Instituto Superior de Engenharia do Porto
Departamento de Engenharia Informática

Voz Sobre IP e Qualidade de Serviço

Projecto
Licenciatura em Engenharia Informática
Ramo de Computadores e Sistemas

Setembro 2004

Elaborado por:
1010874 – Paulo Terra

Orientador:
Eng.º Jorge Pinto Leite

Resumo

Na era da informação, a convergência entre a informática e as telecomunicações constituem um vector tecnológico fundamental para o desenvolvimento económico. As novas tecnologias são parte integrante do nosso quotidiano. Oferecem instrumentos úteis com enorme impacto nas pessoas e nas organizações.
A concorrência, a necessidade de oferecer cada vez mais e melhores serviços, é um dos principais objectivos das organizações nos nossos dias. Para satisfazer esta pretensão, as empresas começaram a dar mais importância à gestão adequada das suas infra-estruturas de rede.
Esta tendência é bem visível nos fabricantes de equipamentos de telecomunicações, que fazem acompanhar as suas soluções com aplicações de gestão mais robustas e eficientes.
Se ao que foi dito, adicionarmos o fenómeno Internet, o enorme crescimento e implantação das redes IP (*Internet Protocol*), o aparecimento de técnicas avançadas de digitalização de voz, mecanismos de controlo e diferenciação de tráfego e novos protocolos de transmissão em tempo real leva-nos a concluir que: é possível transmitir voz em pacotes IP.
A voz sobre pacotes IP (VOIP) é um tema interessante do ponto vista estratégico para o mundo empresarial. É a possibilidade de integrar voz e dados na mesma infra-estrutura de rede, de comunicar a custos mais baixos, é a porta de entrada para novos e melhores serviços. Imagine a possibilidade de integração desta tecnologia com ferramentas *web*, *call center*, *contact centers* e muitas outras funcionalidades. Lentamente, a telefonia IP vai ganhando terreno face às tecnologias tradicionais de comunicação de voz.

Este trabalho pretende explicar o funcionamento básico da telefonia IP, assim como, estudar os mecanismos necessários para a transmissão de voz e dados sobre a mesma rede.

I. Agradecimentos

Gostaria de agradecer, em primeiro lugar, ao Eng.º Jorge Pinto Leite, como meu orientador, me deu todo o apoio necessário, mostrando enorme disponibilidade sempre que o solicitei.

Gostaria também de agradecer a minha mãe e à minha namorada, todo o apoio prestado ao longo da realização deste projecto.

II. Lista de Acrónimos e Abreviaturas

ABR	Available Bit Rate
ACL	Access Control Lists
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Institute
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
AVVID	Architecture for Voice, Video, and Integrated Data
BGP	Border Gateway Protocol
BRI	Basic Rate Interface
CAC	Call Admission Control
CBR	Constant Bit Rate
CBWFQ	Class Based Weighted Fair Queuing
CCM	Cisco Call Manager
CME	Call Manager Express
CIR	Committed Information Rate
COS	Class Of Service
CQ	Custom Queuing
CRRC	Contributing Source Identifier
CRTP	Compressed Real-Time Transport
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSP	Digital Signal Processor
DSU	Digital Service Unit
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FDM	Frequency Division Multiplexing
FIFO	First In First Out
FTP	File Transfer Protocol
GK	Gatekeeper
GW	Gateway
GSM	Global System for Mobile Communications
HDLC	High-level Data Link Control
HDSL	High bit-rate DSL
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IMAP	Internet Message Access Protocol
IntServ	Integrated Services
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union – Telecommunications Sector
IVR	Interactive Voice Response
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LD-CELP	Low- Delay Code Excited Linear Prediction
MAC	Medium Access Control
MC	Multipoint Controller

MCM	Management Call Manager
MCU	Multipoint Conferencing Unit
MMUSIC	Multipart Multimedia Session Control
MP	Multipoint Processor
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
ODBC	Open Database Control
Nrt-VBR	non real time Variable Bit Rate
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
POP	Point of Presence
PPCA	Posto Privado de Comutação Automático
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
PQ	Priority Queuing
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAS	Registration Admission Status
RED	Random Early Detection
RDIS	Rede Digital com Integração de Serviços
RFC	Request For Comments
RIP	Routing Information Protocol
RJ45	Registered Jack 45
ROI	Return of Investment
RSVP	Resource Reservation Protocol
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SSRC	Synchronization Source Identifier
TACACS	Terminal Access Controller Access
TAPI	Telephony Application Programming Interface
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TIFF	Tagged Image File Format
TOS	Type of Service
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UMS	Unified Messaging System
URL	Uniform Resource Locator
VLAN	Virtual Local Area Connection
VoATM	Voice Over ATM
VoFR	Voice Over Frame Relay
VoIP	Voice Over IP
VPN	Virtual Private Network
XML	Extensible Markup Language
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WWW	World Wide Web

III. Índice Geral

IV. Índice de Figuras

V. Índice de Tabelas

1. Introdução

Apesar das condicionantes económicas, o mercado das telecomunicações tem evoluído de uma forma consistente. Numa altura em que só se fala em reduzir custos e controlar despesas, o tema telefonia IP volta a estar na mente de muitos gestores. Trata-se de uma tecnologia com algum tempo de vida, e com boa aceitação no mercado. As grandes organizações foram as primeiras a adoptar esta tecnologia, actualmente qualquer empresa pode adquiri-la. Mas antes de optar por uma solução deste tipo, é aconselhável procurar uma justificação. Por que é que se necessita de uma solução VoIP? Muitas vezes, não são só as questões económicas que interessam as organizações contudo, é um dos factores relevantes na adopção da telefonia IP.
São muitas as razões que levam as organizações a adoptar as soluções VoIP: Mudança para novas instalações, sistemas de cablagem únicos para voz e dados, soluções de voz obsoletas e a rebentar pelas costuras, implementação de novos serviços como voice-mail ou IVR (*Interactive Voice Response*) e reduzir o valor da factura mensal das comunicações intra-empresa. Esta adopção é gradual, as empresas vão introduzindo esta tecnologia nos locais onde faça mais sentido e interligando-a com os sistemas de voz convencionais existentes.
Para garantir fiabilidade e um conjunto de funcionalidades superiores às existentes actualmente com dispositivos digitais, são necessárias implementações complexas de qualidade de serviço (QoS) em redes convergentes de voz e dados. Estas questões e implementações vão estudadas detalhadamente ao longo deste trabalho.

1.1. Enquadramento do Projecto

Este projecto foi efectuado no âmbito da cadeira de projecto do 5º ano do curso de Licenciatura em Engenharia Informática, ramo Computadores e Sistemas.

1.2. Objectivos Propostos

Este projecto, pretende de uma forma geral dar a conhecer o funcionamento básico da telefonia IP da Cisco e estudar detalhadamente políticas de qualidade de serviço (QoS) a implementar numa solução VoIP com vista a:

- garantir um conjunto de funcionalidades superiores aos dispositivos de voz tradicionais;
- rentabilizar as larguras de banda disponíveis;
- detectar valores limites;
- metodologia de implementação perante parâmetros.

1.3. Estrutura do Trabalho

A estrutura do relatório é a seguinte:
O **Capitulo 2** apresenta os conceitos de VoIP, telefonia IP e a sua capacidade associada a aplicações complementares. Apresenta as motivações para a implementação de uma solução VoIP, explicando como é que esta tecnologia pode reduzir os custos e conquistar novos patamares de integração das comunicações de voz e dados, elevando a produtividade dos colaboradores nas empresas.
No **Capitulo 3** é feita uma abordagem aos protocolos (recomendações) H.323 e SIP que suportam a telefonia IP. São também apresentados conceitos teóricos do TCP/IP e o endereçamento IP, não de uma forma exaustiva, mas de modo a identificar claramente o *background* necessário para implementação de uma solução VoIP.
No **Capitulo 4** é descrito o papel do QoS em redes de comutação de pacotes. São apresentadas as razões da importância do QoS em soluções VoIP. Serão discutidos os diferentes níveis de classe/qualidade de serviço.
No **Capitulo 5** são descritos exemplos e comandos essenciais para a implementação de uma solução VoIP, assim como, exemplos típicos de configurações QoS.
Finalmente, no **Capitulo 6** faço uma retrospectiva do trabalho realizado.

2. Introdução á Voz Sobre IP (VoIP)

2.1. A Importância das Telecomunicações

A evolução das tecnologias de informação, contribuíram em larga escala para o aparecimento de ferramentas úteis e com enorme impacto nas pessoas e nas organizações.
Se pensarmos nas telecomunicações e sua relevância no nosso quotidiano, verificamos que estamos rodeados de sistemas com enorme utilidade. As funções essenciais das telecomunicações são:

- assegurar a comunicação entre terminais, telefones computadores, etc.;
- disponibilizar serviços (Internet) função dos ISP (*Internet Service Provider*);
- oferecer acessos a serviços partilhados.

Com o IP, as redes e serviços de comunicações passam por uma evolução tecnológica que reduz os preços e agrega novas funcionalidades, levando as grandes e médias empresas a aderir à Voz sobre IP e à Telefonia IP, para reduzir custos e conquistar novos patamares de integração das comunicações de voz e dados, elevando a produtividade dos colaboradores.

Bem-vindo ao mundo da voz sobre pacotes! Apesar da ideia de voz sobre pacotes não ser nova, actualmente existem soluções integradas que a tornam possível. Esta tecnologia está a evoluir tão rapidamente, que há quem diga que, evolui mais rápido que a própria Internet.

2.2. O que é VoIP

A Voz sobre IP (VoIP) sigla que deriva do inglês "*Voice Over IP*", tecnologia que permite a digitalização e codificação de voz em pacotes IP, utilizando para transmissão a rede de comutação de pacotes IP.

Pacote – *Conjunto finito de bits passível de ser transmitido por uma rede de comunicações de comutação por pacotes. Consiste numa sequência de dígitos binários, de acordo com um formato específico, que inclui os dados a transmitir e também os dados relativos à sinalização da ligação.*

A tecnologia VoIP originou dois segmentos de produtos e serviços complementares:

- VoIP – convergência de voz e dados em rede WAN[1], utilizando o ATM, Frame Relay ou mesmo o PPP para a transmissão de voz, com o objectivo à redução dos custos de telecomunicações;

- Telefonia IP – dispositivos para telefonia baseados em IP, operando em rede local (LAN[2]) e visando a facilidade de uso, integração e aumento da produtividade.

[1] ***WAN****: (Wide Area Network) as redes de area alargada são, em regra, instaladas e exploradas por operadores públicos ou privados de telecomunicações, fornecendo serviços para interligação de clientes individuais ou institucionais*

[2] ***LAN*** *– (Local Area Network) As rede locais permitem a interligação de equipamentos numa área relativamente restrita por exemplo, uma zona de um edifício, um edifício ou um campus. Com extensões que, tipicamente, situam abaixo dos 5 Km.*

O uso da tecnologia VoIP oferece uma série de cenários para os utilizadores do serviço, como pode ver na figura 2.1 .

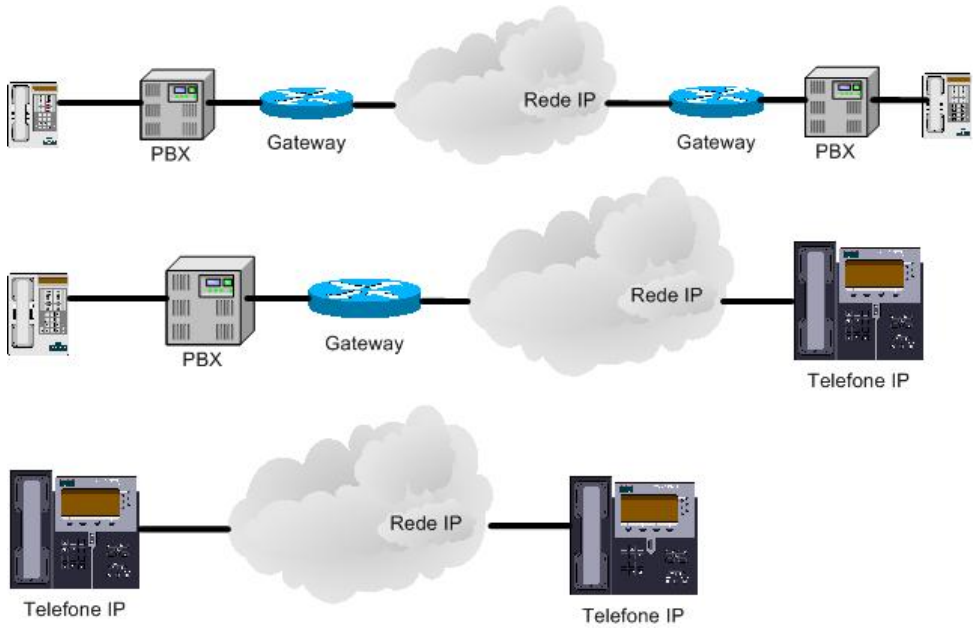

Figura 2.1 – Diversos Cenários VoIP

Na telefonia IP as amostras de voz são acumuladas em pacotes e enviadas pela rede IP. Este envio pode ser encaminhado sem compressão, resultando numa taxa de 64 kbps, tal como iremos ver na telefonia tradicional. No entanto, pode ocorrer compressão, resultando em taxas de voz até 5,3 Kbps, desta forma é possível minimizar a largura de banda utilizada.
Esta tecnologia, por ser baseada em comutação de pacotes, está sujeita a ocorrência de diversos problemas, os quais afectam seriamente a sua qualidade de serviço. Esses problemas são:

- Perda de pacotes;
- Atrasos na entrega de pacotes;
- Variação de atraso (*jitter*).

A Internet é caracterizada por apresentar canais de comunicação com grandes taxas de utilização, obrigando a utilização de filas de espera dos pacotes nas interfaces dos equipamentos de rede. Sendo uma rede onde não existe distinção dos tipos de tráfego, nem responsabilidade a imputar por mau serviço das aplicações. Por esta razão, neste trabalho falaremos apenas de soluções de VoIP e/ou Telefonia IP empresariais, soluções com total garantia de qualidade de serviço tirando o melhor partido das infra-estruturas da rede. O tráfego de Voz é diferenciado de qualquer outro tipo de tráfego, tornando-o prioritário, garantindo assim que não existem atrasos nem quebras nas comunicações de voz.

A velocidade da migração da comunicação de voz tradicional para a IP, na rede telefónica pública (WAN) e empresarial segue factores tecnológicos e económicos.

No público, os investimentos e riscos associados ao tamanho das redes são elevados. Por outro lado, os operadores actuam em regime monopólio. Sendo o risco muito elevado, existe um grande entrave ao desenvolvimento tecnológico nesta área.

No âmbito empresarial, a migração é mais rápida pois a convergência voz e dados, antes cara e restrita às grandes empresas, foi beneficiada pelo aparecimento de novos padrões tecnológicos de encaminhamento de voz sobre IP, produzidos por vários fabricantes especializados, trouxeram a concorrência e a consequente redução de custos.

2.3. Sistemas de Comunicações

Em Portugal as redes são geridas por operadores (operadores de telecomunicações como a ONI, PT, Novis, etc.), que normalmente cobram tarifas pelos serviços de subscrição e utilização. Disponibilizam um conjunto de soluções tecnológicas, permitindo às pessoas e organizações aceder uma grande variedade de serviços, como por exemplo, sistemas de

comunicação elementares, dispositivos para aceder a informação cultural, serviços para aumentar a eficácia das empresas com sistemas de comunicação internos e externos, comercio electrónico, etc.

2.3.1. Classificação das Redes de Telecomunicações

As redes de telecomunicações podem ser consideradas públicas ou privadas. As públicas são que fornecem serviços ao público em geral, as privadas são destinadas exclusivamente ao uso próprio, por empresas ou instituições de grande dimensão.

As redes podem ser ainda classificadas quanto à configuração como: redes endereçadas e rede de difusão.
Nas redes endereçadas, a informação é enviada a um ou mais destinatários predeterminados, através de endereçamento, podendo ou não haver bidireccionalidade.
Nas redes de difusão a informação é enviada num só sentido, para vários ponto de recepção sem endereçamento prévio.

2.3.2. Rede de Voz Tradicional

A rede telefónica pública utiliza fundamentalmente o modo de comutação de circuitos para a transferência de voz pela rede analógica ou digital.

O modo de comutação de circuitos funciona da seguinte forma:

- os recursos são solicitados à rede, no início da chamada através de sinalização
- se a rede tiver disponibilidade, são atribuídos, caso contrário a chamada é rejeitada
- estabelece-se uma conexão entre os sistemas terminais
- pode haver renegociação de recursos ou seja, aumento ou redução de débito
- os recursos são libertados no fim da chamada, através de sinalização

A rede telefónica torna-se atractiva não só como rede de transmissão de informação, mas também como rede de acesso a outras redes (por exemplo, acesso à rede Internet ou acesso a redes ISDN).
A principal limitação da utilização da rede telefónica é ter sido pensada e desenvolvida para a transmissão de voz. Dado que para a transmissão de voz inteligível é apenas necessário a utilização de uma largura de banda de cerca de 3100Hz. Situada entre os 300 e 3400Hz. As ligações telefónicas estão limitadas a este valor. A utilização da linha telefónica para a transmissão de sinais digitais obriga a utilização de modems, que baseiam o seu funcionamento na modulação de amplitude, frequência ou fase de formas de onda analógicas. Mais recentemente são utilizadas tecnologias como o ADSL (*Asymmetric Digital Subscriber Line*) que suportam na mesma linha voz e dados, disponibilizando maior largura de banda.

Um dos aspectos relevantes sobre a utilização das linhas telefónicas é o facto das comunicações serem em função da duração da comunicação e da distância (local, regional, nacional, internacional).

O aparecimento do RDIS, levou a rede digital até ao utilizador. Foram definidos dois tipos de acesso:

- acesso básico (2B+D): dois canais B a 64 kbit/s e um canal D de dados/sinalização a 16 kbit/s; débito total de 192 kbit/s (inclui um canal de sincronização e controlo);
- acesso primário (30B+D): trinta canais B a 64 kbit/s e um canal D de dados/sinalização a 64 kbps; débito total de 2 048 kbit/s (inclui um canal de sincronização e controlo);

São usadas técnicas de multiplexagem para optimizar a utilização dos meios de transmissão.
Em geral, são utilizadas duas técnicas básicas de multiplexagem de sinais:

- multiplexagem por divisão na frequência – (*Frequency Division Multiplexing*, FDM), essencialmente usada para agrupamento e transporte de sinais de voz e/ou sinais analógicos.

- multiplexagem por divisão no tempo – (*Time division Multiplexing* – TDM), para agrupamento e transporte de sinais digitais.

A multiplexagem TDM pode ser feita usando duas hierarquias: a hierarquia Europeia e a hierarquia Americana. A tabela 2.1 e 2.2 resumem essas hierarquias.

Nível	Nº de canais de 64Kbps	Débitos binários
E1 fraccional	N <30	n x 64Kbps
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

Tabela 2.1 – Hierarquia de Multiplexagem Europeia

Nível	Nº de canais de 56Kbps	Débitos binários
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	258048 Mbps

Tabela 2.2 – Hierarquia de Multiplexagem Americana

Os acessos digitais suportam débitos múltiplos de 64 kbps até 2048 kbps (*n* × 64 kbps), permitindo oferecer circuitos dedicados, comutados ou estabelecidos em regime permanente para aplicações de ligação de central local de PPCAs (Postos Privados de Comutação Automática) digitais.

A introdução de sistemas digitais na rede permitiu, entre outras vantagens, rentabilizar meios e oferecer serviços digitais aos assinantes.

Assim, a ligação de centrais digitais às centrais públicas digitais faz-se normalmente sobre ligações a 2 Mbps, correspondentes a 32 canais a 64 kbps, dos quais 30 destinados a comunicações entre utilizadores, um canal de sinalização e um canal de sincronização e controlo. O utilizador pode subscrever a totalidade dos 30 canais disponíveis (circuito E1) ou uma parte deles (por exemplo meio primário, ou seja, 15 canais).

O sistema privado de comutação (PPCA) processa o tráfego entre as suas extensões e assegura a interligação tanto para o tráfego de entrada, como para o tráfego de saída, à rede pública de comutação.

Na telefonia tradicional existe uma conversão analógica-digital que ocorre nas centrais telefónicas (codificação G.711). Essa conversão é baseada na agregação de amostras de voz (de 1 byte) a cada 125µs (frequência de 8Hz), o que se traduz numa largura de banda de 64kbps. Assim, a voz circula num circuito digital de 64Kbps. Sendo essa banda alocada para uma sessão de voz. No extremo o sinal é convertido novamente em analógico para ser enviado ao assinante. Como a telefonia tradicional é baseada em comutação de circuitos, leva a que não existam filas ou ocorram atrasos intermédios.

Quando se estabelece uma chamada na rede de comutação de circuitos é normalmente utilizado um canal de 64Kbps. Isto significa que ao fazer uma chamada, por exemplo, Lisboa Porto é estabelecido um circuito de 64Kbps dedicado desde o início da chamada (Porto) até ao extremo (Lisboa). Quer esteja em conversão ou não, este circuito é dedicado até que a chamada seja desligada, isto significa que mais ninguém pode utilizar este canal.
No caso de um canal de 64 Kbps não estar disponível em qualquer comutação intermédia, o estabelecimento da chamada é interrompido.
Quando se ouve o toque de chamada no destino, significa que o circuito extremo-a-extremo foi estabelecido.

Os operadores de telecomunicações tiveram um grande caminho até conseguirem implementar serviços de chamada em espera, retornar chamada e sistemas de *voicemail*. Este tipo de serviços está agarrado aos sistemas das companhias de comunicações, como por exemplo comutadores, centrais telefónicas, etc.

2.4. A Telefonia IP versus PPCA's

A telefonia IP oferece sistemas programação abertos, se necessitarmos, podemos implementar as nossas próprias aplicações para gestão de chamadas. Isto não seria possível no nosso telefone de casa ou mesmo no trabalho com sistemas PPCA. Os sistemas de voz convencionais, são sistemas fechados e com linguagens de programação específicas. Assim, com sistemas abertos podemos reduzir significativamente os custos de manutenção e suporte aplicacional.
Os PPCAs são sistemas com fraca interoperabilidade. Em sistemas fechados, as alterações ou adições de novos equipamentos terminais são muito dispendiosas. Gostaria de implementar a uma solução de gestão no seu centro de atendimento (*Call Center*)? Com a tecnologia VoIP, é extremamente simples e barato. Tem acesso a toda a documentação que necessita, assim poderá escrever de forma segura o código das suas aplicações. Com sistemas convencionais PPCA, provavelmente, terá que analisar orçamentos para aplicações desenvolvidas por terceiros, que muitas vezes não preenchem os requisitos que pretende, estará a olhar para contractos de manutenção dessas mesmas aplicações, ou a estudar a possibilidade de alteração e reconstrução da aplicação, com custos muito elevados.
Pretende mudar o departamento financeiro para outro piso ou mesmo para ou edifício localizado noutro local? Com o VoIP é simples, apenas terá que pegar nos telefones e liga-los no novo edifício e observar como eles se registam no servidor de gestão (*Call Manger*). Todas as configurações, parâmetros e configurações dos telefones encontram-se no sistema central, sem grande esforço, são novamente associados ao *call manager*. As mesmas actividades com os sistemas tradicionais resultariam na migração das configurações, removendo utilizadores, adicionar esses utilizadores à nova localização, eventualmente para a realização deste serviço seria necessário contratar uma empresa especializada. Mais uma vez, com VoIP as mudanças são completamente transparentes.

2.5. Serviços mais Comuns de Implementação VoIP

Actualmente, a rede pública de telefones usa as redes de comutação de circuitos para transmissão de sinais analógicos. Em contraste, a rede VoIP envia a voz digitalizada sobre rede baseada em comutação de pacotes. Como haveremos de ver, as redes VoIP podem oferecer serviços de voz a preços muito mais competitivos.

O modo de comutação de circuito é uma técnica utilizada para a transferência de informação utilizando redes analógicas ou digitais. Um circuito é suportado directamente sobre um canal físico de comunicação dedicado, onde são usados técnicas de multiplexagem para a sua transmissão. O modo circuito é especialmente adequado para serviços de débito constante sendo necessário um prévio estabelecimento da conexão.

O modo pacote é aplicado a apenas comunicações digitais. O canal de comunicação assenta num fluxo de pacotes, suportando serviços de débito variável. Cada pacote é identificado por um cabeçalho. O cumprimento dos pacotes e a sua frequência pode variar. Caso não exista nada para transmitir o canal não é utilizado.

A grande diferença destes modos é que enquanto no modo circuito o débito do canal é o débito máximo requerido pela fonte para não haver perda de informação, grande parte do tempo o canal está sub-utilizado. No modo pacote é apenas utilizado em cada momento o débito requerido pela fonte, deixando o excedente disponível para outros canais.

2.5.1. Circuitos Dedicados

A rede pública oferece serviços de voz com custos muito elevados. Para evitar esses custos, as organizações recorrem a redes de dados para transmissão de voz entre as suas localizações. Normalmente, são usadas as redes privadas para efectuar chamadas, estas

redes tem um circuito adicional dedicado para comunicações de voz, existindo em cada ponto um *gateway* que faz a interligação com as centrais telefónicas convencionais. Evitando desta forma os elevados custo da rede pública de comunicações.
Os pacotes de voz VoIP podem ser transmitidos sobre vários *links*, usando vários tipos de tecnologias como por exemplo: *Frame Relay*, ATM, circuitos ponto a ponto ou mesmo mais recentemente IP MPLS. Em Portugal é frequente as empresas contratarem níveis de serviço, largura de banda para interligarem as suas diferentes localizações.

2.5.2. VoFR

Voice over Frame Relay (VoFR) é a utilização da rede *Frame Relay* (o nome poderia ser traduzido para comutação de tramas) para transportar pacotes IP, que contêm pacotes de voz digitalizada. Equipamentos com funcionalidades para processamento de voz, telefones IP, *switches* ou *routers*, digitalizam a voz transformando-a em pacotes IP. Os pacotes IP são transmitidos ao seu destino pela rede *Frame Relay*.
O VoFR permite a compressão e transmissão de Voz através de circuitos virtuais permanentes (*PVC – Permanent Virtual Circuit*).

Se analisarmos o seguinte cenário, uma ligação entre Lisboa e Porto num circuito com um CIR (*Committed Information Rate*) de 768Kbps.
Em cada localização, temos uma rede de dados e uma central telefónica PPCA com um interface digital que liga a uma linha E1. Neste exemplo, podemos utilizar os *gateways* da Cisco da serie 2600 ou 3600 para interligar as duas localizações. Estes equipamentos suportam VoFR podendo interoperar entre si. Esta série de equipamentos está equipada com interfaces que ligam directamente à interface digital E1 das centrais PPCA. Estes *gateways* podem ligar-se directamente ao circuito *Frame relay*, através de unidade de serviço digital (*DSU – Digital Service Unit*) ligada à interface série. Com este exemplo de rede, podemos efectuar chamadas de um local para outro. Temos as centrais telefónicas a processar o encaminhamento de chamadas, em quanto os *routers* comprimem e transferem as chamadas. Com o algoritmo de G.729a, podemos reduzir as chamadas de vos até ao 8kbps. Com os cabeçalhos podem chegar ao 10.8Kbps. Apesar do tamanho não ocupar muita largura de banda, pode aumentar à medida que o número de chamadas activas aumenta. Com um circuito de 768Kbps e com codificação G.729a (o algoritmo G.729a comprime a voz até aos 8Kbps e com a sobrecarga do cabeçalho (*overhead*), conseguimos 10.8Kbps), podemos teoricamente ter 70 chamadas concorrentes. Nestes equipamentos temos um problema, apenas conseguem descodificar 24 chamadas de cada vez. Isto porque, cada chamada comprimida ocupa metade do DSP (processador de sinal digital). O que significa, que ao interligar o *routers* com uma central telefónica PPCA ficamos limitados a 24 canais. O número realista de chamadas suportado será 24.
Na maioria destas instalações os dados circulam no mesmo circuito que a voz. Se o número máximo de chamadas é atingido, são utilizados 24 vezes 10.8, aproximadamente 260Kbps. No exemplo de rede apresentado, temos um CIR (*Committed Information Rate*, especifica a quantidade de informação, por unidade de tempo, que pode circular numa interface) de 768Kbps.
No *Frame Relay*, quando é ultrapassado o CIR, a voz e dados podem misturar-se e alguns pacotes podem ser descartados. Imagine o que acontece quando no meio de uma conversação alguns pacotes são descartados. Provavelmente, na perceberá a conversa. A implementação de qualidade de serviço é fundamental para a implementação de voz sobre *Frame Relay*.

2.5.3. VoATM

A Tecnologia ATM (do inglês, *Asynchronous Transfer Mode*) é usada para transportar pacotes de voz digitalizada. Em vez de transportar segmentos de tamanho variável, uma rede ATM transporta pequenos segmentos de tamanho fixo chamadas células. Cada célula tem 53 bytes de comprimento, sendo 5 bytes para o cabeçalho e 48 para a informação. Na rede ATM, os pacotes VoIP são segmentados e colocados dentro destas células. O tamanho fixo destas células ATM oferece inúmeras vantagens. O seu pequeno tamanho significa que a latência e o atraso de cada vez que a célula passa pelo ATM é muito pequeno. Em contraste, o atraso do guardar e enviar (*store-and-forward*) dos pacotes IP através dos *routers* é mais longo, porque o ultimo *bit* do pacote tem que ser recebido antes de ser transmitido. Os comutadores ATM são

extremamente rápidos, a qualidade de serviço oferecido pode ser muito alta. A rede ATM oferece várias classes de serviços (CoS), opções sobre taxa de transferência constante (CBR - *Constante Bit Rate*), especialmente desenvolvida para o transporte de voz e outros protocolos de tempo real. A CBR fornece boa qualidade de serviço minimizando as variações de tempo nas transmissões de células de voz, fenómeno conhecido como *jitter*.

O ATM tem como principal potencialidade o suporte de múltiplos níveis de QoS. Enquanto no IP, é necessário um trabalho mais complexo para implementar o mesmo nível de QoS. O ATM tem esta funcionalidade desde início. Um dos problemas do ATM é não se encontrar disponíveis em todos os locais.

Embora o ATM tivesse tido grande sucesso de mercado em *backbones* WAN, continua com grande dificuldade em se mover para além desse espaço. Com o aumento da popularidade do *gigabit-ethernet*, o ATM terá uma maior dificuldade em se manter nas redes WAN empresariais. As capacidades inerentes de QoS permitem ao ATM um alto desempenho em soluções de grande intensidade de tráfego e aplicações sensíveis ao tempo, como voz e o vídeo. O ATM terá sempre vantagem sobre a *Ethernet* e o *Fast Ethernet* no que se refere à velocidade.
O lugar óbvio para usar VoATM é onde já existam redes ATM instaladas. Se tiver sorte suficiente para ter o ATM no seu bastidor (Armário Técnico), a VoATM torna-se um meio excelente para transmissão de voz. Este meio de comunicação pode ser estendido a sítios remotos. Só assim garantimos que a VoATM chega a todos os locais na rede, caso contrário poderá não ser possível a transmissão da voz a todos os sítios remotos.
As ligações na rede ATM são extremo-a-extermo, as chamadas podem ter origem no Porto, passar por Coimbra e terminar em Lisboa sem ter que codificar e descodificar a chamada múltiplas vezes. Devido à capacidade do ATM em implementar QoS, as chamadas de voz são colocadas nas suas próprias filas de QoS. Isto significa que as chamadas podem ser enviadas para o seu destino sem qualquer degradação na qualidade de serviço, sendo assegurado o seu tempo de chegada.
As várias classes de serviço são abordadas detalhadamente nos capítulos seguintes. De uma forma simplista, os dados e a voz são colocados em filas que são tratadas de forma diferente ao longo da rede ATM.

A figura 2.2 ilustra como pode ser dada prioridade ao tráfego de voz em detrimento dos dados. Neste exemplo, o CBR especifica o tráfego de voz. É assegurada a taxa de transferência ao tráfego de voz, de forma a minimizar a variação do atraso. Ao tráfego de dados é assegurado a fila com taxa de transferência disponível (*available bit rate* ABR). Os dados na fila ABR não têm qualquer garantia de largura de banda. Este tipo de esquema pode satisfazer ambos, voz e dados dentro da mesma rede.

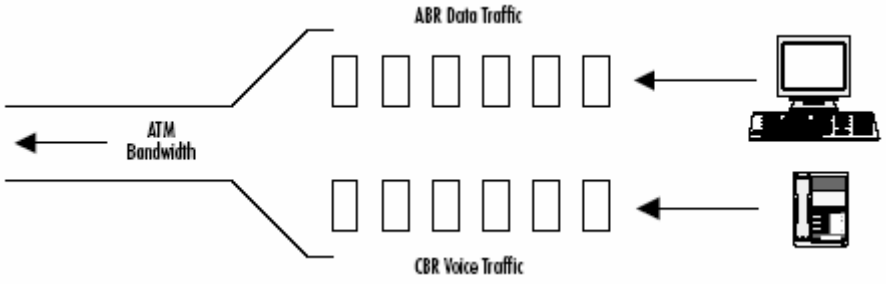

Figura 2.2 – Fila QoS com Tráfego de Voz e Dados

Quando as medidas de QoS do ATM são usadas, a informação é classificada e transportada pelas células. Uma célula no ATM é o equivalente a um datagrama. Sempre que uma chamada de voz é transportada pela rede ATM, é classificada como prioritária. Mais a frente veremos como esta classificação é efectuada. Isto também se verifica para transmissões de vídeo, em que as necessidades são idênticas ás da voz. A única diferença é que as aplicações de vídeo são muito mais exigentes no que respeita a largura de banda.

O ATM é um método completamente diferente na forma como controla o fluxo de dados. Uma das diferenças principais entre o ATM e as redes baseadas em datagramas é que o ATM parte os dados em células.

Numa rede como a *ethernet* o tamanho do datagrama pode variar. Esta variação "obriga" os comutadores a aguardar pela totalidade da *frame* (efeito conhecido como *Store and forward*), sendo transmitida para o endereço destino assim que recebida. Devido ao tamanho fixo das células ATM, este problema não se coloca. Não é necessário nenhum identificador para delimitar a *frame*, permitindo aos comutadores transmitir as células pela rede muito mais rapidamente. O tamanho fixo levanta-nos um problema, é que existe um grande desperdício de espaço nas células sempre que os dados não preencham a sua totalidade. Usando o norma G.729 a voz é segmentada em *frames* de 30 bytes, resultando em 23 *bytes* de *overhead,* figura 2.3.

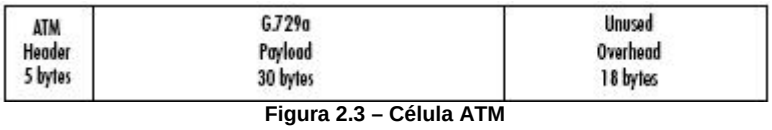

Figura 2.3 – Célula ATM

O ATM suporta o serviço CBR para beneficiar as aplicações de tempo real, com por exemplo a voz.
O serviço CBR implementa uma taxa de transferência específica para a transmissão de pacotes de voz. Esta especificidade minimiza as variações temporais na transmissão dos pacotes de voz, melhorando desta forma a qualidade do serviço para o utilizador final.

Como já referi, a principal vantagem da utilização do ATM está nas políticas de QoS que este tipo de serviços disponibiliza. A capacidade de classificar uma chamada de *voz* extremo-a-extremo é também uma vantagem.
Dependo do orçamento disponível, este tipo de solução é ideal para a implementação em redes de faculdades, hospitais, *campus*, figura 2.4. Este cenário permite-nos grandes larguras de banda e tem a capacidade de oferecer um bom nível de qualidade de serviço para tráfego de dados e voz.

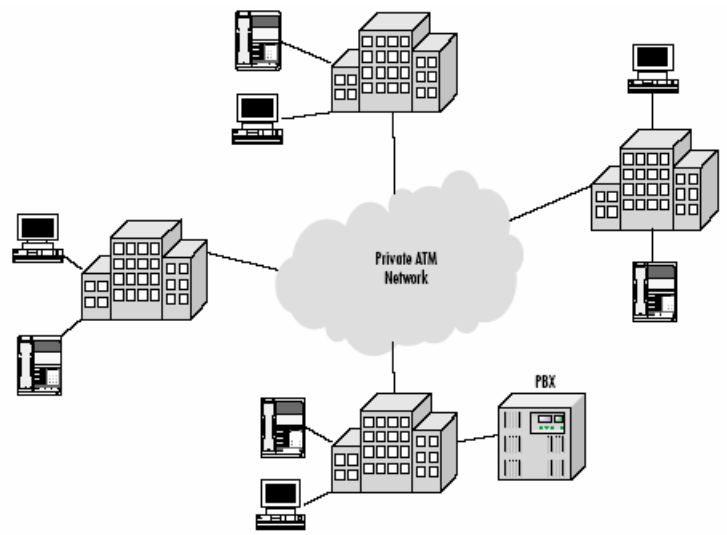

Figura 2.4 – Rede ATM Utilizando Voz e Dados

Um dos problemas que se põe é que nem todas as localidades tem acesso ao ATM. A maioria das vezes, não é possível interligar todas as localizações de uma empresa por circuito ATM. Por isso, o *Frame-Relay* é também uma opção. Podemos ter uma algumas localizações ligadas em circuito ATM e outras em circuito *Frame-Relay*, figura 2.5. Existe alguma similaridade entre estas redes. Provavelmente, no futuro todas as localizações terão acesso a circuitos ATM.

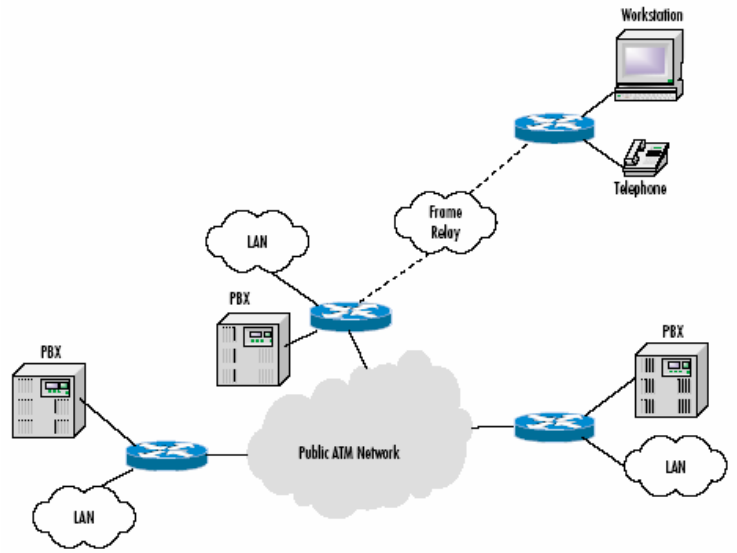

Figura 2.5 – Adicionar um Sitio Remoto pode ser um Problema com o ATM

2.5.4. Ligações Ponto-a-Ponto

São usadas ligações ponto a ponto para interligar as diferentes localizações de uma organização. A organização tem a capacidade de implementar e administrar a sua rede privada. Os protocolos mais comuns ao nível da camada de ligação são *High-Level Data Link Control* (HDLC) e *Point-to-Point Protocol* (PPP).
Nas implementações em que necessitamos de usar ligações ponto-a-ponto através de linhas dedicadas, temos duas alternativas:
A primeira opção é usar voz sobre o protocolo HDLC. O HDLC é um protocolo de nível dois, que usa tipicamente ligações ponto-a-ponto do tipo E1. O VoHDLC é similar ao VoFR. Usando compressão, permite-nos estabelecer múltiplas chamadas sobre um circuito E1. Este tipo de solução é pouco escalável ou seja, foi concebida apenas para ligar ponto-a-ponto os equipamentos da Cisco.
A segunda opção é usar VoIP, pois o uso da VoHDLC e VoFR obriga a codificar e descodificar uma chamada de voz múltiplas vezes. Como o protocolo IP podemos estabelecer uma chamada de voz para qualquer rede destino. Obviamente, neste caso, teremos que considerar a implementação de Qualidade de Serviço.

2.5.5. O MPLS Standard para a Implementação de VPN IP

Esta solução assenta na tecnologia IP, principalmente num conceito de VPN (*Virtual Private Network*) designado por MPLS (*Multi Protocol Label Switching*). Esta VPN é assegurada pelo recurso a tecnologias de *switching*, segurança e privacidade mais avançadas da actualidade.

Este serviço tem desempenho e performance, manifestando-se num serviço muito mais rápido – a informação é encaminhada directamente para o endereço de destino, sem ter de passar por outros sítios de trânsito (como acontece nas tecnologias orientadas à conexão).

A característica de "*Full Mesh*" inerente às VPN IP MPLS é especialmente importante para a voz e para todas as aplicações que venham a ser implementadas numa arquitectura distribuída.

Em termos topológicos a rede MPLS é mais optimizada do que uma rede de circuitos, por exemplo, a comunicação entre qualquer um dos locais é feita de forma directa sem necessidade de trânsito num outro ponto da rede o que introduzirá necessariamente um determinado nível de contenção e atraso.
Se esta simplificação é relevante a nível dos equipamentos, também o é no dimensionamento das larguras de banda pois deixam de se concentrar largura de bandas provenientes de outros locais e passam apenas a necessitar da largura de banda para si próprios.

Em termos de protecção, em caso de falha de qualquer circuito de uma das localizações, podem ser também utilizados "*backup*" nos circuitos de acesso dos locais remotos com base em acessos RDIS.

Na solução MPLS cada local vale por si, ver figura 2.6, à medida que vão sendo ligados os pontos, estes passam logo a poder comunicar entre si.

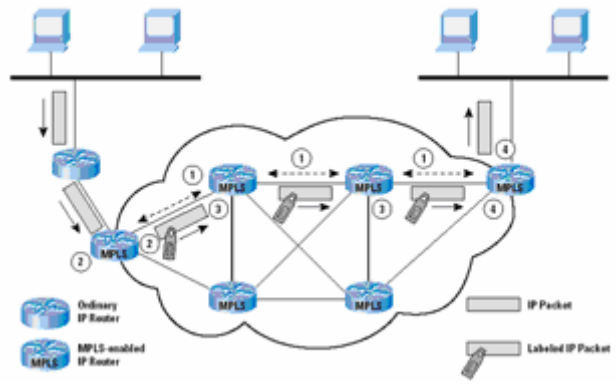

Figura 2.6 – Operação MPLS

Apesar de outras tecnologias já existirem há vários anos com provas demonstradas quanto ao isolamento de dados e fiabilidade, as VPNs MPLS como tecnologia recente, beneficiam das seguintes vantagens:

- disponibilização de um **isolamento de tráfego** semelhante ao obtido nas soluções baseadas no estabelecimento de circuitos lógicos ATM ou *Frame Relay*: o tráfego IP com determinado destino e associado a uma determinada VPN é identificado por etiquetas (*labels*) transportadas nas tramas de nível 2;
- Capacidade de **comutação mais rápida** nos nós de rede: a utilização de etiquetas anexadas ao cabeçalho dos pacotes IP permite que o tráfego IP seja encaminhado para o seu destino em cada nó de rede (*Router* ou Comutador MPLS) sem que seja necessário o processamento de informação de nível 3;
- redução do atraso de **transmissão *extremo-a-extremo***: a redução do tempo de processamento em cada nó permite que o atraso acumulado entre os pontos origem e destino seja fortemente diminuído. O número total de saltos (*hops*) é, eficazmente, reduzido ao mínimo;
- **facilidade de ligação e configuração**: cada *router* de Acesso é um possível ponto de entrada na VPN. A integração de um novo local ou a alteração das características de um já existente, apenas exige uma configuração local no POP (*Point of Presence*) onde é terminada a ligação de acesso e no novo local correspondente;
- **melhor utilização dos recursos de rede**: a ausência de ligações lógicas dedicadas, caso do *Frame Relay*, permite aumentar a taxa de utilização dos recursos por partilha com outros serviços;
- **independência do esquema de endereçamento** usado na rede de transporte: as gamas de endereços usadas nas redes de um cliente poderão ser definidas ao seu critério, não havendo perigo de colisão de endereçamento entre a VPN MPLS e o resto da rede IP;
- em termos topológicos a rede MPLS é **mais optimizada** que qualquer outra tecnologia, por exemplo, a comunicação entre dois locais remotos é feita de forma directa sem necessidade de trânsitos que introduzirão necessariamente um determinado nível de contenção e atraso.

Assim sendo, os serviços a implementar na VPN MPLS poderão beneficiar destas vantagens, nomeadamente no que respeita a:

- **redução do atraso** de comutação e de transmissão, bastante importante na qualidade de serviço do transporte de voz sobre IP (VoIP).

- **aumento da fiabilidade** da solução global, mantendo a conectividade entre os vários locais no caso de falha do ponto central.
- **melhoria de performance** de serviços que necessitem de conectividade directa entre qualquer um dos locais, tais como *intranet*, *e-mail*, Internet, aplicações internas, entre outros.
- possibilidade de **detecção automática de quebra** de comunicações e activação imediata do backup RDIS. Esta activação é feita com base na falta de conectividade entre o *router* dos locais remotos e o ponto central da rede, e não exclusivamente na falha do circuito físico de acesso. Este processo é realizado de uma forma completamente transparente do ponto de vista do utilizador.

2.6. Diferença Topológicas das Redes Tradicionais das Redes "IP *switched*"

A diferenciação e qualidade de serviço são uma realidade na tecnologia IP, como suporte a aplicações de voz, dados ou Internet.

A tecnologia MPLS (*Multi-Protocol Label Switching*) foi desenvolvida de forma a implementar a associação da privacidade e QoS (*Quality of Service*) com a flexibilidade e escalabilidade do IP.
Ao contrário dos protocolos ATM e FR (protocolos orientados à conexão ou ligações ponto-a-ponto) este protocolo caracteriza-se por ser um protocolo não orientado à conexão – permite conectividade de todos os sítios.
Muitas das políticas de QoS implementadas nas redes IP são específicas a cada *router*. Esta é uma das principais barreiras referente á tecnologia IP. Os pacotes IP, actualmente não incluem informação detalhada sobre QoS no respeita aos *bits* de precedência IP. Estamos assistir alguns progressos no respeita as essa etiqueta de QoS, mas ainda existem bastante problemas principalmente em rede congestionadas.

2.7. Telefonia IP

A telefonia IP constitui uma parte da arquitectura de voz e vídeo e integração com dados (AVVID) da Cisco. A telefonia IP, conjunto de soluções complementares que visa, essencialmente, a substituição da centrais telefonias tradicionais (PPCA).

2.7.1. Clientes da Telefonia IP

Telefone com capacidade para digitalizar sinais de voz são conhecidos como clientes de telefonia IP ou simplesmente telefones IP. Estes equipamentos estão equipados com processadores de sinais digitais (DSP's) para realizar essa função. A Cisco oferece uma grande variedade clientes de telefonia IP. Os telefones mais comuns são, os 7910, 7960 e 7940 para além das muitas funcionalidades, incluem um pequeno visor de cristais líquidos (LCD, *Liquid Crystal Display*), botões de controlo, funções de múltipla linha. Existem também telefones de conferência os 7935. Com estes equipamentos, equipados com um comutador *ethernet* de 2 portas, tem-se a possibilidade de ligar um PC directamente ao telefone, sendo necessário apenas um ponto de rede na secretária e no *switch*. A Figura 2.7 mostra alguns modelos.

Figura 2.7 – Clientes de Telefonia IP

2.7.2. Telefones por Software (IP *Softphones*)

O IP *softphone* da Cisco é um telefone virtual que corre em ambiente Windows. No fundo, os computadores pessoais contem um software que permite operar como cliente de telefonia IP. Os PC's contêm colunas e microfones que funcionam similarmente aos telefones IP. O software digitaliza os sinais de voz e envia-os através da rede IP. O telefone por software proporciona um bom ambiente para o desenvolvimento de aplicações TAPI (*Telephony Application Programming Interface*). Exemplo na figura 2.8 de um telefone por software.

Figura 2.8 – IP Softphone

2.7.3. Cisco Call Manager

O Cisco *Call Manager* (CCM) é o software responsável pelo controlo e sinalização de chamadas entre um telefone IP e os restantes componentes de voz numa rede. Este software encontra-se normalmente num servidor e desempenha as mesmas funções que as tradicionais centrais telefónicas PPCA.

As funções básicas do CCM são:

- registar os dispositivos clientes telefones IP;
- processamento de chamadas;
- administração de planos de marcação;
- gestão de recursos.

Nos locais remotos, onde não exista central telefónica pode ser usado um software específico embebido no sistema operativo do router de acesso denominado *Call Manager Express*.
O Cisco *Call Manager Express*, software mais limitado que o CCM, permite que um *router* de acesso Cisco disponibilize processamento de chamadas para telefones IP ligados localmente. Todos os ficheiros e configurações necessárias para os telefones IP estão armazenados internamente no router, dispensando a utilização de servidores ou bases de dados externas para o efeito. O Cisco *Call Manager Express* é tipicamente adequado para soluções com menos de 100 utilizadores, sendo o número de utilizadores suportados dependente do modelo do *router* de acesso utilizado.

2.7.4. Gateways e GateKeepers

O *gateway* é o equipamento responsável pela interoperabilidade da telefonia IP e a rede pública de voz (PSTN). O *gateway* executa a conversão em tempo real da voz digital para voz analogia e vice-versa. Quando a rede VoIP está com problemas (*link* em baixo, congestionada), oferece mecanismos de redundância, encaminhando as chamadas pela rede pública.
O *Gatekeeper* é considerado o "cérebro" da rede, regula os dispositivos que podem iniciar ou receber chamadas.

2.7.5. Comutadores *Ethernet*

OS comutadores *ethernet* (*switches*) da Cisco fornecem um alto desempenho para os telefones IP. Os *switches* têm muitas vantagens relativamente aos *hubs*. Os *switches* permitem velocidades de transmissão muito elevadas, (*Fast Ethernet*). A transmissão de um telefone IP não é propagada para outros telefones IP no mesmo *switch*. Esta funcionalidade elimina as colisões de datagramas entre telefones IP. Existem alguns modelos, que auto alimenta os telefones (funcionalidade de *In-Line Power*), fornecendo corrente eléctrica aos telefones através da rede *ethernet*, eliminando a necessidade de utilização de fontes de alimentação separadas.

2.8. Multimédia Empresarial

Nos dias de hoje, as empresas exigem aplicações multimédia para a distribuição de mensagens de fax e videoconferência directamente para a área de trabalho de cada utilizador. O Fax e o vídeo são exemplos destas aplicações.

2.8.1. Fax

O envio e recepção de faxes, pode beneficiar da utilização de voz em pacotes IP, por exemplo, integração com correio electrónico. O sistema unificado de mensagens da Cisco (*Cisco Unity*) pode encaminhar as mensagens vindas de um fax para qualquer caixa de correio, possibilitando o transporte do fax para qualquer sítio, em ficheiros com formato TIFF (*Tagged Image File Format*). Com este tipo de tecnologia, não é necessário a existência de um equipamento de Fax. Os faxes em papel, normalmente, degradam-se com o número de envios. O fax em correio electrónico pode ser enviado as vezes pretendidas sem perda de qualidade. Uma outra facilidade da utilização deste sistema é, a partir do instante em que esta mensagem fica em *e-mail*, pode ser distribuída por um servidor SMTP (*Simple Mail Transfer Protocol*). O processo de envio também é possível, ou seja, podem enviar uma mensagem por correio com um ficheiro do tipo TIFF anexado e este ser enviado para um equipamento de fax remoto pela rede pública.

2.8.2. Vídeo

Aplicações de videoconferência permitem aos utilizadores comunicarem em grupos através da Internet ou intranet. Tanto a Cisco como a Microsoft oferecem soluções de vídeo empresariais.
O Microsoft *NetMeeting*, é uma das aplicações mais utilizadas para videoconferência. Incluiu áudio, vídeo, transferência de ficheiros, chat e funções de colaboração. O software *NetMeeting* corre em ambientes Windows. As transmissões são baseadas no protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*) que a torna compatível com a infra-estrutura de rede VoIP, porque utilizam os mesmos protocolos de mais baixo nível.

2.9. Substituição das Linhas Dedicadas de Voz

Muitos operadores de telecomunicações já têm no seu leque de produtos, uma grande variedade de interfaces para interligação das redes VoIP, redes transportando pacotes de voz IP, com as localizações com centrais telefónicas PPCA. Estas interfaces possibilitam às organizações manter as suas infra-estruturas de comunicações, ou pelo menos parte delas.
A substituição/renovação da infra-estrutura de comunicações, por parte dos operadores de telecomunicações em Portugal. A substituição dos seus sistemas tradicionais de comunicações, por equipamentos que permitam a digitalização de voz em pacotes IP. A implementação de Infra-estruturas de transporte em fibra óptica, e o aparecimento de tecnologias como IP MPLS (*Multi Protocol Label Switching*), permite a oferta de novas soluções e serviços a custos muito reduzidos.

Até agora a empresas tinham duas opções para estabelecer chamadas de longa distância entre as suas localizações.
A primeira opção é simplesmente estabelecer chamadas de longa distância normais, utilizado a rede pública de comunicações. Se as chamas não forem muitas, os custos podem se baixos comparativamente o valor das linhas dedicadas.
A outra opção é instalar uma linha dedicada entre as centrais telefónicas PPCA das diferentes localizações. Estas ligações são normalmente efectuadas com recurso a linhas dedicadas do tipo E1. A linha E1 é responsável pela transmissão de sinais digitais entre os PPCA. Este tipo de ligação evita que se use a rede pública de comunicações para estabelecimento de chamadas telefónicas. Permite-nos efectuar o número de chamadas que quisermos a um custo fixo ou seja, ao preço do valor do aluguer da linha do tipo E1. Em contra partida, obriga-nos a ter uma linha dedicada para dados é uma linha para voz, aumentado substancialmente os custos.

2.10. Convergência

Uma empresa com várias delegações, tem frequentemente em cada localização uma central telefónica, para que os funcionários possam comunicar entre eles. Em cada localização existe uma linha de comunicação dedicada, mesmo sem qualquer conversação esta linha não pode ser utilizada para outro fim. Com a tecnologia VoIP esta situação não acontece, existe apenas uma linha dedicada que é partilhada com comunicações voz e dados. Caso não exista chamada de voz, a totalidade da linha fica disponível para dados. Desta forma, podemos rentabilizar os recursos disponíveis. Imagine o que pode poupar ao retirar as linhas dedicadas de comunicações de voz. Mesmo que a largura de banda nos circuitos de dados necessitem de ser aumentados, os custos de incremento da linha serão menores do que a instalação e manutenção de um segundo circuito.

2.11. A Rede Pública Comunicações (PSTN) como *Backup*

As organizações utilizam normalmente a rede telefónica pública PSTN para fornecer redundância nas redes VoIP. Os *gateways* de voz permitem esta redundância. Quando a rede VoIP verifica que a rede WAN está em baixo, o *gateway* converte os pacotes de voz digital em voz analógica encaminhando-os pela rede pública.

2.12. Retorno de Investimento

Nem sempre é fácil calcular o retorno do investimento em tecnologias de informação, o que dificulta a adesão de algumas empresas a determinadas soluções.
Nada melhor para ajudar a vender uma solução que um bom plano de amortização e retorno de investimento (do inglês ROI *Return Of Investment*).
Os aspectos a ter em contra para construir uma um plano de investimento são:

- analisar os custos com a telefonia actual;
- detalhar os custos da nova solução, incluindo custos com novos circuitos;
- plano de amortização do investimento comparando os valores anteriores.

Este plano de amortização e/ou retorno de investimento deve estar muito bem documentado, deve-se fazer uso de números, gráficos que mostram como uma solução VoIP pode trazer grandes benefícios financeiros para as organizações.

2.12.1. Analisar os Custos com a Telefonia Actual

Construir um plano para retorno de investimento é o melhor começo quando se pretende decidir se a telefonia IP, pode ou não, fazer algum sentido para o futuro de uma organização.
Ao tentar implementar uma solução de telefonia IP, substituindo a solução baseada em PPCA, o gestor vai questionar como é que esta alteração de comunicações vai ajudar a empresa a poupar dinheiro.
Normalmente, este tipo de alteração envolve centros de atendimento (*Call Centers*), a telefonia IP pode oferecer diferentes e eficientes meios para desenvolver o seu negócio. O primeiro passo é tentar mostrar como é que a solução se paga a si própria. Aos gestores, principalmente os financeiros, não interessa tanto as funcionalidades, interessa sim, como podem reduzir os custos com as comunicações. Provavelmente, umas das grandes despesas que as empresas se deparam no dia a dia.
É importante analisar os custos e a duração das chamadas locais, regionais, nacionais e internacionais e construir uma tabela com esses valores. Depois, verificar os custos com a substituição de linhas dedicadas que interligam as diferentes localizações da empresa.

2.12.2. Desenhar a Nova Solução

Tentar perceber os planos de marcação e os preços, ajuda-nos a construir uma solução realista. Até agora, vimos a substituição das linhas dedicadas como principal vantagem para a mudança de infra-estrutura de comunicações. Esta substituição é relativamente simples. Muitas vezes, podemos utilizar o equipamento existente, alterando apenas a interface de ligação ou

então, adquirir novos equipamentos por exemplo o *router* da Cisco da série 2600 seria uma opção. Esta aquisição depende muito do tipo de utilização que a empresa tem em cada sítio. O que de uma forma directa poderá influenciar nos preços da aquisição de equipamentos.
Outro ponto importante, é determinar a largura de banda necessária para suportar o volume de chamadas. Outro ponto-chave é determinar qual o tipo de circuito a adoptar. Por exemplo, quando efectua chamadas por um circuito *Frame-Relay*, tem disponível uma série funcionalidades que lhe permitem analisar a velocidade e a utilização do circuito. Para conseguir construir uma bom plano de investimento, deverá ter em conta os preços praticados no mercado. Actualmente existe bastante concorrência entre os operadores portugueses, este factor pode ser determinante na escolha do operador, ou mesmo da própria solução.

2.12.3. Manutenção e Suporte

Uma vez que a telefonia IP usa a mesma infra-estrutura dos dados, são usados os mesmos mecanismos para suporte técnico. As equipas técnicas e as ferramentas de gestão são as mesmas, reduzindo significativamente os custos de manutenção e suporte.
A adição, alteração e remoção de telefones IP são muito simples. Sistemas como DHCP (*Dynamic Host Configuration Protocol*), registo automático e interfaces baseados em aplicações *web*, podem facilitar qualquer tipo de alteração.

2.13. Integração e Aplicações Complementares

A substituição das linhas dedicadas de voz pela tecnologia VoIP, assim como, a substituição de centrais telefonias convencionais pela telefonia IP, fica um pouco aquém das potencialidades desta tecnologia. Uma das grandes vantagens desta tecnologia é a possibilidade de integração na rede de soluções complementares de valor acrescentado para o utilizador final e para as organizações.

2.13.1. Sistema Unificado de Mensagens (*Unified Messaging)*

O *Unified Messaging* é um excelente exemplo de como duas redes distintas, rede telefónica e rede de dados, se podem juntar oferecendo melhores serviços. O *voicemail* e o *e-mail* foram sempre entidades separadas. Com o *Unified Messaging*, ambos os sistemas ligam na mesma interface.
A Cisco comprou uma empresa chamada Amteva, que produzia a Amteva *Unified Messaging Systems* (UMS). Agora conhecido como Cisco *Unity*, o UMS corre em plataforma Windows e Solaris. As funcionalidades são:

- parâmetros de configuração baseados em *Lightweight Directory Access Protocol* (LDAP), um *standard* de organização baseado em estrutura de directórios;
- *voicemail* e faxes podem ser acedidos através do protocolo *Internet Message Access Protocol* (IMAP) com um cliente de e-mail. IMAP é um standard comum para o e-mail;
- o e-mail pode ser recebido e enviado pelo telemóvel;
- suporta vários tipos de notificações para a chegada de e-mail, *voicemail* e faxes:
- único número de contacto
- interface de gestão por *web browser*

Os faxes podem ser directamente entregues na caixa de correio do utilizador final, pode ser visualizada a partir de um cliente de e-mail e transferido como uma mensagem através do cliente de *e-mail*. É uma solução escalável que pode gerida via *web browser*.
Os parâmetros de configuração são gravados via arquitectura LDAP. A popularidade do LDAP está a crescer muito rapidamente, sendo um standard aberto, permite a interligação com outras aplicações, fazendo com que o utilizador personalize as suas aplicações.
O *voicemail* e os faxes podem ser acedidos por qualquer sistema que suporte IMAP. O *Unity* usa os *standards* para converter o *voicemail* e os faxes num formato IMAP.
As mensagens de voz (*Voicemail*) são gravadas em ficheiros com formato WAV. OS faxes são guardados em formato TIFF.
Ligado à Internet permite ao utilizador aceder ao seu *voicemail* e faxes sem ter que efectuar uma chamada de longa distância.

O *Unity* pode ser configurado para enviar um SMS (*Short Message Service*) ao utilizador, quando uma nova mensagem de e-mail ou fax é recebida.
Tratando se um sistema baseado na tecnologia IP, a interface baseada em aplicações *Web* foi desenvolvida para permitir o acesso às aplicações, assim como, a possibilidade de aceder e alterar parâmetros de configuração remotamente.

Talvez uma das características mais interessantes desta solução é um único número de contacto, o serviço "*Find-me, follow-me*". A maioria das pessoas tem um número telemóvel ou mais, o número de telefone da empresa e até número de telefone de casa. Pode ser discutível que estar sempre contactável nem sempre é a melhor coisa, mas não existe dúvida que cada vez mais pessoas necessitam deste tipo de acesso. O problema é que teremos que dar os nossos números de contacto a toda gente, e eles tentarão contactá-lo por cada número. O *Unity* permite configurar uma lista de números possíveis de contacto e número de tentativas de ligação. Quando alguém tenta contactá-lo pelo o número do escritório, e não está lá. A pessoa que tenta a chamada recebe uma mensagem que não você não atende o telefone e tem a possibilidade de aguardar enquanto o sistema tenta localiza-lo pelos números alternativos, ou então deixar mensagem de voz. Se a pessoa decidir aguardar é feita a transferência para os números alternativos. Isto significa que pode apenas passar como contacto um único número. Podendo manter os outro números privados.

Este tipo de solução pode ter alguma influência no momento de mudar para a telefonia IP. Este tipo de solução é escalável, permitindo às empresas evoluir de uma forma rápida e a custos reduzidos.

2.13.2. Integração TAPI

Uma das chaves do sucesso da telefonia IP é o aparecimento de *standards* abertos como o TAPI. O TAPI (*Telephony Application Programming Interface*) é uma interface de programação para aplicações telefónicas. Permite aos programadores aceder a informação específica dos telefones recorrendo a aplicações TAPI embebidas nos sistemas.
Esta interface tem benefícios em postos clientes e servidores para diferentes tipos de aplicações.
No servidor, encontramos diversos tipos de serviços de valor acrescentado, permitindo que estes se interliguem uns com os outros. Aplicações como o *voicemail* e *Interactive Voice Reponse* (IVR), podem ser acedidas pelo TAPI. O TAPI facilita a implementação de novas aplicações que nem sequer foram sonhadas com as interfaces proprietárias dos PPCA. A medida que os *standards* evoluem as aplicações vão ficando muito mais robustas.

Por outro lado, o TAPI tem grande impacto nos postos clientes. Algumas aplicações TAPI são simplesmente telefones (*Softphones*). Outras vão um pouco mais longe, as mais avançadas conseguem enviar mensagem para o ecrã. Quando o software recebe uma chamada, regista o nome da pessoa que está ligar, o obvio que esta funcionalidade só acontece se tivermos a informação numa base de dados. Existe a possibilidade, mesmo antes do operador atender o telefone, a aplicação fornecer todo a informação da pessoa que está a ligar. Este tipo aplicação poderá ser implementada num centro de atendimento. Isto permite ao operador numa linha de atendimento (*helpdek*), saber todo o histórico de avarias e problemas que o utilizador já teve, pode tentar resolver o problema e caso não consiga encaminhar para uma segunda linha de atendimento, estes terão acesso a toda a informação evitando que o utilizador tenha que repetir todo novamente. Este tipo de solução melhora em muito a qualidade de serviço das empresas.

2.13.3. Capacidades de Transferência, Encaminhamento e Conferência.

Possibilidades de transferência, encaminhamento e conferência são todo funcionalidades típicas dos PPCAs.
Devido à natureza das chamadas IP, ligações directas ponto-a-ponto, existe a necessidade de implementação de funcionalidades por software.
Para implementar este três serviços na telefonia IP, existe a necessidade de implementação uma aplicação servidora. Este funcionará de ponte de conferência que em conjunto com o *call*

manager servirá este serviços. O primeiro objectivo para estabelecer uma conferência é enviar uma chamada para a ponte (*bridge*) a partir deste ponto é distribuído para os pontos finais.
A transferência e encaminhamento de chamadas são geridos pelo serviço *Communication Manager*.

2.13.4. Transferência de Chamadas

Os telefones IP da Cisco suportam transferência de chamadas. Sinalizando o *Communication Manager* que a chamada pode ser transferida para o destino.

2.13.5. Encaminhamento de Chamadas

A telefonia IP da Cisco Suporta três tipos de encaminhamento de chamadas:

- ***Call Forward All*** encaminha todas as chamadas
- ***Call Forward Busy*** encaminha as chamadas apenas quando a linha esta ocupada
- ***Call Forward No Answer*** encaminha as chamadas quando o telefone não atende ao fim de um número configurável de segundos

2.13.6. Captura de Chamadas e Chamada em Espera

O Serviço de chamada em espera permite manter uma chamada em espera enquanto utiliza o mesmo telefone para efectuar ou transferir outras chamadas.
A captura de chamada permite capturar uma chamada que está a tocar em outro telefone.

2.13.7. Música em Espera

Numa chamada em espera, pode ser colocada musica para entreter a pessoa. O formato pode ser WAV (*Waveform Áudio*), através de um dispositivo externo por exemplo, um leitor CD controlado pelo *Call Manager*

2.13.8. Conferência

Existem dois tipos de conferência:

- ***Ad Hoc* Conferencia –** Permite ao utilizadores ligar e adicionar novos participantes, bastando carregar na tecla de conferência para estabelecer a comunicação.
- ***Meet Me* Conferência –** Permite aos utilizadores estabelecer um número de conferência e divulgar aos participantes. Os participantes juntam-se a conferência marcando o número divulgado.

2.13.9. Web Attendant

O *Web Attendant* da Cisco é uma aplicação TAPI que corre em ambiente Windows e permite ao recepcionista controlar a chamadas recebidas como base numa interface aplicacional *web*.
Com a interface baseado em *web*, cada chamada no sistema é identificada com cores diferentes. As chamadas podem ser atendidas apenas com simples *click* do rato. Chamada em espera e transferência de chamadas podem ser manipulados por um simples arrastar largar.

2.13.10. Listagem e Registo de Chamadas

Mesmo com os reduzidos custos associados ao uso da telefonia IP. As organizações pretendem analisar detalhadamente as listagens das chamadas. Sem este tipo de analise, não é possíveis às empresas determinar onde é que os aumentos de largura de banda são necessárias, ou mesmo ver o número de chamadas perdidas, o que se traduz muitas vezes num mau serviço de atendimento.

Um das componentes da solução de voz da Cisco é a capacidade de capturar os registos de chamadas. O Software *Management Call Manager* (MCM) regista com grande detalhe as

chamadas efectuadas e envias os relatórios para um servidor *Radius* ou TACACS+. Esses relatórios incluem:

- número origem;
- número destino;
- inicio da chamada;
- fim da chamada;
- largura de banda utilizada;

Este software também permite ligações via ODBC (*Open Database Connectivity*) interligando com base dados Access ou SQL.
Este tipo de informação, pode ser compilado numa base dados para posterior análise. Podem ser realizados relatórios com gráficos, permitindo a análise dos números. Estes números podem ser analisados por mês, por ano ou mesmo por dia, dependendo do nível detalhe que se pretende. Por aqui, podemos ver que este tipo de ferramenta é bastante útil. Com esta ferramenta podemos chegar a conclusão que alguns circuitos necessitam de aumento de largura de banda, assim como, outros podem ser diminuídos, pois o seu volume de chamada não justifica a largura de banda disponível, podendo desta forma controlar eficientemente os recursos disponíveis.
Outra vantagem, destes relatórios é poder comparar as facturas dos operadores de comunicações com as nossas listagens de chamadas para controlo de custos.

2.13.11. Logs e Tracing

Existe uma grande variedade de *logs* e *tracing* disponíveis para funções de diagnóstico.

2.13.12. Transcoders

As conversões em tempo-real da voz digitalizada de um CODEC para outro são feitas pelo *Transcoders*.
Um CODEC é um esquema de codificação e descodificação para converter voz analógica para digital, e vice-versa. Uma vez que nem todos os CODEC*s* são compatíveis, os *Transcoders* são usados para traduzir o CODEC de uma zona para outra.
Os *Transcoders* são importantes em chamadas de conferência, quando os participantes não utilizam o mesmo CODEC.

3. Sinalização e Protocolos de Transporte VoIP

Nos últimos anos, assistimos a um enorme desenvolvimento tecnológico que contribuiu em larga escala para a realidade VOIP. Poderíamos citar inúmeras razões para justificar a rápida adopção desta tecnologia, mas a explicação é simples, a tecnologia melhorou consideravelmente. Chamadas que até a pouco tempo, eram praticamente imperceptíveis são agora claras e perceptíveis. A melhoria na qualidade da voz e o aparecimento de novas tecnologias contribuíram definitivamente apara o aparecimento do VoIP. Os protocolos de sinalização VoIP tiveram um papel vital no aumento de confiança desta tecnologia. Os protocolos de sinalização VoIP não só permitem o funcionamento da rede VoIP, como controlam todas as conexões na rede, criando um caminho fixo garantido sobre redes não orientadas à conexão.
Ao longo deste capítulo veremos os protocolos fundamentais para a implementação de uma solução VoIP. Serão abordados os conceitos gerais do TCP/IP, endereçamento IP e dos protocolos de sinalização H.323 e *Session Initiation Protocol* (SIP) e a sua importância na tecnologia VoIP.

3.1. Visão Geral Sobre Redes IP

As redes baseadas no *Internet Protocol* (IP), circulação de pacotes – também designados por datagrama de tamanho variável, são redes não são orientadas à conexão. Numa rede de serviços não orientado a conexão, a informação é transferida entre duas entidades sem que seja estabelecida uma ligação prévia. Os níveis da camada superior do modelo de referência OSI (*Open Systems Interconnection*) da ISO, podem ser orientados à conexão ou não

orientados à conexão. O IP é um protocolo de rede (nível 3 da camada OSI). Este protocolo contém informação de controlo permitindo aos datagramas serem encaminhados, de uma forma não ordenada, garantido o melhor esforço possível para os entregar no destino. Uma mensagem pode conter vários datagramas, estes são ordenados no destino. Tipicamente, o tráfego IP é transmitido sendo primeiro a chegar é primeiro a sair (FIFO, *Firt-In First-Out*). Os pacotes têm tamanho variável por natureza, permitindo a transferência de ficheiros maiores utilizar os pacotes maiores para uma melhor eficiência da rede.

O modelo de referência OSI (*Open Systems Interconnection*), ver figura 3.1, resulta de um projecto conduzido pela Organização Internacional de Normalização (*International Organization for Standardization*, ISO) durante os anos 70 e 80.
O objectivo inicial do projecto era desenvolver um enquadramento que permitisse a elaboração de normas para a interligação de sistemas abertos. Várias razões levaram a que este objectivo não fosse alcançado, na sua generalidade.
Apesar do aparente insucesso da iniciativa da ISO em termos de desenvolvimento de uma arquitectura para interligação de sistemas abertos, desse esforço resultou, um modelo bastante rico em conceitos importantes em termos de comunicação entre sistemas, aplicáveis aos sistemas de comunicação existente hoje em dia.
O desenvolvimento de sistemas abertos permite que uma diversidade de aplicações utilizem uma grande variedades de equipamentos, ou seja, deixam de depender de um único fabricante, podendo escolher equipamentos como base em funcionalidades e capacidades. Os sistemas abertos, se forem levados aos extremos, têm algumas desvantagens, o nível de complexidade pode aumentar significativamente.
O modelo de referência OSI agrupa as funcionalidades de comunicação em sete camadas, de acordo com critério de afinidade, abrangendo aspectos que vão desde o equipamento de interface com meios físicos, até aos protocolos de aplicação.

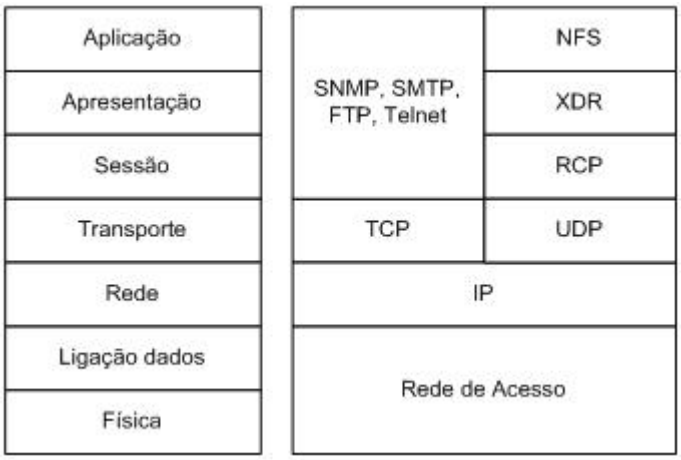

Figura 3.1 – Modelo de Referência OSI

As redes Internet são "*best-effort*", significa que os nós na rede fazem o melhor esforço possível para enviar os pacotes ao seu destino, não garante a transferência fiável da informação.
O protocolo IP não executa qualquer função de recuperação de erros estas recuperações ficam a cargo dos níveis de camada superiores (transporte ou aplicação), o que faz com que as funções desta camada sejam bastante leves, exigindo poucos recursos por partes dos encaminhadores (*routers*) da rede. Esta abordagem tem, no entanto, implicações em termos de qualidade de serviço oferecida pela Internet, levantando alguns problemas quando se pretende usar esta rede para o suporte de aplicações que exigem uma qualidade de serviço fixa.
A Figura 3.2 representa um pacote IP, sendo visíveis os seus diversos campos. Os pacotes contêm toda a informação necessária para que um encaminhador (*router*) os processe, independentemente os pacotes processados anteriormente.

Figura 3.2 – Formato de um Pacote IP

3.2. Protocolos de Transporte

Os pacotes tem origem e destino em sistemas terminais, que albergam as aplicações, e são comutados e encaminhados através da rede pelos *routers*. Quando um *router* recebe um pacote, determina qual o sistema ao qual este deve ser enviado, que será o *host* destino se este se encontrar na mesma rede que o *router* ou será outro *router* no caminho para o *host* destino. O encaminhamento processa-se, assim, salto a salto, com base nas tabelas de encaminhamento armazenadas nos *routers*. A figura 3.3 ilustra o encaminhamento de pacotes de *host* A para um *host* B.

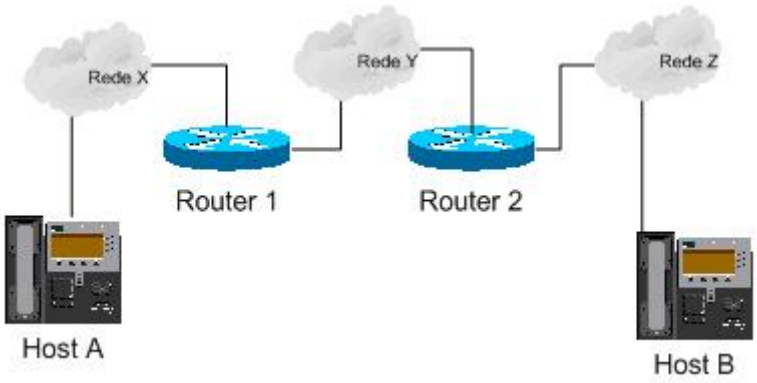

Figura 3.3 – Exemplo de Encaminhamento entre dois *Hosts*

O nível de transporte é um nível de comunicação extremo-a-extremo, sendo os protocolos TCP (*Transmission Control Protocol*), UDP *(User Datagram Protocol*) e RTP (*Real Time Transporte Protocol*) os seus protocolos mais importantes.

3.2.1. TCP

O TCP é um protocolo orientado à conexão, é responsável pela a divisão de uma mensagem em pacotes IP e de os ordenar de forma a construir a mensagem no endereço destino. O TCP é considerado um serviço de transporte seguro. O TCP é um protocolo de nível 4 da camada OSI, que estabelece uma ligação virtual segura. Uma ligação virtual é uma simples associação entre dois processos a correr em duas máquinas. O TCP não é processado ao nível dos *routers* ou *switches*, mas sim ao nível dos terminais. O TCP proporciona à aplicação um circuito virtual e controlo de fluxo, e adapta-se a possíveis congestionamentos na rede. A figura 3.4 ilustra a o formato dos segmentos TCP.
O TCP é responsável por fornecer uma transmissão de dados segura sobre uma rede disponibilizando os seguintes serviços:

- transmissão de segmentos dados;
- multiplexagem (os níveis superiores poder estabelecer comunicações simultaneamente sobre uma única conexão;
- controlo de fluxo eficiente;
- segurança;
- operações *Full duplex*.

A transmissão de dados, entrega os dados com um fluxo fixo contínuo de *bytes*. Cada *byte* é identificado com um número de sequência para que a aplicação não tenha que segmentar os dados em blocos antes de enviar ao TCP. Quando o TCP recebe os bytes, agrupa-os em segmentos de dados e envia para a camada seguinte, sendo o IP responsável pela entrega. Cada pacote tem uma confirmação de envio que indica ao receptor qual o número do próximo pacote a ser enviado. O TCP tem a capacidade de retransmitir os pacotes perdidos.

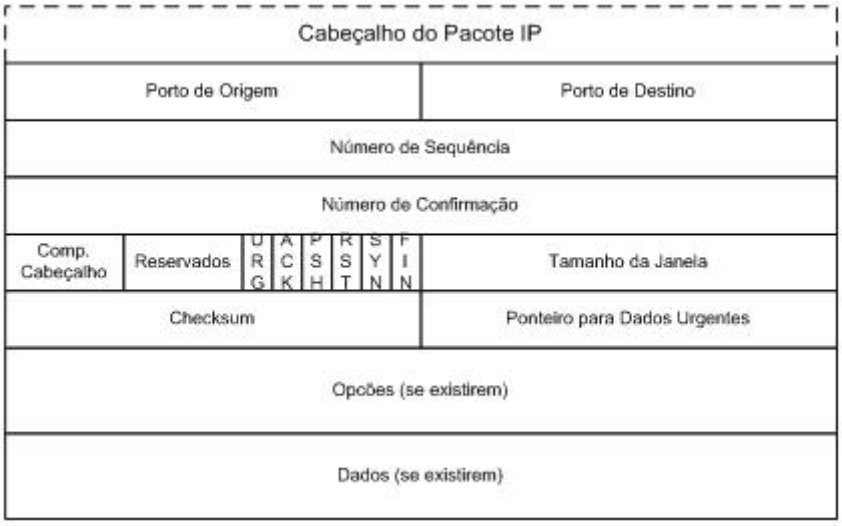

Figura 3.4 – Formato dos Segmentos do Protocolo TCP

3.2.2. UDP

O UDP (*User Datagram Protocol*) é outro protocolo não orientado à conexão, utilizado para a transferência de informação extremo-a-extremo. O UDP não tem qualquer mecanismo fiável que assegure que um pacote enviado seja correctamente recebido portanto, não é considerado um protocolo seguro. O UDP é diferente do TCP é mais indicado para aplicações que não necessitem de confirmação e onde a retransmissão não seja adequada. Por exemplo as consultas do serviço de DNS (Domain Name Service) e a telefonia IP. A figura 3.5 ilustra a o formato dos segmentos do portocolo UDP.

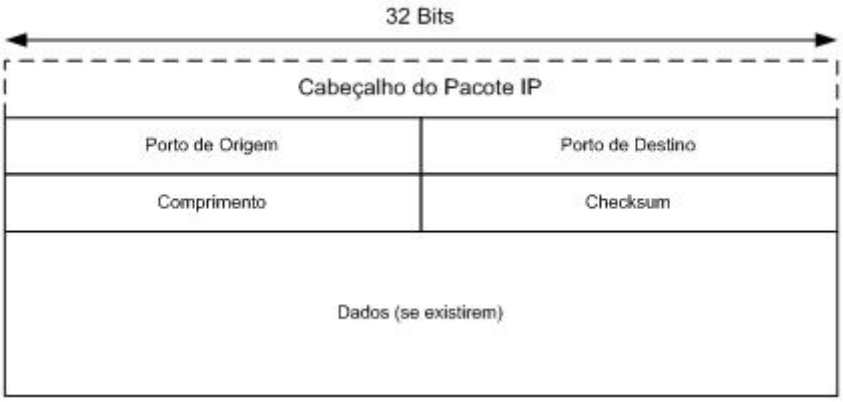

Figura 3.5 – Formato dos Segmentos do Protocolo UDP

O UDP é um protocolo simples usado para VoIP que transfere os datagramas sem qualquer confirmação ou garantia de entrega. Este protocolo necessita que a correcção de erros e a retransmissão seja efectuada por outros protocolos de nível superior. O UDP não tem nenhum mecanismo de controlo de fluxo nem mesmo de retransmissão, simplesmente, actua como interface de processamento entre os níveis superior e inferiores do modelo OSI.
O Cabeçalho UDP contém menos bytes, consumindo menos rede quando comparado com TCP, e porque o UDP não necessita de assegurar a ligação entre origem e destino, o envio é mais rápido. Esta velocidade faz com que UDP seja o protocolo de transporte para VoIP

Para conseguirmos implementar a solução de voz (orientada à conexão) sobre uma rede IP (não orientado a conexão), são necessários algumas alterações ao nível da sinalização (utilizado protocolos para estabelecer e encerrar conexões por exemplo, ITU Q.931 ou H.225). No fundo, teremos que fazer com que uma rede não orientada a conexão pareça uma rede orientada à conexão.

3.2.3. RTP

O protocolo RTP (*Real Time Protocol*) é um protocolo genérico de transporte em tempo real para várias aplicações. A função básica do RTP é multiplexar diversos fluxos de dados de tempo real, (Aplicações multimédia como áudio, vídeo, etc.), sobre um único fluxo de pacotes UDP. O fluxo UDP pode ser enviado a um único destino (*unicast*), ou a vários destinos (*multicast*). Como o RTP utiliza simplesmente o UDP, os seu pacotes não são tratados de maneira especial pelos *routers*, a menos que alguns recursos de qualidade de serviço IP estejam activos. Não existe qualquer garantia de entrega de pacotes.
Cada pacote enviado é numerado sequencialmente. Essa numeração permite ao destino descobrir que falta algum pacote. Se um pacote for omitido, é feita uma aproximação do valor em falta por interpolação. Neste tipo de aplicação a retransmissão não é uma opção prática, pois, o pacote retransmitido provavelmente chegaria tarde de mais para ser útil. Como Consequência o RTP não tem qualquer controlo de fluxo, nenhum controlo de erros, nenhuma confirmação e nenhum mecanismo de retransmissão.
A figura 3.6 ilustra o cabeçalho RTP.

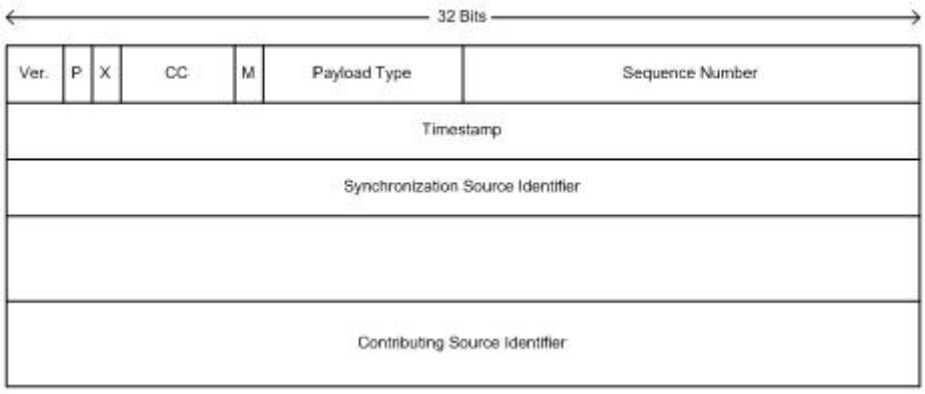

Figura 3.6 – Cabeçalho RTP

O primeiro campo é o *version*, o qual já se encontra na segunda versão.
O *padding* (**P**), quando activado indica que a *payload* sofreu alterações e que os últimos bits devem ser ignorados. Esta alteração pode ser devido a utilização de um algoritmo de encriptação. O ultimo byte do *padding* indica quantos bytes foram acrescentados.
O *bit* **X** indica que um cabeçalho de extensão está presente. O formato e o significado do cabeçalho de extensão não estão definidos. O único detalhe definido é que a primeira palavra de extensão fornece o comprimento.
O campo **CC** contém o número de endereços CSRC que estão presentes, de 0 a 15.
A interpretação do *bit* **M** depende do tipo de cada aplicação. Ele pode ser usado para marcar o início de uma *frame* vídeo, o começo de uma palavra áudio, ou qualquer outro elemento que a aplicação reconheça.
O *Payload Type* identifica o formato do *payload* do pacote RTP, Determinando a interpretação necessária à aplicação. O princípio de construção do RTP faz com que este tenha um campo padrão que será codificado de acordo com a especificidade da aplicação. Para permitir interoperação, o RTP define vários perfis, (por exemplo, um único fluxo áudio) e, para cada perfil podem ser definidos vários formatos de codificação.
O *sequence number* permite a identificação do pacote, permitindo a aplicação destino detectar se ouve o não perda de pacotes. O valor inicial é aleatório, o que dificulta ataques sobre o código encriptado.
O *timestamp* reflecte o início do fluxo do primeiro octeto no pacote RTP. Os *timestamp* são relativos ao início do fluxo, e assim somente as diferenças de *timestamp* são significativas. Os valores absolutos não têm nenhum significado. Este mecanismo permite ao destino realizar

alguma *bufferização* e reproduzir cada amostra depois de um número correcto de milissegundos, contados desde o início do fluxo, dependo de quando chegou o pacote contendo a amostra. O uso do *timestamp* não reduz apenas os efeitos da flutuação, mas também permite a sincronização de vários fluxos.
O *Synchronization Source Identifier* SSRC identifica a fonte de sincronização, devendo esta ser única numa sessão. Ele é escolhido aleatoriamente. Caso haja conflitos de SSCR, existem mecanismos de correcção para este problema.

O *Contributing Source Identifier* CSRC indica a fontes que contribuíram para a formação do fluxo. Para que exista um processamento eficiente do protocolo RTP, o número de ponto de multiplexagem deve ser minimizado. Este princípio decorre do facto de o RTP ser desenhado para usar o modelo de processamento integrado de camadas. A multiplexagem é fornecida pelo endereço de transporte destino, que define uma sessão RTP.

3.2.4. RTCP

O *Real-Time Control Protocol* RTCP é um protocolo necessário para auxiliar e controlar o RTP na transmissão e de dados em tempo real.
A primeira função do RTCP pode ser usada para fornecer feedback sobre a qualidade de transmissão de dados, estando relacionado com o controlo de fluxo, flutuação, largura de banda, congestionamentos e outras propriedades de rede para a origem. Estas informações podem ser usadas pelo processo de codificação para aumentar a taxa de transferência dos dados (oferecer melhor qualidade de serviço) quando a rede estiver com bom funcionamento, ou diminuir a taxa de transferência dos dados quando existirem problemas na rede.
O RTCP também lida com sincronização entre fluxos. O problema é que diferentes fluxos podem utilizar relógios distintos, com granularidade e taxas de flutuação diferentes. O RTCP pode ser utilizado para manter esses elementos sincronizados.
O RTCP ajusta a taxa de envio dos pacote de acordo com o número de utilizadores a utilizar a canal no momento, dependendo do número de participantes o tráfego gerado pode ser grande.

O RTCP fornece um modo para nomear as diversas origens (por exemplo, texto ASCII). Essas informações podem ser exibidas no receptor, a fim de indicar com quem se está a comunicar no momento.

3.3. Endereçamento IP

Cada *host* ligado à Internet é identificado através de um endereço do nível de rede – um endereço IP. Na versão actual do protocolo IP, a versão 4 (conhecida por IPv4), os endereços IP são constituídos por 32 bits, organizados de uma forma a que os bits mais significativos identifiquem a rede e os bits menos significativos o *host* nessa rede.

De forma a permitir redes de diferentes dimensões, foram definidas diferentes classes de endereços IP, representadas na figura 3.7.

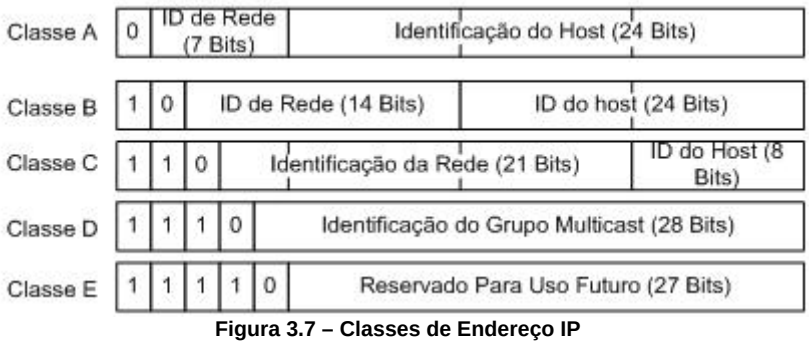

Figura 3.7 – Classes de Endereço IP

Para uma rede de uma classe, o número máximo de *hosts* é condicionado pelo número de *bits* usado para identificar os *hosts* nessa classe. Assim para uma rede de classe C é possível definir 256 endereços, já que a parte do endereço reservada para a identificação de *hosts* tem 8 *Bits.* Note-se desses 256 endereços possíveis nem todos podem ser atribuídos a *hosts*,

alguns são de uso específico, o caso do endereço em que todos os bits são colocados a 1 (endereço de *broadcast*) ou a 0 (normalmente usado para o arranque *hosts* configurados por DHCP.

De modo a facilitar a escrita dos endereços IP, estes podem ser representados na forma decimal, que consiste em quatro números de 0 a 255, separados por pontos, correspondendo cada número à representação decimal do byte correspondente do endereço IP. Por exemplo, o endereço:

11000000.10101000.00001010.00010100

pode ser representado na forma decimal por 192.168.10.20 .
A conversão foi efectuada como base na tabela 3.1 .

Binário	Décimal
00000000	0
00000001	1
00000011	3
00000111	7
00001111	15
00011111	31
00111111	63
01111111	127
11111111	255

Tabela 3.1 – Conversão Binário para Decimal

Assim, as diversas classes de endereços apresentadas na figura 3.7 correspondem, a gama de endereços representadas tabela 3.2 na forma decimal.

Classe	Gama
A	**0**.0.0.0 a **127**.255.255.255
B	**128**.0.0.0 a **191**.255.255.255
C	**192**.0.0.0 a **223**.255.255.255
D	**224**.0.0.0 a **239**.255.255.255
E	**240**.0.0.0 a **247**.255.255.255

Tabela 3.2 – Gamas de Endereços para as Diversas Classes

Na figura 3.7 pode ainda ser observada uma classe de endereços especial: a classe de endereços *multicast*. Os endereços desta classe podem ser utilizados para identificar grupo de máquinas. Ou seja, quando um pacote é enviado para um desses endereços, ele será recebido por todas as máquinas que pertençam a esses grupo. Este tipo de endereços é importante para aplicações de difusão áudio e vídeo.
Dentro de uma dada rede de uma dada classe, a parte reservada para a identificação dos *hosts* poderá ser subdividida, reservando ao *bits* para a identificação das sub-redes.

3.3.1. Espaço de Endereçamento Privado

Os endereços IP não oficiais são genericamente, designados por endereços privados, são definidos 3 espaços de endereçamento deste tipo:

- 10.0.0.0 a 10.255.255.255 (espaço de endereçamento equivalente a uma rede classe A)
- 172.16.0.0 a 172.31.255.255 (espaço de endereçamento a 16 redes de classe B)
- 192.168.0.0 a 192.168.255.255 (espaço de endereçamento a 255 redes de classe C)

Estes espaços de endereçamento podem ser livremente utilizados pelas organizações sem necessidade de qualquer autorização ou coordenação por parte da entidade que regula a atribuição de endereços. As máquinas com endereços nestes espaços de endereçamento podem comunicar livremente dentro das respectivas redes privadas. Não têm, no entanto, conectividade externa, a não ser indirectamente como dispositivos que suportem NAT (*Network Address Translation*, tal como *firewalls*, ou *gateways* de aplicação), nenhum pacote com endereço origem e destino privado será propagado por *routers* na Internet.

3.3.2. Máscara de Sub-Rede

Como já vimos anteriormente, existem duas partes nos endereços IP, a parte que identifica a rede e a parte que identifica o *host*. Todos nós sabemos que a interface de um *host* configurado com o IP não consegue fazer a separação entre a rede o *host*. A mácara de rede dá a resposta a este dilema.
Essa divisão é feita aplicando uma máscara de sub-rede (sequência de 32 *bits* que indica qual a parte do endereço que identifica a rede/sub-rede e qual a parte que identifica a máquina dentro da sub-rede) ao endereço IP.
Pode também ser vista a seguinte notação para a identificação da máscara de sub-rede:

- 193.136.239.64/27

significa que este endereço tem uma máscara de sub-rede de 27 bits e pode ser traduzida por:

- 255.255.255.224 .

A tabela 3.3 mostra-nos a máscara de sub-rede utilizada para cada classe de rede.

Classe	Máscara (em Decimal)	Máscara (em binário)
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

Tabela 3.3 – Máscara de Sub-rede para cada Classe

3.3.3. Sub-redes

Numa dada rede, a parte reservada para a identificação dos *hosts*, poderá ser dividida. Reservam-se alguns desses bits (os mais significativos) para a identificação da sub-rede da rede em causa.
O sub-endereçamento, introduz um novo nível hierárquico de endereçamento. Podemos ver na figura 3.8 .

Figura 3.8 – Hierarquia de Sub-rede

A utilização de sub-endereçamento conduz a uma utilização mais eficiente do espaço de endereçamento. Imagine uma rede classe A como 16.777.214 *hosts*. O *broadcast* e a administração dos *hosts* seria um pesadelo. O encaminhamento é simplificado, todas as sub-redes são vistas do exterior como uma única rede.
A tabela 3.4 mostra-nos o número de redes possíveis utilizando a máscara de sub-rede.

Máscara de Sub-rede	Binário	Número de Redes
0	00000000	1
128	10000000	2
192	11000000	4
224	11100000	8
240	11110000	16
248	11111000	32
252	11111100	64
254	11111110	128
255	11111111	256

Tabela 3.4 – Conversão de Máscara de Sub-rede em Número de Redes

Assim, uma rede classe C poderá ser dividida, por exemplo, em quatro sub-redes, cada uma com espaço de endereçamento de 64 endereços. A tabela 3.5 exemplifica a definição e utilização deste conceito.

Endereço IP	Máscara	Interpretação
192.168.20.137	255.255.255.192	*Host* 9 da rede 192.168.20.128
192.168.20.98	255.255.255.192	*Host* 34 da rede 192.168.20.64
192.168.20.193	255.255.255.192	*Host* 1 da rede 192.168.20.192
192.168.20.12	255.255.255.192	*Host* 12 da rede 192.168.20.0

Tabela 3.5 – Sub-endereçamento e Máscara de Sub-rede

Aplicando uma máscara de sub-rede 192 a um endereço da classe C, criaremos 4 sub-redes. Assim, teremos as seguintes endereços de sub-rede:

- 0 a 63
- 64 a 127
- 128 a 191
- 192 a 255

Uma vez que criamos quatro novas sub-redes necessitamos dos endereços para a rede (todos bits a 0), assim como para *broadcast* (todos bits a 1), então teremos apenas disponíveis os seguintes endereços:

- 1 a 62
- 65 a 126
- 129 a 190
- 193 a 254

3.3.4. Super-netting ou Classeless Inter-Domain Routing

O CIDR (*Classless Inter-Domain Rountig*) surge para ultrapassar a falta de endereços de classe B. De acordo com o CIDR, as necessidades de endereçamento de redes com dimensão superior à dimensão das redes de classe C podem ser supridas utilizando múltiplos endereços de classe C contíguos, por exemplo 2, 4, 8 ou 16 (daí que o CIDR sejam também referido, por vezes de *super-netting*, por oposição ao conceito de sub-netting). Esta agregação de endereços de classe C é muito mais eficiente, em termos de aproveitamento do espaço de endereçamento, do que atribuição de um endereço de classe B que conduz, normalmente, ao desperdício de muitos milhares de endereços. A título de exemplo, considere-se uma rede com quinhentos *hosts*. Anteriormente ao CIDR, essa rede teria que funcionar com um endereço de classe B, levando a um desperdício de 65000 endereços. Com CIDR a mesma rede passa a ter um espaço de 512 endereços, conseguido pela agregação de dois endereços da classe C contíguos.
A adjacência dos endereços de classe C é importante já que permite agregar várias entradas nas tabelas de *routing* dos *routers* numa única entrada, facilitando as decisões de encaminhamento.

3.4. Protocolos de *Routing*

O encaminhamento é uma das principais funções do nível de rede, podendo ser feito de uma forma estática ou dinâmica (por exemplo, criação manual de entradas nas tabelas de encaminhamento), ou de forma dinâmica (por troca de informação automática de encaminhamento entre os *routers*, usando protocolos de encaminhamento apropriados).
O encaminhamento estático pode ser apropriado para pequenas redes e estáveis. É, no entanto, impraticável em redes de grandes dimensões, sendo aconselhável a politica de encaminhamento dinâmico.
São vários os protocolos de *rounting* usados para a troca automática de informação entre os *routers*. A tabela 3.6 ilustra os protocolos relevantes usados nos mecanismos de encaminhamento.

- Sistemas autónomos (*Autonomous Syetms*, AS) – agrupam redes administradas pela mesma entidade, nas quais são usados os mesmos mecanismos de gestão;

- Núcleo de rede (*Core Netwrok*) – rede de *backbone* que interliga os diversos sistemas autónomos;

- Encaminhador interior (*Interior Gateway*) – router usado dentro de um sistema autónomo;

- Protocolo de encaminhamento interior (*Interior Gateway Protocol*, IGP) – protocolo de encaminhamento usado dentro de um sistema autónomo

- Encaminhador exterior (*Exterior Gateway*) – *router* usado na interligação de sistema autónomos;

- Protocolo de encaminhamento exterior (*Exterior Gateway Protocol*, EGP) – protocolo de encaminhamento usado entre sistemas autónomos.

Protocolo	Tipo de encaminhamento		
	interior	exterior	Algoritmo
RIP v1 (*Routing Information Protocol*)	Sim		*distance-vector*
RIP v2 (*Routing Information Protocol*)	Sim		*distance-vector*
IGRP (*Interior Gateway Routing Protocol*)	Sim		*distance-vector*
EIGRP (*Enhanced Interior Gateway Routing Protocol*)	Sim		*distance-vector* + *Link-state*
OSPF (*Open Shortest Path First*)	Sim		*link-state*
EGP (*Exterior Gateway Protocol*)		Sim	-
BGP (*Border Gateway Protocol*)		Sim	-

Tabela 3.6 – Protocolos de *Routing*

3.5. Protocolos de Sinalização e Codificação VoIP

A adaptação da voz analógica nas redes de dados digitais só é possível devido ao processo de converter formas de onda analógica em informação digital realizado por codificadores/descodificadores, normalmente conhecido por CODEC's. Os CODECs utilizam processadores de sinal digital (DSP's), analisando várias formas de voz simultaneamente, geram unidades de informação a intervalos de tempo regulares. Existem diversos *standards* para transformar sinais analógicos. O processo de conversão é bastante complexo. A maior parte das conversões são baseadas em *pulse code modulation* (PCM) ou variações desta modulação.

Na conversão analógica para digital (e vice-versa), os CODEC's podem comprimir os dados e realizar o cancelamento de eco. A compressão do sinal permite poupar largura de banda. No entanto, para se conseguir compressão os CODEC's necessitam de analisar um conjunto de amostras de voz de forma antecipada (l*ookahead*), logo estes CODECs são mais complexos e geram maiores atrasos da codificação e descodificação.

A utilização de compressão e/ou supressão de silencio podem resultar em grandes poupanças de largura de banda. No entanto, existem algumas aplicações que podem ser adversamente afectadas com a compressão (por exemplo, os esquemas de compressão podem afectar o funcionamento dos modems, podem provocar atrasos na transmissão, etc.).

São vários os algoritmos que podemos utilizar para melhorar a qualidade da voz, utilizando a menor taxa de transmissão, o menor atraso, e menor complexidade de implementação. Na tabela 3.7 são apresentados os *standards* de codificação mais importantes, abrangidos pelo ITU (*International Telecommunications Union*). Podemos ver que o preço a pagar por se reduzir a largura de banda é o aumento do atraso de conversão.

Standard ITU	Descrição	Largura de Banda (Kbps)	Atraso de Conversão/Codificação (ms)
G.711	PCM	64	< 1.00
G.721	ADPCM	32, 16, 24, 40	< 1.00
G.728	LD-CELP	16	~ 2.5
G.729	CS-ACELP	8	~15.00 a 25.00
G.723.1	Multirate CELP	6.3, 5.3	~ 30.00 a 70.00

Tabela 3.7 – Standards de Codificação ITU

A tabela 3.8 mostra-nos a relação entre o modelo de referência OSI e os protocolos VoIP.

Nível da Camada OSI	Standards
Apresentação	G.711, G.721, G.729, etc
Sessão	H.323, H.245, H.225, RTCP
Transporte	RTP, UDP
Rede	IP, RSVP, WFQ
Ligação	PPP, Frame Relay, ATM, etc

Tabela 3.8 – Modelo de Referência OSI e os Standard H.323

De seguida apresentam-se alguns detalhes de alguns standards ITU:

- ITU-T G.711 (PCM)
  - 64 Kbps (50 ou 33 pacotes por segundo);
  - Intervalos de 20 ou 30 ms;
  - Atraso de processamento e complexidade mínimos

O sistema PCM é definido na recomendação do ITU G.711. Ele codifica um único canal de voz realizando uma amostragem de 8.000 vezes por segundo de 8 *bits*, afim de fornecer voz descomprimida a 64 Kbps.

- ITU-T G729a
  - 8 Kbps (50 ou 33 pacotes por segundo);
  - Intervalos de 20 0u 30 ms;
  - Codificação ACELP (*Algebraic-Code-Excited Linear-Prediction*);
  - 10 ms (*frame*),
  - 5 ms (*lookahead*),
  - 10 ms (processamento) = 25 ms

- ITU-T G.723.1
  - 5,3 Kbps (158 *bits* / 30 ms);
  - 6,3 Kbps (189 *bits* / 30 ms);
  - Tipos de Condicação:
    - ACELP para 5.3 Kbps
    - ML-MQL para 6.3 Kbps;
  - Algoritmo parecido com o G.729, no entanto com aior janela de observação (180 amostras);
  - Atraso de codificação
    - 30 ms (*frame*),
    - 7,5 ms (*lookahead*),
    - 30 ms (processamento) = 67,5 ms.

O protocolo G.723.1 aceita um bloco de 30 ms de voz e utiliza a codificação preditiva com o objectivo de reduzi-las a 24 *bytes*. Este algoritmo oferece uma taxa de saída de 6,3 ou 5,3 Kbps (factores de compactação 10 e 12), respectivamente, com pequena perda de qualidade.

3.6. Protocolo H.323

O H.323 é provavelmente a norma mais importante de suporte na telefonia IP. Para evitar que cada fornecedor projectasse a sua própria pilha de protocolos, o que provocaria grandes problemas no funcionamento, vários construtores interessados reuniram-se, sobre a alçada da ITU, no sentido de construírem um protocolo genérico de suporte à telefonia IP. A primeira versão do H.323 surge em 1996. Esta primeira tentativa permitia comunicações em ambiente de rede local (LAN's) que se baseava no estabelecer de chamadas com protocolos proprietários sem qualquer tipo de qualidade de serviço. Esta recomendação foi revista em 1998, tornando a base para os primeiros sistemas de telefonia IP.
A recomendação H.323 define um conjunto de componentes, protocolos e procedimentos necessários para fornecer comunicações (áudio, vídeo e dados) sobre redes IP.

O H.323 faz referência a um grande número de protocolos específicos para a codificação de voz, configuração de chamadas, sinalização, e transporte de dados. A tabela 3.9 mostra os diferentes protocolos de suporte para áudio e vídeo e dados.

Multimédia	Formatos
Áudio	G.711, G722, G.723.1, G.728, G.720, GSM
Vídeo	H.261, H262, H.263
Dados	Série de recomendações T.120

Tabela 3.9 – Formatos Multimédia Reconhecidos na Arquitectura H.323

Todos os sistemas H.323 devem ter suporte para G.711 (sistema PCM), (protocolos para codificação e descodificação e de compressão de voz na rede telefónica), sendo no entanto permitidos outros protocolos de compressão de voz. São usados diferentes algoritmos de compressão admitindo diferentes compromissos entre qualidade e largura de banda. Uma vez que são permitidos diversos algoritmos de compressão, existe a necessidade de um protocolo de suporte para a sua negociação. Este protocolo é designado por H.245. A figura 3.9 mostra a interoperabilidade e o papel dos vários protocolos H.323.

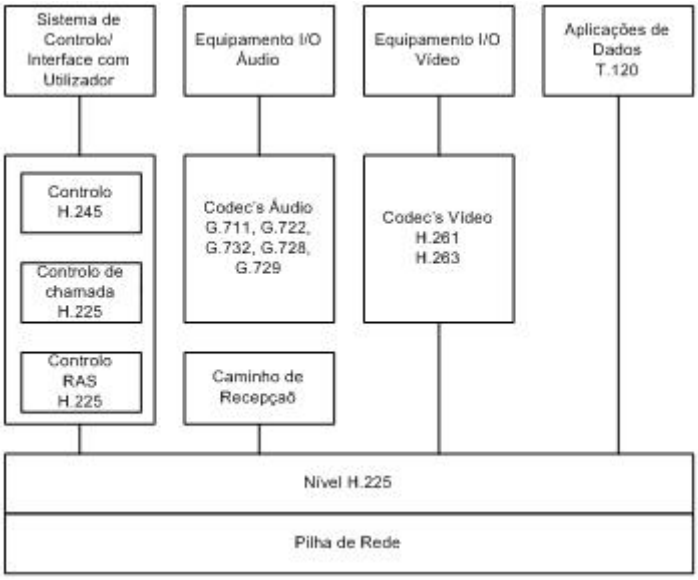

Figura 3.9 – Interoperabilidade do Protocolo H.323

3.6.1. Componentes H.323

Para que se possa utilizar e perceber correctamente o protocolo H.323, é fundamental perceber a importância e as funcionalidades dos seus diversos componentes. Apesar do protocolo H323 ser usado em várias aplicações, (como por exemplo, VoIP, videoconferência e outras), o processamento H.323 é distribuído por vários componentes:

- terminais;
- *gateways*;
- *gatekeepers*;
- *Mutipoint Control Units* (MCU's).

A figura 3.10 ilustra os diferentes componentes do protocolo H.323.

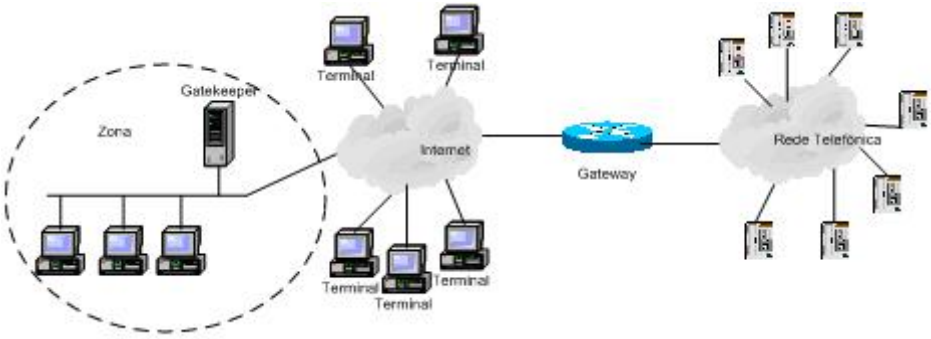

Figura 3.10 – Modelo da Arquitectura H.323

Os terminais fornecem a interface com o utilizador e o protocolo H.323. Os terminais são responsáveis pela comunicação multimédia, (como áudio, vídeo e dados), bidireccional em tempo real.
No caso do VoIP, o terminal H.323 é normalmente um telefone IP. No caso do vídeo, é um terminal de videoconferência. O H.323 pode ser encontrado num PC, é o caso do software da Microsoft *NetMetting* que permite transmitir voz e vídeo no PC do utilizador. Para que um dispositivo seja considerado um terminal H.323, o dispositivo em causa deve conter os seguintes itens:

- interface de rede;
- CODECs áudio;
- software H.323.

Os terminais H.323 tem que suportar obrigatoriamente o G.711, sendo o G.723.1 e o G.729 recomendados para aplicações onde a largura de banda seja reduzida. O suporte para vídeo e dados é opcional; o uso do H.261 é obrigatório nas transmissões vídeo. Os protocolos H.245 e H.225 são usados para funções de controlo, e o RTP é usado para o controlo de sequencia dos pacotes.

A principal função do *gateway* é fornecer os meios para que uma rede H.323 comunique com outras redes, tipicamente a rede telefónica pública (PSTN). Para fornecer esta interoperabilidade o *gateway* é responsável pela adaptação da sinalização, controlo de fluxos, e conversão multimédia entre as diferentes redes. É utilizado para iniciar, manter e terminar uma chamada.
O protocolo usado para a sinalização de chamada é o H.225, e para a sinalização de canais multimédia é o H.245, sendo os protocolos RTP e RTCP usados para a transmissão e controlo respectivamente.

Os *gatekeepers* regulam todos os dispositivos terminais que podem iniciar e/ou receber chamadas. Muitos autores consideram que os *gatekeepers* são o "cérebro" da rede H.323. Sempre que existam *gatekeepers* numa rede H.323, é obrigatório que os terminais utilizem os seus serviços. A arquitectura H.323 utiliza um conceito de zona que compreende o gatekeeper e todos os conceitos que ele controla como podemos observar na figura 3.10.
O gatekeeper deve providenciar a todos os dispositivos registados os serviços de controlo de admissão, tradução de endereços e controlo de largura de banda. Antes de iniciar qualquer chamada o H.323 utiliza o protocolo RAS (*Registration Admission Status*) para permitir que os dispositivos entrem ou saiam da zona, ou seja, autorização para efectuar chamadas. Os critérios que devem ser utilizados pelo *gatekeeper* para a autorização de chamadas não são especificados no H.323 ficando a critério da implementação.
O *gatekeeper* é um dispositivo que tem o controlo sobre as chamadas realizadas e/ou recebidas pelos os dispositivos na zona sob a sua responsabilidade, sendo uma importante fonte de informação para fins de contabilização de chamadas e *billing*.

O MCU (*Mutipoint Control Units*) dá suporte necessário a conferências envolvendo mais do que dois dispositivos terminais. Gere os recursos e as negociações de *CODECs* de transmissão áudio e vídeo entre diferentes terminais.
Um MCU e constituído por dois componentes funcionais:

- O *Multipoint Controller* (MC) - manipula a negociação H.245 com todos os dispositivos que vão participar na conferência, identificando a capacidade de áudio e vídeo comum a todos, determinando assim um modo comum a ser adoptado. Cada dispositivo estabelece uma sessão bidireccional com o MC.
- O *Multipoint Processor* (MP) é responsável por converter informação multimédia para diferentes formatos, ou por combinar áudio proveniente de várias fontes, transmitindo o fluxo combinado para todos os dispositivos.

3.6.2. O Funcionamento do H.323

O processo para estabelecer e manter uma chamada com o protocolo H.323 e muito complexo. A seguir será explicado as fases e os recursos necessários para se efectuar uma chamada H.323. A figura 3.11 ajuda a perceber como estes protocolos se relacionam entre si.

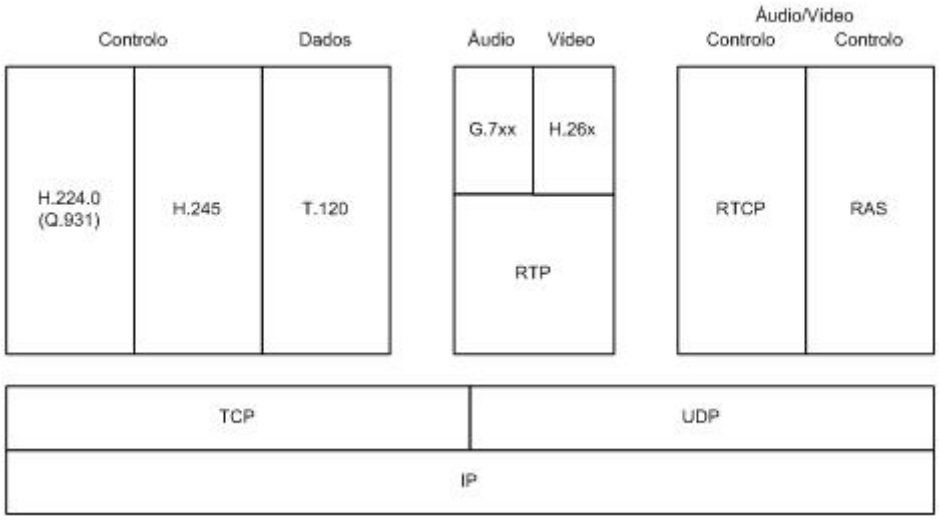

Figura 3.11 – Pilha Protocolar H.323

Agora que conhecemos um pouco mais dos dispositivos e os protocolos que fazem com que H.323 funcione, veremos as diferentes fases e procedimentos necessários para estabelecer uma ligação. Que são:

- descoberta e registo;
- configuração da chamada;
- negociação sinalização de fluxo;
- negociação do controlo de fluxo ;
- terminar chamada.

Durante a fase de descoberta e registo o terminal tem que descobrir o *gateKeeper* (GK) e, para isso, efectua um *broadcast* de um pacote UDP de forma a descobrir o GK. O Registo é efectuado para determinar qual é a zona a que o dispositivo esta associado, (zona, é um conjunto de componentes H.323 geridos por um único GK). Logo que o GK responde, o dispositivo terminal aprende o endereço IP do GK. Nesta fase, regista-se com o GK, enviando uma mensagem RAS num pacote UDP. A figura 3.12 mostra a fase de descoberta da zona por parte do terminal.

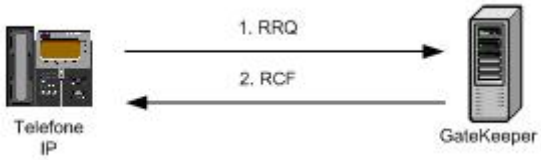

Figura 3.12 – Descoberta e Registo

1. O telefone IP envia uma mensagem RAS H.245 *Request to Register* (RRQ) ao GK.
2. O GK confirma o registo enviando uma mensagem *Registration Confirmation* (RCF) de retorno ao Telefone IP.

O telefone IP volta a enviar uma mensagem RAS ao GK a solicitar a largura de banda. Só depois da largura de banda ser concedida é que é possível iniciar a configuração da chamada. A ideia de solicitar a largura de banda tem como objectivo de permitir ao GK limitar o número de chamadas, evitando assim saturar a linha de saída, e desse modo oferecer a qualidade de serviço desejado.

Depois da concessão da largura de banda, o telefone envia uma chamada Q.931 de configuração através de uma ligação TCP. A configuração da chamada utiliza os protocolos existente na rede telefónica, que são orientados à conexão, e portanto, o TCP é necessário. Esta mensagem especifica o número de telefone que está a ser chamado. O GK responde com uma mensagem Q.931 para confirmar a recepção correcta da solicitação. Nesta fase o GK encaminha a mensagem de configuração da chamada para o *gateway*.

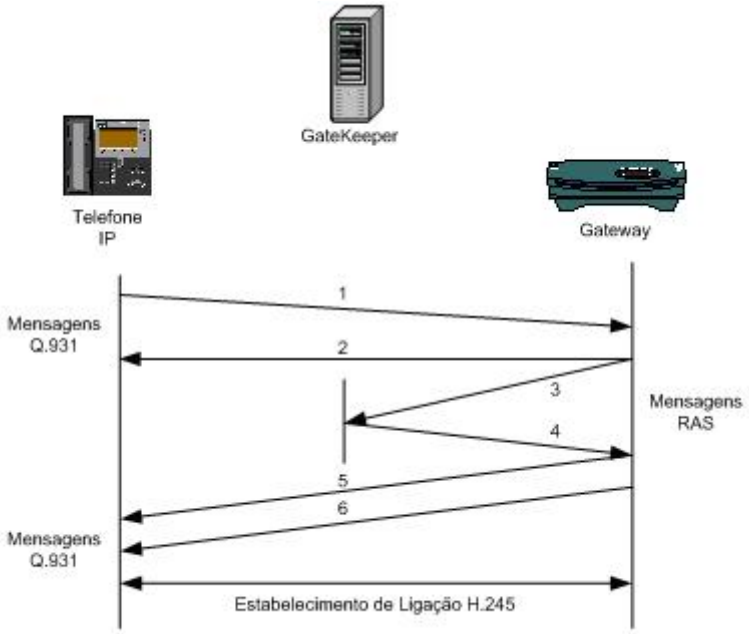

Figura 3.13 – Configuração de Chamada

A configuração da chamada é baseada na norma ITU-Q.931 (H.225 é um subconjunto da Q.931), que fornece os meios para estabelecer, manter e terminar uma chamada. A figura 3.13 ilustra a configuração de uma chamada utilizando o protocolo H.323.

1. O telefone envia uma mensagem H.225 de sinalização para o *gateway*, solicitando uma conexão.
2. O *gateway* envia uma mensagem de retorno ao telefone IP, avisando que pode avançar com a chamada.
3. O *gateway* envia uma mensagem RAS ao GK a solicitar autorização para a chamada
4. O GK envia uma mensagem de retorno ao *gateway* indicando a autorização para a chamada
5. O *gateway* envia uma mensagem H.225 ao telefone IP, alertando que a chamada foi estabelecida
6. O *gateway* envia uma mensagem ao telefone IP, confirmando a chamada, a chamada é estabelecida.

Após o estabelecimento da ligação, apenas o *gateway* se encontra envolvido na chamada, os pacotes seguintes ignoram o *gatekeeper* e vão directamente para o endereço IP do *gateway*. Neste momento, só temos um canal entre as duas partes. Trata-se apenas de uma conexão da camada física para a movimentação de *bits*.

O protocolo H.245 é agora usado para negociar os parâmetros dos canais da camada lógica. Múltiplos canais lógicos de diversos tipos (áudio, vídeo e dados) são permitidos para uma única chamada. O H.245 abre um canal lógico para cada tipo de transferência. Os canais podem ser unidireccionais ou bidireccionais. A figura 3.14 ajuda a visualizar como o H.323 utiliza os canais virtuais

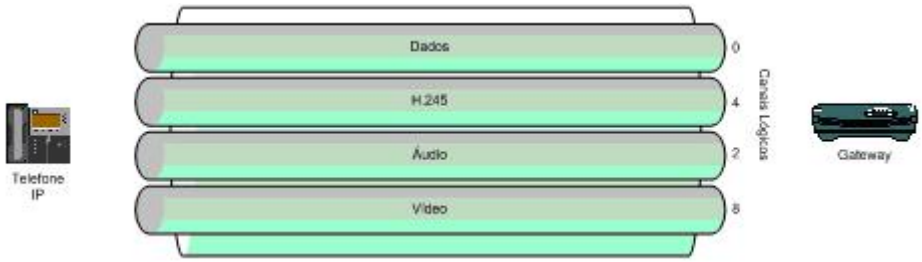

Figura 3.14 – Configuração de Canais Lógicos

Cada lado anuncia os seus recursos, (por exemplo, se pode lidar com vídeo ou conferência de chamadas, quais os CODECs aceites, etc.) depois de cada dispositivo saber qual o tipo de CODEC que cada um pode manipular, são configurados os canais, e estabelecidos os protocolos para comunicarem. Depois de concluídas as negociações, o fluxo de dados pode começar a utilizar o protocolo RTP. Este é gerido pelo RTCP, o qual desempenha uma função importante no controlo de tráfego. Quando uma das partes desliga o telefone, o canal de sinalização do H.225/Q.931 encerrará a ligação. Quando a chamada é encerrada, o telefone IP volta a conectar-se com o *gatekeeper* com mensagem RAS de forma a proceder a libertação da largura de banda que tinha recebido.

3.7. Session Initiation Protocol (SIP)

Dada a complexidade do protocolo H.323, projectado pela ITU, para muitas pessoas ligadas a Internet trata-se de um protocolo típico de empresas de telecomunicações: grande, complexo e inflexível. Assim sendo, o *Internet Engineering Task Force* (IETF) estabeleceu um comité, (*Multipart Multimedia Session Control*, MMUSIC), para projectar um protocolo, baseado no *Simple Mail Transport Protocol* (SMTP) e no *Hypertext Transfer Protocol* (HTTP), mais simples e mais modular de utilização de voz sobre IP. O Resultado foi *Session Initiation Protocol* (SIP), descrito na RFC 3261.

O SIP define os procedimentos para efectuar chamadas, videoconferência e outras conexões multimédia na Internet. O SIP é um protocolo do nível de aplicação, independente dos níveis protocolares inferiores (TCP, UDP, ATM, *Frame-Relay*). É baseado na arquitectura cliente/servidor, na qual o cliente inicia a chamada e o servidor responde a essa chamada. O SIP foi projectado para interoperar com aplicações de Internet existentes. Por exemplo ele define os números de telefone como URL's (*Uniform Resource Locator*), para que as páginas *Web* possam conter esses números, bastando apenas um *click* do rato sobre a hiperligação para iniciar a chamada. Podem também ser utilizados endereços IP do tipo IPv4 e IPv6 ou mesmo números de telefone reais.
Sendo o SIP um protocolo de texto baseado nos *standards* Internet (HTTP e SMTP), permite que operações de *debugging* e resolução de problemas sejam facilitadas.
O SIP é um protocolo mais recente que o H.323, sem maturidade e o suporte da empresas de telecomunicações. Contudo, devido a sua simplicidade, escalabilidade, modularidade e facilidade interoperar com outras aplicações, tornou-se num protocolo atractivo para comunicações de voz sobre IP.

O SIP disponibiliza os seguintes serviços:

- determina a localização do ponto terminal alvo – suporta resolução de endereços, mapeamento de nomes e redireccionamento de chamadas;
- determina as capacidades, recursos do ponto terminal destino – com *Session Description Protocol* (SDP) determina os serviços (de mais baixo nível) entre os dispositivos terminais. Por exemplo, as conferências[1] são estabelecidas usando apenas recursos comuns entre os dois pontos terminais.
- determina a disponibilidade do ponto terminal – se uma chamada não pode ser estabelecida por causa do ponto terminal, o SIP determina se o "chamado" se encontra ao telefone ou não atende devido ao número de toque (*rings*) ter sido atingido. Este envia uma mensagem de retorno indicando porque é que o "chamado" está indisponível.
- Estabelece uma sessão entre origem e destino – se a chamada pode ser efectuada o SIP estabelece uma sessão entre a origem e o ponto terminal destino. O SIP suporta

alteração dos parâmetros de uma chamada durante uma sessão por exemplo, adição de outro ponto terminal numa conferência ou alteração das características do meio ou mesmo CODEC's.

- suporta mecanismos para transferência e terminação de chamadas – o SIP suporta a transferência de chamada de um ponto terminal para outro. No final da chamada, são terminadas todas sessões com os participantes.

[1] *O termo conferencia, significa estabelecer uma sessão (ou chamada) entre dois ou mais pontos terminais.*

O SIP pode estabelecer sessões de duas partes (ligações telefónicas comuns) sessões de várias partes (onde todos podem ouvir e falar) e sessões com um emissor e vários receptores (*multicast*).

3.7.1. Componentes do SIP

O SIP é um protocolo ponto-a-ponto. Os pontos terminais numa sessão são chamados *User Agents* (UAs). Um *user agent* pode funcionar em um dos seguintes papeis:

- *User Agent Client* (UAC) – uma aplicação cliente que inicia o pedido SIP;
- *User Agent Server* (UAS) – uma aplicação servidor que contacta o cliente quando recebe o pedido SIP e devolve a resposta em beneficio do utilizador.

Tipicamente um ponto terminal SIP pode actuar como cliente e/ou servidor. Quem define se um ponto terminal funciona como cliente ou servidor é o utilizador que inicia o pedido.

Os servidores SIP podem interoperar com outros servidores aplicacionais como por exemplo, servidores LDAP (*Lightweight Directory Access Protocol*), aplicações de base dados ou aplicações XML (*Extensible Markup Language*). Estes serviços fornecem ao utilizador autenticação, serviços de directório e *billing*.

Os componentes físicos da arquitectura SIP podem ser agrupados em duas categorias: Clientes e Servidores. A figura 3.15 ilustra arquitectura SIP.

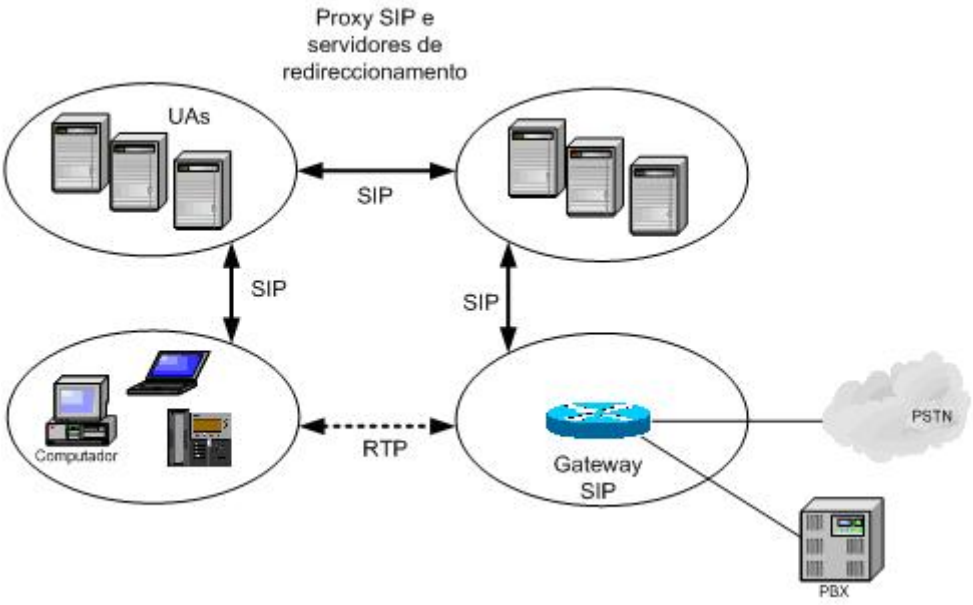

Figura 3.15 – Arquitectura SIP

Os clientes SIP incluem:

- Telefones – que podem actuar como UAS ou UAC. *Softpones* (PCs com capacidades telefónicas instaladas)
- *Gateways* – fornecem controlo de chamadas. Os *gateways* fornecem vários serviços, os mais comuns são os mecanismos de tradução entre os dispositivos terminais SIP

com outro tipo de terminais. Esta função inclui tradução entre formatos de transmissão, definição de CODECs áudio e Vídeo e configuração de chamadas.

Os servidores SIP incluem:

- *Proxy Server* – o servidor *proxy* é um dispositivo intermédio que recebe pedidos SIP e encaminha-os de acordo com os objectivos do cliente. Basicamente, os servidores proxy recebem mensagens SIP e encaminha-as para o próximo servidor SIP na rede. Os servidores *proxy* disponibilizam funções de autenticação, autorização, controlo de acesso à rede, retransmissão fiável de pedidos e segurança.
- *Redirect Server* – os servidores de redireccionamento fornecem informação ao cliente acerca do próximo salto (*Hop*) ou saltos que a mensagem deve tomar.
- *Registrar Server* – o servidor de registo, como o próprio nome indica, processa os pedidos dos UACs e regista a sua corrente localização. Normalmente, este servidor encontra-se na mesma localização que o *redirect* ou *proxy server*.

3.7.2. O Funcionamento do Protocolo SIP

O SIP é um protocolo de texto (ASCII) que usa pedidos e respostas para estabelecer comunicações entre vários componentes de uma rede.
Os utilizadores numa rede SIP são identificados por um único endereço. Um endereço SIP é similar a um endereço de e-mail por exemplo, userID@dominio.pt. A identificação pode ser ainda o nome do utilizador, número de telefone (endereço E164).
O utilizador regista o seu ID com o *registrar server,* assim como, a sua localização. O *registrar server* fornece esta a informação ao servidor de localização.
Quando o utilizador inicia a chamada, uma mensagem SIP é enviada para o servidor proxy ou *redirect.* O pedido inclui o endereço do "chamador" e o endereço do chamado.
O utilizador final pode movimentar-se por vários sítios terminais, a localização do utilizador pode ser dinamicamente registada pelo servidor SIP.
A tabela 3.10 apresenta as mensagens do protocolo SIP.

Tipo		Método	Descrição
Pedido		INVITE	Solicita a inicialização de uma sessão
		ACK	Confirma que a sessão foi iniciada
		BYE	Solicita o término de uma sessão (necessita de confirmação pelo outro lado)
		OPTIONS	Consulta um ponto terminal sobre os seus recursos, em geral é usado antes da sessão ser iniciada
		CANCEL	Cancela uma solicitação pendente
		REGISTER	Informa um servidor de redireccionamento sobre a localização actual do utilizador
Resposta	Informação	100 TRYING	Acção em curso, mas o utilizador não foi encontrado
		180 RINGING	Encontrada uma localização registada do utilizador, que foi alertado
	Sucesso	200 OK	O pedido foi bem sucedido
	Redireccionamento	300 Multiple Choices	O utilizador poderá ser encontrado num dos vários endereços indicados
		301 Moved Permanently	O utilizador passou a usar o endereço indicado
		302 Moved Temporarity	O utilizador poderá ser encontrado no endereço indicado

Tabela 3.10 – Mensagens do SIP

Para estabelecer uma sessão, o "chamador" envia uma mensagem *INVITE* para o servidor proxy. O servidor proxy determina o caminho e encaminha o pedido para o ponto terminal, o "chamado".
O "chamado" envia a resposta ao *proxy* , o qual, encaminha a resposta ao "chamador".

O servidor *proxy* envia uma mensagem para as duas partes envolvidas. A sessão está então estabelecida entre o "chamador" e o "chamado". O RTP é usado para a comunicação entre os pontos terminais. A figura 3.16 ilustra a configuração de uma sessão usando o servidor *proxy*

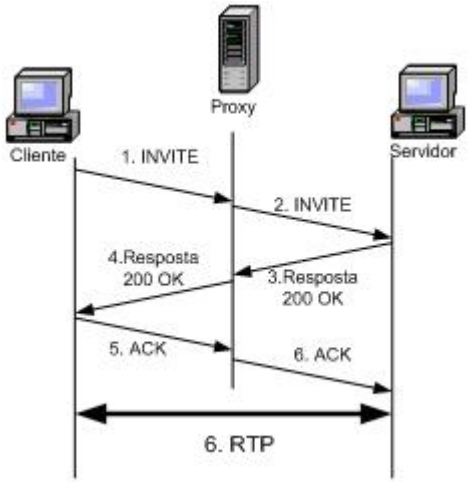

Figura 3.16 – Configuração de uma Sessão Com Servidor *Proxy*

3.8. Comparação entre o Protocolo SIP e o H.323

O SIP e H.323 foram projectados para endereçar sessões de controlo e funções de sinalização em arquitecturas distribuídas de controlo de chamadas.
Ambos permitem comunicações com dois ou mais participantes, utilizando computadores ou telefones como pontos terminais, admitem negociações de parâmetros, criptografia e utilizam os protocolos RTP e RTCP para transporte e controlo, respectivamente. Apesar das semelhanças, também apresentam diferenças. A tabela 3.11 apresenta as diferenças e semelhanças destes protocolos.

O protocolo H.323 é constituído por múltiplos protocolos incluindo, Q.931 para a sinalização, H.245 para a negociação e o RAS (*Registration Admission Status*) para controlo de sessões. Este protocolo é considerado por muitos, um protocolo grande, pesado, complexo e rígido, típico das empresas de telecomunicações, difícil de adaptar a soluções futuras.
Pelo o contrário, o SIP é um protocolo típico da Internet e funciona trocando mensagens simples de texto ASCII. É um protocolo com boa interoperação com os outros protocolos da Internet, mas não muito bom com os protocolos de sinalização do sistema telefónico existente. Por ser um protocolo altamente modular e flexível, (modelo VoIP IETF), pode ser facilmente adaptado a novas aplicações.

Item	SIP	H.323
Projectado Por	IETF	ITU
Serviços e inteligência de rede	Fornecida por servidores (Proxy, Redirect, Registrar)	Fornecida pelos Gatekeepers
Compatibilidade com PSTN	Ampla	Sim
Compatibilidade com a Internet	Sim	Não
Modelo Usado	Internet/WWW	Telefonia/Q.SIG
Arquitectura	Modular	Monolítica
Dimensão	O SIP lida apenas com a configuração	Pilha de protocolos completa
Negociação de Parâmetros	Sim	Sim
Protocolo de média	RTP/RTCP	RTP/RTCP
Formato de mensagens	ASCII	Binário (ASN.1 Enconding)
Outros protocolos usados	Protocolos IETF/IP, Mime, http e SDP	Protocolos ITU/ISDN,H.225, H.245, H.450
Interoperabilidade	Alargada	Alargada
Sinalização de Chamadas	SIP sobre TCP ou UDP	Q.931 sobre TCP
Chamadas de Vários participantes	Sim	Sim
Conferências Multimédia	Não	Sim
Endereçamento	URL	Número de Host ou telefone
Término de Chamadas	Explícito ou por timeout	Explícito ou encerramento por TCP
Transmissão de mensagens Instantâneas	Sim	Não
Criptografia	Sim	Sim
Implementação	Moderada	Grande e complexa
Status	Boas perspectivas de êxito	Extensamente Distribuído

Tabela 3.11 – Comparação entre o SIP e o H.323

4. Qualidade de Serviço

A qualidade da voz em redes de comutação de pacotes IP (VoIP) é de extrema importância para o bom funcionamento da telefonia IP.
A perda de pacotes, os atrasos, a variação de atrasos e os congestionamentos contribuem para a degradação da qualidade da voz.
Para se obter a qualidade de serviço desejada, são necessários mecanismos que reduzam o número de pacotes descartados em momentos de saturação na rede, minimizem os atrasos existentes durante uma ligação.

4.1. O que é o QoS?

O QoS (*Quality of Service*) é um conjunto de mecanismos, ferramentas disponíveis para que os administradores de rede possam aplicar diferentes níveis de serviço aos pacotes IP que circulam numa rede.
Nem todos os protocolos são sensíveis aos congestionamentos de rede. Por exemplo, o FTP (*File Transfer Protocol*) é um protocolo tolerante a atrasos e a limitações de largura de banda. Para o utilizador, o FTP pode demorar um pouco mais a descarregar um ficheiro para o computador. Para o utilizador existe a apenas o problema da lentidão, mas não o impede de completar a operação. Por outro lado, aplicações de voz e vídeo são particularmente sensíveis aos atrasos na rede. Se os pacotes demoram demasiado tempo a atingir o seu destino, o resultado do discurso é distorcido ou seja, imperceptível. O QoS pode ser usado para aplicar níveis de serviço previsíveis a estas aplicações. O QoS pode também ser utilizado a outras aplicações críticas das organizações.

4.2. Aplicações para QoS

Aqui ficam algumas razões para implementar QoS numa topologia de rede:

- dar prioridade a aplicações críticas na rede;
- rentabilizar a infra-estrutura de rede maximizando o seu uso;
- aplicar melhores performances para aplicações sensíveis a atrasos, como no caso da voz e vídeo;
- em resposta a alteração de fluxos na rede.

Muitas vezes, para melhorar a performance de uma rede, aumentar a largura de banda era a solução. Contudo, aumentar a largura de banda nem sempre garante a melhor performance. Poderá existir na rede protocolos que causem congestionamentos ocupando, logo à partida, toda a largura de banda disponível. A forma mais justa para solucionar o problema é analisar o tráfego no *bottleneck* (zonas onde se verificam os congestionamentos), determinar a importância de cada protocolo na aplicação e definir a estratégia no sentido de prioritizar o acesso à largura de banda. O QoS permite ao administrador de rede controlar a largura, a latência, a variação de atraso (*jitter)* e a perda de pacotes numa rede.
Aplicações *multicast* como, *streaming* multimédia e VoIP necessitam de certos níveis de serviço, especialmente porque são aplicações susceptíveis a atrasos e a variação de atrasos. As fracas performances são imediatamente notadas pelo utilizador final. Estas fracas performances levam os utilizadores a abrirem incidências nas equipas de manutenção. Estes problemas podem ser resolvidos proactivamente, o administrador poderá gerir novas aplicações aplicando as técnicas de QoS. É importante relembrar que a implementação de QoS não é uma solução mágica que resolve todos os problemas numa rede. Contudo, conhecendo as opções disponíveis, o administrador de rede estará em melhor posição para resolver os problemas de qualidade e saturação na rede.
No respeita ao atraso, para se poder manter uma conversa interactiva, o atraso máximo extremo-a-extremo deve ser inferior a 150 ms (ITU-T), embora na prática, valores de 200 ms ainda sejam toleráveis. Existem diversas componentes de atrasos que podem influenciar o mesmo:

- atrasos nos codificadores de voz (25 ms – G.729a, até 100 ms – G.723.1);
- *buffers* de compensação de filas de *jitter* (30 a 60 ms);
- filas dos elementos da rede (variável);
- propagação do meio físico (10 ms / 1000 km);
- atrasos de serialização (tempo para a transmissão de pacotes que estão em fila no *buffer* de transmissão FIFO (*First In First Out*) da interface física).

4.3. Níveis de QoS

O QoS pode ser dividido em três níveis diferentes, também conhecidos como modelos de serviço. Estes modelos de serviço definem um conjunto de potencialidades QoS extremo-a-extremo. O QoS extremo-a-extremo é a capacidade da rede oferecer um nível de serviço específico de tráfego de um extremo ao outro.
Os três níveis de serviço são:

- *Best-effort* – serviço melhor-esforço;
- *Integrated Service* - serviço integrado;
- *Differentiated Service* - serviço diferenciado.

O serviço *best-effort*, como o próprio nome indica, é quando a rede faz todos os esforços possíveis, na tentativa de entregar os pacotes ao seu destino. Com este serviço, não há qualquer garantia que o pacote chegue ao destino. O HTTP e o FTP são exemplos de aplicações que podem funcionar neste modelo. Contudo, modelo não é aconselhável apara aplicações sensível a atrasos, flutuações de largura de banda e outras variações das condições de rede. As aplicações telefónicas necessitam de uma largura de banda mínima garantida para funcionar correctamente. O uso do *best-effort* para aplicações deste tipo provocaria cortes na chamada durante uma conversação.

O modelo de serviço integrado (*Integrated service*) garante um nível de serviço ás aplicações, negociando os parâmetros extremo-a-extremo. As aplicações requisitam o nível de serviço desejado para o seu bom funcionamento aos mecanismo de QoS, que reservam os recursos necessários antes da aplicação começar a transmitir. É importante notar que a aplicação só começará a transmitir quando receber um sinal com garantias que a rede pode suportar os recursos requisitados pelos mecanismos de QoS. Para realizar esta tarefa a rede utiliza um mecanismo chamado *Admission Control*.
O *admission control* é um mecanismo que evita que a rede fique sobrecarregada. A rede não envia o sinal à aplicação para iniciar a transmissão dos dados, se não conseguir satisfazer o pedido de QoS. A aplicação começando a transmitir os dados, os recursos reservados são mantidos extremo-a-extremo até que a aplicação termine, ou até que a largura de banda reservada exceda o permitido pela aplicação.
A Cisco tem dois mecanismos para fornecer os serviços integrados. Eles são, o *Resource Reservation Protocol* (RSVP) e o *Intelligent Queuing*. O *intelligent Queuing* inclui técnicas como o *Weighted Fair Queuing* (WFQ) e *Weighted Random Early Detection* (WRED).
O RSVP é um protocolo proprietário usado para sinalizar os requisitos de QoS de uma aplicação. É importante notar que o RSVP não é um protocolo de *routing*, (protocolos de *routing* são técnicas utilizadas para o encaminhamento dos pacotes entre equipamentos *routers*, ver secção 3.4). Os RSVP trabalha em conjunto com os protocolos de *rounting* para determinar qual o melhor caminho de rede para fornecer o QoS desejado.

O modelo serviço diferenciado inclui um conjunto de mecanismos de classificação e marcação permitindo a diferenciação e o tratamento de tráfego baseados nos parâmetros dos pacotes. O serviço define as características importantes associadas à transmissão de pacotes pelos nós da rede. Os atributos podem ser especificados em termos quantitativos (por exemplo, valores de débito, atraso, variação de atraso e/ou perdas de pacotes, expressa sobre a forma determinística ou probabilística) e em termos de prioridade relativa a acessos aos recursos da rede.

4.4. Classificação

Na classificação de pacotes é necessário implementar mecanismos que permitam identificar e marcar cada pacote ou fluxo de rede, facilitando um posterior tratamento diferenciado.
Tal classificação, deve ser realizada o mais próximo possível da origem, podendo ser feita tanto no nível 2 (nível de ligação de dados) como no nível 3 (nível de rede).

A classificação de pacotes no nível 2 é feita através dos campos definidos na norma 802.1p (*Layer* 2 *Class os Service*) e no nível 3, a classificação é feita através do campo *IP Precedence / Differentiated Services Code Point* (DSCP), figura 4.1 utilizando o campo (*Type of Service*) do cabeçalho IPv4.

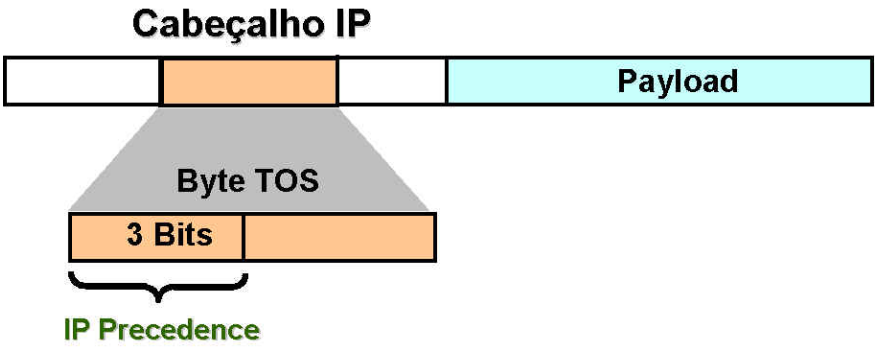

Figura 4.1 – Precedência IP no Campo TOS

Com o objectivo de suportar na mesma infra-estrutura IP aplicações de dados (não sensíveis a atrasos) e aplicações com requisitos de tempo real, tornou-se necessário a criação de extensões ao modelo *best-effort*, que incluam o suporte de diferentes níveis de QoS e a capacidade de gerir a atribuição de recursos por classes de serviços.

Desta forma é possível recorrer a dois mecanismos diferentes, mas que utilizam o mesmo campo de cabeçalho IP, a precedência IP ou a utilização de serviços diferenciados (DSCP).
O campo *Type of Service* é destinado a distinguir diferentes classes de serviço. Quando se trata de voz digitalizada a entrega rápida vence a transmissão segura. Para a transferência de ficheiros, uma transmissão segura e mais importante que uma transmissão rápida.

A precedência IP utiliza os 3 bits mais significativos do campo TOS para especificar a prioridade de 0 a 7 (o valores 6 e 7 são reservados para controlo e não devem ser utilizados pelo administrador de rede), por defeito os pacotes são marcados com o bit zero. Os *bits* 3 a 6 são usados para especificar os serviços diferenciados (conhecido por *Differentiated Services Code Point* DSCP, RFC 2475).

4.5. Reduzir os Congestionamentos na Rede

A necessidade de largura de banda e rápidos tempos de resposta são uma das necessidades frequentes das aplicações que circulam nas nossas redes. É tarefa do administrador de rede assegurar que essas aplicações tenham níveis satisfatórios de performance, assim como, garantir o uso eficiente as larguras de banda disponíveis.
Para evitar congestionamentos na rede, existem vários mecanismos de QoS que podem ser aplicados nas interfaces dos *routers*. Os mecanismos de QoS são os siguintes:

- *Compressed Real-Time Transporte Protocol* (CRTP)
- Queuing
  - *Prioriary Queing* (PQ)
  - *Custom Queuing* (CQ)
  - *Weighted Fair Queuing* (WFQ)
  - *Class-Based Weighted Fair Queuing* (CBWFQ)
- Classificação de pacotes
- Precedência IP
- Politicas de encaminhamento
- *Resource Reservation Protocol* (RSVP)
- *Call Admission Control* (CAC)

4.5.1. Compressão do Protocolo RTP

O protocolo CRTP (*Compressed Real-Time Transport Protocol*) define o mecanismo que reduz a sobrecarga (*overhead*) do cabeçalho do protocolo RTP, eliminando a informação redundante entre pacotes. Por exemplo, imagine uma *stream* multimédia com 100 pacotes, onde os primeiros 99 têm cabeçalhos idênticos e os últimos os sinais de fim de transmissão. Porque é que os *routers* deveriam transmitir a mesma informação 99 vezes?
O RTP, como já vimos anteriormente, é o protocolo usado para a transmissão de tráfego multimédia (aplicações com requisitos de tempo real, como áudio e vídeo) sobre uma rede IP.

A compressão do cabeçalho aumenta a eficiência da rede, especialmente nas rede com largura de banda reduzida, (bastante utilizado em linhas *frame-relay*, HDLC e encapsulamento PPP).
A figura 4.2 ilustra a compressão de um cabeçalho RTP.

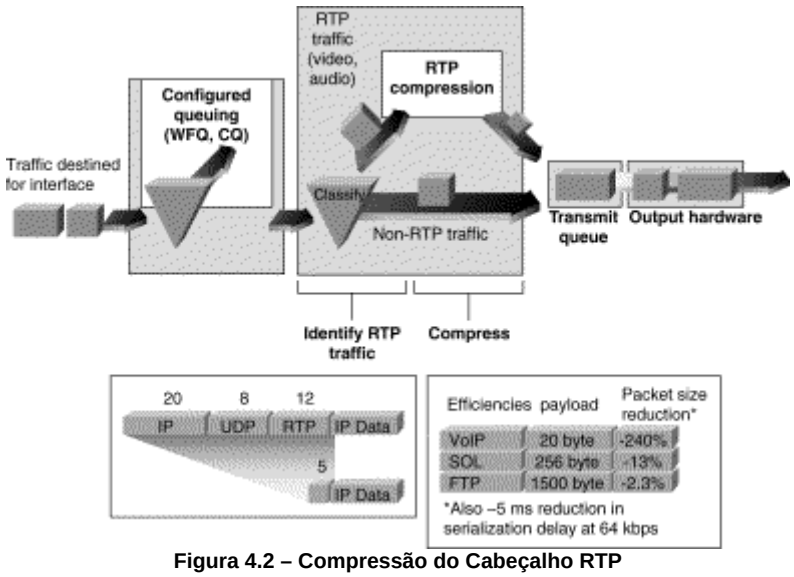

Figura 4.2 – Compressão do Cabeçalho RTP

O pacote RTP tem 40 *bytes* para o cabeçalho (IP / UDP / RTP) e 20 a 150 *bytes* para os dados. Com a compressão do cabeçalho RTP podemos reduzir os 40 *bytes* para 5 ou 2 *bytes*, reduzindo desta forma consideravelmente a sobrecarga na rede IP.

4.5.2. Queuing

É importante percebermos os conceitos básicos do processo de funcionamento do *queuing*. Nos *routers*, as *queues* funcionam como "zonas de espera". A *queue* (fila de espera) retém os pacotes até que existam recursos suficientes disponíveis para o seu encaminhamento pela interface de saída. Se não existir qualquer nível de saturação (congestionamento) na rede, os pacotes são encaminhados imediatamente. As *queues* são usadas nos casos em que a circulação de pacotes é muito superior a capacidade de processamentos das interfaces de saída. Por exemplo, um *router* ligando uma interface *fast ethernet* (LAN) a uma interface E1 (WAN), o circuito vê chegar grandes quantidades de informação pela interface LAN mais rápido do que aquilo que pode enviar pela interface de saída WAN. Neste caso, a *queue* coloca o tráfego numa "zona de espera" para que a interface WAN possa processar toda informação. Isto é o normal funcionamento da rede, não significando qualquer problema de congestionamento.
São vários os tipos de *queuing* que podem beneficiar a rede VoIP. São eles:

- Custom Queuing
- Priority Queuing
- WFQ
- CBWFQ

O algoritmo *custom queuing* (CQ) permite configurar o número de *bytes* (ou número de pacotes) que se pretende encaminhar quando a fila está a ser servida. O CQ processa o tráfego especificando o número de bytes que são servidos por cada classe de tráfego. As filas são servidas em ciclos (*round-robin*), onde são processados os pacotes definidos antes de passar a próxima fila. Podem ser definidas até 16 filas, a fila zero é reservada para mensagens de sistema (sinalização, *keep-alive*). A configuração CQ não é dinâmica, logo não se adapta as alterações das condições de rede. A figura 4.3 mostra o funcionamento do CQ.

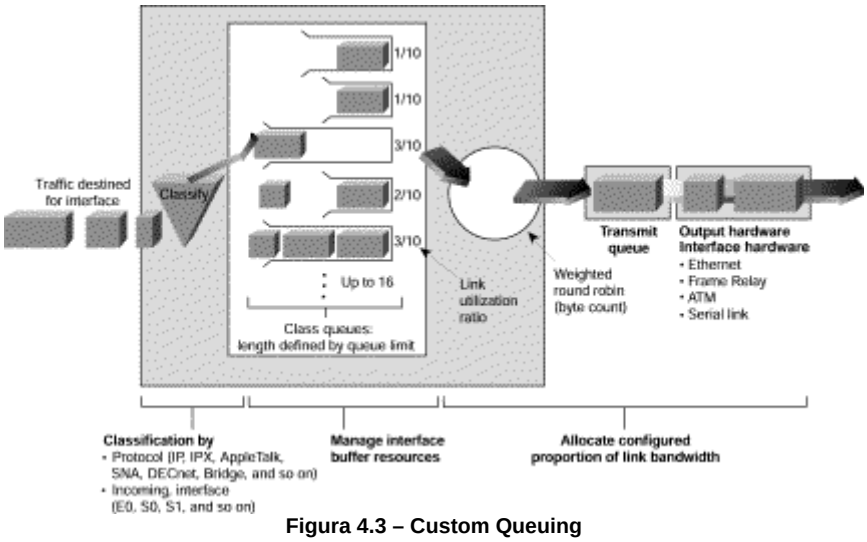

Figura 4.3 – Custom Queuing

O algoritmo *Priority Queing* (PQ) define como o tráfego é servido em quatro níveis de prioridade.
OS quatro níveis de prioridade são:

- Alta
- Media
- Normal
- Baixa

A fila de prioridade mais alta é servida até ficar vazia, só depois são servidas sequencialmente a filas de prioridade mais baixa.
Os pacotes que não tenha qualquer classificação de prioridade são servidos pela fila de prioridade normal.
É importante notar que este tipo de *queuing*, em locais com largura de banda reduzida, pode fazer com que as filas de prioridade mais baixa nunca sejam servidas.
A figura 4.4 mostra o funcionamento do PQ.

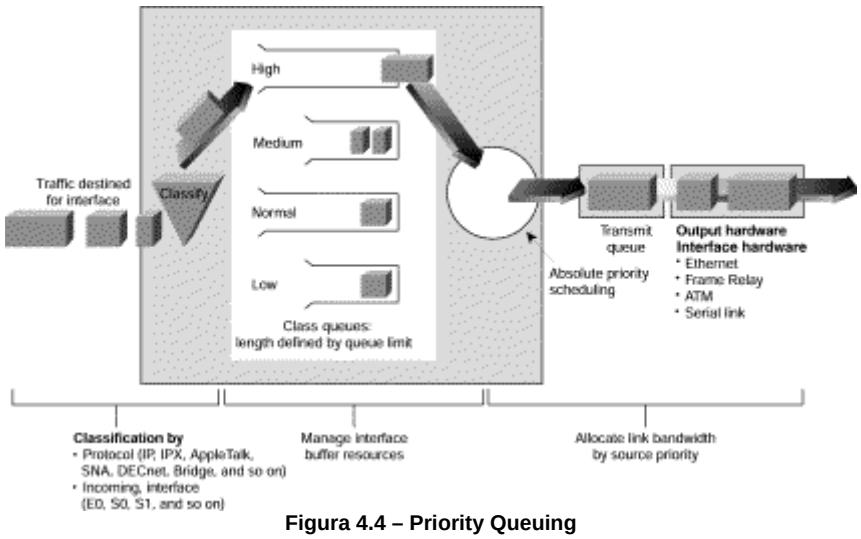

Figura 4.4 – Priority Queuing

O algoritmo *Weighted Fair Queuing* (WFQ) é um mecanismo de gestão dinâmico que define a largura de banda "justa" a todo o fluxo de tráfego de uma rede. O WFQ atribui pesos aos pacotes definindo qual quantidade de largura de banda permitida numa conversação relativamente a outras conversações.
O WFQ classifica o tráfego em diferentes fluxos (sessões) baseado no endereçamento do cabeçalho da mensagem, incluindo características como endereço destino, endereço origem, porto e o tipo de serviço (TOS).

Existem duas categorias de fluxo:

- sessões com muita largura de banda;
- sessões com pouca largura de banda.

As sessões com muita largura de banda partilham o serviço de transmissão proporcionalmente de acordo com os pesos atribuídos a cada pacote. As sessões com pouca largura de banda, a grande maioria do tráfego numa rede, recebe um serviço especial, permitindo que os pacotes sejam encaminhados num tempo aceitável.
O WFQ coloca o tráfego nas filas de espera antes da transmissão. A ordem da remoção dos pacotes nas filas e determinada pelo tempo virtual da entrega do ultimo *bit* de cada pacote.
O WFQ adapta-se dinamicamente a alterações das condições da rede, sendo bastante útil em conexões série (E1, T1) inferiores a 2 Mbps.
A figura 4.5 mostra o funcionamento do WFQ.

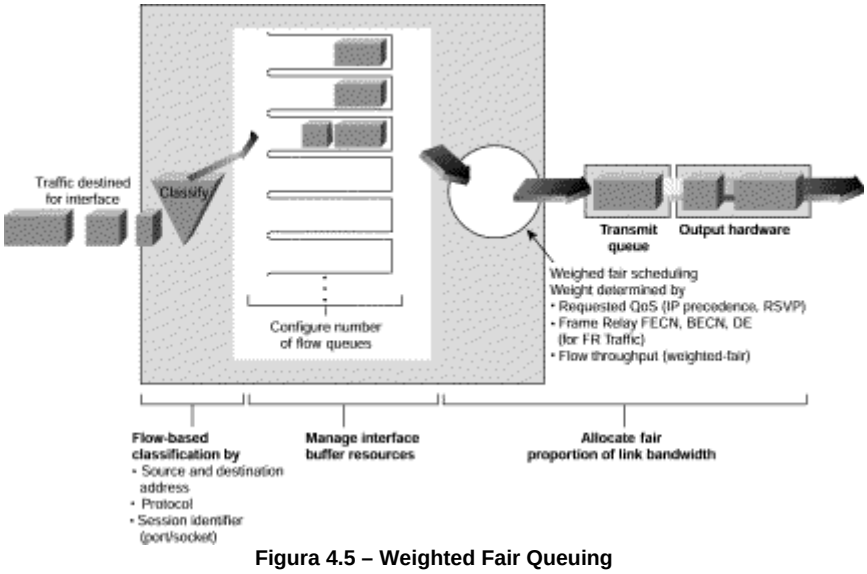

Figura 4.5 – Weighted Fair Queuing

A *class-based Weighted Fair Queing* (CBWFQ) é uma extensão do WFQ que suporta funcionalidades de classe de tráfego definidas pelo utilizador. Com o CBWFQ, são definidas classes baseadas em critérios de *match* incluindo protocolos, listas de controlo de acesso (*Access Control Lists* ACLs) e interfaces de entrada. Os pacotes que satisfaçam os critérios de da classe constituem o tráfego dessa classe. É reservada uma fila de espera por cada classe, o tráfego pertencente à classe é redireccionado para a respectiva fila espera.
Uma vez definida a classe com base no critério de *match*, podemos atribuir as suas características. Para caracterizar a classe podem ser definidos atributos como largura de banda, pesos e o limite máximo do pacote. A atribuição da largura de banda a uma classe, é a garantia da largura de banda de entrega da classe em momentos de congestionamento na rede.
Para caracterizar a classe também se pode especificar o limite da fila de espera, que é o número máximo de pacotes que a fila pode acumular. Os pacotes pertencentes a uma classe estão sujeitos a largura de banda e aos limites da fila dessa classe.
Depois de uma fila atingir o limite configurado na classe, a chegada de novos pacotes acciona o serviço *tail drop* ou *packet drop*, dependendo do tipo de politica que a classe tem configurada. O *tail drop* é usado por defeito nas classes CBWFQ podendo no entanto ser configurado o *packet drop*, usado no *weighted random early detect* (WRED), como meios de evitar o congestionamento nas filas de espera.
Se a classe por defeito for configurada com o comando "*bandwidth policy-map*", todo o tráfego não classificado é colocado numa única fila e tratado de acordo com a largura de banda configurada. Se a classe por defeito for configurada pelo comando "*fair-queuing*", todo o tráfego não classificado é encaminhado com a política *best-effort*. Os pacotes classificados são tratados pelos mecanismos de diferenciação de tráfego de cada classe.

A classificação do fluxo é um tratamento *standard* WFQ. Os pacotes com o mesmo endereço IP origem, endereço IP destino, porto TCP ou UDP origem e destino são classificados como pertencentes ao mesmo fluxo. O WFQ reserva a mesma largura de banda para cada fluxo.
No CBWFQ cada pacote, que verifique as politicas configuradas na classe, é marcado com o peso dessa classe. Os pacotes que chegam à interface de saída são classificados de acordo com os critérios de *mach* (filtros) definidos pelo utilizador, sendo depois marcado com o respectivo peso. O peso associado a cada pacote depende da largura de banda configurada na classe.
Depois de especificado o peso para o pacote, estes são encaminhados para as respectivas filas de espera, sendo estas servidas de uma forma justa.

4.6. Classificação de Pacotes

Muitas vezes, existe a necessidade de classificar o tráfego nas redes. As razões para a classificação variam de rede para rede, os pacotes são normalmente marcados com "*flags*" para fazer deles mais ou menos importantes relativamente a outros pacotes na rede, identificando aqueles que podem ser descartados.
A marcação com "*flags*" pode ser feita de várias maneiras, e os níveis de classificação dependem dos métodos utilizados. O uso de esquemas de prioridade como o *random early detection*[1] (RED) e o *adaptive bit rate* (ABR) forçam os *routers* a analisar as *streams* de dados e as características de congestionamento e desta forma, aplicam mecanismos de controlo de congestionamento às *streams* de dados. O uso da classificação de tráfego dentro de um pacote retira a capacidade de decisão dos *routers* e estabelece níveis de serviço que são necessários para fluxos de tráfego particulares. O *router* tenta fornecer ao pacote o nível de QoS desejado.

A classificação de pacotes pode ser efectuada com base nos valores da tabela 4.1.

Tipo de Tráfego	Classificação do Tráfego		
	Precedência IP	CoS	DSCP
Tráfego de Voz	5	5	EF
Tráfego de sinalização Voz	3	3	AF31
Videoconferência	4	4	AF41
Streaming Vídeo	1	1	AF13
Dados Críticos GOLD	2	2	AF21-23
Dados Críticos SILVER	1	1	AF11-13
Less-Than-Best-Effort	0	0	2-6
Best-Effort	0	0	BE

Tabela 4.1 – Recomendações de Classificação de Tráfego

[1] ***Random Early Detection*** *é um mecanismo para prevenção e inibição de congestionamento. O algoritmo analisa anticipadamente o tráfego utilizando as funções de controle de congestionamento TCP, descartando pacotes aleatoriamente e indicando à origem para reduzir a taxa de de transmissão, evitando assim situações de congestionamento antes que ocorra picos de tráfego. Quando activado numa interface, o RED começa a descartar pacotes a uma taxa que pode ser previamente configurada.*

4.7. Precedência IP

A precedência IP (do inglês *IP Precedence*) é um parâmetro configurável nos pontos de chamada que define o valor da prioridade na rede. É manualmente atribuído ao ponto de chamada na infra-estrutura VoIP através do seguinte comando:

```
dial-peer voice 10 VoIP
ip precedence 5
```

Este comando deve ser usado para dar mais prioridade aos pacote VoIP que ao pacotes de dados *standard*, quando estes partilham a mesma largura de banda disponível. Veremos como os atributos de precedência IP influenciam os algoritmos de CBWFQ e como em conjunto podem aumentar a performance de voz numa rede.

Existem vantagens e desvantagens na utilização destes métodos de QoS no VoIP. Um dos factores mais importantes a ter em conta é o tipo de atributos de QoS que a rede pode suportar, (na Cisco, existem diferentes versões de sistemas operativos (IOS), a funcionalidades variam de versão para versão). É importante perceber o tipo de tráfego que circula na rede para os dados e para a voz, para que não seja cortado nenhum tráfego de dados vital.
Lembre-se dos seguintes pontos ao decidir quais os algoritmos a usar:

- A precedência IP é um método de controlo mais confortável para os administradores de rede. Pode escolher o nível de precedência que se encontra disponível para o tráfego onde pretende activar o QoS. Não pode ser controlado dinamicamente; é configurado manualmente em cada ponto de chamada. Contudo, o QoS poderá levar a uma sobrecarga de administração devido aos refinamentos necessários.
- O *Resource Reservation Protocol* (RSVP) é mais complexo de configurar no início, pois os níveis de tráfego tem que ser analisados e ajustados em cada parte física. O RSVP é extremamente poderoso, em *links* com muitos congestionamentos e *links* WAN mais lentos. Poderá ajustar-se dinamicamente ao sistema sem desperdiçar largura de banda.
- Recomenda-se o uso do método precedência IP em vez do RSVP devido ao esforço de desempenho da tecnologia RSVP. A precedência IP é um método de controlo mais estável.

4.8. Politicas de Encaminhamento

O *Policy Routing* é um método pela qual podem ser direccionados os pacotes, baseado em critérios (politicas), para tomar rotas diferentes aquelas que seriam tomadas pelos protocolos de encaminhamento *standards*. O *policy routing* classifica o tráfego baseado em lista de controlo de acesso (*Access Control Lists*, ACL) aplicado às políticas classe de serviço. A classificação e a aplicação de politicas são configuradas por um filtro de pacotes chamado *route map*. O *route map* consiste em dois tipos: *match* e o *set*. O comando *match* compara o pacote com a lista *standard* ou estendida (*Standard* ou *Extended Access List*) e/ou o tamanho do pacote. O comando *Set* determina a acção que é tomada pelo pacote que faz *matching* onde se podem atribuir os seguintes atributos:

- precedência IP;
- próximo salto IP;
- interface;
- próximo salto por defeito;
- interface por defeito.
-

Com o uso do *policy routing* os pacotes são encaminhados automaticamente sem que seja verificada se a rota existe ou não na tabela de encaminhamentos.

4.9. Resource Reservation Protocol

O *Resource Resarvation Protocol* (RSVP) é o protocolo usado para reservar largura de banda extremo-a-extremo num fluxo IP para fluxos de tráfego *multicast* ou *unicast*. A grande diferença do RSVP dos restantes protocolos *standards* de encaminhamento é que o RSVP trabalha em todo o fluxo, em vez de encaminhar apenas *datagramas* individuais. A reserva é feita desde o nó receptor até ao nó envio e a conexão é uma sessão simples, então o tráfego nos dois sentidos necessita de duas sessões RSVP individuais. Uma sessão consiste num fluxo de dados para um determinado destino e protocolo, identificado pelo endereço destino, protocolo e pelo porto destino.

Existem três tipos de tráfego RSVP:

- *Best-effort* é o tráfego IP *standard* não orientado à conexão, onde os protocolos de nível superior são responsáveis pela detecção de erros e controlo de fluxo;
- *Rate sensitive* é a classe onde o fluxo necessita de uma taxa constante (por exemplo, 128 Kbps ou 384 Kbps) evitando atrasos na filas com a negociação de largura de banda;
- *Delay sensitive*:

- *Controlled delay* para aplicações não tempo real;
- *Predictive Delay* é usado para voz, vídeo e outras aplicações de tempo real.

4.10. Call Admission Control

O *Call Admission Control* (CAC) é um termo genérico que descreve o método pela qual um nó pode prevenir que sejam requisitados mais recursos do que aqueles que a rede pode suportar num determinado momento, estes mecanismos preservam a qualidade das transmissões existentes. Muitas vezes utilizado em aplicações de voz ou videoconferência, o CAC rejeita os pedidos de recursos à rede se a aplicação necessitar mais largura de banda do que aquela que se encontra disponível. Por exemplo, se uma interface está configurada com 128 Kbps e estando em progresso cinco chamadas de VoIP necessitam de 24 Kbps cada, o CAC previne que uma sexta chamada seja iniciada, porque esta chamada iria degradar a qualidade das chamadas activas. Este sistema assegura que as ligações existentes mantenham a largura de banda de que necessitam. Quando uma conexão é rejeitada, o nó origem poderá, dependendo da configuração da rede, encontrar um caminho alternativo ou então dar um sinal de ocupado.
A figura 4.6 ilustra o encaminhamento de uma chamada quando um circuito está totalmente ocupado

Existem diferentes métodos para implementar o CAC, mas para os objectivos do VoIP, o mais utilizados são o RSVP e as zonas de largura de banda do *gateway* H.323. O *gatekeeper*, neste caso, analisa a rede tomando decisões de *Call Admission* baseado em cálculos estáticos para aceitar ou rejeitar uma chamada como ilustra a figura 4.6. O *gatekeeper* subtrai à largura de banda disponível o valor requisitado pela nova ligação e em função do resultado determina se aceita ou descarta a ligação.

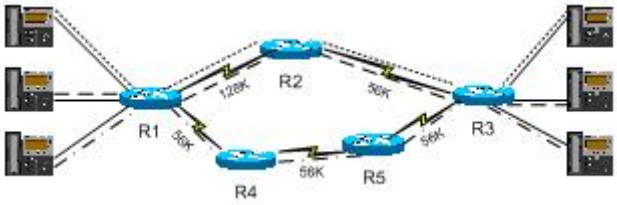

Figura 4.6 – Funcionamento do *Call Admission Control*

4.11. Prioridade RTP

A prioridade RTP (*Real-Time Transport Protocol*) define a prioridade para a transmissão de dados UDP sensíveis a atrasos. Com o comando *ip rtp priority* os utilizadores podem especificar um porto RTP que terá prioridade sobre as outras filas de espera na mesma interface. Uma vez configurado, os pacotes identificados com o porto RTP prioritário terá prioridade sobre os restantes pacotes na interface. As políticas das filas prioridade RTP são baseadas na largura de banda total, e não no número individual de conexões. Contudo, se a fila está configurada para 128Kbps, reserva a totalidade da largura de banda mas não previne o excesso de números de chamadas. O resultado, pegando no exemplo anterior, se existem cinco chamadas com 24kbps cada, a sexta chamada poderá ser aceite, reduzindo a largura de banda de cada chamada para 21Kbps, por esta razão, é da responsabilidade do utilizador garantir que a largura de banda reservada não seja excedida.

4.12. Traffic Shapping

O *Traffic Shapping* é um método para controlar a transmissão de dados de saída nas interfaces limitando o tráfego a uma determinada taxa de transmissão. Existem dois tipos de *traffic shaping*: *Frame Relay Traffic Shaping* (FRTS) e o *Generic Traffic Shaping* (GTS).

O FRTS usa uma variedade de comandos para gerir o fluxo de tráfego no sentido de evitar ou reduzir congestionamentos na rede. Os comandos incluem o *Committed Information Rate* (CIR), *Forward Explicit Congestion Notification* (FCEN*), Backward Explicit Congestion Notification* (BCEN) e o *Excess Information Rate* (EIR). Por exemplo, com o FRTS pode-se

limitar o CIR à taxa de transferência pico do tráfego de saída para cada circuito virtual (VC), procedimento denominado por *rate enforcement*. Pode obter-se uma maior granularidade no controlo de tráfego, aplicando técnicas de *queuing* como *proprity queuing* ou *custom queuing* em cada circuito virtual ou ao nível da sub-interface.

O GTS é um método de controlo ao nível da interface. O tráfego de saída é limitado a uma determinada taxa de transmissão usando o sistema *Token Bucket* [2], sendo os picos de tráfego armazenados em filas de espera para limitar o fluxo. Desta forma, o tráfego que reúne determinado perfil pode ser modelado (*Shape*) no sentido de reduzir os congestionamentos. O GTS aplica-se apenas às interfaces de saída, com o uso de listas de acesso para classificar e seleccionar o tráfego.

[2] ***Token Bucket*** é uma definição formal para taxa de transferência. Possui três componentes: um tamanho em bits (burst size), também chamado de committed burst (Bc) que especifica quanto pode ser enviado num determinado intervalo de tempo; uma taxa média (mean rate) em bps, também chamada de CIR (Committed Information Rate), que especifica quantos dados, em média, podem ser enviado por unidade de tempo; e um intervalo de tempo (Tc) em segundos.

4.13. Weighted Random Early Detection

O *Weighted Random Early Detection* (WRED) é um método que os *routers* utilizam para gerir as suas filas de espera (implementação Cisco) de forma a evitar congestionamentos antes que estes ocorram. O WRED baseia o seu funcionamento no RED, que analisa o tráfego numa classe específica de uma interface e descarta os pacotes à medida que os congestionamentos aumentam. Quando a origem detecta pacotes descartados, diminui a taxa de transferência. As filas de espera tem limites, uma vez cheias, os pacotes são descartados por não existirem mais recursos disponíveis para os suportar, este fenómeno é conhecido como *Tail Dropping*. O *tail dropping* é indesejado porque descarta os pacotes sem qualquer tipo de selecção, o *router* não consegue identificar a prioridade. O WRED resolve este problema, descartando os pacotes com base nos níveis de precedência IP.
O WRED trabalha melhor com o tráfego TCP porque quando os pacotes são descartados, o TCP regula o tráfego, reduzindo o número de congestionamentos. Por esta razão, o WRED pode causar problemas numa rede onde circule grandes quantidades de tráfego UDP. O UDP não se ajusta a descarte de pacotes e não regula as velocidades de transmissão.

4.14. Fragmentação e Interleaving

A fragmentação e o *interleaving* são o método utilizado para reduzir os atrasos das aplicações de tempo real, como o caso do VoIP. Considere um pacote FTP com 1500 *bytes* a tentar passar numa ligação série de 128Kbps. O pacote demora cerca de 94ms a passar essa ligação. Um pacote VoIP que chegue depois do pacote FTP será forçado a esperar cerca de 94ms. Considerando que um pacote VoIP extremo-a-extremo não deverá demorar mais do que 150ms, podemos ver que a espera terá um impacto significativo na qualidade da voz figura 4.7.
O LFI (*Link Fragmentation and Interleaving*) resolve este problema, fragmentando os pacotes grandes em *datagramas* mais pequenos para que os pacotes de tempo real possam ser intercalados durante a transmissão, reduzindo o atraso. A figura 4.8 Ilustra um exemplo desta aplicação.

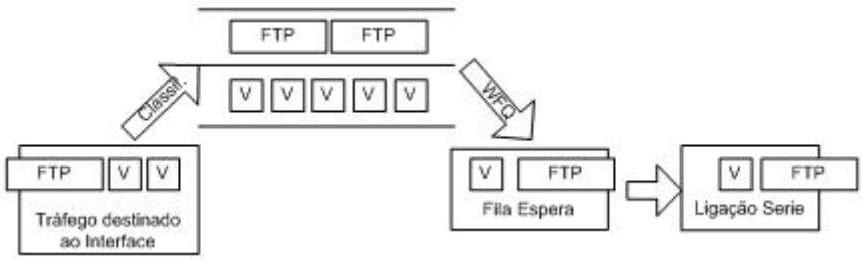

Figura 4.7 – Transmissão sem LFI

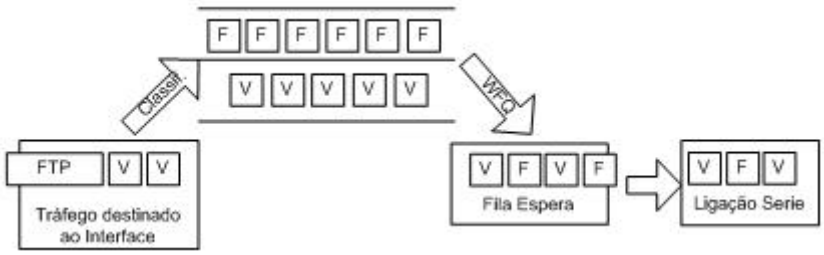

Figura 4.8 – Transmissão com LFI

5. Configurações de Soluções VoIP

Depois de apresentados os conceitos básicos que suportam a tecnologia VoIP, chegou o momento de apresentar um caso prático de uma implementação típica de VoIP. A figura 5.1 ilustra um caso possível para a implementação da telefonia IP.

As principais motivações para a implementação do VoIP são:

- a optimização dos recursos instalados, nomeadamente no que respeita a largura de banda;
- gestão de uma única infra-estrutura de rede;
- custo de manutenção mais baixos;
- custo de exploração mais baixos, redução dos circuitos de comunicação alugados, rentabilizando as larguras de banda disponíveis.

Estas são algumas das razões que levam as empresas as redefinir as suas estratégias, que passa por implementar uma infra-estrutura única para suportar voz e dados com capacidade para no futuro suportar a implementação de outros serviços, como videoconferência ou mesmo o serviço unificado de mensagens (*Unified Messaging*).

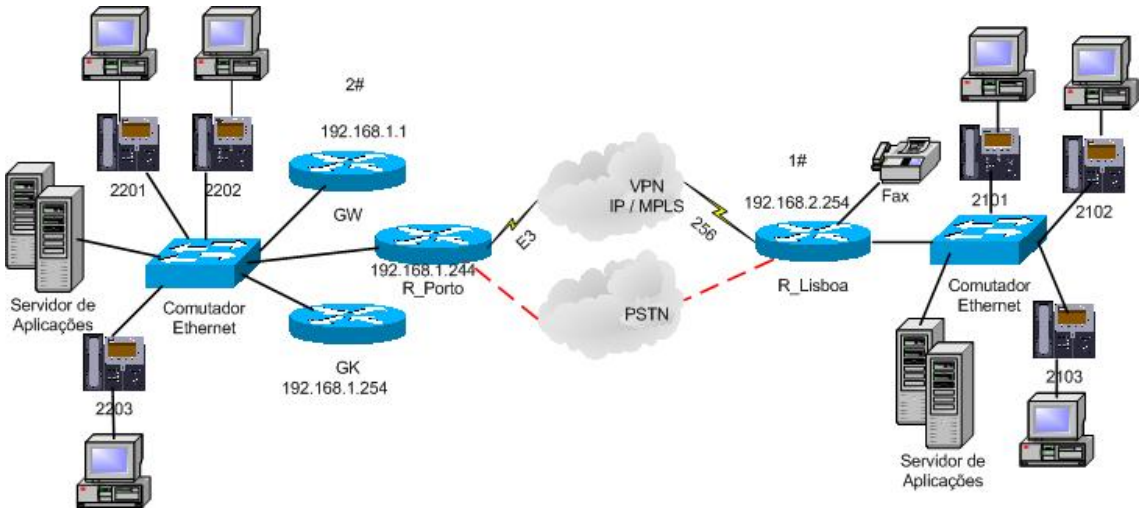

Figura 5.1 – Cenário Típico de uma Solução VoIP

5.1. *Backbone* IP/MLPS

A interligação dos sítios Porto e Lisboa é feita através da criação de uma VPN IP MPLS com suporte de ligação de dados e voz (voz IP corporativa). Este tipo de infra-estrutura reúne os requisitos de qualidade de serviço e fiabilidade capazes de suportar voz. Com este tipo de ligação consegue-se simplificar a gestão da infra-estruturas de comunicações, aumentado consideravelmente a largura de banda disponível e ainda reduzindo os custos de exploração do aluguer de circuitos. Este tipo de soluções é apresentado pelos operadores de telecomunicações em Portugal.

5.2. Características dos acessos

No Porto para ligação principal foi utilizado um circuito de ligação digital E3 que liga via ATM ao PoP (*Point of Presence*) do operador. Em redundância poderíamos optar por uma ligação de Feixe Hertzianos de igual capacidade. O suporte físico é efectuado em fibra óptica

Em Lisboa a largura de banda contratada é 256 Mbps, o transporte IP até ao PoP do operador é suportado em *Frame Relay*. Fisicamente a ligação é suportada sobre o circuito 256 Mbps.

A ligação à rede pública, para locais onde se utilize o CME (*Call Manager Express*), é feita através de dois acessos básicos RDIS que ligam directamente no router. Para locais onde possam existir centrais telefónicas os acessos ligam directamente às centrais PPCA.

5.3. *Routers* Multiserviço

No porto foi utilizado o *router* (R_Porto) 3725 da Cisco que garante a convergência de voz e dados. Estes *routers* asseguram os seguintes serviços:

- Encaminhamento IP
- Qualidade de Serviço IP
- Processamento de Voz
- Encaminhamento de chamadas de voz

Em termos de hardware o *router* suporta as seguintes interfaces:

- Duas interfaces *fast ethernet* para ligação à rede local de dados.
- uma interface série E3 para ligação à VPN IP MPLS

Em Lisboa (R_Lisboa) o *router* utilizado é o 2611XM, suporta até 48 utilizadores.

Em termos de hardware suporta as seguintes interfaces:

- duas interface fast ethernet para ligação à rede local;
- Duas ISDN BRI para ligação de 4 canais de voz à rede pública telefónica
- uma interface FXS para ligação do Fax
- Uma interface serial X.21 DTE para interligação ao PoP do operador.

5.4. Componentes de Telefonia IP

As componentes de telefonia IP utilizadas neste cenário são:

- Comutadores *Ethernet*
- Call Manager Express
- *Gateway* (GW) para possíveis PBX existentes e a ligação PSTN
- *GateKeeper* (GK) H.323
- Telefones IP

Durante a fase de implementação desta tecnologia é comum a existência de soluções mistas de telefonia, onde existam os telefones IP e as centrais telefónicas convencionais com os respectivos telefones.

5.4.1. Comutadores *Ethernet*

Os comutadores *ethernet* (*Switchs*) utilizados são os modelos 3500 ou 2950 da Cisco, tendo os primeiros funcionalidades de *inline power*, permitindo a alimentação dos telefones através do cabo *ethernet*. Estes equipamentos suportam a norma 802.1p de forma a prioritizar o tráfego de voz em detrimento do restante tráfego na rede *ethernet*.

5.4.2. Call Manager Express

Trata-se de um componente de software, instalada nos equipamentos *routers*. O CME tem como missão gerir procedimentos relacionados com o estabelecimento de chamadas e registo

de telefones. Para isso utiliza um protocolo de sinalização proprietário da Cisco, designado por *Skinny Client Control Protocol* (SCCP), cujas mensagens são transportadas sobre o TCP e utiliza o porto 2000.

O CME introduz dois conceitos:

- **Ephone** – representação de um telefone IP
- **Epheone-dn** – representação de uma extensão telefónica

Exemplificando:

```
ephone  1
 mac-address 000C.85BE.68BF
 type 7940
 button  1:1 2:2
!
ephone  2
 mac-address 000C.CE3A.754E
 type 7940
 button  1:3 2:4
!
ephone  3
 mac-address 000C.CE35.22FE
 type 7940
 button  1:5 2:6
!
ephone-dn  4
 number 2201
 name Paulo Sérgio
 call-forward busy 2200
 call-forward noan 2200 timeout 15
 application app_h450_transfer
!
ephone-dn  5
 number 2202
 name Paulo Terra
 call-forward busy 2200
 call-forward noan 2200 timeout 15
 application app_h450_transfer
```

5.4.3. *Gateway* de VoIP

OS *gateways* são configurados com base em *routers* multiserviços (*router* Cisco Modelo 3745 com uma interface *ethernet* e uma interface série E1). Estes equipamentos desempenham funções de *gateways* e a de gestores de telefonia com base no software CME. Os *gateways* convertem chamadas telefónicas IP em chamadas telefónicas analógicas e vice-versa. Nesta função são utilizadas as ligações E1 entre o *router* e a central.

5.4.4. Gatekeepers H.323

Os *gatekeeper* são também configurados com base nos *routers* Cisco (*router* Cisco Modelo 2620XM ENTERPRISE PLUS H.323 com uma interface *fast ethernet*).
Esta *feature* tem como principais benefícios a optimização e simplificação da rede de voz corporativa (VoIP). Assim, consegue-se de uma forma centralizada gerir e efectuar a autorização das chamadas de voz.

5.4.5. Telefones IP

São utilizados os telefones da Cisco modelo 7940, equipados com dois botões de linhas/recursos programáveis que permitem efectuar até quatro chamadas simultâneas. Possui também um *display* de cristais líquidos baseado em *pixels*. O *display* possui recursos como data e hora, nome e número do chamador.
Este telefone, tem ainda um comutador *ethernet* de duas portas, que permite a conexão directa com a rede local *ethernet* através uma interface RJ-45 com uma única conectividade para o telefone e o PC de um mesmo local. Estes telefones podem ainda ser auto alimentados pelos

comutadores *ethernet* (modelo da cisco *Catalyst 3500 inline power*), ou então com o uso de um transformador de corrente AC.

Para além das componentes de *hardware* são utilizadas configurações ao nível do sistema operativo (IOS) instalados nos *routers*. A versão recomendada para suportar estas funcionalidades é a versão 12.2.
Configurações para:

- Processamento de voz
  - Codificação (e descodificação) feita por CODECs G.729r8
  - Compressão (e descompressão) realizada de acordo com o CODEC G.729 permite reduzir a ocupação de uma chamada para os 26Kbps
  - Marcação do campo TOS (*Type Of Service*) dos pacotes IP relativos ao Tráfego de voz com IP *precedence critical*.

- Qualidade de serviço – a marcação do campo TOS é imprescindível para a implementação de qualidade de serviço. Tendo em conta que é necessário eliminar as perdas e atrasos dos pacotes pertencentes ao tráfego de voz, é usado um mecanismo de prioritização de tráfego designado por Low Latency Queueing (LLQ). O tráfego é classificado de acordo com critérios previamente definidos e associados as filas de saída. A cada fila é atribuída uma determinada prioridade.

- Sinalização – é utilizado o protocolo de sinalização Q.931 e Q.SIG, o qual é responsável pelas funcionalidades básicas de telefonia (realização de chamadas). Este protocolo de sinalização, permite a interligação com as centrais telefónicas convencionais.

- Encaminhamento de chamadas – nos *routers* são definidas rotas que, de acordo com o plano de numeração da rede telefónica, determinam o correcto encaminhamento das chamadas entre os diversos sítios.

5.5. Comando de Configuração IOS

Aqui são apresentados alguns exemplos de configurações com base em comandos dos sistemas operativos (IOS) dos *routers*. Assume-se que o utilizador está familiarizado com as configurações nos *routers*. Caso não esteja aconselha-se a leitura da documentação Cisco que normalmente acompanha os equipamentos.

5.5.1. Configuração do comutador *Ethernet*

No caso de Lisboa, podem ser configurados duas VLANs, uma para voz VLAN 10 e uma para dados VLAN 1.
A configuração do comutador *ethernet* poderia ser a seguinte:

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW_Lisboa
!
```

Configuração WRR (*Weighted Round Robin*) do COS ao nível dos acessos

```
wrr-queue bandwidth 20 1 80 0
wrr-queue cos-map 1 0 1 2 4
wrr-queue cos-map 3 3 6 7
wrr-queue cos-map 4 5
ip subnet-zero
!
```

```
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 switchport mode trunk
 switchport voice vlan 10
 mls qos trust device cisco-phone
 mls qos trust cos
 spanning-tree portfast trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode trunk
 switchport voice vlan 10
 mls qos trust device cisco-phone
 mls qos trust cos
 spanning-tree portfast trunk
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode trunk
 switchport voice vlan 10
 mls qos trust device cisco-phone
 mls qos trust cos

…

interface FastEthernet0/24
 description Ligacao Router
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan1
 ip address 192.168.2.125 255.255.255.128
 no ip route-cache
```

5.5.2. Configuração do *Router*

A configuração para o *router* de Lisboa pode ser a seguinte:

```
version 12.2
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_Lisboa
!
tdm clock bri-auto
ip subnet-zero
!
!
```

Exclusão de endereços de DHCP

```
no ip domain lookup
ip dhcp excluded-address 192.168.2.125
ip dhcp excluded-address 192.168.2.126
```

```
ip dhcp excluded-address 192.168.2.254
!
```

Configuração de endereços DHCP para a rede de dados

```
ip dhcp pool IP_dados
  network 192.168.2.0 255.255.255.128
  default-router 192.168.2.126
!
```

Configuração de endereços DHCP para a rede de voz

```
ip dhcp pool IP_voz
  network 192.168.2.128 255.255.255.128
  default-router 192.168.2.254
  option 150 ip 192.168.2.254
!
```

Para performance de compressão RTP (*Cisco Express Forwarding*), utilizado nas versões anterior de IOS.

```
ip cef
!
```

Definição do tipo de protocolo de sinalização Q.931

```
isdn switch-type basic-net3
isdn voice-call-failure 0
!
voice call send-alert
voice call carrier capacity active
voice rtp send-recv
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
```

Classificação dos pacotes de Voz

```
 class-map match-any VoIP
  description VoIP
  match protocol rtp
  match access-group 101
!
!
 policy-map qos
  class VoIP
   priority 100
  class class-default
   fair-queue
!
```

Correspondência das linhas externas com as respectivas extensões.

```
translation-rule 1
 Rule 1 ^1 2101
 Rule 2 ^2 2102
 Rule 3 ^3 2103
!
```

Definição da *Gateway* de Voz e configuração do *call Admission Control*

```
interface Loopback0
 ip address 172.16.45.254 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id lisboagw ipaddr 192.168.1.254 1718
 h323-gateway voip h323-id lisboagw
 h323-gateway voip tech-prefix 1#
 h323-gateway voip bind srcaddr 172.16.45.254
```

```
!
interface FastEthernet0/0
 no ip address
 speed auto
 no cdp enable
!
interface FastEthernet0/0.1
 description VLAN DADOS
 encapsulation dot1Q 1 native
 ip address 192.168.2.126 255.255.255.128
 no cdp enable
!
interface FastEthernet0/0.10
 description VLAN VOZ
 encapsulation dot1Q 10
 ip address 192.168.2.254 255.255.255.128
 no cdp enable
!
interface Serial0/0
 bandwidth 256
 no ip address
 ip nbar protocol-discovery
 encapsulation frame-relay IETF
 load-interval 30
 frame-relay traffic-shaping
!
interface Serial0/0.17 point-to-point
 ip address 10.16.11.230 255.255.255.252
 frame-relay interface-dlci 17
  class class_dlci_17
!
interface Serial0/0.1001 point-to-point
 ip address 172.31.247.252 255.255.255.0
 frame-relay interface-dlci 1001
!
interface BRI1/0
 no ip address
 isdn switch-type basic-net3
!
interface BRI2/0
 description RDIS N 21331111-9
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
 isdn send-alerting
 isdn sending-complete
 isdn static-tei 0
!
interface BRI2/1
 description RDIS N 21331111-9
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
 isdn send-alerting
 isdn sending-complete
 isdn static-tei 0
!
router rip
 version 2
 timers basic 15 30 45 35
```

```
 network 192.168.0.0
 network 10.16.0.0
 no auto-summary
!
!
map-class frame-relay class_dlci_17
 frame-relay cir 256000
 frame-relay bc 2560
 frame-relay be 0
 frame-relay mincir 256000
 frame-relay fair-queue
 frame-relay fragment 128
```

Configuração IP RTP Priority *starting-rtp-port-number port-number-range bandwith*

```
 frame-relay ip rtp priority 16384 16383 75
access-list 101 permit ip any any precedence critical
access-list 101 permit ip any any dscp ef
access-list 101 permit tcp any any range 1718 1720
!
voice-port 2/0
 translate called 1
 compand-type a-law
 cptone PT
!
voice-port 2/1
 translate called 1
 compand-type a-law
 cptone PT
!
voice-port 3/0
 cptone PT
!
voice-port 3/1
 cptone PT
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 91 pots
 destination-pattern 2101
 port 3/1
 no register e164
!
dial-peer voice 330 voip
 application app_h450_transfer
 max-conn 2
 destination-pattern 213...
 session target ras
 no vad
!
dial-peer voice 310 voip
 application app_h450_transfer
 max-conn 2
 destination-pattern 21..
 session target ras
 no vad
!
dial-peer voice 300 voip
```

```
 application app_h450_transfer
 destination-pattern 22..
 session target ras
 no vad
!
dial-peer voice 1 pots
 application app_h450_transfer
 destination-pattern 02.......
 progress_ind alert enable 8
 progress_ind progress enable 8
 progress_ind progress enable 8
 progress_ind connect enable 8
 direct-inward-dial
 port 2/0
 prefix 2
 no register e164
!
dial-peer voice 2 pots
 application app_h450_transfer
 destination-pattern 02.......
 progress_ind alert enable 8
 progress_ind progress enable 8
 progress_ind connect enable 8
 direct-inward-dial
 port 2/1
 prefix 2
 no register e164
!
dial-peer voice 3 pots
 application app_h450_transfer
 destination-pattern 01T
 progress_ind alert enable 8
 progress_ind progress enable 8
 progress_ind connect enable 8
 direct-inward-dial
 port 2/0
 prefix 1
 no register e164
!
gateway
 emulate cisco h323 bandwidth
!
 max-ephones 24
 max-dn 48
ip source-address 192.168.2.254 port 2000
 application app_h450_transfer
 transfer-pattern 22..
 transfer-pattern 21..
 transfer-pattern 0.........
 moh music-on-hold.au
 time-format 24
 date-format dd-mm-yy
dn-webedit
 time-webedit
 transfer-system full-consult
!
!
ephone-dn  1
 number 2101
 name Paulo
```

```
 call-forward busy 2102
 call-forward noan 2102 timeout 15
 application app_h450_transfer
!
!
ephone-dn  2
 number Sergio
 name RecepcaoL2
 call-forward busy 2101
 call-forward noan 2101 timeout 15
 application app_h450_transfer
!
!
ephone-dn  3
 number 2103
 name Terra
 call-forward busy 2101
 call-forward noan 2101 timeout 15
 application app_h450_transfer
!
!
ephone  1
 mac-address 000C.85BE.68BF
 type 7940
 button  1:1 2:2
 !
ephone  2
 mac-address 000C.CE3A.754E
 type 7940
 button  1:3 2:4
 !
ephone  3
 mac-address 000C.CE35.22FE
 type 7940
 button  1:5 2:6
 !
```

5.5.3. Configuração da Placa FXS

As placas FXS são utilizadas para interligar equipamentos analógicos aos *routers* como por exemplo, os faxes. Esta placas são instaladas nos *slots* de expansão do *routers* permitindo a ligação dos equipamentos.
Todos os parâmetros de configuração têm valores por defeito, estes valores são adequados para a maioria das situações.

Os seguintes comandos são obrigatórios na configuração de uma placa FXS:

- Signal type
- Call progress tone
- Ring frequency
- Ring number
- PLAR connection mode
- Music threshold
- Description
- VAD
- Comfort noise

Siga estes passos para a configuração de uma placa FXS:

1. Entre no modo privilegiado:

router>**enable**

2. Entre no modo de configuração global:

   router#**configure terminal**

3. Identifique qual os *slots* a configurar válidos para os modelos de *routers* 2600 e 3600:

   router(config)#**voice-port** *nm-module/vic-module/port-number*
   router(config)#**voice-port** *slot/port* (Cisco 175x/1760 and MC3810)

5. Seleccione o sinal apropriado para iniciar a chamada:

   router(config-voiceport)#**signal** *[loop-start|ground-start]*

6. Seleccione o código do país apropriado, por defeito está *northamerica*:

   router(config-voiceport)#**cptone** *country-code*

7. Configure o tipo de conexão para a porta de voz. Se a conexão for com um PBX, use a opção ***tie-line***. Se a conexão for *Private line Automatic Ring Down* (PLAR), use a opção **plar.** Se a conexão for PLAR *off-premises extension,* use a opção *plar-opx*.

   router(config-voiceport)#**connection** *{tie-line* **|** *plar* **|** *plar-opx} string*

   String . representa o número de telephone de destino

   Plar – *Private line automatic ringdown*, usado para ligar automaticamente ao uma atributo destino, bastando levantar o auscultador. Não sendo necessário as marcação de qualquer digito para estabelecer a ligação.

   Tie-line – específica que o porto é uma conexão dedicada ao PBX.

   Plar-opx – PLAR *off-premises extension,* utilizando esta opção, o porto de voz local fornece a resposta antes do porto remoto receber a resposta. Este método garante que a chamada é atendida antes que o fluxo da chamada seja completado.

8. Configurar a frequência em Hertz do sistema que se encontra ligado ao router:

   router(config-voiceport)#**ring frequency** *[25| 50]*
   router(config-voiceport)#**ring frequency** *[20| 30] (*Cisco MC3810router)

9. Configurar o número máximo de toques antes de atender a chamada:

   router(config-voiceport)#**ring number** *number*

10. Especificar um tipo diferente de toque, ou então definir um novo: Cada atributo especifica um tempo para o toque e o intervalo de tempo entre cada toque:

    router(config-voiceport)#**ring cadence** {[*pattern01* | *pattern02* | *pattern03* | *pattern04* | *pattern05* | *pattern06* | *pattern07* | *pattern08* | *pattern09* | *pattern10* | *pattern11* | *pattern12*] | [*define pulse Interval*]}

12. Especifica a impedância, de acordo com especificações do PBX:

    router(config-voiceport)#**impedance** *[600c|600r|900c|complex1|complex2]*

13. Configura os limites em decibéis para a música em espera:

    router(config-voiceport)#**music-threshold** *number*

14. Comando Opcional: Configura uma descrição para a :

    router(config-voiceport)#**description** *string*

15. Configura um barulho de fundo de conforto para quando não existe qualquer ruído:

    router(config-voiceport)#**comfort-noise**

16. Comando Opcional: Activa o voice activity detection (VAD):

    router(config-voiceport)#**vad**

    vad- *Voice activity detection* é um algoritmo que detecta o silêncio, característica de uma conversação com dois sentidos, suprimindo a transmissão de pacotes com informação dentro deles.

5.5.4. Configuração Q.931

O Q.931 é usado para configurar a sinalização num circuito ISDN. Este processo ocorre no nível da camada de rede da pilha protocolar. Os passos para configurar uma interface ISDN PRI com Q.931 são os seguintes:

1. Seleccionar o tipo de serviços de comutação ISDN PRI:

   router(config)#**isdn switch-type primary-net3**

2. Configurar o controlador ISDN T1/E1:

   router(config)#**controller {T1 | E1}** *slot/port*
   router(config-controller)#**pri-group timeslots** *range*

3. Sair do modo de configuração do controlador T1/E1:

   router(config-controller)#**exit**

4. Configurar o canal D da interface ISDN:

   router(config)#**interface serial0/0:***n*

5. Configurar o protocolo ISDN como *slave* ou *master*:

   router(config)#**isdn protocol-emulate** *{network | user}*

6. Activar ou desactivar a corrente fornecida pelo NT RDIS:

   router(config-if)#**[no] line-power**

7. Permitir a receber chamadas de voz:

   router(config-if)#**isdn incoming-voice voice**

5.5.5. Configuração Q.SIG

A configuração do protocolo Q.SIG com os *routers* Cisco permite conectividade com as centrais telefónicas convencionais PBXs. O Q.SIG é baseado nos *standards* Q.921 e Q.931, permitindo a aceitação de chamadas de outras localizações (Europa e Estados Unidos).
OS comandos usados para a configuração do QSIG num circuito ISDN são:

1. Configurar o protocolo QSIG no modo de configuração global:

router(config)#**isdn switch-type primary-qsig**

2. No canal D do interface ISDN (por exemplo, o interface serial0:23) configure o seguinte comando:

   router(config-if)#**isdn protocol-emulate** {*user* | *network*}

5.5.6. Configurar um *Gateway* H.323

Para configurar um *gateway* básico H.323, necessitamos de activar as funcionalidades do *gateway* de VoIP. Fazemos isto, utilizando o comando gateway. Para activar essa funcionalidade, usamos os seguintes comandos:

1. Entrar no modo Global de configuração:

   Router#**configure terminal**

2. Activar a gateway de VoIP:

   Router(config)#**gateway**

3. Sair do modo de configuração:

   Router(config-gateway)#**exit**

O próximo passo na configuração do *gateway* é configurar os parâmetros da interface. Primeiro definimos qual o interface que será apresentado à rede VoIP. Na rede deverá apenas existir uma interface designado como interface *gateway* H.323.
Depois de definida a interface, configuramos o *gateway* para descobrir o *gatekeeper*, ou por *multicast* ou por designação de um *host* específico.
Finalmente, configuramos o número de identificação do *gateway* e os prefixos que o *gateway* deve registar no *gatekeeper*.
Neste exemplo consideramos que os endereços para o *gateway* e para o *gatekeeper* seriam 192.168.1.1 e 192.168.1.254, respectivamente.

1. Entrar no modo de configuração da interface:

   router(config)#**interface ethernet 1/0**

2. Configurar o IP para a interface assim como a máscara de sub-rede:

   router(config-if)#**ip address 192.168.1.1 255.255.255.0**

3. Designar a interface como *gateway* H.323:

   router(config-if)#**h323-gateway voip interface**

4. Especificar o nome para a *gatewa*y associada à interface. A interface usa a identificação (ID) quando comunica com o *gatekeeper*:

   router(config-if)#**h323-gateway voip h323-id interface-id**

5. Especificar o nome do *gatekeeper* associado a este *gateway* e como o *gateway* pode encontra-lo. A identificação do gatekeeper deve ser exactamente a mesma que se encontra configurada no *gatekeeper*.

   router(config-if)#**h323-gateway voip id Portogk 192.168.1.254 1719**

6. Definir o nome H.323 para o *gateway*, identificado este *gateway* ao *gatekeeper* associado.

router(config-if)#**h323-gateway voip h323-id Portogw@exemplo.com**

5.5.7. Configurar um *Gatekeeper* H.323

Configurar um *router* Cisco com funcionalidades de *gatekeeper* envolve o registo de uma zona de influência.

1. Entrar no modo de configuração global:

   router#**configure terminal**

2. Activar a funcionalidade de *gatekeeper* no router:

   router(config)#**gatekeeper**

3. Especificar a zona controlada pelo *gatekeeper*:

   router(config-gk)#**zone local *portogk exemplo.com 192.168.1.254***

4. Configurar o gatekeeper para conhecimento dos seus prefixos ou dos prefixos remotos:

   router(config-gk)#**zone prefix portogk@exemplo.com 22 . . . . . .**

   interface FastEthernet0/0
   ip address 192.168.1.254 255.255.255.0
   speed 100
   full-duplex
   gatekeeper
   zone local gk exemplo.com 192.168.1.254
   zone local portogw exemplo.com
   zone local lisboagw exemplo.com
   zone prefix gk 22.. gw-priority 10 portogw
   zone prefix lisboagw 21.. gw-priority 10 lisboagw
   bandwidth interzone zone lisboagw 256

5.6. Exemplos de Configuração QoS em VoIP

No capítulo 4 vimos alguns dos principais mecanismos de qualidade de serviço, chegou a altura de implementar alguns desses métodos.

5.6.1. Configurar a Compressão RTP

O seguinte exemplo ilustra o encapsulamento *Frame Relay* encapsulation activando a compressão do cabeçalho RTP:

```
interface serial 0
ip address 1.0.0.2 255.0.0.0
encapsulation frame-relay
no keepalive
frame-relay map ip 1.0.0.1 17 broadcast rtp header-compression
```

Este comando apenas actua no mapeamento especificado. O número 17 representa o DLCI.

5.6.2. Configurar o Custom Queuing

Para configurar o *costum queuing* são necessários os seguintes passos:

- Definir uma lista de *custom queue.*
- Fazer corresponder a lista a um interface.

Uma das tarefas mais importantes é a definição da prioridade da lista, porque é neste ponto que é determinada a classificação de pacotes.

```
Router1#configure terminal
Router1(config)#queue-list 1 queue 1 ?
Router1(config)#queue-list 1 queue 1 byte-count ?
\\<0-16777215> size in bytes
Router1(config)#queue-list 1 queue 1 byte-count 3000
Router1(config)#queue-list 1 queue 2 byte-count 3000
Router1(config)#queue-list 1 queue 3 byte-count 3000
Router1(config)#queue-list 1 queue 3 limit ?
\\<0-32767> number of queue entries
Router1(config)#queue-list 1 queue 4 limit 60
Router1(config)#queue-list 1 queue 5 limit 60
Router1(config)#queue-list 1 queue 6 limit 60
Router1(config)#end
Router1#
```

Uma vez configurada a lista de *custom queueing*, o segundo passo é associar a lista a uma interface. Neste exemplo, a lista é aplicada à interface série 0/0.

```
Router1#configure terminal
Router1(config)#interface serial 0/0
Router1(config-if)#custom-queue-list 1
Router1(config-if)#end
Router1#
```

5.6.3. Configurar Priority Queuing

Os passos para a configuração do *priority queuing* são:

- Definir a *priority list.*
- Aplicar a lista a uma interface

Definir a fila prioritária.

```
router1(config)#priority-list ?
\\<1-16> Priority list number
Router1(config)#priority-list 1 ?
Router1#configure terminal
Router1(config)#priority-list 1 protocol appletalk high
Router1(config)#priority-list 1 interface ethernet 0/0 medium
Router1(config)#priority-list 1 protocol ip normal
Router1(config)#priority-list 1 default low
Router1(config)#end
Router1#
```

Configuração dos limites da fila

```
Router1#configure terminal
\\Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#priority-list 4 queue-limit ?
\\<0-32767> High limit
Router1(config)#priority-list 4 queue-limit 200 ?
```

\\<0-32767> Medium limit
Router1(config)#**priority-list 4 queue-limit 200 400 ?**
\\<0-32767> Normal limit
Router1(config)#**priority-list 4 queue-limit 200 400 600 ?**
\\<0-32767> Lower limit
Router1(config)#**priority-list 4 queue-limit 200 400 600 800**
Router1(config)#**end**
Router1#

Aplicar a lista prioritária a uma interface.

Router1#**configure terminal**
Router1(config)#**interface serial 0/0**
Router1(config-if)#**priority-group 1**
Router1(config-if)#**exit**
Router1(config-if)#**end**
Router1#

5.6.4. Configurar o Weight Fair Queuing

Activar o *Weight Fair Queuing* a uma interface

Router1#**configure terminal**
Router1(config)#**interface serial 0/0**
Router1(config-if)#**fair-queue 512 1048 10**
\\Number of dynamic queues must be a power of 2 (16, 32, 64, 128,256, 512, 1024)
Router1(config-if)#**fair-queue 512 1024 10**
Router1(config-if)#**end**
Router1#

5.6.5. Configurar o Class-Based Weight Fair Queuing

Antes de iniciar a configuração do CBWFQ, primeiro temos que determinar quantas classes são necessárias para caracterizar todo o tráfego. Também temos que conhecer os critérios que vamos usar para mapear o tráfego nas classes e a largura de banda a atribuir a cada classe. Existem três passos para a configuração CBWFQ:

1. Definir as classes – determina qual o tráfego atribuído a cada classe
2. Criar politica de mapeamento – determina a forma como o tráfego é manipulado.
3. Aplicar as politicas às interfaces – nenhuma politica QoS é activada até que seja atribuída a uma interface.

Definir as classes.

router1#**config terminal**
router1(config)#**class-map Gold**
router1(config-cmap)#**match access-group name Gold**
router1(config)#**ip access-list extended Gold**
router1(config-ext-nacl)#**permit ip any any precedence flash-override**

A tabela 5.1 mostra os níveis de precedência IP e os nomes associados.

Precedência IP	Nome
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash-override
5	Critical
6	Internet

7	Network

Tabela 5.1 – Níveis de Precedência IP

```
router1(config)#class-map Silver
router1(config-cmap)#match access-group name Silver
router1(config-cmap)#class-map Bronze
router1(config-cmap)#match access-group name Bronze
router1(config-ext-nacl)#ip access-list extended Silver
router1(config-ext-nacl)#permit ip any any precedence flash
router1(config)#ip access-list extended Bronze
router1(config-ext-nacl)#permit ip any any precedence immediate
```

Criar Politicas

Agora que foram definidas as classes, podemos avançar para o segundo passo, criar as politicas de mapeamento.

```
router1(config)#policy-map PPP-T1
router1(config-pmap)#class Gold
router1(config-pmap-c)#bandwidth 216
```

Com o comando *config-pma-c* podem ser utilizados os seguintes parâmetros:

- **Bandwith** – largura de banda (em Kbps ou em percentagem)
- **Queue-limit** – Tamanho máximo para a fila para *tail drop*
- **Random-detect** – Activa o WRED com politica de descarte de pacotes

```
router1(config)#policy-map PPP-T1
router1(config-pmap)#class class-default
router1(config-pmap-c)#bandwidth 31
```

Aplicar as politicas às interfaces

```
router1(config)#interface serial 0/0
router1(config-if)#service-policy output PPP-T1
```

5.6.6. Configurar a Classificação de Pacotes

A Classificação de pacotes pode ser executada de variadas maneiras. Os dois métodos abordados foram a precedência IP e a *Policy-Based Routing* (PBR).

A precedência IP, numa implementação VoIP, é normalmente configurada no ponto de chamada.

```
Router1(config-dial-peer)#ip precedence precedence
Router1(config)#dial-peer voice 1 voip
Router1(config-dial-peer)#ip precedence 6
```

A configuração do PBR é feita do seguinte modo:

```
route-map map-name [permit | deny] sequence-number
match length min max
match ip address [access-list-number | name]
set ip precedence [number | name]
set ip next-hop ip-address
set interface interface-type interface-number
set ip default next-hop ip-address
set default interface interface-type interface-number
interface interface-type interface-number
ip policy route-map map-name
```

5.6.7. Configuração do RSVP

Com o RSVP configuramos a largura de banda disponível e o valor máximo reservado para cada conexão indivudual.

```
interface interface-type interface-number
bandwidth bandwidth
ip rsvp bandwidth available-bandwidth max-bandwidth
```

5.6.8. Call Admission Control

A configuração do *Call Admission Control* pode ser a implementada com os seguintes comandos:

```
ip address 172.16.45.254 255.255.255.255
h323-gateway voip interface
h323-gateway voip id lisboagw ipaddr 192.168.1.254 1718
h323-gateway voip h323-id lisboagw
h323-gateway voip tech-prefix 1#
h323-gateway voip bind srcaddr 172.16.45.254
!
voice-port 0/0/0
!
voice-port 0/0/1
!
dial-peer voice 1 voip
destination pattern ….
session target ras
!
dial-peer voice 2 pots
destination pattern 1001
port 0/0/0
!
dial-peer voice 3 pots
destination pattern 1002
port 0/0/1
!
Gateway
```

5.6.9. Configuração de Traffing Shapping

O FRTS e o GTS usam métodos similares para manter as taxas de transferência durante os períodos de *buffering* de tráfego. A tabela 5.2 Ilustra os parâmetros do *traffic Shapping*.

Termo FTRS	Termo GTS	Descrição
CIR	Bit Rate	*Committed Information Rate*: a taxa de transferência media enviada por uma interface de saída
Bc	Burst size	Committed Brust; Número de *bits* transmitidos num período de tempo específico Tc
Be	Excess burst size	Excess Brust; Número de bits que podem ser transmitidos durante o primeiro intervalo de uma transmissão depois de um período de não transmissão
Mincir	N/A	Taxa de transferência mínimos durante os períodos de congestionamento.
Tc	Tc	Intervalo de tempo igual ao Bc/CIR

Tabela 5.2 – Terminologia Traffic-Shapping

Router1 (config)#**interface s1/0**

```
Router1 (config–if)#encapsulation frame-relay
Router1 (config–if)#frame-relay traffic-shaping
Router1 (config)#interface s1/0.100 point-to-point
Router1 (config–if)#ip address 10.10.10.101 255.255.255.252
Router1 (config–if)#frame-relay traffic-rate 128000 144000
Router1 (config–if)#frame-relay adaptive-shaping becn
Router1 (config–if)#frame-relay mincir 32000
Router1 (config–if)#frame-relay interface-dlci 100
```

5.6.10. Configuração do WRED para evitar congestionamentos

Os comandos para configurar o WRED são:

```
random-detect
random-detect precedence precedence min-threshold max-threshold mark-prob-denominator
random-detect exponential-weighting-constant weighting-factor
```

A tabela 5.3 ilustra os parâmetros que podem ser utilizados na configuração WRED.

Precedência IP	Min-threshold	Max-threshold	MPD
0	20	40	10
1	22	40	10
2	24	40	10
3	26	40	10
4	28	40	10
5	31	40	10
6	33	40	10
7	35	40	10
RSVP	37	40	10

Tabela 5.3 – Valores por Defeito nos Parâmetros WRED

5.6.11. Configuração do Link Fragmentation e Interleaving

Exemplo da configuração do LFI a um interface,

```
router1(config)#interface Multilink 1
router1(config-if)#ip address 10.10.10.101 255.255.255.252
router1(config-if)#ppp multilink interleave
router1(config-if)#fair-queue
router1(config-if)#ppp multilink fragment-delay 20

router1(config)#interface s1/0
router1(config-if)#ppp multilink
router1(config-if)#multilink-group 1
```

6. Conclusões

O mercado da telefonia IP tem muitos caminhos disponíveis para o seu crescimento. Ao longo deste trabalho, vimos algumas considerações básicas para esses caminhos. Contudo, teremos que ter alguns cuidados, pois existem algumas limitações.

Um bom ponto de partida para sua implementação, será substituir as linhas dedicadas de voz. Esta alteração deve ser gradual, as soluções de voz convencional e as soluções de telefonia IP podem coexistir.
Devem também ser efectuados estudos no sentido de determinar qual o tipo de sistema de comunicações e equipamentos a adoptar, dependendo do tipo de funcionalidades e localização da organização.

Factores como:

- capacidade disponível;
- crescimento da companhia ;
- custo com telefones adicionais;
- custos com o *upgrade* ;
- custos de manutenção e suporte anuais

podem incorrer em custos adicionais, quando estiver a alterar os sistemas de comunicações convencionais.
Para o utilizador final estas alterações na rede são completamente transparentes, provando a maturidade da tecnologia.

A realização de chamadas telefónicas, o transporte de dados e a sinalização só são possíveis devido à existência de protocolos como H.323 e SIP. Estes protocolos disponibilizam um conjunto de funcionalidades que nos permitem a interoperabilidade entre os diferentes equipamentos que constituem a rede.
A interoperabilidade de soluções de diferentes fabricantes constitui ainda um obstáculo que, urge ultrapassar.

A qualidade de serviço é de uma importância vital, pois só assim, conseguimos a implementação de redes convergentes e com elevado nível de desempenho. Este desempenho só é possível se forem aplicadas as técnicas, classe/qualidade de serviço, ajustadas às funcionalidades da rede. É importante relembrar que estas funcionalidades dependem do tipo de equipamento e das versões de software utilizado.

A grande vantagem na implementação de uma solução de telefonia IP, para além da redução dos custos, é a possibilidade de integração com outros serviços, como por exemplo, o correio electrónico através de soluções de *Unified Messaging*.

7. Referências Bibliográficas

1. UyLess Black, Voice Over IP, Prentice Hall
2. Walter J. Goralski & Matthew C. Kolon; IP Telephony, McGrawHill
3. Kevin Brown , IP Telephony Unveiled Cisco Press
4. Cisco, Call Manager Express 3.0 Systems Administrator Guide
5. Edmundo Monteiro, Fernando Boavida, Engenharia de redes Informáticas, 4ª Edição, FCA Editora
6. Charles Riley, Best Damn Cisco Internetworking, Syngress
7. Martin Walshaw, Design and Deploy IP Telephony Solutions, Syngress
8. Cisco, Cisco IP Telephony Network Design Guide, Cisco Press
9. Cisco, Cisco IP Telephony QoS Design Guide
10. Cisco, Cisco VoIP Over Frame Relay, ATM and IP; Student Guide, Cisco Press
11. Configuring Voice over IP for the Cisco 3600 Series
    Http://www.cisco.com
12. QoS for Voice Over IP Solutions Guide
    Http://www.cisco.com
13. Configure Cisco IP Phone Support
    Http://www.cisco.com
14. Quality of Service for Voice Over IP
    Http://www.cisco.com