Mestrado em Engenharia Informática
Dissertação
Relatório Final

# Segurança, Privacidade, QoS e QoE em Plataformas VoIP

Hugo Tiago dos Santos Fonseca
hfonseca@student.dei.uc.pt

Orientador:
Paulo Simões
Data: 2 de Setembro de 2014



FCTUC DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

# Resumo

A evolução tecnológica permitiu o crescimento de aplicações e serviços baseados no Protocolo da Internet, levando ao surgimento de novas formas de comunicação que antes eram inimagináveis. Estas comunicações realizam-se normalmente em ambientes de rede partilhada, como a Internet, conduzindo a preocupações ao nível da segurança e da garantia de Qualidade de Serviço e de Qualidade de Experiência. Para além destas questões, o surgimento de novos modelos de negócio ameaça muitos provedores de serviço, que por sua vez se tentam defender implementando técnicas de estrangulamento de tráfego nas suas redes. O estrangulamento de tráfego, habitualmente designada por *traffic shaping*, leva à degradação intencional das comunicações de voz, que por si só já são bastante sensíveis às restrições da rede, acrescendo a necessidade de níveis adequados de privacidade.

Esta dissertação apresenta as melhorias e modificações realizadas na Plataforma Nubitalk, mais concretamente ao nível do reforço da segurança e privacidade e do suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência. Após a identificação de vulnerabilidades da plataforma, foram propostas várias soluções de modo a lidar com cada um dos pontos identificados. As alterações tem como objetivo reforçar a segurança da comunicação, reduzir a deteção e classificação do tráfego, melhorar a experiência do utilizador e monitorizar os parâmetros da comunicação. Pretende-se obter, após os desenvolvimentos, uma plataforma mais robusta e capaz de enfrentar os desafios atuais colocados à comunicação VoIP.

# Palavras-Chave

"Privacidade",
"Segurança",
"Session Initiation Protocol (SIP)",
"Técnicas de detecção e classificação",
"Voice over IP" (VoIP).

# Índice

# Lista de Figuras

# Lista de Tabelas

# Glossário

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ALG | Application Layer Gateways |
| B2BUA | Back2Back User Agent |
| BSCW | Basic Support for Cooperative Work |
| CBR | Constant Bit Rate |
| CIA | Confidentiality, Integrity and Availability |
| CISUC | Centro de Investigação e Sistemas da Universidade de Coimbra |
| CODEC | Coder-Decoder |
| CRC | Conferência sobre Redes de Computadores |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DOS | Denial of Service |
| DPI | Deep Packet Inspection |
| DSR | Design Science Research |
| FTP | File Transfer Protocol |
| GSM | Global System for Mobile Communications |
| HTTP | Hypertext Transfer Protocol |
| IANA | Internet Assigned Numbers Authority |
| IAPMEI | Instituto de Apoio às Pequenas e Médias Empresas e à Inovação |
| ICE | Interactive Connectivity Establishment |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia System |
| IP | Internet Protocol |
| IPSec | IP Security Protocol |
| ISP | Internet Service Providers |
| ITU-T | International Telecommunication Union Telecommunication Standardization |
| LAN | Local Area Network |
| LCT | Laboratório de Comunicação e Telemática |
| MGC | Media Gateway Controller |

| | |
|---|---|
| MGCP | Media Gateway Control Protocol |
| MIDCOM | Middlebox Communications |
| MITMA | Man-In-The-Middle Attack |
| MOS | Mean Opinion Score |
| NAPT | Network Address and Port Translation |
| NAT | Network Address Translation |
| NAT/F | NAT and Firewall |
| NGMAST | Next Generation Mobile Apps, Services and Technologies |
| OTT | Over The Top |
| P2P | Peer-To-Peer |
| PABX | Private Automatic Branch Exchange |
| PBX | Private Branch Exchange |
| PESQ | Perceptual Evaluation of Speech Quality |
| POST | Plain Old Telephone Service |
| PSTN | Public Switched Telephone Network |
| QoE | Quality of Experience |
| QoS | Quality of Service |
| QREN | Quadro de Referência Estratégico Nacional |
| RCS | Rich Communication Services |
| RFC | Request for Comments |
| RTCP | Real-Time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| RTSP | Real-Time Streaming Protocol |
| RTT | Round-Trip Time |
| SBC | Session Border Controller |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SNMP | Simple Network Management Protocol |
| SRTCP | Secure Real-Time Transport Control Protocol |
| SRTP | Secure Real-time Transport Protocol |
| SSL | Secure Sockets Layer |
| STUN | Simple Traversal of Udp through NAT |
| SVN | Subversion |

| | |
|---|---|
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol over IP |
| TIE | Traffic Identification Engine |
| TLS | Transport Layer Security |
| TSTAT | TCP Statistic and Analysis Tool |
| TURN | Traversal Using Relay NAT |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UDP | User Datagram Protocol |
| UMTS | Universal Mobile Telecommunication System |
| UPnP | Universal Plug and Play |
| URI | Uniform Resource Identifier |
| VAD | Voice Activity Detection |
| VBR | Variable Bit Rate |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| ZRTP | Z and Real-time Transport Protocol |

# Capítulo 1
# Introdução

Com o aumento dos recursos computacionais disponível aos utilizadores, e com os avanços no acesso e eficiência das tecnologias de rede de acesso, como cabo ou fibra e redes móveis 3G e 4G, abriu-se o caminho para a generalização de aplicações baseadas no Protocolo da Internet (IP – *Internet Protocol*). Um dos exemplos mais representativos são as aplicações de comunicação de Voz baseadas em IP (VoIP – *Voice over IP*), suportadas por uma grande variedade de dispositivos, desde os computadores de secretária até aos dispositivos móveis como os *smartphones*.

Com o surgimento deste tipo de aplicações ocorreu uma modificação no paradigma de comunicação. Fornecidas maioritariamente como serviços *over-the-top* (OTT), as aplicações VoIP ganharam grande popularidade devido ao seu baixo custo, facilidade de uso e suporte à mobilidade, contribuindo para a preferência sobre os sistemas de voz tradicionais. Algumas dessas aplicações são baseadas em normas abertas, tais como o Protocolo de Iniciação de Sessão (SIP – *Session Initiation Protocol*) [RFC3261] e H.323 [ITUTH.323], enquanto outras usam soluções proprietárias, como as aplicações *Skype* [Skype], *Google Talk* [GTalk] e *Yahoo! Voice* [Yahoo].

**Motivação**

O facto de o meio de comunicação de muitas das aplicações VoIP ser partilhado levanta questões de segurança, privacidade e garantias de Qualidade de Serviço (QoS - *Quality of Service*) e de Qualidade de Experiência (QoE - *Quality of Experience*).

Para a realização da comunicação é necessário garantir os seguintes aspetos: a confidencialidade, a integridade e a disponibilidade (CIA – *Confidentiality, Integrity and Availability*). A confidencialidade é um dos aspetos mais importantes no domínio da segurança. Os ataques de interceção de comunicação (MITMA - *Man-In-The-Middle Attack*) podem comprometer a confidencial da informação, devendo esta ser assegurada por meio de mecanismos de encriptação. A autenticidade é complementar ao aspeto confidencialidade, garantindo que os participantes das chamadas são legítimos e conduzindo ao uso de mecanismos de encriptação nos canais de controlo. A disponibilidade está relacionada com a rapidez do sistema. Este aspeto é normalmente ameaçado por ataques de negação e inundação de serviço (DoS – *Denial of Service*). A utilização de mecanismos de validação de mensagens legítimas, a fim de descartar as falsas, evita este tipo de ataques. No entanto, é necessário ter em conta que a introdução de mecanismos de encriptação e validação de mensagens, de forma a garantir a CIA, pode levar, muitas vezes, a uma degradação da QoS e QoE, sendo necessário ponderar os níveis adequados de segurança.

Para além das questões da segurança, existe a necessidade de garantir a privacidade da comunicação. As aplicações VoIP são extremamente sensíveis a problemas com a comunicação, devido à natureza da rede que não é ideal, não garantindo, frequentemente, os níveis adequados de QoS e QoE. Um exemplo é o constrangimento de tráfego (*traffic shaping*), introduzido, muitas vezes, de forma deliberada pelos operadores de comunicação e internet (ISP – *Internet Service Providers*). As comunicações de voz e dados sempre foram a principal receita de muitas operadoras de comunicações, contribuindo o aparecimento de aplicações VoIP concorrentes para a diminuição das receitas do mercado de telecomunicações. Ainda que as operadoras tenham adaptado o seu modelo de negócio, oferecendo planos de comunicações baseados em VoIP, devido à grande concorrência, muitas optaram por se

defender introduzindo mecanismos de bloqueio e estrangulamento, assim como reduzindo a prioridade do tráfego deste tipo de aplicações na sua rede. Portanto, é de extrema importância desenvolver técnicas e mecanismos capazes de mascarar ou alterar o tráfego das aplicações VoIP, a fim de evitar bloqueios, estrangulamentos e perdas de qualidade.

**Enquadramento**

A presente dissertação enquadra-se num projeto de investigação e desenvolvimento tecnológico, parcialmente financiado pelo programa do Quadro de Referência Estratégica Nacional (QREN) [Qren] e pela empresa Collab S.A [Collab]. Este projeto está a ser desenvolvido no Laboratório de Comunicações e Telemática (LCT) do Centro de Investigação e Sistemas da Universidade de Coimbra (CISUC) [CISUC], para a empresa Collab S.A. que desenvolve e comercializa, além de outros produtos, a Plataforma Nubitalk [Collab2012].

O telefone já existe há mais de 100 anos e tornou-se uma parte crítica de qualquer ambiente de negócios. Em termos globais, a migração das centrais automáticas de distribuição telefónicas (PABX - *Private Automatic Branch Exchange*) para ambientes IP-PBX (*Private Branch Exchange*) criou uma mudança das características tradicionais em soluções de comunicação baseadas em *software*. O Nubitalk é uma plataforma de comunicações que tem como objetivo fornecer uma solução de comunicação para clientes empresariais. A plataforma integra funcionalidades de central telefónica empresarial, fornecida por serviços IP-PBX, serviços de presença e outras funcionalidades de *Rich Communication Services* (RCS). Para além destas, a plataforma também suporta algumas funcionalidades de *Contact Center* automatizado, tais como personalização de receção e estabelecimento de comunicações, filas de espera, menus de voz e relatórios detalhados.

O paradigma de funcionamento do Nubitalk corresponde a uma abordagem híbrida entre uma aplicação OTT e uma plataforma integrada com a infraestrutura do operador. Por um lado, toda a comunicação entre os terminais móveis e a plataforma funciona integralmente sobre a internet sem qualquer garantia de qualidade de serviço, à semelhança do *Skype*, do *Google Talk* e do *Yahoo! Voice*. Por outro lado, a plataforma Nubitalk é plenamente integrada com a infraestrutura do operador, nomeadamente ao nível dos Sistemas de Multimédia IP (IMS – *IP Multimedia System*), em aspetos como planos de numeração, ligação a filas de espera, menus de voz e convergência fixo-móvel. Este paradigma de funcionamento encontra-se diretamente ligado à estratégia de comercialização da plataforma, que se apresenta aos operadores de telecomunicações como uma plataforma *white label*, que pode ser depois comercializada junto dos seus clientes como uma solução mais vantajosa.

Por fim, a Plataforma Nubitalk introduz os seus próprios clientes para terminais fixos e móveis, incluindo a vertente VoIP/SIP, permitindo aos utilizadores complementar a telefonia tradicional com soluções VoIP. Por todas as características referidas, esta plataforma permite a redução dos custos de telecomunicações e o usufruto de funcionalidades acrescidas, que conduzem a uma convergência de serviços e dispositivos.

**Objetivos da Dissertação**

O objetivo geral desta dissertação consistiu em analisar, propor e introduzir melhorias e modificações na Plataforma Nubitalk, tendo em conta dois aspetos concretos: o reforço da segurança e privacidade; e o suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência.

O primeiro objetivo corresponde à necessidade de analisar e reforçar a segurança da plataforma. Após uma análise geral do seu funcionamento, verificou-se que existiam falhas graves ao nível da comunicação, entre o cliente e o servidor. Parte da comunicação é realizada de forma não protegida, o que permite a terceiros intercetar e roubar informações. Tendo em mente que o Nubitalk é usado por clientes empresariais e operadoras de comunicações, transmitindo informação com conteúdo sensível, é de extrema importância lidar com falhas de segurança. O aumento dos níveis de segurança da comunicação, contribui naturalmente para o aumento da privacidade, ou seja, para a redução da capacidade de detetar e aplicar técnicas e mecanismos de constrangimento de tráfego. No entanto após um estudo, verificou-se que existem classificadores que recorrem às características particulares da comunicação VoIP, tentando encontrar padrões na análise do tráfego de rede, usando para esse fim mecanismos baseados em estatística, heurística ou de aprendizagem de máquina. Assim, é importante estudar várias alternativas em termos de evasão de tráfego, para iludir os classificadores mais sofisticados.

Em termos de Qualidade de Serviço e de Qualidade de Experiência, os desenvolvimentos incidiram principalmente sobre melhorias à experiência da comunicação da plataforma. O facto de a plataforma não ter capacidades para lidar com mecanismos de bloqueio de rede leva à impossibilidade de estabelecer comunicação, quando os clientes se encontram em redes protegidas (como por exemplo *hotspots*). Este cenário reduz a competitividade da plataforma quando comparada com outras aplicações VoIP puramente OTT (por exemplo a aplicação Skype). Outro melhoramento consiste na introdução de mecanismos de interoperabilidade que possibilitem a integração e comunicação de dispositivos clientes. Esta alteração permite melhorar a integração do Nubitalk com a infraestrutura de operadoras de comunicação. Por fim, ao nível da qualidade, os desenvolvimentos irão incidir sobre a monitorização dos parâmetros das chamadas que, por sua vez, serão guardados numa base de dados. Desta forma, é possível identificar condicionantes nas redes e agir em conformidade.

**Estrutura do Documento**

Este documento está organizado conforme se ilustra na Figura 1. No capítulo dois é apresentado o Estado de Arte, com ênfase no tema VoIP, introduzindo as componentes mais relevantes para a Plataforma Nubitalk (o protocolo SIP, os dispositivos de rede que interferem na comunicação VoIP, mecanismos de mapeamento de endereços (NAT – *Network Address Translation*) [RFC1631] e mecanismos de Firewall [RFC2979], técnicas e mecanismos de deteção e classificação VoIP). O capítulo três apresenta sucintamente a Plataforma Nubitalk e contém uma descrição das soluções propostas resultantes da análise da comunicação da plataforma e os objetivos estipulados para a dissertação. O capítulo quatro resume o trabalho desenvolvido e o capítulo cinco apresenta os resultados obtidos. Por fim, no capítulo seis estão identificadas as principais conclusões do trabalho desenvolvido.

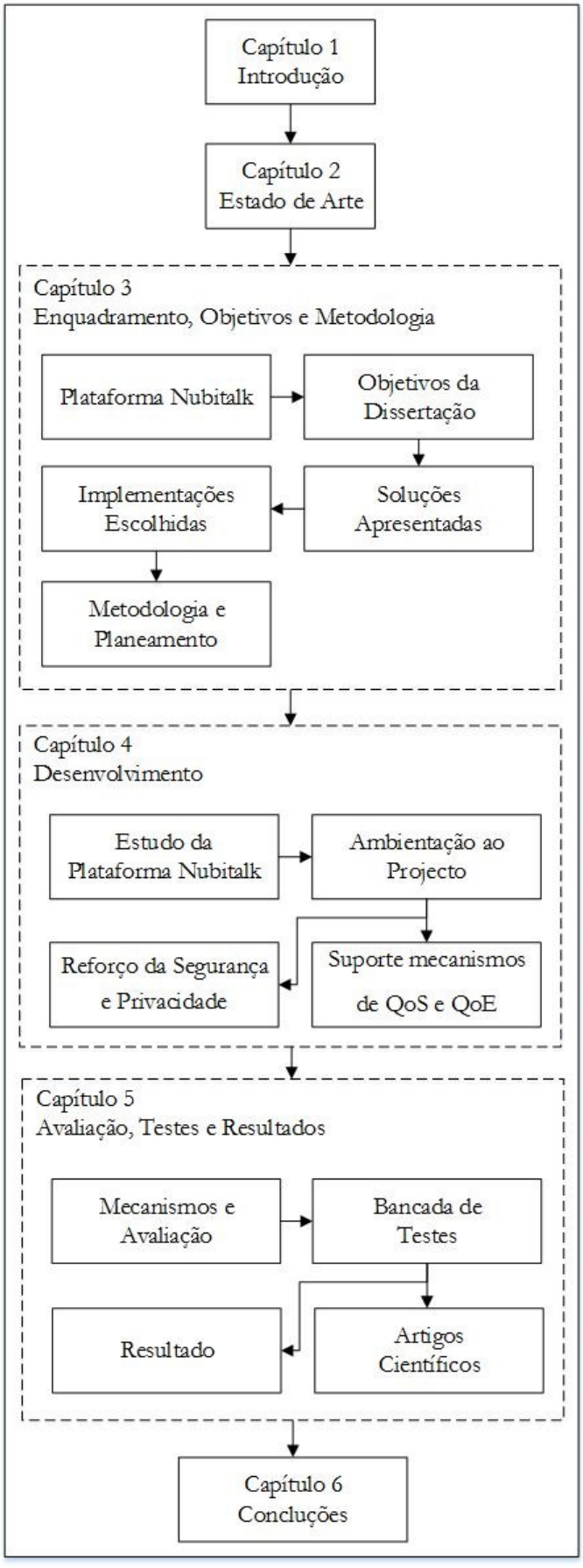



Figura 1 – Estrutura do documento

# Capítulo 2
# Estado de Arte

Neste capítulo irão ser abordados os protocolos, técnicas e mecanismos mais relevantes para a dissertação. O capítulo começa por uma breve introdução ao surgimento da comunicação VoIP, seguida pela introdução do protocolo SIP (visão global e estabelecimento de sessões). São descritas as limitações do protocolo, relativas aos dispositivos de rede e soluções propostas. Por fim, é apresentado uma avaliação de várias técnicas e mecanismo de deteção e classificação de tráfego VoIP. São abordadas as metodologias clássicas e as metodologias baseadas em padrões e fluxos, terminando com o exemplo de deteção e classificação da aplicação Skype.

Ao nível da comunicação VoIP, existem vários protocolos relevantes, como o protocolo de sinalização H.323 ou protocolo de transporte em tempo real (RTP – *Real-Time Protocol*) [RFC3550]. No entanto, estes não foram contemplados em detalhe para o Estado De Arte pois encontravam-se fora do âmbito da dissertação.

## 2.1. Introdução ao VoIP

Antes do aparecimento e difusão das tecnologias suportadas pelo protocolo de internet (IP), as comunicações de voz eram realizadas com recurso a telefones analógicos, mais tarde substituídos por telefones digitais, que utilizavam um serviço telefónico fixo, conhecido como *Plain old telephone service* (POST) [Varshney 2002].

Os serviços como o POST recorrem a uma rede de comutação de circuitos, que cria caminhos dedicados (circuito), entre a origem e o destino. Opostamente, as redes IP baseiam-se na comutação de pacotes, dividindo a informação em pacotes, que são posteriormente enviados e encaminhados pelos vários nós, que compõem a rede. Este tipo de redes permite maximizar o débito, mas introduz uma complexidade adicional e uma elevada variação nos níveis de QoS e QoE, não sendo um meio de comunicação ideal para aplicações multimédia.

O conceito VoIP surgiu da necessidade de utilizar as redes baseadas na comutação de pacotes para a comunicação multimédia. O objetivo do VoIP consiste na comunicação de voz em redes IP, tentando equiparar-se em qualidade às redes baseadas na comutação de circuitos. Manter a QoS e QoE semelhante aos das redes de comutação de circuitos não é elementar. No entanto, as aplicações VoIP tentam compensar as dificuldades aliciando com a redução dos custos operacionais e de infraestrutura, assim como pela oferta de novos serviços aos utilizadores.

O processo de comunicação de voz, através dos protocolos VoIP, pode ser decomposto em quatro partes distintas: a sinalização, a codificação/descodificação (CODEC), o transporte e o controlo. Os protocolos de sinalização permitem criar e gerir ligações e chamadas entre dois pontos. Os CODECs existem para converter os sinais analógicos em sinais digitais, que são posteriormente enviados pelos protocolos de transporte, que garantem o transporte dos sinais digitais em tempo real, através da rede. Por último, existem os protocolos de controlo que gerem os pontos de acesso, nos quais a informação de uma rede é convertida para outra rede, como, por exemplo, na comunicação entre redes IP e redes públicas de telefonia comutada (PSTN – *Public Switched Telephone Network*) [Goode2002].

Com o crescente aumento das aplicações baseadas em IP, como, por exemplo, as aplicações baseadas em VoIP, surgiram múltiplos protocolos abertos e proprietários para lidar com os vários componentes da sinalização, codificação/descodificação, transporte e controlo. Os mais conhecidos encontram-se nas normas desenvolvidas pelo *Internet Engineering Task Force* (IETF) e *International Telecommunication Union Telecommunication Standardization* (ITU-T) [Weback2005].

Ao nível da sinalização, os protocolos abertos mais conhecidos são o SIP e o H.323, normas propostas, respetivamente pelo IETF e ITU-T. Estes protocolos são acompanhados pelas normas G.711 [ITUTG.711] e G.729 [ITUTG.729], ao nível dos CODECs, e pelos protocolos RTP e protocolo de transporte de *stream* em tempo real (RTSP – *Real-Time Streaming Protocol*) [RFC2326], ao nível do transporte. Por fim, são normalmente usados os protocolos de controlo de *Media Gateway* (MGCP – *Media Gateway Control Protocol*) [RFC3435] e H.248 (MEGACO) [ITUTH.248], para lidar com os aspetos de controlo. [Weback2005].

## 2.2. Protocolo SIP

O protocolo SIP é um protocolo de sinalização, desenvolvido pela IETF, para gestão de sessões multimédia. Baseia-se no protocolo de transferência de hipertexto (HTTP – *Hypertext Transfer Protocol*) [RFC2068], em que as entidades SIP são identificadas por identificadores uniformes de recursos (URI - *Uniform Resource Identifier*), semelhantes a endereços de correio eletrónico com nome de utilizador e domínio (sip:utilizador@domínio) [Thernelius2000].

### Visão global

A especificação do SIP está definida nas normas (RCF - *Request for Comments*) IETF, com sua descrição detalhada. Para a criação de sessões multimédia existe a necessidade de atender às seguintes vertentes:

- **Localização**: determinar a localização dos utilizadores, participantes na comunicação.
- **Disponibilidade**: determinar o estado de cada utilizador, para participar em comunicações.
- **Capacidade**: determinar os parâmetros de comunicação de multimédia suportados, que o utilizador possui.
- **Iniciação de Sessões**: o estabelecimento dos parâmetros de sessão de comunicação para ambos os utilizadores.
- **Gestão de Sessões**: gestão de sessão de comunicação, incluindo a transferência e termino de sessões, modificação dos parâmetros de sessão e invocação de serviços.

Para além das vertentes descritas atrás, existe também a possibilidade de realizar o mapeamento de identificadores e do redireccionamento, o que leva à mobilidade por parte dos utilizadores [Pandya1995].

O protocolo SIP não constitui, por si só, um sistema de comunicação completo, sendo apenas um dos componentes. A sinalização, pode ser utilizada com outros protocolos, para construir uma arquitetura multimédia completa. O SIP não fornece serviços, mas sim primitivas, que podem ser utilizadas para os implementar. Um exemplo disso são as primitivas utilizadas para fornecer a localização atual do utilizador ou para fornecer a entrega da descrição da sessão de comunicação. A mesma primitiva pode ser usada para implementar vários serviços. As mensagens SIP podem passar através de redes diferentes, embora o SIP não ofereça capacidades de reserva de recursos de rede. Ao nível da segurança, o protocolo SIP implementa um conjunto de serviços que incluem autenticação (tanto de utilizador para utilizador, como de utilizador para servidor), proteção de integridade, encriptação e privacidade de serviços.

O SIP distingue várias entidades que constituem a arquitetura de uma infraestrutura de comunicação. A Figura 2 ilustra as entidades elementares, que interagem entre si, e constituem a arquitetura básica. Existem, contudo, outras entidades que podem fazer parte da arquitetura, dependendo das necessidades e da implementação. Na especificação do protocolo SIP estão descriminadas quatro entidades distintas:

- **Agente Utilizador** (UA - *User Agent*), que pode ser um utilizador final (UAC - *User Agent Client*) ou um servidor (UAS - *User Agent Server*);
- **Servidor Proxy**, uma entidade intermediária que atua como um cliente ou servidor com o propósito de fazer pedidos em nome de outros clientes;
- **Servidor de Redirecionamento**, que tem como objetivo mapear endereços, como, por exemplo, localização de utilizadores, e devolve essa informação;
- **Servidor de Registo**, que regista os utilizadores numa base de dados com a respetiva informação.

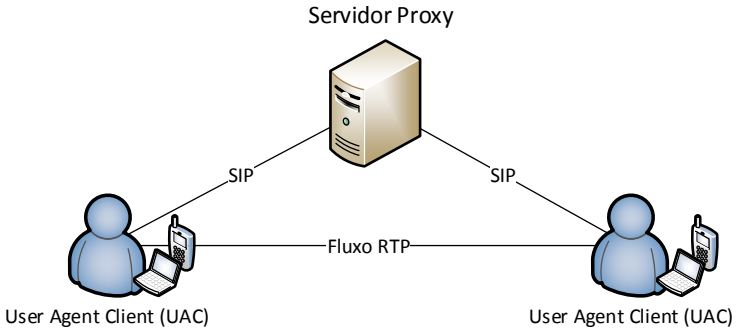



Figura 2 – Arquitetura tradicional do SIP.

### Sessões de Comunicação SIP

A comunicação entre as várias entidades SIP é realizada através de mensagens. À semelhança do protocolo HTTP, existem dois tipos de mensagens: mensagens de pedido e mensagens de resposta. As mensagens de pedido contêm métodos que são usados para iniciar e terminar chamadas, confirmar respostas, registar utilizadores e consultar capacidades. As mensagens de respostas contêm códigos numéricos, baseados no protocolo HTTP, do tipo provisório, que são usados para indicar progresso, e do tipo final, que são usados para terminar a comunicação SIP.

As sessões SIP são criados usando um procedimento de três passos, à semelhança do protocolo de controlo de transmissão (TCP – *Transmission Control Protocol*) [RFC0793]. Quando um agente A (UAC) pretende comunicar com outro agente B (UAC), aquele envia uma mensagem de pedido com o método *invite* e com a descrição da sessão, que contém informação sobre a codificação áudio e a configuração do canal de comunicação. O agente B (UAC) aceita o pedido, enviando uma mensagem de resposta contendo o código 2xx (*success*) e adiciona a sua informação sobre a codificação áudio e a configuração do canal de comunicação. O passo final ocorre quando o agente A (UAC) envia uma mensagem de pedido com o método *ACKnowledge,* a confirmar ao agente B (UAC). A Figura 3 esquematiza a comunicação simples entre dois agentes (UAC). Com as informações sobre a codificação áudio e a configuração do canal de ambos os agentes (UAC) é utilizado um protocolo de transporte, sendo o mais comum o RTP, para estabelecer a comunicação de voz.

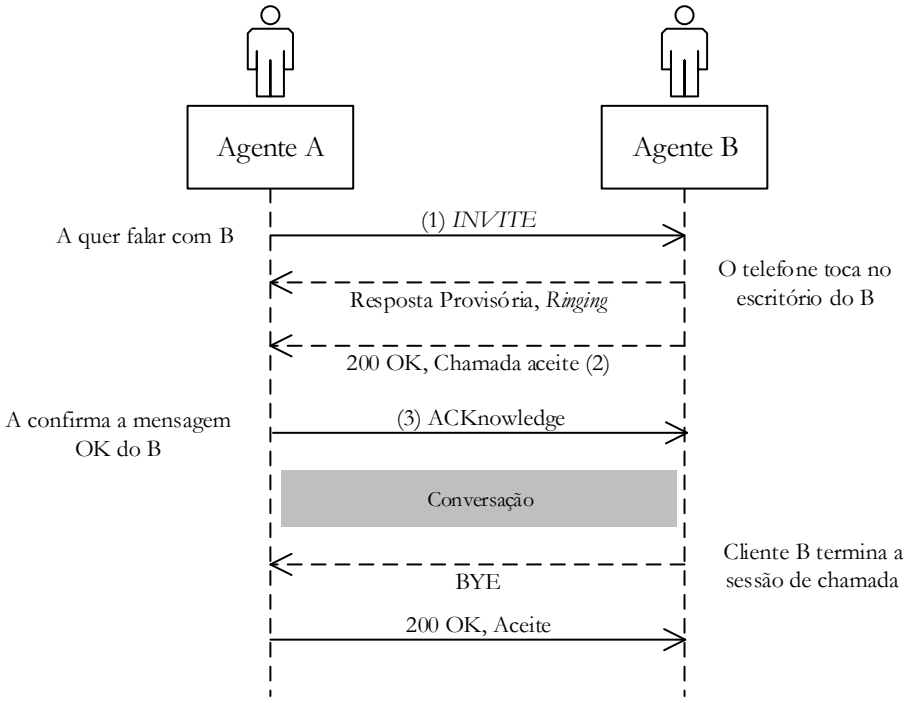



Figura 3 – Estabelecimento de sessão SIP (adaptado de [Thernelius2000])

O cenário anterior ilustra apenas a comunicação, usando as mensagens do protocolo SIP, em que estão envolvidos dois agentes (UAC). No entanto, antes de se iniciar a comunicação entre os agentes (UAC), existe a necessidade de descoberta, ou seja, de localização dos agentes. A localização dos agentes é realizada através do servidor SIP. Quando um agente (UAC) pretende determinar a localização de outro, é enviada uma mensagem de pedido com o método *invite* para o servidor SIP. Por sua vez, o servidor SIP questiona o servidor de registo e reage escolhendo um de dois procedimentos: reencaminha o pedido para o agente (UAC) destino, como ilustrado na Figura 4, ou responde de volta ao agente (UAC) origem com a informação da localização, como ilustrado na Figura 5. O servidor SIP encontra-se, então, a funcionar em modo de *proxy* ou em modo de redirecionamento, respetivamente.

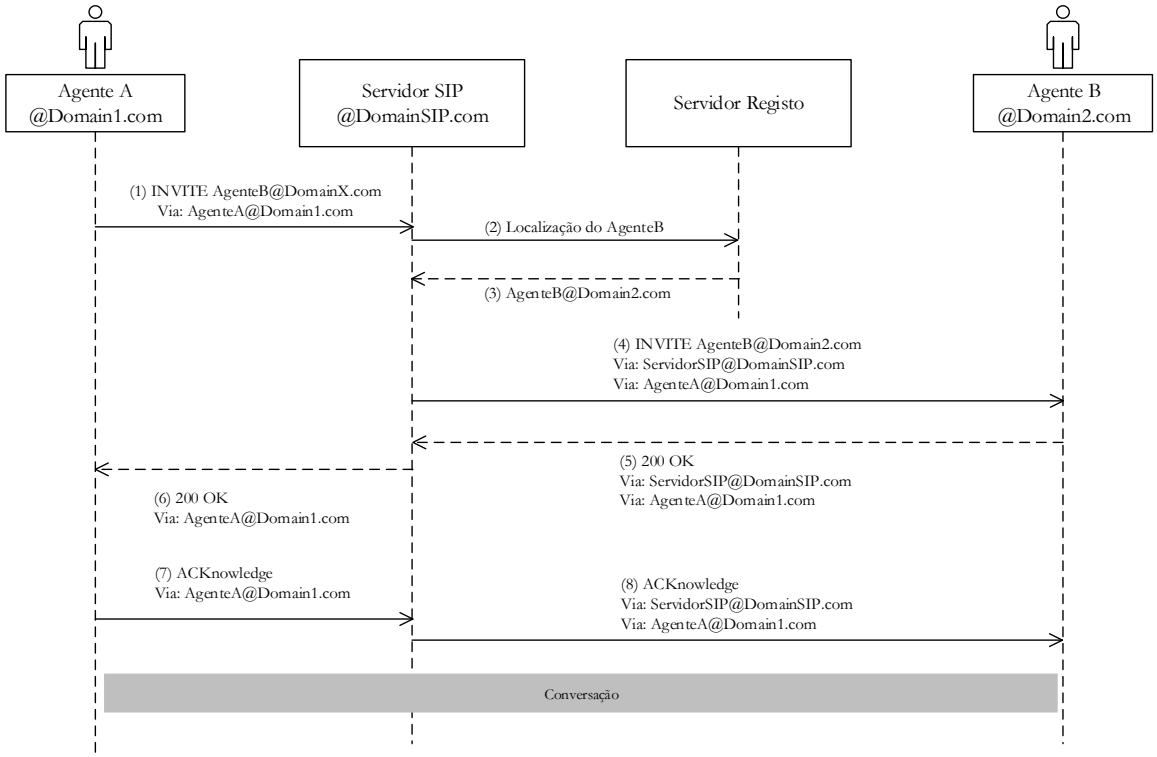



Figura 4 – Comunicação SIP, em modo proxy (adaptado de [Thernelius2000])

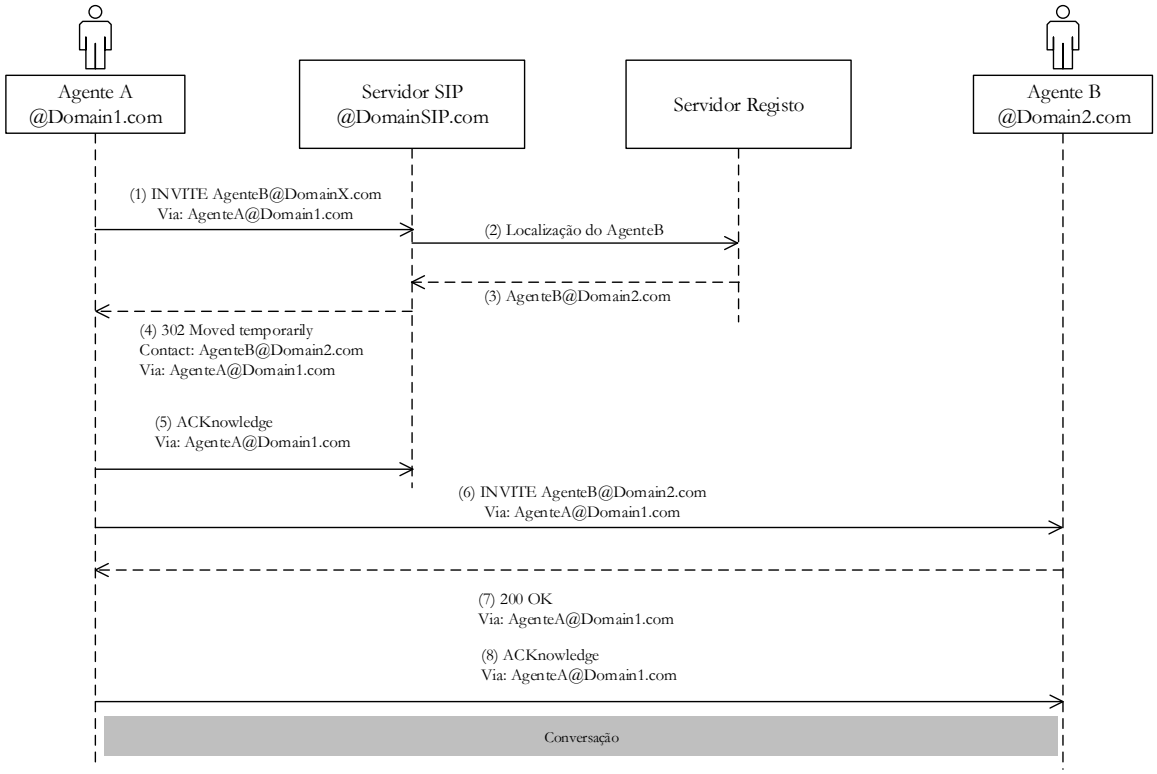



Figura 5 – Comunicação SIP, em modo redireccionamento (adaptado de [Thernelius2000])

De forma geral, a maioria dos agentes (UAC) encontram-se em redes privadas, por detrás de dispositivos e mecanismos de rede, que criam condicionantes à passagem da sinalização e da comunicação. Estes dispositivos e mecanismos estabelecem a ligação entre as redes privadas e públicas, alterando ou bloqueando o tráfego de rede. O subcapítulo seguinte apresenta, em mais detalhe, os vários dispositivos e mecanismos de rede, a sua interferência na comunicação VoIP e as várias soluções existentes para lidar com essa interferência.

## 2.3. Limitações do Protocolo SIP

A rede da internet é normalmente representada por um conjunto de redes de área local (LAN – *Local Area Network*) e redes de área alargada (WAN – *Wide Area Network*) que se encontram interligadas por dispositivos de rede, como *gateways*, *routers*, *switchs*, *bridges* ou *repeaters*. A maioria das redes LAN, como redes de casas, escolas, laboratórios ou escritórios, estão separadas por dispositivos de rede e mecanismos de fronteira que permitem a separação da rede privada da rede pública. Estes mecanismos têm como objetivo fornecer funcionalidades de conectividade, controlo, gestão e segurança.

Os dispositivos de rede e mecanismos de fronteira colocam, muitas vezes, impedimentos à comunicação VoIP, devido à alteração que realização na comunicação quando esta passa entre as redes privadas e públicas. Os mecanismos de mapeamento e de segurança são os que mais interferem nas comunicações VoIP, como a sinalização do protocolo SIP [Thernelius2000] [Khlifi2006].

### Mecanismos de Mapeamento

Os mecanismos de mapeamento de rede, normalmente designado por NAT, são mecanismos que mapeiam os endereços IP de uma rede privada para uma rede pública, situados na fronteira entre as duas redes. Estes foram originalmente pensados como uma solução a curto prazo para o problema do esgotamento dos endereços IP, que iria ser resolvido na próxima geração de IP, o IPv6. Os mecanismos de NAT estão, normalmente, integrados nos dispositivos de *router* e o processo de mapeamento ocorre de forma transparente, sendo os endereços e cabeçalhos IP convertidos da rede privada para a rede pública.

Existem vários tipos de NAT, descritos no RFC [RFC2663], que se distinguem pelo modo como é realizado o mapeamento entre as redes, sendo os mais comuns o NAT estático e o NAT dinâmico. A Figura 6 ilustra um cenário tradicional de NAT.

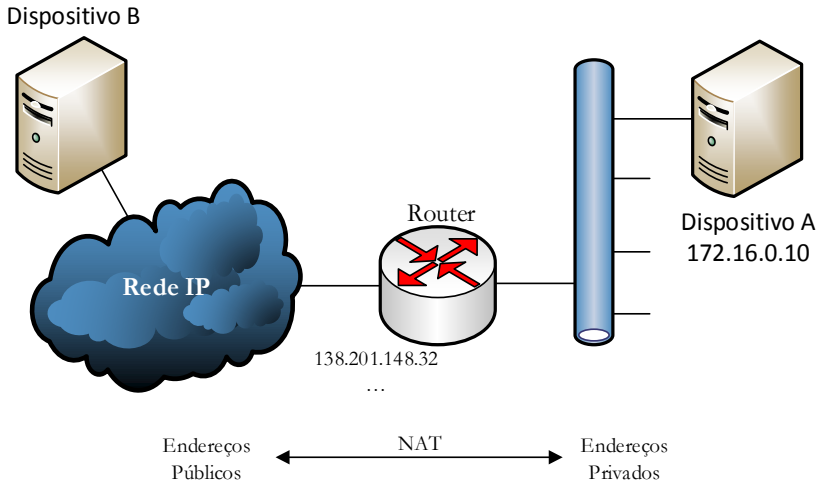



Figura 6 – Cenário tradicional de NAT (adaptado de [Thernelius2000])

O NAT estático, como o próprio nome indica, mapeia um endereço da rede privada num endereço da rede pública de forma estática. Este processo é realizado por um administrador de rede ou por meio de um protocolo, como o protocolo de configuração dinâmica do anfitrião (DHCP – *Dynamic Host Configuration Protocol*) [RFC 2131].

O NAT dinâmico, ao contrário do NAT estático, realiza o mapeamento de endereços da rede privada em endereços da rede pública de forma dinâmica. Os endereços da rede pública são agregados numa *pool* de endereços, que por sua vez são mapeados para os dispositivos da rede privada, quando da sua necessidade. A eficiência desta solução baseia-se no facto de que nem todas as máquinas da rede privada necessitam de estar ligadas à rede pública ao mesmo tempo.

A maioria das redes de pequena dimensão, como redes domésticas ou de escritórios, têm apenas um único endereço IP para a rede pública. Nos mecanismos de NAT básicos, após o seu mapeamento, deixa de ser possível atribuir novos endereços, limitando assim a acessibilidade à rede pública, para os dispositivos que se encontram na rede privada. Neste tipo de cenários, é usada uma versão bastante popular do mecanismo de NAT dinâmico, o mecanismo de mapeamento de endereços e portos (NAPT – *Network Address Port Translation*). O NAPT realiza o mapeamento de endereços da rede privada em endereços da rede pública de forma dinâmica mas usando também o número de portos, ou seja, um endereço da rede privada é mapeado num endereço da rede pública e numa determinada porta desse endereço. As Figuras 7 e 8 ilustram o mecanismo de NAPT.

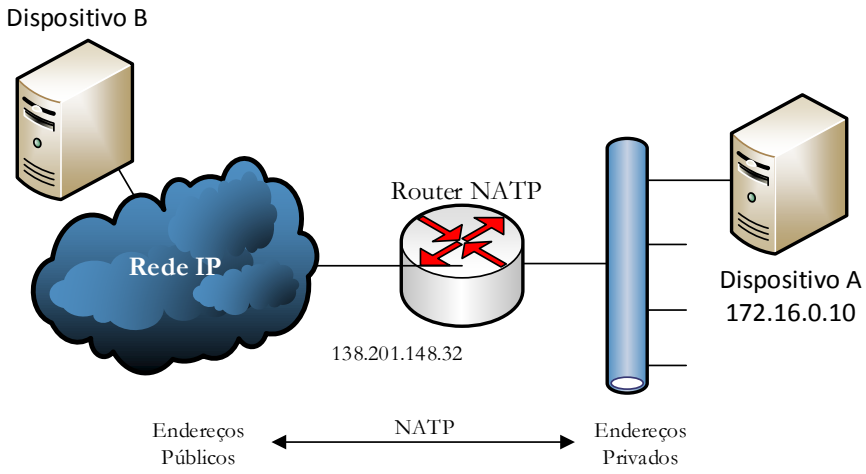



Figura 7 – Cenário de NAPT (adaptado de [Thernelius2000])

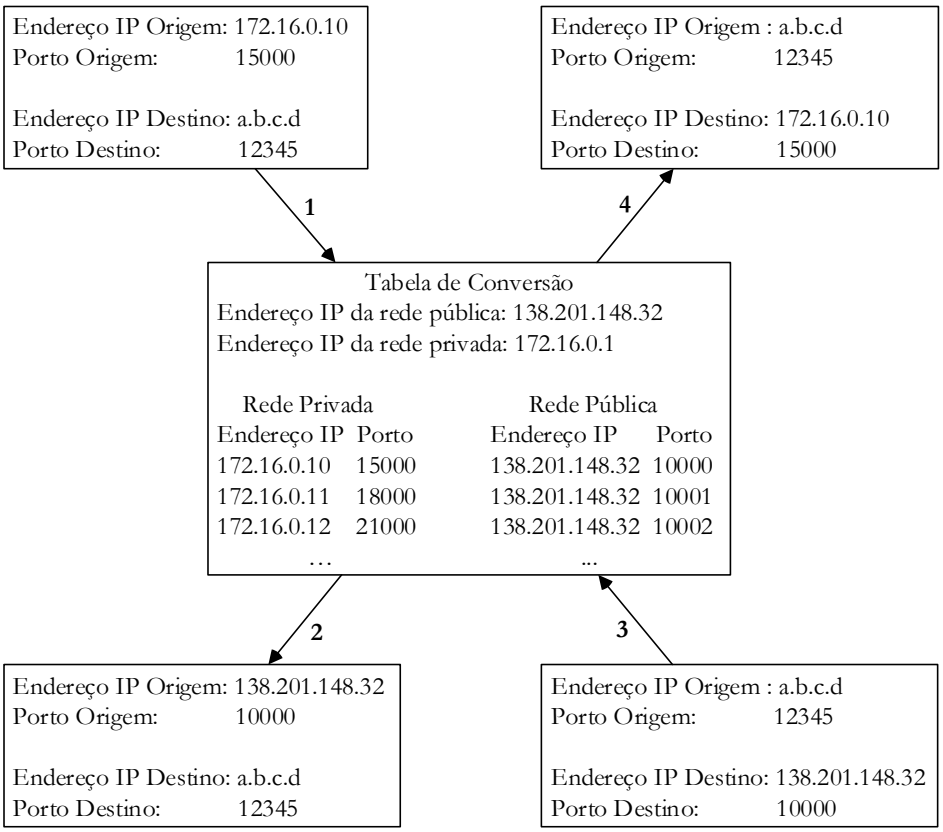



Figura 8 –Tabela de conversão de NAPT (adaptado de [Thernelius2000])

O mapeamento de um endereço IP público num endereço IP privado e num porto pode ser realizado de vários modos, havendo várias implementações distintas do mecanismo de NAPT. A Figura 9 ilustra um cenário tradicional de um *router* com mecanismos de NAPT, para exemplificar as versões diferentes de mapeamento.

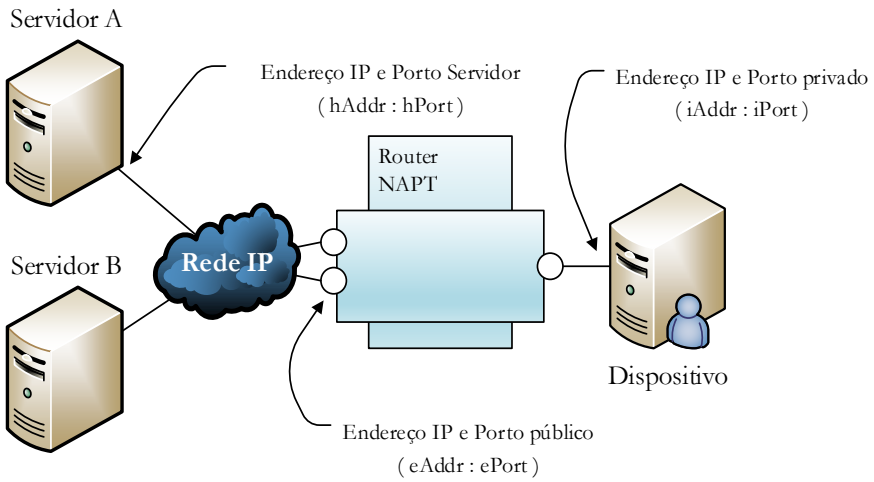



Figura 9 – Cenário de *router* com mecanismos NAPT

O *Full-Cone* NAT, também conhecido como *One-To-One* NAT ocorre quando um endereço IP e porto privado (iAddr:iPort) são mapeados num endereço IP e porto público (eAddr:ePort) e toda a comunicação irá ser enviada pelo endereço IP e porto público (eAddr:ePort). Qualquer dispositivo público (hAddr:hPort) pode comunicar para o endereço IP e porto privado (iAddr:iPort), através do endereço IP e porto público (eAddr:ePort).

O *Restricted-Cone* NAT diz respeito ao cenário em que um endereço IP e porto privado (iAddr:iPort) são mapeados num endereço IP e porto público (eAddr:ePort) e toda a comunicação irá ser enviada pelo endereço IP e porto público (eAddr:ePort). Um dispositivo público (hAddr) pode comunicar para o endereço IP e porto privado (iAddr:iPort), através do endereço IP e porto público (eAddr:ePort), apenas se tiver sido contactado pelo endereço IP e porto privado (iAddr:iPort) previamente. Neste mapeamento, o porto do dispositivo público (hPort) não é tido em conta.

O *Port-Restricted Cone* NAT surge quando um endereço IP e porto privado (iAddr:iPort) são mapeados num endereço IP e porto público (eAddr:ePort) e toda a comunicação irá ser enviada pelo endereço IP e porto público (eAddr:ePort). Um dispositivo público (hAddr:hPort) pode comunicar para o endereço IP e porto privado (iAddr:iPort), através do endereço IP e porto público (eAddr:ePort), apenas se tiver sido contactado pelo endereço IP e porto privado (iAddr:iPort) previamente. Neste mapeamento, o porto do dispositivo público (hPort) é tido em conta.

Por último, tem-se o cenário *Symmetric* NAT, em que, para cada comunicação de um dispositivo privado (iAddr:iPort) e para um dispositivo público (hAddr:hPort) são mapeados um endereço IP e porto público único (eAddr:ePort). Se existirem múltiplas comunicações para o mesmo dispositivo público (hAddr), mas com portos distintos (hPort), são realizados mapeamentos de endereços IP e portos públicos diferentes (eAddr:ePort). Apenas dispositivos públicos, que tenham sido contactados por dispositivos privados, podem comunicar de volta.

**Mecanismos de Firewall**

Um mecanismo de Firewall é um mecanismo implementado com o propósito de aplicação de regras de segurança e políticas de gestão, geralmente situado na fronteira entre a rede privada e pública, que filtra a passagem da comunicação. Este mecanismo tem um conjunto de regras, que são usadas como base para a aplicação de filtros, e toda a comunicação que não cumpra as regras é filtrada e descartada. A Figura 10 ilustra o cenário tradicional de uma Firewall.

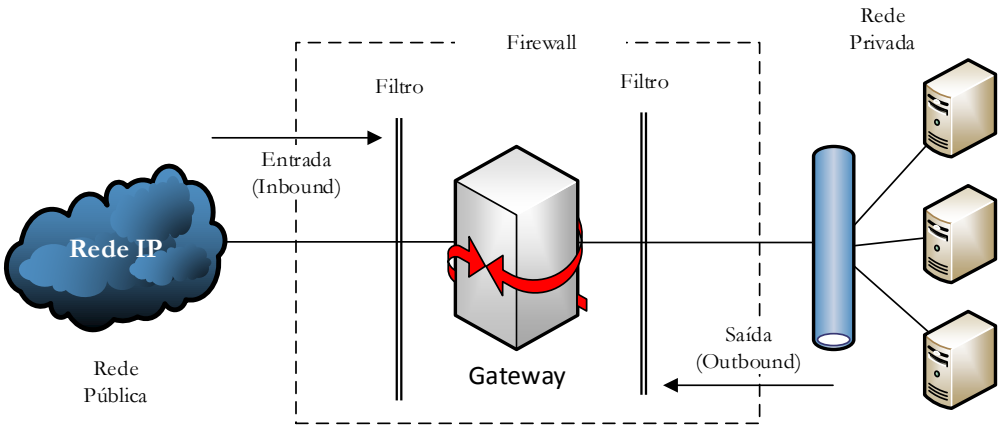



Figura 10 – Cenário tradicional de Firewall (adaptado de [Thernelius2000])

Nas redes de pequena dimensão, como casas e escritórios, a Firewall é usada normalmente como mecanismo de segurança, bloqueando a comunicação indesejada proveniente da rede pública. Quando um dispositivo da rede privada inicia uma comunicação com a rede pública, o mecanismo de Firewall cria uma regra de entrada, para que o dispositivo da rede pública possa comunicar com o dispositivo da rede privada. Após um determinado período de tempo sem comunicação, essa regra é removida e já não é possível a comunicação da rede pública para a rede privada através desse canal.

Nas redes de dimensão média e grande, como laboratório ou edifícios, a Firewall é usada como mecanismo de segurança e de aplicação de políticas de gestão de tráfego. Para além de bloquear comunicação indesejada da rede pública, também impede a comunicação proveniente da rede privada, implementando assim políticas de gestão de tráfego. Os mecanismos de Firewall existem em diferentes implementações, sendo os mais conhecidos os de *Packet Filtering* e *Application Level*.

Os mecanismos de Firewall baseados em *Packet Filtering* inspecionam os cabeçalhos dos pacotes de informação, ou seja, o cabeçalho IP, como base para a aplicação das regras. Os parâmetros mais relevantes para os filtros tendem a ser os endereços IP (origem e destino) e o número do porto (origem e destino), podendo utilizar-se outros parâmetros disponíveis. Estes mecanismos existem em duas variantes, as que não têm memória, normalmente designadas como *stateless*, e as que têm memórias, normalmente designadas por *statefull*.

O último tipo de Firewall, *Application Level*, normalmente designado por *Application Level Gateway* (ALG), é um mecanismo mais sofisticado. Ao contrário dos mecanismos mais rudimentares, o ALG é desenvolvido tendo em conta as aplicações e serviços que irá apoiar, desta forma é possível alcançar níveis de segurança mais elevados. Com suporte para protocolos baseados em TCP e protocolos de comunicação de *datagram* (UDP – *User Datagram Protocol*) [RFC0768], e utilizado em conjunto com mecanismos de NAT, o ALG analisa o tráfego e substitui os endereços IP e portos da rede privada pelos da rede pública, tanto ao nível do cabeçalho IP, como ao nível do corpo da mensagem [RFC 2663]. Existem várias implementações deste mecanismo, sendo as mais conhecidas para o protocolo de transferência de ficheiros (FTP – *File Transfer Protocol*) [RFC0959], o sistema de nomes de domínios (DNS – *Domain Name System*) [RFC1034] e o protocolo simples de gestão de rede (SNMP – *Simple Network Management Protocol*) [RFC1157].

**Condicionantes dos Dispositivos de Rede**

De uma forma geral, grande parte dos agentes (UAC) encontram-se em redes domésticas, redes privadas ligadas à rede pública através de dispositivos como *routers*, que utilizam mecanismos de resolução de endereços NAT e de Firewall (NAT/F). Estes mecanismos, por sua vez, intercetam o tráfego e criam limitação à comunicação VoIP SIP.

As comunicações SIP baseiam-se em estabelecer sessões entre utilizadores, através dos clientes. No entanto, os agentes (UAC) por detrás de mecanismos NAT/F podem facilmente estabelecer ligações da rede privada, mas têm dificuldades em receber as respectivas respostas das redes públicas. As Figuras 11 e 12 ilustram dois cenários contendo o serviço SIP e vários agentes, localizados em várias redes privadas e públicas interligadas por mecanismos NAT/F.

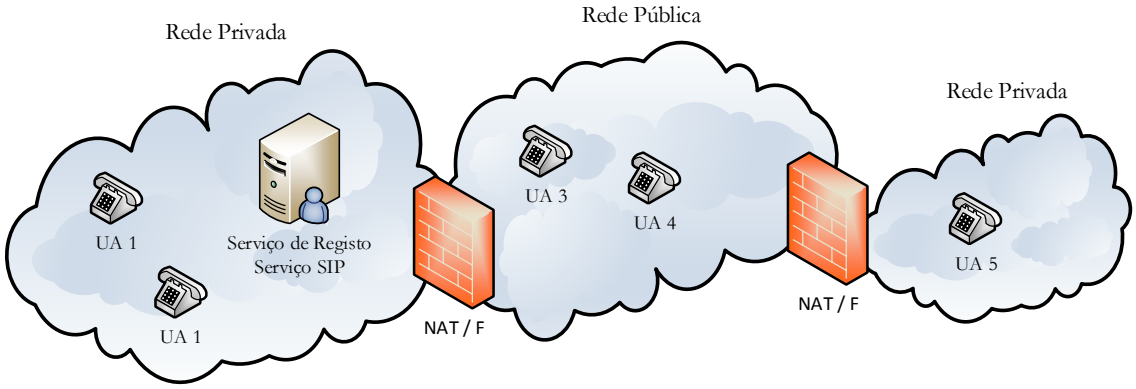



Figura 11 – Cenário com servidor SIP em rede privada (adaptado de [Khlifi2006])

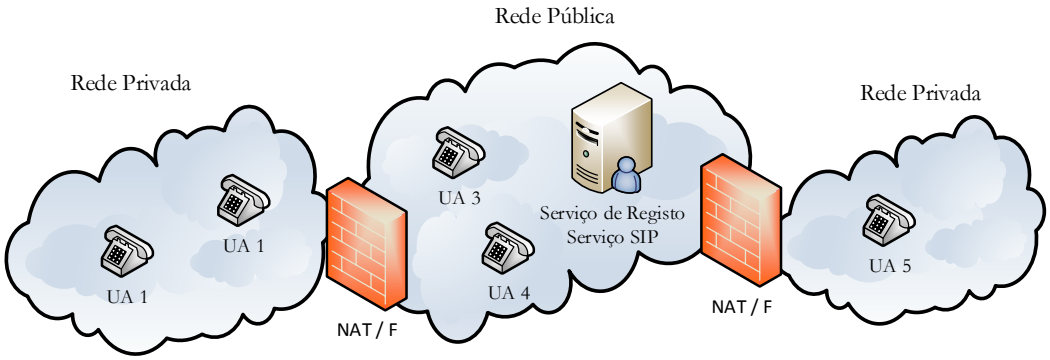



Figura 12 – Cenário com servidor SIP em rede pública (adaptado de [Khlifi2006])

Existem, simplificadamente, duas limitações à comunicação SIP geradas pelos mecanismos de NAT/F: problemas de registo e problemas de estabelecimento e descrição de sessão.

No cenário da Figura 11, os agentes (UAC) 3, 4 e 5 irão enviar os pedidos de registo para o serviço SIP, que se encontra por detrás do mecanismo NAT/F. Caso não existam portos abertos para a comunicação da rede pública passar, estes pedidos irão ser descartados e os vários agentes (UAC) não irão ser capazes de se registar no serviço SIP. Para o cenário da Figura 12 os agentes (UAC) 1, 2 e 5, que se encontram numa rede privada, irão enviar no corpo da mensagem do pedido de registo os seus IP da rede privada. Isto significa que não irão obter resposta pois, tanto o servidor SIP, como os restantes agentes (UAC), não serão capazes de interpretar os endereços da rede privada.

Em ambos os cenários, quando os agentes (UAC) que se encontram em redes privadas tentarem estabelecer uma sessão, irão enviar os seus endereços IP privados, tanto para o contacto como para o canal de comunicação. Quando os destinatários, que não se encontrem na mesma rede, tentarem o estebelecimento da sessão, esta irá falhar, visto que irá ser impossível resolver os endereços IP. O mesmo se passa na comunicação, pois os protocolos de transportes não serão capazes de estabelecer comunicação para endereços IP e portos privados.

Em ambos os cenários, os mecanismos de NAT/F irão, não só bloquear a comunicação das redes públicas para a rede privada, mas também irão fechar canais de comunicação aberto da rede privada, se não forem utilizados por longos períodos de tempo.

**Abordagens Propostas**

Várias soluções têm sido propostas para lidar com as condicionantes descritas anteriormente, sejam apresentadas em RFC, projetos do IETF, ou mesmo soluções proprietárias de alguns provedores de serviços VoIP. A primeira abordagem consiste em resolver as condicionantes, com o recurso ao uso de mecanismos intermediários ou auxiliares entre os dispositivos de rede e os clientes, localizados na rede privada. A segunda abordagem consiste em usar técnicas, baseadas em clientes e servidor, tentando detetar as alterações realizadas pelos dispositivos de rede no tráfego. Por fim, existem algumas soluções que possibilitam aos serviços e às aplicações SIP comunicar com os dispositivos de rede.

Como já foi referido atrás, os mecanismos de ALG têm, para além das funcionalidades tradicionais, a capacidade de entender e alterar as mensagens SIP. Estes mecanismos analisam o cabeçalho e o corpo das mensagens, realizando as modificações necessárias, como o mapeamento dos endereços IP e portos da rede privada para a rede pública. O ALG tem a vantagem de ser transparente, colocando, no entanto, sérias limitações de escalabilidade e velocidade, assim como reservas a novas implementação de novos protocolos VoIP.

Para superar as limitações impostas pelos mecanismos de ALG, foram desenvolvidos mecanismos designados por *Middlebox Communications* (MIDCOM) [RFC3303]. Estes mecanismos permitem aos agentes (UAC) e servidores SIP controlarem os mecanismos de NAT/F, podendo reservar, abrir ou fechar portos. Este serviço permite eliminar a necessidade de desenvolver aplicações com reconhecimento de mecanismos NAT/F. Contudo, o MIDCOM apresenta duas limitações graves. Os administradores de sistemas não aceitam que os mecanismos de Firewall sejam controlados pelas aplicações, por questões de segurança, e a aplicação do MIDCOM necessita da atualização e do suporte de mecanismos NAT/F existentes e das aplicações VoIP.

Os *Session Border Controllers* (SBC) [RFC5853] são dispositivos de rede recentes, que muitas soluções VoIP propõem. Não existe uma definição específica das implementações ou serviços que estes mecanismos devem ou não suportar. Enquanto alguns destes são simples ALG, outros têm suporte para a alteração da comunicação de sinalização e transporte SIP. Os mecanismos de SBC controlam os fluxos de sinalização e de multimédia e encontram-se, habitualmente, entre os mecanismos de NAT/F e a rede pública. São capazes das mesmas funcionalidades dos mecanismos de ALG, no entanto, exigem que alguns portos estáticos permaneçam abertos para o acesso da rede pública à rede privada.

O *Universal Plug and Play* (UPnP) [RFC6970] é um protocolo proposto pela Microsoft, para descoberta e controlo de dispositivos de rede. Este protocolo baseia-se na mesma filosofia do MIDCOM mas a um nível mais próximo dos agentes (UA). O UPnP permite a um agente descobrir a existência de mecanismos NAT/F e requisitar o mapeamento do seu endereço IP e porto da rede privada. Os mecanismos de NAT/F respondem com o endereço IP e porto para a rede pública, podendo o agente enviar as mensagens SIP já com essa informação. Este protocolo, para além de não ser suportado por todos os mecanismos NAT/F, tende a ser rejeitado pelos administradores de rede, devido a questões de segurança e ao facto de não solucionar todos os problemas.

O *Simple Traversal of Udp through NAT* (STUN) [RFC3489] é a solução mais conhecida para lidar com a passagem de comunicação VoIP por mecanismos de NAT/F. Esta solução consiste na troca de mensagens entre cliente e servidor, o que permite às aplicações descobrir a presença e o tipo de mecanismos NAT/F, assim como o endereço IP e porto, que lhes é atribuído após o mapeamento. O processo de descoberta consiste no envio de um pedido, na forma de uma mensagem UDP, do cliente STUN a um servidor STUN, que se encontra na rede pública. Esta mensagem pode passar por um ou mais mecanismos NAT/F, que alteram o endereço IP e o porto da mensagem. O servidor, por sua vez, responde com uma mensagem, contendo no corpo o endereço IP e porto do pedido original. O cliente pode, então, verificar se o seu endereço IP e porto foi mapeado por algum mecanismo NAT/F. O STUN permite ultrapassar os mecanismos de NAT do tipo *Full-Cone*, *Restricted-Cone*, *Port-Restricted Cone* mas não o mecanismo do tipo *Symmetric* NAT. Isto deve-se ao facto de que, para cada endereço IP destino, o mapeamento é diferente, não sendo possível utilizar a informação obtida pelo servidor STUN. Infelizmente, a maioria dos mecanismos NAT/F usados hoje em dia são *Symmetric* NAT.

Visto o STUN não resolver todos os casos possíveis para atravessar mecanismos NAT/F, um novo mecanismo *Traversal Using Relay NAT* (TURN) [RFC5766] foi proposto. Este mecanismo permite serviços de reencaminhamento para as mensagens, entre a origem e o destino. O princípio do TURN é bastante simples e baseia-se também num cliente e servidor. O cliente envia uma mensagem ao servidor, para este alocar um endereço IP e porto, e o servidor responde ao cliente com essa informação. A partir deste momento, as mensagens do agente (UAC) passam a conter o endereço IP e porto alocados no servidor. Quando um agente (UAC), situado na rede pública, pretende comunicar com o agente (UAC), situado na rede privada, este usa o servidor de TURN como um mecanismo intermédio de comunicação. O TURN ainda se encontra em desenvolvimento e apresenta a desvantagem de necessitar de consumir largura de banda, visto que os dados são transmitidos duas vezes, afetando também a qualidade dos serviço, pois introduzindo atrasos e *jitter*.

O mecanismo *Interactive connectivity establishment* (ICE) [RFC5245] é a terceira solução para unificar os mecanismos de STUN e TURN. Este é composto por um agente que tenta encontrar todas as possíveis combinações de endereços IP e portos, que permitam a passagem de fluxos de multimédia, através dos mecanismos de NAT/F. Após serem encontradas várias combinações, usando o STUN e TURN, essas combinações são incluídas no corpo da mensagem, de forma a criar uma lista ordenada de atributos para a comunicação de multimédia, designados por *alts*. Se uma *alt* falhar para o envio da comunicação, o agente passa ao seguinte. O mecanismo de ICE ainda se encontra em desenvolvimento e está a ser lentamente adotado pelas aplicações VoIP. Este mecanismo lida apenas com as questões da comunicação do transporte e não com a sinalização.

## 2.4. Segurança em comunicações VoIP

A transmissão VoIP apresenta várias vantagens em termos de custos e facilidade de utilização. No entanto, traz vários desafios relacionados com a segurança e a privacidade das comunicações. É fundamental garantir a autenticação e a privacidade de uma comunicação de voz, bem como a confidencialidade do conteúdo e dos participantes Pretende-se, aqui, descrever os principais ataques e ameaças, a que o VoIP é suscetível, e os protocolos e mecanismos de segurança atualmente utilizados nas comunicações de voz.

**Ameaças e Ataques**

Os aspetos mais importantes para garantir na comunicação são a confidencialidade, a integridade e a disponibilidade (CIA). A confidencialidade é um dos aspetos mais importantes no campo da segurança, que lida com os ataques como interceção de chamadas. A confidencialidade deve ser assegurada por mecanismos de encriptação. A autenticidade é complementar à confidencialidade. A autenticidade garante que os participantes da comunicação são legítimos. A disponibilidade está, sobretudo, relacionada com a funcionalidade do sistema. Este especto é normalmente ameaçado por ataques de inundação de rede e DOS e deve ser assegurado por mecanismos de validação de mensagens.

Atualmente existem ferramentas de captura e análise de tráfego, como o *Wireshark* [Wshark], *FerramentasRTP*, *Oreka* [Oreka], *VoIPong* [VPong], *VoIPMonitor* [VMonitor], que permitem a interceção e replicação do tráfego de voz não encriptado. O *Wireshark* permite a interceção e registo do tráfego de um interface, suportando ferramentas de identificação de tráfego, descodificação e análises de fluxos, entre outros. A ferramenta RTP é um *software* que inclui um conjunto de ferramentas para enviar, receber e reproduzir pacotes RTP, obtidos através da interceção de tráfego, como o *Wireshark*. O *Oreka*, *VoIPong* e *VoIPMonitor* são ferramentas que detetam comunicação VoIP, com capacidade de interpretar vários protocolos de sinalização, transporte e CODEC, convertendo-a para ficheiros áudio.

**Protocolos e Mecanismos de Segurança**

A comunicação VoIP está, geralmente, associada a dois protocolos: SIP e RTP. O protocolo SIP, como já foi descrito anteriormente em detalhe, lida com a sinalização. Os mecanismos de segurança normalmente usados, para a sinalização, passam pela encriptação das mensagens, usando, por exemplo, protocolo de transporte seguros (TLS – *Transport Layer Security*) [RFC5246], e pelo uso de portos não normalizados, aumentando assim a evasão. O protocolo RTP lida com a transmissão de dados, que inclui as características específicas da transmissão entre outras informações. No entanto, não implementa qualquer tipo de mecanismos de segurança ou encriptação. Estas funcionalidades são alcançadas com a utilização de protocolos seguros, como o protocolo de transporte em tempo real seguro (SRTP – *Secure Real-time Transport Protocol)* [RFC3711] e o protocolo de transporte em tempo real encriptado (ZRTP – *Z and Real-time Transport Protocol*) [RFC6189], ou com recurso a mecanismos de rede que implementam funcionalidades de segurança e encriptação, como as redes virtuais privadas (VPN – *Virtual Private Network*) [RFC4026] e protocolo de segurança IP (IPSEC – *IP Security Protocol*) [RFC4301].

[Alexander2009] realizaram vários testes de comparação de métricas de QoS para as comunicações VoIP, com e sem recurso a mecanismos de segurança. Nestes testes, foram utilizados três tipos de dispositivos, *softphones* (*Snom* e *Twinkle*) e *hardphone*, com três tipos de encriptação diferentes usando a norma de criptografia avançada (AES – *Advanced Encryption Standard*) (128bits, 192bits e 256bits) [RFC3962]. Também foram estudados o uso de protocolos seguros diferentes, como o SRTP, ZRTP e TLS. Os resultados demonstraram que o tempo de processamento necessário aumentava, em 10% para o uso de chaves de 192 bits e 20% para o uso de chaves de 256 bits, comparativamente com o uso de chaves de 128 bits. Também foi percetível que o atraso e o *jitter*, utilizando o protocolo SRTP com uma chave de 128 bits, eram desprezáveis.

[Barbieri2002] realizaram uma análise extensa ao uso de IPSec nas comunicações VoIP. Neste artigo, concluiu-se que o IPSec consome bastantes recursos, aumentado o tamanho dos pacotes em cerca de 50%. Este aumento é justificado pelos cabeçalhos adicionados aos pacotes IP originais, demonstrando também aumentos dos atrasos na comunicação, devido ao tempo necessário para a encriptação. O uso de diferentes algoritmos de encriptação afeta o tamanho dos pacotes, sendo uma escolha importante para as comunicações VoIP.

## 2.5. Mecanismos e Técnicas de Detecção e Classificação de Tráfego VoIP

Os mecanismos e as técnicas de deteção e classificação para aplicações de rede, dos quais são um exemplo as aplicações VoIP, não são um desenvolvimento recente. Este é um campo de pesquisa ativo devido aos desenvolvimentos de novas técnicas e mecanismos, mas também devido à evolução dos protocolos e aplicações VoIP. Como resultado do trabalho desenvolvido nesta área, foram aparecendo várias técnicas e mecanismos desenvolvidos por organizações académicas e por organizações privadas.

**Metodologias Clássicas**

A maioria dos artigos da literatura, [Fonseca2013] e [Fonseca2014], menciona duas técnicas clássicas de detecção e classificação de tráfego: baseadas em análise de portos estáticos TCP/IP e baseadas em análise de protocolos. No entanto, com a evolução dos protocolos estas técnicas tornaram-se obsoletas e não oferecem, nos dias de hoje, resultados precisos.

A técnica baseada em análise de portos estáticos TCP/IP assenta na monitorização de um conjunto de portas pré-definidas, usadas como padrão por um protocolo ou uma aplicação, podendo o número das portas TCP e UDP utilizadas ser consultado, com alguma exatidão, por uma lista fornecida pela *Internet Assigned Numbers Authority* (IANA) [IANA]. Contudo, a capacidade de detecção e classificação usando esta técnica já não é eficiente. Isto deve-se ao facto de não existir um controlo sobre as portas utilizadas pelas aplicações, visto que muitas abandonaram o conceito de utilizar portos pré-definidas e passaram a usar portas dinâmicas.

A técnica baseada em análise de protocolos consiste na utilização de aplicações ou equipamentos de monitorização de rede, que recolhem informação através dos pacotes e dos fluxos de comunicação. Em seguida, com recurso a assinaturas ou modelos de fluxo de tráfego, as aplicações procedem, utilizando a informação recolhida, à sua classificação. Esta técnica baseia-se no conhecimento prévio dos protocolos e no acesso à informação dos pacotes. O rápido aparecimento de novas aplicações, assim como a utilização de técnicas de encriptação, contribuiu para o aumento da complexidade do uso desta técnica, tornando-a frequentemente desencorajada e, muitas vezes, impossível de pôr em prática.

Visto que as técnicas de análise de portos e protocolos, por questões de utilização de portos aleatórios e encriptação, tornaram a classificação de tráfego bastante difícil, surgiu um conjunto de técnicas com base estatística, heurística e em algoritmos de aprendizagem, que não necessitam de conhecimento de portos ou protocolos. Estas técnicas podem ser agrupadas em dois grupos distintos: a mais comum, que consiste na análise do comportamento das aplicações em termos do tráfego de rede gerado, e a menos comum, que consiste em modelar o canal de comunicação do tráfego de protocolos, a fim de encontrar desvios ao normal funcionamento.

## Metodologias Baseadas em Padrões

A encriptação coloca novos desafios na identificação da comunicação, levando à pesquisa de novas formas de classificar o tráfego VoIP. Em [Gomes2012] é proposta uma abordagem com base nos padrões de tráfego de comunicação, que permite uma análise em tempo real, inclusive de tráfico encriptado. A técnica consiste em calcular a entropia do tamanho dos pacotes de dados de diferentes CODECs, utilizando uma janela deslizante para capturar os pacotes transmitidos para cada fluxo, como ilustra a Figura 13.

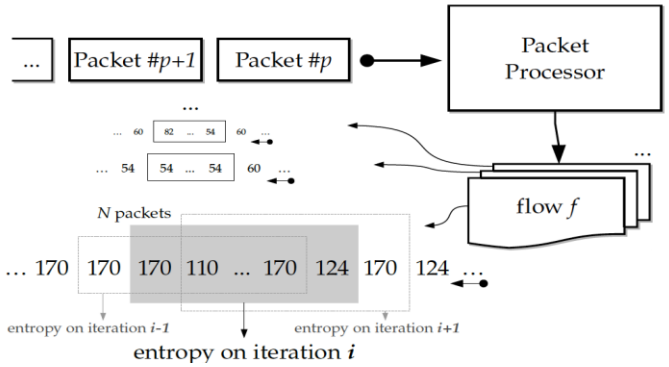



Figura 13 – Calculo de entropia com janela deslizante (retirado de [Gomes2012])

Cada novo pacote recebido é associado a uma janela deslizante correspondente, sendo descartado o último pacote, se a janela estiver cheia. A cada iteração, a entropia é recalculada, permitindo avaliar a evolução ao longo do tempo. A Figura 14 ilustra uma comparação entre a entropia e o tamanho dos pacotes, de sessões VoIP, usando os CODECs com taxas de fluxos constantes (CBR – *Constant Bit Rate*) e variaveis (VBR – *Variable Bit Rate*), respectivamente.

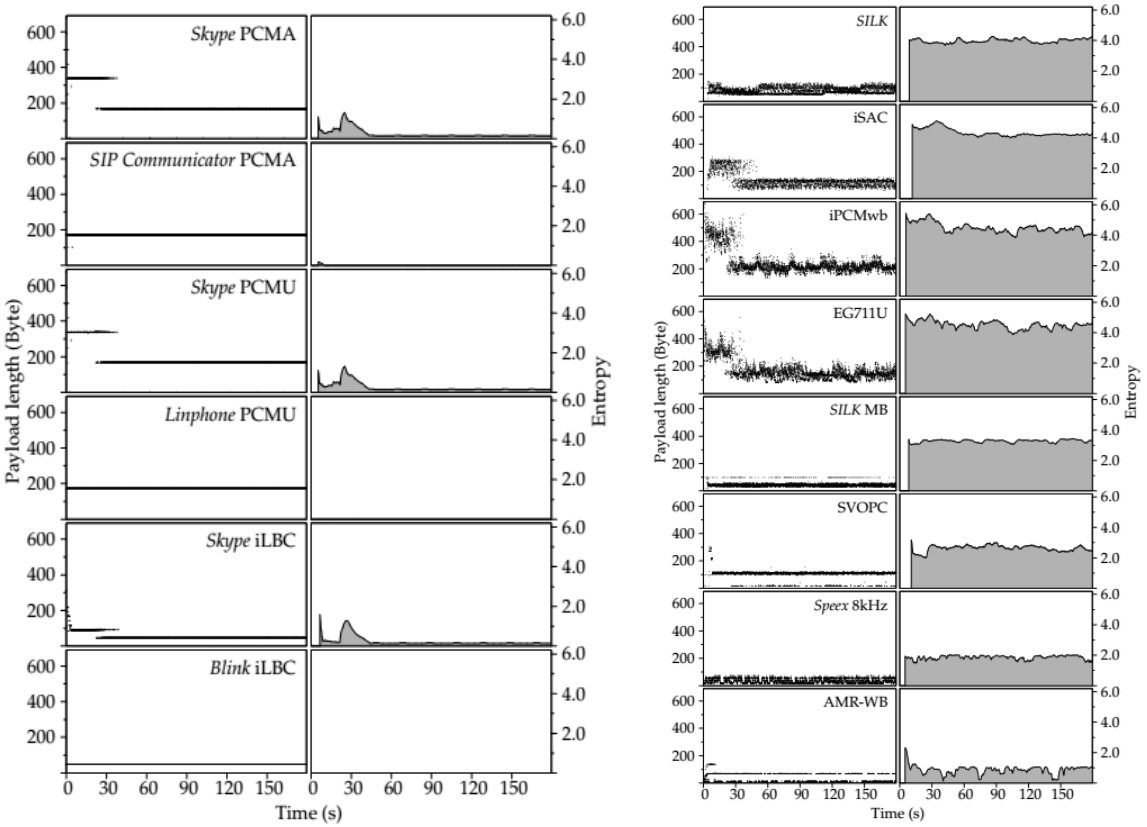



Figura 14 – Análise de CODECs CBR e VBR (retirado de [Gomes2012])

O CODEC CBR tem uma entropia próxima de 0, pois o tamanho dos pacotes é sempre igual. No caso do CODEC VBR, a entropia apresenta valores superiores, pois o tamanho dos pacotes é bastante heterogéneo. Utilizando os parâmetros estudados e aplicando a metodologia descrita, é possível criar um classificador de tráfego que permite identificar fluxos VoIP.

Em [Idrees2008], é apresentada uma análise comparativa de parâmetros de rede de vários tipos de aplicações, caracterizando as várias aplicações com base nas características do seu tráfego, como o tamanho dos pacotes, o débito médio de pacotes e tempo entre chegada de cada pacote. Este artigo apresenta as diferenças evidentes entre os padrões de tráfego VoIP e os padrões de tráfego de outras aplicações da Internet. O tráfego VoIP tem uma assinatura explícita, devido ao seu alto débito médio de pacotes e à média de tamanho de pacotes reduzida. A Tabela 1 apresenta a diferença dos parâmetros de rede das várias aplicações estudadas.

Tabela 1 – Caracterização de vários tipos de tráfego(retirado de [Idrees2008])

| | VOIP Google Talk | VOIP msn | VOIP Skpe | VOIP yahoo | Download | msnchat+ download | msn text chat | Game play | Funny Video |
|---|---|---|---|---|---|---|---|---|---|
| Time | 1m5s | 3m15s | 6m17s | 1m20s | 5m29s | 41m39s | 20m52s | 9m5s | 2m1s |
| Traffic b/w 1st and last packet | 65.660s | 1097.863s | 377.521s | 680.864s | 329.495s | 2499.539s | 1252.718s | 545.1043s | 121.508 |
| Packets | 1361 | 6919 | 9387 | 18700 | 689 | 12276 | 5040 | 1145 | 1039 |
| Average packet/sec | 21 | 35.468 | 24.865 | 27.465 | 2.091 | 4.911 | 4.023 | 2.101 | 8.551 |
| Avg packet size | 178 bytes | 105 bytes | 166 bytes | 125 bytes | 442 bytes | 577 bytes | 414 bytes | 423 bytes | 737 bytes |
| Bytes | 243531 | 726550 | 1565394 | 2349353 | 304923 | 7093194 | 2089413 | 485163 | 766204 |
| Avg Bytes/sec | 3708.982 | 3724.387 | 4146.514 | 3450.545 | 925.425 | 2837.805 | 1667.904 | 890.038 | 6305.8 |
| Avg Mbits/sec | 0.030 | 0.03 | 0.033 | 0.028 | 0.007 | 0.023 | 0.013 | 0.007 | 0.05 |

Com base nos resultados da análise obtida, é proposto um algoritmo de detecção que captura dos fluxos, com débito médio entre os 20 e 40 (pps) e com tamanho médio de pacotes entre os 100 e os 200 (bytes). Devido ao algoritmo ser de caracter genérico, os resultados obtidos na detecção não são bastante precisos, levando a bastantes resultados falsos positivos.

[Wu2008] tem como objectivo a identificação de fluxos de comunicação VoIP, com base nos padrões de conversas humanas. A técnica consiste na utilização dos padrões de tráfego gerados pela conversa humana, com sequências curtas da actividade da voz, ao contrário da análise dos tempos dos pacotes e de todo o fluxo da sessão, tornando-se assim uma técnica mais resistente à variação dos parâmetros de rede. Esta escolha é justificada com base nas desvantagens de várias técnicas de detecção, descritas a seguir.

- O uso de diferentes protocolos de comunicação, como o SIP e o H.323, entre outros, juntamente com a utilização de portas aleatórias, faz com que a análise baseada em portos seja ineficaz.

- A multiplicidade de aplicações VoIP distintas e a utilização de encriptação torna a análise baseada em protoloco difícil e ineficiente.

- A maioria dos mecanismos de identificação VoIP, mais comuns, tem dificuldades em lidar com os períodos de actividade e silêncio da comunicação humana, como, por exemplo, mecanismos de supressão de silêncio (VAD - *Voice Activity Detection*).

Devido a estas condicionantes, é proposto um classificador de tráfego em tempo real que tem como base os padrões da conversação humana, sendo robustos aos mecanismos de supressão de silêncio e às dinâmicas do tráfego VoIP.

O tráfego é apresentado numa cadeia de Markov de quatro estados, sendo os estados A e B correspondentes a um utilizador a comunicar, o estado D representa ambos os utilizadores a comunicar simultaneamente e o estado M a um silêncio mutuo. As Figuras 15 e 16 ilustram o modelo de quatro estados de Markov e ilustram um modelo de conversação, repectivamente.

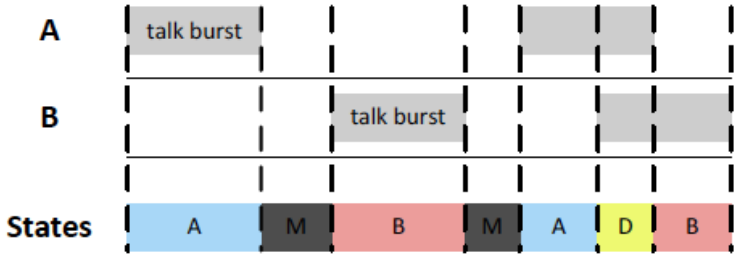



Figura 15 – Padrão de conversa entre dois utilizadores (retirado de [Wu2008])

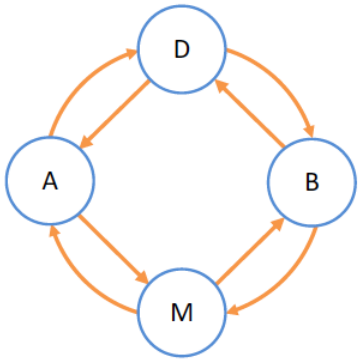



Figura 16 – Modelo de conversação baseado em quatro estados (retirado de [Wu2008])

Através da análise de vários tipos de tráfego, como HTTP, *Peer-To-Peer* (P2P), jogos *online*, Telnet e VoIP, foi possível observar padrões distintivos no modelo de quatro estados de Markov, sendo possível distinguir o padrão do tráfego VoIP dos outros padrões. A Figura 17 ilustra os padrões dos vários tipos de tráfego.

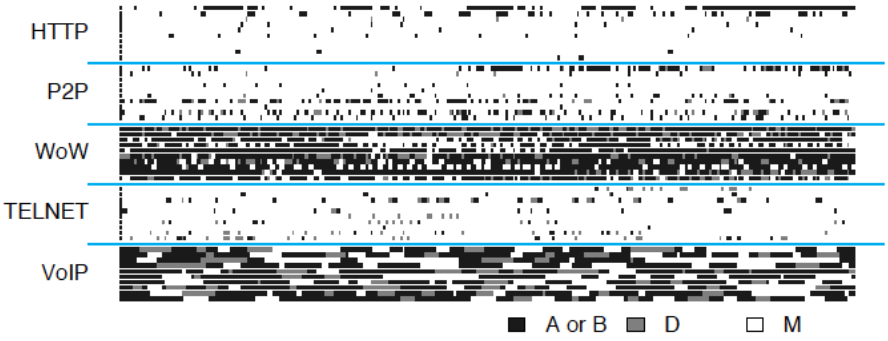



Figura 17 – Padrões de tráfego de várias aplicações (retirado de [Wu2008])

- No tráfego HTTP, não existe comunicação simultânea (estado D). O cliente executa um pedido que é respondido pelo servidor, não existindo mais comunicação, ou seja, período de silêncio, até um novo pedido por parte do um cliente. Este comportamento é visível no diagrama de estados, surgindo, após um estado A, um estado B seguido pelo estado M (período de silêncio).

- O tráfego *Peer-To-Peer* é representado por um estado de comunicação periódico, que representa o *download* e *upload* de dados.

- O tráfego de jogos apresenta bastante interação entre o cliente e o servidor. O cliente informa o servidor dos comandos e acções do utilizador e o servidor actualiza os dados do cliente. Este tipo de comunicação, com pedidos independentes, leva a uma serie de interações distintivas.

- O padrão do tráfego Telnet é semelhante ao do HTTP, com a principal diferença que existe comunicação em simultâneo (estado D) e períodos de silêncio mais longos (estado M).

- O tráfego VoIP é o que apresenta um padrão mais relevante. Conforme descrito no artigo, é possível identificar as seguintes características distintivas: cada um dos quatro estados tende a manter-se por um período longo; a frequência e a duração dos estados representativos da comunicação de um utilizador é mais elevada comparativamente ao estado representativo da comunicação de ambos os utilizadores; existem duas possibilidades para o estado M: silêncio de curta duração, indicativo de lacunas entre palavras e frases, e o silêncio de longa duração, indicativo de espera de resposta ou pensamento. O padrão de estados do tráfego VoIP é claramente representativo da conversação humana, sendo altamente interativo, bidirecional e independente, em ambas as direções.

Os resultados do algoritmo proposto, baseado na cadeia de Markov, demonstram que é possível caracterizar e identificar o tráfego VoIP, com um elevado nível de precisão de verdadeiros positivos, de 97%. Esta metodologia pode ser aplicada a protocolos que utilizem encriptação, nos quais exista mecanismos VAD, com ou sem a utilização de CODECs VBR.

**Metodologias Baseadas em Modelos de Fluxos**

Em [Freire2008] e [Freire2009], é apresentada uma técnica de detecção aplicada ao protocolo HTTP. Esta técnica consiste em analisar o comportamento normal do protocolo HTTP para definir as suas características mais relevantes. A técnica difere dos algoritmos previamente apresentadas, devido a facto de não caracterizar o comportamento das aplicações VoIP, ao nível do tráfego gerado, mas sim o comportamento do canal de comunicação em que o tráfego é injetado.

O primeiro passo para caracterizar o comportamento normal do protocolo HTTP é o de criar um modelo de fluxo do mesmo. Ambos os artigos utilizam o mesmo modelo que identifica os parâmetros mais relevantes. O modelo proposto discrimina os seguintes cinco parâmetros, como os mais relevantes:

- Tamanho do pedido web;
- Tamanho da resposta web;
- Tempo de chegada entre cada pedido consecutivo;
- Número de pedidos por página;
- O tempo de recepção da página.

Para escolher os melhores valores para os parâmetros do modelo anterior, é necessário um conjunto de dados de treino e o teste *Goodness-Of-Fit*. Este modelo é utilizado para medir se uma distribuição particular pode ser satisfatório, como um modelo de população. Após identificar os valores e treinar o algoritmo para o modelo normal, são utilizados os testes de Qui-quadrado (X2) e Kolmogorov-Smirnov (D), para gerar pontuações para cada parâmetro acima descrito. A pontuação representa o quanto um determinado fluxo se desvia dos valores esperados, em cada parâmetro, para o tráfego normal numa navegação web, ou seja, sem tráfego de aplicações VoIP.

O número de pedidos e o tempo de recepção de cada página tem um valor único e estão correlacionados, sendo o número de pedidos usado como um filtro para descartar os fluxos mais pequenos. O tamanho do pedido, o tamanho da resposta e o tempo de chegada entre cada pedido consecutivo são usados para gerar pontuações para os testes X2 e D. Com estes três valores, o fluxo é classificado como legítimo ou não. Para classificar a totalidade do fluxo HTTP, os resultados obtidos, de cada componente, são combinados. Se a maioria for identificada como sendo proveniente de aplicações VoIP, o fluxo HTTP de tráfego é classificado como de uma aplicação de VoIP.

**Ferramentas e Mecanismos de Degradação**

Dado o volume elevado de dados que são transmitidos pelas redes de hoje, algumas companhias começaram a oferecer *hardware* específico com *software* proprietário, construído com o intuito de permitir que os seus clientes (incluindo os operadores das redes) tenham um melhor controlo e visualização da informação que passa nas redes. Estas companhias, tais como a *BlueCoat* [Blue], *Sandvine* [Sand] e *ArborNetworks* [Arbor], entre outras [Exinda] [Cymp] [Allot], são exclusivamente dedicadas à criação de *software* e otimização de *hardware*, de forma a promover soluções para controlo de redes, incluindo funcionalidades como a análise de tráfego encriptado, mecanismos de constrangimento de tráfego e garantias a QoS e QoE, entre outros.

No entanto, este tipo de ferramentas não são apenas desejadas pelos operadores de comunicações, sendo cada vez mais procuradas por entidades que fornecem acesso à rede a vários utilizadores, como, por exemplo, entidades que detenham *hotspots*. Estas entidades pretendem controlar e observar as suas redes, de forma a gerir um acesso uniforme a todos os utilizadores. Em alguns casos, as entidades oferecem planos de comunicação com clientes proprietários aos visitantes, com o intuito destes não usarem aplicações OTT, tais como o Skype. Neste contexto, as ferramentas de degradação de tráfego, para além do controlo da QoS e QoE, são usadas para limitar o acesso às aplicações VoIP.

Existem no mercado vários equipamentos comerciais de baixo custo e processamento, que oferecem soluções mais vantajosas do que as soluções dos operadores de comunicação, permitindo um melhor controlo da rede. Soluções como o *NetEqualizer* [NetE] e o *NetGladiator* [NetG], entre outras [Meraki] [Nomadix] [AntL], oferecem equipamentos que aplicam mecanismos de *deep packet inspection* (DPI) a todos os dados transmitidos, de maneira a classificar e bloquear o tráfego de rede indesejado. Este tipo de mecanismos tem a desvantagem de necessitar de poder computacional, que aumenta caso o tráfego seja encriptado, tornando-se muitas vezes impraticável.

Estes classificadores analisam o tráfego de rede não encriptado, classificando-o e bloqueando-o. Para lidar com o tráfego encriptado são normalmente usadas duas medidas: o tráfego é descartado ou limitado a uma certa largura de banda. Por norma, os detetores e classificadores de tráfego analisam as seguintes métricas de rede: a persistência do fluxo de dados, a quantidade de fluxos ativos, o período de tempo em que o fluxo está ativo, o congestionamento geral da rede e a largura de banda usada pelo fluxo, em função congestionamento geral da rede. As ações tomadas pelos detetores e classificadores são em função das respostas obtidas às métricas descritas.

# Capítulo 3
# Enquadramento, Objetivos e Metodologia

Este capítulo apresenta em mais detalhe o enquadramento e os objectivos da dissertação, com a informação detalhada do funcionamento da Plataforma Nubitalk e do projecto Nubitalk respectivamente, para que em seguida seja compreensivel as escolhas e as soluções propostas apresentadas. Ainda neste capítulo encontra-se descrita a metodologia e o planeamento.

## 3.1. Apresentação da Plataforma Nubitalk

As tendências atuais das comunicações têm um impacto significativo sobre os arquiteturas dos serviços de voz, assim como sobre as soluções e arquiteturas para enfrentar os desafios e as oportunidades que surgem. As operadoras de telecomunicações fixas e móveis estão a implementar novas gerações de redes IP, o que leva ao surgimento de uma gama de plataformas e serviços, que antes não eram possíveis. Os clientes podem agora migrar da tradicional telefonia para soluções VoIP, reduzindo assim os seus custos de telecomunicações e beneficiando de uma rede única, em vez da tradicional rede para voz e rede para dados.

A serviço Nubitalk, como já foi referido, consiste numa plataforma de comunicações de voz, que integra funcionalidades de central telefónica empresarial, fornecida por serviços IP-PBX, serviços de presença e outras funcionalidades de RCS, acrescentando mecanismos automatizados de *Contact Center*. A comunicação de voz é disponibilizada como um serviço OTT e, ao nível da comercialização, a Plataforma Nubitalk apresenta-se como uma solução *white label* para operadores de comunicações, permitindo a integração com planos de numeração, mecanismos *legacy*, IMS, filas de espera, menus de voz, relatórios detalhados, etc..

## Visão global

A Plataforma Nubitalk é constituída por vários módulos. O núcleo da plataforma está ilustrado na Figura 18 e é constituído pelos seguintes serviços: *OnePark*, *OneContact* e *OnePBX*.

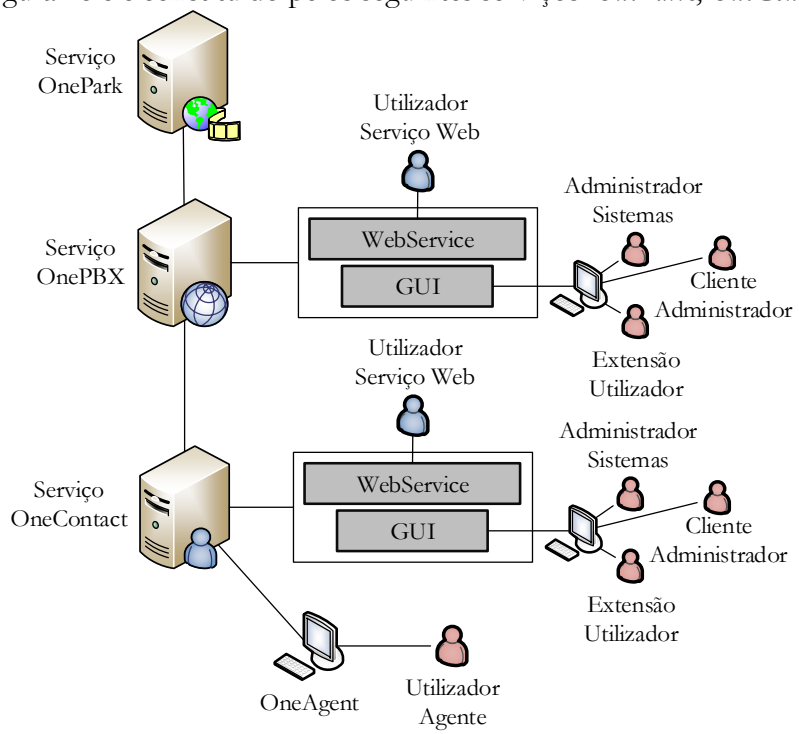



Figura 18 – Núcleo da Plataforma Núbitalk

O serviço *OnePark* é responsável pela gestão de conteúdos de multimédia, assemelhando-se a um *Media Server*. O serviço *OneContact* é a solução proprietária automatizada de *Contact Center,* baseada em IP, que oferece, entre outras, funcionalidades de gestão de contatos, vídeo, mensagens instantâneas e correio eletrónico. O serviço *OnePBX* é um serviço que implementa todas as funcionalidades de controlo das chamadas. Cada um dos serviços disponibiliza interfaces que permitem a sua configuração e gestão, assim como a interligação com outros serviços externos. A Figura 19 ilustra a integração do núcleo da Plataforma Nubitalk numa arquitetura simples, com os protocolos SIP e RTP.

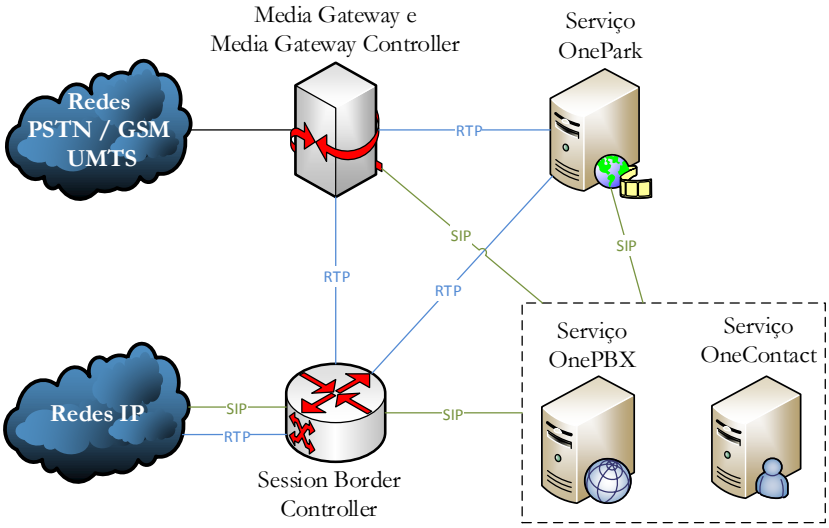



Figura 19 – Comunicação do núcleo da Plataforma Núbitalk

O serviço *OnePBX* constitui o componente principal da comunicação de voz da Plataforma Nubitalk. As funcionalidades deste baseiam-se no IP PBX, usando um modelo lógico de comunicação VoIP *back-to-back user agent* (B2BUA). Neste modelo lógico o servidor serve de intermediário entre os clientes, implementando as funcionalidades de controlo das chamadas e facilitando a implementação de planos de numeração. Ao nível protocolar, o serviço *OnePBX* suporta os seguintes protocolos:

- *Session Initiation Protocol* (SIP), responsável para sinalização e estabelecimento de sessões de comunicação;
- *Session Description Protocol* (SDP), responsável pela negociação e descrição das sessões de comunicação;
- *Real-Time Transport Protocol* (RTP), responsável pelo transporte de multimédia, podendo esta ser codificada em G.729 ou G.711 para o áudio e H.263 para o vídeo;
- *Real-Time Control Protocol* (RTCP), responsável para controlo do protocolo RTP;
- *Hypertext Transfer Protocol* (HTTP), responsável pela comunicação web com o OnePBX;
- Serviço Web, responsável pela integração com sistemas externos.

A arquitetura da plataforma pode ser apresentada como um modelo simplificado, no qual, para além do núcleo, apenas existem os clientes finais (fixos ou móveis) dispersos na rede, usando uma filosofia de comunicações VoIP SIP OTT. No entanto, a plataforma também permite a integração com outros dispositivos e mecanismos, normalmente utilizados por operadoras de comunicações, criando assim uma arquitetura mais completa, a qual está ilustrada na Figura 20.

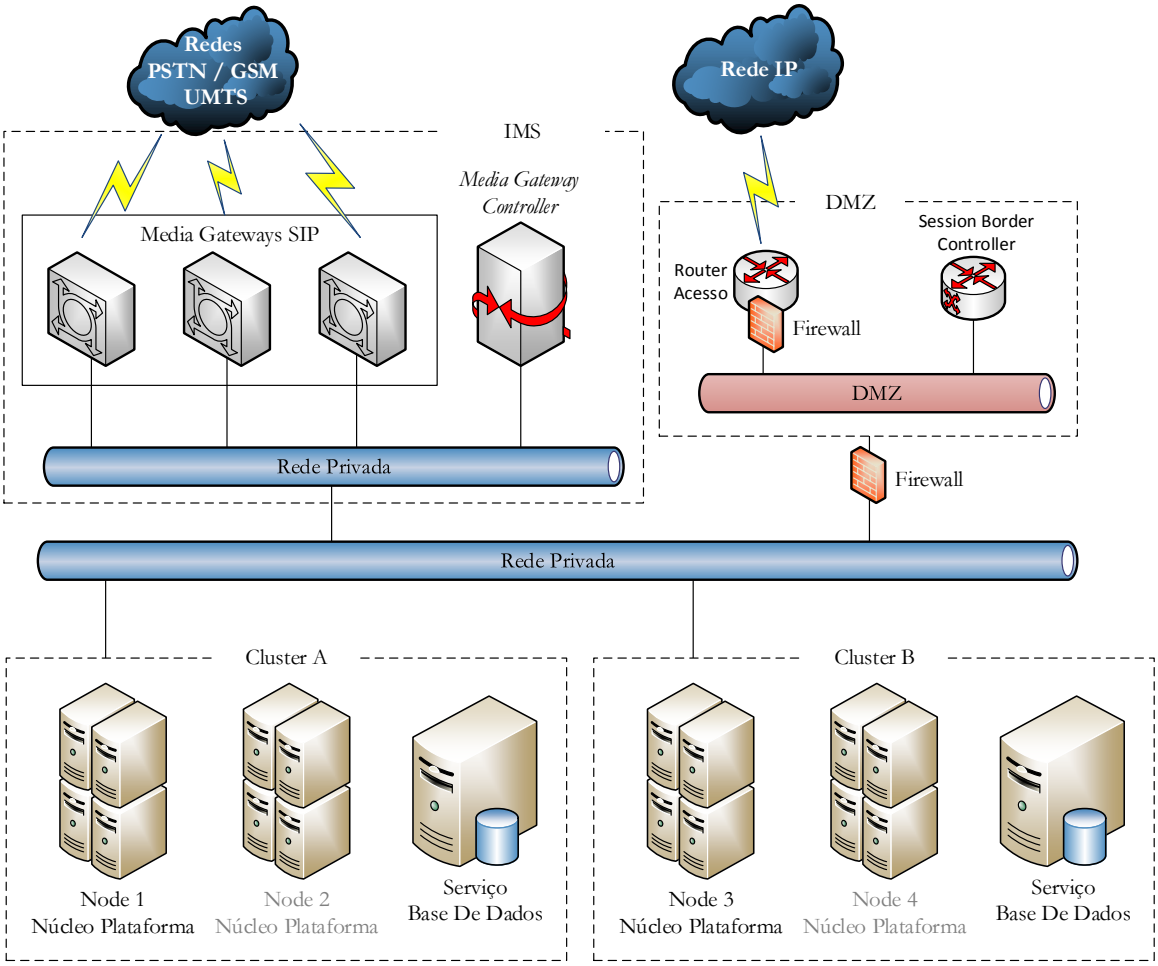



Figura 20 – Arquitetura da Plataforma Núbitalk

Ao nível da arquitetura, o cenário mais complexo onde a Plataforma Nubitalk pode ser integrada é composto por três redes distintas: rede privada, rede privada de perímetro (DMZ – *Demilitarized Zone*) e rede pública. Os componentes do núcleo são agrupados em *clusters* de máquinas, para lidar com a disponibilidade, e encontram-se ligados aos serviços de base de dados, aos *Media Gateways, Media Gateway Controller* (MGC) e dispositivos *legacy*. Esta configuração permite uma integração e uma arquitetura flexível, para lidar com vários cenários.

Nos serviços de base de dados são guardadas todas as informações da plataforma. Os *Media Gateway* e *Media Gateway Controller* são responsáveis pelo controlo e gestão da informação que passa da rede IP para a rede fixa PSTN, redes móveis *Global System for Mobile Communications* (GSM) e *Universal Mobile Telecommunication System* (UMTS), sendo compatíveis com os vários RFC [RFC2327] [RFC3261] [RFC3550]. Ao nível dos dispositivos *legacy,* existe a comunicação com soluções PBX tradicionais, desde que estas suportem o protocolo SIP.

Relativamente aos dispositivos de rede, existe a possibilidade de utilização de um SBC proprietário, designado OneSIPConnector. Este mecanismo, após a configuração das gamas de IP das várias redes privadas, soluciona a interferência dos mecanismos de NAT sobre a comunicação VoIP. Encontrando-se na zona limite entre a rede privada e a rede pública, o SBC inspeciona a passagem do tráfego, realizando as alterações necessárias para tornar transparente a localização de clientes em redes privadas.

Finalmente, a Plataforma Nubitalk tem uma aplicação cliente designada "Nubitalk", que pode ser utilizada tanto em dispositivos móveis como em dispositivos fixos, e que consiste numa aplicação de comunicação VoIP SIP com suporte para funcionalidades de RCS. Sendo o serviço Nubitalk uma solução de convergência suporta também outros clientes SIP VoIP. Para além das aplicações clientes VoIP, existem também aplicações específicas para as várias funcionalidades disponíveis, como agentes do *Contact Center* ou agentes de configuração, que podem encontrar-se dispersas pela rede pública.

## 3.2. Objetivos da Dissertação

Nesta secção retomamos e descrevemos, em maior detalhe, os objetivos da dissertação já identificados no capítulo da Introdução. Como já foi referido anteriormente, o objetivo geral consiste em analisar, propor e introduzir melhorias e modificações na Plataforma Nubitalk, tentando combater alguns aspetos e características menos positivas da mesma. A dissertação foca-se em duas áreas concretas: o reforço da segurança e privacidade; e o suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência.

Esta dissertação enquadra-se no projeto Nubitalk, que como já foi descrito consiste num projeto de investigação e desenvolvimento tecnológico de parceria entre o LCT e a empresa Collab. O principal objetivo do projeto Nubitalk foi conceber e desenvolver uma plataforma de convergência fixo-móvel que permita a empresas e organizações de pequena e média dimensão contratar, configurar e utilizar, de modo bastante rápido, económico e flexível, serviços de comunicações mais sofisticados e que não estariam, normalmente, ao seu alcance. Os requisitos do projeto centram-se na atuação ao nível dos seguintes aspetos:

**Considerações sobre CODECs e QoE:** foram investigadas soluções para comutação dinâmica de CODECs que fazem uso das características do protocolo RTP. Este mecanismo permite manter a integridade das comunicações SIP usando clientes clássicos, ao mesmo tempo que abre a possibilidade do cliente Nubitalk poder implementar um mecanismo de adequação dos CODECs, às condições do canal de comunicação que constitui uma mais-valia para o produto.

**Considerações sobre mecanismos de monitorização de QoS e QoE:** este aspeto realizou-se sobre a forma da análise de mecanismos de monitorização de QoS para incorporação na plataforma Nubitalk, assim como mecanismos de feedback de QoE. Toda a informação recolhida era em seguida armazenada numa base de dados.

**Segurança das comunicações:** atuações sobre a forma de proteção na sinalização e na comunicação de voz. Contudo, existiu a necessidade de ponderar potenciais penalizações decorrentes dos processos de encriptação e encapsulamento, com o impacto em termos de latência e eficiência. Neste sentido, o esforço desenvolvido foi levado a cabo com o objetivo de proporcionar o balanço adequado entre segurança e desempenho.

**Considerações sobre mecanismos de *profiling* e degradação de tráfego:** foi realizada investigação de um conjunto de soluções para proteção, não só do tráfego de voz ao nível da rede, mas também no sentido de averiguar de que modo este poderá ser camuflado, de modo a evadir os mecanismos de deteção e classificação normalmente utilizados pelos operadores de telecomunicações e operadores de infraestrutura.

O objetivo do reforço da segurança e privacidade constituiu em analisar a Plataforma Nubitalk e atuar nas componentes mais desprotegidas da comunicação. Adicionalmente aos mecanismos de segurança, que por si só já contribuem para o aumento da privacidade, existe a necessidade de analisar possíveis modificações à comunicação. A Plataforma Nubitalk, na sua forma mais simples, disponibiliza a comunicação de voz como um serviço OTT, muitas vezes competidor de serviços semelhantes disponibilizados por operadoras de comunicação, que também são responsáveis pelo serviço de internet. Este cenário levanta questões de competitividade, que pode levar ao estrangulamento de tráfego. Existe então a necessidade de propor metodologias para reduzir a possibilidade de deteção do tráfego VoIP gerado pela Plataforma Nubitalk.

O objetivo de dar suporte à Qualidade de Serviço e à Qualidade de Experiência, incidiu principalmente em lidar com as condicionantes à experiência de utilização da plataforma. Sendo o ponto forte da plataforma a sua capacidade de integração com serviços e infraestruturas dos operadores de comunicações, é importante o suporte de um vasto número de dispositivos clientes, muitas vezes incompatíveis entre si. Para além da capacidade de integração, existe a necessidade do estabelecimento de comunicação independentemente da configuração da rede. A plataforma deve ser provida de mecanismos para lidar com os dispositivos de rede, que se interponham à passagem da comunicação, proporcionando assim uma melhor experiencia aos utilizadores.

Finalmente existe a possibilidade de adquirir informações sobre o estado das comunicações. Estas informações possibilitam a apresentação de informação viável aos utilizadores sobre o estado dos serviços e ao mesmo tempo permitem *feedback* sobre o estado da comunicação, como relatórios para a Plataforma Nubitalk. As métricas da QoS medem o desempenho a partir da perspetiva da rede e são representativas da capacidade de uma rede para fornecer diferentes níveis de serviço. As abordagens de QoS são focadas para os impactos das condições de rede no nível da qualidade de transmissão, não refletindo o impacto na experiência do utilizador final. Devido às restrições das redes IP é fundamental avaliar as condições da rede através de métricas de Qualidade de Serviço e de Qualidade de Experiência, podendo assim adaptar as comunicações VoIP para essas condições.

## 3.3. Soluções Propostas para Reforço da Segurança e Privacidade

Um dos objetivos descritos no capítulo da Introdução diz respeito ao reforço da segurança e da privacidade, atuando nas componentes da plataforma ao nível da comunicação.

O reforço da segurança na comunicação passa pelo recurso a mecanismos de encriptação e pela utilização de protocolos seguros. A Plataforma Nubitalk, ao nível da comunicação VoIP, faz uso dos seguintes protocolos: protocolo SIP para a sinalização, protocolos RTP para o transporte áudio e vídeo e o protocolo RTCP para o relatório e monitorização das métricas de QoS. Destes, apenas o protocolo SIP tem mecanismos de segurança, fazendo uso de um protocolo de transporte encriptado (TLS).

Os protocolos RTP e RTCP não implementam nenhum mecanismo de segurança e encriptação nas suas normas. As funcionalidades de segurança e encriptação podem ser obtidas usando várias técnicas, mecanismos ou protocolos. Ao nível da camada de rede, podem ser utilizadas redes privadas, como as VPN, que fornecem ligações ponto a ponto, utilizando protocolos de túnel com funcionalidades de segurança e encriptação. Ao nível da camada IP, podem ser utilizados IPSec, que implementam mecanismos de segurança e encriptação dos pacotes IP da comunicação. Por fim, ao nível da camada de aplicação, podem ser utilizados protocolos de transporte encriptados, como o *Secure Sockets Layer* (SSL) [RFC6101] e o TLS, ou protocolos de transporte seguros para comunicações VoIP, SRTP, *Secure Real-time Control Protocol* (SRTCP) e o ZRTP, que se destinam a fornecer autenticação, integridade e encriptação à comunicação.

A utilização de protocolos de transporte seguros para comunicações VoIP, como o SRTP e o SRTCP, é a escolha natural para o reforço da segurança. Esta preferência deve-se ao facto de estes protocolos não introduzirem alterações profundas no paradigma de funcionamento e permitirem a escalabilidade da plataforma, sem prejuízo da qualidade de experiência do utilizador final. As alterações ao nível da camada de rede e da camada IP não são, por norma, suportadas pelos dispositivos móveis e são tendencialmente prejudiciais para a comunicação, introduzindo aumentos no atraso, *jitter* e consequentemente perdas de QoS e QoE.

A utilização de mecanismos de segurança e encriptação, como já foi descrito, contribui, por si só, para um aumento da privacidade, porém, não a elimina totalmente. Os classificadores de tráfego mais básicos, com base em análise de portos ou protocolos, podem funcionar para algumas aplicações, mas são facilmente evitados com o recurso a portos aleatórios ou encriptação. No entanto, após um estudo alargado, apresentado no capítulo anterior, verificou-se que existem várias técnicas e mecanismos que permitem detetar o tráfego VoIP, mesmo quando este usa canais seguros ou encriptados. Estes classificadores recorrem a parâmetros das aplicações e às métricas de rede, tentando encontrar padrões através da utilização de mecanismos baseados em estatística, heurística ou aprendizagem computacional. Grande parte dos classificadores recorre às métricas do tráfego VoIP como intervalos de transmissão, tamanhos ou débito de envio dos pacotes.

Para contornar os mecanismos de deteção e classificadores mais básicos, a Plataforma Nubitalk utiliza portos não normalizados e sustenta a comunicação com recurso a mecanismos de encriptação. Para lidar com os mecanismos de deteção e classificação mais sofisticados, existe a necessidade de alterar as métricas características do tráfego VoIP, injetar pacotes adicionais em intervalos aleatórios, alterando o débito e o intervalo entre os pacotes, assim como alterar o tamanho dos pacotes, através da agregação ou amostragem, o que torna mais difícil a identificação do tráfego. Ambas as soluções podem levar a um aumento de latência ou *jitter*, uma vez que estão a ser feitas alterações na comunicação.

## 3.4. Soluções Propostas de Suporte a Mecanismos de QoS e QoE

Um dos objetivos descritos no capítulo da Introdução consiste no suporte a mecanismos de QoS e QoE. Após o estudo da plataforma verificou-se a existência de várias limitações, ao nível da experiência para o utilizador e ao nível da informação do serviço.

Sendo um ponto forte da Plataforma Nubitalk a capacidade de integrar com os serviços e a infraestrutura dos operadores de comunicações, é de extrema importância proporcionar mecanismos autónomos que possuam as seguintes características: lidar com dispositivos de rede, que se interponham à passagem da comunicação, e permitir a interoperabilidade entre os dispositivos clientes incompatíveis. Para além das alterações descritas ao nível da experiência, existe a possibilidade de obter métricas de QoS da comunicação, que permitam medir o desempenho da plataforma a partir da perspetiva da rede, representando a capacidade desta para fornecer níveis de serviços.

Os dispositivos de rede que se interpõem à passagem da comunicação podem atuar ao nível da camada de aplicação, transporte ou de rede, bloqueando as comunicações. Habitualmente, estes encontram-se nos extremos das redes privadas, fazendo a ligação para a rede pública, como no caso dos *hotspots*. As configurações mais usadas permitem apenas a passagem de comunicação por canais de tráfego Web, bloqueando toda a restante comunicação. Para lidar com estes dispositivos, como a *Firewall*, existem várias técnicas já apresentadas no capítulo do Estado de Arte. A solução mais simples consiste em passar a comunicação por canais que se encontram abertos, alterando os dispositivos clientes e os servidores. No entanto, dando preferência a mecanismos autónomos à plataforma, ou seja, que possam ser introduzidos sem alterações de fundo na arquitetura, a utilização de técnicas de STUN/TURN e ICE apresenta uma solução mais viável. A Figura 21 ilustra a solução proposta.

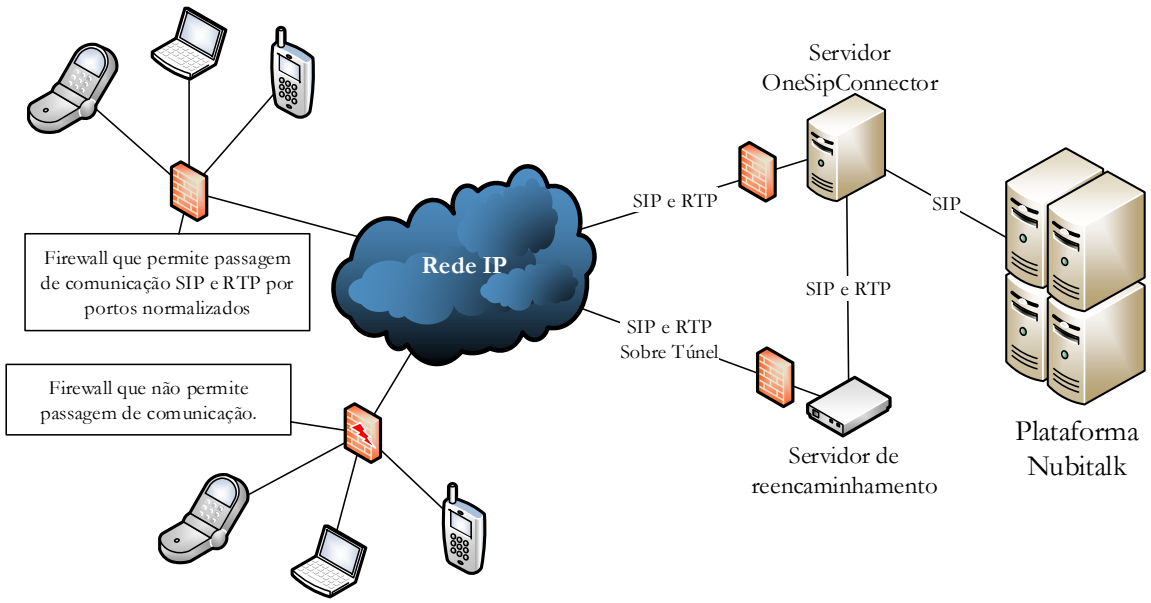



Figura 21 – Proposta de solução com mecanismos STUN/TURN

São utilizados servidores intermédios, com técnicas de STUN/TURN e ICE, que permitem a divisão da comunicação em duas partes distintas: uma, em que são usados portos e protocolos não normalizados, adaptando-se assim a comunicação aos dispositivos de rede; e uma segunda, na qual a comunicação é realizada pelos portos e protocolos normalizados. Para este fim, foi realizado um estudo a vários mecanismos de STUN/TURN, passando por bibliotecas até implementações de servidores completos, com o objetivo de avaliar várias soluções. As bibliotecas de desenvolvimento consideradas foram *reTurn* [ReTurn], *AnyFirewall* [AnyF], *Libnice* [Libnice] e *ice4j* [ICE4j]. Das várias implementações completas destacam-se as seguintes:

- *Restund* [Restund] é um servidor STUN e TURN modelar, com módulos autenticação, base de dados, estatísticas e relatórios; não tem documentação aceitável nem atualização correntes;

- *Numb* [Numb] é um serviço STUN e TURN disponibilizado após registo, que permite lidar com questões de NAT para a comunicação SIP, servindo como intermediário quando a comunicação direta não é possível;

- *TurnServer* [TurnS] é um servidor aberto de TURN, que suporta endereçamento IPv6 e comunicação, usando o protocolo TCP; apresenta boa documentação, no entanto, as atualizações não são correntes;

- *RFC5766-Turn-Server* [RFC5766TurnS] é um servidor STUN e TURN, que suporta endereçamento IPv6 e comunicação, usando o protocolo TCP, mecanismos de ICE e comunicação segura (TLS); apresenta boa documentação e atualizações correntes.

Para lidar com a incompatibilidade dos utilizadores que não se encontrem dentro do "domínio" da Plataforma Nubitalk, foi necessário introduzir mecanismos autónomos intermediários entre os vários clientes. Estes mecanismos permitem utilizar todas as funcionalidades adicionais da plataforma, sem impedir a comunicação entre os "utilizadores Nubitalk" e terceiros, suportando, assim, três cenários distintos.

O primeiro cenário é o das comunicações entre dois utilizadores localizados dentro do "domínio Nubitalk", ilustrado na Figura 22. Este cenário é o mais simples, uma vez que todos os clientes envolvidos utilizam a aplicação Nubitalk. Neste cenário, as chamadas são feitas sem a necessidade de mecanismos intermediários.

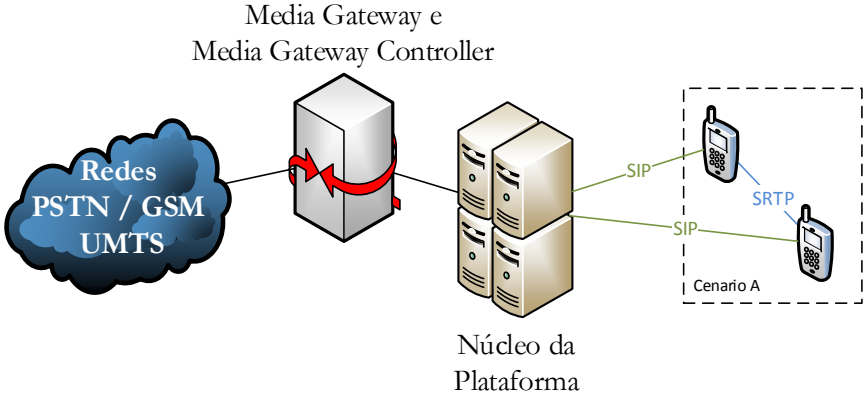



Figura 22 – Cenário A de comunicação VoIP

Há também o cenário das comunicações entre um utilizador localizado dentro do "domínio Nubitalk" e um "utilizador SIP" que use outro cliente de voz, ilustrado na Figura 23. Neste cenário, é tida em conta a necessidade de modificações na comunicação (*transcoding*). Usando mecanismos intermediários, como *Media Proxies,* é possível subdividir em duas partes a comunicação, permitindo assim o uso de diferentes configurações de chamada e CODECs para cada cliente.

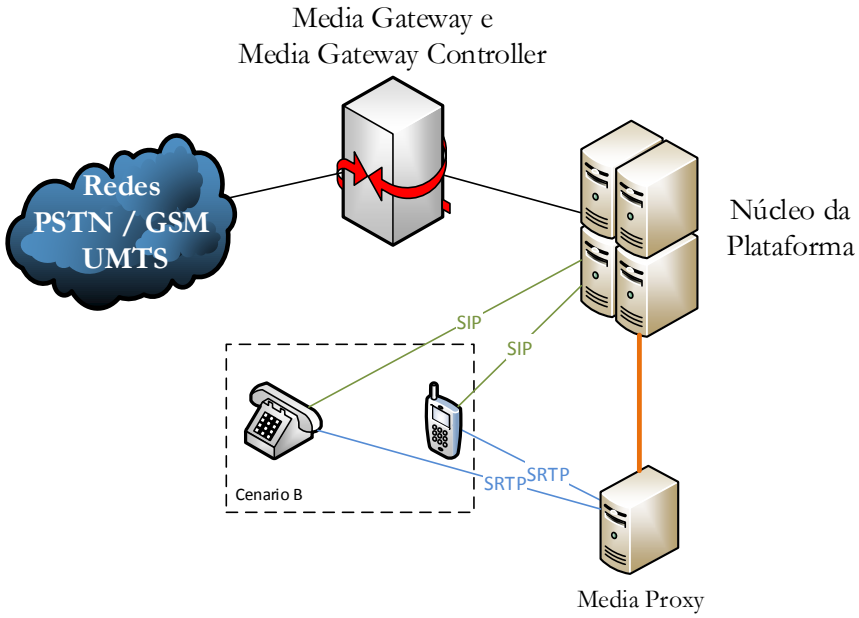



Figura 23 – Cenário B de comunicação VoIP

Por último, ilustrado na Figura 24, tem-se o cenário das comunicações entre um utilizador localizado dentro do "domínio Nubitalk" e um utilizador que esteja localizado numa rede pública, fixa ou móvel. Este cenário é semelhante ao cenário anterior. A diferença prende-se no facto de um dos clientes se encontrar por detrás de *Media Gateway*.

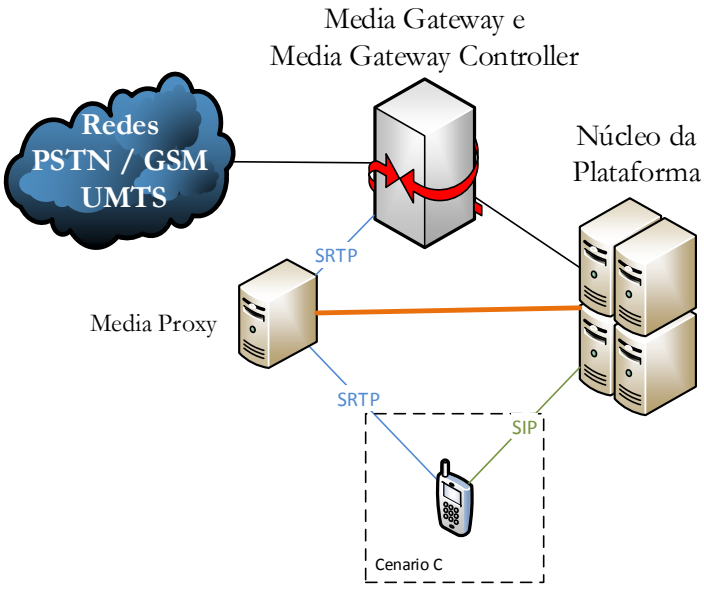



Figura 24 – Cenário C de comunicação VoIP

Para auxiliar a gestão dos mecanismos de *Media Proxy*, foi sugerida a utilização de mecanismos de gestão e balanceamento de carga, designado por Pool *Broker*. A Figura 25 seguinte ilustra o objetivo do mecanismo de *Pool Broker*.

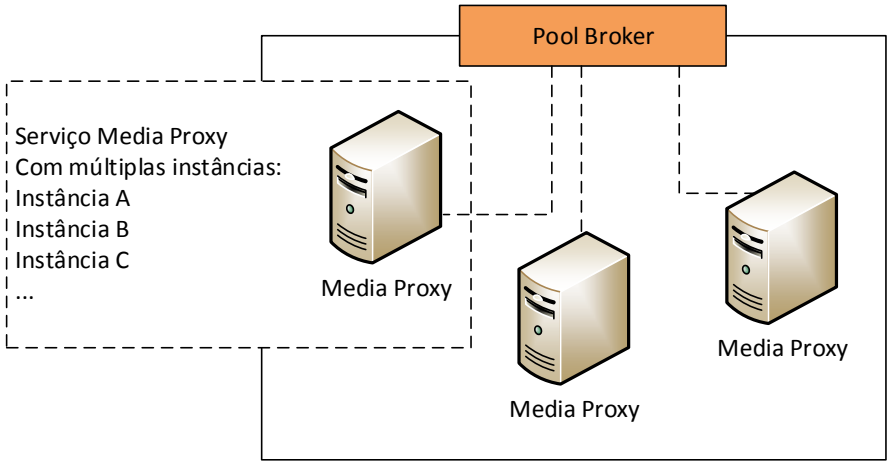



Figura 25 – Funcionamento do *Pool Broker*

Esta abordagem deu origem a várias arquiteturas, em que a diferença consistia no posicionamento do mecanismo, tendo em conta os restantes dispositivos de rede que são utilizados pela Plataforma Nubitalk. A primeira possibilidade coloca o *Pool Broker* juntamente com os dispositivos de rede, SBC. Em seguida, os *Media Proxy* são posicionados de modo a adquirir um endereço de IP público, como ilustrado na Figura 26. Esta arquitetura facilita a interligação dos clientes aos *Media Proxies* mas implica um uso de vários endereços IP públicos.

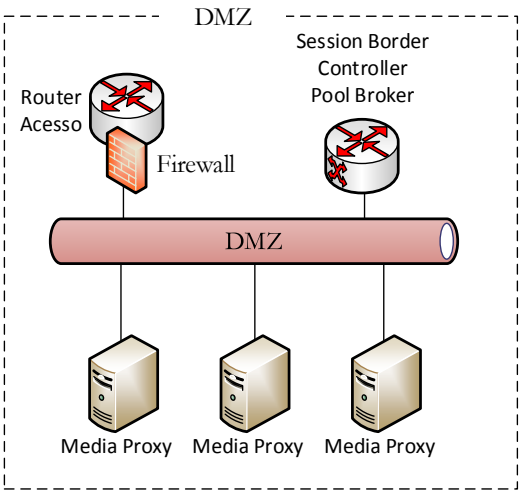



Figura 26 – Arquitetura da Plataforma Núbitalk cenário 1

Caso o número de endereços IP públicos fosse uma condicionante, outra arquitetura possível seria a utilização do *Pool Broker* como um mecanismo intermédio entre os clientes e os *Media Proxy*, eliminado assim a necessidade de vários endereços IP públicos, como ilustra a Figura 27. Esta solução introduz mais um elemento no caminho da comunicação, o que levar à degradação da QoS e QoE.

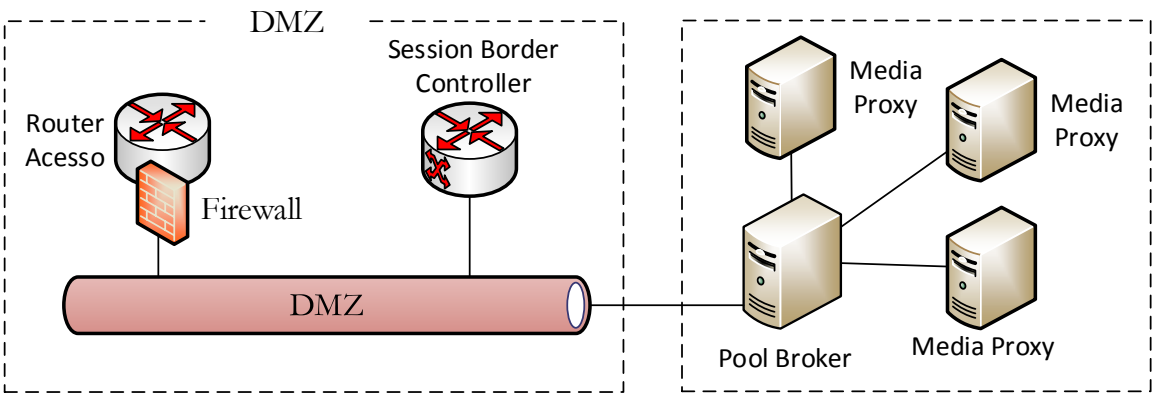



Figura 27 – Arquitetura da Plataforma Núbitalk cenário 2

Ambas as soluções apresentadas anteriormente têm que lidar com a presente arquitetura da Plataforma Nubitalk. Uma das suas condicionantes é a existência de mecanismos, como o SBC, para lidar com dispositivos de rede que implementam NAT. Estes dispositivos podem ser genéricos ou proprietários, o que levanta questões sobre a passagem de comunicação modificada com as funcionalidades que se desejam implementar. A Figura 28 ilustra a colocação dos *Media Proxy* tendo em conta os mecanismos de SBC.

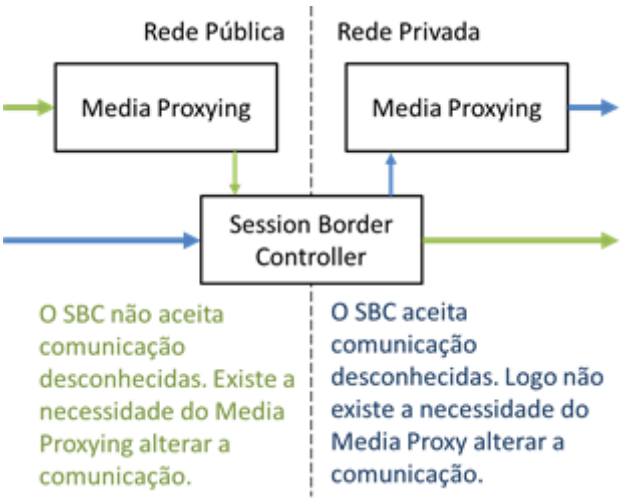



Figura 28 – Comunicação com SBC e *Media Proxy*

Por fim, foi sugerida a necessidade de obter métricas de QoS da comunicação, para medir o desempenho da plataforma a partir da perspetiva da rede. Esta alteração é realizada ao nível dos terminais clientes, para a obtenção das métricas, e ao nível dos servidores, para o armazenamento. O envio das métricas para o servidor pode ser realizado de várias formas: no final de cada chamada, é enviada a informação, fazendo um uso mais intensivo da rede de dados; após a realização de várias chamadas ou após o tamanho da informação ultrapassar um determinado limite é enviada a informação, fazendo desta maneira um uso mais poupado da rede de dados.

## 3.5. Enquadramento na Estratégia do Parceiro de Projeto

A seguir ao estudo dos vários pontos fracos da Plataforma Nubitalk e a uma apresentação de várias soluções propostas, foi realizada uma reunião presencial com o parceiro do projeto Nubitalk, a Collab. Esta reunião realizou-se no final da primeira fase de trabalhos da dissertação com o objetivo de avaliar as soluções propostas, identificando as que seriam implementadas, a fim de se proceder ao início da segunda fase de trabalhos.

Da perspetiva do parceiro de projeto, as soluções que envolvessem modificações ao nível do paradigma de funcionamento, quer pela introdução de extensões aos elementos da plataforma, quer pela alteração profunda da comunicação, foram tidas em consideração, mas rejeitadas para serem implementadas. O código fonte do servidor *OnePBX* e *OneSIPConnector* não foi fornecido, pelo que, em ambos, nenhuma modificação podia ser realizada. Ao nível do cliente Nubitalk, apenas foi fornecido código fonte de uma versão antiga com o intuito das alterações serem modelares, ou seja, fáceis de aplicar em versões mais recentes.

Das várias soluções propostas, a Collab considerou prioritárias para a implementação do contorno de dispositivos de rede que se interpõem à passagem da comunicação, as propostas de alterações à comunicação, tornando-a mais evasiva, e mecanismos auxiliares de obtenção das métricas de QoS das chamadas. O contorno de dispositivos de rede que bloqueiam a comunicação, apesar de se encontrar descrito nas soluções propostas, foi um pedido feito pela Collab no decorrer da reunião, tendo sido a introdução desta proposta apenas considerada na segunda fase dos trabalhos da dissertação.

Da perspetiva da dissertação, as alterações, tanto do reforço de segurança e privacidade, como do suporte de mecanismos de QoS e QoE, ao nível dos servidores *OnePBX* e *OneSIPConnetor*, encontravam-se fora do âmbito do trabalho, pois iriam consumir grande parte dos recursos e levavam à necessidade de uma análise mais profunda e detalhada dos elementos da plataforma. Assim, as contribuições da dissertação para o projeto Nubitalk foram as seguintes:

- A contribuição principal consistiu na implementação das soluções escolhidas pela Collab, sob a forma de código desenvolvido modelarmente, ou seja, que permitia a sua inserção em versões mais recentes com o mínimo de esforço, e sob a forma de componentes adicionais à plataforma, permitindo a sua instalação e mantendo a sua compatibilidade com a plataforma base;

- Outra contribuição consistiu nas propostas das várias soluções, que, por escolha da Collab, não foram consideradas para implementação, visto que continham alterações mais profundas aos elementos que constituíam o núcleo da Plataforma Nubitalk;

- Por fim, foram apresentados conceitos e conhecimentos práticos que podem ser utilizados futuramente nas novas versões da Plataforma Nubitalk; esta contribuição engloba o estudo feito a mecanismos de deteção e classificação de tráfego VoIP, identificando os parâmetros das aplicações e as métricas do tráfego mais relevantes, e o estudo feito à comunicação da Plataforma Nubitalk, identificando o seu comportamento com configurações diferentes.

As soluções propostas que o parceiro de projeto considerou válidas e, tendo em vista o tempo já consumido para a análise detalhada das várias soluções, foram atribuídos os desenvolvimentos na recolha de métricas QoS e respetivo envio para a base de dados a outro investigador do LCT (Vítor Fonseca). Esta dissertação irá incidir, ao nível dos desenvolvimentos, avaliação, testes e resultados, sobre o contorno aos mecanismos de bloqueio e as alterações da comunicação para lidar com os mecanismos de deteção e classificação.

## 3.6. Metodologia

A metodologia de pesquisa e conceção científica (DSR - *Design Science Research*) [Hevner2004] é uma metodologia que tem como objetivo produzir aprendizagem, como consequência de pesquisa científica, ou seja, resolver problemas com o intuito de produzir aprendizagem. Esta metodologia caracteriza-se pelo processo de iteração das fases que a compõem, diferenciando-se das metodologias de investigação mais convencionais devido ao papel da conceção. No DSR, a conceção é importante na avaliação das teorias mas também no seu desenvolvimento.

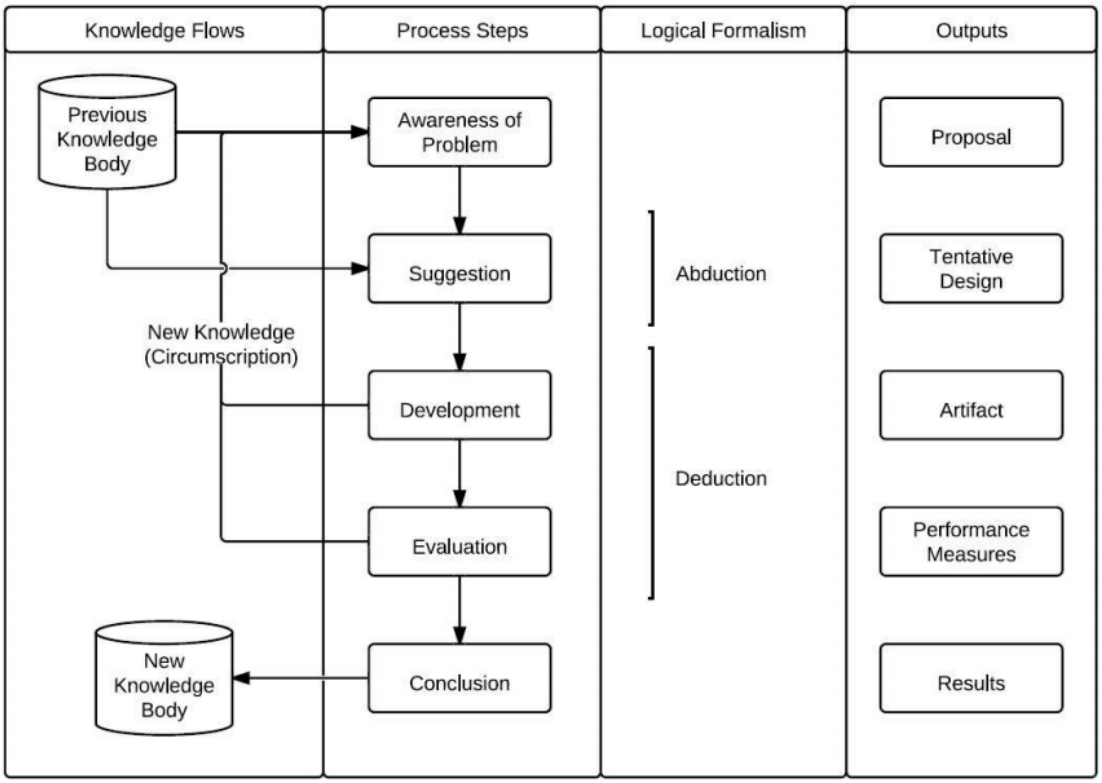



Figura 29 – Diagrama do DSR (retirado de [Hevner2004])

A metodologia DSR pode ser utilizada em várias áreas desde que a conceção seja possível. Esta é composta por cinco fases, como ilustrado na Figura 29.

- Descoberta do problema: compreende a definição e a identificação de um problema. O estado da arte é o resultado desta fase, que ajuda na contribuição da identificação e definição do problema.

- Proposta de resolução: corresponde à criação de uma solução para o problema que é concebida a partir do estado da arte e investigação anteriormente realizada. Desta fase resultam os modelos conceptuais e arquitetura de *software*.

- Desenvolvimento/prototipagem: representa o desenvolvimento real. Nesta etapa é produzido *software* a partir dos modelos e da arquitetura criada na fase anterior. O resultado desta fase representa uma prova de conceito, demonstrando que a solução é possível.

- Validação: como o próprio nome indica, é a validação do protótipo criado na etapa anterior, utilizando modelos de validação. Se estes não existirem podem ser concebidos na fase da proposta de resolução. Esta fase fornece feedback para as fases anteriores, o que permite um desenvolvimento iterativo e incremental.

- Conclusão: esta fase corresponde à conclusão do projeto. É neste momento que é produzido novo conhecimento sobre o problema, solução e modelos, protótipos e resultados.

Esta metodologia é adequada para o projeto, tanto de um ponto de vista global, como para os objetivos individuais, pois permite o fácil e ágil desenvolvimento das metas a alcançar. A metodologia DSR pode ser utilizada tendo em conta os objetivos transversais da Plataforma Nubitalk ou individualmente para as várias soluções propostas, dado que não se sobrepõem uma à outra.

Para além da metodologia já descrita, dentro de cada grupo de trabalho eram realizadas reuniões semanais com o objetivo de avaliar e rever o progresso das tarefas ativas e o planeamento das tarefas seguintes. Este método permitia um melhor acompanhamento do estado global do projeto e do trabalho realizado pelos vários elementos, assim como favorecia a ação de brainstorming. Para a comunicação entre os vários parceiros eram realizadas conferências quinzenais, nas quais se apresentava o ponto de situação do estado trabalho de cada grupo e eram avaliadas as decisões mais críticas relativamente aos desafios encontrados nas várias tarefas.

Além das metodologias aqui assinaladas, o grupo manteve um repositório documental com acesso partilhado, baseado na ferramenta *Basic Support for Cooperative Work* (BSCW) [BSCW], ilustrado na Figura 30.

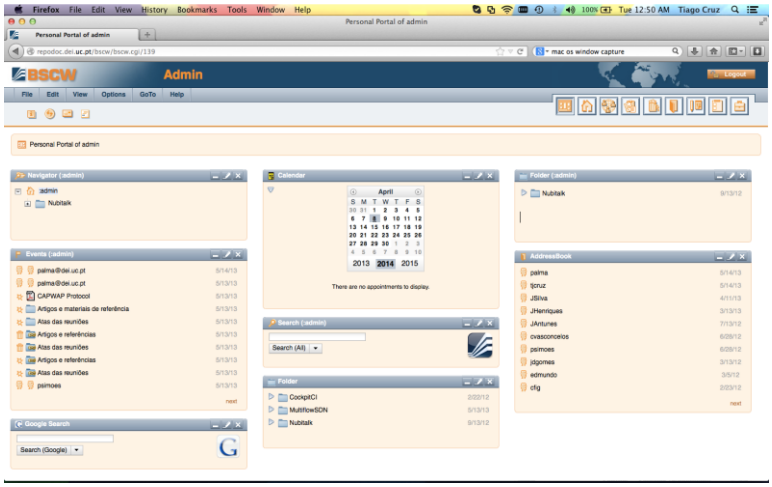



Figura 30 – Ferramenta *Basic Support for Cooperative Work* (BSCW)

O *software* BSCW é uma ferramenta de trabalho cooperativa desenvolvida pela Fraunhofer Society que suporta um conjunto de características, entre as quais se destacam os calendários partilhados e a gestão documental, com suporte para versões. Este repositório foi complementado por um servidor Subversion (SVN) para gestão e controlo de revisões, ao nível do código, permitindo o trabalho concorrente das equipas de desenvolvimento sobre uma mesma base de código gerida e organizada de forma estruturada.

## 3.7. Calendarização

A calendarização da dissertação foi dividida em duas fases distintas. A primeira consistiu no estudo e avaliação dos componentes da Plataforma Nubitalk, com as propostas de melhorias e desenvolvimentos, a serem avaliadas pela Collab. A segunda fase consistiu, para o restante período de trabalho, na restruturação e implementação das opções escolhidas. O planeamento do trabalho encontra-se descrito no Anexo A, apresentado num diagrama de Gantt, estando descrito de forma sucinta a seguir.

1) Planeamento para a primeira fase do trabalho:
   a) Integração com o projeto Nubitalk. Esta fase é de adaptação ao projeto e à Plataforma Nubitalk.

   b) Análise da comunicação e dos componentes relevantes para a mesma da Plataforma Nubitalk. Esta fase corresponde a uma compreensão do funcionamento da plataforma com ênfase na identificação dos pontos fracos.

   c) Criação de um Estado de Arte. Nesta fase foi pretendido um estudo alargado dos vários temas resultantes do ponto anterior e da análise da plataforma. O objetivo desta fase é desenvolver conhecimento sólido sobre o tema da dissertação.

   d) Definição dos objetivos e propostas de desenvolvimentos tendo em conta os pontos fracos identificados sobre a plataforma. Esta fase corresponde à apresentação de propostas de implementação, com detalhe das modificações a implementar e das ferramentas a utilizar.

   e) Apresentação das alterações ao parceiro do projeto, Collab, a fim de se compreender das várias propostas, quais as que deviam ser implementadas. Esta fase também tem o objetivo de validar o planeamento do trabalho para a segunda fase.

   f) Escrita da documentação sobre a primeira fase do trabalho, contendo a informação dos vários elementos anteriormente descritos. Nesta fase, está incluída a criação de um artigo científico que depois foi submetido a uma conferência.

2) Planeamento para a segunda fase do trabalho:
   a) Apreciação das considerações e escolha das soluções propostas, após a reunião com o parceiro de trabalho.

   b) Desenvolvimento e implementação das propostas escolhidas, para a Plataforma Nubitalk. Esta fase compreende os desenvolvimentos ao nível da segurança e privacidade o suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência.

c) Testes de validação às propostas. Esta fase corresponde aos testes de validação das implementações, usando para esse fim várias ferramentas e uma banca de testes.

d) Escrita do relatório final da Dissertação e de outro artigo científico, assim como a documentação oficial para o projeto Nubitalk.

Ao nível do planeamento e tendo em conta possíveis atrasos, foram incluídos alguns dias extra, em ambas as fases do trabalho, aos quais não foram atribuídas tarefas. Assim, é possível lidar com atrasos ou modificações necessárias ao planeamento previsto inicialmente. Também para lidar com potenciais imprevistos, algumas das tarefas da segunda fase já foram iniciadas a fim de detetar eventuais alterações. É importante mencionar que a entrega final da dissertação foi adiada para Setembro por vários motivos. No final da primeira fase do plano de trabalhos, após a reunião com o parceiro de projeto a Collab e por escolha deste, foram inseridos novos desenvolvimentos e foram alteradas as prioridades das já existentes, já com algumas implementações em progresso. Também existiu a necessidade de apoiar alguns aspetos do projeto Nubitalk, alheios à dissertação, mais concretamente a realização de documentações oficiais e relatório finais para as entidades do QREN e ao Instituto de Apoio às Pequenas e Médias Empresas e à Inovação (IAPMEI).

# Capítulo 4
# Trabalho Desenvolvido

O capítulo quatro pretende dar uma visão do trabalho realizado ao longo da dissertação, tendo especial atenção às fases de desenvolvimento. Este inicia com a fase de estudo da Plataforma Nubitalk, passa pela descrição do ambiente de desenvolvimento e termina com os desenvolvimentos para o reforço da segurança e privacidade e os desenvolvimentos de suporte de mecanismos de QoS e QoE.

## 4.1. Estudo e Análise da Plataforma Nubitalk

O primeiro passo consistiu em analisar de forma geral a Plataforma Nubitalk, ao nível da comunicação de rede e dos protocolos usados. Tendo em vista os objetivos referentes ao reforço da segurança e privacidade e ao suporte de mecanismos de QoS e QoE, foram identificados vários pontos fracos ao nível da segurança e privacidade na comunicação, deficiências ao nível da experiência de utilização e melhoramentos possíveis ao suporte de mecanismos auxiliares à QoS.

Após a fase anterior e consecutiva identificação dos problemas, procedeu-se ao seu estudo, bem como à elaboração de várias soluções propostas. Desta fase, resultou o conhecimento exposto no capítulo do Estado De Arte, assim como a descrição de várias soluções, encontradas em detalhe no capítulo anterior. Estas soluções foram apresentadas ao parceiro do projeto, a Collab, de forma a serem avaliadas e a se proceder à identificação das que iriam ser implementadas. Desta apresentação, resultou a introdução de novos problemas a lidar, ajustes necessários às propostas apresentadas e a escolha das implementações a serem realizadas na segunda fase dos trabalhos da dissertação.

## 4.2. Ambiente de Desenvolvimento

Os desenvolvimentos relativos à Plataforma Nubitalk focaram-se ao nível do cliente e da introdução de novos serviços. Para a alteração dos elementos da plataforma, que foram disponibilizados pela Collab, foi necessário uma adaptação às ferramentas e ambientes de desenvolvimento, mais concretamente ao sistema operativo iOS. A ferramenta de desenvolvimento usada para este sistema operativo foi o Xcode, necessária para desenvolver aplicações para dispositivos móveis iPhone.

Ao mesmo tempo da adaptação ao ambiente de desenvolvimento e às ferramentas utilizadas, foi necessária uma compreensão das bibliotecas usadas pelo cliente Nubitalk. Para a comunicação VoIP, é utilizado o protocolo SIP, sendo suportado e implementado pela biblioteca PJSIP [PJSIP]. O PJSIP é uma biblioteca livre e aberta, orientada à comunicação multimédia, que implementa protocolos normalizados como SIP, SDP, RTP, STUN, TURN e ICE. Esta biblioteca combina o protocolo de sinalização com uma *framework* rica em funcionalidades de multimédia e de mecanismos transversais ao NAT. A biblioteca tem suporte para áudio, vídeo, presença e mensagens instantâneas, tendo uma documentação extensa e atualizações regulares.

Para além das adaptações já descritas, procedeu-se à compreensão do funcionamento da comunicação VoIP, tanto ao nível da sinalização como ao nível do transporte, tendo em conta o modelo lógico implementado pela Plataforma Nubitalk. Neste modelo, a comunicação da sinalização e do transporte passam pelo servidor, sendo sempre utilizado na sinalização o servidor *OnePBX* como intermediário, enquanto a componente do transporte de voz e vídeo, pode ser realizada tanto com recurso a um mecanismo intermédio, como pode ser realizada diretamente entre ambos os clientes, de ponto a ponto, caso ambos possuam compatibilidade.

Finalmente, procedeu-se à implementação da bancada de testes, para a realização dos procedimentos de avaliação e de testes das soluções implementadas. Esta bancada de testes era composta pelos elementos básicos necessários à comunicação VoIP, vários clientes situados em redes com características diferentes e por mecanismos de *probing,* para inspecionar o tráfego de rede. No capítulo seguinte, encontra-se com um maior nível de detalhe a descrição do ambiente e dos elementos que constituem a bancada de testes.

## 4.3. Desenvolvitos de Reforço da Segurança e Privacidade

Para lidar com os desenvolvimentos referentes ao reforço da segurança e privacidade foram propostas várias soluções. Para a segurança, as propostas consistiam em utilizar técnicas de encriptação ou protocolos seguros. Por sua vez, as propostas para a privacidade consistiam em analisar alterações a parâmetros de tráfego ou a comportamentos da comunicação, tornando-a mais evasiva às técnicas e mecanismos de deteção e classificação de tráfego.

Após a reunião com o parceiro de projeto, apenas a solução de analisar as alterações a parâmetros de tráfego ou a comportamentos da comunicação foi escolhida para ser implementada. Neste sentido, procedeu-se ao estudo e análise de técnicas e mecanismos de deteção e classificação de tráfego VoIP, com o intuito de identificar quais as características das aplicações e as métricas do tráfego de rede mais relevantes. A identificação destas métricas serviu para propor alterações à comunicação da plataforma, que iriam posteriormente ser implementadas. No entanto, algumas das características da plataforma, como a utilização de portos ou protocolos normalizados, não foram consideradas para serem alteradas por escolha do parceiro de projeto.

Após uma análise à biblioteca PJSIP, verificou-se que se poderiam alterar as métricas do tráfego gerado pela comunicação, usando para esse fim os mecanismos de VAT ou as várias codificações existentes. A primeira implementação consistiu em usar os mecanismos de VAT, ou seja, mecanismos que permitem detetar ausência de fala e não enviar assim pacotes de dados, reduzindo o número de pacotes enviados. A segunda implementação consistiu em testar codificações diferentes, tentando identificar as que melhor se comportavam, tendo em conta as várias métricas características do tráfego VoIP. A fim de analisar as alterações e as implementações propostas, foram avaliados vários classificadores de tráfego genéricos, utilizados pelos mecanismos de *probing* da bancada de testes. Estes encontram-se descritos em detalhe no capítulo seguinte e serviram para avaliar o grau de deteção e classificação que as soluções implementadas apresentavam.

## 4.4. Desenvolvimentos de Suporte de Mecanismos de QoS e QoE

Para lidar com suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência foram propostas várias modificações. Para a melhoria da experiência de utilização da plataforma, foram propostas modificações ao nível dos canais de comunicação e introduções de mecanismos auxiliares intermédios, que permitiam realizar a comunicação entre clientes incompatíveis. Para os mecanismos de suporte ao QoS foram propostas alterações do cliente Nubitalk, a fim de obter as métricas da comunicação.

Após a reunião com o parceiro de projeto, as introduções de mecanismos auxiliares intermédios foram colocadas de parte, trocando a sua implementação pelo solucionamento das condicionantes dos dispositivos de rede aos canais de comunicação. Esta decisão teve como base a reclamação de vários utilizadores, que não conseguiam utilizar o cliente Nubitalk, quando situados atrás de dispositivos de rede que bloqueavam a comunicação. O pedido de resolução deste problema apenas foi apresentado durante a reunião com o parceiro de projeto, o que levou a uma alteração no plano de trabalhos. Quanto ao desenvolvimento dos mecanismos de suporte ao QoS, este foi considerado como válido, sendo a sua implementação realizada por outro elemento de grupo de trabalho.

Para o contorno dos dispositivos de rede, que introduziam bloqueios na comunicação, foram utilizados mecanismos intermédios de STUN/TURN. Neste sentido, foram analisadas várias implementações existentes dos mecanismos, apresentadas no capítulo anterior, e foi estudado a configuração mais correta para as mesmas. O cliente Nubitalk também foi alterado para poder comunicar diretamente com os mecanismos, sendo também necessário identificar a melhor configuração. A utilização da comunicação no porto 80 ou 443 e via o protocolo TCP foi a configuração mais adequada, tendo em conta as limitações impostas pelos dispositivos de rede. Existiram, no entanto, algumas limitações impostas pela biblioteca usada no cliente, o PJSIP, que não permitia a utilização de encriptação na comunicação, isto é, o suporte de protocolo TLS na comunicação entre o cliente e os mecanismos de STUN/TURN.

# Capítulo 5
# Validação, Testes e Resultados

Este capítulo pretende apresentar os mecanismos e procedimentos usados para a avaliação e testes das várias implementações propostas para esta dissertação. Para além da descrição já mencionada, este capítulo ainda apresenta os vários resultados obtidos no decorrer do plano de trabalho.

## 5.1. Validação

Para validar os desenvolvimentos, referentes aos objetivos estabelecidos para a dissertação, foram utilizadas várias técnicas e aplicações, que simulavam os cenários reais. Neste subcapítulo, é apresentado um estudo dos vários dispositivos, mecanismos e aplicações que foram tidos em conta, assim como uma comparação entre eles.

Para lidar com o reforço da segurança e privacidade, mais concretamente com os dispositivos de rede que se interpõem na comunicação, como, por exemplo, a Firewall, foi montado um cenário, no qual a validação era realizada recorrendo a dois processos. Inicialmente procedeu-se à configuração da Firewall das máquinas, no caso do cenário em causa, a configuração do mecanismo de iptables para o sistema operativo Linux, com a configuração semelhante à usada por dispositivos de rede, simulando assim os ambientes *hotspot*. Em seguida, foi usado um dispositivo comercial *router* sem fios, que utilizava uma configuração de *firmware* semelhante às usadas pelos dispositivos de redes de ambientes *hotspots*. Em ambos os cenários, os canais de comunicação usados permitiam apenas a passagem de tráfego usando o protocolo TCP e pelos portos 80 e 443. Estes cenários permitiram a realização de testes funcionais que foram complementados com uma avaliação de várias métricas de Qualidade de Serviço. Na realização dos vários testes foi usada a ferramenta Wireshark para verificar a passagem do tráfego pelas várias máquinas.

Para a validação do suporte de mecanismos de QoS e QoE, foram estudados vários mecanismos e técnicas de deteção e classificação de tráfego VoIP. Existem vários mecanismos de deteção de tráfego que aplicam múltiplas técnicas, seja em tempo real ou *off-line,* para fins estatísticos. Os mecanismos em tempo real, não só introduzem latências nas comunicações, como necessitam de elevado poder de processamento. A fim de contornar os mecanismos DPI, foram surgindo outras técnicas de classificações baseadas no tráfego gerado. Estas técnicas usam parâmetros como o tamanho, o débito e o intervalo de tempo dos pacotes, bem como métricas para determinar o funcionamento das aplicações e não necessitam do conhecimento prévio dos protocolos ou portos que são usados.

A maioria dos classificadores de tráfego comerciais emprega uma metodologia semelhante ao DPI. Esta escolha traz várias implicações, como já foi referido e pode criar estrangulamento nas redes com bastante tráfego. Por este motivo, foi feito um estudo a várias aplicações e foi dada preferência a ferramentas gratuitas e de código aberto. As ferramentas de classificação, mais relevantes, consideradas estão descritas a seguir.

- *CoralReef* [CReef] é um *software* que recolhe, analisa e monitoriza o tráfego da rede em tempo real ou de amostras. Esta aplicação analisa um interface à escolha do utilizador.

- *Filtro L7* [FL7] é um classificador de rede que identifica as aplicações com base na informação da camada de aplicação, ou seja, a informação dos pacotes. Baseia-se em sistemas de expressões regulares e funciona em sistemas baseados em Unix. Esta aplicação necessita de algum poder de processamento e recursos de memória.

- *TCP Statistic and Analysis Tool* (TStat) [TSTAT] é um *software* de classificação de tráfego de rede que gera diversos relatórios em tempo real: amostras e histogramas, entre outros. O TStat tem a capacidade de análise de fluxos de dados através de amostras TCP, assim como de protocolos RTP/RTCP.

- *Traffic Identification Engine* (TIE) [TIE] é um *software* de classificação de tráfego de rede que analisa tráfego em tempo real ou a partir de amostras, gerando amostras e relatórios web. Sendo uma ferramenta de código aberto, permite alterações a fim de implementar vários sistemas de classificação. Este *software* funciona em sistemas operativos baseados em Unix.

Foram realizados vários testes para verificar quais das várias ferramentas obtinham melhores resultados de deteção e usabilidade. O teste consistia em realizar comunicação VoIP, recorrendo às aplicações Skype e Nubitalk, com o objetivo de as detetar na rede. Dos vários *softwares* apresentados, os que mostraram ter melhores resultados de deteção foram o TIE e o TSTAT. Ao nível da usabilidade, a ferramenta de eleição foi o TIE, não só devido a sua facilidade de instalação, utilização e recolha de resultados, mas também à versatilidade dos mecanismos de deteção e classificação que esta suportava. A configuração permitia utilizar vários mecanismos de deteção e classificação, como o Filtro L7, permitindo assim melhores resultados.

## 5.3. Bancada de Testes

Para a realização da validação e dos testes das soluções implementadas, foi necessário criar uma Bancada de Testes. A Figura 31 ilustra o núcleo da plataforma simplificada, considerando que, para fins de testes, apenas havia a necessidade de conter o *OneSIPConnector*, o *OnePBX*, uma Base de Dados e um servidor de STUN/TURN.

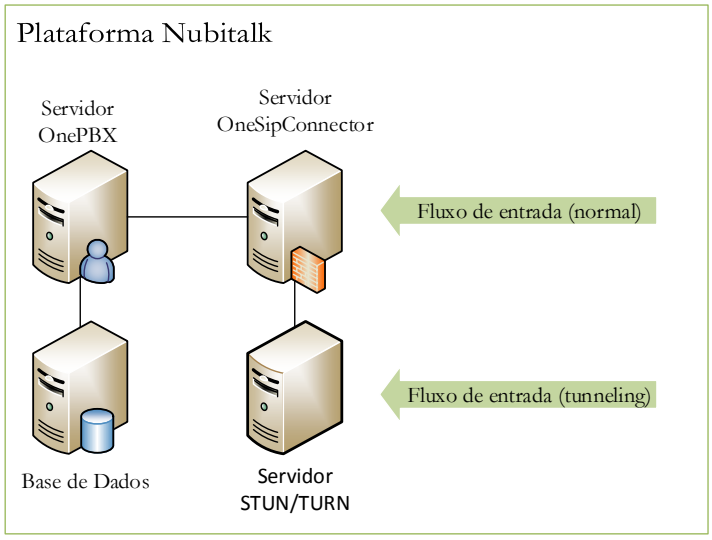



Figura 31 – Núcleo da Plataforma Nubitalk no ambiente de teste

A Figura 32 ilustra o cenário de testes, no qual se integra o núcleo anteriormente descrito, e que foi montado para a realização das validações e dos testes. A bancada de testes é composta pelos elementos que se seguem.

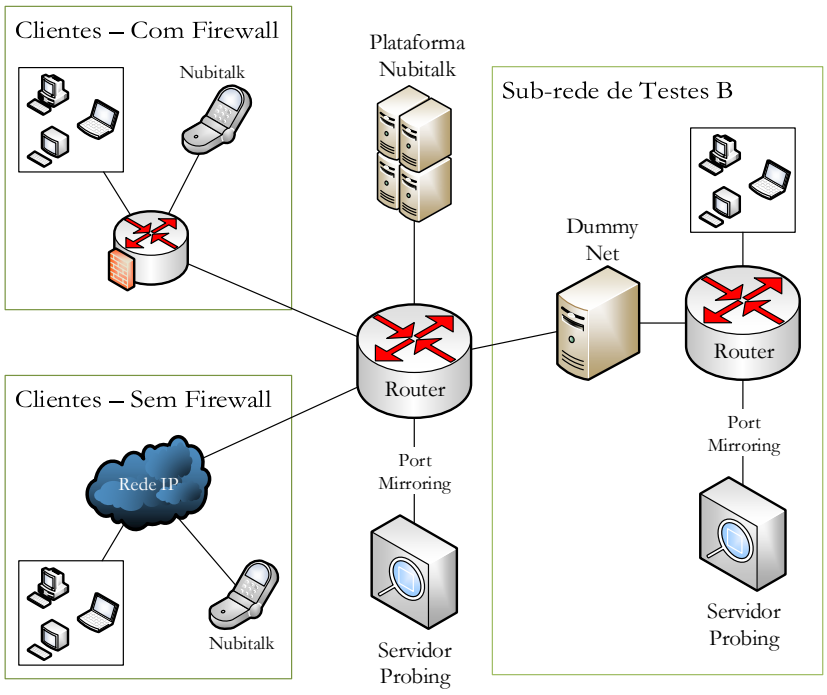



Figura 32 – Bancada de Testes

A plataforma Nubitalk representa os elementos do núcleo da plataforma necessários para a realização da validação e dos testes. Para além dos elementos base, este componente também tem um servidor de STUN/TURN, com as implementações TurnServer e RFC5766-Turn-Server descrita na secção do desenvolvimento.

Os servidores de *Probing* representam máquinas contendo aplicações de inspeção e deteção de tráfego de rede. Estas aplicações recebem uma cópia do tráfego passado na rede (*Port Mirroring*) e têm aplicações de deteção e classificação de tráfego, Wireshark, TIE e TSTAT. Estas máquinas servem para simular os mecanismos de deteção e classificação de tráfego de rede, sem as desvantagens de aumentar as latências na comunicação.

Os clientes VoIP representam os clientes VoIP da Plataforma Nubitalk e de dispositivos fixos, como *desktops*. Existem dois cenários diferentes, em que os clientes se encontram: sem recurso a mecanismos de rede limitadores, nos quais não existe nenhum impedimento à comunicação, e com recurso a mecanismos de rede limitadores, sendo exemplo disso uma Firewall, nos quais a comunicação é realizada apenas por alguns canais de comunicação, simulando assim ambientes como *hotspots*.

Para além do cenário já descrito, foi montado uma segunda rede de testes, Sub-Rede de Testes B, constituído por um servidor de *Probing*, um cliente VoIP e um servidor DummyNet [DNET]. O objetivo desta sub-rede era poder simular degradações de rede, usando para isso o servidor DummyNet. No entanto, após a reunião com os parceiros de trabalho verificou-se, e tendo em vista os desenvolvimentos desta dissertação, que não iriam ser usados mecanismos de degradação nos testes a realizar.

## 5.3. Testes e Resultados

Após a realização da validação, descritas anteriormente, foram realizados testes comparativos. O objetivo destes era dar uma visão, ao nível das métricas da rede, da introdução de mecanismos ou alteração da configuração da comunicação. Não foram realizados testes de carga, performance, escalabilidade ou testes relativos à QoE (*Mean Opinion Score* (MOS) [ITUTMOS] ou *Perceptual Evaluation of Speech Quality* (PESQ) [ITUTPESQ]) visto que estes não se encontravam no âmbito da Dissertação.

As métricas apresentadas na realização dos testes são obtidas pelo cliente móvel Nubitalk. A biblioteca usada disponibiliza as métricas por chamada, para o número de pacotes (total de pacotes, tamanho dos pacotes, pacotes descartados, pacotes perdidos), os valores de *jitter* (máximo, mínimo, média) e os valores de *Round-Trip Time* (RTT) (máximo, mínimo, média). Estes valores eram apresentados do ponto de vista da transmissão (Tx) e receção (Rx).

Das métricas obtidas as mais relevantes para as aplicações VoIP são a perca de pacotes e o *jitter*. O aumento da perca de pacotes tem um impacto negativo sobre o desempenho da aplicação, enquanto o *jitter* representa a variação do atraso entre os pacotes enviados. Para a obtenção dos resultados foram realizadas várias chamadas, com a duração de cinco a seis minutos cada, que foram repetidas até que os resultados fossem conclusivos. As tabelas com os valores obtidos encontram-se apresentadas em detalhe no Anexo C.

### Resultados dos Reforço da Segurança e Privacidade

Para lidar com os desenvolvimentos referentes ao reforço da privacidade foram testadas várias abordagens. Os primeiros testes apresentam os resultados das métricas da utilização de mecanismos de VAT, enquanto os segundos testes apresentam os resultados das métricas usando codificações diferentes. Estes são comparados com a comunicação normal, no qual a aplicação escolhe a codificação a usar de uma lista. Todos os testes foram acompanhados pela utilização dos classificadores genéricos, que se encontravam colocados no serviço de *probing*.

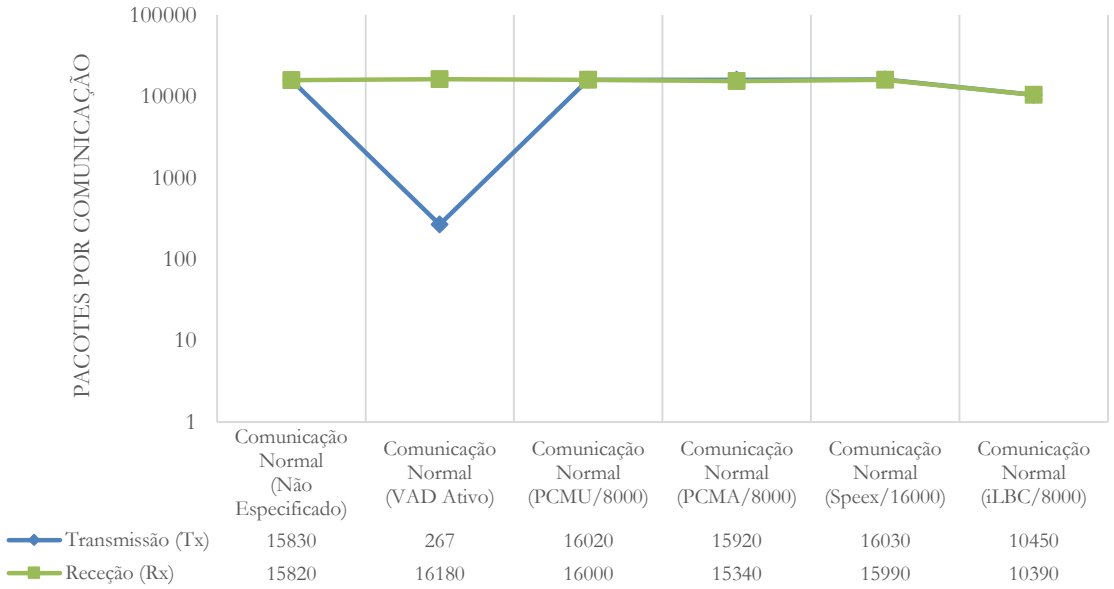
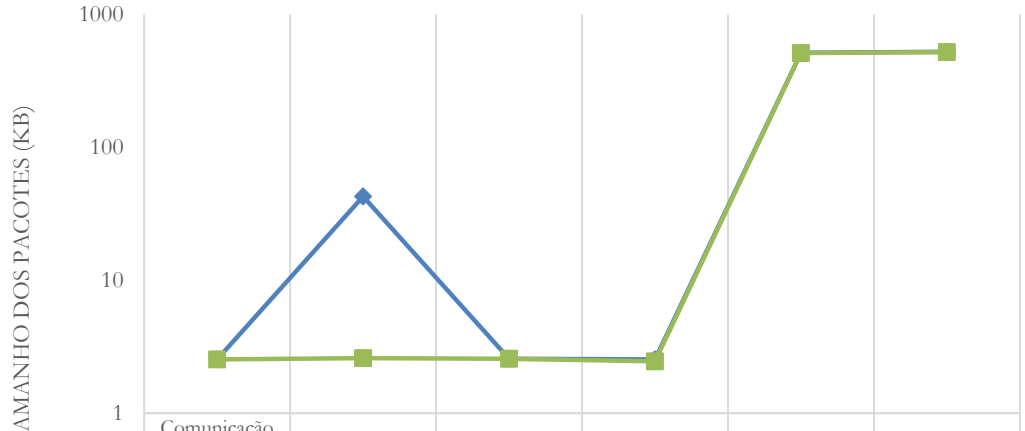
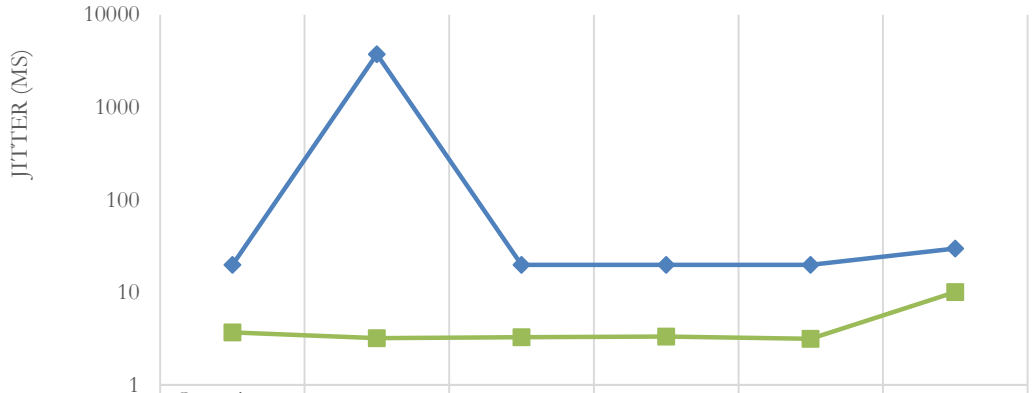



Figura 33 – Média de pacotes por chamada.




| | Comunicação Normal (Não Especificado) | Comunicação Normal (VAD Ativo) | Comunicação Normal (PCMU/8000) | Comunicação Normal (PCMA/8000) | Comunicação Normal (Speex/16000) | Comunicação Normal (iLBC/8000) |
|---|---|---|---|---|---|---|
| Transmissão (Tx) | 2,535 | 42,690 | 2,568 | 2,545 | 514,62 | 525,080 |
| Receção (Rx) | 2,533 | 2,593 | 2,567 | 2,453 | 513,49 | 522,340 |

Figura 34 – Tamanho médio dos pacotes (KB)




| | Comunicação Normal (Não Especificado) | Comunicação Normal (VAD Ativo) | Comunicação Normal (PCMU/8000) | Comunicação Normal (PCMA/8000) | Comunicação Normal (Speex/16000) | Comunicação Normal (iLBC/8000) |
|---|---|---|---|---|---|---|
| Transmissão (Tx) | 19,897 | 3759,769 | 19,878 | 19,877 | 19,94 | 29,905 |
| Receção (Rx) | 3,694 | 3,201 | 3,294 | 3,337 | 3,16 | 10,081 |

Figura 35 – Valores médios de *jitter* (ms)

A partir do gráficos, ilustrados nas Figuras 33, 34 e 35, podemos verificar que a utilização de mecanismos de VAD ou CODECs, diferenciados, introduziram alterações ao nível do número e tamanho de pacotes. Os mecanismos de VAD reduzem o número de pacotes enviados e aumentam o tamanho destes, no entanto introduzem valores de *jitter* elevados. Ao nível da utilização de diferentes CODECs os valores do número de pacotes e do *jitter* não mostram alterações significativas. Os valores do tamanho dos pacotes no caso dos CODECs Speex e iLBC deveriam ser inferiores aos restantes, o que leva a pressupor a existência de um erro na obtenção das métricas. Não foram consideradas os resultados dos pacotes descartados e perdidos pois os valores não eram significativos. Para comunicação normalizada, a biblioteca PJSIP não apresentava valores de RTT.

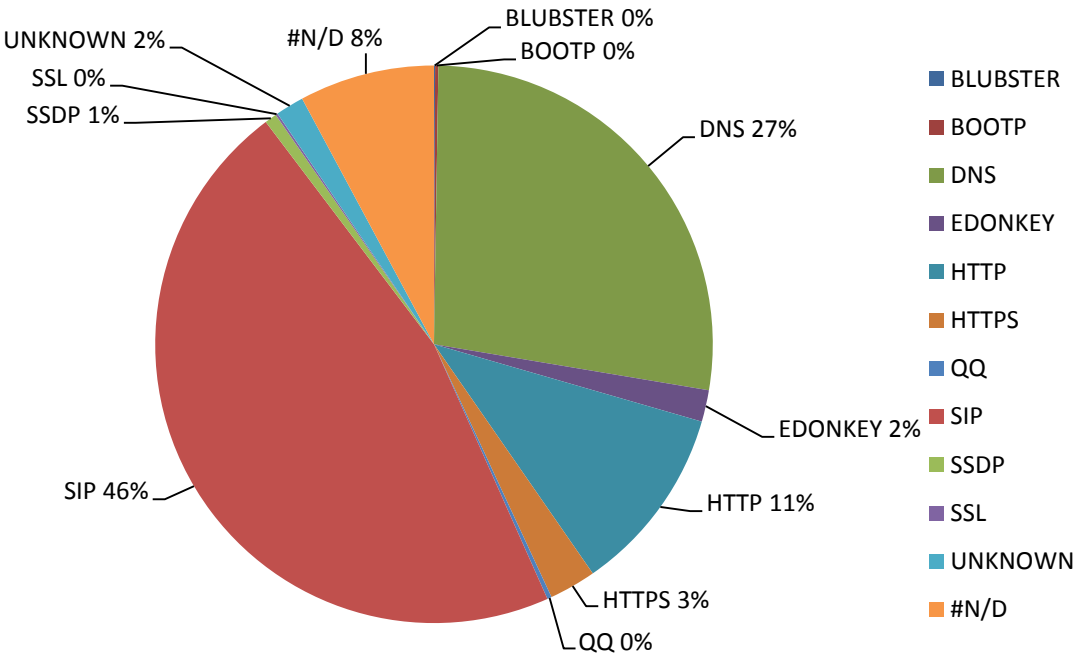



Figura 36 – Aplicações detetadas pelos classificadores

Ao nível das ferramentas utilizadas para a deteção e classificação, não foi visível a modificação dos valores obtidos sem as alterações propostas, ilustrados na Figura 36. Este cenário pode ficar a dever-se ao facto de não terem sido utilizados de portos aleatórios e protocolos encriptados com as alterações realizadas, sendo que as extensões aos classificadores possuíam informação de deteção dos portos e protocolos normalizados.

### Resultados dos Suporte de Mecanismos de QoS e QoE

Para o contorno dos dispositivos de rede, que introduziam bloqueios na comunicação, foi modificado o cliente para a comunicação passar pelo servidor RFC5766-Turn-Server. A este nível foram usadas duas configurações: a comunicação pelo porto 80 e suportadas pelo protocolo TCP, a comunicação pelo porto 80 suportada pelo protocolo UDP.

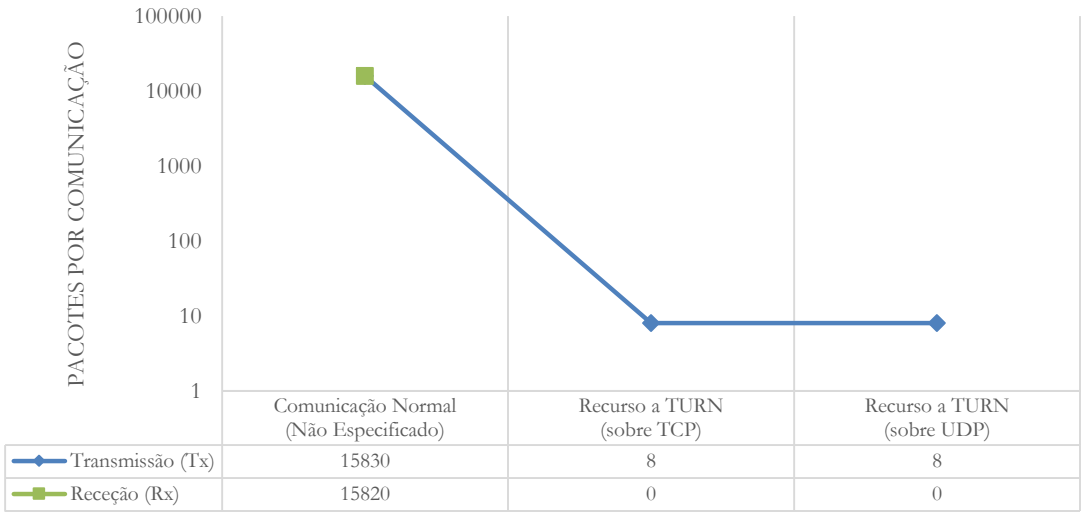
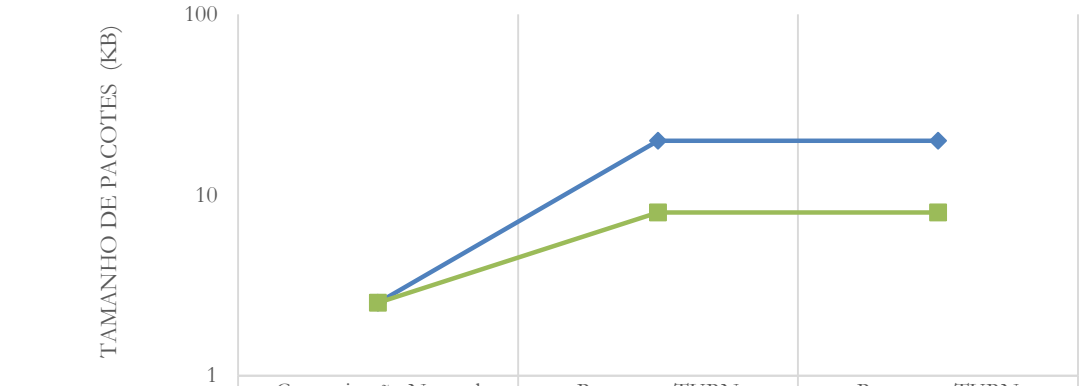
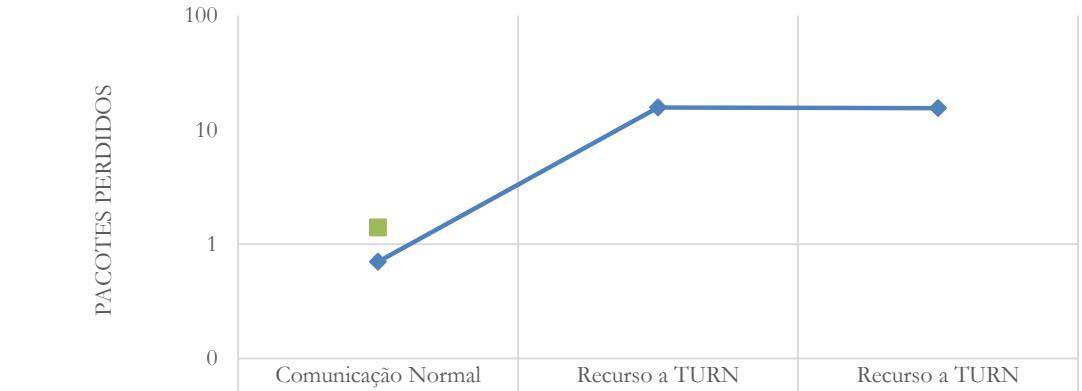



Figura 37 – Média de pacotes por chamada



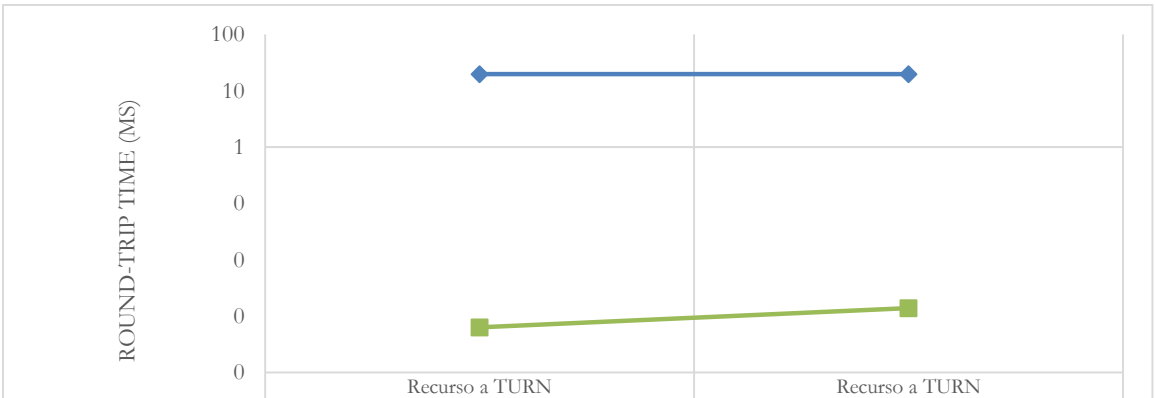

| | Comunicação Normal (Não Especificado) | Recurso a TURN (sobre TCP) | Recurso a TURN (sobre UDP) |
|---|---|---|---|
| Transmissão (Tx) | 2,535 | 20 | 20 |
| Receção (Rx) | 2,533 | 8 | 8 |

Figura 38 – Tamanho médio de pacotes (KB)




| | Comunicação Normal (Não Especificado) | Recurso a TURN (sobre TCP) | Recurso a TURN (sobre UDP) |
|---|---|---|---|
| Transmissão (Tx) | 1 | 16 | 16 |
| Receção (Rx) | 1 | 0 | 0 |

Figura 39 – Média de pacotes perdidos por chamada




| | Recurso a TURN (sobre TCP) | Recurso a TURN (sobre UDP) |
|---|---|---|
| Transmissão (Tx) | 19,875 | 19,876 |
| Receção (Rx) | 0,001 | 0,001 |

Figura 40 – Valores de médios de RTT (ms)

Os testes, ilustrados nas Figuras 37, 38, 39 e 40, realizados com o recurso de mecanismos intermédios (STUN/TURN) mostraram que o número de pacotes e o tamanho destes apresenta-se sempre constante para todas as chamadas. Estes valores devem-se à interpretação que a biblioteca PJSIP faz das ligações aos mecanismos intermédios, representando apenas o estabelecimento da ligação e não as métricas da comunicação de voz. Sendo que nas versões mais recentes da biblioteca já é possível obter métricas de QoS dos mecanismos STUN/TURN e ICE.

No entanto foram apresentados valores de RTT para a comunicação, sendo que estes não são suficientemente elevados para deteriorar a comunicação de voz. Outro resultado apresentou um aumento significativo na perca de pacotes, situação não detetada na comunicação sem recurso a mecanismos de STUN/TURN.

## 5.4. Artigos Científicos

Uma das etapas da dissertação consistiu em analisar em detalhe mecanismos e técnicas de deteção e classificação de tráfego VoIP. Esta análise resultou na aquisição de um leque de conhecimentos, o que levou à redação de artigos científicos sobre mecanismos de deteção e classificação de tráfego VoIP e técnicas de evasão. Após o desenvolvimento do Estado de Arte, foram escritos dois artigos científicos, que foram submetidos a conferências. Ambos os artigos encontram-se no Anexo B da dissertação.

O primeiro artigo [Fonseca2013] expõe um estudo sobre técnicas de deteção e classificação de tráfego para aplicações VoIP. Neste trabalho apresenta-se um estudo de técnicas de deteção e classificação de tráfego gerado por protocolos VoIP, com ênfase em duas categorias principais: com base no perfil de padrões de tráfego de rede e com base em modelos de fluxos de comunicação, para a deteção de anomalias; sendo em seguida discutidas algumas das técnicas mais populares dentro de cada um destes dois grupos. São também descritas técnicas clássicas, ainda que de forma mais sucinta. Este artigo foi submetido à 13ª Conferência sobre Redes de Computadores [CRC2013], na qual foi aceite como um resumo estendido. Um segundo artigo [Fonseca2014] também decorrente do Estado De Arte e do aprofundamento do artigo anterior foi submetido à 8ª conferência *Next Generation Mobile Apps, Services and Technologies* [NGMAST2014], na qual foi aceite como um artigo completo.

Para além dos artigos já mencionados, encontra-se em produção um terceiro artigo, com base nos resultados obtidos na realização da dissertação. Este trabalho apresenta as alterações realizadas ao nível da comunicação, para lidar com as técnicas e os mecanismos de deteção e classificação do tráfego VoIP e os resultados obtidos. Tendo em conta ambos os artigos anteriormente referidos e o capítulo do Estado De Arte, foram realizados várias modificações para permitir a alteração comportamental da aplicação cliente Nubitalk, focando os comportamentos da aplicação e as métricas do tráfego gerado mais relevantes para a sua deteção. Visto ainda se encontrar numa fase embrionária, o artigo ainda não foi submetido a nenhuma conferência.

# Capítulo 6
# Conclusão e Trabalho Futuro

Como já foi referido anteriormente, com a evolução das tecnologias surgiram novas gerações de redes e aplicações que tiram partido destas. As aplicações VoIP são um exemplo disto, permitindo a comunicação de voz de forma simples e com baixos custos para os utilizadores. No entanto, o facto da comunicação se realizar em ambientes de rede partilhada possibilita vários problemas intrínsecos a este tipo de redes. Para além destes problemas, também os provedores de serviços e operadoras de telecomunicações, afetados pela necessidade de manterem serviços de qualidade e pela diminuição das receitas tentam defender os seus modelos de negócio, por vezes, prejudicando o uso das aplicações VoIP.

A dissertação centra-se no reforço da segurança e privacidade e no suporte de mecanismos de Qualidade de Serviço e de Qualidade de Experiência. Tendo estes objetivos em mente, foram propostas várias soluções que contribuíram para o melhoramento e modificação a vários níveis da Plataforma Nubitalk. Destas, foram implementas e validadas várias soluções. Ao nível dos contributos para a Plataforma Nubitalk e para o parceiro de projeto, a dissertação atuou em várias frentes: primeiro foi desenvolvido código e módulos para lidar com vários problemas identificados, mantendo a compatibilidade com a plataforma base, em seguida foram apresentadas soluções para lidar com problemas que necessitavam de alterações ao núcleo da plataforma e finalmente, através de conceitos que podem ser usados futuramente em novas versões da plataforma.

Na realização da dissertação existiram algumas dificuldades, principalmente no que diz respeito ao planeamento da escolha das soluções a implementar. O parceiro de projeto no decorrer da dissertação alterou as prioridades das soluções propostas, tendo sido introduzidos novos desafios que necessitaram de um estudo. Estas alterações, com a condicionante de soluções compatíveis com a plataforma base, dificultaram e limitaram as implementações possíveis. Para além das condicionantes colocadas pelo parceiro de projeto, existiam limitações ao nível dos equipamentos utilizados. O cliente Nubitalk usado encontrava-se desenvolvido para iOS, um sistema operativo que limita os desenvolvimentos, e utilizava uma biblioteca para comunicações VoIP desatualizada, que não possui o suporte para muitas das funcionalidades necessárias implementas nas versões mais recentes.

De forma geral todos os objetivos foram cumpridos, apesar de algumas das soluções propostas não terem sido implementadas. Trabalhos futuros passam pelo desenvolvimento e alterações ao nível do núcleo da plataforma, sem a alteração do modelo de negócios, e pela introdução de novas funcionalidades inovadoras ao nível da codificação de voz e dos mecanismos de QoS e QoE. Também está a ser considerada a introdução do CODEC Opus [RFC6716] assim com o desenvolvimento do mecanismo E-Model [ITUTEMODEL] para o mesmo.

# Referências

[Alexander2009] A.L. Alexander, A.L. Wijesinha, e R. Karne, "An Evaluation of Secure Real-Time Transport Protocol (SRTP) Performance for VoIP" em Third International Conference on Network and System Security 95-101, 2009.

[Allot] Allot Inc, "Allot Netenforcer", http://www.allot.com/NetEnforcer_AC-500.html

[AntL] AntLabs Solutions, "Ant Lab", http://www.antlabs.com/

[AnyF] Eyeball Networks Inc, "AnyFirewall", http://www.anyfirewall.com/

[Arbor] Arbor Networks, "Arbor" http://www.arbornetworks.com/network-security-&-visibility-products.html

[Backes2013] M. Backes, G. Doychev, M. Dürmuth, e B. Köpf, "Speaker recognition in encrypted voice streams" em Computer Security, 2010.

[Barbieri2002] R. Barbieri, D. Bruschi e E. Rosti, "Voice over IPsec: analysis and solutions." em 18th Annual Computer Security Applications Conference 261-270, 2002.

[Biondi2005] P. Biondi e F. Desclaux, "Skype uncovered - Security study of Skype," EADS, 2005.

[Blue] Blue Coat Packetshapper, "BlueCoat", http://www.bluecoat.com/products/packetshaper/

[BSCW] Fraunhofer FIT e OrbiTeam Software, "Basic Support for Cooperative Work", https://public.bscw.de/pub/

[Chen2006] K. Chen, C. Huang, P. Huang, e C. Lei, "Quantifying Skype user satisfaction", em ACM SIGCOMM Computer Communication, vol. 36, 2006.

[Chuah2000] C. Chuah e R. Katz, "Statistical Analysis of Packet Voice Traffic in Internet Multimedia Applications", 2000.

[CISUC] Universidade de Coimbra, "Centre for Informatics and Systems", https://www.cisuc.uc.pt/

[Collab] Collab S.A., "Collab", http://www.collab.com/pt

[Collab2012] Collab S.A, "OnePBX and Nubitalk - Product Description", Lisboa, 2012

[CRC2013] 13ª Conferencia sobre Redes de Computadores, CRC 2013, http://crc2013.ipleiria.pt/, 2013.

[CReef] CAIDA, CoralReef Software Suit2, http://www.caida.org/tools/measurement/coralreef/.

[Cymp] Untangle Inc, "Cymphonix", http://www.cymphonix.com/

[DNet] The dummynet project, "Dummynet", http://info.iet.unipi.it/~luigi/dummynet/

[Exinda] Exinda Smarter WAN Optimization, "Exinda", http://go.exinda.com/SmarterWANOptimization.html

[FL7] Filtro L7, "Application Layer Packet Classifier for Linux", http://l7-filter.sourceforge.net/.

[Fonseca2013] H. Fonseca, E. Monteiro, P. Simões e T. Cruz, "Técnicas de detecção e classificação de tráfego para aplicações de Voz sobre IP (VoIP)", em 13ª Conferencia sobre Redes de Computadores, Novembro, 2013.

[Fonseca2014] H. Fonseca, E. Monteiro, P. Simões e T. Cruz, "A comparison of classification techniques for detection of VoIP traffic", submetido à IEEE Symposium on Computers and Communications, Janeiro, 2014.

[Freire2008] E. Freire, A. Ziviani e R. Salles, "Detecting VoIP Calls Hidden in Web Traffic," em IEEE TNSM, vol. 5, no. 4, 2008.

[Freire2009] E. Freire, A. Ronaldo e M. Salles, "On Metrics to Distinguish Skype Flows from HTTP Traffic," em J Netw Syst Manage 17:53-72, 2009.

[Gomes2012] J. Gomes, "Classification of Peer-to-Peer Traffic by Exploring the Heterogeneity of Traffic Features Through Entropy", Março, 2012.

[Goode2002] B. Goode, "Voice Over Internet Protocol (VoIP)", em Proceedings of the IEE, Vol. 90, N. 9, Setembro, 2002.

[GTalk] Google Inc, "Google Talk", http://www.google.com/hangouts/.

[Hevner2004] A. Hevner, S. March, J. Park, e S. Ram, "Design science in information systems research", em MIS Quarterly, Vol. 28, 2004.

[IANA] IANA, "Port numbers", http://www.iana.org/assignments/port-numbers.

[ICE4j] NLnet Foundation, "Ice4j", https://code.google.com/p/ice4j/

[Idrees2008] F. Idrees e U. Khan, "A Generic Technique for Voice over Internet Protocol (VoIP) Traffic Detection", em IJCSNS, 2008.

[ITUTEMODEL] ITU-T Recommendation E-Model, "The E-model: a computational model for use in transmission planning ", Fevereiro, 2014.

[ITUTG.711] ITU-T Recommendation G.711, "Pulse code modulation (PCM) of voice frequencies", Fevereiro, 2000.

[ITUTG.729] ITU-T Recommendation G.729, "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)", Junho, 2012.

[ITUTH.245] ITU-T Recommendation H.245, "Control protocol for multimedia communication", Maio, 2011.

[ITUTH.248] ITU-T Recommendation H.248.1, "Gateway control protocol: Version 3, Março, 2013.

[ITUTH.263] ITU-T Recommendation H.263, "Video coding for low bit rate communication", Janeiro, 2005.

[ITUTH.323] ITU-T Recommendation H.323, "Packet-based multimedia communications systems", Dezembro, 2009.

[ITUTMOS] ITU-T Recommendation P.800.1, "Mean Opinion Score (MOS) terminology", Julho, 2003.

[ITUTPESQ] ITU-T Recommendation P.862, "Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs", Fevereiro, 2001.

[Kang2007] H. Kang, L. Zhang, S. Ranjan e Nucci, "SIP-based VoIP traffic behavior profiling and its applications." em Proceedings of the 3rd annual ACM workshop on Mining network data, 2007.

[Khlifi2006] Hechmi Khlifi, Jean-Charles Grégoire, and James Phillips, "VoIP and NAT/Firewalls: Issues, Traversal Techniques, and a Real-World Solution", em IEEE Communications Magazine, Julho, 2006.

[Libnice] Farstream, "Libnice", http://nice.freedesktop.org/wiki/

[Meraki] Meraki Solutions, "Meraki", http://www.meraki.com/

[NetE] APconnections Inc, "NetEqualizer", http://www.netequalizer.com/

[NetG] APconnections Inc, "NetGladiator", http://www.netgladiator.net/

[NGMAST2014] 8th International Conference on Next Generation Mobile Apps, Services and Technologies, "NGMAST 2014", http://www.ngmast.com/

[Nomadix] Nomadix Inc, "Nomadix Solutions", http://www.nomadix.com/

[Numb] Viagénie, "Numb", http://numb.viagenie.ca/

[OPUS] Opus Interactive Audio Codec, "Opus", http://www.opus-codec.org/

[Oreka] SourceForge.net, "Oreka", http://oreka.sourceforge.net/

[Pandya1995] R. Pandya, "Emerging mobile and personal communication systems" em IEEE Communications Magazine, Vol. 33, Junho, 1995.

[Perényi2007] M. Perényi e S. Molnár, "Enhanced Skype Traffic Identification," em Budapest University of Technology & Economics, Department of Telecommunications & Media Informatics, Budapest, Hungary, 2007.

[PJSIP] Teluu Ltd., "PJSip", http://www.pjsip.org/

[Qren] Quadro de Referência Estratégica Nacional, "QREN", http://www.qren.pt/np4/home

[Restund] Creytiv Software, "Restund", http://www.creytiv.com/restund.html

[ReTurn] reSIProcate, "reTurn", https://www.resiprocate.org/ReTurn_Overview

[RFC0768] J. Postel, "User Datagram Protocol", RFC 768, Agosto, 1980.

[RFC0793] Information Sciences Institute, "Transmission Control Protocol", RFC 793, Setembro, 1981.

[RFC0959] J. Postel, "File Transfer Protocol (FTP)", RFC 959, Outubro, 1985.

[RFC1034] P. Mockapetris, "Domain Names -Concepts and Facilities", RFC 1034, Novembro, 1987.

[RFC1157] J. Case, "A Simple Network Management Protocol (SNMP)", RFC 1157, Maio, 1990.

[RFC1631] K. Egevang, "The IP Network Address Translator (NAT)", RFC1631, Maio, 1994.

[RFC1928] M. Leech, "SOCKS Protocol Version 5", RFC 1928, Março, 1996.

[RFC2068] R. Fielding, "Hypertext Transfer Protocol - HTTP/1.1", RFC 2068, Janeiro, 1997.

[RFC2326] H. Schulzrinne, "Real Time Streaming Protocol (RTSP)", RFC 2326, Abril 1988.

[RFC2327] M. Handley, "SDP: Session Description Protocol", RFC 2327, Abril, 1988.

[RFC2818] E. Rescorla, "HTTP Over TLS", RFC 2818, Maio, 2000.

[RFC2979] N. Freed, "Behavior of and Requirements for Internet Firewalls", RFC 2979, Outubro, 2000.

[RFC3261] J. Rosenberg, "SIP: Session Initiation Protocol", RFC 3261, Junho, 2002.

[RFC3303] P. Srisuresh, "Middlebox Communication Architecture and Framework," RFC 3303, Agosto, 2002.

[RFC3435] F. Andreasen, "Media Gateway Control Protocol (MGCP) Version 1.0", RFC 3435, Janeiro, 2003.

[RFC3489] Rosenberg, "STUN — Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, Março, 2003.

[RFC3550] H. Schulzrinne, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, Julho, 2003.

[RFC3711] M. Baugher, "The Secure Real-time Transport Protocol (SRTP)", Março, 2004.

[RFC3951] S. Andersen, "Internet Low Bit Rate Codec (iLBC)", RFC 3951, Dezembro, 2004.

[RFC3962] K. Raeburn, "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, Fevereiro, 2005.

[RFC5246] T. Dierks, "The Transport Layer Security (TLS) Protocol", RFC 5246, Agosto, 2008.

[RFC5246] T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, Agosto, 2008.

[RFC5249] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", Abril, 2010.

[RFC5766] R. Mahy, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", Abril, 2010.

[RFC5766TurnS] Project Turn Server, "rfc5766-turn-server", https://code.google.com/p/rfc5766-turn-server/

[RFC6101] A. Freier, "The Secure Sockets Layer (SSL) Protocol Version 3.0", RFC 6101, Agosto, 2011

[RFC6189] P. Zimmermann, "ZRTP: Media Path Key Agreement for Unicast Secure RTP", RFC 6189, Abril, 2011.

[RFC6716] JM. Valin, "Definition of the Opus Audio Codec", Setembro, 2012.

[RFC6970] M. Boucadair, "Universal Plug and Play (UPnP) Internet Gateway Device - Port Control Protocol Interworking Function", RFC 6970, Julho, 2013.

[Sand] Sandvine Incorporated ULC, "Sandvine Traffic Management", http://www.sandvine.com/products/traffic_management.asp

[Skype] Microsoft Inc., "Skype", http://www.skype.com/

[Thernelius2000] Fredrik Thernelius, "SIP, NAT, and Firewalls" em Department of Teleinformatics at the Royal Institute of Technology in Stockholm, Maio, 2000.

[TIE] TIE, "Traffic Identification Engine", http://tie.comics.unina.it/.

[TSTAT] Tstat, "TCP STatistic and Analysis Tool", http://tstat.tlc.polito.it/index.shtml

[TurnS] Strasbourg University, "TurnServer", http://turnserver.sourceforge.net/

[Varshney 2002] U. Varshney, A. Snow, M. McGivern e C. Howard, "Voice Over IP", em Communications Of The ACM, Vol. 45 Nº1, Janeiro, 2002.

[VMonitor] VoIPmonitor, "VoIPmonitor", http://www.voipmonitor.org/

[VPong] EnderUNIX project, "VoIPong", http://www.enderunix.org/voipong/

[Weback2005] Kevin Weback, "Using VoIP to Compete", em Harvard Business Review Setembro, 2005.

[Wshark] Wireshark Foundation, "Wireshark", https://www.wireshark.org/

[Wu2008] C. Wu, K. Chen, Y. Chang, e C. Lei, "Detecting VoIP Traffic Based on Human Conversation Patterns.", 2008.

[Yahoo] Yahoo! Inc, "Yahoo Message", http://messenger.yahoo.com/.