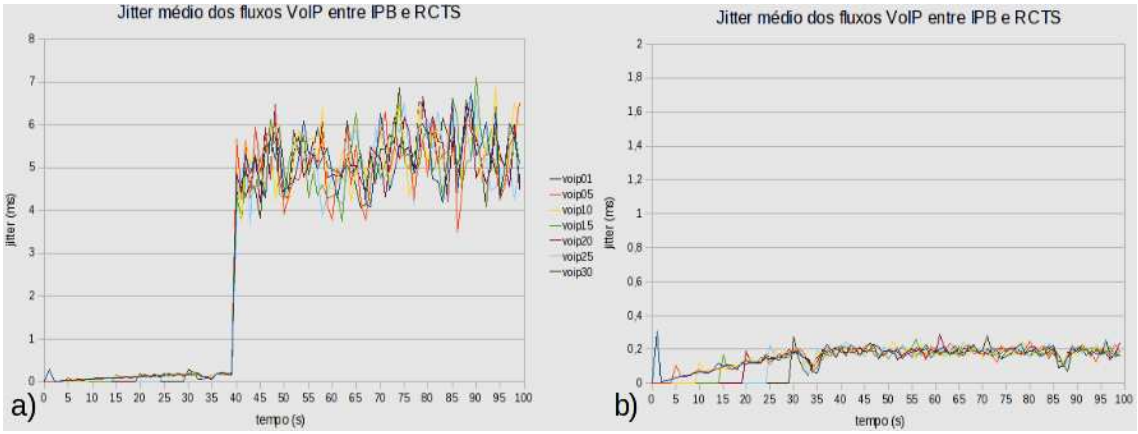

Figura 6.24: *Jitter* dos fluxos VoIP entre IPB e a Internet: a) simulação AF; b) simulação EF

- simulação EF: o atraso apresenta valores médios entre os 3,6 e os 4 milisegundos. Analisando o comportamento deste parâmetro para os diversos fluxos ao longo do tempo (figura 6.23, b)), verificamos que se nota um ligeiro aumento a partir do instante 40 segundos, mas mesmo assim quase insignificante, mantendo-se sempre no intervalo de valores entre 3 e 4 milisegundos até ao fim da simulação.

Considerou-se anteriormente que uma conversação VoIP deixa de ser perceptível a partir de valores de atraso superiores a 150 ms em cada sentido. Neste sentido, e após a análise atrás apresentada, podemos afirmar que, quanto ao factor **atraso**, a aplicação das medidas de prioritização descritas também foram eficazes para assegurar a qualidade do serviço VoIP. As políticas definidas na simulação AF são eficazes, no entanto, obtém-se ainda melhores resultados com as políticas da simulação EF.

Por último, constata-se que a variação média do *jitter* nos trinta fluxos em apreciação se situa entre os três e os cinco milisegundos, para a simulação AF e entre os 0,15 milisegundos e os 0,2 milisegundos, para a simulação EF. Analisando o com-

portamento deste parâmetro ao longo do tempo (figura 6.24), verificamos que:

- simulação AF: até ao instante em que o fluxo UDP se inicia (40 segundos), o valor médio de *jitter* se situa entre os zero e 1 milisegundos. A partir deste instante, e por efeito do referido fluxo UDP, o *jitter* médio cresce para valores entre os 3,5 e os 7 milisegundos.

- simulação EF: o valor médio de *jitter* começa em valores muito próximo de zero e vai crescendo gradualmente até que estabiliza, por volta do segundo 40, em torno dos 0,2 milisegundos. Trata-se no entanto de valores extremamente baixos, mesmo quando comparados com os obtidos na simulação AF.

Tendo-se constatado anteriormente que é possível manter uma conversação de voz com boa qualidade com um *jitter* até 30 ms (desde que os outros parâmetros identificados estejam também dentro dos limites aceitáveis), podemos concluir que, também no que depende deste parâmetro, a implementação das políticas de priorização descritas permitem assegurar a qualidade de serviço necessária à realização das trinta chamadas de voz com qualidade aceitável, no caso da simulação AF e com excelente qualidade, no caso da simulação EF.

Capítulo 7

Conclusões e perspectivas de trabalho futuro

7.1 Conclusões do trabalho realizado

Concluídos, no capítulo anterior, os trabalhos de teste e análise de resultados, importa, nesta recta final, proceder a uma análise retrospectiva do trabalho realizado, extraír daí algumas conclusões e delinear perspectivas de desenvolvimentos futuros à volta do tema abordado.

Os objectivos traçados para este trabalho incluiam:

- a descrição dos trabalhos de implementação de um serviço VoIP no Instituto Politécnico de Bragança – projecto VoIP@IPB – e sua interacção com um outro projecto promovido à escala nacional pela FCCN – projecto VoIP@RCTS;
- a identificação dos principais requisitos de QoS para implementação de um serviço VoIP e definição das métricas usadas na sua medição;
- a identificação dos pontos críticos, ao nível da infra-estrutura de rede, que pudessem condicionar o funcionamento do serviço VoIP@IPB;
- o teste e a avaliação, recorrendo a um ambiente de simulação, de diferentes alternativas de implementação de QoS, por forma a assegurar o normal funcionamento do serviço VoIP nos pontos indicados atrás.

O primeiro objectivo foi cumprido ao longo do capítulo 4, com a identificação das motivações que deram origem ao projecto VoIP@IPB, a descrição da sua arquitectura, dos detalhes de implementação e estado actual.

Da análise realizada, concluiu-se que a rede telefónica convencional do IPB é actualmente uma infra-estrutura desactualizada e com algumas limitações estruturais.

Concluiu-se também que, ao contrário da primeira, a rede de dados desta instituição é, na generalidade, uma infra-estrutura recente, correctamente dimensionada e com capacidade para acomodar eficazmente novos serviços de rede que sobre ela venham a ser desenvolvidos. Há no entanto dois pontos da infra-estrutura que são excepções a esta situação, já que se constituem como pontos de estrangulamento de tráfego e que, por isso mesmo, importa monitorizar e gerir com mais atenção:

- Ligação entre a Rede do Campus de Santa Apolónia e a rede da ESTGM.

  Trata-se de um circuito MPLS de 4 Mbps, alugado a um operador de telecomunicações, que é utilizado para transportar o tráfego de dados, gerado por mais de 1000 utilizadores, entre esta escola e: a) os serviços electrónicos do IPB, localizados num *datacenter* no Campus de Santa Apolónia (e-mail, diversos serviços web internos, aplicações administrativas); b) a Internet.

  Dado o baixo débito desta ligação, quando comparado com padrões de débito actuais, a mesma mostra sinais de congestionamento durante parte significativa de um dia normal de funcionamento da Instituição.

- Ligação entre a Rede do IPB e a Internet. É actualmente baseada num circuito de 100 Mbps, gerido pela FCCN, que permite o acesso diário de até 6700 alunos e mais de 500 funcionários (docentes e não docentes) à Internet.

Feita a identificação e caracterização destes dois pontos, procedeu-se de seguida à análise dos factores determinantes para o funcionamento de um serviço VoIP em conformidade com o esperado. Desta análise, resultou a identificação dos seguintes parâmetros e respectivos limites máximos toleráveis por um serviço deste tipo:

- perda de pacotes: trata-se de um factor cujo limite de tolerância varia significativamente de codec para codec. No entanto, genericamente é aceite o valor de 1% de perdas como limite máximo acima do qual o serviço se degrada irremediavelmente.

- atraso: de acordo com a norma G.114 da ITU-T [73], o atraso máximo fim-a-fim não deve ultrapassar os 150 milisegundos.

- *jitter*: o valor de 30 milisegundos é normalmente aceite como o limite máximo para a variação do atraso em serviços deste tipo.

Definido o âmbito de actuação do presente trabalho – avaliação dos requisitos necessários à operação de serviços VoIP nos dois links identificados atrás – e caracterizados os parâmetros a avaliar – perda de pacotes, atraso e *jitter* –, partiu-se de seguida para a realização de um conjunto de testes, em ambiente de simulação, com o objectivo de determinar quais as políticas mais adequadas para assegurar o normal funcionamento do serviço VoIP referido.

Para a realização destes testes, recorreu-se à utilização do simulador e emulador de tráfego *NCTUns*. Apesar das vantagens apresentadas por esta ferramenta (descrita na secção 5.2), importa concluir nesta fase que a mesma apresenta também algumas limitações, nomeadamente ao nível da documentação de alguns modelos e protocolos suportados. Em concreto, não foi possível identificar e caracterizar, com o detalhe e rigor necessários, os mecanismos de escalonamento de pacotes usados nas implementações dos PHB AF e EF da *framework DiffServ*.

Os testes foram realizados em simulações independentes para cada um dos pontos identificados. Para cada um destes pontos, foram divididos em duas categorias:

- a) testes sem aplicação de políticas de QoS, ou seja, todo o tráfego tratado em modo *best-effort*;

- b) aplicando um tratamento diferenciado ao tráfego VoIP relativamente ao restante tráfego. Nesta fase, foram avaliadas duas alternativas de tratamento diferenciado:
  - i) *DiffServ* com marcação e PHB AF para tráfego VoIP e marcação BE para restante tráfego;
  - ii) *DiffServ* com marcação e PHB EF para tráfego VoIP e marcação BE para restante tráfego.

Dos resultados obtidos, cuja análise detalhada foi efectuada ao longo do capítulo 6, podem extrair-se as seguintes conclusões finais:

- Sem a implementação de um mecanismo de tratamento diferenciado, o tráfego VoIP é irremediavelmente afectado pelo restante tráfego de rede, em situações de congestão. Em situações deste tipo, muito facilmente a perda de pacotes ultrapassa o limite aceitável de 1%, provocando por isso a inoperacionalidade do serviço.

- A implementação de mecanismos de diferenciação com base na *framework DiffServ* revelou-se adequada para condicionar o tráfego, em função das políticas definidas.

- A utilização do *DiffServ* com marcação e PHB AF para o tráfego VoIP e marcação BE para o restante tráfego, nas ligações em análise, revelou minimizar o impacto negativo produzido no tráfego VoIP pela situação de congestionamento.

  Com um correcto dimensionamento do *rate limiting* das classes AF e BE, é possível assegurar o funcionamento de um serviço VoIP dentro dos limites mínimos aceitáveis, não podendo no entanto estes limites ser considerados óptimos. Não é possível assegurar um serviço VoIP com óptimas condições de funcionamento fundamentalmente devido ao factor perdas de pacotes, já que, de acordo com os testes realizados, a eliminação completa deste factor negativo demonstra-se impossível em situações de congestão na rede.

- Com políticas *DiffServ* baseadas na marcação e PHB EF para o tráfego VoIP e marcação BE para o restante tráfego, é possível, para as ligações em análise e de acordo com os pressupostos descritos, assegurar a operacionalidade do serviço VoIP descrito com a máxima qualidade.

  Nesta situação, pode verdadeiramente classificar-se este como um Serviço *Premium* oferecido pela rede, já que os valores obtidos para os 3 parâmetros em apreciação – perda de pacotes, atraso e *jitter* –, se situam sempre próximos dos intervalos mínimos óptimos em função das caracteristicas das infra-estruturas físicas.

  De facto, a implementação do PHB EF com base na utilização de um mecanismo de escalonamento do tipo *priority queuing* garante aos serviços que dele usufruem o melhor nível de qualidade de serviço. Porque este mecanismo dá

completa primazia ao tráfego EF relativamente ao restante tráfego, torna-se fundamental garantir que este não vai absorver a maior parte (ou mesmo a totalidade) dos recursos existentes. A utilização de um mecanismo do tipo *token bucket* é altamente recomendada para evitar esta situação.

7.2 Perspectivas de trabalho futuro

Retiradas as devidas conclusões do trabalho produzido, importa agora traçar algumas linhas de orientação sobre perspectivas de desenvolvimentos futuros do mesmo.

Os testes efectuados ao longo do presente trabalho ficaram limitados à avaliação de dois cenários concretos, que foram tratados de forma independente. Na realidade, cada um destes cenários pode também interagir com o outro já que, com a implementação do projecto VoIP@RCTS, as chamadas VoIP com origem na ESTGM e destino em números externos ao IPB terão de atravessar os dois pontos identificados (o oposto também se verifica). Por este motivo, em termos de trabalho futuro, poderá e deverá ser também equacionada a análise do comportamento do transporte de tráfego VoIP, desde a ESTGM, passando pela infra-estrutura do Campus de Santa Apolónia, até à RCTS.

Como foi referido, o projecto VoIP@IPB visa a implementação de um serviço VoIP sobre a infra-estrutura de comunicação de dados do IPB. Tal significa que, não apenas os dois pontos analisados, mas toda a infra-estrutura será utilizada para transportar tráfego VoIP.

Apesar de uma infra-estrutura de rede local se encontrar normalmente sobredimensionada face à sua taxa de utilização diária, tal não quer dizer que seja possível assegurar, na totalidade do tempo, todas as condições necessárias ao correcto funcionamento de um serviço de VoIP. Dadas as características do tráfego que normalmente circula numa rede local de média ou grande dimensão, há naturalmente situações esporádicas em que também ocorre congestão ou atrasos e variações de atraso acima do normal.

Surge assim uma outra perspectiva de análise, que pode ser desenvolvida na sequência deste trabalho: avaliação das características de uma rede de campus e determinação dos mecanismos necessários para assegurar o funcionamento de serviços VoIP com qualidade nestas infra-estruturas.

Tratando-se tipicamente de infra-estruturas bastante heterogéneas, quer em termos de tráfego que aí circula, quer em termos de equipamentos que as suportam, uma possível abordagem poderá passar pela respectiva segmentação lógica em diferentes VLAN's (IEEE 802.1Q) e consequente implementação de mecanismos de QoS de nível 2, com base na norma IEEE 802.1p. Fica no entanto esta perspectiva em aberto para análise mais detalhada em eventuais trabalhos futuros que dêm continuidade ao aqui apresentado.

Bibliografia

[1] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. *RTP: A Transport Protocol for Real-Time Applications. RFC 3550*. IETF. 2003

[2] J. Rosenberg et. al. *SIP: Session Initiation Protocol. RFC 3261*. IETF. 2002

[3] D. Kuhn, T. Walsh, S. Fries. *Security Considerations for Voice Over IP Systems*. Recommendations of the National Institute of Standards and Technology - NIST. 2005.

[4] *Integrated Services (IntServ) charter em http://www.ietf.org/html.charters/intserv-charter.html*.

[5] *Differentiated Services (DiffServ) charter em http://www.ietf.org/html.charters/diffserv-charter.html*.

[6] J. Postel. *Internet Protocol. RFC 791*. USC/Information Sciences Institute, 1981.

[7] J. Mogul. *Broadcasting Internet Datagrams. RFC 919*. 1984.

[8] J. Mogul. *Broadcasting Internet Datagrams in the Presence of Subnets. RFC 922*. 1984.

[9] J. Mogul, J. Postel. *Internet Standard Subnetting Procedure. RFC 950*. 1985.

[10] E. Gerich. *Guidelines for Management of IP Address Space. RFC 1466*. 1993.

[11] K. Hubbard, M. Kosters, D. Conrad, D. Karrenberg, J. Postel. *Internet Registry IP Allocation Guidelines. RFC 2050*. 1996.

[12] S. Kirkpatrick, M. Stahl, M. Recker. *Internet Numbers. RFC 1166*. 1990.

[13] R. Hinden. *Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR). RFC 1517*. 1993.

[14] Y. Rekhter, T. Li. *An Architecture for IP Address Allocation with CIDR. RFC 1518*. 1993.

[15] V. Fuller, T. Li, J. Yu, K. Varadhan. *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy. RFC 1519*. 1993.

[16] Y. Rekhter, C. Topolcic. *Exchanging Routing Information Across Provider Boundaries in the CIDR Environment. RFC 1520*. 1993.

[17] J. Hawkinson, T. Bates. *Guidelines for creation, selection, and registration of an Autonomous System (AS). RFC 1930*. 1996.

[18] C. Hedrick. *Routing Information Protocol. RFC 1058*. 1988.

[19] G. Malkin. *RIP Version 2. Carrying Additional Information. RFC 1723*. 1994.

[20] J. Moy. *OSPF Version 2. RFC 2328*.

[21] Y. Rekhter, T. Li. *A Border Gateway Protocol 4 (BGP-4). RFC 1771*. 1995.

[22] S. Bradner, A. Mankin. *The Recommendation for the IP Next Generation Protocol. RFC 1752*. 1995.

[23] S. Deering, R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification. RFC 1883*. 1995.

[24] A. Santos. *IPv6 - A nova versão do protocolo IP*. DI, Universidade do Minho, 1998.

[25] R. Gilligan, E. Nordmark. *Transition Mechanisms for IPv6 Hosts and Routers. RFC 1933*. 1996.

[26] R. Callon, D. Haskin. *Routing Aspects Of IPv6 Transition. RFC 2185*. 1997.

[27] P. Izzo. *Gigabit Networks: Standards and Schemes for next-generation networking*. John Wiley and Sons, Inc, 2000.

[28] F. Halsall. *Data Communications, Computer Networks and Open Systems*. Addison–Wesley, 4th edition, 1996.

[29] R. Braden, D. Clark, S. Shenker. *Integrated Services in the Internet Architecture: an Overview. RFC 1633.* 1994.

[30] S. Shenker, J. Wroclawski. *General Characterization Parameters for Integrated Service Network Elements. RFC 2215*. 1997.

[31] S. Shenker, J. Wroclawski. *Network Element Service Specification Template. RFC 2216*. 1997.

[32] K. Nichols, S. Blake, F. Baker, D. Black. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474*. 1998.

[33] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. *An Architecture for Differentiated Services. RFC 2475*. 1998.

[34] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. *Assured Forwarding PHB Group. RFC 2597*. 1999.

[35] B. Davie, A. Charny, J.C.R. Bennett et al. *An Expedited Forwarding PHB. RFC 3246*. 2002.

[36] K. Nichols, V. Jacobson, L. Zhang. *A Two-bit Differentiated Services Architecture for the Internet. RFC 2638*. 1999.

[37] S. Floyd, V. Jacobson. *Random Early Detection Gateways for Congestion Avoidance*. IEEE/ACM Transactions on Networking, V.1 N.4, 1993, p. 397-413.

[38] S. Floyd, R. Gummadi, S. Shenker. *Adaptive RED: An Algorithm for Increasing the Robustness of RED's Active Queue Management*. AT&T Center for Internet Research at ICSI. 2001.

[39] D. Lin, R. Morris. *Dynamics of Random Early Detection*. Proceedings from ACM SIGCOMM 97. 1997, p. 127-137.

[40] J. Saltzer, D. Reed, D. Clark. *End to End Arguments in System Design*. ACM Transactions in Computer Systems, 1984.

[41] *White Paper - The Need for QoS*. Stardust.com, Inc, 1999.

[42] P. Fegunson, G. Huston. *Quality of Service in the Internet: Fact, Fiction or Compromise?*. INET'98, 1998.

[43] J. Wroclawski. *Specification of the Controlled-Load Network Element Service. RFC 2211*. 1997.

[44] S. Shenker,C. Partridge, R. Guerin. *Specification of Guaranteed Quality of Service. RFC 2212*. 1997.

[45] R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin. *Resource Reservation Protocol (RSVP) – Version 2 Functional Specification. RFC 2205*. 1997

[46] J. Wroclawski. *The use of RSVP with IETF Integrated Services. RFC2210*. 1997

[47] E. Monteiro, F. Boavida. *Engenharia de Redes Informáticas*. FCA, 2000.

[48] J. Postel. *User Datagram Protocol. RFC 768*. 1980.

[49] J. Postel. *Transmission Control Protocol. RFC793*. 1981.

[50] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear. *Address Allocation for Private Internets. RFC 1918*. 1996.

[51] *IEEE 802.11, Wireless LAN MAC and Physical Layer Specifications*. Editors of IEEE, 1997.

[52] X. Xiao, L. Ni. *Internet QoS: the Big Picture*. Department of Computer Science, Michigan State University. 1999.

[53] E. Rosen, A. Viswanathan, R. Callon. *Multiprotocol Label Switching Architecture. RFC 3031*. 2001.

[54] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas. *LDP Specification. RFC 3036*. 2001.

[55] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus. *Requirements for Traffic Engineering over MPLS. RFC 2702*. 1999.

[56] E. Crawley, R. Nair, B. Rajagopalan, H. Sandick. *A Framework for QoS-based Routing in the Internet. RFC 2386*. 1998.

[57] S. Floyd, and V. Jacobson. *Link-sharing and Resource Management Models for Packet Networks*. IEEE/ACM Transactions on Networking, Vol. 3 No. 4, pp. 365-386, 1995.

[58] S. McCanne, S. Floyd. *ns-2 Network Simulator, http://www.isi.edu/nanam/ns/*.

[59] E. Menezes, D. Sadok, J. Kelner, P. Pereira, P. Pinto. *Service Management for Differentiated Services Networks*.

[60] R. Gibbens, S. Sargood, F. Kelly, H. Azmoodeh, R. Macfadyen, N. Macfadyen. *An Approach to Service Level Agreements for IP networks with Differentiated Services*. Statistical Laboratory, University of Cambridge, 2000.

[61] Y. Bernet, P. Ford, R. Yavatkar, F. Baker, L. Zhang, M. Speer, R. Braden, B. Davie, J. Wroclawski, E. Felstaine. *A Framework for Integrated Services Operation over Diffserv Networks. RFC 2998*. 2000.

[62] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. *SIP: Session Initiation Protocol. RFC 3261*. 2002.

[63] *Página do OpenSER, http://www.kamailio.org*, acesso em Janeiro de 2009

[64] *Página do Asterisk: http://www.asterisk.org*, acesso em Janeiro de 2009

[65] *Página da Digium: http://www.digium.com*, acesso em Janeiro de 2009

[66] P. Faltstrom, M. Mealling. *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM). RFC 3761*, IETF. 2004

[67] N. Rodrigues, A. Alves. *Implementação de Serviços de Telefonia IP numa Instituição de Ensino Superior.* Procedings do WCSETE'2006 - World Congress on Computer Science, Enginneering and Technology Education, pág. 925 a pág. 929, Santos/SP, 19/3/2006

[68] *Página do projecto VoIP@RCTS: http://www.fccn.pt/voip*. FCCN, acedido em 12/2008.

[69] M. Paredes-Farrera, M. Fleury, M. Ghanbari. *Precision and Accuracy of Network Traffic Generators for Packet-by-Packet Traffic Analysis*, University of Essex, United Kingdom. 2006.

[70] ITU-T P-Series Recommendations. *Methods for Subjective Determination of Transmission Quality - Series P: Telephone Transmission Quality; Methods for Objective and Subjective Assessment of Quality*, ITU-T. 1996.

[71] ITU-T P-Series Recommendations. *P.862: Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs*, ITU-T. 2001.

[72] Cisco Whitepaper. *Quality of Service for Voice over IP*, Cisco Systems.

[73] ITU-T G-Series Recommendations. *ITU-T Recommendation G.114: One-way transmission time*, ITU-T. 2003.

[74] T. Szigeti, C. Hattingh. *End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs*, Cisco Press. 2005.

[75] N. Carvalho, L. Guido, M. Baptista. *VoIP@RCTS: Requisitos mínimos de LAN e WAN*, FCCN. 2007.

[76] *Página do simulador OPNET: http://www.opnet.com.* acedido em 01/2009.

[77] S.Y. Wang, C.L. Chou, C.H. Huang, C.C. Hwang, Z.M. Yang, C.C. Chiou, and C.C. Lin *The Design and Implementation of the NCTUns 1.0 Network Simulator*. Computer Networks, Vol. 42, Issue 2, June 2003, pp.175-197.

[78] S.Y. Wang, H. T. Kung. *A simple methodology for constructing extensible and high-fidelity TCP/IP network simulators*. IEEE INFOCOM099, March 21-25, New York, USA, 1999.

[79] S.Y. Wang, C.L. Chou and C.C. Lin. *The GUI User Manual for the NCTUns 4.0 Network Simulator and Emulator*. Network and System Laboratory, Department of Computer Science, National Chiao Tung University, Taiwan. 2007.

[80] *Página do simulador NCTUns: http://nsl10.csie.nctu.edu.tw.* acedido em 01/2009.