FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Projecto de uma rede de comunicações, com disponibilidade garantida nos serviços, para o suporte ao negócio

Luís Miguel de Carvalho Maia

VERSÃO DEFINITIVA

Relatório de Projecto
Mestrado Integrado em Engenharia Informática e Computação

Orientador: João Manuel Couto das Neves

17 de Julho de 2009

Projecto de uma rede de comunicações, com disponibilidade garantida nos serviços, para o suporte ao negócio

Luís Miguel de Carvalho Maia

Relatório de Projecto
Mestrado Integrado em Engenharia Informática e Computação

Aprovado em provas públicas pelo Júri:

Presidente: João António Correia Lopes

Arguente: Gerardo Rocha

Vogal: João Manuel Couto das Neves

17 de Julho de 2009

Resumo

Numa economia que se revela cada vez mais competitiva, os novos requisitos de negócio, o crescimento das aplicações que os suportam e a evolução das Tecnologias de Informação juntam-se exigindo novas formas de comunicação que permitam a interacção perfeita dos vários componentes à escala mundial e sem falhas. As empresas chegam à conclusão que as redes de comunicações não são mais, apenas, uma forma de interligação, tomando a cada dia que passa um papel mais relevante na forma como melhoram o desempenho do negócio e dos processos.

Pela importância que as infra-estruturas de redes de comunicações tomam actualmente, o processo de análise, arquitectura e desenho não deve produzir resultados pouco fundamentados e não reproduzíveis. O projecto de redes de comunicações deve constituir uma actividade lógica, reproduzível e defensável. É por isso essencial a utilização de metodologias que auxiliam a criação de infra-estruturas mais sólidas, mais disponíveis, mais documentadas e mais expansíveis, e tudo isto em espaços de tempo mais reduzidos. A utilização de metodologias cria uma forma sistemática de desenho de arquitecturas de redes que ajuda a garantir que os requisitos das organizações são cumpridos, independentemente da complexidade das aplicações a suportar e das tecnologias a usar.

Este relatório pretende por isso constituir um caso de estudo de um projecto de uma rede de comunicações, com disponibilidade garantida nos serviços, para o suporte ao negócio de uma instituição financeira, cuja actividade é marcada por elevadas exigências ao nível do controlo do risco operacional.

Assim, após definir concretamente a abordagem a utilizar para o projecto da rede de comunicações, tendo em conta as metodologias e modelos existentes na bibliografia de referência, serão aqui apresentados os resultados obtidos em cada uma das fases que constituem o projecto, que são:

- **Preparação**: levantamento dos requisitos requeridos pela organização;
- **Planeamento**: caracterização da infra-estrutura de rede existente, identificação dos seus problemas e síntese de requisitos identificados;
- **Desenho**: apresentação dos detalhes técnicos da infra-estrutura proposta, que foi:
    - Desenhada tendo em conta os dados recolhidos nas fases de preparação e planeamento;
    - Preparada para implementar procedimentos de *Disaster Recovery* que permitirão garantir a continuidade dos serviços críticos em caso de catástrofe;

    - Comprovada e testada através do uso de ferramentas de emulação e virtualização;
- **Implementação**: descrição das actividades efectuadas para a implementação da solução proposta;

A realização deste projecto pretende atingir dois objectivos fundamentais, que constituem a base da motivação, do esforço e da dedicação envolvida. O primeiro objectivo é o desenvolvimento de uma infra-estrutura de comunicações que sirva de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio da instituição em estudo. O segundo objectivo prende-se com a criação de um caso de estudo que acompanhe o ciclo de vida de uma infra-estrutura de rede com base numa metodologia bem definida, permitindo assim validá-la, no caso particular de uma organização com requisitos bastante específicos relativos à sua área de negócio, e também auxiliar e guiar a sua utilização através da concretização num caso prático documentado pormenorizadamente.

Abstract

In an economy which every day becomes more competitive, the new requirements of business, the growth of applications that support them and the development of Information Technology, require new ways of communication to enable seamless interaction of different components on a global scale and without failures. Companies conclude that the communications networks are not any more, only, a form of interconnection, taking every day a greater role in how to improve the performance of the business and processes.

Because of the importance that the communications networks currently take, the process of analysis, architecture and design should be logical, reproducible, and defensible. It is therefore essential to use methodologies that help to create robust, available, documented and scalable network infrastructures, and all of this, in a small amount of time. The use of methodologies creates a systematic approach to design network architectures helping to ensure that the requirements of the organizations are met, regardless of the complexity of applications and technologies to use.

This report pretends to be a case study of a project for a communications network, with guaranteed availability in services to support the business of a financial institution whose business is marked by high standards in the control of operational risk.

Thus, after defining the approach to use, analyzing the methodologies and models in the literature of reference, it will be presented the results at each stage of the project, which are:

- **Preparation**: identification of the requirements required by the organization;
- **Planning**: characterization of the existing network, identifying their problems and summarizing the identified requirements;
- **Design**: presentation of the technical details of the proposed infrastructure, which was:
    - Designed analyzing the data collected during the preparation and planning;
    - Prepared to implement Disaster Recovery procedures that will ensure the continuity of critical services in case of disaster;
    - Proven and tested through the use of tools of emulation and virtualization;
- **Implementation**: description of activities to implement the proposed solution;

This project aims to achieve two key objectives, which form the basis of the motivation, the effort and dedication involved. The first objective is the development of a network infrastructure to serve as a reliable foundation for the tools and information resources that support the business of the organization under study. The second objective is to create a case

study that follows the life cycle of a network infrastructure on the basis of a well defined methodology, trying to validate it, in the particular case of an organization with very specific requirements concerning their business and also assist and guide their future use by creating a case study documented in detail.

Agradecimentos

Ao meu orientador, João Neves, por me ter escolhido para a realização deste projecto, onde tive oportunidade de aplicar e aumentar os meus conhecimentos num projecto real com requisitos exigentes e por me ter orientado e supervisionado, com todo o seu conhecimento e experiência.

A toda a minha família, em particular a minha mãe, Lilita Maia, ao meu pai José Maia e ao meu irmão, Daniel Maia, pelos exemplos de sucesso e glória que têm sido ao lutar sempre para atingir os seus objectivos pessoais e profissionais com sucesso.

À minha namorada, Sara Silva, pela paciência em momentos de maior pressão, pelo suporte e força constante e pelo amor que tem demonstrado por mim.

Aos colegas de curso com quem tive o prazer de trabalhar, pelas experiências partilhadas, pelas noites de estudo, pelos trabalhos realizados com sucesso e pelo esforço conjunto que nos permitiu concluir este grande desafio. O esforço valeu a pena.

À FEUP, em particular ao MIEIC por, com as suas dificuldades e exigências, me preparar para enfrentar com sucesso os problemas do mundo real. Espero conseguir, com o meu trabalho e dedicação, que a marca "MIEIC" continue associada a uma sucessão de sucessos sem cessar.

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Símbolos

ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CBAC	Context-Based Access Control
CNA	Cisco Network Assistance
DC	Domain Controller
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DR	Disaster Recovery
DRS	Disaster Recovery Site
DRP	Disaster Recovery Plan
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
ICMP	Internet Control Message Protocol
IGC	Instituto Gestor de Capital
IETF	Internet Engineering Task Force
IIS	Internet Information Services
IOS	Internetwork Operating System
IP	Internet Protocol
ISI	Instituto de Serviços Informáticos
ISO	International Organization for Standardization
ISP	Internet Service Provider
MNAAD	Mccabe's Network Analysis, Architecture and Design
MPLS	MultiProtocol Label Switching
MTA	Message Transfer Agent
NAT	Network Address Translation
NEXT	Near End Crosstalk

NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PPDIOO	Cisco Prepare, Plan, Design, Implement, Operate and Optimize
QoS	Quality of Service
RFID	Radio-Frequency IDentification
RPO	Recovery point objective
RPS	Redundant Power Supply
RTO	Recovery time objective
SCR	Standby Continuous Replication
SDM	Cisco Router and Security Device Manager
SI	Sistemas de Informação
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
SSH	Secure Shell
SQL	Structured Query Language
TCP	Transmission Control Protocol
TI	Tecnologias de Informação
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
VTP	Vlan Trunkin Protocol
WPAD	Web Proxy Autodiscovery Protocol
WSUS	Windows Software Update Services

Capítulo 1

Introdução

Este capítulo contextualiza brevemente o projecto aqui documentado, apresentando e descrevendo o contexto e ambiente em que foi realizado, a motivação que o sustentou, os objectivos que se pretendeu atingir e a forma como o resultado será aqui exposto.

1.1 Descrição do Problema

Em seguida será descrito o problema para o qual se relata a solução, o contexto em que ele se insere, apresentadas as motivações para o esforço envolvido na procura da melhor solução e especificados os objectivos a cumprir quando o projecto terminar.

1.1.1 A Empresa

De forma a descrever o contexto em que o problema se insere, é apresentada sucintamente, a empresa onde foi realizado o projecto. Para preservar a privacidade e segurança da infra-estrutura de rede que suporta o negócio da empresa em causa, esta será designada, daqui em diante por Instituto Gestor de Capital (IGC). A apresentação e descrição da empresa é fundamental pelo facto de o negócio onde se insere requerer e justificar o esforço e investimento envolvido neste projecto.

O IGC desenvolve um processo de negócio que é o da gestão de activos. Este negócio consiste na tomada de decisões de investimento em activos financeiros e imobiliários tendo em vista a optimização da relação lucro/risco de cada Fundo. A gestão de activos é uma actividade marcada por elevadas exigências de especialização técnica, controlo de riscos, eficiência, credibilidade e defesa, independente dos interesses dos clientes. A sua missão é maximizar o valor dos activos sob gestão, de acordo com as necessidades de longo prazo dos clientes.

O IGC foi criado em 1999 e assumiu o papel de entidade gestora de fundos em regime de capitalização, podendo disponibilizar esses serviços a entidades públicas e privadas. O IGC está

integrado numa *holding* cujos constituintes desenvolvem uma actividade bastante distinta da sua.

Desde a sua criação, o IGC encetou um esforço sistemático no sentido de adoptar as melhores práticas no desenvolvimento da sua actividade principal de gestão de activos. Desde 2003 que o Instituto trabalha por objectivos e por projectos e, desde 2004, assumiu a Qualidade como uma das linhas orientadoras do seu desempenho. Até ao final de 2006 o IGC privilegiou o esforço para estruturar e medir os seus processos, tendo desenvolvido um sistema de informação de gestão para monitorizar os seus resultados. Concretizou-se assim a máxima Medir, Gerir, Criar Valor. Em 2007 obteve a certificação de qualidade de acordo com os requisitos da Norma ISO 9001:2000, que foi o resultado de ter assumido a Qualidade como uma das linhas orientadoras do seu desempenho.

Os custos totais de funcionamento do IGC, em 2007, atingiram um valor de, aproximadamente, 2 000 000 Euros, o que corresponde a 0.03% do montante médio gerido durante o ano, mantendo ao seu serviço 24 colaboradores.

Em 2007, os fundos sob a gestão do IGC obtiveram uma taxa de rentabilidade de cerca de 4.08%, com um nível de risco medido pelo desvio padrão anualizado de 2.66%. O valor desses fundos, em 31 de Dezembro de 2007, era de cerca de 7 560 000 000 Euros. O montante médio sob gestão ao longo de 2007 foi de 7 012 000 000 Euros (aproximadamente). [1]

Os números apresentados permitem mostrar que, apesar da reduzida dimensão do IGC, este desenvolve uma actividade de risco com grandes quantias monetárias envolvidas, o que permite justificar as necessidades tão específicas que serão satisfeitas ao nível dos Sistemas de Informação (SI) / Tecnologias de Informação (TI) da organização e por outro lado, as quantias investidas para a criação de uma infra-estrutura com disponibilidade garantida nos serviços de suporte ao negócio.

1.1.2 Motivação

A realização deste projecto pretende atingir dois objectivos fundamentais, que constituem assim a base da motivação, do esforço e da dedicação envolvida, para a sua conclusão com sucesso e dentro dos prazos estabelecidos.

O primeiro objectivo é o melhoramento e desenvolvimento de uma infra-estrutura de comunicações que sirva de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio da instituição em estudo.

O segundo objectivo prende-se com a criação de um caso de estudo que acompanhe o ciclo de vida de uma infra-estrutura de rede.

1.1.3 A rede do IGC

A integração do IGC numa *holding* de dimensão considerável permite-lhe ter acesso a um conjunto de serviços informáticos disponibilizados a todos os constituintes pelo Instituto de Serviços Informáticos (ISI), nome fictício.

Por essa razão, a componente de TI tem sido, desde a criação do IGC, suportada pelo ISI. No entanto, com a crescente necessidade de suportar SI especializados e específicos para o negócio da gestão de activos, o IGC tem gradualmente lutado pela independência da gestão da

infra-estrutura informática interna, pelo facto de sentir que o serviço padrão, prestado pelo ISI, de forma não diferenciada a todos os constituintes da *holding*, dificulta que as TI/SI disponíveis sirvam de alicerce fiável ao negócio do IGC. Actualmente, e por essa razão, algumas TI/SI internas são geridas e mantidas de forma autónoma, na medida do possível, relativamente ao ISI, havendo no entanto uma integração obrigatória na sua rede, que abrange todos os seus elementos.

Assim, actualmente, os serviços de comunicações de acesso ao exterior, o serviço de e-mail e o serviço de autenticação/gestão dos utilizadores são geridos pelo ISI o que, segundo o IGC, cria barreiras na forma de trabalhar dos seus colaboradores pois a sua disponibilidade instável, limitação e elevado tempo de resposta a problemas dificulta a utilização de ferramentas fundamentais na área de negócio do IGC que é, como já foi referido, uma actividade particularmente exigente em termos de controlo de risco operacional.

1.1.4 Objectivos

Estando presente a insatisfação já referida relativamente à actual infra-estrutura de rede do IGC, o projecto levado a cabo e aqui documentado apresenta os seguintes objectivos específicos:

- Caracterização e identificação dos requisitos da rede, sistemas e serviços que suportam o negócio do IGC;
- Avaliação e proposta de soluções para garantir: a disponibilidade determinada dos serviços informáticos, a possibilidade da infra-estrutura de rede ser utilizada como alicerce fiável no negócio do IGC e a continuidade do funcionamento das TI/SI críticas em caso de catástrofe na sede do IGC;
- Iniciar a implementação da infra-estrutura proposta.

Adicionalmente, o trabalho aqui desenvolvido pretende contribuir para a criação de um caso de estudo que coloca em prática um conjunto de metodologias que acompanham o ciclo de vida da infra-estrutura de rede de uma organização, permitindo assim validar as metodologias existentes e documentadas em diversa bibliografia, no caso particular de uma organização com requisitos bastante específicos relativos à sua área de negócio. A criação de casos de estudo poderá auxiliar a utilização das metodologias disponíveis através da sua concretização num caso prático.

1.2 Estrutura do relatório

O resultado do projecto realizado será descrito neste relatório da seguinte forma e sequência:

1. **Introdução**: contextualização breve do projecto descrevendo os seus objectivos e a motivação que o sustentou;
2. **Estado da Arte**: apresentação do actual estado da arte relativo a modelos e metodologias que auxiliam o processo de desenho de infra-estruturas de redes de comunicações;

3. **Abordagem ao Problema**: descrição da metodologia utilizada para resolver o problema e exposição dos resultados das fases de Preparação e Planeamento que permitirão especificar, através de uma análise cuidada, os requisitos da infra-estrutura a desenhar;
4. **Desenho da Solução**: descrição detalhada da infra-estrutura de rede de comunicações para servir de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio;
5. **Implementação**: descrição das actividades efectuadas para a implementação da solução proposta;
6. **Conclusões e Trabalho Futuro**: síntese da solução desenhada e o potencial que trará ao IGC, avaliação da forma como foram cumpridos os objectivos e previsão do trabalho que seguirá as fases seguintes do ciclo de vida da infra-estrutura de rede aqui desenvolvida.

Capítulo 2

Estado da Arte

Este capítulo apresenta o actual estado da arte relativo a modelos e metodologias que auxiliam o processo de desenho de infra-estruturas de redes de comunicações.

Começa-se por apresentar os dois modelos baseados em camadas cuja utilização facilita o desenvolvimento, implementação, manutenção e descrição das redes de comunicações [4] e de seguida são apresentadas duas metodologias que acompanham o ciclo de vida de uma rede, o que permite beneficiar das seguintes vantagens: diminuir o custo total de aquisição, aumentar a disponibilidade da rede, melhorar a agilidade do negócio que a rede suporta e aumentar a sua expansibilidade acelerando o acesso a serviços e aplicações [3]. Finalmente são apresentados os conceitos fundamentais e modelos auxiliares à construção de um plano de Recuperação de Desastres, que permite garantir a continuidade do funcionamento das SI/TI críticas das organizações em caso de catástrofes.

2.1 Modelos de Camadas

De seguida serão apresentados e comparados os modelos de redes de comunicações Open Systems Interconnection (OSI) e TCP/IP, que são baseados em camadas e que seguem por isso os seguintes princípios:

- As funções são decompostas e organizadas em camadas;
- Cada camada realiza um conjunto de funções relacionadas, suportadas num protocolo;
- Cada camada fornece serviços à camada superior escondendo-lhe os detalhes de implementação;
- Cada camada usa serviços da camada inferior;
- Mudanças internas numa camada não implicam mudanças nas outras camadas.

2.1.1 Modelo OSI

É difícil abordar a temática das Redes de Comunicações sem fazer referências ao modelo OSI desenvolvido pela International Organization for Standardization (ISO). O modelo OSI surge em 1970 para colmatar a necessidade de um Modelo Arquitectónico de Referência, face às necessidades dos utilizadores de explorarem os serviços fornecidos pelos operadores de rede uma vez que, até ao seu aparecimento, os utilizadores estavam completamente dependentes das soluções de um determinado fabricante (soluções fechadas) [5]. Por outro lado, começaram a implantar-se redes públicas de comunicações, baseadas em diferentes tecnologias, protocolos de acesso e serviços [5] o que dificultava a sua utilização em grande escala devido à falta de uniformização.

O Modelo OSI define regras de interacção entre sistemas abertos, isto é, sistemas que obedecem a normas universais de comunicação e cujo comportamento externo está de acordo com o prescrito pelo modelo. Este modelo define princípios, conceitos e relações entre componentes. É um modelo abstracto e não um modelo de implementação e cria as bases para a especificação e aprovação de standards por organizações de normalização reconhecidas internacionalmente [5]. É geral e flexível e apesar de ter sido desenvolvido em 1984, continua a ser usado como o modelo de descrição de redes e serviços que se desenvolveram desde então [5], daí a importância da sua abordagem neste relatório.

O Modelo OSI, ilustrado na figura 1, propõe uma organização funcional em 7 camadas.

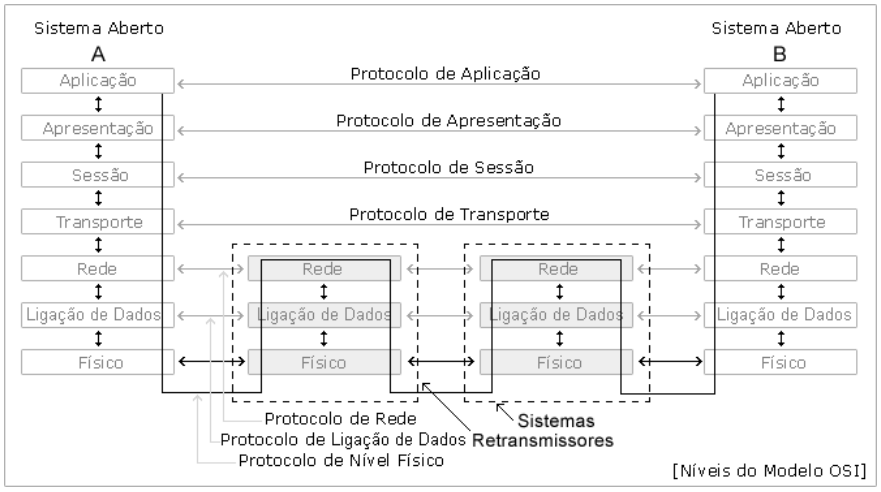


Figura 1 Modelo de referência OSI [6]

A figura 2 pretende ilustrar a forma como interagem as várias componentes que constituem uma rede de comunicações com e sem o Modelo OSI. Sem este modelo as redes eram difíceis de perceber e de implementar [7]. Com o Modelo OSI as redes podem ser divididas em várias partes geríveis e este constitui uma linguagem comum para explicar os seus componentes e a sua funcionalidade [7].

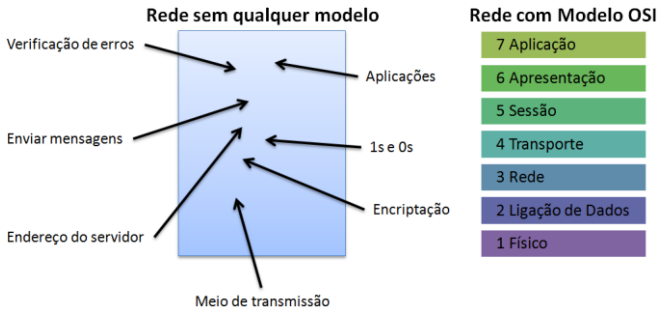


Figura 2 Interacção dos componentes de uma rede de comunicações com e sem o Modelo OSI [7]

A tabela 1 resume as funções associadas a cada camada do modelo.

Tabela 1 Funções das várias camadas do Modelo OSI [5]

Camada	**Funções**
Física	Características mecânicas, eléctricas e funcionais da interface física entre sistemas (conectores, nível de sinal, códigos de transmissão, sincronização).
Ligação de Dados	Estabelecimento, manutenção e terminação de uma ligação de dados. Encapsulamento de dados em tramas para transmissão. Controlo de Fluxo e Controlo de Erros (no caso de ligação fiável).
Rede	Transferência de informação (multiplexagem e comutação) entre nós da rede. Encaminhamento de pacotes através da rede. Serviço independente da tecnologia e dos serviços nativos de sub-redes físicas.
Transporte	Transferência de informação extremo-a-extremo entre equipamentos terminais. Serviço independente do serviço de Rede (ou dos serviços nativos de sub-redes). Adaptação ao serviço de Rede (fragmentação, multiplexagem de fluxos de dados). Eventualmente, Controlo de Erros (serviço fiável) e Controlo de Fluxo.
Sessão	Controlo do diálogo entre processos e mecanismos de sincronização.
Apresentação	Representação de informação (formatos, códigos) independente do conteúdo. Resolução de diferenças sintácticas e negociação da sintaxe de transferência.
Aplicação	Criação do ambiente para comunicação entre aplicações (aspectos semânticos). Aplicações genéricas (transferência de ficheiros, correio electrónico, etc.). Funções de gestão.

Apesar da grande utilização do modelo OSI como modelo de referência, a sua falta de implementação pode ser justificada pelas críticas que lhe estão associadas:

- Quando surgiu este modelo, o modelo TCP/IP, descrito na secção seguinte deste documento, era já utilizado em muitas universidades de investigação. Devido à importância deste mercado, muitos fabricantes começaram a implementar o modelo TCP/IP e quando surgiu o modelo OSI não o quiserem suportar até serem obrigados [6];
- As camadas inferiores (rede e ligação de dados) têm funcionalidades a mais e repetitivas [6];
- As camadas superiores (sessão e apresentação) são vazias em termos de funcionalidade e ignoradas em algumas implementações [6];
- Algumas funções, como o endereçamento, controlo de fluxo e controlo de erros repetem-se em várias camadas [6];

- Dada a complexidade do modelo, as implementações inicialmente feitas estão associadas a "fraca qualidade", face às implementações do Modelo TCP/IP cujas implementações iniciais tiveram enorme sucesso [6].

2.1.2 Modelo TCP/IP

O Modelo TCP/IP foi inicialmente desenvolvido no âmbito da ARPANET, que começou por ser uma rede experimental financiada pelo Departamento de Defesa dos Estados Unidos da América, e que ligava universidades e centros de investigação [5]. Os protocolos especificados por este modelo foram implementados antes da maior parte daqueles descritos no Modelo OSI [5].

Um dos objectivos fundamentais requerido pelo Departamento de Defesa dos EUA era a capacidade de as ligações suportadas por este protocolo se manterem activas enquanto o seu destino e origem se mantiverem funcionais, mesmo que algumas máquinas intermédias de comunicação deixassem de funcionar [6]. Para cumprir este objectivo foi necessário criar uma arquitectura extremamente flexível [6].

O Modelo TCP/IP, tal como o Modelo OSI, apresenta uma organização funcional baseada em camadas, seguindo por isso também os princípios referidos na secção anterior. Este apresenta no entanto uma arquitectura baseada em apenas 4 camadas. A figura 3 ilustra a arquitectura do Modelo TCP/IP comparando-o com o Modelo OSI.

A tabela 2 resume as funções associadas a cada camada deste modelo.

Tabela 2 Funções das várias camadas do Modelo TCP/IP [6]

Camada	**Funções**
Estação-para-rede	Funções pouco especificadas e raramente discutidas na bibliografia. Permite a ligação ao meio físico, possibilitando o envio de pacotes IP.
Internet	Funções similares à camada de Rede do Modelo OSI. Define o formato do pacote e o protocolo IP (Internet Protocol). Permite a entrega de pacotes IP nos destinatários pretendidos. O encaminhamento de pacotes tem um papel fundamental.
Transporte	Funções similares à camada de Transporte do Modelo OSI. São aqui definidos dois protocolos fundamentais: • Transmission Control Protocol (TCP) – protocolo com ligação (*connection-oriented*) que garante a comunicação fiável extremo-a-extremo • User Datagram Protocol (UDP) – protocolo sem ligação (*connectionless*) e sem garantias de comunicação fiável extremo-a-extremo
Aplicação	Concentra as funções das camadas de Aplicação, Apresentação e Sessão do Modelo OSI. Alguns protocolos especificados nesta camada são: Telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), entre muitos outros.

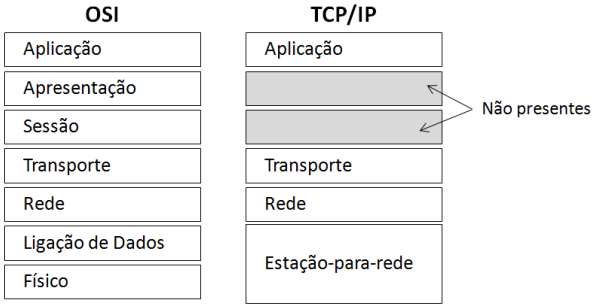


Figura 3 Modelo TCP/IP em comparação com o Modelo OSI [6]

Apesar da sua utilização à escala global, o Modelo TCP/IP não é perfeito e são-lhe frequentemente apontadas as seguintes críticas:

- Não faz uma distinção clara entre a especificação e a implementação. Por essa razão não é muito utilizado como uma guia para desenhar novas infra-estruturas de rede baseadas em novas tecnologias [6].
- Por ser demasiado específico, não é usado para descrever outras pilhas de protocolos, por exemplo, é extremamente complexo descrever a tecnologia Bluetooth utilizando este modelo [6].
- Não distingue a camada física da camada de ligação de dados, que desempenham funções bastante distintas [6].

2.2 MNAAD

Análise, arquitectura e desenho de redes foi, no passado, considerado uma arte que combinava um conjunto de regras pessoais para avaliar e escolher as tecnologias; conhecimento das tecnologias, serviços e protocolos e experiência acerca do que funcionava e não funcionava na prática. Esta combinação de factores produzia resultados pouco explicados e raramente reproduzíveis [2]. Esta forma pouco clara e explicada de projectar infra-estruturas de rede foi aceite inicialmente, no entanto, o facto de essas infra-estruturas serem actualmente consideradas críticas e com grande influência no negócio das organizações, o projecto de redes de comunicações deve constituir uma actividade lógica, reproduzível e defensável [2]. É esta a motivação para a criação da metodologia Mccabe's Network Analysis, Architecture and Design (MNAAD).

A MNAAD pretende ajudar a identificar e aplicar serviços de rede e níveis de desempenho necessários para satisfazer os utilizadores. Esta metodologia tem como objectivo ajudar a perceber os problemas que a rede em análise deverá resolver, determinar os serviços e o desempenho necessário para lidar com tais problemáticas [2]. A abordagem defendida por esta metodologia toma as infra-estruturas de rede como um sistema que disponibiliza vários serviços aos utilizadores e cuja combinação particular das várias tecnologias, técnicas e aplicações existentes permite abranger determinada quantidade e qualidade do conjunto de serviços disponibilizados, assim como a sua capacidade de adaptação a novos serviços [2].

A MNAAD é constituída por três processos fundamentais: Análise, Arquitectura e Desenho. Os processos estão interligados e o output de um processo é usado directamente como o input do seguinte havendo assim um fluxo de informação da Análise para a Arquitectura e da Arquitectura para o Desenho, tal como se encontra esquematizado na figura 4.

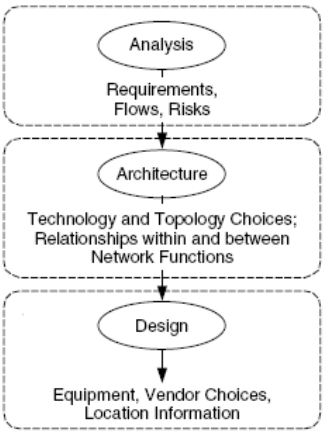


Figura 4 Fluxo de informações entre o processo de Análise, Arquitectura e Desenho [2]

No processo de Análise pretende-se perceber o que é que os utilizadores, aplicações e equipamentos necessitam da rede e definir, determinar e descrever as relações entre os utilizadores, aplicações, equipamentos e rede. Deve ser também percebido o comportamento da actual infra-estrutura em várias situações. Resumidamente o processo de Análise tem dois objectivos: ouvir os utilizadores e as suas necessidades e perceber o sistema. A figura 5 resume a informação que deve ser recolhida e o resultado do processo de Análise.

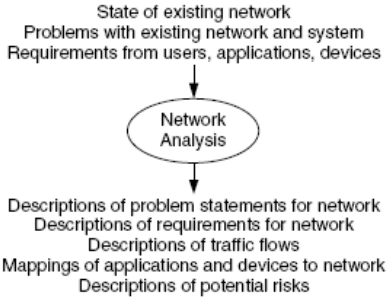


Figura 5 Inputs e outputs do processo de Análise [2]

O processo de Arquitectura usa a informação do processo de Análise para desenvolver uma arquitectura conceptual e de alto nível da nova infra-estrutura. Nesta fase tomam-se decisões acerca das topologias e da tecnologia a adoptar e determinadas as relações entre as várias funções da rede: endereçamento/encaminhamento, gestão da rede, desempenho e segurança. A figura 6 resume a informação usada e o resultado do processo de Arquitectura.

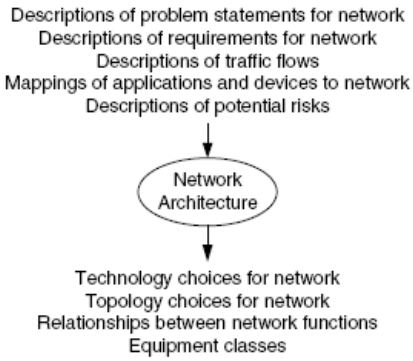


Figura 6 Inputs e outputs do processo de Arquitectura [2]

No processo de Desenho é criado o detalhe físico da arquitectura correspondendo à fase final da metodologia. Detalhe físico da arquitectura inclui: esquemas da rede, selecção dos fornecedores e dos equipamentos. Durante a fase de Desenho é usado um processo de avaliação dos fornecedores e equipamentos, baseado no output do processo de análise e arquitectura onde são definidos os objectivos de desenho, tal como minimizar os custos ou maximizar o desempenho. Por outro lado, nesta fase são avaliados alguns *trade-offs* tal como custo *versus* desempenho ou simplicidade *versus* funcionalidade. A figura 7 resume a informação usada e o resultado do processo de Desenho.

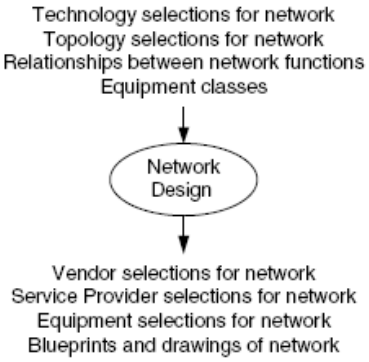


Figura 7 Inputs e outputs do processo de Desenho [2]

2.3 PPDIOO

Nesta secção é apresentado, do ponto de vista da Cisco Systems (adiante designada por Cisco), o ciclo de vida de uma rede de comunicações assim como uma metodologia de desenho que o acompanha. Será aqui descrita e explorada cada fase da metodologia em discussão.

Novos requisitos de negócio, o crescimento das aplicações e a evolução das TI juntam-se actualmente exigindo novas arquitecturas de rede [3]. As empresas chegam à conclusão que as redes de comunicações não são mais, apenas, uma forma de interligação [3]. Estas, a cada dia que passa, tomam um papel cada vez mais relevante na forma como melhoram o desempenho do negócio e dos processos [3].

O objectivo principal da metodologia aqui apresentada é descrever uma forma sistemática de desenho de arquitecturas de redes que ajude a garantir que os requisitos das organizações são cumpridos, independentemente da novidade ou complexidade das aplicações a suportar e das tecnologias a usar [8].

O ciclo de vida aqui apresentado é o Cisco Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO). A figura 8 esquematiza as fases que estão envolvidas no ciclo de vida PPDIOO.

De seguida são então descritas as várias fases do ciclo de vida PPDIOO:

- **Preparação** – esta fase envolve o estabelecimento de requisitos organizacionais, desenvolvimento de uma estratégia, a proposição de um esquema conceptual de alto nível da arquitectura e a identificação das tecnologias que poderão melhor suportar a arquitectura. [3]

- **Planeamento** – esta fase envolve a identificação dos requisitos, que se baseiam nos objectivos da rede, onde esta será instalada e o que lhe vai requisitar serviços. Nesta fase faz-se a análise da rede já existente, em caso disso, e é determinando se esta é capaz de suportar a nova arquitectura. [3]
- **Desenho** – é executado o desenho da rede de comunicações que irá suportar os requisitos organizacionais recolhidos na fase da Preparação assim como os requisitos identificados na fase de Planeamento, através da análise da rede já existente, quando for esse o caso. Para além do suporte de todos os requisitos, a arquitectura de rede desenhada deve garantir a disponibilidade, confiabilidade, segurança, escalabilidade e desempenho da nova infra-estrutura. [3]
- **Implementação** – é implementada a nova infra-estrutura de rede tendo especial cuidado para, em caso de uma rede já existente, não provocar a sua quebra de serviço ou criar pontos de vulnerabilidade. [3]
- **Operação** – esta fase envolve a manutenção do correcto funcionamento da infra-estrutura instalada. [3]
- **Optimização** – envolve a gestão proactiva de toda a rede tendo como principal objectivo a identificação e resolução de problemas antes que a sua gravidade coloque em causa a continuidade do funcionamento do negócio da organização. [3]

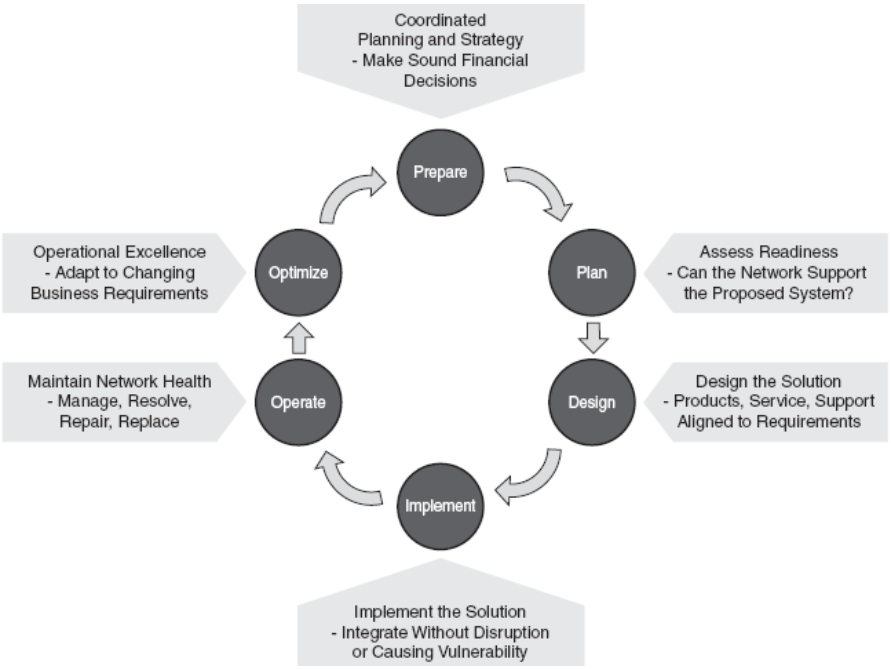


Figura 8 Ciclo de vida PPDIOO [3]

O ciclo de vida apresentado, do ponto de vista do negócio, apresenta as seguintes vantagens [9]:

- **Diminuição do custo de manutenção da rede** – diminuir os custos associados à manutenção da rede assim como da sua evolução para suportar novas tecnologias;
- **Aumentar a agilidade do negócio** – melhorar capacidade da organização responder de forma rápida às mudanças do negócio e às condições do mercado;

- **Acelerar o acesso a novas aplicações e serviços** – o acesso rápido a novas aplicações e serviços de suporte ao funcionamento da organização, através de uma infra-estrutura de rede escalável, contribui fortemente para o aumento da agilidade do negócio;
- **Aumentar a disponibilidade** – garantir a continuidade do funcionamento das principais ferramentas que suportam o negócio da organização, através de uma infra-estrutura redundante e segura que permita responder rapidamente a problemas;

Além da descrição das várias fases do ciclo de vida de uma rede, apresentadas através do PPDIOO, a Cisco apresenta a metodologia que acompanha o referido ciclo de vida, sendo que os vários passos são descritos de seguida:

1. Identificar os requisitos do cliente: são identificados os requisitos iniciais junto do cliente. Corresponde à fase de Preparação. [3]
2. Caracterizar a infra-estrutura existente: envolve a caracterização da actual infra-estrutura, verificando cuidadosamente a sua integridade e qualidade. Corresponde à fase de Planeamento. [3]
3. Desenhar a topologia da rede e soluções: é criado o desenho detalhado da nova solução. São tomadas decisões relativamente à infra-estrutura de rede, infra-estrutura dos serviços e aplicações. Um protótipo ou um projecto-piloto deve ser utilizado como *Proof of Concept*, para identificar e corrigir problemas antes da implementação de toda a infra-estrutura. Corresponde à fase de Desenho. [3]
4. Planear a implementação: são preparados os procedimentos de implementação para acelerar e clarificar a sua execução. Deve ser feita uma previsão dos custos associados. Corresponde à fase de Desenho. [3]
5. Implementar e verificar a infra-estrutura: é implementada a infra-estrutura desenhada e preparada nos passos anteriores. Corresponde à fase de Implementação. [3]
6. Monitorar e opcionalmente redesenhar: após a colocação em operação da rede desenhada, procede-se à sua monitorização constante procurando eventuais erros ou problemas. Se existem problemas e necessidade de intervenção frequentes poderá ser necessário proceder ao seu redesenho sendo que esta acção deve ser evitada se todos os passos anteriores forem executados cuidadosamente. Corresponde à fase de Operação e Optimização. [3]

2.4 Disaster Recovery

Face à grande dependência das organizações nas TI/SI, há negócios que não podem sobreviver se as ferramentas informáticas utilizadas não estiverem disponíveis 24 horas por dia [10]. Uma simples quebra na disponibilidade do serviço pode afectar gravemente o negócio e não sendo possível evitar essas quebras, é necessário estar preparado e prever como lidar com elas [10]. Essa previsão é normalmente traduzida num Plano de Continuidade de Negócio – Business Continuity Plan (BCP) que refere todas as actividades necessárias para manter uma organização em funcionamento durante um período de interrupção anormal [10]. A Recuperação de Desastres – Disaster Recovery (DR) faz parte do BCP e pode ser definido como: capacidade de manter em funcionamento os serviços em caso de uma catástrofe, mesmo que com capacidade ou desempenho reduzido [11]. O plano de DR (DRP) lida com situações onde as operações não podem ser resumidas no mesmo sistema ou no mesmo *site* e onde existem

procedimentos manuais para activar sistemas de *backup* que irão suportar a continuação das operações [11].

O desenvolvimento técnico de uma estratégia que suporte a capacidade de DR é apenas uma tarefa num conjunto de passos complexos que devem estar incluídos na criação de um DRP e onde devem ser envolvidos os vários departamentos e níveis de gestão da organização [12]. Sumariamente, os passos envolvidos são [12]:

1. Desenvolver um plano de contingência de negócio e dos seus processos prioritários;
2. Realizar uma avaliação de risco;
3. Conduzir uma Análise de Impacto no Negócio – Business Impact Analysis (BIA);
4. Desenvolver estratégias e planos de Continuidade e Recuperação do negócio;
5. Conduzir actividades de sensibilização, testes e treino do DRP;
6. Conduzir a manutenção do DRP.

De seguida são descritos sumariamente alguns conceitos fundamentais envolvidos num DRP e que auxiliam o processo de criação de uma infra-estrutura capaz de o suportar:

- Declaração de desastre – decisão que uma catástrofe aconteceu e é necessário dar início aos procedimentos de DR [11];
- Recovery time objective (RTO) – tempo necessário até que as IT estejam disponíveis após uma catástrofe [11];
- Recovery point objective (RPO) – localização temporal dos dados que serão restaurados e utilizados após o desastre [11];
- *Site* primário – localização principal das TI da organização [11];
- *Site* de DR – Disaster Recovery Site (DRS) – localização onde se encontram os sistemas a usar em caso de catástrofe [11];

A figura 9 esquematiza os conceitos descritos.

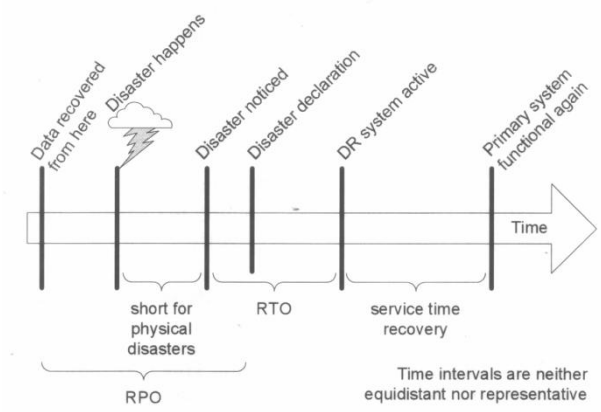


Figura 9 Esquematização de conceitos associados a um DRP

Relativamente a modelos de arquitecturas de alto nível de sistemas de DR são normalmente sugeridos os seguintes [11]:

- ***Shared Systems***: todos os sistemas são utilizados e o trabalho é distribuído por ambos [11];
- ***Hot standby***: são mantidos sistemas de DR que não são utilizados, mas têm o mesmo *software*, configuração e informação dos sistemas primários, estando prontos a serem activados a qualquer momento [11];

- ***Cold standby***: são mantidos sistemas de DR que não são utilizados nem actualizados com a informação dos sistemas primários. Apenas são actualizados em caso de catástrofe com as cópias de segurança efectuadas [11].

A figura 10 ilustra cada uma das arquitecturas referidas. As arquitecturas descritas podem ser caracterizadas e comparadas através dos seguintes parâmetros: RTO, RPO e Custo. Assim, a solução *Shared Systems* é a que apresenta o melhor RTO e RPO pelo facto de todos os sistemas serem utilizados em simultâneo obrigando a que a informação nos vários sites seja a mesma, mas apresenta também um elevado custo pela sua necessidade de manutenção de circuitos de comunicação de alta velocidade que permitem a sincronização constante dos vários sistemas e o acesso por parte dos utilizadores a sistemas remotos como se tratassem de sistemas locais. O modelo *Cold Standby* caracteriza-se pelo menor custo mas também por um RTO e RPO elevado. A solução *Hot Standby* apresenta características intermédias comparativamente com as restantes.

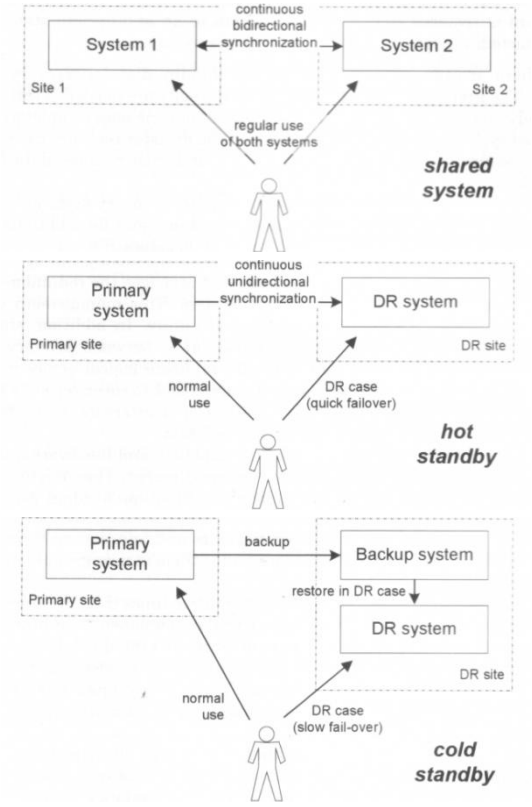


Figura 10 Arquitecturas de DR: *Shared Systems, Hot Standby* e *Cold Standby*

2.5 Conclusões

Das metodologias e modelos apresentados é importante referir que, na pesquisa bibliográfica efectuada existiu grande dificuldade em encontrar documentos que relatavam a sua aplicação em casos reais com objectivos específicos e bem definidos. As referências consultadas, apesar de em cada fase fazerem a ligação com casos práticos, esta não é feita de uma forma pormenorizada, e muitas vezes não é utilizado sempre o mesmo caso descrevendo a sua evolução ao longo das várias etapas. Por um lado isso torna a bibliografia mais rica por tentar abordar um maior número de casos e de especificidades, fazendo com que a fonte se adapte a várias realidades. Por outro, pode dificultar o seu entendimento e criar barreiras à sua

utilização principalmente por pessoas menos experientes. Por essa razão, a existência de casos de estudo que documentem todo o processo de criação/reestruturação de uma rede de comunicações aplicando as metodologias referidas contribui para uma melhor compreensão e maior facilidade de utilização destes métodos.

Relativamente ao DR ficou claro a sua importância cada vez maior e também o facto de o desenvolvimento de um DRP envolver muito trabalho e a participação essencial dos vários departamentos e níveis de gestão da organização, nas várias fases que o constituem. Neste documento apenas será abordada a análise da componente técnica para suportar um DRP, daí a importância dos modelos de arquitectura referenciados para a criação de uma infra-estrutura capaz de o suportar, de acordo com as necessidades da organização em estudo.

Capítulo 3

Abordagem ao Problema

Com base na pesquisa efectuada e cujos resultados foram apresentados no capítulo anterior, correspondente ao Estado da Arte, neste capítulo começa-se por descrever a metodologia utilizada para resolver o problema e de seguida são descritos os resultados da execução das fases de Preparação e Planeamento que permitirão especificar, através de uma análise cuidada, os requisitos da infra-estrutura a desenhar na fase seguinte.

3.1 Metodologia Utilizada

A análise das metodologias apresentadas no Estado da Arte, permite verificar que estas apresentam bastantes semelhanças e a utilização de forma complementar das duas metodologias contribui para uma abordagem mais rica e mais fundamentada.

Pelo facto de IGC possuir já e mostrar preferência por equipamentos da Cisco, pelo facto da experiência das pessoas envolvidas no projecto ser na sua grande maioria com equipamento deste fabricante, por este ser líder de mercado estando os seus equipamentos associados a grande nível de estabilidade e desempenho [13], face à grande quantidade de documentação que lhe está associada e à forma prática como se encontra descrita, facilitando assim a sua adaptação num curto espaço de tempo, será utilizada como base da metodologia a seguir, aquela apresentada pela Cisco. Esta será complementada com a MNAAD fundamentalmente na fase de análise de requisitos e secção de análise de fluxos, processos que se encontram explicados de forma muito clara e completa na bibliografia da 2ª metodologia apresentada.

Face à duração prevista de apenas 20 semanas para o projecto, que deve incluir a escrita deste relatório, não será possível percorrer e abordar aqui todas as fases do PPDIOO pelo facto de o arranque da fase de implementação estar dependente de prazos de entrega de equipamentos a adquirir e também por eventuais circuitos de acesso a contratar. Por esta razão a meta principal a atingir será o início da fase de implementação, sendo descrito de forma sucinta o que se encontra já implementado quando a produção deste documento estiver concluída.

Assim, serão documentadas no capítulo seguinte, os resultados da execução de cada uma das fases: Preparação, Planeamento, Desenho e Implementação. Nas fases de Planeamento, de Desenho e de Implementação será utilizada para descrever os resultados, uma abordagem em camadas/níveis, seguindo um modelo que toma em consideração as qualidades e defeitos dos dois modelos de camadas já referidos, OSI e TCP/IP. Serão assim utilizadas as seguintes camadas/níveis:

- Nível Físico que corresponderá à descrição e análise das ligações físicas entre os vários componentes da infra-estrutura;
- Nível Lógico onde será analisado a forma lógica de interligação dos equipamentos de Nível 2 (*switches*);
- Nível de Rede que corresponderá à análise da topologia ao nível da camada IP, dando particular enfoque aos equipamentos de Nível 3 (*routers*) e abordando protocolos de encaminhamento implementados ou a implementar;
- Nível Aplicacional onde serão descritos e analisados os principais serviços/aplicações utilizados;

Seguidamente são apresentadas as fases a percorrer e as actividades executadas, inputs utilizados e outputs esperados em cada uma delas.

- **Preparação:**
  - Actividades:
    - Levantamento junto da organização dos requisitos requeridos
  - Inputs:
    - Reuniões de acompanhamento
  - Outputs:
    - Requisitos requeridos pela organização
- **Planeamento**
  - Actividades:
    - Caracterização da infra-estrutura de rede, sistemas e serviços que suportam o negócio da instituição
  - Input:
    - Requisitos requeridos pela organização
  - Outputs:
    - Requisitos da infra-estrutura de rede a desenhar
- **Desenho**
  - Actividades:
    - Avaliação e projecto de soluções para garantir disponibilidade determinada, incluindo o suporte de um DRP
    - Consulta de Internet Service Providers (ISP's) para avaliação de cenários práticos de implementação e previsão de custos
    - *Proof of Concept*: simulação parcial da infra-estrutura proposta
  - Input:
    - Requisitos da infra-estrutura de rede a desenhar
  - Outputs:

- Descrição da infra-estrutura/solução proposta com o custo previsto para a sua implementação

- **Implementação**
  - Actividades
    - Definir requisitos mínimos para serviços a contratar a ISP's
    - Avaliar tecnicamente as propostas apresentadas pelos ISP's
  - Input:
    - Descrição da infra-estrutura/solução proposta com o custo previsto para a sua implementação
  - Output:
    - Requisitos mínimos para ISP's
    - Avaliação técnica das propostas apresentadas pelos ISP's
    - Resumo do estado da implementação

A figura 11 apresenta o cronograma previsto para a conclusão das várias actividades identificadas na secção anterior.

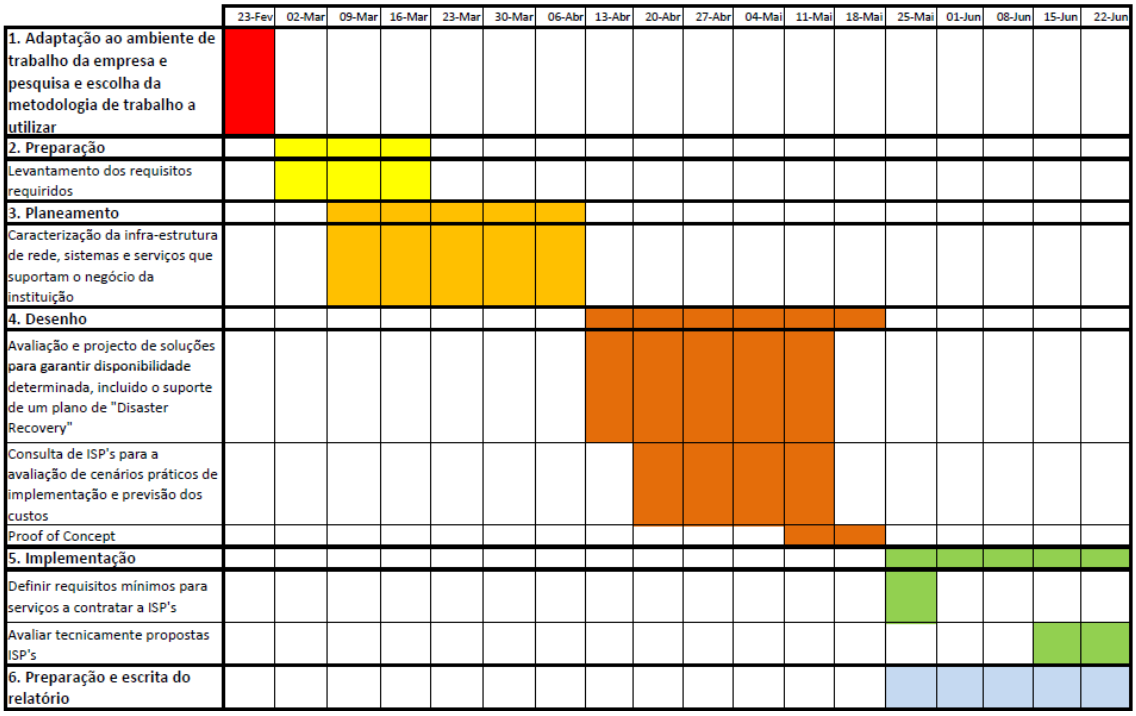


Figura 11 Cronograma das actividades

Nas secções seguintes serão então apresentados e discutidos os resultados da execução de cada uma das fases que constituem a metodologia utilizada.

3.2 Preparação: requisitos requeridos

Nesta secção encontram-se identificados os requisitos da infra-estrutura de rede e informática, requeridos pelo IGC:

- Exigência de Fiabilidade e Disponibilidade no acesso à Internet.
- Fiabilidade/Confiança no serviço de e-mail. Garantir a entrega e um tempo de entrega médio das mensagens reduzido.

- Implementação de um servidor de e-mail interno para suporte à troca de mensagens na Intranet, facilitando a comunicação entre os utilizadores locais e outros serviços ou processos locais que o requeiram, como por exemplo, as ferramentas de *Workflow*.
- Tendo em conta a actividade do IGC, em que o risco operacional deve ser o mínimo possível, e pelo património elevado que lhe está confiado, parece imprescindível a exigência de Segurança da Informação e dos respectivos fluxos.
- Pela criticidade da informação do IGC e pela dependência crescente do Negócio na infra-estrutura de rede e informática, parece ser um requisito fundamental a criação de uma infra-estrutura que suporte políticas e procedimentos de DR definidas pelo IGC.
- Disponibilizar aos utilizadores do IGC um serviço de acesso remoto à rede, quer para teletrabalho quer para operações de manutenção à infra-estrutura.

3.3 Planeamento: caracterização da solução existente

Para a caracterização da actual infra-estrutura de rede que suporta o negócio do IGC e para identificar os seus requisitos, primeiro será apresentada a sua visão geral sendo de seguida analisadas, de forma mais detalhada, as camadas física, lógica, rede e aplicação.

3.3.1 Visão Geral

A representação topológica da infra-estrutura da rede de comunicações que suporta a actividade do IGC é apresentada na figura 12.

As instalações do IGC estão distribuídas em 2 escritórios, localizados no Porto e em Lisboa, sendo estes interligados através da rede do ISI que, para além disso, é o fornecedor do serviço de acesso à Internet.

Nas instalações no Porto está localizada a sede do IGC, sendo aqui realizadas quase todas as actividades do Instituto e estando por isso, aqui concentradas quase na totalidade, as infra-estruturas SI/TI que suportam o negócio. Na rede do Porto estão normalmente activos cerca de 25 utilizadores.

As instalações de Lisboa consistem no que se pode tipificar, do ponto de vista da rede, como uma pequena filial e onde se encontram normalmente, no máximo, 4 utilizadores.

Apesar de na figura 12 os utilizadores e servidores serem representados por “nuvens” distintas, não existe qualquer segmentação das redes, sendo que a rede no Porto é uma rede com uma estrutura plana que utiliza o bloco de endereços 172.20.8.0/24 e a rede em Lisboa, igualmente com uma estrutura plana, utiliza o bloco de endereços 172.26.19.0/24.

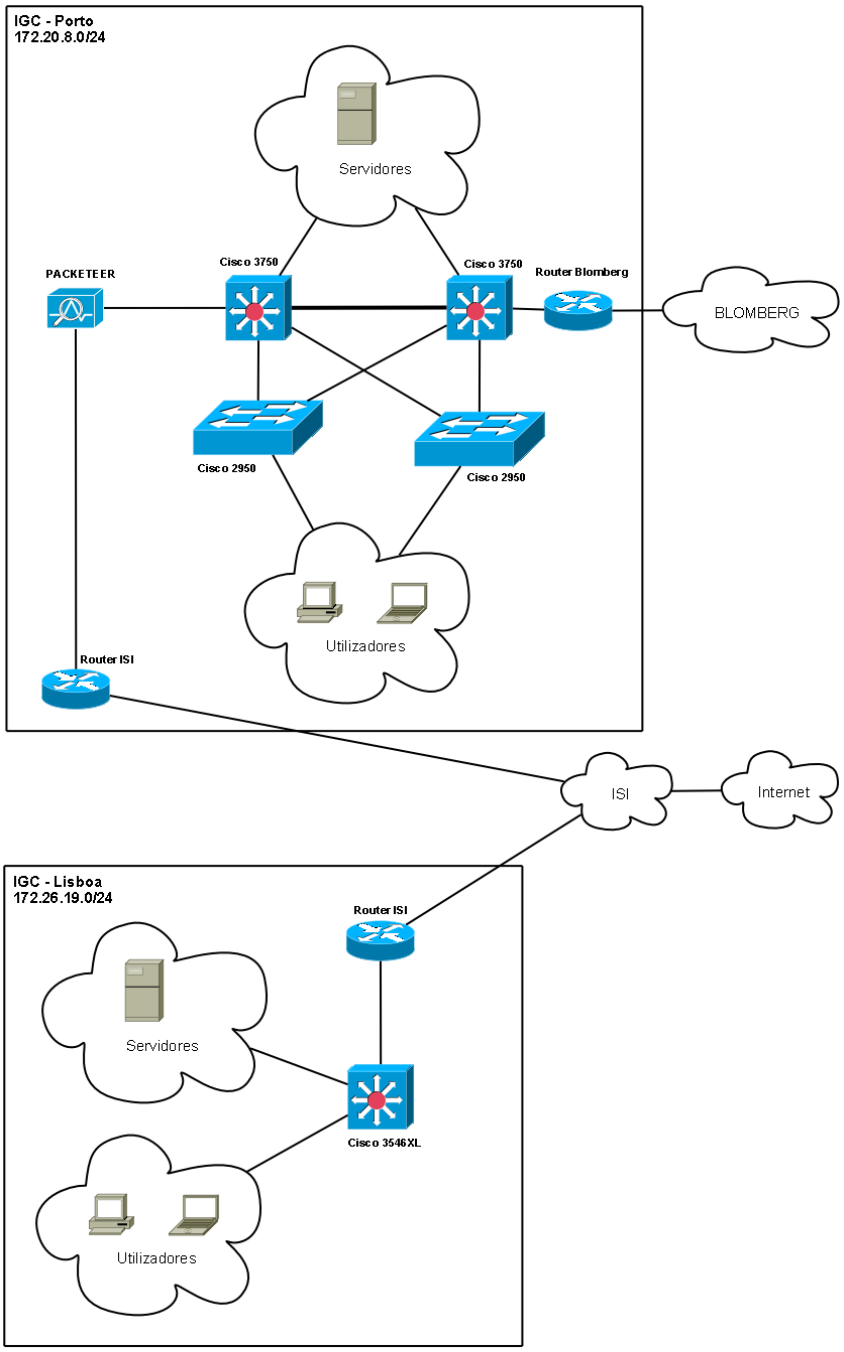


Figura 12 Representação topológica da infra-estrutura da rede de comunicações do IGC

3.3.2 Análise Física

A análise física efectuada, tem o objectivo de caracterizar as infra-estruturas físicas que suportam a rede do IGC e de verificar o estado da cablagem, assim como a execução do levantamento da forma como os diversos equipamentos de rede se encontram interligados.

3.3.2.1 Caracterização do Pólo Técnico do Porto

É no pólo técnico do Porto que se encontra alojada a quase totalidade das infra-estruturas físicas que suportam a rede de comunicações do IGC. O pólo técnico é uma sala com cerca de 30 m2.

O controlo de acessos à referida sala é feito através do mecanismo de controlo de acessos implementado no Instituto, que se baseia em terminais de leitura de impressão digital ou leitura de um cartão Radio-Frequency IDentification (RFID), controlado pelo *software* TimeREPORT versão 3.4.0 Beta 7, sendo todo o equipamento (*software* + terminais) da ACronym – Informação e Tecnologia. Este *software* tem configurado, com autorização de acesso ao Pólo Técnico, apenas aos colaboradores responsáveis pelas TI/SI. O acesso às instalações por pessoas sem a autenticação do sistema de controlo de acesso é controlado fazendo o registo numa folha onde é indicada a data de entrada e saída, o motivo, o nome da pessoa e o nome do colaborador do Instituto que acompanhou.

O suporte à alimentação eléctrica da sala é socorrido por uma Uninterruptible Power Supply (UPS) GE LanPro S3, trifásica, de 20 kVA, sendo desconhecida a autonomia do sistema para os diferentes padrões de carga – normalmente esta é em média 40% da carga total aceite pela UPS. A manutenção deste equipamento é efectuada com uma regularidade anual, pela empresa LCPower - Luis Carneiro, Soluções de Energia, SA, que foi a empresa que forneceu e instalou a unidade. Esta UPS fornece o socorro de energia em caso de falha, a todas as tomadas do pólo técnico e às tomadas vermelhas que se encontram nas várias caixas de energia espalhadas (uma por caixa) pelo chão das instalações IGC.

Para o controlo ambiental da sala – manutenção das condições de temperatura e humidade – está instalado um único sistema de ar condicionado, programado para manter a temperatura a 21ºC. De acordo com os registos de um sensor localizado na bancada de servidores, a humidade na sala é 45%. Devido à insuficiência do desempenho do sistema de ar condicionado, junto do armário dos servidores encontra-se uma ventoinha para ajudar a circulação do ar. O chão é revestido por material que não tem características anti-estáticas.

As figuras seguintes pretendem ajudar a caracterizar o pólo técnico do Porto.

Figura 13 Fotografias do chão do pólo técnico do Porto

Figura 14 Fotografias do sistema de ar condicionado do pólo técnico do Porto

Figura 15 Fotografias do sistema de socorro da alimentação eléctrica do Pólo técnico do Porto

Figura 16 Fotografia da bancada de servidores do pólo técnico do Porto

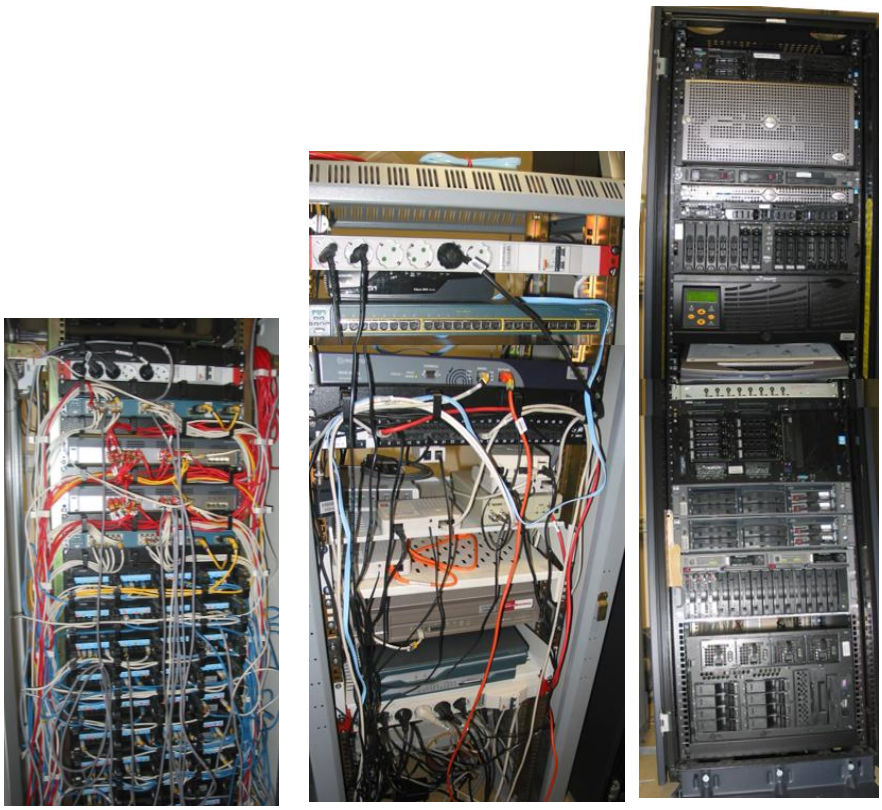


Figura 17 Fotografias do Armário LAN, Armário WAN e Armário Servidores (da esquerda para a direita) do pólo técnico do Porto

3.3.2.2 Caracterização do Pólo Técnico de Lisboa

No escritório de Lisboa não existe qualquer sala dedicada às infra-estruturas da rede de comunicações. Existe somente um armário onde se encontra um *switch*, os *routers* de acesso e os *patchs* de ligação da cablagem. O único servidor alojado em Lisboa encontra-se ligado atrás de uma secretária na entrada das instalações.

Aqui não existe qualquer controlo de acesso a estas infra-estruturas, nem qualquer controlo e manutenção das condições ambientais para a operação dos equipamentos, nem qualquer sistema de socorro em caso de falha de energia eléctrica.

3.3.2.3 Ensaios de conformidade da Cablagem

De forma a verificar o estado da infra-estrutura da cablagem estruturada que suporta as ligações dos diversos equipamentos de rede do Instituto foram efectuados testes de conformidade e certificação de Categoria 6, que deverá garantir a qualidade correspondente à Classe E de acordo com a norma EN50173 [14]. O equipamento de teste utilizado foi o DTX-1800 da marca FLUKE Networks. É importante referir que os testes efectuados não contemplam os cabos de ligação (chicotes) que ligam os *patch panels* dos bastidores aos equipamentos. A figura 18 ilustra a forma como foram realizados os testes.

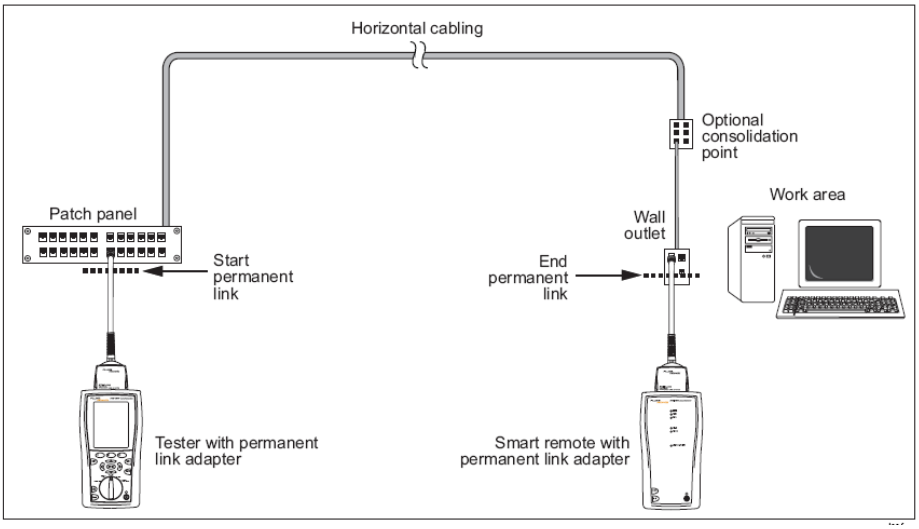


Figura 18 Ilustração dos ensaios de conformidade da cablagem efectuados [15]

3.3.2.3.1 Porto

Em Abril de 2005, aquando da instalação do sistema de cablagem estruturada actualmente em uso, foram realizados testes de certificação e elaborado o respectivo relatório. Assim, dada a existência deste foi decidido, face aos prazos apertados do projecto, não efectuar novamente testes a todas as tomadas da rede, fazendo novos testes apenas a uma amostragem de cerca de 30% do número de pontos de acesso existentes, que são 216 no total. Os pontos de acesso escolhidos para amostra foram escolhidos de forma a serem representativos da realidade, através da escolha de pontos de acesso localizados a distâncias diversas do pólo técnico e classificados como laranjas, azuis e verdes (esta codificação foi estabelecida nos testes efectuados em 2005 e corresponde respectivamente aos pontos que falharam, aos que passaram no limite das especificações da norma e aos que passaram com sucesso).

Com o objectivo de caracterizar a amostra, de seguida são apresentados 2 gráficos: o primeiro pretende mostrar as distâncias de cabo dos vários pontos de acesso escolhidos para teste; o segundo mostra a quantidade de pontos de acesso escolhidos em relação aos resultados obtidos no relatório de 2005.

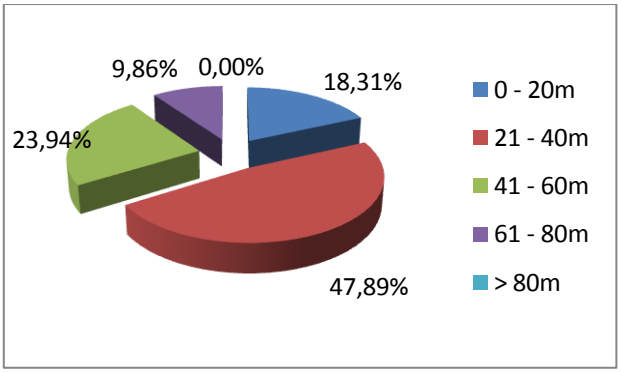


Figura 19 Distâncias de cabo dos vários pontos de acesso escolhidos para teste no Porto

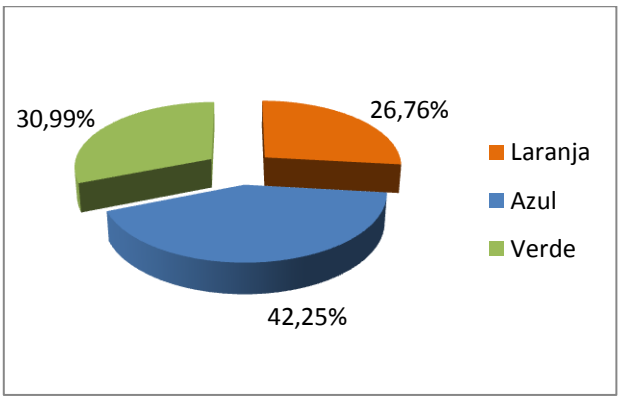


Figura 20 Quantidade de pontos de acesso escolhidos para teste no Porto, em relação aos resultados obtidos no relatório de 2005

Os resultados dos testes de certificação são apresentados através dos gráficos seguintes. A figura 21 mostra os resultados dos testes de certificação efectuados no Porto, à amostragem de 32% dos pontos. A figura 22 permite comparar os resultados obtidos com os resultados do teste efectuado em 2005.

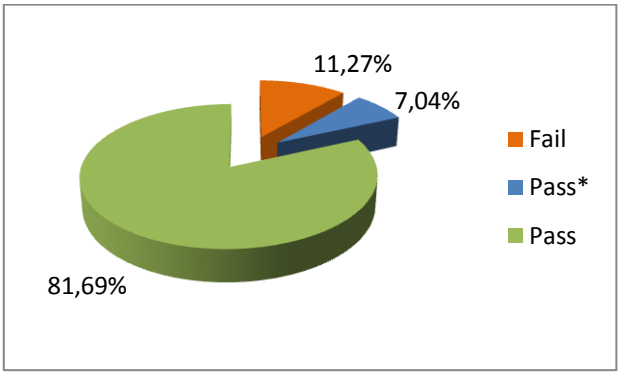


Figura 21 Resultados dos testes de certificação efectuados no Porto

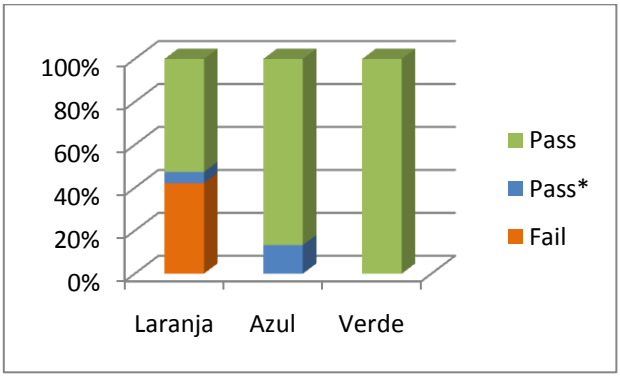


Figura 22 Comparação dos resultados obtidos no Porto com os resultados do teste efectuado em 2005

A figura 22 mostra que os testes realizados em 2005 apresentam piores resultados do que os aqui documentados, enfraquecendo assim a hipótese de uma possível degradação da cablagem estruturada. É possível até observar que todos os testes classificados como verde em 2005 continuaram a passar, os testes classificados como azul, grande parte deles passa também e dos classificados como laranja metade deles passam e apenas os restantes falham. Os resultados obtidos podem ser justificados pelo facto de o equipamento utilizado nos ensaios em 2005,

naturalmente ter várias limitações técnicas, próprias do desenvolvimento tecnológico da época, e que actualmente estão ultrapassadas em modelos de equipamento mais precisos como o utilizado nestes ensaios, permitindo por isso resultados mais fiáveis.

É possível assim concluir que é seguro utilizar as tomadas classificadas como azuis e verdes uma vez que estas passaram nos ensaios de certificação. Quanto às tomadas classificadas como laranja pode ser arriscado a sua utilização uma vez que grande parte delas não passou nos testes de certificação de Categoria 6 efectuados. No entanto, alguns destes pontos de acesso passam com sucesso os ensaios se os limites dos testes baixarem para as especificações Categoria 5e.

Quanto à causa da falha nos testes efectuados, esta está na sua maioria relacionada com o parâmetro Near End Crosstalk (NEXT) que é originada, normalmente, por uma de duas razões: fonte de ruído que provoca interferências electromagnéticas nos cabos ou então na sua conectorização, a descarnagem ser maior do que o necessário deixando os condutores sem a blindagem que os protege contra interferências [16]. Uma nova e correcta conectorização dos cabos terá grande probabilidade de resolver a maioria destes problemas.

3.3.2.3.2 Lisboa

Como não existe nenhum relatório acerca dos resultados de testes de certificação efectuados no escritório de Lisboa, nem uma classificação das tomadas em laranja, azul e verde, tal como no Porto, foram efectuados testes de certificação à totalidade dos pontos de acesso da cablagem estruturada em Lisboa. O gráfico da figura 23 mostra a distribuição das distâncias dos pontos de rede.

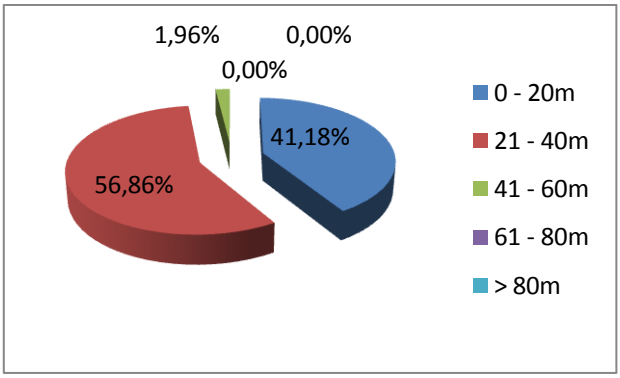


Figura 23 Distribuição das distâncias dos pontos de rede testados em Lisboa

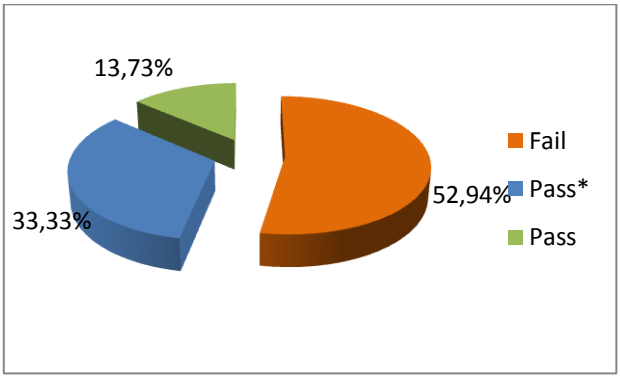


Figura 24 Resultados dos testes de certificação efectuados em Lisboa

Os resultados apresentados através do gráfico da figura 24 revelam o mau estado em que a cablagem estruturada do escritório de Lisboa se encontra. Sobre as causas de falha nos testes, para além do parâmetro NEXT, já explicado na secção anterior, há cabos danificados com condutores que não estabelecem ligação.

Se os limites dos testes efectuados baixarem para Categoria 5e os resultados obtidos são apresentados na figura 25.

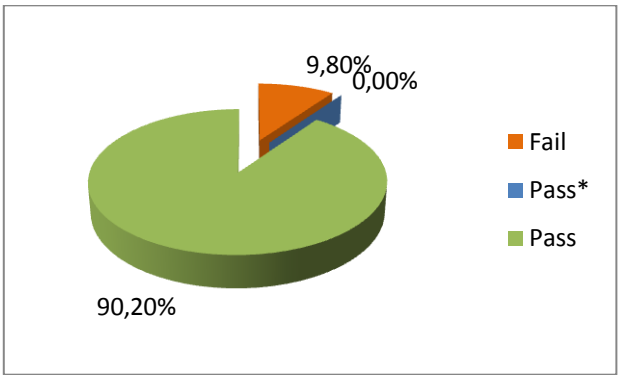


Figura 25 Resultado dos testes de certificação efectuados em Lisboa (Categoria 5e)

3.3.2.4 Esquema Físico Porto

De seguida serão apresentados os resultados do levantamento efectuado das interligações dos diversos equipamentos. Na figura 26 é apresentada a forma como se encontram ligados os equipamentos de *switching* da rede do Porto.

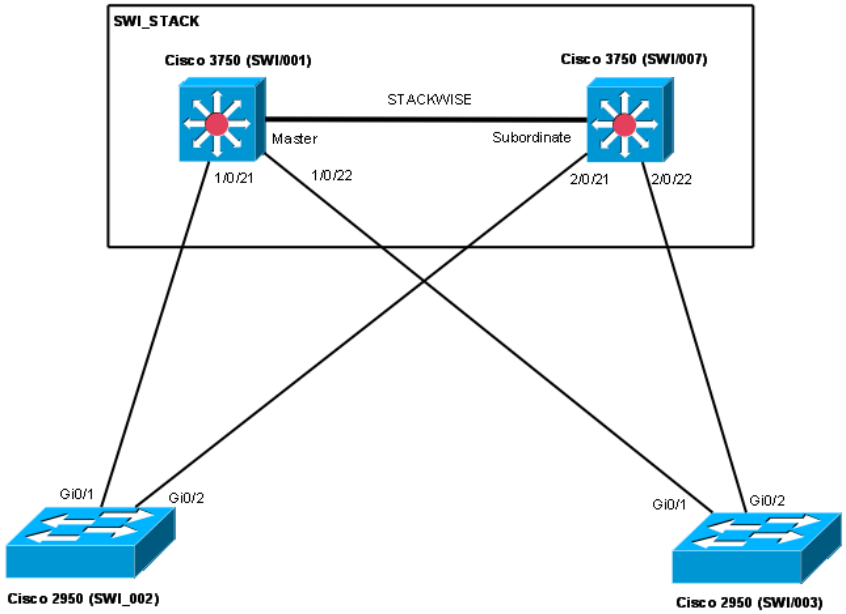


Figura 26 Diagrama da interligação dos equipamentos de *switching* no Porto

A figura 26 permite ilustrar que o *Core* da rede é assegurado através de 2 *switches multilayer* (Cisco 3750 com 24 portas de cobre em 1000BASE-T) que se encontram interligados através da tecnologia proprietária da Cisco, Cisco StackWise, em que um dos *switches* desempenha o papel de *Master* e o segundo o papel de *Subordinate* [17]. A tecnologia Cisco StackWise permite interligar os 2 *switches* fazendo com que, do ponto de vista de administração, estes funcionem como se fosse apenas um *switch* [17]. Os 2 *switches* de acesso

(Cisco 2950 com 24 portas de cobre a 100Mbit e 2 portas de uplink, em cobre a 1Gbit) que suportam as estações de trabalho dos utilizadores encontram-se ligados ao *Core* através de 2 cabos Unshielded Twisted Pair (UTP), ligados às 2 portas a 1 Gbit e aos 2 *switches* que formam o *Core*, proporcionando assim a continuidade do serviço em caso de falha de um dos circuitos de ligação ou de um dos *switches* do *Core*.

Na figura 27 e 28 é ilustrada a forma como os diversos servidores que suportam os serviços informáticos do Instituto são ligados aos equipamentos da rede e, de forma simples, como são alimentados electricamente. Como se pode observar, os servidores encontram-se ligados através de, grande parte deles, ligações redundantes aos 2 *switches* do *Core* proporcionando assim uma continuidade do serviço em caso de falha de uma placa de rede ou de um dos *switches*. Em termos de alimentação energética, grande parte dos servidores possuem 2 fontes de alimentação permitindo assim uma alimentação eléctrica redundante, tendo havido o cuidado de cada fonte de alimentação ter sido ligada a fases diferentes da UPS.

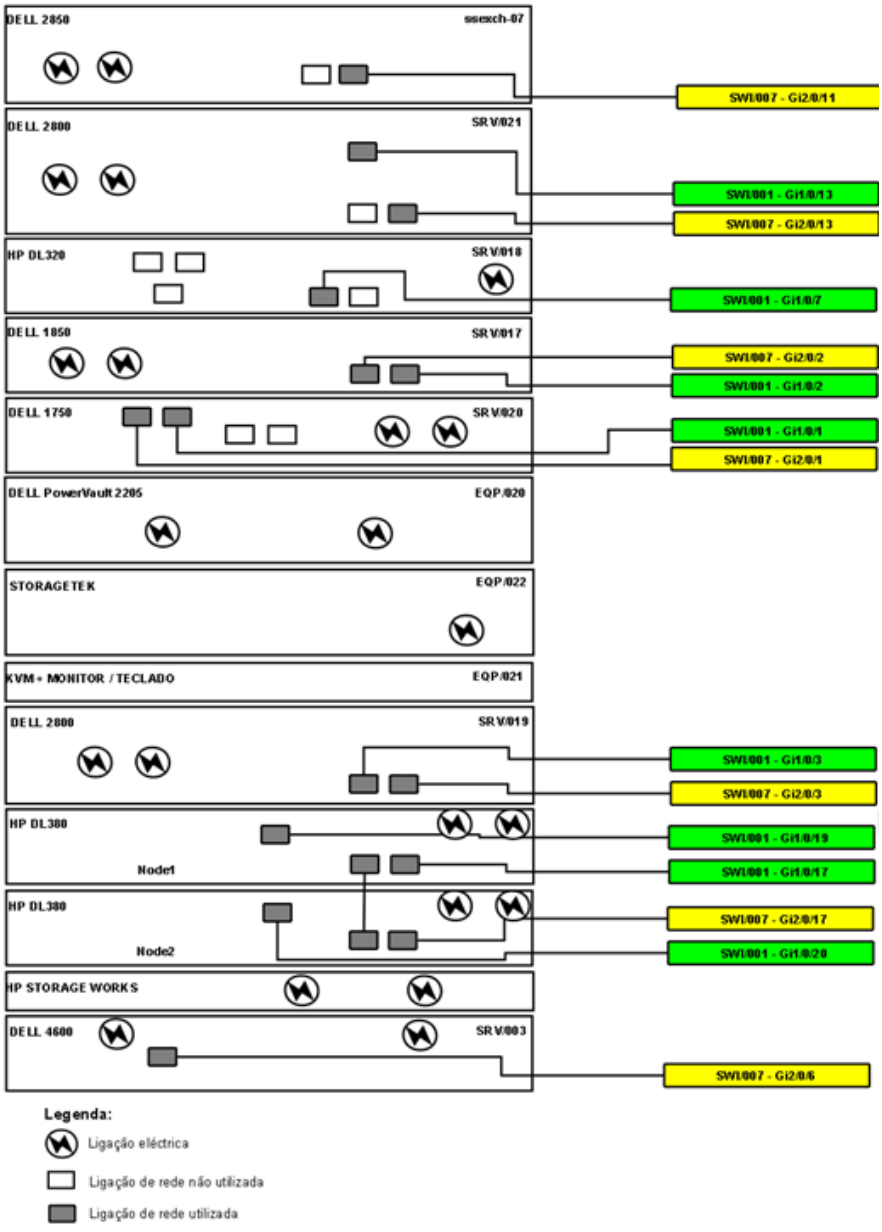


Figura 27 Esquema das ligações dos servidores localizados no "Armário Servidores"

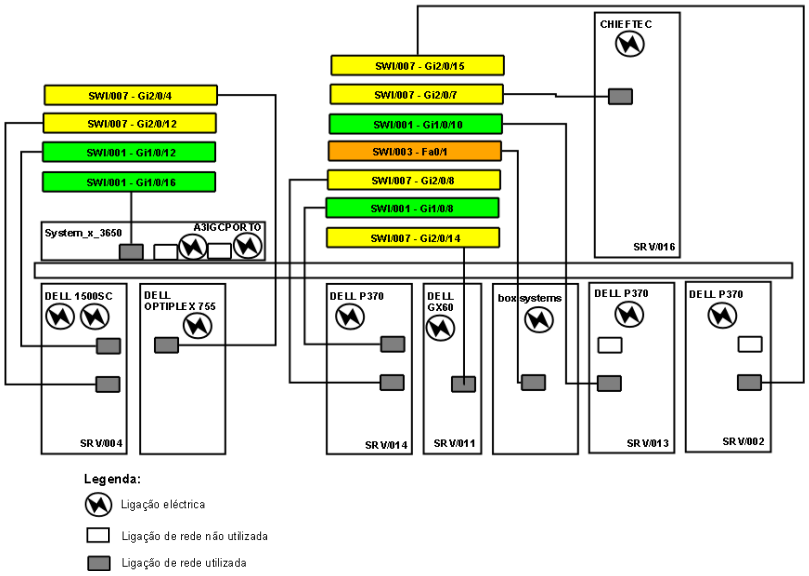


Figura 28 Esquema das ligações dos servidores localizados na "Bancada de Servidores"

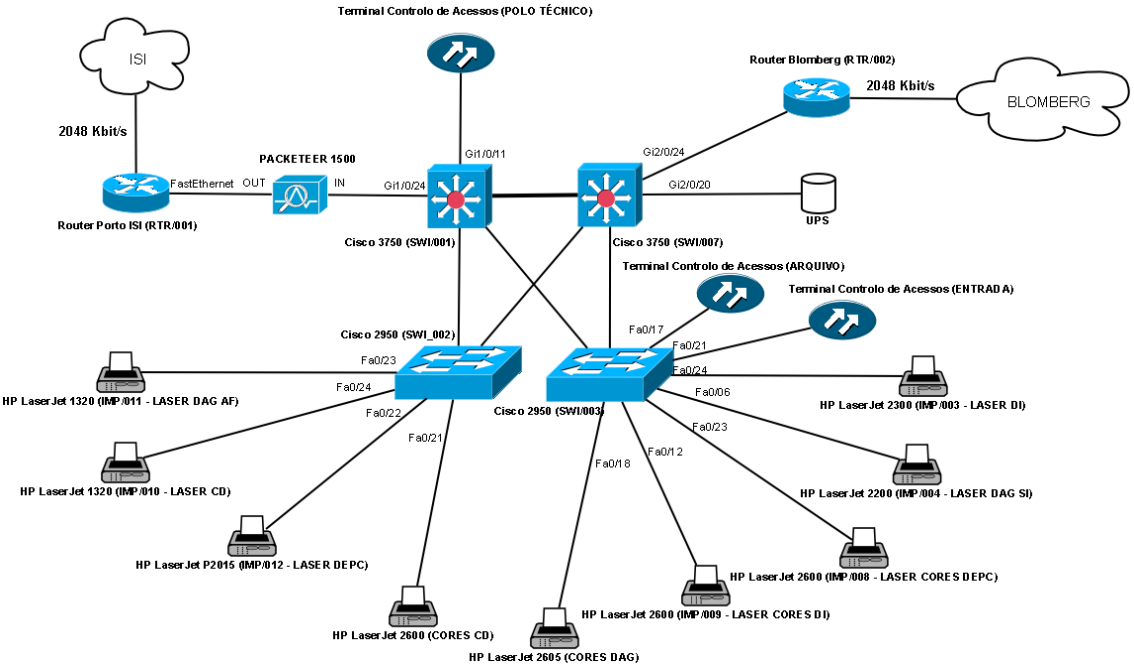


Figura 29 Esquema de interligação de *Routers*, Impressoras e Terminais de Controlo de Acesso no Porto

O esquema da figura 29 mostra a forma como se encontram ligados aos equipamentos de *switching*, os equipamentos de comunicações para o exterior (*router* do ISI que dá acesso à sua rede que fornece o acesso ao escritório de Lisboa e à Internet e o *router* da Blomberg), as impressoras, a UPS e os terminais de controlo de acesso.

3.3.2.5 Esquema Físico Lisboa

As interligações dos equipamentos no escritório de Lisboa estão esquematizadas através do diagrama da figura 30, que inclui as interligações dos servidores, *router* do ISI que dá acesso à

sua rede e que fornece o acesso ao escritório do Porto e à Internet, impressoras e do terminal de controlo de acessos.

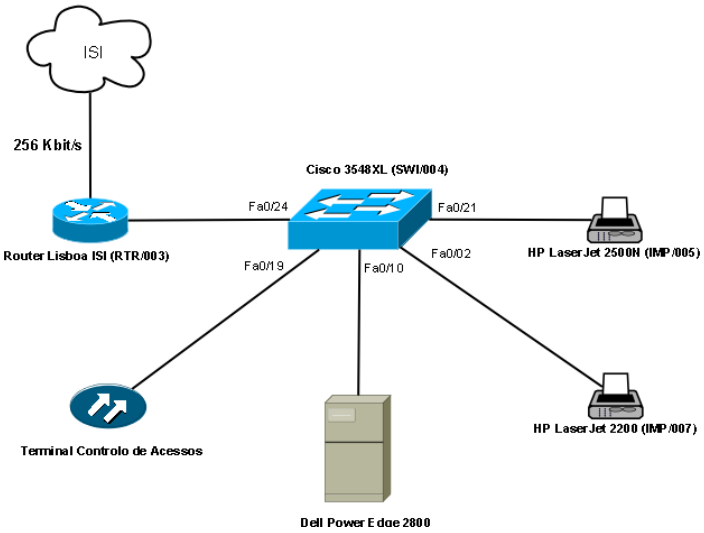


Figura 30 Esquema de interligação de Servidores, *Routers*, Impressoras e Terminais de Controlo de Acesso em Lisboa

3.3.3 Análise Lógica

Nesta secção é realçada e analisada a forma como se encontram logicamente ligados os equipamentos activos da rede com base na análise estatística, obtida através do *software* de monitorização SolarWinds[1] e MRTG[2], da utilização das diferentes principais portas dos *switches* permitindo avaliar e caracterizar a utilização da rede e se a sua capacidade está de acordo com os requisitos de tráfego.

3.3.3.1 Caracterização dos Activos de Rede no Porto

Anteriormente, neste documento foi apresentada a forma como se encontram fisicamente interligados os vários equipamentos de rede no Porto. Nesta secção é caracterizada a forma como estão configuradas logicamente essas ligações.

A figura 31 esquematiza as ligações lógicas dos equipamentos de rede no Porto. Começando pela análise das interligações dos *switches*, os de acesso encontram-se ligados aos *switches* de *Core*, cada um através de um *EtherChannel* o que permite que as duas ligações físicas sejam utilizadas logicamente como que de uma se tratasse, com capacidade próxima da soma das duas [18]. Esta tecnologia, baseada na especificação IEEE 802.3ad, permite para além do aumento da capacidade de transmissão, uma convergência rápida caso uma das ligações físicas falhe, passando o tráfego a ser encaminhado por apenas um dos cabos, havendo a mínima perca de tramas [18] [19]. Os EtherChannel's estão configurados como *TRUNK* o que significa que o tráfego que passa por eles pode pertencer a várias *VLAN's* [4].

De notar que o protocolo Spanning-Tree, que faz o controlo de ligações redundantes entre *switches* com o objectivo de evitar *loops* na rede [4], encontra-se desactivado em todos os

[1] Software de Gestão de Redes. Para mais informações consultar: http://www.solarwinds.com/
[2] Software de Monitorização de Tráfego. Para mais informações consultar: http://oss.oetiker.ch/mrtg/

switches através da instrução "`no spanning-tree vlan 1`", desactivando assim a protecção contra a criação de malhas na rede e, portanto, a geração de *loops*, o que obriga a um correcto planeamento antes de efectuar quaisquer novas ligações ou inclusões de *switches* na rede.

Em termos de detecção automática de velocidade das portas e do tipo de transmissão, *full-duplex* ou *half-duplex*, esta encontra-se configurada manualmente em quase todas as portas com equipamentos ligados, através das instruções "`speed 100`"/"`speed 1000`" e "`duplex full`"/ "`duplex half`". As seguintes portas encontram-se a funcionar em modo *half-duplex*: SWI_STACK(Gi1/0/11), SWI_STACK(Gi2/0/24), SWI_002(Fa0/11), SWI_003(Fa0/12), SWI_003(Fa0/17) e SWI_003(Fa0/21).

Em relação às ligações dos servidores aos *switches*, aqueles que possuem ligações redundantes, estão configurados com um dos seguintes protocolos de *fail-over*: "Intel® Advanced Network Services" ou "Broadcom NetXtreme Gigabit Ethernet Teaming", que permitem a configuração de 2 placas de rede de modo a que uma delas apenas funcione caso a primeira falhe. O protocolo da Intel detecta as falhas de rede utilizando tráfego do tipo *broadcast* ou *multicast* [20] que no caso do IGC, se encontra configurado para tráfego do tipo *broadcast*, o que significa que, estando os equipamentos de rede ligados todos à mesma *VLAN* (VLAN1), à excepção de 2 servidores que se encontram ligados na VLAN2 (ver figura 21), todos terão que processar tráfego gerado pelos vários servidores causado por este protocolo e será ocupada largura de banda na rede que poderia ser utilizada para enviar informação [20]. O protocolo da Broadcom não utiliza tráfego *broadcast* nem *multicast* [21] pelo que não origina eventuais *broadcast storms* ao contrário do protocolo da Intel.

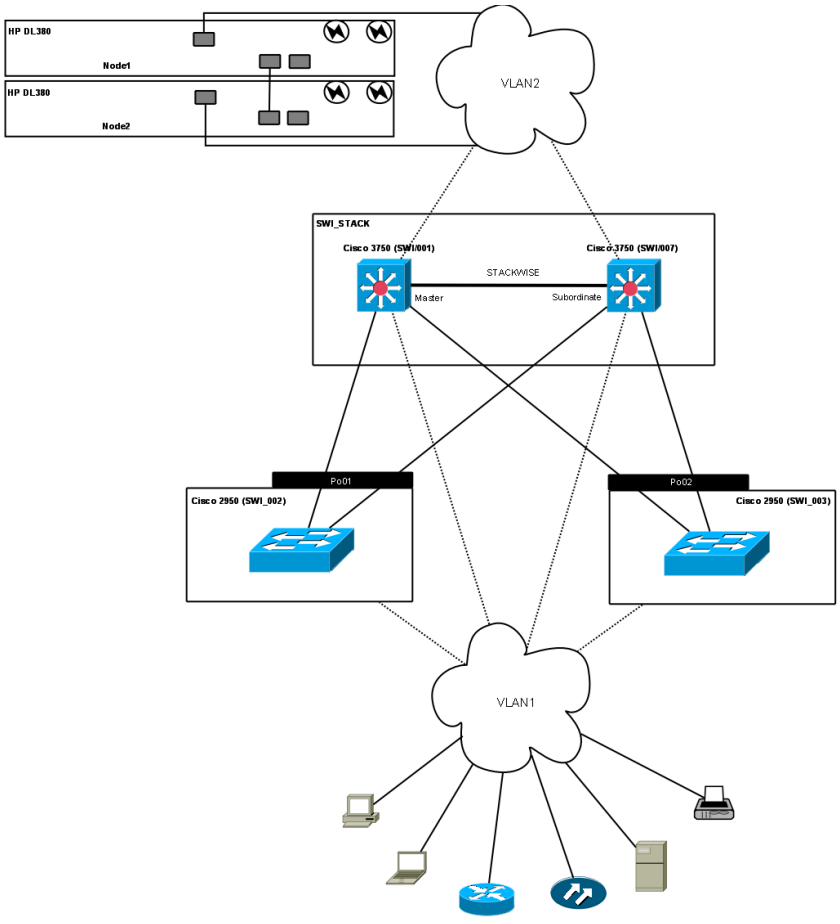


Figura 31 Esquema de ligações lógicas de equipamentos no Porto

O protocolo "Broadcom NetXtreme Gigabit Ethernet Teaming" é apenas utilizado pelo servidor SRV/014 (ver figura 16). Os restantes servidores com placas de rede redundantes utilizam o protocolo "Intel® Advanced Network Services".

Acerca da ligação à rede do ISI, é importante referir que, de acordo com a informação fornecida pela equipa técnica do ISI, esta disponibiliza um acesso a 2048 kbit/s, em que 1024 kbit/s estão reservados para a ligação ao *proxy* HTTP(S) da rede do ISI (que é de uso obrigatório). Os outros 1024 kbit/s são utilizados para todos os restantes serviços da rede, onde estão incluídos o e-mail, o acesso à rede do ISI e a ligação ao escritório de Lisboa do IGC.

3.3.3.2 Caracterização dos Activos de Rede em Lisboa

Em termos lógicos, o escritório de Lisboa, devido à simplicidade da rede de comunicações que o suporta, não apresenta pormenores de relevo a destacar nesta secção para além da configuração manual em quase todas as portas do *switch*, das instruções "`speed 100`"/"`speed 1000`" e "`duplex full`"/ "`duplex half`" que desactivam a detecção automática e tipo de transmissão. As seguintes portas encontram-se a funcionar em modo *half-duplex*: LISBOA-3500XL(Fa0/2) e LISBOA-3500XL(Fa0/19).

3.3.3.3 Tráfego na Rede

Os resultados da análise estatística obtida através do *software* de monitorização SolarWinds e que podem ser consultados no anexo A, permitem obter as seguintes conclusões:

- Os maiores picos de tráfego na rede interna são fora do horário normal de trabalho e podem ser justificados pelas políticas de *backup* implementadas, que estão descritas mais à frente neste documento;
- Na ligação para o exterior no Porto, através do *router* do ISI, o padrão de tráfego verificado resulta fundamentalmente dos fluxos associados ao *backup* de Lisboa, das limitações impostas nos serviços disponíveis e pelo uso obrigatório do *proxy* HTTP(S) no acesso à Internet. Mais pormenores sobre o tipo de tráfego poderão ser encontrados mais à frente neste relatório;
- No Porto, em todas as portas dos vários *switches*, o tráfego transmitido nunca é nulo, o que indicia a existência de determinado tráfego constante na rede que será identificado mais à frente neste documento;
- A estrutura que suporta a rede local do IGC suporta perfeitamente as suas exigências em termos de largura de banda de tráfego solicitadas, uma vez que todas as portas analisadas se encontram, em termos de utilização, muito abaixo do seu limite.
- Em Lisboa, as estatísticas recolhidas permitem concluir que a capacidade de acesso ao exterior disponível se encontra utilizada na sua totalidade (256 kbit/s) durante as horas normais de trabalho e, portanto, a comunicação entre o escritório do Porto e de Lisboa é estrangulada por esta limitação de acesso ao exterior. Assim, a largura de banda de apenas 256 kbit/s revela-se insuficiente para a actividade do escritório de Lisboa.

3.3.4 Análise da Rede

Nesta secção são apresentadas as informações ao nível da Rede, abordando sobre tudo a configuração IP da rede assim como caracterizando e analisando os principais fluxos de tráfego.

As figuras 32, 33 e 34 esquematizam a configuração IP da rede do Porto.

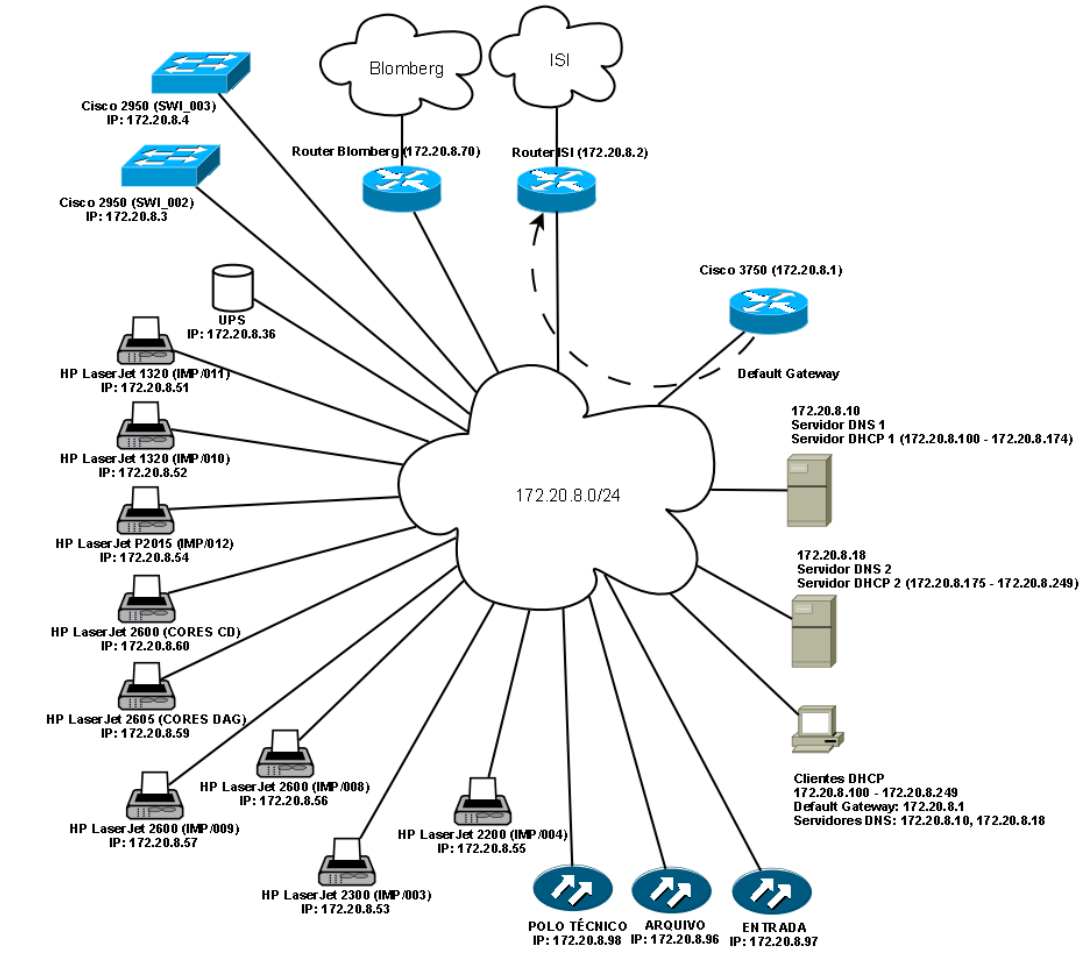


Figura 32 Diagrama IP da rede do Porto

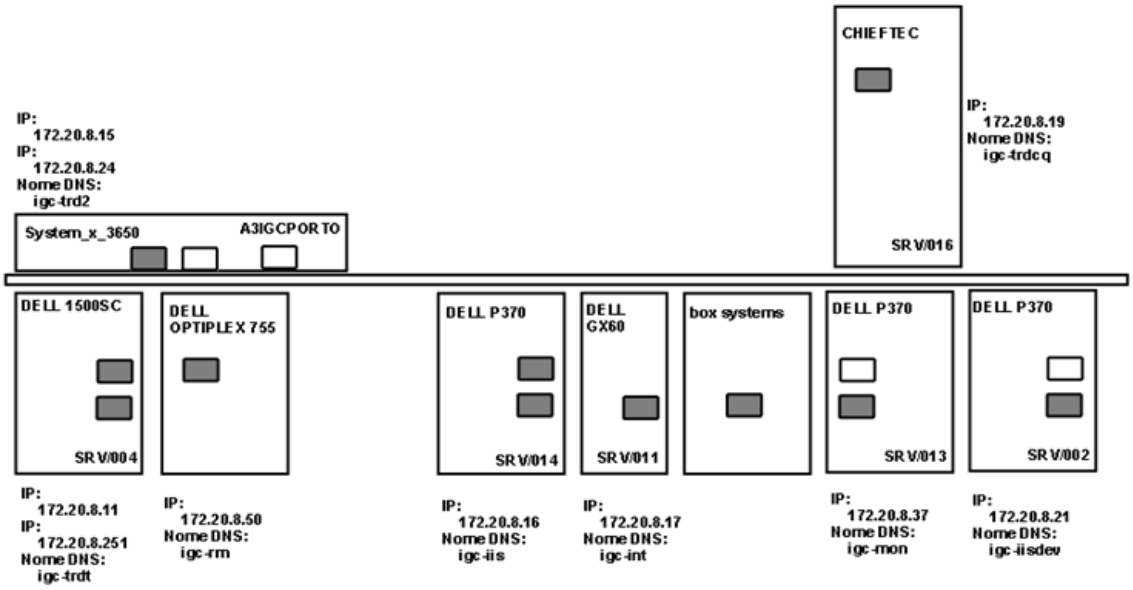


Figura 33 Endereços IP dos diversos servidores da “Bancada de Servidores”

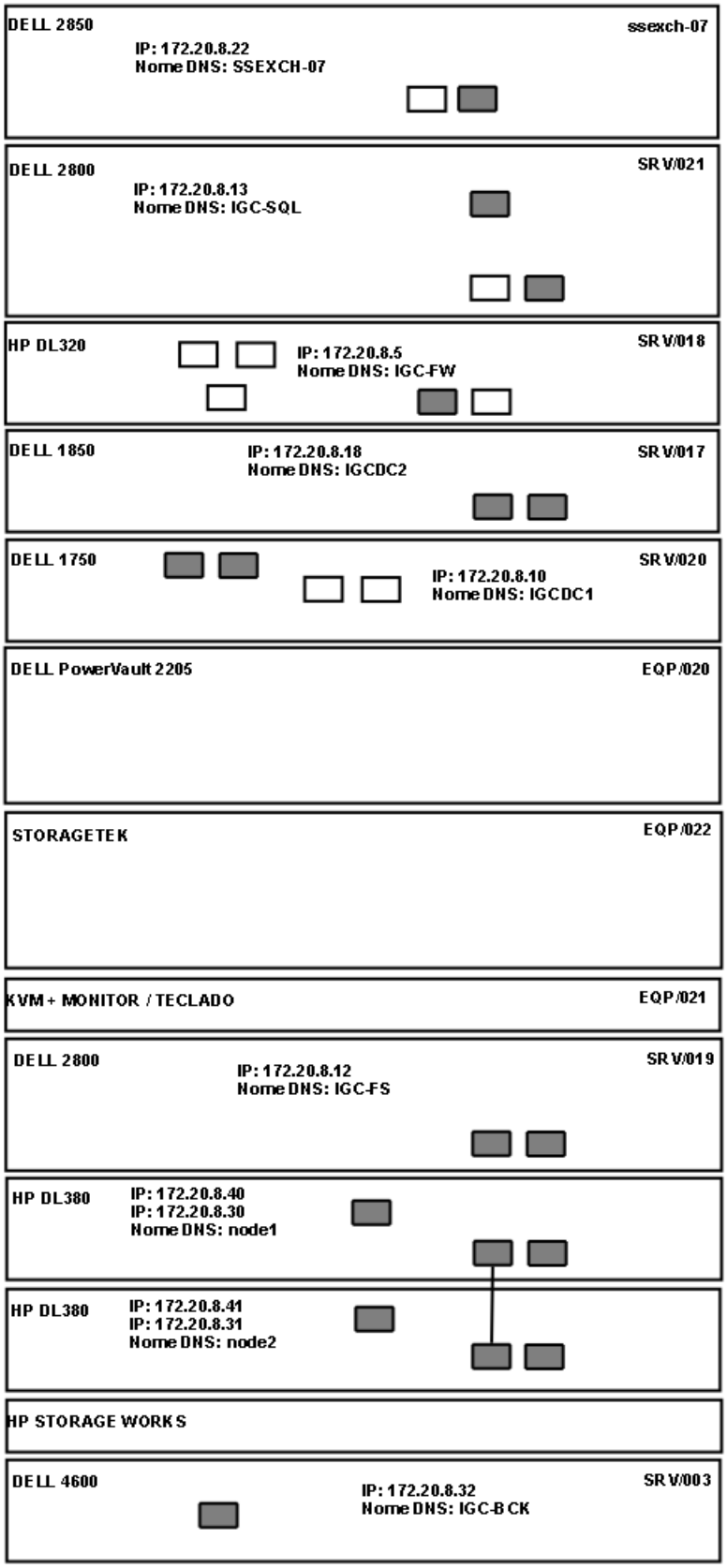


Figura 34 Endereços IP dos diversos servidores do "Armário de Servidores"

A figura 35 esquematiza a configuração IP da rede de Lisboa.

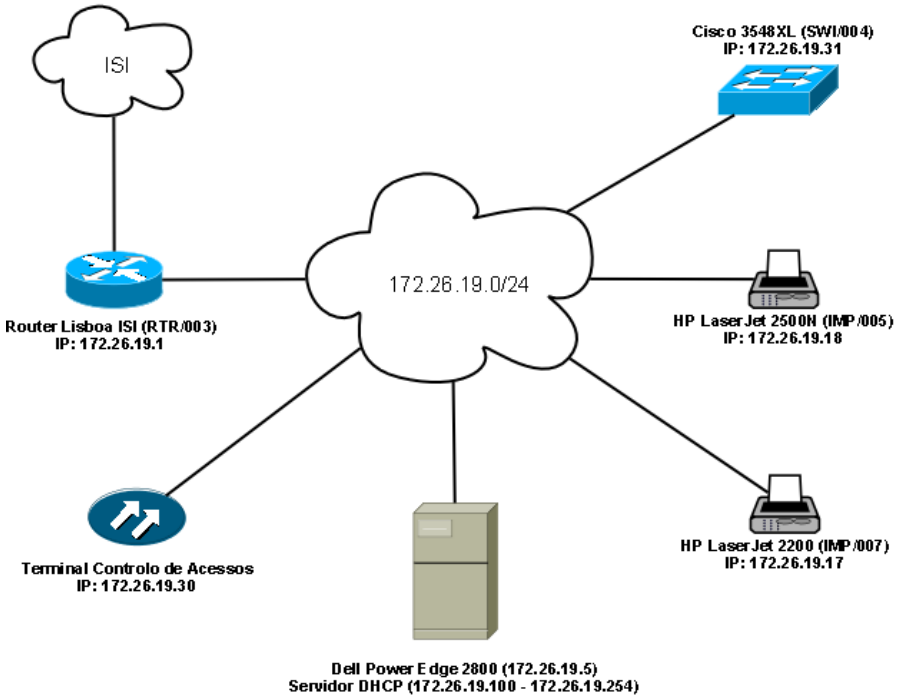


Figura 35 Diagrama IP da rede de Lisboa

3.3.4.1 Análise de fluxos de tráfego

Para analisar os fluxos de comunicação dos servidores considerados mais importantes e de forma a perceber as quantidades de tráfego transferidas, parceiros de comunicação frequentes e a distribuição temporal das transferências de dados foi utilizado o *software* NTOP[3]. Para a recolha de dados com o NTOP foi utilizado o protocolo Switched Port Analyzer (SPAN) [22] que permitiu enviar uma cópia do tráfego de uma ou mais portas do *switch* para a porta onde estava ligada a estação com o NTOP. Os dados obtidos através do NTOP são amostras de 24 horas recolhidas durante a semana. Para além destes dados, será possível analisar as estatísticas produzidas pelo equipamento PACKETEER 1500 cujos dados se baseiam numa amostra mensal. As estatísticas aqui em análise podem ser consultadas no anexo B.

Analisando todas as estatísticas relacionadas com os principais fluxos de tráfego presentes na rede de comunicações do IGC é possível concluir o seguinte:

- Existe claramente uma situação próxima de uma *broadcast storm* uma vez que a presença de pacotes do tipo *broadcast*, que são enviadas para todos os equipamentos da rede uma vez que não há segmentação através de *VLAN*'s, apresenta percentagens muito elevadas. Esta *broadcast storm* é causada pelo protocolo de *fail-over* da Intel utilizado nos servidores e já referido anteriormente neste documento. É importante referir que este tipo de pacotes obriga ao seu processamento, por parte de todos os equipamentos que os recebem, o que pode não ser verdadeiramente crítico para os servidores e estações de trabalho cuja capacidade de processamento é elevada, mas para outros dispositivos como impressoras e terminais de controlo de acesso pode representar uma

[3] Software de análise de tráfego de rede. Para mais informações consultar http://www.ntop.org

grande fatia da sua capacidade de processamento. O tamanho destes pacotes é reduzido, daí a elevada percentagens de pacotes com tamanho inferior a 64 bytes;

- As maiores transferências de dados são causadas pelas políticas de *backup* e que são normalmente realizadas durante a noite, o que permite concluir novamente que capacidade prestada pela rede local do IGC é perfeitamente suficiente para as suas necessidades. Os *backups* envolvem normalmente os servidores IGC-BCK e IGC-MON que são por isso parceiros de comunicação com maiores transferências de informação;
- Na ligação para o exterior, o padrão de tráfego verificado resulta fundamentalmente: dos fluxos associados ao *backup* de Lisboa, dos fluxos com os servidores do ISI, das limitações impostas nos serviços disponíveis e pelo uso obrigatório do *proxy* HTTP(S) no acesso à Internet. Destes fluxos podemos evidenciar: o Microsoft-DS que é o protocolo utilizado pela Microsoft para a transferência de ficheiros [23] e é justificada pelo acesso por parte de Lisboa a ficheiros localizados no IGC-FS no Porto e também pelos *backups* efectuados ao servidor de ficheiros de Lisboa; BITS que é o protocolo utilizado pela Microsoft para transferência das actualizações automáticas dos seus sistemas operativos [24] o que revela que existem estações/servidores a transferir estas actualizações; DCOM que é o protocolo utilizado pelo *Microsoft Exchange Server* para a troca de informação [25] e justifica-se pelo facto do servidor de correio dos utilizadores do IGC estar alojado no pólo técnico do Porto; e outros bastante conhecidos como o HTTP (acesso à internet), MSN Messenger, Simple Network Management Protocol (SNMP) – protocolo de gestão da rede utilizado pelo SolarWinds –, etc.

3.3.5 Análise Aplicacional/Serviços

De seguida serão apresentados os vários serviços suportados pela infra-estrutura de rede do IGC. Todos os serviços/aplicações são actualmente suportados pelo Sistema Operativo Microsoft Windows 2003 Server R2.

3.3.5.1 TRADER

A aplicação TRADER assume no negócio do IGC um papel fundamental pois, de uma forma muito simplificada, permite o registo de todas as transacções e eventos nos activos que compõem a carteira dos fundos sob gestão, a valorização dessas carteiras de activos e o respectivo cálculo de rentabilidades. Este serviço é suportado pelos servidores NODE1 e NODE2, configurados com a tecnologia Oracle Real Application Clusters[4].

Existe também uma máquina dedicada à realização de testes relacionados com a plataforma do TRADER, que corresponde ao servidor SRV/016 – IGC-TRDCQ (172.20.8.19).

Sobre o TRADER é relevante referir que este SI é fornecido pela CODEWARE com a qual o IGC tem contrato de manutenção, manutenção essa que é efectuada remotamente através de uma linha RDIS ligada a um modem no SRV/004 – IGC-TRDT executando o seguinte procedimento: a Codeware liga de determinado número para a linha RDIS associada a este servidor que, através de um mecanismo de *call-back*, desliga a chamada e procede à ligação

[4] Para mais informações consultar o White Paper: Oracle Real Application Clusters 10g (2005)

telefónica para a Codeware, activando de seguida uma conexão *dial-in*, que irá permitir o acesso à rede permitindo assim o acesso a este servidor em particular. A falta de implementação mecanismos de segurança não impõe quaisquer restrições a esta ligação havendo assim um o acesso total à rede do IGC.

3.3.5.2 Servidor de Base de Dados – SQL

O serviço de base de dados Microsoft Structured Query Language (SQL) Server é suportado pelo servidor SRV/021 – IGC-SQL (172.20.8.13) e é utilizado para armazenar os dados de todas as Bases de Dados do IGC à excepção daquelas que suportam os TRADER's. Este serviço encontra-se suportado pela versão 2000 Standard do Microsoft SQL Server.

3.3.5.3 Servidor de Ficheiros

Os servidores de ficheiros armazenam os ficheiros das áreas pessoais dos utilizadores assim como os ficheiros de partilha dos diversos departamentos evitando o armazenamento de ficheiros a nível local das máquinas facilitando assim a realização de cópias de segurança.

No Porto o serviço de ficheiros é suportado pelo SRV/019 – IGC-FS (172.20.8.12). Armazena os ficheiros partilhados pelos diversos departamentos e os ficheiros das áreas pessoais dos utilizadores do Porto.

Em Lisboa o serviço de ficheiros é suportado pelo Dell Power Edge 2800 – IGC-FSLX (172.26.19.5). No entanto, este servidor apenas armazena os ficheiros das áreas pessoais dos utilizadores de Lisboa. Para aceder aos ficheiros partilhados pelos diversos departamentos, os utilizadores de Lisboa têm que aceder ao servidor de ficheiros do Porto.

3.3.5.4 Intranet

O serviço de Intranet proporciona aos utilizadores do IGC uma automatização de diversos processos como marcação de tarefas, armazenamento e organização de documentos, entre muitos outros, visando facilitar e organizar o fluxo da informação entre os diversos trabalhadores do Instituto. Este serviço é suportado pelo servidor SRV/014 - IGC-IIS (172.20.8.16) que tens instalado o Internet Information Services (IIS) da Microsoft que recorre a uma base de dados SQL disponibilizada pelo serviço de Base de Dados SQL descrito anteriormente. Existe também um servidor dedicado à execução de uma plataforma de desenvolvimento da Intranet que é o SRV/002 – IGC-IISDEV (172.20.8.21).

3.3.5.5 Monitorização da Rede

A actual infra-estrutura da rede de comunicações do IGC é monitorizada pelo *software* SolarWinds, instalado no servidor SRV/013 – IGC-MON (172.20.8.37) que recebe as *traps* SNMP e mensagens SYSLOG dos diversos equipamentos, monitoriza através de SNMP os diversos servidores e equipamento activo de rede do Instituto. O SolarWinds recorre a uma base de dados SQL alojada no servidor SQL do IGC.

Para além do já referido, o IGC-MON tem instalado o Cisco Network Assistant utilizado para a gestão através de interface gráfico dos *switches* da Cisco.

3.3.5.6 E-mail

O serviço de e-mail é um dos serviços mais críticos para o negócio do IGC, uma vez que algumas das ordens de compra e venda de activos são transmitidas aos intermediários financeiros autorizados, através de automatismos específicos, que utilizam o e-mail como veículo de transmissão da informação. Perante esta criticidade, nesta secção será, numa primeira fase, descrito e caracterizado o serviço de e-mail e numa segunda fase, apresentados os resultados de um teste de carga que foi executado ao serviço.

Como forma de descrever o serviço de e-mail prestado pelo ISI é apresentado no esquema da figura 36, o caminho ou seja, os servidores que encaminham as mensagens enviadas/recebidas pelo IGC.

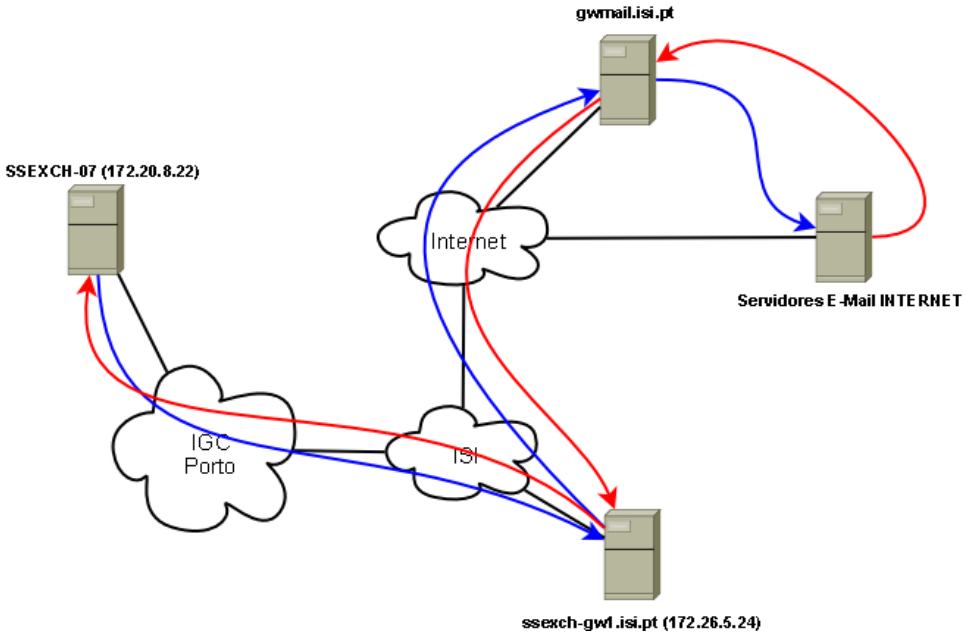


Figura 36 Caminho das mensagens electrónicas enviadas/recebidas pelo IGC

Uma vez que os e-mails mais críticos e que são enviados com mais frequência são aqueles destinados aos intermediários financeiros, foi feito o levantamento e caracterizados os domínios mais frequentemente utilizados:

Domínio: citigroup.com

Servidores de E-mail:

- cluster12.us.messagelabs.com (Prioridade: 10, Origem: United States);
- cluster12a.us.messagelabs.com (Prioridade: 20, Origem: United States).

Domínio: morganstanley.com

Servidores de E-mail:

- mx4.morganstanley.com (Prioridade: 0, Origem: United States);
- mx5.morganstanley.com (Prioridade: 10, Origem: United States);
- mx6.morganstanley.com (Prioridade: 10, Origem: United States);

- mx1.morganstanley.com (Prioridade: 10, Origem: United States);
- mx2.morganstanley.com (Prioridade: 10, Origem: United States).

Domínio: hsbc.com
Servidores de E-mail:

- symailserver.hsbc.co.uk (Prioridade: 10, Origem: United Kingdom);
- nwmailserver.hsbc.co.uk (Prioridade: 20, Origem: United Kingdom).

Domínio: db.com
Servidores de E-mail:

- smtp1.db.com (Prioridade: 10, Origem: United States);
- smtp7.db.com (Prioridade: 15, Origem: United States);
- smtp8.db.com (Prioridade: 10, Origem: United States);
- smtp6.db.com (Prioridade: 10, Origem: United States);
- smtp2.db.com (Prioridade: 10, Origem: United States);
- smtp0.db.com (Prioridade: 10, Origem: United States).

As cópias de segurança das contas de utilizadores do serviço de e-mail são feitas, segundo o ISI, diariamente através do servidor A3IGCPORTO que guarda a informação no servidor A3IGCPORTO. É no entanto relevante referir que o equipamento para efectuar o *backup* do e-mail veio duplicar os mecanismos de *backup* de informação de forma desnecessária, dado que o Instituto possui uma política de *backups* definida, suportada por *hardware* e *software* específico e adequado.

É possível comprovar, através da análise de fluxos, a transferência de 21.8 GB de dados durante a noite entre o servidor de e-mail e o A3IGCPORTO, o que leva a crer que seja devido ao *backup* às contas de e-mail. No entanto, a experiência passada do IGC demonstra a existência de falhas no processo de *backup* às caixas de correio electrónico, uma vez que na única situação em que foi necessário recuperar informação acidentalmente apagada, o ISI revelou-se incapaz de o fazer.

Com o objectivo de detectar e perceber os atrasos na entrega de mensagens frequentes no IGC, durante 13 dias foram enviados e-mails com uma cadência de 10 minutos, de uma caixa de correio do domínio isi.pt, alojada no servidor de e-mail localizado na sede do IGC do Porto, para caixas de correio alojadas em 5 domínios distintos. As contas dos destinatários do correio electrónico enviado foram programadas para fazer o reenvio automático do correio recebido para a conta do ISI, utilizada para enviar os e-mails. Para a elaboração de estatísticas que mostrem a qualidade do serviço prestado ou seja, o atraso dos e-mails enviados/recebidos que são extremamente críticos para o Instituto será medido o tempo que cada mensagem leva desde o seu envio até à sua recepção na conta de onde foi enviada, pertencente ao domínio isi.pt. Estes parâmetros foram lidos com base nos campos “Date Sent” e “Date Received” apresentados no Microsoft Outlook.

Nas estatísticas apresentadas de seguida calculou-se a média das durações de entrega dos e-mails numa base diária (24 horas e *WorkHours* que considerou-se ser das 8:00 às 18:00) e na distribuição pelos vários domínios dos destinatários utilizados.

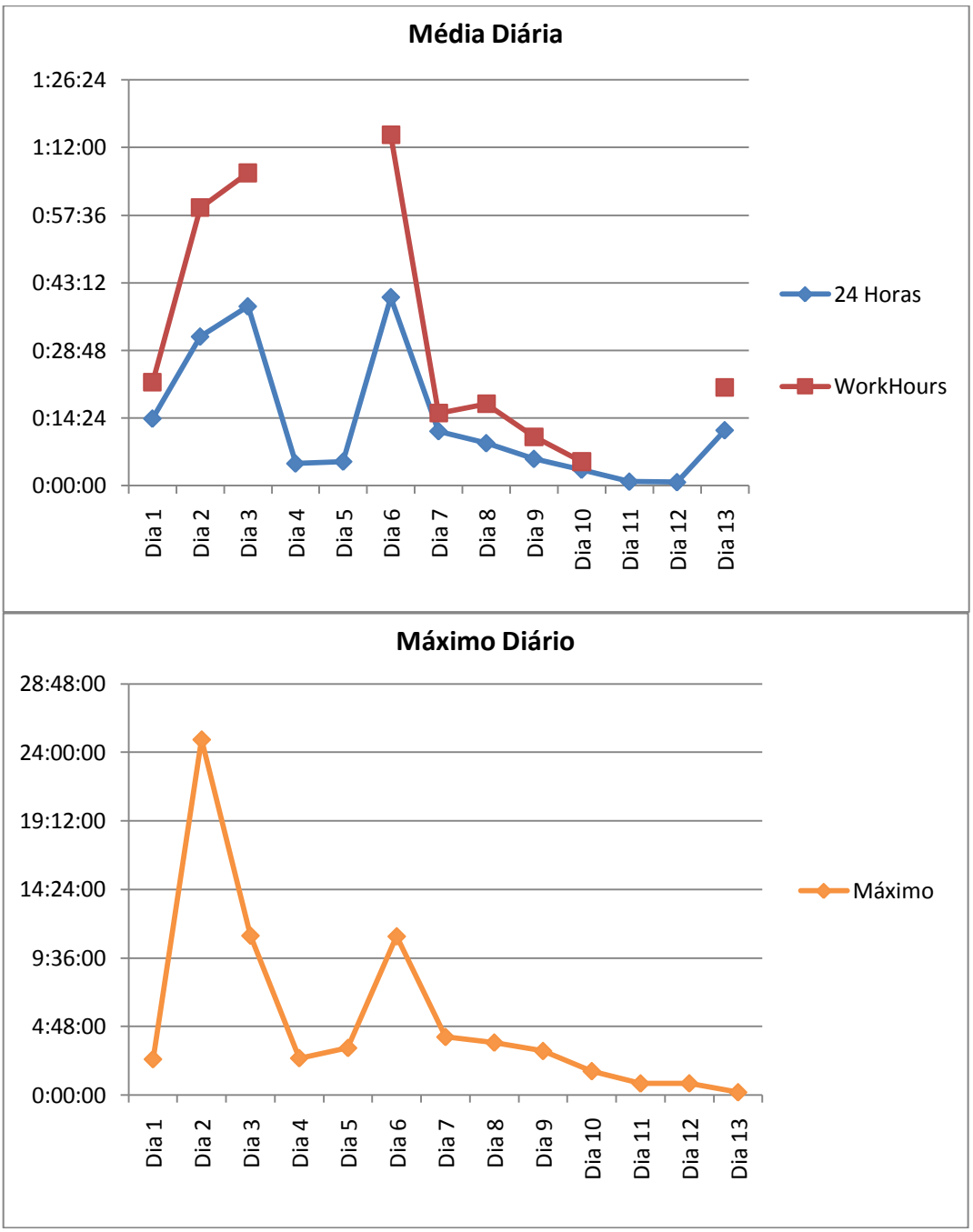


Figura 37 Distribuição diária dos tempos de entrega dos e-mails

As estatísticas apresentadas revelam um atraso médio de entrega das mensagens em 24 horas, de cerca de 14 minutos e em *WorkHours* de 33 minutos. É notória a diferença do atraso da entrega das mensagens em 24 horas e em *WorkHours*. Os 33 minutos de atraso médio nas entregas das mensagens em *WorkHours* é crítico para o negócio do IGC, uma vez que as ordens transmitidas aos *brokers* possuem hora limite para execução, o que leva a crer que ordens enviadas muito perto do prazo limite apresentem uma probabilidade alta de não serem entregues a tempo, situação que, de resto, já se verificou.

A distribuição diária dos atrasos na entrega dos e-mails é muito inconstante sendo difícil caracterizar o serviço prestado ISI classificando-o por isso como inconstante e insuficiente perante as necessidades do IGC.

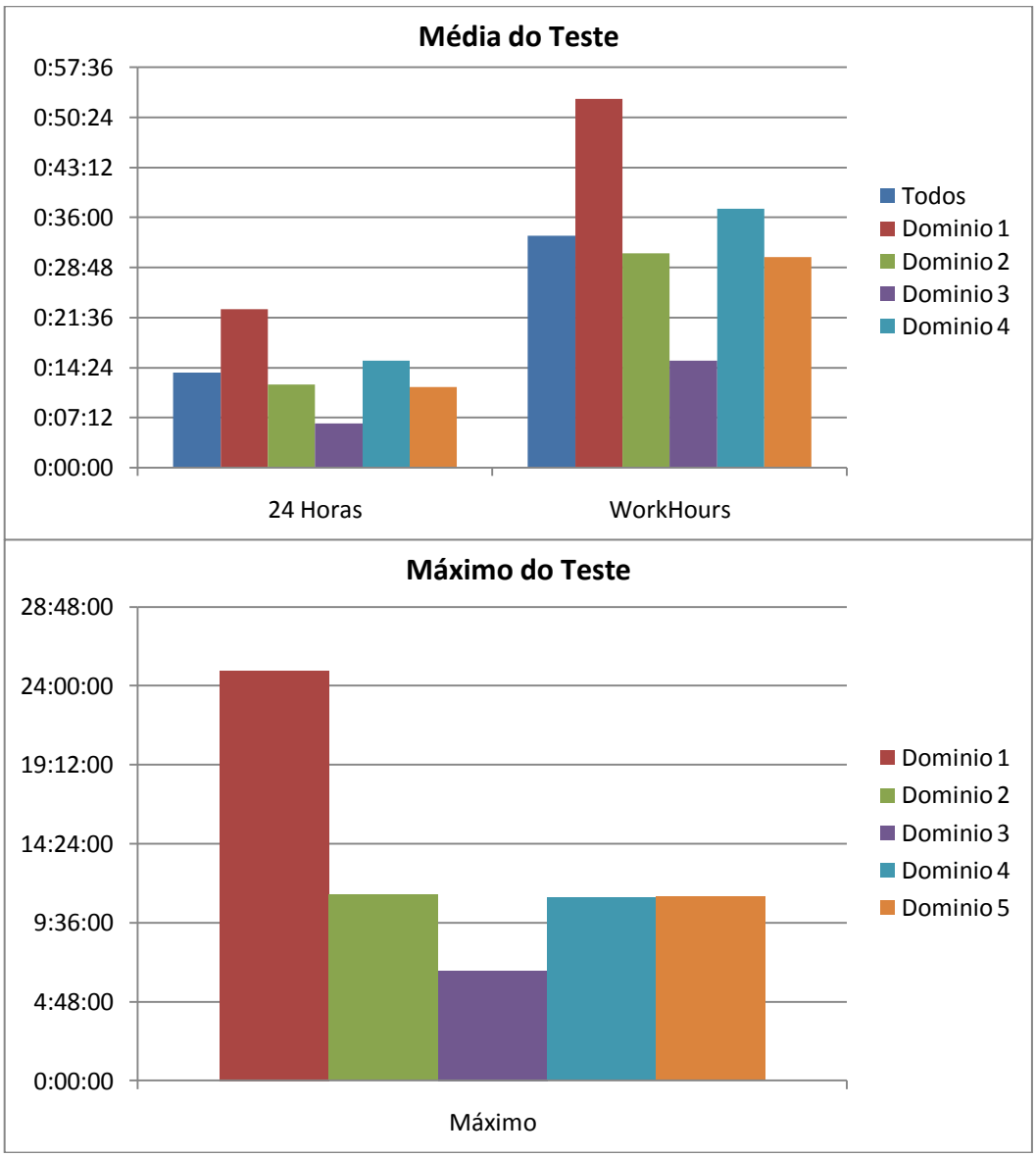


Figura 38 Distribuição por domínio do destinatário dos tempos de entrega dos e-mails

De forma a obter uma comparação, foi efectuado um teste em condições semelhantes e realizado nos mesmos dias, utilizando uma conta de correio alojada num domínio alugado que não oferece qualquer garantia de qualidade de serviço e embora tenha sido enviado um menor número de mensagens e utilizados apenas 3 domínios como contas para os destinatários das mensagens, foram usados os mesmos parâmetros para a obtenção dos dados da demora a entregar as mensagens.

Nos gráficos apresentados de seguida o termo "IGC" refere-se aos e-mails enviados a partir da conta do domínio isi.pt e o termo "COMPARAÇÃO" refere-se aos e-mails enviados a partir da conta alojada num domínio alugado.

Da análise dos gráficos pode-se concluir que o desempenho demonstrado pelo serviço de e-mail prestado pelo ISI é muito inferior ao do serviço de COMPARAÇÃO.

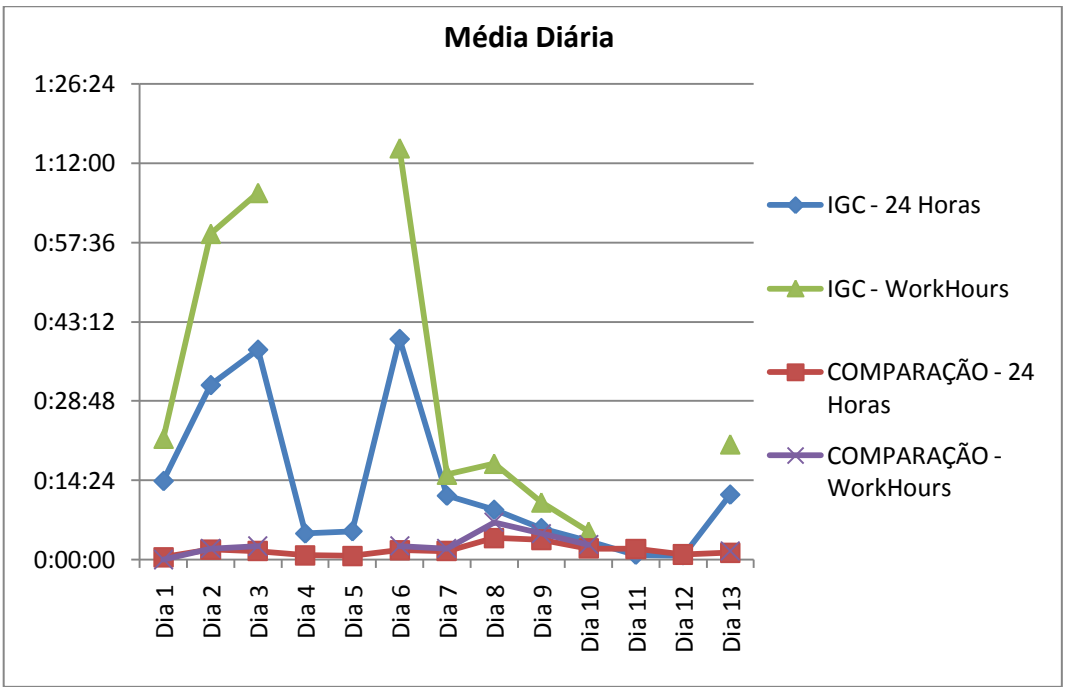


Figura 39 Comparação diária dos tempos de entrega dos e-mails

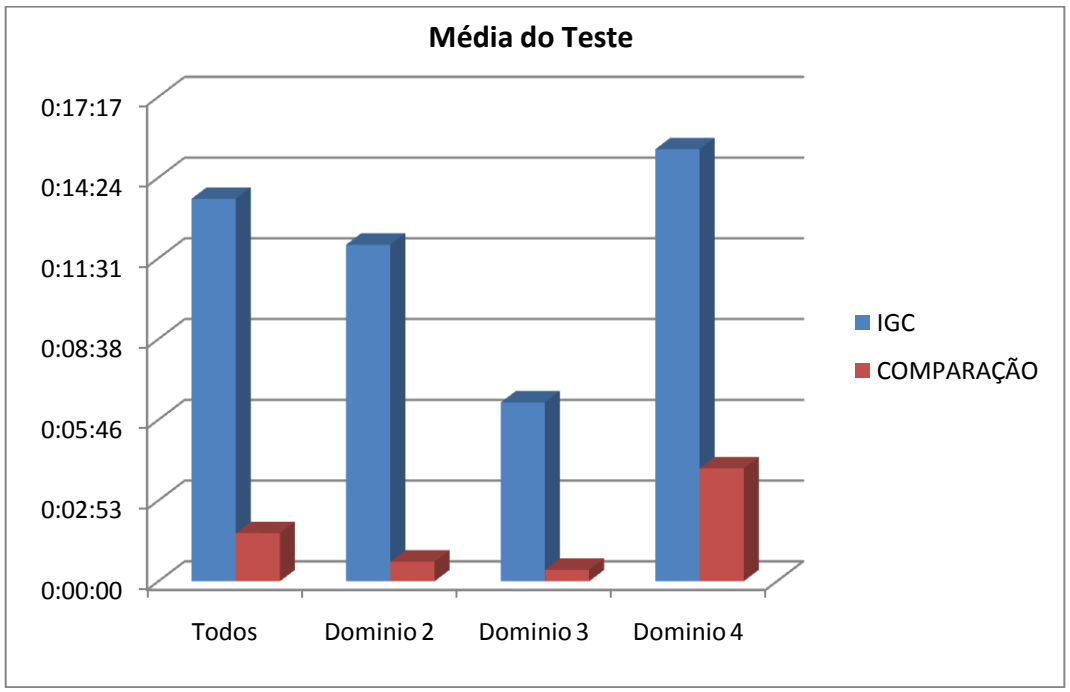


Figura 40 Comparação por domínio do destinatário dos tempos de entrega dos e-mails

3.3.5.7 Active Directory

O serviço de Active Directory (AD), responsável pela autenticação dos utilizadores no IGC, é prestado pelo ISI. O IGC diz respeito a um subdomínio denominado "igc.isi.pt" que é gerido de forma idêntica aos restantes subdomínios do ISI. O "igc.isi.pt" é suportado por 2 servidores instalados no escritório do Porto do IGC, que são os seguintes: SRV/020 – IGCDC1 (172.20.8.10) e SRV/017 – IGCDC2 (172.20.8.18).

Apesar do serviço de AD ser prestado pelo ISI, existe acesso de administração ao subdomínio do IGC. Desta forma, as políticas de segurança implementadas no "igc.isi.pt" podem ser definidas pelo IGC, no entanto, estas políticas podem também ser alteradas pelos administradores de topo, o que resulta na autorização do ISI para implementar políticas desenhadas por eles.

Para descrever o serviço da AD, no Anexo C, é apresentado o levantamento das políticas de grupo actualmente em efeito do domínio "igc.isi.pt".

Após analisar a configuração do serviço e as políticas de segurança implementadas, é relevante referir o seguinte:

- Na política CD, os drivers da impressora de Lisboa estão a ser instalados a partir do servidor de ficheiros do Porto (172.20.8.12) o que pode atrasar o tempo de execução do processo de Login nos PC's para os utilizadores onde esta política é aplicada;
- Nas políticas DAG, DEPC, DI, os drivers da impressora de Lisboa estão a ser instalados a partir do servidor "fef1edbdc" que não é um nome resolvido através do serviço DNS;
- Os drivers das impressoras são instalados localmente em todas as estações de trabalho o que resulta na comunicação das impressoras com vários computadores simultaneamente o que pode provocar uma falta de capacidade de resposta por parte das impressoras para atender todos os pedidos e pode esta ser a causa da falha frequente dos scripts de instalação das impressoras;
- O facto de o subdomínio da AD em que está incluído o IGC ser tratado de forma igual aos restantes subdomínios do ISI é uma fonte geradora de conflitos uma vez que as políticas de segurança aplicadas pelos administradores de topo são espalhadas por todos os subdomínios e, sendo o perfil dos utilizadores do IGC bastante distinto dos restantes utilizadores do ISI, pode haver políticas implementadas que entrem em conflito com as definições dos computadores no domínio igc.isi.pt. Exemplo disto são as políticas "Unat7" que proibiu a utilização de "Offline Files", funcionalidade utilizada pelos portáteis do IGC e a política "IE7 policy" que criou conflitos na utilização do Internet Explorer;
- Por diversas ocasiões, os técnicos do ISI actuaram sobre máquinas colocadas nas instalações do IGC (sem qualquer aviso e/ou pedido de autorização), tendo-se verificado a introdução de ficheiros infectados com vírus em servidores do Instituto, concretamente nos Controladores de Domínio – Domain Controller (DC). A figura 41 mostra alguns dos registos das detecções dos referidos vírus;

File	Status	Infection Name
C:\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\DOMAIN\SCRIPTS\DESKTOP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\SYSVOL\DESKTOP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\DOMAIN\SCRIPTS\ISABEL.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\SYSVOL\DESKTOP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\DOMAIN\SCRIPTS\DESKTOP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\SYSVOL\SYSVOL\DESKTOP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINNT\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24
C:\WINZIP_TMP.EXE	File was cured; system cure performed	Win32/Blackmal.FICME24

Figura 41 Vírus introduzidos pelos técnicos do ISI

- O facto de os subdomínios serem tratados de forma equivalente e haver uma relação de confiança implementada, cria a possibilidade de em qualquer estação do ISI ser possível realizar autenticação no subdomínio IGC e vice-versa o que abre espaço para a tentativa de descoberta de utilizadores/passwords e, no pior dos casos, caso se falhe a autenticação mais de 3 vezes, desencadear o processo de bloqueio da conta impedindo o utilizador vítima de executar login na sua máquina. Sobre esta situação resta acrescentar a presença constante de tentativas com e sem sucesso de autenticação, quer nos servidores quer nas máquinas afectas a colaboradores do IGC, com origem de máquinas localizadas nos restantes subdomínios. Esta situação foi reportada várias vezes à entidade que gere o domínio de topo, o ISI, sem que qualquer explicação fosse dada ou qualquer acção fosse desenvolvida no sentido de impedir que tal aconteça;
- É ainda importante referir que todos os utilizadores do subdomínio IGC são administradores locais das máquinas o que para além de permitir a instalação de *software* não autorizado, abre portas para vírus/ataques que necessitem de acesso de administrador, que é naturalmente cedido pelo facto de todos terem essa permissão.

3.3.5.8 Proxy Web

O serviço de Proxy Web, de utilização obrigatória, como intermediário das comunicações feitas sobre HTTP(s) para a Internet está a cargo do servidor SRV/018 - IGC-FW (172.20.8.5). Este servidor tem instalado o *software* da Microsoft, ISA Server 2004.

Este servidor encontra-se configurado para aceitar ligações de qualquer rede, destinadas a qualquer rede, executadas por qualquer utilizador. Não existe assim qualquer protecção sobre quem utiliza este serviço, estando ele disponível a qualquer computador que lhe consiga estabelecer uma ligação.

Os pedidos HTTP(s) efectuados a este servidor são de seguida redireccionados para "ssproxysvc.isi.pt" sendo que pedidos HTTP utilizarão a porta 80 e os pedidos HTTPs utilizarão a porta 8443. Não é permitido o acesso à Internet em HTTP(S) sem a utilização do proxy.

De seguida são apresentadas as principais estatísticas produzidas pelo ISA Server 2004 durante o mês de Março de 2009 que, são representativas das estatísticas de todos os outros meses.

A figura 42 apresenta os endereços IP das estações que geraram mais tráfego, que foi processado pelo servidor Proxy, durante o período atrás referido.

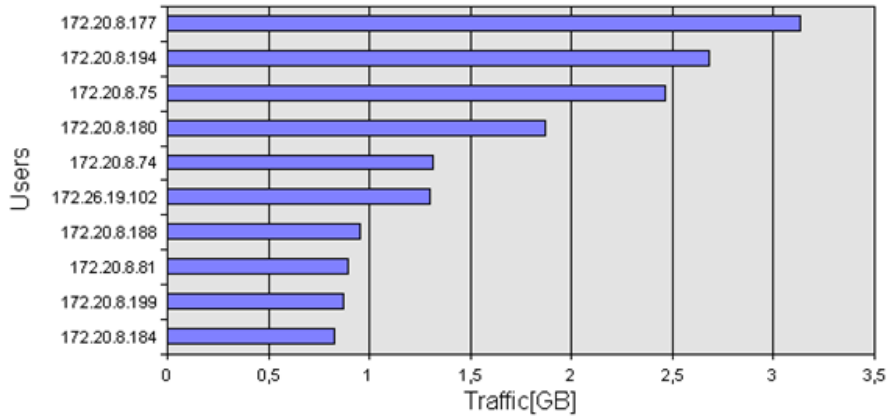


Figura 42 Endereços IP que geraram mais tráfego no serviço de Proxy em Março de 2009

A figura 43 apresenta os endereços dos sites mais visitados.

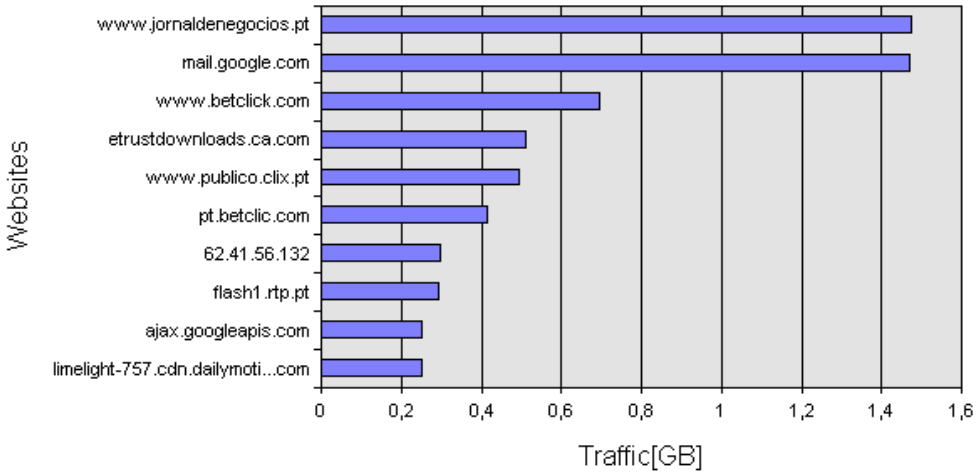


Figura 43 Endereços dos sites mais visitados

A figura 44 apresenta as estatísticas da eficácia da cache mantida pelo servidor proxy.

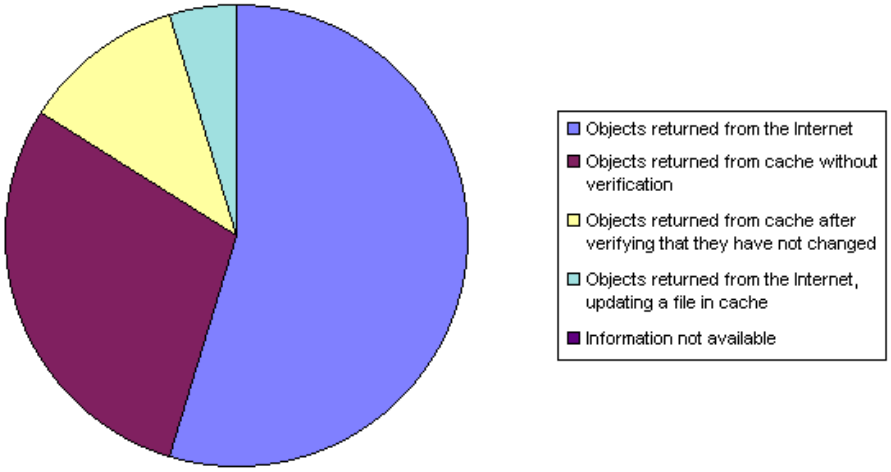


Figura 44 Estatísticas da eficácia da cache mantida pelo servidor proxy

A figura 45 apresenta a estatística mensal do tráfego gerado.

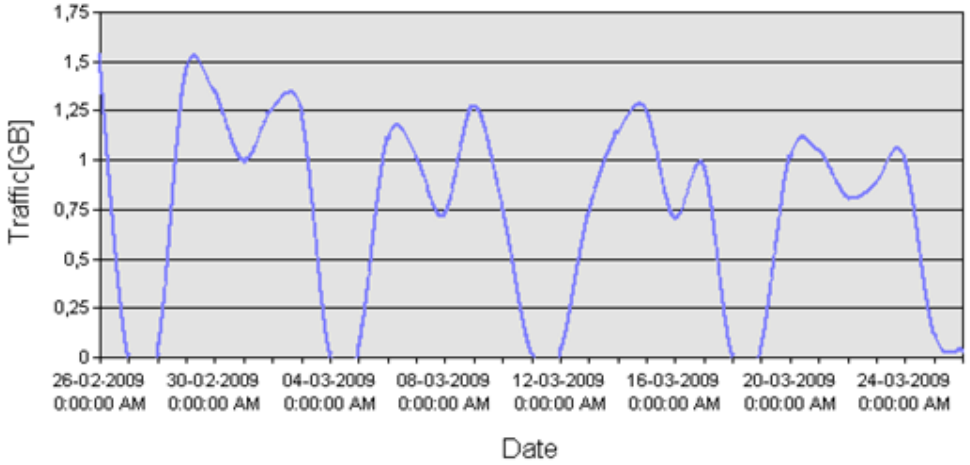


Figura 45 Estatística mensal do tráfego gerado no Proxy

A figura 46 apresenta a estatística diária do tráfego gerado.

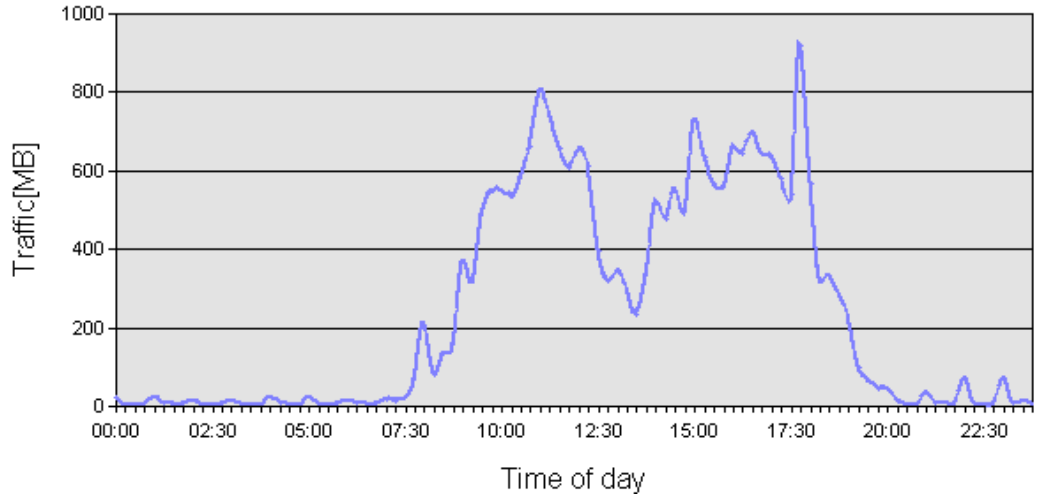


Figura 46 Estatística mensal do tráfego gerado no Proxy

A figura 47 apresenta a média de utilização diária, das 8:00 às 18:00, do serviço de Proxy.

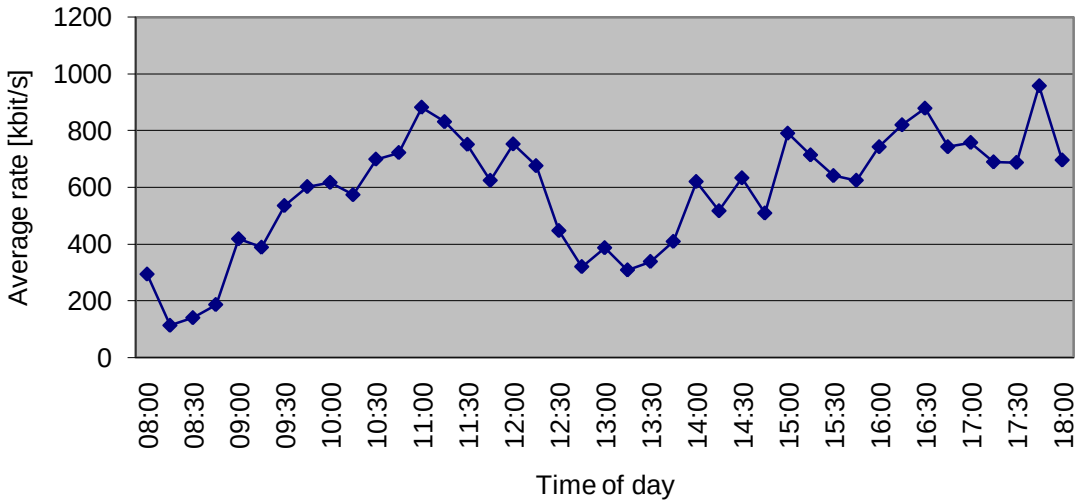


Figura 47 Média de utilização diária do serviço de Proxy

Sobre as estatísticas apresentadas é importante dar relevo aos seguintes aspectos:

- As estatísticas da eficácia da cache mantida pelo servidor proxy apresentam um desempenho bastante satisfatório o que leva a concluir que a implementação deste serviço contribuiu para um melhor desempenho no acesso à Internet;
- Um dos endereços IP que gera mais tráfego mensalmente é 172.26.19.102 que pertence à rede do escritório de Lisboa. O tráfego gerado por este IP contribui no entanto para a saturação do circuito de acesso ao exterior no escritório do Porto, devido aos fluxos que são criados por este tráfego e se encontram esquematizados na figura 48. Através da análise do esquema apresentado, é possível observar a quantidade de fluxos de tráfego bidireccionais criados no circuito de acesso ao exterior no Porto.

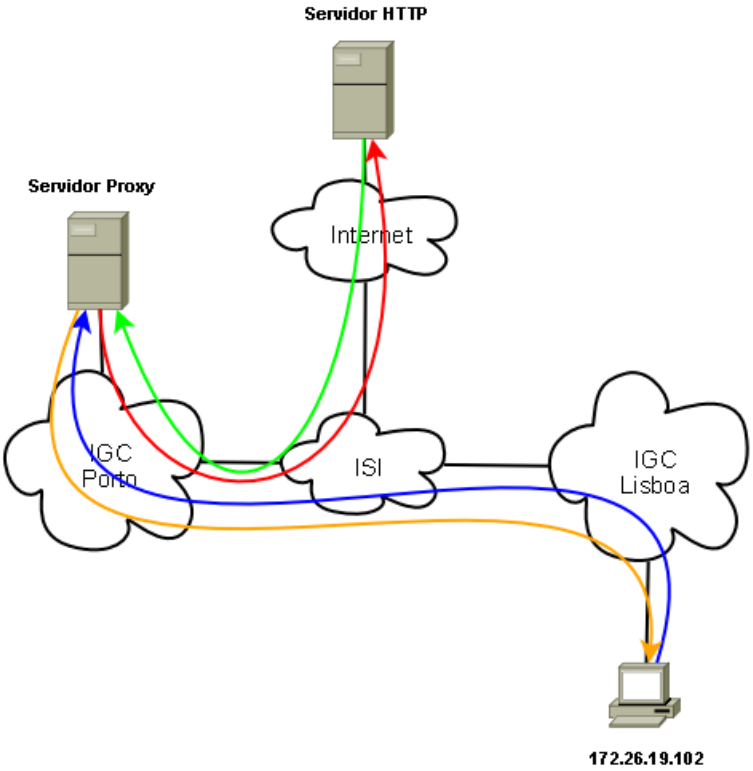


Figura 48 Esquema dos fluxos de tráfego criados por um acesso à internet de um IP de Lisboa

- O padrão de tráfego apresentado na figura 47 é coerente com o típico verificado numa empresa durante o horário normal de trabalho. No entanto, os dados referentes ao volume de tráfego não permitem fazer conclusões sobre a utilização efectiva da banda disponível no circuito de acesso ao exterior porque este proxy não comunica directamente, pela Internet, com os sites de origem dos URLs solicitados, mas apenas faz o reenvio dos pedidos dos URLs para o proxy disponibilizado pelo ISI ("ssproxysvc.isi.pt").

3.3.5.9 Serviço de Resolução de Nomes – DNS

O serviço de resolução de nomes, DNS, é suportado pelos servidores SRV/020 – IGCDC1 (172.20.8.10) com o papel de servidor primário e SRV/017 – IGCDC2 (172.20.8.18) com o papel de servidor secundário. Em seguida são apresentadas as definições mais relevantes relativas à configuração deste serviço:

Forwarding Lookup Zone: igc.isi.pt

Reverse Lookup Zones:

- 172.26.19.x Subnet;
- 172.25.2.x Subnet;
- 172.23.33.x Subnet;
- 172.23.37.x Subnet;
- 172.20.8.x Subnet

Servidores DNS para a zona igc.isi.pt:

- igcdc2.igc.isi.pt (172.20.8.18)
- ssrootdc1.ssroot.isi.pt (172.26.3.5)
- ns2.isi.pt (172.20.1.13)
- ns1.isi.pt (172.26.3.2)
- igcdc1.igc.isi.pt (172.20.8.10)
- ssrootdc3.ssroot.isi.pt (172.26.3.7)

Intervalo de Actualização (Refresh Interval): 15 minutos
Intervalo de Tentativa (Retry Interval): 10 minutos
Tempo de expiração (Expiration time): 1 dia
Tempo de Vida Mínimo (Minimum TTL): 1 hora
Forwarders: 172.26.3.5, 172.26.3.7, 172.26.3.2, 172.20.1.13

3.3.5.10 Serviço de Atribuição Automática de Configurações – DHCP

O escritório do Porto tem 2 servidores responsáveis por fazer a atribuição automática de configurações às estações de trabalho configuradas como cliente Dynamic Host Configuration Protocol (DHCP). De seguida são sintetizadas as configurações dos 2 servidores DHCP.

Servidor: SRV/020 – IGCDC1 (172.20.8.10)
Opções DHCP:
Gama IP's atribuídos: 172.20.8.100 - 172.20.8.174
Default Gateway: 172.20.8.1
Servidores DNS: 172.20.8.10, 172.20.8.18
Domínio DNS: igc.isi.pt
Servidor NTP: 172.20.8.10
Reservas:

- MAC: 001e4fa33693 – IP: 172.20.8.74
- MAC: 0015c559a353 - IP: 172.20.8.78
- MAC: 001e4fa2b749 - IP: 172.20.8.79
- MAC: 009027bee112 - IP: 172.20.8.80

Duração das atribuições (Lease duration): 8 dias
Actualização automática registos DNS: SIM

Servidor: SRV/017 – IGCDC2 (172.20.8.18)
Opções DHCP:
Gama IP's atribuídos: 172.20.8.175 - 172.20.8.249
Default Gateway: 172.20.8.1
Servidores DNS: 172.20.8.10, 172.20.8.18
Domínio DNS: igc.isi.pt
Servidor NTP: 172.20.8.10
Reservas:

- MAC: 0015c559a353 - IP: 172.20.8.78

- MAC: 001e4fa2b749 - IP: 172.20.8.79
- MAC: 500814ac - IP: 172.20.8.80
- Mac: 0002b3a85d8f – IP: 172.20.8.81

Duração das atribuições (Lease duration): 8 dias

Actualização automática registos DNS: SIM

No escritório de Lisboa a atribuição automática de endereços IP está a cargo de apenas um servidor. De seguida estão sintetizadas as configurações DHCP desse servidor.

Servidor: Dell Power Edge 2800 – IGC-FSLX (172.26.19.5)

Opções DHCP:

Gama IP's atribuídos: 172.26.19.100 - 172.26.19.254

Default Gateway: 172.26.19.1

Servidores DNS: 172.26.3.5, 172.26.3.7, 172.23.3.2, 172.20.8.18, 172.20.8.10

Domínio DNS: igc.isi.pt

Servidor WINS: 172.26.3.4, 172.26.3.11, 172.20.8.5

Reservas:

- MAC: 000d56ddac35 - IP: 172.26.19.40
- MAC: 000c6e33b51b - IP: 172.26.19.74
- MAC: 0015c559a353 - IP: 172.26.19.78
- MAC: 0015c559a47b - IP: 172.26.19.79

Duração das atribuições (Lease duration): 1 dia

Actualização automática registos DNS: NÃO

É importante referir a configuração de 5 endereços IP (172.26.3.5, 172.26.3.7, 172.23.3.2, 172.20.8.18, 172.20.8.10) com funções de servidores DNS que correspondem a endereços IP localizados na rede do ISI e no pólo técnico do IGC no Porto (os últimos 2), originando que os pedidos de resolução de nomes sejam efectuados ou na rede do ISI ou no escritório do Porto do IGC o que obriga a que o tráfego de resolução de nomes passe sempre pela ligação para o exterior que é apenas de 256 kbit/s. Foi solicitado ao ISI que o servidor de Lisboa fizesse a resolução de nomes, pedido esse que foi recusado.

3.3.5.11 Serviço Blomberg

Nesta secção é feita a caracterização do serviço de ligação à Blomberg com a apresentação das rotas estáticas definidas nos terminais da Blomberg, que usam como gateway de saída o *router* da Blomberg, e das rotas anunciadas dinamicamente por esse *router* através do protocolo RIPv2.

As rotas estaticamente configuradas nos terminais Blomberg são:

Network Destination	Netmask	Gateway	Interface	Metric
69.184.0.0	255.255.0.0	172.20.8.70	172.20.8.196	1
199.105.176.0	255.255.248.0	172.20.8.70	172.20.8.196	1
199.105.184.0	255.255.254.0	172.20.8.70	172.20.8.196	1
205.183.246.0	255.255.255.0	172.20.8.70	172.20.8.196	1
208.134.161.0	255.255.255.0	172.20.8.70	172.20.8.196	1

As rotas anunciadas dinamicamente pelo *router* da Blomberg, através do protocolo RIPv2, são:

```
Network              Netmask              Metric
69.184.0.0           255.255.255.192             4
69.184.1.0           255.255.255.192             2
69.184.36.0          255.255.255.192             4
69.184.36.64         255.255.255.192             4
69.184.37.0          255.255.255.192             2
69.184.37.64         255.255.255.192             2
69.184.40.0          255.255.255.192             4
69.184.40.64         255.255.255.192             4
69.184.54.64         255.255.255.192             2
69.184.54.128        255.255.255.192             2
199.105.181.0        255.255.255.192             4
199.105.181.64       255.255.255.192             2
199.105.181.192      255.255.255.192             2
208.134.161.0        255.255.255.192             4
208.134.161.15       255.255.255.255             4
208.134.161.16       255.255.255.255             4
208.134.161.17       255.255.255.255             4
208.134.161.30       255.255.255.255             4
208.134.161.41       255.255.255.255             4
208.134.161.43       255.255.255.255             4
208.134.161.45       255.255.255.255             4
208.134.161.46       255.255.255.255             4
208.134.161.64       255.255.255.192             4
208.134.161.128      255.255.255.192             2
208.134.161.192      255.255.255.192             2
```

Pelos dados apresentados, parece evidente que há informação de routing redundante e desnecessária nas configurações, o que poderá, eventualmente, resultar na inacessibilidade de algumas rotas caso sejam feitas alterações aos anúncios de routing para a Blomberg.

3.3.5.12 Políticas de Backup Implementadas

O *software* utilizado para a realização de *backups* de forma automatizada é o CA BrightStore ArcServe. Este *software* encontra-se programado para implementar o esquema de *backups* caracterizado através da tabela 3

Tabela 3 Esquema de *backups* implementado no IGC

Backup	Schedule	Armazenamento	Retenção
Diario	Segunda a Sexta, às 23:59:00	Interno	7 dias
DiarioTape	Segunda a Sexta, no final do job diário	Externo	7 dias
Mensal	4º Sábado do Mês, às 23:59:00	Interno	12 Meses
MensalTape	4º Sábado do Mês, no final do Job mensal	Externo	12 Meses
Anual	Retirada a tape do Job mensal de Dezembro	Interno	5 Anos
AnualTape	Retirada a tape do Job mensal de Dezembro	Externo	5 Anos

Todos os *backups* realizam cópias de segurança de todos os servidores através de agentes específicos da CA consoante as aplicações/serviços que suportam. Os *backups* Diario, Mensal e Anual são armazenados no array de discos do IGC os restantes são armazenados em suportes magnéticos. Estes suportes são enviados para o exterior, através de um serviço da ESEGUR, de

forma a garantir a disponibilidade dos dados em caso de desastre no escritório do Porto. Os *backups* DiárioTape são recolhidos às 2ªs, 4ªs e 6ªs feiras. Os restantes *backups* armazenados em suporte magnético são enviados para o exterior mediante solicitação do IGC não havendo assim recolhas pré-programadas.

Sobre as políticas de *backup* implementadas é importante referir que os *backups* do TRADER não são feitos através do *software* de *backups* implementado devido a incompatibilidade com o ORACLE e à forma como o TRADER se encontra configurado. Os *backups* são então executados através das opções de *backup* do ORACLE e guardados no IGC-MON, devido à sua grande capacidade de armazenamento, e este sim tem o agente da CA a correr. No entanto o servidor IGC-MON não está alimentado electricamente através de qualquer sistema redundante nem tem sequer ligação de rede redundante aos 2 *switches* do *Core*, o que revela um ponto de fragilidade na política de *backups* implementadas uma vez que caso haja uma avaria na placa de rede ou na fonte de alimentação do IGC-MON que não seja detectada, durante esse período não serão executados quaisquer *backups* ao TRADER.

O IGC sente que, apesar de garantirem que não há informação perdida em caso de desastre no escritório do Porto, o tempo de recuperação em caso de catástrofe ou seja, o tempo necessário desde um possível desastre até que os colaboradores do IGC tenham novamente acesso à informação que necessitam para trabalhar é demasiadamente elevado e por essa razão consideram como requisito importante a criação de uma infra-estrutura que suporte políticas e procedimentos de DR e que garanta um tempo menor de acesso à informação em caso de catástrofe.

3.3.6 Síntese de Incidentes Relevantes

Nesta secção são sintetizados os incidentes identificados que se consideram relevantes:

- As condições técnicas (eléctricas, ambientais e físicas) das infra-estruturas dos pólos técnicos do Porto e Lisboa são insuficientes, inexistentes ou inadequadas para o fim a que se destinam;
- A ligação de acesso ao exterior no escritório de Lisboa encontra-se completamente esgotada quer durante as horas normais de trabalho quer durante o período da noite em que é efectuado o *backup* ao servidor de ficheiros em Lisboa. A reduzida largura de banda desta ligação causa um ponto de estrangulamento na ligação ente o escritório do Porto e Lisboa, o que impede uma maior utilização da largura de banda disponível no circuito de acesso no Porto;
- Os dados transferidos entre o escritório do Porto e Lisboa viajam, na rede do ISI, sem qualquer tipo de protecção que garanta a sua confidencialidade e integridade;
- Na rede local do Porto existe um excesso de tráfego de pacotes *broadcast* provocado pelo protocolo da Intel de *fail-over* utilizado nos servidores que, devido à existência de um único domínio de *broadcast* uma vez que não estão implementadas *VLAN*'s, os seus pacotes são processados por todos os equipamentos ligados à rede;
- Tanto no Porto como em Lisboa, há portas dos *switches* a funcionar em modo *half-duplex*. Caso não seja uma limitação dos equipamentos ligados a essas portas, tal constitui um subaproveitamento da capacidade de comunicação disponível;

- O facto de as impressoras comunicarem directamente com todas as estações de trabalho, não havendo um servidor de impressões a intermediar esta comunicação, pode provocar uma falta de capacidade de resposta por parte das impressoras para atender todos os pedidos e pode ser esta a causa da falha frequente dos seus scripts de instalação;
- O facto de o subdomínio da AD em que está incluído o IGC ser tratado de forma igual aos restantes subdomínios do ISI revela-se uma falha de segurança, uma vez que não existem quaisquer protecções que regulem o tráfego entre os vários subdomínios; tal poderia fazer sentido no restante universo da holding onde se insere o IGC, mas não incluindo lá o IGC uma vez que o seu negócio e o perfil dos seus utilizadores são totalmente diferentes dos restantes;
- Os utilizadores do subdomínio IGC são administradores locais das máquinas o que para além de permitir a instalação de *software* não autorizado, abre portas para vírus/ataques que precisem de acesso de administrador que é naturalmente cedido pelo facto de todos os utilizadores terem essa permissão;
- Um dos endereços IP que gera mais tráfego HTTP, mensalmente, é 172.26.19.102 que pertence à rede do escritório de Lisboa. O tráfego gerado por este IP contribui no entanto para a saturação do circuito de acesso ao exterior no escritório do Porto, devido aos fluxos que são criados por este tráfego e se encontram esquematizados na figura 48;
- O servidor IGC-MON está a ser utilizado para a realização de tarefas críticas como é o caso da execução de *backups*, tratando-se no entanto de um servidor sem quaisquer mecanismos de redundância de fonte de alimentação nem redundância de ligação à rede;
- Não está disponível o serviço Network Time Protocol (NTP) que permita sincronizar e manter actualizado o relógio de tempo real nos servidores e clientes da rede;
- O serviço de e-mail prestado ISI teve um comportamento caracterizado como inconstante e insuficiente para as necessidades do IGC;
- Desde o dia 12 de Março, pelas 10:00, até ao dia 13, pelas 11:00, o IGC esteve sem acesso ao serviço de E-mail e com problemas na comunicação entre os escritórios do Porto e de Lisboa. De acordo com a informação que foi possível obter junto da equipa técnica do ISI, tal deveu-se a alterações da configuração dos *routers* de acesso do ISI. Do ponto de vista da relação Fornecedor de Serviço e Utilizador, para além dos problemas resultantes desta interrupção do serviço, parece ser injustificado a realização deste tipo de alterações sem previamente notificar o utilizador (IGC) e eventualmente combinar a melhor altura para o fazer.

3.4 Conclusões

Neste capítulo pretende-se apresentar as conclusões mais relevantes sobre o estudo elaborado na fase de preparação e planeamento, que deverão servir como ponto de partida para o desenho da nova infra-estrutura. Para cada um destes pontos identificados é apresentada uma avaliação sumária, com referência a eventuais soluções ou estudos alternativos.

As necessidades de acesso específicas para no Porto e em Lisboa configuram requisitos para a avaliação de cenários alternativos de interligação dos pólos e acesso à Internet. Apesar de

parecer ser indispensável a avaliação e resolução deste problema de uma forma global e integrada, são referidos a seguir problemas de acesso ao exterior, pontuais e específicos.

A reduzida largura de banda disponível para o acesso ao exterior em Lisboa poderá ser resolvida com a negociação do aumento da sua capacidade ou através da contratação de um ISP que forneça um serviço que permita interligar as redes do Porto e Lisboa com maior capacidade de transmissão dados.

O facto dos dados transferidos entre Porto e Lisboa viajarem na rede do ISI sem qualquer protecção que garanta a sua confidencialidade e integridade pode ser solucionado com a implementação de mecanismos criptográficos.

A aparente não utilização de toda a largura de banda disponível no circuito de acesso ao exterior poderá ser explicada pelo facto de a única forma de sair para a Internet ser através do proxy disponibilizado pelo ISI, limitando a largura de banda a 1024 kbit/s e invalidando a utilização de outros serviços importantes que poderão facilitar a actividade do IGC.

A existência excessiva de tráfego do tipo *broadcast* que se espalha a toda a rede do Porto, pode ser atenuada através da implementação de vários domínios de *broadcast* com base na criação de *VLAN*'s ou através da reconfiguração do referido protocolo para não utilizar tráfego deste tipo.

A existência de portas dos *switches* a funcionar em modo *half-duplex* deve ser analisada, procurando descobrir a causa de tal acontecer. Tal poderá ser devido à limitação dos equipamentos, a ligação de equipamentos com cabos incorrectos ou a má configuração.

Para evitar a comunicação das impressoras com todas as estações de trabalho poderá ser implementado um servidor de impressão que intermedeie e controle os pedidos de impressão.

Os problemas de segurança associados à AD poderão ser resolvidos através da implementação de mecanismos de controlo de acesso que regulamentem o acesso à rede local do IGC ou através da implementação de um mecanismo de autenticação dos utilizadores separado do ISI.

O facto de os utilizadores serem administradores locais das estações de trabalho não deve acontecer e por isso essa permissão deve ser retirada após estudar a razão da sua existência, se houver alguma, de forma a criar mecanismos seguros que contemplem tal razão.

O facto de o serviço de e-mail prestado pelo ISI ter sido caracterizado como insuficiente e inconstante perante as necessidades do IGC, aponta para a necessidade da implementação ou contratação de um serviço de e-mail que garanta fiabilidade/confiança e um tempo de entrega médio das mensagens reduzido.

Portanto, parece ser justificada a análise cuidada dos problemas e requisitos identificados e a apresentação de cenários de soluções, de forma a permitir que a rede de comunicações do IGC sirva de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio.

Capítulo 4

Desenho da Solução

Neste capítulo é apresentada a infra-estrutura de rede de comunicações para servir de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio do IGC. O desenho da solução proposta foi executado tendo em conta os dados recolhidos nas fases de preparação e planeamento, que permitiram identificar os requisitos de rede e os problemas que impedem a utilização fiável da actual infra-estrutura.

Após descrever detalhadamente a solução desenhada serão apresentados os resultados da sua simulação parcial com o objectivo de validar a sua arquitectura e prever eventuais problemas que possam surgir na fase de implementação, constituindo assim um *Proof of Concept* da solução proposta.

4.1 Desenho: infra-estrutura proposta

Nesta secção é descrita a infra-estrutura proposta expondo os seus detalhes técnicos, focando concretamente os vários sites que a constituem, descrevendo a forma como serão interligados e previstos os custos associados à sua implementação.

4.1.1 Visão Geral

A figura 49 apresenta de forma global a infra-estrutura que será descrita detalhadamente nas secções seguintes.

São identificadas quatro áreas funcionais distintas, coincidentes com as áreas propostas para a operação do protocolo de routing a implementar, o Open Shortest Path First (OSPF). A área 0 inclui as interligações entre os três sites: Porto, Lisboa e DRS. A área 1 inclui o pólo do Porto, estando representadas as diferentes *VLAN*'s propostas para a operação e gestão. A área 2 inclui o site de Lisboa com a rede local e clientes. A área 3 inclui o DRS.

Também estão representadas na figura 49, ligações locais à rede do ISI (na parte inferior da imagem), no Porto e em Lisboa, que poderão ser estabelecidas alternativamente como solução redundante à ligação dos sites Porto e Lisboa.

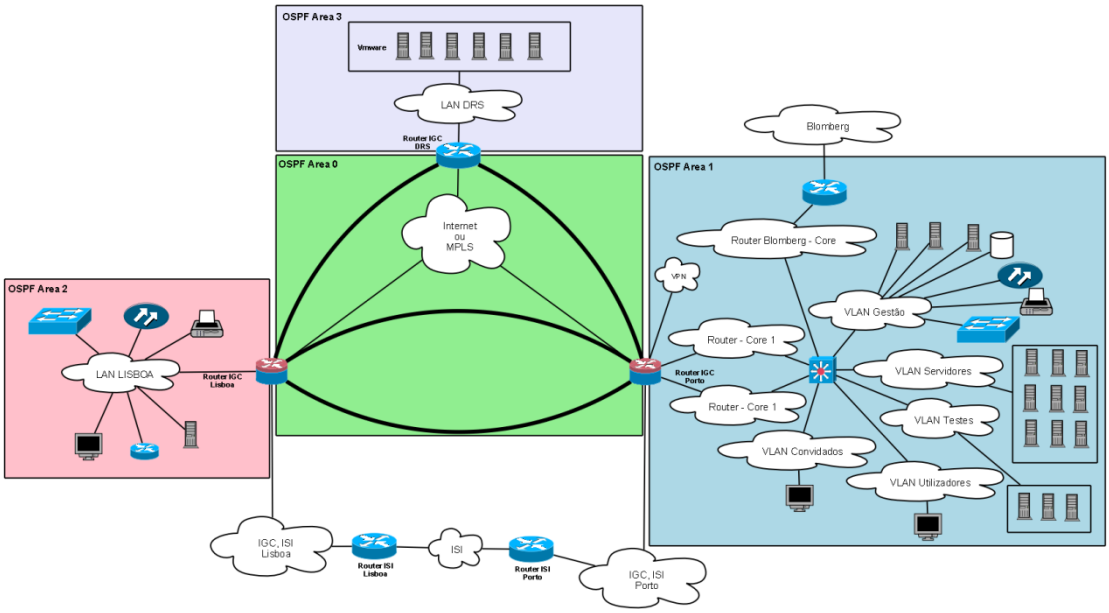


Figura 49 Visão geral da infra-estrutura proposta

4.1.2 Site do Porto

Nesta secção descrever-se-á a estrutura que suportará a infra-estrutura da rede de comunicações no site de Porto que suporta a maioria dos SI do IGC.

4.1.2.1 Nível Físico

A descrição física da infra-estrutura aqui descrita tem já em conta a aquisição de material diverso que o IGC realizou no final do ano de 2008, com vista o melhoramento do pólo técnico do Porto. Assim, a infra-estrutura física que suportará a rede de comunicações no Porto deverá seguir o esquema apresentado na figura 50.

Para garantir fiabilidade e disponibilidade é recomendável que os servidores tenham fontes de alimentação de energia redundantes, por exemplo, usando duas fontes alimentadas por fases distintas. O mesmo princípio é recomendado para os equipamentos activos da rede. Assim, os *switches* e o *router* deverão ser suportados por uma fonte de alimentação externa alternativa Cisco Redundant Power Supply (RPS).

Na ligação à rede, todos os servidores deverão ser ligados de uma forma redundante a 2 *switches* do *Core* da rede, de maneira a que se garanta a continuidade da ligação à rede caso um dos *switches* ou placa de rede do servidor falhe. Por sua vez, cada *switch* de acesso tem também uma ligação redundante aos *switches* do *Core*. O equipamento denominado por "router IGC" terá que ser adquirido e será o responsável pelas comunicações com o exterior.

Para não sobrecarregar o diagrama não foram especificados os servidores que irão suportar os diversos serviços que a rede disponibilizará aos seus utilizadores.

A lista de servidores que irá suportar os serviços já instalados e a instalar é apresentada de seguida:

- **MON** – máquina a adquirir.
- **DC1** – máquina a adquirir.
- **EXCHANGE** – máquina a adquirir.
- **TUX** – máquina a adquirir.
- **PVS** – máquina já adquirida no final de 2008 (Dell 2950).
- **TRADERCQ1** – máquina adquirida no final de 2008. (Dell 2950)
- **TRADERCQ2** – máquina adquirida no final de 2008. (Dell 2950)
- **VM** – máquina adquirida no final de 2008. (Dell 1950)
- **IIS** – máquina adquirida no final de 2008. (Dell 1950)
- **DC2** – actual IGCDC2 (DELL 1850 – SRV/017)
- **BCK** – actual IGC-BCK (DELL 4600 – SRV/003)
- **FS** – actual IGC-FS (DELL 2800 – SRV/019)
- **PROXY** – actual IGC-FW (HP DL320 – SRV/018)
- **SQL** – actual IGC-SQL (DELL 2800 – SRV/021)
- **NODE1** – actual NODE1 (HP DL380)
- **NODE2** – actual NODE2 (HP DL380)

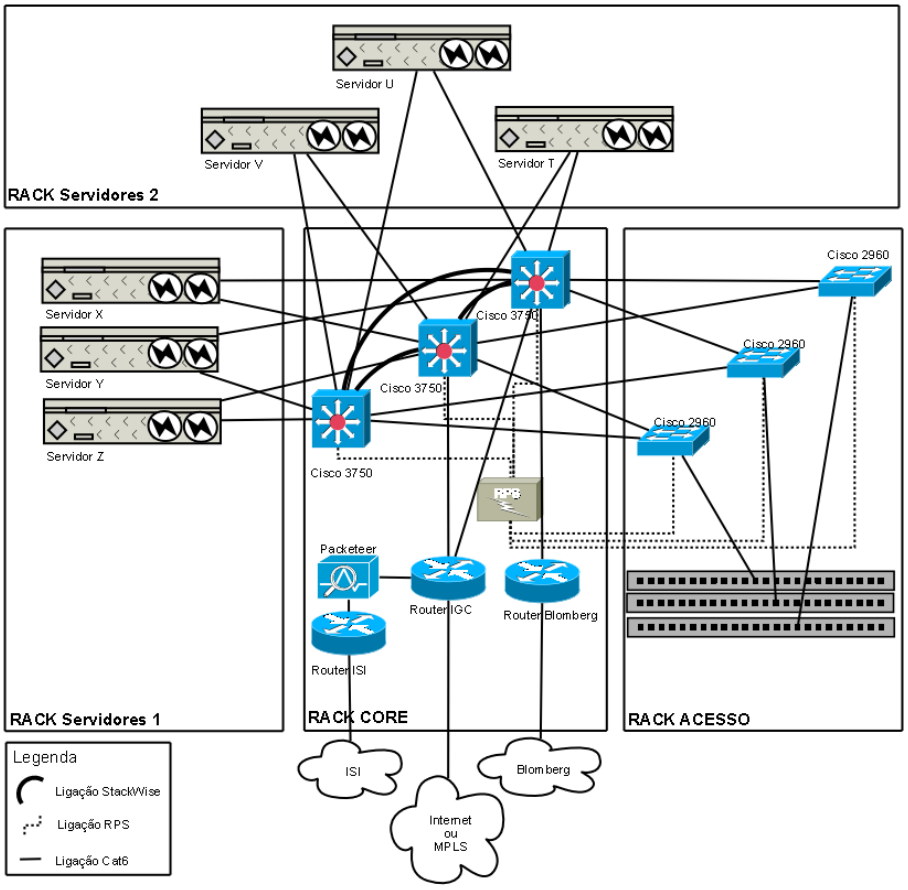


Figura 50 Infra-estrutura física de suporte à rede de comunicações no Porto

A figura 51 representa na planta a disposição dos armários que irão albergar os servidores e os equipamentos activos da rede no pólo técnico do Porto.

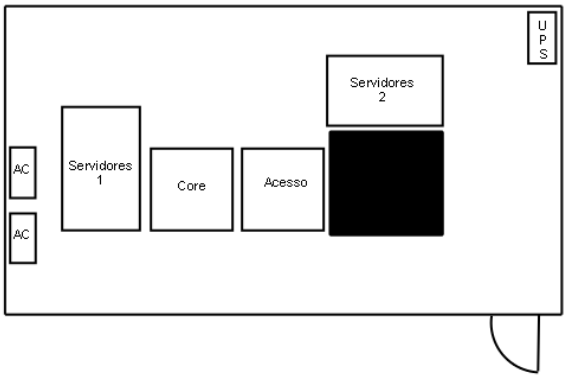


Figura 51 Disposição dos armários no Pólo Técnico do Porto

4.1.2.2 Nível Lógico

Ao nível lógico, serão implementadas *VLAN*'s que permitirão segmentar o tráfego na rede [26] assim como implementar mecanismos de segurança mais elevados, filtrando criteriosamente o tráfego entre as diversas redes [27]. O diagrama da figura 52 mostra como será organizada a rede do Porto em termos lógicos.

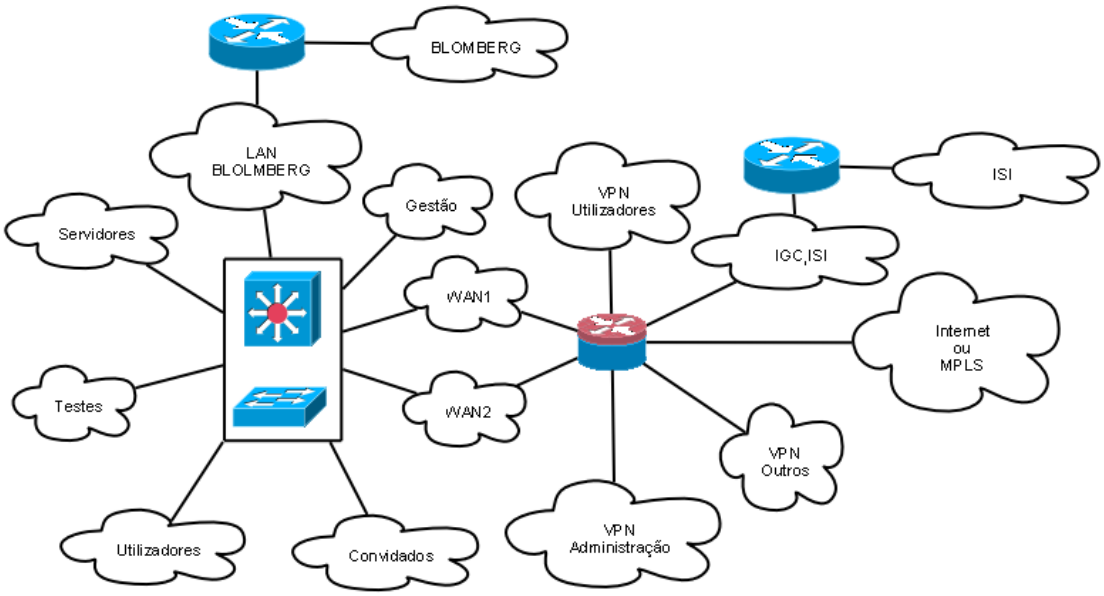


Figura 52 Esquema de nível lógico da rede do Porto

A seguir é feita uma breve descrição de cada *VLAN* e rede de interligação:

- **Gestão** – segmento de rede que suportará os serviços relacionados com a gestão e monitorização da infra-estrutura da rede e onde serão ligados os activos de rede (*routers* e *switches*), impressoras, UPS e terminais de controlo de acesso.
- **Servidores** – segmento de rede que suportará os servidores de produção do IGC.
- **Testes** – segmento de rede que suportará os servidores utilizados para testes e/ou desenvolvimento.
- **Utilizadores** – segmento de rede que suportará os colaboradores do Instituto.
- **Convidados** – segmento de rede que suportará a ligação à Internet de pessoas externas ao IGC, como por exemplo consultores ou auditores.

- **WAN1 e WAN2** – ligações ponto-a-ponto, de nível 3, feitas com o *router* que será responsável por reencaminhar o tráfego para o exterior.
- **LAN BLOMBERG** - ligação ponto-a-ponto, de nível 3, feita com o *router* que será responsável por reencaminhar o tráfego para a Blomberg.
- **VPN Utilizadores** – segmento de rede privado / Virtual Private Network (VPN) que receberá ligações do exterior por parte dos colaboradores o Instituto e que permitirá o acesso remoto a serviços como o e-mail e servidor de ficheiros.
- **VPN Administração** – VPN que receberá ligações do exterior para realizar operações de manutenção à infra-estrutura de rede.
- **VPN Outros** – VPN que receberá ligações do exterior para a realização de operações específicas e/ou temporárias como por exemplo realização de acções de manutenção/intervenção por parte da Codeware ao serviço do TRADER.
- **IGC,ISI** – segmento de rede que corresponde à rede do ISI onde se encontra actualmente ligada a rede do IGC

As *VLAN*'s deverão ser distribuídas para todos os equipamentos de *switching* utilizando o protocolo Vlan Trunking Protocol (VTP) de forma a manter coerente o nome e o número de identificação associado às diversas *VLAN*'s e reduzir o trabalho de administração [28]. A cada *VLAN* está associado uma interface lógica no *switch* de *Core* que corresponderá à default gateway de cada segmento de rede e encaminhará os pacotes para o exterior desse segmento.

Por razões de segurança e também para obrigar a um controlo administrativo da mudança de ligações à rede, a cada porta dos vários *switches* (à excepção daquelas associadas à *VLAN* Convidados) será associado o endereço MAC da estação de trabalho ou servidor que será lá ligado. Desta forma, a cada porta dos *switches* apenas se poderá ligar uma estação de trabalho ou servidor que deverá ser fixa. Alterações nestas ligações implicam a reconfiguração do *switch* o que obriga ao controlo das alterações efectuadas ao nível das ligações à rede. As portas que não têm qualquer dispositivo ligado devem ser desligadas administrativamente para que novas ligações à rede passem obrigatoriamente pelo controlo administrativo da rede.

4.1.2.3 Nível da Rede

Nesta secção apresentar-se-á a descrição da topologia do escritório ao nível da camada IP da rede apresentado o mapeamento dos IP's que serão utilizados assim como serão distribuídas as rotas para o resto da rede através de um protocolo de routing.

Na figura 53 apresenta-se a proposta para o mapa de endereçamento IP a utilizar na nova estrutura.

Como se pode verificar, propõe-se a utilização de endereços IP privados, de acordo com as recomendações da Internet Engineering Task Force (IETF) [29], da gama de IP's 192.168/16 para todo o endereçamento privado da rede do IGC.

A cada segmento de rede referido na secção anterior é atribuída uma rede IP com uma máscara de 24 bits a "1" (/24), ou seja 255.255.255.0, à excepção das ligações VPN e das ligações ponto-a-ponto. Nas ligações ponto-a-ponto será utilizada uma máscara de 30 bits (/30), ou seja 255.255.255.252. Desta forma, nos segmentos de rede com máscara /24 ficarão disponíveis 254 endereços para poderem ser atribuídas às interfaces de rede dos equipamentos e

o endereço 254 será utilizado sistematicamente pela "default gateway" ou seja, será atribuído ao *router* que encaminhará todo tráfego não destinado à rede local em que está inserido.

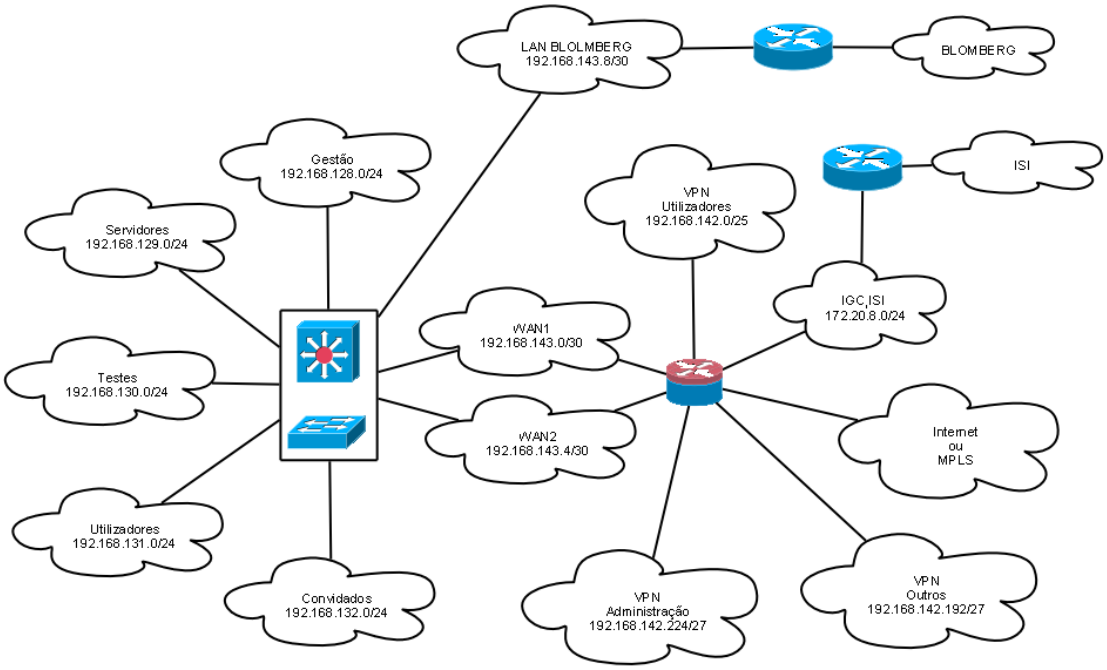


Figura 53 Mapa do endereçamento IP da rede do Porto

O protocolo de routing proposto para gerir dinamicamente o encaminhamento do tráfego entre as diferentes redes dos sites do IGC (Porto, Lisboa e DRS) é o OSPF, normalizado pelo IETF no RFC2328/STD0054 e, como tal, deverá ser suportado por todos os fabricantes de equipamento específico para processamento de routing.

A rede do escritório do Porto constituirá uma área no protocolo OSPF. De forma a não sobrecarregar em termos de processamento o *switch* do *Core* da rede do Porto, este constituirá uma área do tipo "Totally Stubby" o que se traduzirá em apenas lhe ser anunciado rotas do tipo "default", permitindo reduzir assim o tamanho da sua tabela de rotas, o que se traduz numa poupança de memória [30], e não o obrigando a recalcular essa tabela cada vez que há uma alteração de rotas nos restantes sites. Desta forma, é esperado que o *switch* do *Core*, tenha na sua tabela 2 rotas do tipo 0.0.0.0, aprendidas por OSPF e que apontarão para o *router* do IGC no Porto. Além destas rotas este terá as rotas locais associadas às interfaces lógicos de cada *VLAN*. O *router* de acesso ao exterior localizado no Porto desempenhará então o papel de *Area Border Router* fazendo a interligação da área do Porto à área 0 (backbone) que será constituída pelas ligações inter-sites.

De forma a possibilitar expansões futuras, como acréscimo de outras *VLAN*'s ficará disponível para utilização futura a seguinte gama de endereços: do 192.168.133.0 até ao 192.168.141.255. Na gama atribuída aos acessos VPN ficará também disponível para futuras utilizações os endereços do 192.168.142.129 ao 192.168.142.191.

A área OSPF correspondente à área do Porto poderá, face aos endereços utilizados/reservados, ser então resumida através do endereço agregado 192.168.128.0/20.

Em termos de segurança, a comunicação entre as diversas redes e do exterior para a rede do Porto será regulamentada por listas de controlo de acesso /Access Control List (ACL) que apenas permitirão o tráfego desejado e necessário entre os vários segmentos, bloqueando o

restante tráfego. As ACL's permitirão a filtragem do tráfego com base no seu IP de origem e destino assim como a porta TCP/UDP utilizada para efectuar a comunicação [31]. Estas listas deverão ser desenhadas na altura da implementação de acordo com as configurações das aplicações utilizadas de forma a se fazer o levantamento fidedigno dos fluxos de comunicação permitidos. Alterações futuras deverão ser feitas com base numa análise de toda a rede com o objectivo de garantir que não se abrirá oportunidades para tráfego não desejado e que pode ser usado de forma maliciosa.

4.1.2.4 Nível Aplicacional

Nesta secção são descritos os serviços que serão alvo de instalação ou reconfiguração no site do Porto. Assim, os serviços que se encontrem actualmente em funcionamento e que não sejam aqui referidos, serão alvo apenas de adaptação ao novo ambiente mas sem alterações ao nível da sua arquitectura e modo de funcionamento.

4.1.2.4.1 Serviço de protecção da Rede – *Firewall*

A *firewall* que irá proteger a rede do Porto será constituída por 2 elementos fundamentais:

- Componente Context-Based Access Control (CBAC) disponibilizada pelo *router* que inclui as seguintes funcionalidades: filtragem e inspecção de tráfego de forma inteligente baseada nas informações da camada de aplicação e de sessão, o que permite abrir temporariamente portas para o exterior de acordo com as sessões negociadas; alertar e auditar os fluxos de comunicação que passam pelo *router*; implementar um mecanismo de Intrusion Detection System (IDS) para detectar intrusões com base num conjunto de "assinaturas" disponibilizadas (características associadas a fluxos de comunicação que os permitem identificar como possíveis ameaças de segurança) [32].
- Servidor em Linux (TUX) que irá fazer a intermediação de diversos serviços que necessitam o contacto directo com a Internet evitando assim o contacto directo dos servidores internos do IGC com o exterior. Esses serviços serão: resolução de nomes na Internet (DNS externo), sincronização do relógio (protocolo NTP) e envio de e-mails para a Internet (protocolo SMTP).

4.1.2.4.2 Serviço de Autenticação

O serviço de autenticação dos utilizadores do IGC será disponibilizado por um sistema baseado em Microsoft AD instalado e configurado numa plataforma Microsoft Windows 2003 R2. Será criado um domínio denominado "igc.pt" que representará o topo de uma nova floresta controlada pelo IGC. A implementação das políticas de segurança a implementar será baseado na análise das políticas implementadas actualmente, executada na fase de Preparação, e o objectivo será não provocar grandes alterações na forma de utilizar os sistemas informáticos do Instituto aos seus utilizadores.

O sistema de AD será suportado por 2 servidores (DC1 e DC2, ambos DC's) instalados no pólo técnico do Porto garantindo assim, através de redundância de dados e sistemas físicos, uma maior disponibilidade do sistema que regulará o acesso aos meios informáticos do Instituto.

A configuração do serviço AD deverá utilizar a opção de criação de diversos sites associados aos endereços IP de cada site. Assim, o site do Porto ficará então associado à rede 192.168.128.0/20. A utilização desta funcionalidade da AD permite controlar a frequência de actualizações enviadas entre os diversos sites permitindo assim evitar que as actualizações do serviço de autenticação congestionem os circuitos que interligarão os diversos sites [33]. Todos os DC's do IGC deverão ser configurados como Global Catalog de forma a guardarem uma réplica total das informações armazenadas na AD [33] garantindo assim a disponibilidade de todas as funcionalidades do sistema de autenticação caso falhe um DC.

4.1.2.4.3 Serviço de Resolução de Nomes – DNS

Em ambientes baseados no serviço de AD da Microsoft, o serviço DNS desempenha um papel de relevo, sendo este fulcral para o seu correcto funcionamento uma vez que é utilizado para armazenar informações diversas do domínio [33]. Por esta razão, os servidores que desempenharão o papel de DC, desempenharão também o papel de servidores DNS internos, guardando as informações necessárias para o correcto funcionamento da AD assim como os dados que relacionam os nomes das diversas máquinas com o seu endereço IP.

A resolução de nomes a nível externo, isto é, endereços públicos da Internet, ficará a cargo do serviço BIND instalado e configurado no servidor TUX que será responsável pelo contacto com os servidores de nomes dos diversos domínios da Internet. Desta forma, evita-se o contacto directo dos servidores responsáveis pela AD com o exterior, protegendo-os assim de eventuais ataques ou vírus. Assim, todos os pedidos efectuados aos servidores DNS internos, pelos utilizadores do Instituto, para a resolução de nomes na Internet serão reencaminhados por estes para o servidor TUX que tratará de os resolver e informar os servidores internos. Como forma de redundância, o DC2 terá configurado como forwarders secundários os IP's dos servidores DNS do ISP contratado. Com isto, consegue-se que na pior das situações, apenas o DC2 tenha contacto directo com a Internet e limitado aos IP's dos servidores DNS do ISP.

4.1.2.4.4 Serviço de Atribuição Automática de Configurações – DHCP

De forma a facilitar a administração das estações de trabalho, estas deverão ser configuradas para receber as suas configurações de acesso à rede (endereço IP, máscara, default gateway, servidores DNS e sufixo do domínio) através do serviço DHCP.

O serviço DHCP ficará também a cargo dos DC's. Estes deverão ser configurados para atribuir IP's às *VLAN*'s Utilizadores e Convidados cujos pedidos DHCP deverão ser reencaminhados para estes pelo *switch* de *Core*. Um dos servidores DHCP do Porto deverá ser configurado para atribuir IP's às estações de trabalho em Lisboa para garantir que, caso o servidor de Lisboa falhe, as estações de trabalho serão configuradas correctamente para aceder à rede. O *router* de Lisboa será configurado para reencaminhar os pedidos DHCP para esse servidor caso não seja detectada resposta aos pedidos DHCP localmente na rede de Lisboa.

Assim, o serviço DHCP será configurado de forma redundante em 2 servidores (os 2 DC) e devido à falta de mecanismos de sincronização automática das configurações do serviço DHCP, qualquer alteração feita a este nível deverá ser manualmente configurada em ambos os

servidores. Haverá também redundância na configuração do servidor DHCP em Lisboa e no servidor no Porto que atribuirá IP's à rede de Lisboa em caso de falha do servidor local.

Relativamente à *VLAN* Convidados, as definições do Proxy para acesso à Internet devem ser dadas às estações de trabalho através do protocolo Web Proxy Autodiscovery Protocol (WPAD) utilizando o serviço DHCP.

Às estações de trabalho dos colaboradores do IGC deverá ser atribuído, através do serviço DHCP, um endereço IP fixo através da configuração de uma reserva que associará o endereço MAC da interface de rede da estação de trabalho, com o IP pretendido.

4.1.2.4.5 Serviço de Proxy de acesso à Internet

O acesso à Internet por parte dos utilizadores da rede do IGC deverá ser feito por intermédio de um servidor Proxy baseado no *software* Microsoft ISA Server que será instalado e configurado no servidor PROXY.

O serviço de Proxy deverá ser configurado para intermediar o serviço HTTP(S). O acesso ao serviço de Proxy deverá ser autenticado evitando assim a sua utilização não autorizada. Assim, na *VLAN* Utilizadores serão utilizadas as credenciais dos utilizadores para autenticar no domínio "igc.pt" a partir das suas estações de trabalho. No caso da *VLAN* Convidados, o acesso deverá ser apenas permitido a utilizadores que serão criados na AD mas que serão associados a um grupo que apenas permitirá o acesso ao serviço de Proxy, impedindo tudo o resto. Para além do aumento da segurança, o serviço de Proxy autenticado, permitirá a elaboração de estatísticas de acesso associadas ao nome dos utilizadores em vez do endereço IP da estação de trabalho.

4.1.2.4.6 Serviço de E-mail

Para suportar o serviço de e-mail será instalada e configurada uma solução baseada no Microsoft Exchange Server 2007 em conjunto com o Message Transfer Agent (MTA) Postfix que é um pacote de *software* de uso gratuito e cujo bom desempenho e facilidade de configuração é comummente reconhecido [34].

A escolha do Microsoft Exchange Server 2007 para a base do serviço de gestão das caixas de correio dos colaboradores do Instituto, apesar do seu preço de licenciamento e dos requisitos em termos de sistema físico de suporte, baseou-se fundamentalmente nos seguintes pontos:

- Minimizar as alterações ao nível de utilização do serviço de e-mail por parte dos colaboradores, uma vez que o actual servidor de e-mail é baseado no Microsoft Exchange;
- Maximizar a compatibilidade com os restantes serviços informáticos que se baseiam na sua totalidade num ambiente Microsoft;
- Maior facilidade de administração e manutenção por parte dos colaboradores do IGC responsáveis pelos SI;
- Maior facilidade de integração com o sistema centralizado de *backups* que o Instituto dispõe baseado no *software* CA Arcserve para o qual já foi inclusive adquirida licença para o agente de *backups* do Exchange Server 2007;
- Disponibilização de acesso via WEB, através de um browser, a um ambiente muito idêntico ao utilizado no cliente Outlook, com acesso a todas as informações (mensagens

recebidas e enviadas, calendário, tarefas, etc.) permitindo assim um acesso remoto ao serviço de e-mail;

- Pela funcionalidade Standby Continuous Replication (SCR) disponibilizada a partir da versão 2007 SP1 que permitirá a manutenção de um sistema de e-mail a utilizar em caso de desastre do principal e disponibilizará as mesmas funcionalidades do sistema primário [35].

O servidor Postfix estará incluído na configuração da *firewall* do IGC, será configurado como servidor SMTP e terá as seguintes responsabilidades:

- Receber do serviço de E-Mail *Relay* - que deverá ser contratado a um ISP - as mensagens e reencaminhá-las para o Microsoft Exchange Server que tratará de as colocar nas caixas de correio dos utilizadores.
- Enviar as mensagens para o exterior, sendo este responsável por contactar directamente com os servidores de correio dos restantes domínios utilizados.

A contratação do serviço de E-Mail *Relay* a um ISP baseia-se fundamentalmente em duas razões:

- Assegurar a actualização de listas de SPAM que ficará então a cargo do ISP. Para um serviço que suportará em média 30 utilizadores, não se justifica o investimento de tempo por parte de alguém especializado neste assunto de forma a garantir a diminuição da percentagem de SPAM entregue aos utilizadores finais.
- Aumentar o nível de segurança uma vez que os domínios externos não contactarão directamente com a ligação à Internet do IGC mas sim com o ISP que deverá estar munido de mecanismos de protecção que garantam a segurança das ligações com o exterior.

Pretende-se com este modelo funcional distribuir o trabalho de processamento do serviço de e-mail da organização e reforçar a sua segurança. O servidor Exchange será responsável por fornecer o serviço de e-mail aos utilizadores do Instituto e para processar todo o tráfego de mensagens com o exterior comunicará unicamente com o servidor Postfix. Com este constrangimento de segurança evita-se o acesso directo do exterior ao sistema que guardará as mensagens dos utilizadores.

O Postfix fará o diálogo directo com os servidores externos na Internet para o envio das mensagens do Instituto e comunicará com o servidor de E-Mail *Relay* do ISP para a recepção de todo o tráfego de e-mail do exterior (após a filtragem do SPAM).

O esquema da figura 54 ilustra a arquitectura de funcionamento do serviço de e-mail proposto.

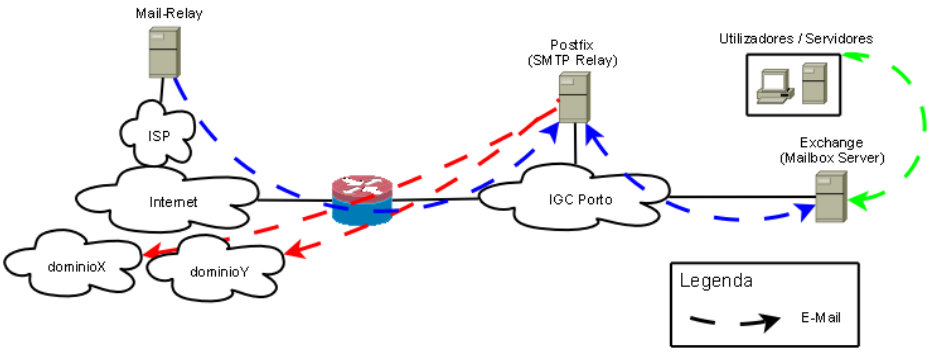


Figura 54 Arquitectura do funcionamento do serviço de e-mail

4.1.2.4.7 Serviço de Impressão

O serviço de impressão ficará a cargo de um servidor Windows 2003 R2 (PVS) onde serão instalados os drivers de impressão de todas as impressoras. Para as estações de trabalho dos colaboradores do Instituto imprimirem documentos ligar-se-ão ao servidor de impressão que será responsável pelo envio do trabalho para a impressora. Este sistema permite limitar assim com quem comunicam as impressoras evitando que estas tenham dificuldade em gerir a solicitação de vários pedidos em simultâneo. Por outro lado poder-se-ão implementar mecanismos centralizados de controlo de acesso e de gestão das impressões.

A figura 55 ilustra o funcionamento e arquitectura do serviço de Impressão.

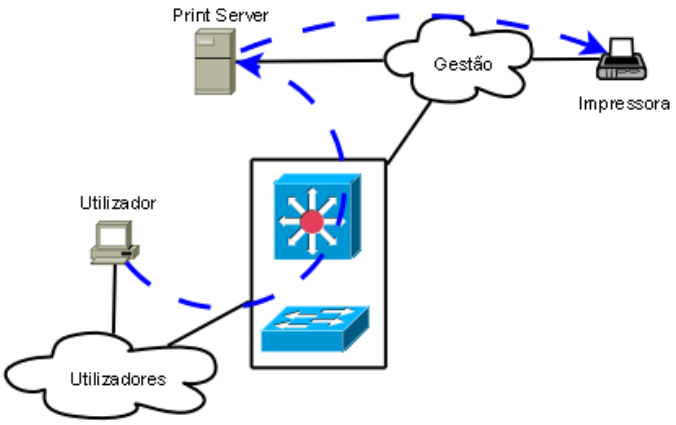


Figura 55 Arquitectura do funcionamento do serviço de Impressão

4.1.2.4.8 Serviço de Sincronização de Relógio (NTP)

De forma a manter actualizada e sincronizada a hora do relógio de tempo real nos servidores e clientes da rede do IGC no servidor TUX será instalado o serviço de NTP.

Todas as estações de trabalho, servidores e equipamentos de rede deverão ser configurados para utilizar este servidor, garantindo assim o seu relógio actualizado e sincronizado.

4.1.2.4.9 Serviço de actualizações Microsoft (WSUS)

No servidor PVS, será configurado o serviço Windows Software Update Services (WSUS) que será responsável por fornecer às estações de trabalho as actualizações dos sistemas operativos da Microsoft.

4.1.2.4.10 Serviço de monitorização da rede

De forma a monitorizar a infra-estrutura de rede assim como gerir os seus componentes dedicar-se-á um servidor com Windows 2003 R2 onde será instalado o *software* SolarWinds que será reconfigurado para monitorizar a nova infra-estrutura. Neste servidor será também instalado todo o tipo de *software* utilizado para gerir os activos de rede, nomeadamente o Cisco Network Assistance (CNA) e o Cisco Router and Security Device Manager (SDM).

Apenas este servidor terá acesso à consola de gestão dos equipamentos activos da rede (*routers* e *switches*), preferencialmente através de Secure Shell (SSH) quando suportado ou então por telnet.

Os equipamentos de rede deverão ser configurados para enviar para este servidor as traps SNMP assim como os seus registos de eventos via SYSLOG.

Neste servidor será também instalado o *software* de controlo de acessos responsável por receber dos terminais de controlo de acesso os registos de entradas e saídas e também onde se registam novos utilizadores.

Desta forma numa única máquina será possível obter uma visão geral do estado da infra-estrutura de rede assim como de um único sítio realizar operações de manutenção.

4.1.2.4.11 Mapeamento Aplicações Servidores

De seguida apresenta-se o resumo da correspondência de servidores e funções que desempenharão:

- **MON** – SolarWinds + ferramentas de gestão da rede + Controlo de Acessos
- **PVS** – Servidor de impressão + Antivírus + WSUS
- **DC1** – DC + Servidor DNS Interno + Servidor DHCP
- **DC2** – DC + Servidor DNS Interno + Servidor DHCP
- **BCK** – Servidor de *backups*
- **FS** – Servidor de Ficheiros
- **PROXY** – Servidor Proxy HTTP(S) e FTP
- **EXCHANGE** – Servidor de Caixas de Correio + Outlook Web Access
- **TUX** – SMTP + NTP + DNS Externo
- **IIS** – Servidor HTTP para a Intranet
- **SQL** – Servidor SQL
- **NODE1** – TRADER Nó 1
- **NODE2** – TRADER Nó 2
- **TRADERCQ1** – TRADER Testes 1
- **TRADERCQ2** – TRADER Testes 2

4.1.3 Site de Lisboa

O site de Lisboa do IGC é caracterizado como uma pequena filial onde se encontram normalmente poucos utilizadores. Descrever-se-á nesta secção a infra-estrutura que suportará então a filial de Lisboa.

4.1.3.1 Nível Físico

Relativamente ao nível físico, é recomendável que no escritório de Lisboa seja criado um espaço dedicado para as infra-estruturas das TI e onde seja garantida a refrigeração do ar através de um equipamento de ar condicionado, apesar da reduzida dimensão dos recursos.

Caso a solução de DR seja suportada pelo escritório de Lisboa é então essencial e urgente, que sejam criadas as condições físicas mínimas que permitam garantir a continuidade do funcionamento de todos os sistemas que serão lá colocados. Nesta secção será considerado que o site de Lisboa suportará apenas os utilizadores do Instituto e não o DRS.

O esquema apresentado na figura 56 mostra os equipamentos previstos para o site de Lisboa. Como se pode visualizar através do esquema apresentado, o escritório de Lisboa será suportado localmente apenas por um servidor que desempenhará diversas funções descritas na Análise Aplicacional.

Relativamente à figura, o único equipamento do esquema que não foi ainda adquirido é o "router IGC" que será responsável pelas comunicações com o exterior.

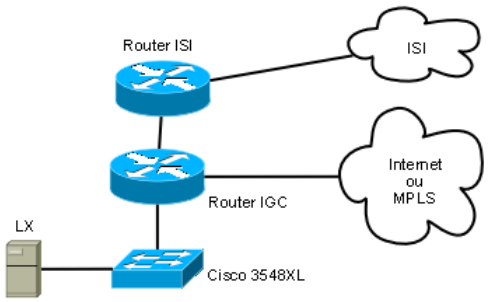


Figura 56 Esquema físico do Site de Lisboa

4.1.3.2 Nível Lógico

Em termos lógicos, a rede do site de Lisboa será constituída por apenas uma rede que será ligada ao *switch* Cisco 3548XL. Assim, todos os equipamentos estarão do ponto de vista operacional como estando ligados a um único segmento de rede e portanto, com um único domínio de difusão ao nível da ligação lógica. Esta configuração justifica-se uma vez que, face à reduzida dimensão da rede, não é necessária a segmentação com *VLAN*'s.

Por razões de segurança e também para obrigar a um controlo administrativo da mudança de ligações à rede, a cada porta do *switch* será associado o endereço MAC da estação de trabalho ou servidor que será lá ligado. Desta forma, a cada porta apenas se poderá ligar uma estação de trabalho ou servidor que deverá ser fixa. Alterações nestas ligações implicam a reconfiguração do *switch* o que obriga ao controlo das alterações efectuadas ao nível das ligações à rede. As portas que não têm qualquer dispositivo ligado devem ser desligadas administrativamente para que novas ligações à rede passem obrigatoriamente pelo controlo administrativo da rede.

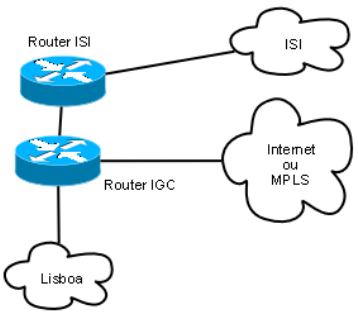


Figura 57 Esquema de nível lógico da rede de Lisboa

4.1.3.3 Nível da Rede

Ao nível da camada IP da rede o escritório de Lisboa será suportado por uma única rede IP com uma máscara de 24 bits a "1" (/24), ou seja 255.255.255.0. Ao escritório de Lisboa será então atribuída a rede 192.168.144.0/24 o que significa que ficarão disponíveis 254 endereços para poderem ser atribuídas às interfaces de rede dos equipamentos e o endereço 254 será utilizado pela "default gateway" ou seja, será atribuído ao *router* que encaminhará todo tráfego não destinado à rede local em que está inserido.

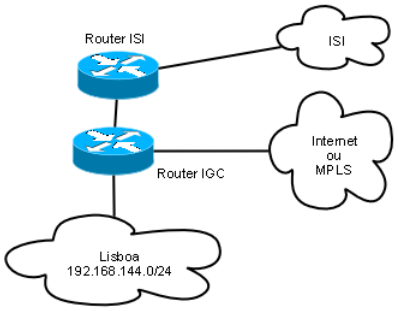


Figura 58 Mapa de endereçamento IP da rede de Lisboa

A rede do escritório de Lisboa constituirá também uma área no protocolo de routing OSPF. O *router* de acesso ao exterior desempenhará então o papel de *Area Border Router* fazendo a interligação da área de Lisboa à área 0 (backbone) que será constituída pelas ligações inter-sites.

De forma a possibilitar expansões futuras, como acréscimo de *VLAN*'s ficará disponível para utilização posterior o bloco de endereços: do 192.168.145.0 ao 192.168.151.255.

A área OSPF correspondente à área de Lisboa será inicialmente representada através do endereço 192.168.144.0/24.

Em termos de segurança, a comunicação do/para exterior para/da rede de Lisboa será regulamentada por listas de controlo de acesso (ACL's) que apenas permitirão o tráfego desejado e necessário.

4.1.3.4 Nível Aplicacional

Nesta secção são descritos os serviços que serão alvo de instalação localmente em Lisboa. Os restantes serviços a utilizar em Lisboa serão suportados no Pólo Técnico do Porto.

4.1.3.4.1 Serviço de Autenticação

A autenticação dos utilizadores do IGC no escritório de Lisboa ficará a cargo de um sistema baseado em AD instalado e configurado sobre Microsoft Windows 2003 R2 no servidor LX. Este servidor assumirá o papel de DC do domínio "igc.pt" e será associado ao site de Lisboa que é constituído pela rede 192.168.144.0/24. A sincronização entre os vários DC será feita de forma automática sendo que a sua periodicidade dependerá da capacidade circuito que interligará os 2 escritórios.

A colocação de um DC em Lisboa justifica-se de forma a garantir que os utilizadores poderão identificar-se na rede caso a ligação Porto-Lisboa falhe e também de forma a aumentar a velocidade deste procedimento.

4.1.3.4.2 Serviço de Resolução de Nomes – DNS

O servidor LX, DC para o site de Lisboa, desempenhará também o papel de servidor DNS interno e externo, guardando as informações necessárias para o correcto funcionamento da AD assim como os dados que relacionam os nomes das diversas máquinas com o seu endereço IP de toda a rede do IGC e contactando também os servidores DNS dos domínios na Internet. Desta forma evitar-se-á o tráfego dos pedidos DNS na ligação Porto-Lisboa.

4.1.3.4.3 Serviço de Ficheiros

O servidor LX deverá ser configurado como servidor de ficheiros de forma a possibilitar que os ficheiros das contas pessoais dos colaboradores de Lisboa sejam guardadas localmente aumentando assim a rapidez de acesso aos ficheiros e no procedimento de autenticação no sistema em caso de Roaming Profiles e evitando um congestionamento no circuito Lisboa-Porto. Assim, os utilizadores de Lisboa apenas utilizarão o servidor de ficheiros no Porto para aceder aos ficheiros comuns. No entanto, diariamente deverá ser feita uma cópia dos ficheiros das contas pessoais dos utilizadores no servidor de ficheiros no Porto, para que, caso o servidor LX falhe, seja garantida a continuidade da utilização do sistema por parte dos colaboradores de Lisboa.

4.1.3.4.4 Serviço de Atribuição Automática de Configurações – DHCP

De forma a facilitar a administração das estações de trabalho, estas deverão ser configuradas para receber as suas configurações de acesso à rede (endereço IP, máscara, default gateway, servidores DNS e sufixo do domínio) através do serviço DHCP.

O serviço DHCP ficará também a cargo do servidor LX. No entanto, o *router* de Lisboa será configurado para reencaminhar os pedidos DHCP para o servidor DHCP do Porto caso não seja detectada resposta aos pedidos DHCP localmente garantindo assim que as estações receberão as configurações de acesso à rede caso o servidor LX falhe.

4.1.3.4.5 Serviço de Proxy de acesso à Internet

O acesso à Internet por parte dos utilizadores da rede do IGC no Porto deverá ser feito por intermédio de um servidor Proxy baseado no *software* Microsoft ISA Server que será instalado e configurado também no servidor LX.

O serviço de Proxy deverá ser configurado para intermediar o serviço HTTP(S). O acesso ao serviço de Proxy deverá ser autenticado evitando assim a sua utilização não autorizada.

4.1.4 Site de DR

Nesta secção serão descritos os meios utilizados para suportar os serviços críticos do IGC em caso de desastre no Pólo Técnico do Porto.

4.1.4.1 Requisitos

De acordo com os critérios estabelecidos pelo IGC, com base num projecto de Gestão de Risco que se encontra a decorrer, os sistemas críticos do Instituto e para os quais é necessário garantir a continuidade do funcionamento em caso de desastre, são:

- Serviço de autenticação
- TRADER
- E-Mail
- Servidor de Ficheiros
- Intranet

Para todos os sistemas e serviços identificados, o IGC definiu como indispensável em caso de desastre a reposição dos dados referentes ao dia anterior e uma paragem máxima dos serviços de 24 horas.

4.1.4.2 Solução

A seguir é descrita a solução proposta de acordo com os requisitos identificados na secção anterior, tendo em conta a dimensão e quantidade dos serviços a suportar e o número de utilizadores que a rede do IGC suporta.

Manter-se-á um DRS que poderá corresponder à contratação do serviço de *Housing* num datacenter de um ISP (aluguer de espaço num bastidor, condições ambientais controladas, segurança dos acessos, garantia de fornecimento de alimentação de energia e acesso à Internet) ou ao alojamento no escritório de Lisboa, se este for alvo de remodelações de forma a dotá-lo de melhores condições para garantir a continuidade do funcionamento dos serviços.

O DRS incluirá uma única máquina com características de hardware determinadas para suportar uma plataforma de virtualização. Para esta plataforma é recomendada a utilização de Vmware devido ao seu baixo custo, à garantia de compatibilidade com vários sistemas operativos e bom desempenho [36].

4.1.4.3 Cenários Avaliados

A manutenção de um DRS sincronizado com o site do Porto cria 4 cenários que devem ser avaliados:

- **Cenário 1H** – alojamento do servidor de DR num datacenter contratando o aluguer mensal desse serviço e transferir para lá, através de um circuito digital, as informações de sincronização dos diversos sistemas. Este cenário segue uma arquitectura *Hot Standby*;
- **Cenário 1L** – colocar no escritório de Lisboa o servidor DR e transferir para lá, através de um circuito digital, as informações de sincronização dos diversos sistemas. Este cenário segue uma arquitectura *Hot Standby*;
- **Cenário 2H** – alojamento do servidor de DR num datacenter contratando o aluguer mensal desse serviço e transferir para lá, através do transporte de tapes de *backups* (Tape Shipping), as informações de sincronização dos diversos sistemas. Este cenário segue uma arquitectura *Cold Standby*;

- **Cenário 2L** – colocar no escritório de Lisboa o servidor DR e transferir para lá, através do transporte de tapes de *backups* (Tape Shipping), as informações de sincronização dos diversos sistemas. Este cenário segue uma arquitectura *Cold Standby*.

De seguida descreve-se sumariamente as características/particularidades de cada cenário:

- ***Housing*** – pelo facto de o servidor, neste cenário, residir dentro da rede de um ISP, é mais fácil e barato obter velocidades de acesso ao exterior mais elevadas, o que permite a realização de testes ao DRP sem necessidade de deslocação física dos colaboradores do Instituto e em caso de desastre permite que os utilizadores trabalhem de forma remota; este serviço tem no entanto custos associados e obriga à aquisição de um *router* para o DRS.
- **Lisboa** – este cenário obriga ao aumento da largura de banda disponível no escritório de Lisboa o que se traduz num aumento dos custos associados. O facto da largura de banda equivalente à disponível num serviço de *Housing* ter custos bastante elevados, leva a considerar e por isso analisar, duas situações distintas:
    - **Situação 1** – A largura de banda a contratar para Lisboa será mais reduzida do que aquela contratada num cenário de *Housing* não permitindo assim a realização de testes ao DRP remotamente e em caso de desastre obrigar a deslocação dos colaboradores para Lisboa;
    - **Situação 2** – A largura de banda a contratar para Lisboa será equivalente à disponível num cenário de *Housing* permitindo assim executar testes ao DRP remotamente e em caso de desastre trabalhar também remotamente.

  As duas situações apresentam as seguintes características em comum: evitam a compra de mais um *router* e obrigam a que as condições do escritório de Lisboa sejam remodeladas para garantir a refrigeração dos equipamentos de forma eficaz e investir num sistema que garanta a continuidade do funcionamento das infra-estruturas em caso de falha energética. Em termos lógicos, o escritório de Lisboa sofrerá as seguintes alterações, relativamente à figura 56.

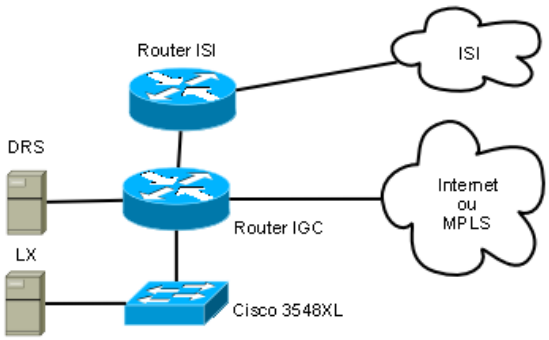


Figura 59 Alterações se Lisboa suportar as infra-estruturas de DR

- **Sincronização por Circuito Digital** – o envio das informações de sincronização, entre o site do Porto e o DRS, através de um circuito digital obriga à contratação de circuitos com maior capacidade (esta diferença será quantificada na secção da análise de fluxos) o que se traduzirá em custos mais elevados (esta diferença será quantificada na secção da previsão de custos). No entanto, este cenário permite a sincronização mais frequente entre os 2 sites, garantindo que em caso de desastre, a informação existente no DRS seja mais recente ou seja, menor RPO.

- **Sincronização por Tape Shiping** – a utilização de tapes para sincronizar os dados dos 2 sites (Porto e DR) permite a contratação de circuitos de interligação com menor capacidade (esta diferença será quantificada na secção da análise de fluxos) o que se traduzirá em custos mais reduzidos (esta diferença será quantificada na secção da previsão de custos). No entanto, é necessário referir que o serviço de Tape Shipping tem custos associados quer para o transporte quer para o armazenamento das Tapes. Este cenário reduz no entanto a periodicidade da sincronização entre os 2 sites aumentando assim o RPO.

Apesar de, à partida, a solução de *Housing* em junção com a opção de sincronização através de circuito digital ser mais favorável, a análise de custos feita mais à frente permitirá comparar em termos de custos as duas soluções escolhendo assim a melhor solução de forma mais fundamentada.

4.1.4.4 Máquinas Virtuais de Desastre

As máquinas virtuais previstas, que suportarão os serviços críticos em caso de desastre são as seguintes:

- **DCD (Domain Controller Disaster)** – suportará o serviço de autenticação e gestão dos utilizadores;
- **FSD (File Server Disaster)** – suportará o serviço de partilha de ficheiros;
- **EXCHANGED (Exchange Disaster)** – suportará as caixas de correio dos utilizadores;
- **SMTPD (SMTP Disaster)** – assegurará a recepção dos e-mails por parte do serviço de e-mail *relay* contratado e enviará os e-mails para o exterior;
- **TRADERD (TRADER Disaster)** – suportará a aplicação responsável pela gestão da carteira dos fundos geridos pelo IGC, o TRADER;
- **SQLD (SQL Disaster)** – garantirá o acesso aos dados das diversas bases de dados, nomeadamente da INTRANET.
- **IISD (IIS Disaster)** – suportará o acesso à INTRANET.

Para o cenário 1, correspondente a uma arquitectura em *Hot Standby* a sincronização será feita da seguinte forma nas várias máquinas virtuais:

- **DCD** – servidor que corresponderá a um DC do domínio "igc.pt" que será sincronizado com os DC primários e manterá por isso as informações sobre os utilizadores do Instituto (credenciais de acesso, organização por grupos, políticas do domínio, entre outras) e informações sobre o serviço de resolução de nomes, DNS, que tem um papel fundamental no funcionamento da AD [33]. A sincronização deste servidor com os servidores primários será feita de forma automática utilizando os mecanismos de replicação de DC entre sites.
- **FSD –** servidor que corresponderá a um servidor de ficheiros que manterá uma réplica de todos os ficheiros partilhados no Servidor de Ficheiros primário. A sincronização dos ficheiros entre este servidor e o servidor de ficheiros do pólo técnico do Porto utilizará a tecnologia de Distributed File System (DFS) Replication disponível a partir da versão R2 do Windows 2003 [37].
- **EXCHANGED** – servidor que corresponderá a um servidor Microsoft Exchange que funcionará sobre o mecanismo de SCR, disponível a partir da versão SP1 do Microsoft

Exchange 2007, e para onde serão enviados os ficheiros de LOG do sistema de Exchange primário de forma a manter uma réplica sincronizada do serviço de E-mail [35].

- **SMTPD** – este servidor não necessita de nenhuma sincronização automática. Será configurado na altura da sua instalação e a partir daí é importante garantir que alterações feitas ao nível da configuração do serviço de SMTP primário sejam replicadas manualmente igualmente neste servidor.
- **TRADERD** – servidor que corresponderá a um servidor ORACLE que funcionará sobre o mecanismo de Data Guard e para onde serão enviados os ficheiros de LOG do sistema de TRADER primário de forma a manter uma réplica sincronizada do serviço de TRADER [38]. Para a configuração deste serviço será essencial a colaboração da CODEWARE. Assim será disponibilizada à Codeware uma máquina virtual com o sistema operativo Windows 2003 R2 instalado e onde deverá ser instalado e configurado o Oracle para receber os logs do TRADER de produção. Entre esta máquina e o TRADER de produção será disponibilizada largura de banda dimensionada de acordo com os dados dos tamanhos dos LOGS fornecidos pela CODEWARE.
- **SQLD (SQL Disaster)** – servidor que corresponderá a um servidor SQL para onde serão transferidos e aplicados os ficheiros de *backup* executados pelo *software* centralizado de *backup* (ARCServe). A actual versão de SQL instalada no servidor IGC-SQL, versão 2000 standard, não suporta qualquer mecanismo de log shipping automatizado [39] pelo que, até à actualização da versão do servidor SQL para uma mais recente, que é recomendado, a sincronização da máquina SQLD e do servidor SQL instalado no site do Porto será feita através da cópia do ficheiro de *backup* executado diariamente.
- **IISD (IIS Disaster)** – servidor que corresponderá a um servidor IIS para onde serão transferidos os ficheiros de *backup* executados pelo *software* centralizado de *backup* (ARCKServe). O IIS não suporta qualquer mecanismo de sincronização automatizado pelo que a sincronização da máquina IISD e do servidor IIS instalado no site do Porto será feita através da cópia e aplicação do ficheiro de *backup* executado diariamente.

Para o cenário 2, correspondente a uma arquitectura em *Cold Standby*, as máquinas virtuais serão pré-instaladas de forma a, em caso de desastre, estarem prontas a receber o conteúdo das tapes enviadas e armazenadas.

4.1.5 Interligação dos Sites e ligação à Internet

Nesta ligação são previstos os circuitos necessários para interligar os vários sites assim como fornecer-lhes o acesso à Internet.

4.1.5.1 Análise de fluxos

Antes de descrever e avaliar os diversos cenários de ligação dos diversos Sites, é necessário analisar os fluxos de comunicação entre eles de forma a dimensionar a largura de banda mínima dos circuitos que os irão ligar.

Para a análise dos fluxos foram considerados os seguintes cenários:

- **Cenário 1** – Sincronização da informação entre o site do Porto e o DRS é feita através de um circuito de dados;
- **Cenário 2** – Sincronização da informação entre o site do Porto e o DRS é feita através de tape shipping.

O site do Porto desempenha no IGC o papel central no que respeita à infra-estrutura de comunicações. Desta forma, para justificar o dimensionamento dos circuitos de acesso que interligarão o site do Porto aos restantes sites, foi realizada uma análise dos fluxos ascendentes, pelo facto de débitos elevados de *Upstream* terem normalmente custos mais elevados, no site do Porto, que é então apresentada e descrita de seguida.

Cenário 1 – Fluxos Horas de Trabalho

FLUXO1

- **Descrição:** Tráfego para Lisboa
- **Dimensionamento:** 1024 kbit/s
- **Comentário:** O dimensionamento deste fluxo baseia-se na qualidade de serviço a prestar ao escritório de Lisboa, escolhida pelo IGC. Essa escolha baseou-se no tamanho médio dos ficheiros no directório Comum do servidor de Ficheiros, 2 MB, que considerou ser o que iria provocar mais tráfego e ser utilizado mais frequentemente. Assim, foi escolhido que um utilizador de Lisboa demoraria cerca de 18 segundos para descarregar um ficheiro de 2 MB.

FLUXO2

- **Descrição:** SMTP
- **Dimensionamento:** 512 kbit/s
- **Comentário:** Como referência, um e-mail de 500 KB demorará cerca de 9 segundos a ser entregue ao destinatário.

FLUXO3

- **Descrição:** Acesso por VPN
- **Dimensionamento:** 256 kbit/s
- **Comentário:** Como referência, descarregar um ficheiro de 2 MB, demorará cerca de 1 minuto e 15 segundos.

FLUXO4

- **Descrição:** Sincronização do TRADER.
- **Dimensionamento:** 256 kbit/s
- **Comentário:** Através da informação fornecida pela Codeware considerou-se uma média diária de informação gerada pelo TRADER igual a 700 MB repartida em LOGS de 51 MB. Para transferir 700 MB a uma velocidade de 256 kbit/s são necessárias cerca de 7 horas, o que equivale sensivelmente a um dia de trabalho. O envio será feito mal seja gerado um novo LOG o que significa que, em média, um LOG gerado estará no DRS passado 30 minutos.

FLUXO5

- **Descrição:** Sincronização do EXCHANGE
- **Dimensionamento:** 512 kbit/s
- **Comentário:** Estima-se que para a utilização do serviço de e-mail para a quantidade de utilizadores do IGC 512 kbit/s serão suficientes para enviar os LOGS gerados pelo EXCHANGE, que não podem ser quantificados com exactidão devido a não ser possível analisar os LOGS do actual serviço de e-mail.

FLUXO6

- **Descrição:** Utilizadores
- **Dimensionamento:** 256 kbit/s
- **Comentário:** Estima-se que seja suficiente para a quantidade de utilizadores do IGC, um fluxo de 256 kbit/s (*Upstream*) que será utilizado, por exemplo, para efectuar pedidos de páginas na Internet, enviar ficheiros através da Internet, entre outros.

FLUXO7

- **Descrição:** *Backup* do IIS
- **Dimensionamento:** 384 kbit/s
- **Comentário:** Para a sincronização do IIS serão enviados para o DRS os ficheiros gerados pelo servidor de *Backups*. O *backup* diário feito actualmente ao IIS ocupa cerca de 1200 MB que serão portanto enviados em cerca de 8 horas. Será enviado durante o dia o *backup* feito na noite anterior que corresponde aos dados do dia anterior.

Cenário 1 – Fluxos fora das Horas de Trabalho

FLUXO1

- **Descrição:** Acesso por VPN
- **Dimensionamento:** 128 kbit/s
- **Comentário:** Como referência, descarregar um ficheiro de 2 MB, demorará cerca de 2 minuto e 30 segundos.

FLUXO2

- **Descrição:** Sincronização File Share
- **Dimensionamento:** 2816 kbit/s
- **Comentário:** O dimensionamento deste fluxo baseia-se análise que foi feita no sentido de verificar a quantidade de informação que é, em média, alterada diariamente nas pastas partilhadas do servidor de ficheiro. Com base na estatística elaborada considerou-se que em média eram alterados cerca de 8200 MB que serão portanto enviados em cerca de 8 horas (sensivelmente o tempo da janela de *backup* disponível – das 0:00 às 8:00).

FLUXO3

- **Descrição:** *Backup* do SQL
- **Dimensionamento:** 1024 kbit/s
- **Comentário:** Para a sincronização do IIS serão enviados para o DRS os ficheiros gerados pelo servidor de *Backups*. O *backup* diário, feito actualmente ao SQL, ocupa cerca de 3000 MB que serão portanto enviados em cerca de 8 horas.

FLUXO4

- **Descrição:** SMTP
- **Dimensionamento:** 128 kbit/s
- **Comentário:** Como referência, um e-mail de 500 KB demorará cerca de 40 segundos a ser entregue ao destinatário.

Tabela 4 Resumo dos fluxos do Cenário 1

Horas de Trabalho		**Fora das Horas de Trabalho**	
Fluxo	**Dimensionamento**	**Fluxo**	**Dimensionamento**
Tráfego para Lisboa	1024 kbit/s	Acesso por VPN	128 kbit/s
SMTP	512 kbit/s	Sincronização File Share	2816 kbit/s
Acesso por VPN	256 kbit/s	*Backup* do SQL	1024 kbit/s
Sincronização TRADER	256 kbit/s	SMTP	128 kbit/s
Sincronização EXCHANGE	512 kbit/s		
Utilizadores	256 kbit/s		
Backup do IIS	384 kbit/s		
TOTAL	**3200 kbit/s**	**TOTAL**	**4096 kbit/s**

Cenário 2 – Fluxos Horas de Trabalho

FLUXO1

- **Descrição:** Tráfego para Lisboa
- **Dimensionamento:** 1024 kbit/s
- **Comentário:** igual ao Cenário 1

FLUXO2

- **Descrição:** SMTP
- **Dimensionamento:** 512 kbit/s
- **Comentário:** igual ao Cenário 1

FLUXO3

- **Descrição:** Acesso por VPN
- **Dimensionamento:** 256 kbit/s
- **Comentário:** igual ao Cenário 1

FLUXO4

- **Descrição:** Utilizadores
- **Dimensionamento:** 256 kbit/s
- **Comentário:** igual ao Cenário 1

Cenário 2 – Fluxos fora das Horas de Trabalho

FLUXO1

- **Descrição:** Acesso por VPN
- **Dimensionamento:** 128 kbit/s
- **Comentário:** igual ao Cenário 1

FLUXO2

- **Descrição:** SMTP
- **Dimensionamento:** 128 kbit/s
- **Comentário:** igual ao Cenário 1

Tabela 5 Resumo dos fluxos do Cenário 2

Horas de Trabalho		**Fora das Horas de Trabalho**	
Fluxo	**Dimensionamento**	**Fluxo**	**Dimensionamento**
Tráfego para Lisboa	1024 kbit/s	Acesso por VPN	128 kbit/s
SMTP	512 kbit/s	SMTP	128 kbit/s
Acesso por VPN	256 kbit/s		
Utilizadores	256 kbit/s		
TOTAL	**2048 kbit/s**	**TOTAL**	**256 kbit/s**

A análise de fluxos mostra que em termos de dimensão do circuito a contratar para o site do Porto é necessário para o cenário 1 um circuito de 4096 kbit/s, que será usado na grande maioria do tempo devido aos fluxos de sincronização fora das horas de trabalho, e para o cenário 2 são necessários apenas 2048 kbit/s, sendo que a sua utilização fora das horas de trabalho será muito reduzida.

A análise de custos permitirá verificar se a diferença de custos dos dois cenários compensa os custos associados às operações de "tape shippping".

4.1.5.2 Cenários de Interligação dos vários sites

Nesta secção serão apresentadas as diversas formas de interligação dos vários cenários descrevendo as tecnologias usadas e tentando sumarizar as suas vantagens e desvantagens.

Relativamente à forma de interligar os diversos sites surgem, como rede de interligação, 2 cenários possíveis:

- **Cenário A** – utilizar a Internet para estabelecer túneis lógicos entre os vários sites, utilizando mecanismos criptográficos para garantir a confidencialidade e integridade dos dados, uma vez que vão viajar numa rede pública. Os túneis seriam baseados no protocolo Generic Routing Encapsulation (GRE) que permite encapsular os pacotes de dados do tipo *multicast* [40] utilizados pelos protocolos de routing, nomeadamente pelo OSPF [41], para a troca de informações de routing. Relativamente aos mecanismos criptográficos, para garantir a confidencialidade dos dados seria utilizado o protocolo Advanced Encryption Standard (AES), face à sua resistência e desempenho [42], e o protocolo Secure Hash Algorithm (SHA) para garantir a integridade dos dados.

- **Cenário B** – utilizar a rede privada do ISP, que com base na tecnologia MultiProtocol Label Switching (MPLS), permite ao ISP encaminhar os pacotes dos diversos clientes de forma rápida e privada, através de VPN's MPLS, utilizando uma rede que apesar de privada (do ISP) é partilhada por vários clientes sem que haja qualquer relação entre os pacotes dos diversos clientes [43].

A tabela 6 faz uma análise comparativa dos 2 cenários:

Tabela 6 Análise comparativa da utilização da Internet ou de uma VPN MPLS

Cenário A	**Cenário B**
Difícil implementar mecanismos de marcação de tráfego para QoS controlado pelo facto de se basear na Internet, caracterizada por prestar um serviço "best-effort" [44]	Mais fácil implementar mecanismos de marcação de tráfego para QoS controlado [44] [45]
A administração de túneis GRE com mecanismos criptográficos é mais complexa e causa algum overhead [43]	Não há necessidade de utilizar mecanismos criptográficos uma vez que os dados não viajam numa rede pública [43]
Cada site tem um acesso à Internet o que obriga à implementação de um *firewall* em cada um, aumentado assim a dificuldade de administração e manutenção da infra-estrutura. Aumenta no entanto a velocidade de acesso à Internet uma vez que cada site tem uma ligação directa.	O acesso à Internet é feito de forma centralizada o que reduz a administração e controlo de *firewall*'s a uma único sítio mas também reduz a velocidade de acesso à Internet uma vez que será utilizado o único acesso para todos os colaboradores.

Para cada cenário A e B é necessário avaliar a opção de um DRS baseado num serviço de *Housing* ou suportado no escritório de Lisboa e para cada um desses casos a avaliação de a sincronização dos dados através de circuito digital ou através de tape shipping.

Resumindo, devem ser avaliados os seguintes cenários:

- **Cenário A1H** – Interligação através da Internet com sincronização dos dados através de circuito digital e DRS em *Housing*;

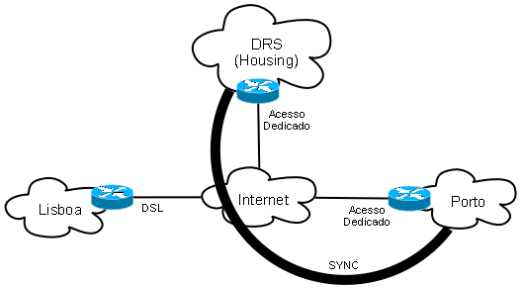


Figura 60 Esquema lógico Cenário A1H

- **Cenário A1L** – Interligação através da Internet com sincronização dos dados através de circuito digital e DRS em Lisboa;

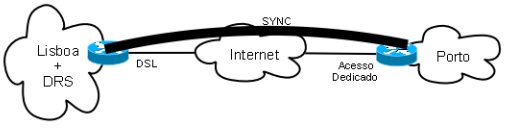


Figura 61 Esquema lógico Cenário A1L

- **Cenário A2H** – Interligação através da Internet com sincronização dos dados através de tape shipping e DRS em *Housing*;

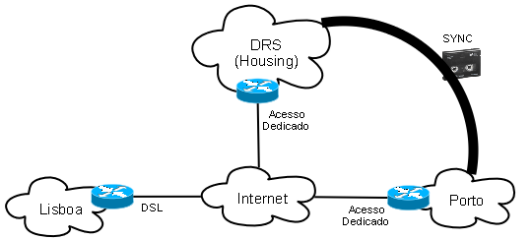


Figura 62 Esquema lógico Cenário A2L

- **Cenário A2L** – Interligação através da Internet com sincronização dos dados através de tape shipping e DRS em Lisboa;

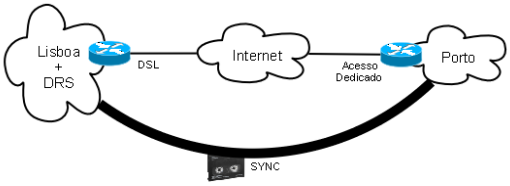


Figura 63 Esquema lógico Cenário A2L

- **Cenário B1H** – Interligação através de MPLS com sincronização dos dados através de circuito digital e DRS em *Housing*;

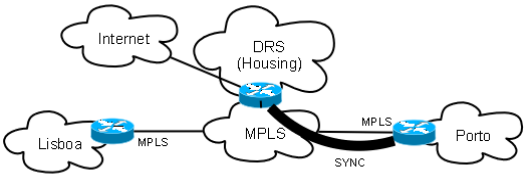


Figura 64 Esquema lógico Cenário B1H

- **Cenário B1L** – Interligação através de MPLS com sincronização dos dados através de circuito digital e DRS em Lisboa;

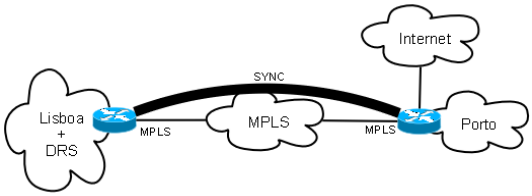


Figura 65 Esquema lógico Cenário B1L

- **Cenário B2H** – Interligação através de MPLS com sincronização dos dados através de tape shipping e DRS em *Housing*;

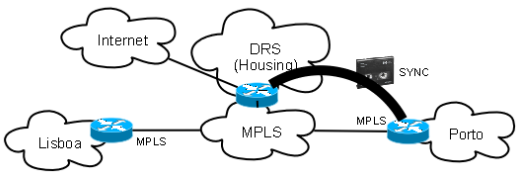


Figura 66 Esquema lógico Cenário B2H

- **Cenário B2L** – Interligação através de MPLS com sincronização dos dados através de tape shipping e DRS em Lisboa;

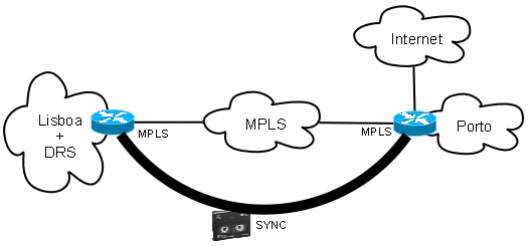


Figura 67 Esquema lógico Cenário B2L

Em qualquer um destes cenários de interligação, se a infra-estrutura actual do ISI permitir o estabelecimento de um túnel GRE entre Porto e Lisboa, é possível utilizar esse túnel como forma alternativa de interligação do Porto e Lisboa. Nesta situação de recurso, da comunicação entre Porto e Lisboa ser garantida pela rede do ISI, a ligação fica limitada pela velocidade do acesso em Lisboa que é apenas de 256 kbit/s.

4.1.5.3 Dimensionamento dos circuitos de Interligação

Seguidamente, para cada cenário identificado na secção anterior, são apresentadas as dimensões mínimas para os diversos circuitos, com base na análise de fluxos realizada:

- **Cenário A1H**
  - Ligação Internet Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
  - Ligação Internet Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
  - Ligação Internet *Housing*: 4 Mbit/s (down) / 4 Mbit/s (up)
- **Cenário A1L**
  - Ligação Internet Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
  - Ligação Internet Lisboa:
    - 4 Mbit/s (down) / 1 Mbit/s (up) (obriga deslocação física)
    - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente)
- **Cenário A2H**
  - Ligação Internet Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
  - Ligação Internet Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
  - Ligação Internet *Housing*: 4 Mbit/s (down) / 4 Mbit/s (up)
- **Cenário A2L**
  - Ligação Internet Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
  - Ligação Internet Lisboa:
    - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física)
    - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente)
- **Cenário B1H**
  - Ligação MPLS Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
  - Ligação MPLS Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
  - Ligação MPLS *Housing*: 4 Mbit/s (down) / 4 Mbit/s (up)
  - Ligação Internet Centralizada: 2 Mbit/s (down) / 2 Mbit/s (up)
- **Cenário B1L**
  - Ligação MPLS Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
  - Ligação MPLS Lisboa:

        - 4 Mbit/s (down) / 4 Mbit/s (up)
    - Ligação Internet Centralizada:
        - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física)
        - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente)
- **Cenário B2H**
    - Ligação MPLS Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
    - Ligação MPLS Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
    - Ligação MPLS *Housing*: 2 Mbit/s (down) / 2 Mbit/s (up)
    - Ligação Internet Centralizada: 2 Mbit/s (down) / 2 Mbit/s (up)
- **Cenário B2L**
    - Ligação MPLS Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
    - Ligação MPLS Lisboa:
        - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física)
        - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente)
    - Ligação Internet Centralizada:
        - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física)
        - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente)

4.1.6 Previsão de Custos

Nesta secção serão apresentados apenas os custos totais envolvidos para a aquisição de equipamento e *software* necessário para a implementação da infra-estrutura proposta. O anexo D apresenta os detalhes desses custos.

4.1.6.1 Custos de Aquisição de Equipamento e Software

Tendo por base os detalhes apresentados no anexo D, os custos envolvidos para aquisição de equipamento e *software* são os seguintes:

- O custo de um *router* com capacidades de *firewall* para o Porto oscilará na seguinte gama de valores: **de 3400€ até 7500€ + IVA**.
- O custo de um *router* com capacidades de *firewall* para Lisboa oscilará na seguinte gama de valores: **de 800€ até 3500€ + IVA.**
- O custo de um *router* com capacidades de *firewall* para o DRS oscilará na seguinte gama de valores: **de 800€ até 3500€ + IVA.**
- Para a aquisição de licenças haverá um custo associado de cerca de **8800€ + IVA.**

O custo total de aquisição de equipamento e *software* oscilará então entre a seguinte gama de valores: **de 13800€ até 23300€ + IVA.**

4.1.6.2 Custos dos Serviços dos ISP's

A tabela 7 resume as informações relativas aos preços fornecidos pelos vários ISP's, para os circuitos e serviços a contratar para os vários cenários avaliados. Os detalhes dos custos apresentados na tabela 8 podem ser consultados no Anexo D.

Tabela 7 Resumo das cotações dos vários ISP's para os vários cenários

Cenário	ISP1	ISP2	ISP3	ISP4
A1H	Total: 3782,9€ (1) Total: 4731,9€ (2) Total: 6631,9€ (3)	Total: 1060€ (1) Total: 1130€ (2) Total: 1200€ (3) Total: 1260€ (4)	Total: 1309,54€ (1) Total: 1401,85€ (2) Total: 1494,15€ (3) Total: 1586,46€ (4)	Total: 1650€
A1L	Total: 2796,9€ (1/ODF) Total: 3745,9€ (2/ODF) Total: 5645,9€ (3/ODF) Total: 5232,9€ (1/PTR) Total: 6181,9€ (2/PTR) Total: 8081,9€ (3/PTR)	Total: 860€ (1/ODF) Total: 930€ (2/ODF) Total: 1000€ (3/ODF) Total: 1060€ (4/ODF) Total: 1540€ (1/PTR) Total: 1610€ (2/PTR) Total: 1680€ (3/PTR) Total: 1740€ (4/PTR)	Total: 1109,54€ (1/ODF) Total: 1201,85€ (2/ODF) Total: 1294,15€ (3/ODF) Total: 1386,46€ (4/ODF) Total: 1973,08€ (1/PTR) Total: 2065,39€ (2/PTR) Total: 2158,69€ (3/PTR) Total: 2250€ (4/PTR)	
A2H	Total: 1119,9€ (1) Total: 3045,9€ (2) Total: 3994,9€ (3) Total: 6894,9€ (4)	Total: 890€ (1) Total: 1060€ (2) Total: 1130€ (3) Total: 1200€ (4) Total: 1260€ (5)	Total: 1217,23€ (1) Total: 1309,54€ (2) Total: 1401,85€ (3) Total: 1494,15€ (4) Total: 1586,46€ (5)	
A2L	Total: 957,9€ (1/ODF) Total: 2883,9€ (2/ODF) Total: 3832,9€ (3/ODF) Total: 5732,9€ (4/ODF) Total: 3306,9€ (1/PTR) Total: 5232,9€ (2/PTR) Total: 6181,9€ (3/PTR) Total: 8081,9€ (4/PTR)	Total: 760€ (1/ODF) Total: 930€ (2/ODF) Total: 1000€ (3/ODF) Total: 1070€ (4/ODF) Total: 1130€ (5/ODF) Total: 1370€ (1/PTR) Total: 1540€ (2/PTR) Total: 1610€ (3/PTR) Total: 1680€ (4/PTR) Total: 1740€ (5/PTR)	Total: 1104,23€ (1/ODF) Total: 1196,54€ (2/ODF) Total: 1288,85€ (3/ODF) Total: 1381,15€ (4/ODF) Total: 1473,46€ (5/ODF) Total: 1880,77€ (1/PTR) Total: 1973,08€ (2/PTR) Total: 2065,39€ (3/PTR) Total: 2157,69€ (4/PTR) Total: 2250€ (5/PTR)	Total: 1650€ (ODF)
B1H		Total: 1630€ (1 a): Total: 1880€ (1 b) Total: 1650€ (2 a) Total: 1900€ (2 b) Total: 1740€ (3 a) Total: 1990€ (3 b) Total: 1770€ (4 a) Total: 2020€ (4 b)	Total: 1423,21€ (1) Total: 1515,52€ (2) Total: 1607,82€ (3) Total: 1700,13€ (4)	Total: 1700€
B1L		Total: 1600€ (1 ODF) Total: 1850€ (1 PTR) Total: 1620€ (2 ODF) Total: 1870€ (2 PTR) Total: 1710€ (3 ODF) Total: 1960€ (3 PTR) Total: 1740€ (4 ODF) Total: 1990€ (4 PTR)		
B2H		Total: 1600€ (1 a) Total: 1850€ (1 b) Total: 1630€ (2 a) Total: 1880€ (2 b) Total: 1650€ (3 a) Total: 1900€ (3 b) Total: 1740€ (4 a) Total: 1990€ (4 b) Total: 1770€ (5 a) Total: 2020€ (5 b)	Total: 1330,9€ (1) Total: 1423,21€ (2) Total: 1515,52€ (3) Total: 1607,82€ (4) Total: 1700,13€ (5)	Total: 1700€
B2L		Total: 1540€ (1 a) Total: 1790€ (1 b) Total: 1820€ (1 b PTR) Total: 1570€ (2 a) Total: 1820€ (2 b) Total: 1850€ (2 b PTR) Total: 1590€ (3 a) Total: 1840€ (3 b) Total: 1870€ (3 b PTR) Total: 1680€ (4 a) Total: 1930€ (4 b) Total: 1960€ (4 b PTR) Total: 1710€ (5 a) Total: 1960€ (5 b) Total: 1990€ (5 b PTR)	Total: 1130,9€ (1 ODF) Total: 1223,21€ (2 ODF) Total: 1315,52€ (3 ODF) Total: 1407,82€ (4 ODF) Total: 1500,13€ (5 ODF)	

São utilizadas as seguintes abreviaturas na tabela 7:

- ODF – Obriga Deslocação Física
- PTR – Permite Trabalhar Remotamente

Para cada cenário foram consultados vários níveis de serviço sendo que o nível mais baixo, assinalado com "(1)", corresponde aos requisitos mínimos identificados, e os restantes, assinalados com "(2)", "(3)", "(4)" e "(5)" correspondem a serviços com características gradualmente superiores.

O ISP2 foi aquele que forneceu a maior quantidade de informação e, de uma forma geral, os preços mais baixos. Por essa razão, a análise efectuada de seguida para comprar os diversos cenários em termos de custos, utiliza apenas as cotações fornecidas pelo ISP2.

A comparação dos custos dos cenários de manter um DRS em *Housing versus* a manutenção dessas infra-estruturas no escritório de Lisboa (excluindo os custos directos associados às obras de instalação e manutenção das infra-estruturas de electricidade e condições ambientais, para além de outros custos indirectos) é resumida na tabela 8.

Tabela 8 Comparação de custos para cenário com DRS em *Housing versus* Lisboa

Housing	**Lisboa (ODF)**	**Lisboa (PTR)**	**Diferença (*Housing* – ODF)**	**Diferença (*Housing* – PTR)**
1.060 €	860 €	1540 €	200 €	-480 €
890 €	760 €	1370 €	130 €	-480 €
1.630 €	1.600 €	1850 €	30 €	-220 €
1.600 €	1.540 €	1820 €	60 €	-220 €

A diferença de custos entre a opção *Housing* e a opção do DRS em Lisboa, com necessidade de deslocação dos trabalhadores em caso de desastre, é pouco significativa, sendo a mensalidade da opção *Housing* em média 11% mais cara. A diferença entre a opção *Housing* e a opção do DRS em Lisboa com possibilidade de trabalhar remotamente em caso de desastre é elevada, sendo a opção do DRS em Lisboa 32% mais cara, somente pelo agravamento da largura de banda necessária. Assim, face às comparações feitas anteriormente, considera-se a opção *Housing* mais vantajosa.

A tabela 9 compara os custos dos circuitos associados a uma sincronização do DRS e dos servidores primários através de circuito digital *versus* a utilização de Tape Shipping (*Hot Standby versus Cold Standby*).

Tabela 9 Comparação de custos para cenário com sincronização digital *versus* tape shippping

Sincronização Digital	**Sincronização Tape Shipping**	**Diferença**
1.060 €	890 €	170 €
860 €	760 €	100 €
1.630 €	1.600 €	30 €
1.600 €	1.540 €	60 €

A diferença de mensalidades entre a sincronização através do circuito de dados e o *backup* por tape shipping é em média de 9%. Actualmente o serviço contratado pelo IGC para fazer o transporte e armazenamento das tapes nas instalações da Maia da empresa de segurança, com a frequência de 3 vezes por semana, tem uma mensalidade de 330€. Para cumprir os requisitos especificados pelo IGC para o DR seria necessário aumentar a periodicidade do serviço para diária, e por isso esse custo deverá ser naturalmente superior. Tendo em conta que a

sincronização digital permite a transferência de informação para o DRS com maior frequência, garantindo que em caso de desastre, a informação a utilizar é mais actual. Por tudo isto considera-se a opção de sincronização digital a melhor opção.

Finalmente, faz-se a comparação dos custos associados à ligação dos diversos sites utilizando como base a Internet *versus* uma rede privada em MPLS contratada a um ISP.

Tabela 10 Comparação de custos para cenário de ligação pela Internet *versus* VPN MPLS

	Internet	**MPLS**	**Diferença**
Velocidade Mínima	1.060 €	1.630 €	570 €
Velocidade Mínima	860 €	1.600 €	740 €
Velocidade Mínima	890 €	1.600 €	710 €
Velocidade Mínima	760 €	1.540 €	780 €
Velocidade Máxima	1.260 €	2.020 €	760 €
Velocidade Máxima	1.060 €	1.990 €	930 €
Velocidade Máxima	1.260 €	2.020 €	760 €
Velocidade Máxima	1.130 €	1.960 €	830 €

A tabela 10 mostra que a opção MPLS é substancialmente mais cara que a opção Internet (cerca de 76% mais cara). Esta diferença de preço agrava-se quando se trata de opções com necessidade de maior largura de banda, ou seja: com a opção Internet, o diferencial para obter velocidades maiores - o que permite proporcionar aos utilizadores uma melhor qualidade do serviço - é mais reduzido relativamente à opção MPLS.

Apesar das vantagens técnicas que a solução MPLS apresenta, considera-se que perante as necessidades e requisitos do IGC, a utilização da Internet para interligar os vários sites da instituição, com recurso a túneis encriptados, é uma boa solução. Esta permite, com custos inferiores, obter uma melhor qualidade de serviço perceptível pelos utilizadores da rede, uma vez que cada site terá um acesso à Internet individual, aumentando assim consideravelmente a velocidade de acesso ao exterior.

Portanto, de acordo com aquelas que foram consideradas as melhores opções, o custo da interligação dos vários sites irá variar desde 953€ até 1153€, tratando-se de uma infra-estrutura com as seguintes características:

- Ligação dedicada à Internet no Porto com velocidades de 4 até 10 Mbit/s, sendo a velocidade mais baixa associada ao menor custo (953€) e a velocidade mais alta associada ao maior custo (1153€);
- Ligação ADSL em Lisboa com velocidades de 24 Mbit/s (*Downstream*) / 1 Mbit/s (*Upstream*) com taxa de contenção implícita;
- Serviço de *Housing*;
- Serviço de E-mail *Relay* com protecção anti-Spam e administração do domínio.

4.1.7 Conclusões

Neste capítulo pretende-se apresentar as conclusões consideradas mais relevantes sobre a solução que permitirá dotar o IGC de uma infra-estrutura de rede de comunicações fiável, como consequência dos resultados obtidos do trabalho desenvolvido na fase de planeamento e preparação.

A solução agora apresentada pretende satisfazer os requisitos técnicos identificados, onde foram detectadas várias falhas e fragilidades da infra-estrutura de rede de comunicações existente, dificultando o objectivo desta servir de alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio do IGC.

A análise de diversos cenários possíveis para a infra-estrutura da rede do IGC e de diferentes tecnologias para os suportar permitiu desenhar uma solução que, relativamente à actual infra-estrutura, apresenta as seguintes vantagens:

- É disponibilizado um acesso à Internet que, a curto prazo, não constitui à partida a limitação na utilização da rede;
- A velocidade da interligação do escritório do Porto ao de Lisboa é pelo menos 4 vezes superior;
- O serviço de acesso à Internet terá uma disponibilidade garantida por um Service Level Agreement (SLA) implícito de, no mínimo, 99,50% ou outro a negociar;
- O serviço de e-mail é gerido pelo IGC e dotado de mecanismos que pretendem assegurar e garantir a sua fiabilidade em termos de disponibilidade e de tempo de entrega médio das mensagens;
- O serviço de autenticação é gerido pelo IGC e permitirá o controlo, a resposta atempada e a personalização de perfis específicos para os utilizadores do Instituto;
- O IGC pode prontamente proceder às alterações operacionais ou de segurança nos seus acessos ao exterior, sempre que tal for necessário;
- Possibilidade de disponibilizar aos utilizadores um serviço de acesso remoto à rede, quer para teletrabalho quer para operações de manutenção à infra-estrutura;
- Possibilidade de disponibilizar acesso remoto, seguro e controlado a prestadores de serviços, para a realização de operações de manutenção a serviços específicos;
- Implementação de mecanismos que permitem garantir a Segurança da Informação e dos respectivos fluxos, a nível interno e externo;
- Infra-estrutura de suporte a um DRP que permite assegurar a continuidade do funcionamento dos sistemas e serviços críticos do IGC, em caso de desastre no pólo do Porto;
- A contratação do serviço de *Housing* compreende o aluguer do espaço num bastidor de comunicações e acessoriamente a garantia de:
    - Condições ambientais controladas,
    - Segurança física dos acessos,
    - Fornecimento de alimentação de energia, com fontes socorridas,
    - Acesso à Internet;
- A contratação do serviço de *Housing* permite excluir os custos associados à instalação e manutenção das infra-estruturas equivalentes no pólo técnico de Lisboa;
- Se o IGC optar por contratar a solução a 10 Mbit/s poderá considerar disponibilizar o serviço de comunicação de Voz e Vídeo sobre IP entre os escritórios do Porto e Lisboa e, eventualmente, com outros parceiros na Internet.

4.2 *Proof of Concept*

Nesta secção serão apresentados os resultados do processo de simulação parcial da infra-estrutura proposta de forma a concluir a fase de desenho, com o objectivo de validar a arquitectura e prever eventuais problemas que possam surgir na fase de implementação.

A simulação foi feita recorrendo às seguintes ferramentas:

- Vmware Server [5]– Plataforma de virtualização de sistemas operativos gratuita que permitirá simular os servidores abrangidos nesta infra-estrutura de testes;
- GNS3 [6]– Interface gráfico que permite interagir com o Dynamips, emulador do Internetwork Operating System (IOS), sistema operativo de todos os *routers* Cisco tornando assim possível simular com grande realismo toda a topologia de routing envolvida na infra-estrutura de rede proposta.

4.2.1 Infra-estrutura de interligação dos sites

Para simular e testar a infra-estrutura que interligará os vários sites que constituem a arquitectura proposta, foi construída, no GNS3, a rede representada na figura 68.

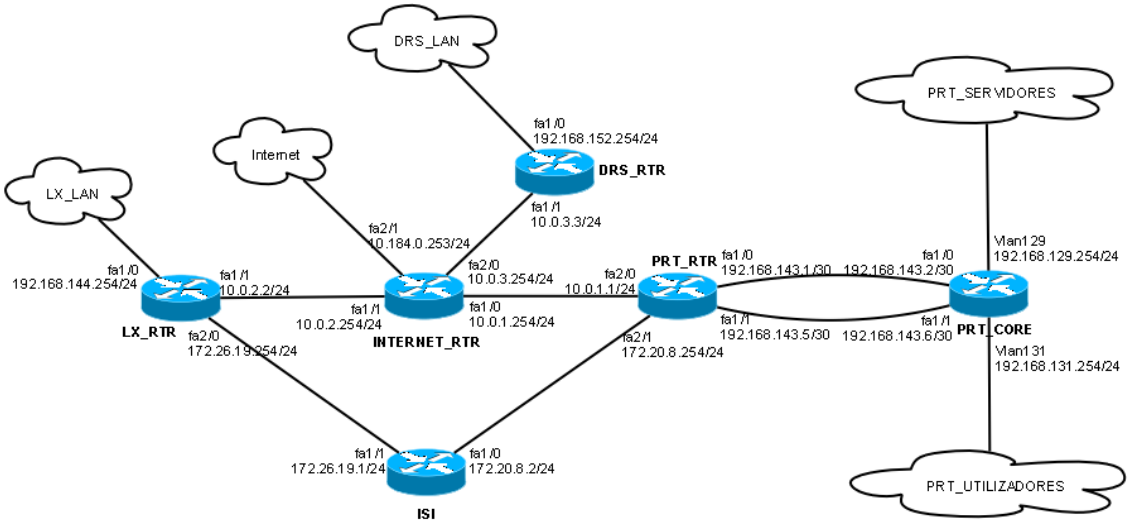


Figura 68 Arquitectura da infra-estrutura utilizada para *Proof of Concept*

As redes PRT_SERVIDORES, PRT_UTILIZADORES, LX_LAN e DRS_LAN fazem a ligação com as redes do Vmware, VMNET2, VMNET3, VMNET4 e VMNET5. As placas de rede das máquinas virtuais utilizadas para testes serão depois associadas a estas redes garantindo que se encontram em segmentos de rede virtualmente separados.

4.2.1.1 Túneis de ligação ponto-a-ponto

De seguida são referidos e comentados os comandos fundamentais utilizados para a configuração de túneis GRE nos *routers* do Porto, Lisboa e DRS de forma a permitir uma ligação ponto-a-ponto entre Porto e Lisboa e Porto e DRS. As configurações apresentadas baseiam-se nas recomendações e orientações da referência [46]. Como exemplo serão apenas

[5] Para mais informações consultar: http://www.vmware.com
[6] Para mais informações consultar: http://www.gns3.net

apresentadas as configurações correspondentes ao site do Porto, sendo a estrutura da configuração dos restantes sites idêntica.

```
interface Tunnel0
 ! Largura de banda da interface lógica indicada em kbit/s. É importante a definição deste parâmetro pois vai ser utilizado pelo protocolo de encaminhamento (OSPF) para fazer a selecção do melhor caminho
 bandwidth 10480
 ! Definição do endereço IP com um prefixo /30 correspondendo por isso a uma ligação ponto-a-ponto
 ip address 192.168.160.1 255.255.255.252
 ! Interface que será a origem do túnel que corresponde neste Tunnel0 à interface que liga à Internet
 tunnel source FastEthernet2/0
 ! IP de destino do túnel que corresponde neste Tunnel0 ao IP da interface do Router de Lisboa que liga à Internet
 tunnel destination 10.0.2.2

interface Tunnel1
 bandwidth 256
 ip address 192.168.160.5 255.255.255.252
 ! Interface que será a origem do túnel que corresponde neste Tunnel1 à interface que liga à rede do ISI
 tunnel source FastEthernet2/1
 ! IP de destino do túnel que corresponde neste Tunnel1 ao IP da interface do Router de Lisboa que liga à rede do ISI
 tunnel destination 172.26.19.254

interface Tunnel2
 bandwidth 10240
 ip address 192.168.160.9 255.255.255.252
 ! Interface que será a origem do túnel que corresponde neste Tunnel2 à interface que liga à Internet
 tunnel source FastEthernet2/0
 ! IP de destino do túnel que corresponde neste Tunnel2 ao IP da interface do Router de DRS que liga à Internet
 tunnel destination 10.0.3.3
```

Após a configuração dos comandos anteriores a conectividade é verificada através do estado das interfaces lógicas e utilizando o protocolo Internet Control Message Protocol (ICMP), através do comando ping.

```
! Verificação do estado das interfaces lógicas
PRT_RTR#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet2/0            10.0.1.1        YES NVRAM  up                    up
FastEthernet2/1            172.20.8.254    YES NVRAM  up                    up
Tunnel0                    192.168.160.1   YES NVRAM  up                    up
Tunnel1                    192.168.160.5   YES NVRAM  up                    up
Tunnel2                    192.168.160.9   YES NVRAM  up                    up

! Testes de conectividade através de pacotes ICMP
! Teste de conectividade Lisboa pela Internet
PRT_RTR#ping 192.168.160.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/124/188 ms

! Teste de conectividade Lisboa pela rede do ISI
PRT_RTR#ping 192.168.160.6
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/112/132 ms

! Teste de conectividade DRS pela Internet
PRT_RTR#ping 192.168.160.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.160.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/113/120 ms
```

As configurações apresentadas permitem estabelecer conectividade ponto-a-ponto entre Porto e Lisboa e Porto e DRS mas a informação enviada viaja sem qualquer tipo de protecção que garanta a sua confidencialidade e integridade sobre a Internet e a rede do ISI tal como prova a imagem seguinte que corresponde a uma captura feita, através do Wireshark, dos pacotes que atravessam o *router* que simula a Internet.

No.	Time	Source	Destination	Protocol	Info
12	9.347000	192.168.160.1	192.168.160.2	ICMP	Echo (ping) request
13	9.391000	192.168.160.2	192.168.160.1	ICMP	Echo (ping) reply
14	9.445000	192.168.160.1	192.168.160.2	ICMP	Echo (ping) request
15	9.503000	192.168.160.2	192.168.160.1	ICMP	Echo (ping) reply
16	9.553000	192.168.160.1	192.168.160.2	ICMP	Echo (ping) request
17	9.598000	192.168.160.2	192.168.160.1	ICMP	Echo (ping) reply

Figura 69 Captura Wireshark comprovando a falta de confidencialidade dos dados transmitidos sobre túneis sem protecção

Para proteger os dados enviados será utilizada suite de protocolos IPSEC aplicada aos túneis GRE [46], acrescentando os seguintes comandos à configuração apresentada atrás:

```
! Configuração da política isakmp utilizada para a negociação inicial dos parâmetros de segurança a utilizar que são definidos através do "transform-set" parametrizado mais abaixo
crypto isakmp policy 10
 ! Encriptação AES com chave de 192 bits
 encr aes 192
 ! Autenticação através de chave partilhada
 authentication pre-share

! Chave partilhada para ligação com Lisboa pela Internet
crypto isakmp key INTERNET123456 address 10.0.2.2
! Chave partilhada para ligação com Lisboa pela rede do ISI
crypto isakmp key ISI123456 address 172.26.19.254
! Chave partilhada para ligação com DRS pela Internet
crypto isakmp key DRS123456 address 10.0.3.3
! Definição dos parâmetros de segurança utilizados na comunicação: confidencialidade dos dados garantida através de encriptação AES, integridade dos dados garantida através de SHA e encriptação do pacote IP original através de ESP garantindo a confidencialidade dos dados do pacote IP
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac

! Criação de um perfil qua aplica o "transform-set" criado anteriormente
crypto ipsec profile TUNNEL-ESP-AES-SHA
 set transform-set ESP-AES-SHA
interface tunnel0
 ! Alteração do modo de funcionamento do tunnel0 para ipsec
 tunnel mode ipsec ipv4
 ! Aplicação do perfil ipsec anteriormente criado
 tunnel protection ipsec profile TUNNEL-ESP-AES-SHA

interface tunnel1
```

```
 ! Alteração do modo de funcionamento do tunnel1 para ipsec
 tunnel mode ipsec ipv4
 ! Aplicação do perfil ipsec anteriormente criado
 tunnel protection ipsec profile TUNNEL-ESP-AES-SHA

interface tunnel2
 ! Alteração do modo de funcionamento do tunnel2 para ipsec
 tunnel mode ipsec ipv4
 ! Aplicação do perfil ipsec anteriormente criado
 tunnel protection ipsec profile TUNNEL-ESP-AES-SHA
```

Após a aplicação dos comandos referidos, uma nova captura feita através do Wireshark, dos pacotes que atravessam o *router* que simula a Internet, permite verificar a confidencialidade dos dados.

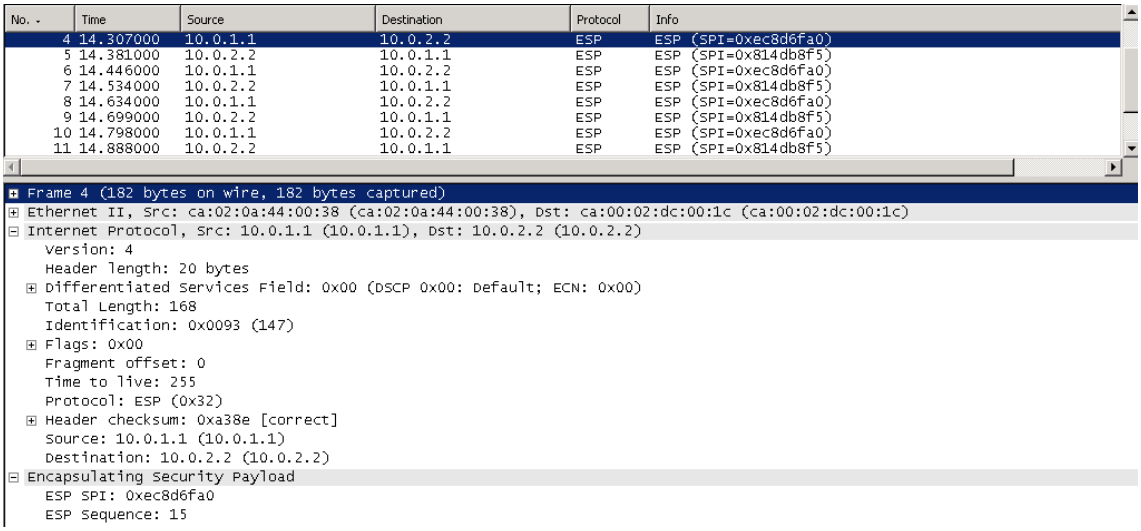


Figura 70 Captura Wireshark comprovando a confidencialidade dos dados transmitidos sobre túneis com protecção IPSEC

4.2.1.2 OSPF

Criadas as ligações ponto-a-ponto entre os *routers* que estabelecem a ligação ao exterior nos vários sites, o próximo passo é a configuração do protocolo de encaminhamento escolhido, o OSPF. Este protocolo irá permitir o anúncio automático das sub-redes de cada site aos restantes assim como, no caso da ligação entre Porto e Lisboa, uma vez que existe uma ligação redundante (através da Internet e do ISI) escolher a melhor ligação e seleccionar automaticamente a secundária em caso de falha da ligação primária. As configurações apresentadas de seguida baseiam-se nas recomendações e orientações da referência [30]. Novamente, serão apenas apresentadas como exemplo as configurações correspondentes ao site do Porto.

Porto (*Router* de ligação ao exterior):

```
! Criação do processo OSPF 111. O número identificativo do processo, 111, tem apenas
significado local não sendo por isso necessário ser o mesmo em todos os routers, apesar
de na configuração apresentada ser sempre 111
router ospf 111
 ! Area 0 será autenticada com de passwords cifradas pelo algoritmo MD5
 area 0 authentication message-digest
 ! Area 1 será autenticada com de passwords cifradas pelo algoritmo MD5
 area 1 authentication message-digest
```

```
 ! Area 1 será do tipo Totally Stubby o que significa que não lhe serão anunciadas redes de outras áreas (do tipo IA) e de redes externas (do tipo EX)
 area 1 stub no-summary
 ! Sumarização das sub-redes que constiturem a área 1 através do range 192.168.128.0/20 originando assim que às restantes áreas, 0, 2 e 3 uma rede ao invés de todas as sub-redes que constituem a rede do Porto
 area 1 range 192.168.128.0 255.255.240.0
 ! Desactivação dos anúncios OSPF na interface que liga à Internet
 passive-interface FastEthernet2/0
 ! Desactivação dos anúncios OSPF na interface que liga à rede do ISI
 passive-interface FastEthernet2/1
 ! Activação do OSPF nas na interface que liga ao Core da rede do Porto (FastEthernet1/0)
 network 192.168.143.1 0.0.0.0 area 1
 ! Activação do OSPF nas na interface que liga ao Core da rede do Porto (FastEthernet1/1)
 network 192.168.143.5 0.0.0.0 area 1
 ! Activação do OSPF nas na interface que liga a Lisboa pela Internet (Tunnel0)
 network 192.168.160.1 0.0.0.0 area 0
! Activação do OSPF nas na interface que liga a Lisboa pela rede do ISI (Tunnel1)
 network 192.168.160.5 0.0.0.0 area 0
! Activação do OSPF nas na interface que liga ao DRS pela Internet (Tunnel2)
 network 192.168.160.9 0.0.0.0 area 0

! Definição da password a utilizar para autenticar nas várias interfaces
interface Tunnel0
 ip ospf message-digest-key 1 md5 OSPF0123456
interface Tunnel1
 ip ospf message-digest-key 1 md5 OSPF0123456
interface Tunnel2
 ip ospf message-digest-key 1 md5 OSPF0123456
interface FastEthernet1/0
 ip ospf message-digest-key 1 md5 OSPF1123456
 ! Definição do tipo de rede como ponto-a-ponto. Como se trata de uma interface de rede do tipo Ethernet procede por defeito à eleição de um Designated Router o que não faz sentido na ligação ponto-a-ponto que é.
 ip ospf network point-to-point
interface FastEthernet1/1
 ip ospf message-digest-key 1 md5 OSPF1123456
 ip ospf network point-to-point
```

Porto (Core):

```
router ospf 111
 area 1 authentication message-digest
 area 1 stub no-summary
 ! Desactivação dos anúncios OSPF na interface que liga à Vlan Servidores
 passive-interface vlan 129

 ! Activação do OSPF nas na interface que liga ao router de acesso ao exterior (FastEthernet1/0)
 network 192.168.143.2 0.0.0.0 area 1
  ! Activação do OSPF nas na interface que liga ao router de acesso ao exterior (FastEthernet1/1)
 network 192.168.143.6 0.0.0.0 area 1
 ! Activação do OSPF nas na interface que liga à vlan Servidores (Vlan 129)
 network 192.168.129.254 0.0.0.0 area 1

interface FastEthernet1/0
 ip ospf message-digest-key 1 md5 OSPF1123456
 ip ospf network point-to-point
interface FastEthernet1/1
```

```
 ip ospf message-digest-key 1 md5 OSPF1123456
 ip ospf network point-to-point
```

Configurados os *routers* que irão participar no protocolo OSPF verificar-se-á o seu correcto funcionamento através da observação das tabelas de encaminhamento e da execução de testes de conectividade utilizando o protocolo ICMP, através do comando traceroute.

```
PRT_RTR#show ip route ospf
O IA 192.168.144.0/24 [110/10] via 192.168.160.2, 00:35:31, Tunnel0
O    192.168.129.0/24 [110/2] via 192.168.143.6, 00:35:46, FastEthernet1/1
                      [110/2] via 192.168.143.2, 00:35:46, FastEthernet1/0
O IA 192.168.152.0/24 [110/10] via 192.168.160.10, 00:35:31, Tunnel2
O    192.168.128.0/20 is a summary, 00:35:46, Null0

PRT_CORE#show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.143.5, 00:36:07, FastEthernet1/1
               [110/2] via 192.168.143.1, 00:36:07, FastEthernet1/0

LX_RTR#show ip route ospf
     192.168.160.0/30 is subnetted, 3 subnets
O       192.168.160.8 [110/106] via 192.168.160.1, 00:36:15, Tunnel0
O IA 192.168.152.0/24 [110/107] via 192.168.160.1, 00:36:15, Tunnel0
O IA 192.168.128.0/20 [110/98] via 192.168.160.1, 00:36:15, Tunnel0

DRS_RTR#show ip route ospf
O IA 192.168.144.0/24 [110/11121] via 192.168.160.9, 00:36:42, Tunnel0
     192.168.160.0/30 is subnetted, 3 subnets
O       192.168.160.0 [110/11120] via 192.168.160.9, 00:36:42, Tunnel0
O       192.168.160.4 [110/11501] via 192.168.160.9, 00:36:42, Tunnel0
O IA 192.168.128.0/20 [110/11112] via 192.168.160.9, 00:36:42, Tunnel0

LX_RTR#traceroute 192.168.129.254
Type escape sequence to abort.
Tracing the route to 192.168.129.254
  1 192.168.160.1 108 msec 136 msec 116 msec
  2 192.168.143.6 176 msec 152 msec 130 msec

DRS_RTR#traceroute 192.168.129.254
Type escape sequence to abort.
Tracing the route to 192.168.129.254
  1 192.168.160.9 100 msec 136 msec 172 msec
  2 192.168.143.6 128 msec 112 msec  116 msec
```

Os testes de conectividade apresentam os resultados esperados. De seguida simular-se-á uma falha na ligação à Internet de Lisboa, sendo apresentadas as novas tabelas de encaminhamento após a convergência do protocolo OSPF e executados novos testes de conectividade usando o comando traceroute comprovando desta forma a tolerância da infra-estrutura proposta a falhas.

```
PRT_RTR#show ip route ospf
! Passa a ser utilizado o Tunnel1 que é estabelecido sobre a rede do ISI
O IA 192.168.144.0/24 [110/391] via 192.168.160.6, 00:01:22, Tunnel1
O    192.168.129.0/24 [110/2] via 192.168.143.6, 00:48:03, FastEthernet1/1
                      [110/2] via 192.168.143.2, 00:48:03, FastEthernet1/0
O IA 192.168.152.0/24 [110/10] via 192.168.160.10, 00:47:48, Tunnel2
O    192.168.128.0/20 is a summary, 00:48:03, Null0

PRT_CORE#show ip route ospf
! A tabela de encaminhamento deste router não sofre qualquer alteração pelo facto de se
tratar de uma área do tipo Totally Stubby. Isto permite, tal como previsto, proteger o
```

```
router do Core não ocupando o seu processamento com alterações sofridas nas restantes
áreas do OSPF
O*IA 0.0.0.0/0 [110/2] via 192.168.143.5, 00:47:32, FastEthernet1/1
               [110/2] via 192.168.143.1, 00:47:32, FastEthernet1/0
```

```
LX_RTR#show ip route ospf
! Passa a ser utilizado o Tunnel1 que é estabelecido sobre a rede do ISI
     192.168.160.0/30 is subnetted, 3 subnets
O       192.168.160.8 [110/399] via 192.168.160.5, 00:01:44, Tunnel1
O       192.168.160.0 [110/399] via 192.168.160.5, 00:01:44, Tunnel1
O IA 192.168.152.0/24 [110/400] via 192.168.160.5, 00:01:44, Tunnel1
O IA 192.168.128.0/20 [110/391] via 192.168.160.5, 00:01:44, Tunnel1
```

```
DRS_RTR#show ip route ospf
! É actualizado o custo para chegar à rede de Lisboa
O IA 192.168.144.0/24 [110/11502] via 192.168.160.9, 00:01:26, Tunnel0
     192.168.160.0/30 is subnetted, 3 subnets
O       192.168.160.0 [110/11120] via 192.168.160.9, 00:48:24, Tunnel0
O       192.168.160.4 [110/11501] via 192.168.160.9, 00:48:24, Tunnel0
O IA 192.168.128.0/20 [110/11112] via 192.168.160.9, 00:48:24, Tunnel0
```

```
LX_RTR#traceroute 192.168.129.254
Type escape sequence to abort.
Tracing the route to 192.168.129.254
! Novo caminho percorrido pelos pacotes
  1 192.168.160.5 104 msec 132 msec 144 msec
  2 192.168.143.2 200 msec 150 msec 112 msec
```

4.2.2 Serviços

A figura 71 mostra os servidores que foram simulados através de máquinas virtuais em Vmware nesta fase de *Proof of Concept*. Os servidores simulados permitirão observar o comportamento do serviço de autenticação e respectivo DR, serviço de partilha de ficheiros e respectivo DR e serviço de e-mail e respectivo DR.

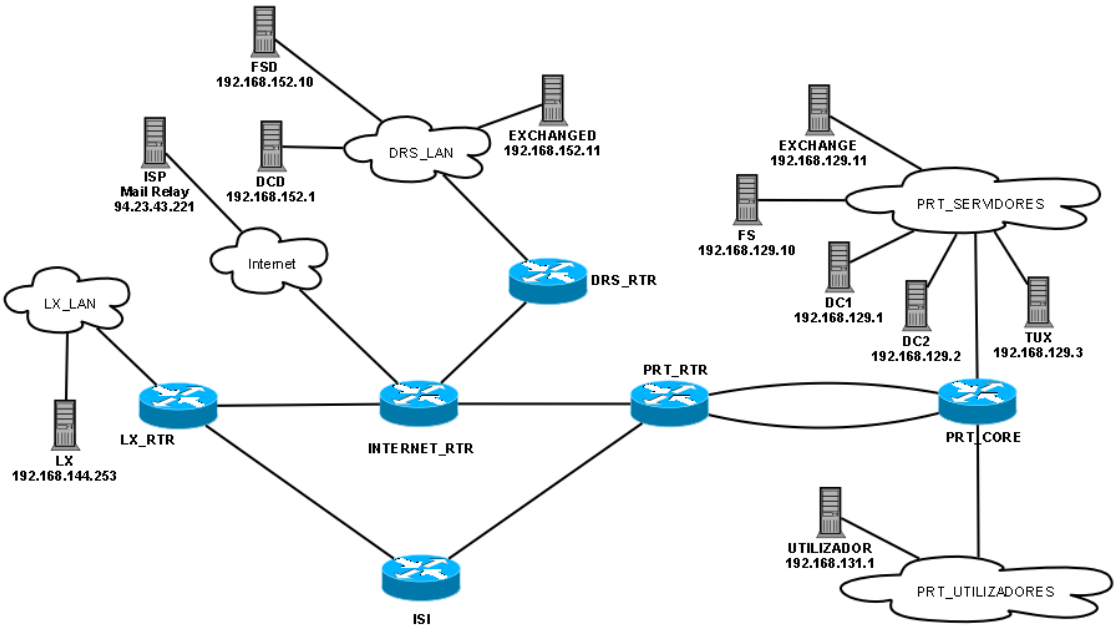


Figura 71 Servidores simulados para *Proof of Concept*

4.2.2.1 Serviço de Autenticação: Active Directory

Para a configuração do serviço de Autenticação foi utilizado o utilitário "dcpromo" nos seguintes servidores: DC1, DC2, LX e DCD. Após executar o referido utilitário no DC1, criando-se a estrutura do domínio "peer-link.net" (nome do domínio utilizado para testes), foram parametrizados, através da aplicação "Active Directory Sites and Services", os Sites, Subnets e Inter-Site Transports da AD, para optimizar a transferência de informação entre os vários servidores, uma vez que se encontram em sites distintos. Após a personalização dos diversos parâmetros, os restantes servidores, DC2, LX e DCD foram promovidos a DC's do domínio "peer-link.net". Todos os DC's foram configurados como Global Catalog de forma a guardarem uma réplica total das informações armazenadas na AD [33]. A figura 72 ilustra os parâmetros configurados na aplicação Active Directory Sites and Services.

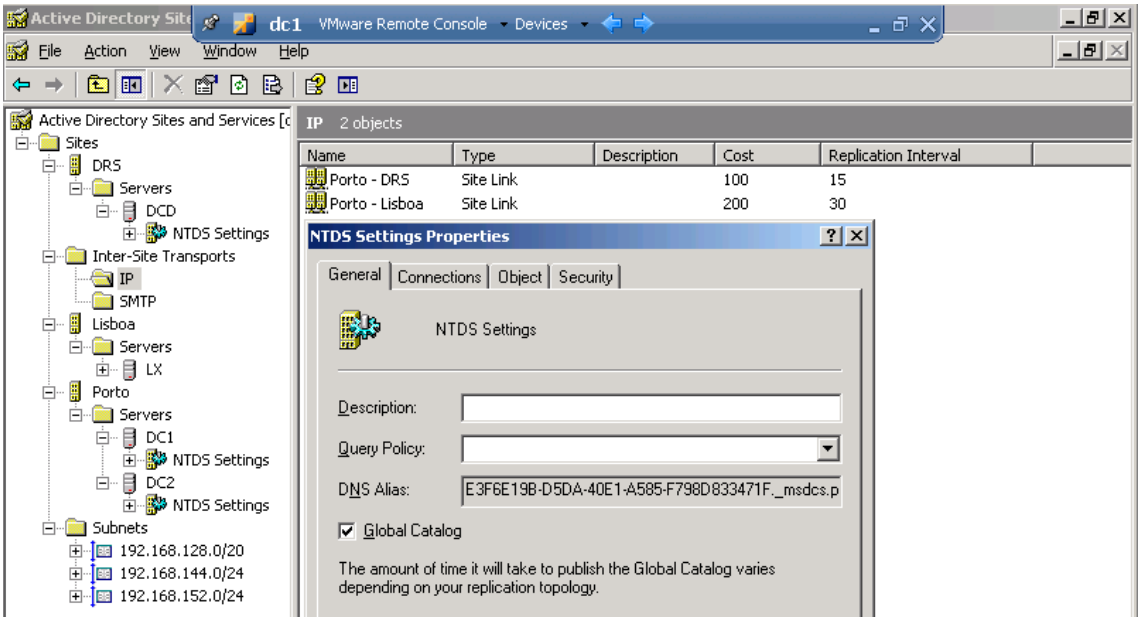


Figura 72 Parâmetros configurados na aplicação Active Directory Sites and Services

Após executar as configurações referidas, foram realizados os seguintes testes:

- Criar um novo utilizador no servidor DC1. Verificar que este utilizar é conhecido nos restantes DC passado o tempo máximo de replicação (15 minutos para DRS e 30 minutos para Lisboa);
- Desligar servidor DC1 e tentar autenticar um utilizador no Porto. Verificar se o servidor DC2 executa a validação do utilizador:
- Desligar servidor LX e tentar autenticar um utilizador em Lisboa. Verificar se o servidor DC1 ou DC2 executam a validação do utilizador;
- Formatar servidores DC1 e DC2, instalar o Sistema Operativo de novo e promovê-los a DC's novamente. Verificar se é possível fazer essa promoção através dos dados armazenados no servidor DCD.

Todos os testes foram executados e os resultados esperados foram obtidos.

4.2.2.2 Serviço de Partilha de Ficheiros

Para o teste ao serviço de Partilha de Ficheiros foi criada uma pasta partilhada, C:\Share_Z, no servidor FS. Após isso foi criado um "Replication Group", através do utilitário DFS Management, entre o servidor FS e o servidor FSD [37]. O "Replication Group" foi configurado como unidireccional ou seja, apenas será enviada informação do servidor FS para o FSD e se por engano forem feitas alterações no FSD estas não serão replicadas para o FS, apenas o contrário. Podia ter sido definido o período temporal para a replicação de modificações, o que para efeitos de teste, não foi utilizado, efectuando-se a replicação imediatamente. A figura 73 ilustra os parâmetros do "Replication Group" criado: "Disaster Recovery".

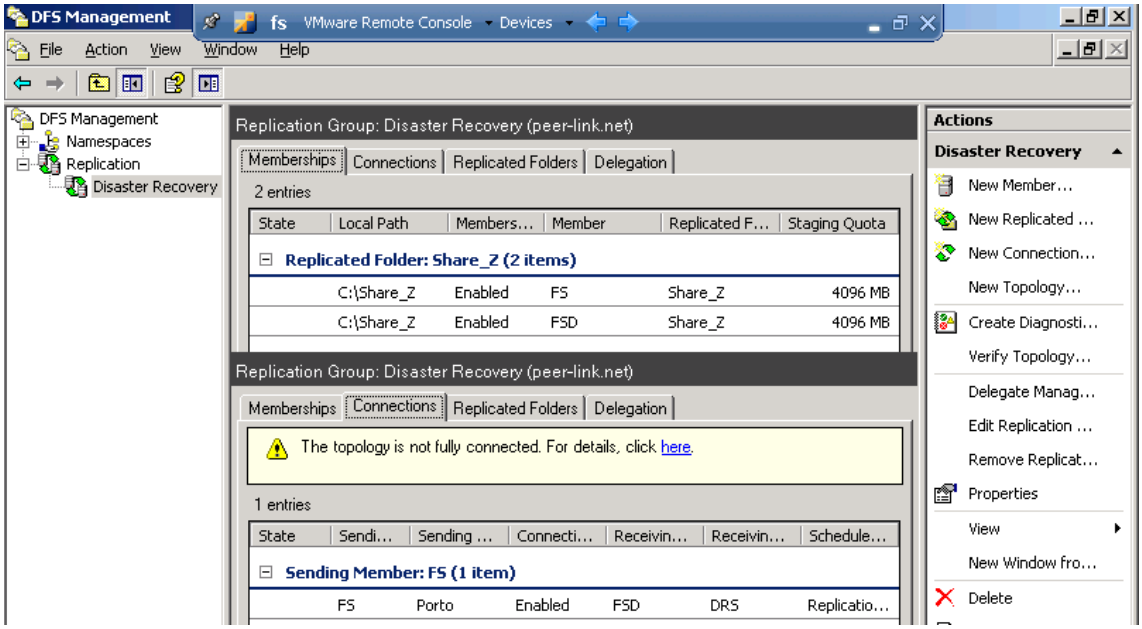


Figura 73 Parâmetros configurados no "Replication Group" denominado "Disaster Recovery"

Após a configuração do serviço DFS foram executados os seguintes testes:

- Colocar um ficheiro com extensão ".zip", com cerca de 139 MBytes, no directório c:\Share_Z do servidor FS. Verificar se o ficheiro é replicado para o servidor FSD.
- Adicionar um ficheiro de cerca de 15 MBytes ao ficheiro ".zip" existente. Verificar se o ficheiro é copiado todo novamente, correspondendo a uma transferência de aproximadamente 144 MBytes ou se é efectuada uma transferência menor.

O primeiro teste foi executado e o resultado esperado foi obtido. O segundo teste correspondeu a uma transferência bastante reduzida, menos de 15 MBytes, o que significa que este serviço replica as modificações dos ficheiros de forma bastante eficiente. A eficiência deste serviço pode ser verificada através dos relatórios de diagnóstico que podem ser criados através do utilitário DFS Management. A figura 74 apresenta sumariamente o relatório criado após a execução do 2º teste. O relatório permite verificar que apenas foram transferidos um total de 139.43 MBytes que correspondem à cópia inicial do ficheiro ".zip" de 139 MBytes para o FSD e à sua actualização, acrescentando-lhe um ficheiro de 15 MBytes.

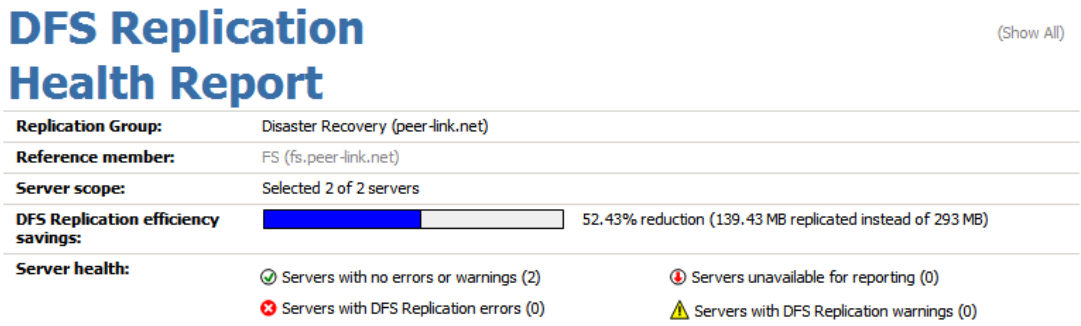


Figura 74 Exemplo de um relatório de diagnóstico criado pela ferramenta DFS Management

4.2.2.3 Serviço de E-mail: Postfix + Exchange

Para testar o serviço de e-mail, com uma arquitectura idêntica aquela proposta na fase de Desenho, foram executados os seguintes passos:

1. Configurar o serviço Postfix no servidor TUX.
    a. Ficheiro /etc/postfix/main.cf [47][48]:

```
myhostname = tux.peer-link.net
mydestination = peer-link.net
# Redes em que o Postfix confia. Ele próprio e o Exchange
mynetworks = 127.0.0.0/8, 192.168.129.11
# Ficheiro com nome dos domínios para o qual se fará relay de e-mails
relay_domains = hash:/etc/postfix/relay_domains
# Para cada domínio com relay activo indica o servidor SMTP de destino
transport_maps = hash:/etc/postfix/transport
# Função para ocultar o caminho que as mensagens percorrem internamente
header_checks = regexp:/etc/postfix/header_checks
```

    b. Ficheiro /etc/postfix/relay_domains

```
peer-link.net    OK
```

    c. Ficheiro /etc/postfix/transport

```
peer-link.net    smtp:[192.168.129.11]
```

2. Configurar o Microsoft Exchange 2007 SP1 no servidor EXCHANGE [49]:
    a. Instalar Exchange com as seguintes funções: Mailbox, Client Access, Hub Transport.
    b. Criar um "Receive Connector", que apenas permite a recepção de e-mails vindos do servidor TUX (192.168.129.3). Ver figura 75.
    c. Criar um "Send Connector", que configura o Exchange para enviar os e-mails através do servidor TUX (192.168.129.3). Ver figura 76.
    d. Criar um "Storage Group" chamado PEERLINK, com uma "Mailbox Database" chamada Mailbox. Ver figura 77.
3. Configurar o Microsoft Exchange 2007 SP1 no servidor EXCHANGED [49]:
    a. Instalar Exchange com as seguintes funções: Mailbox, Client Access, Hub Transport.

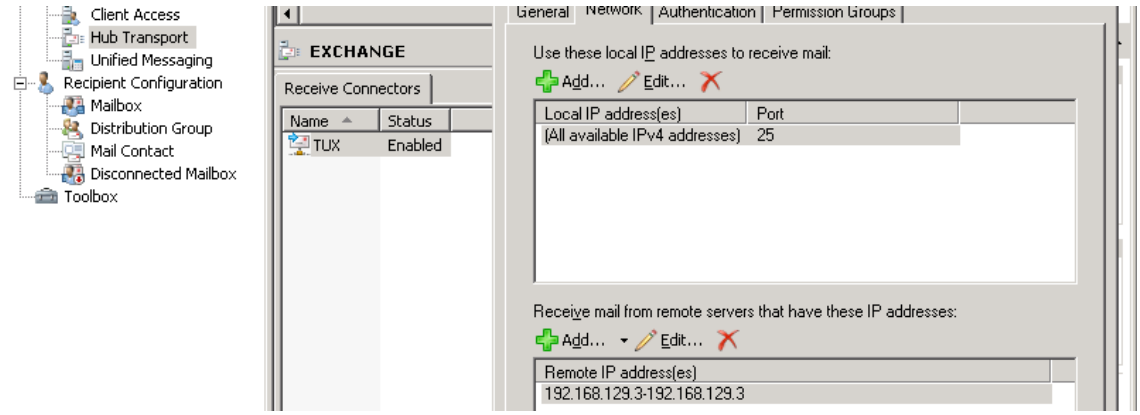


Figura 75 Configuração do Receive Connector no Exchange para o servidor TUX

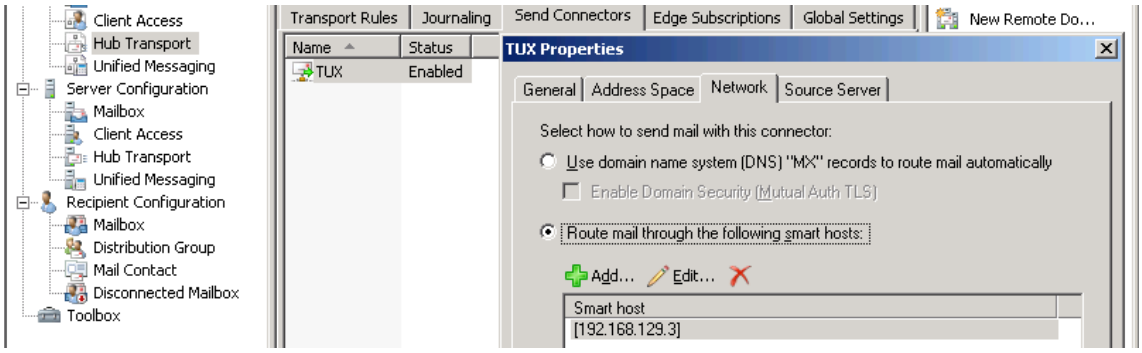


Figura 76 Configuração do Send Connector no Exchange para o servidor TUX

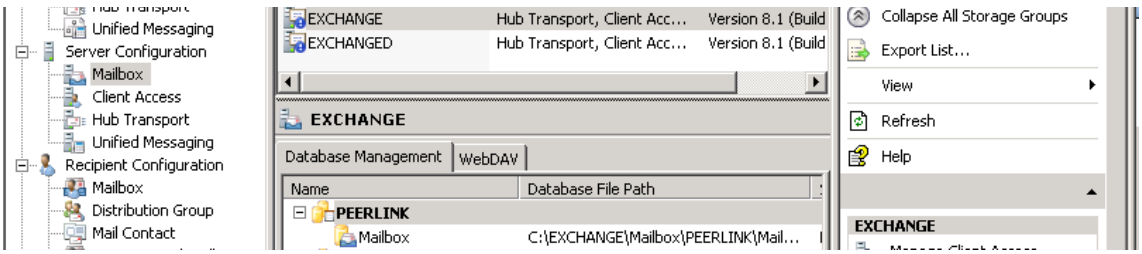


Figura 77 Storage Group "PEERLINK" com Mailbox Database "Mailbox"

4. Activar funcionalidade SCR [50]:
    a. Executar o comando de activação na Exchange Management Shell do servidor EXCHANGE:

```
enable-storagegroupcopy -identity peerlink -replaylagtime 0.0:5:0 -truncationlagtime 1.0:0:0 -standbymachine exchanged
```

    b. Verificar se o SummaryCopyStatus se encontra em estado Healthy, com o comando:

```
get-storagegroupcopystatus -standbymachine exchanged
```

Para verificar o correcto funcionamento do serviço de e-mail, foram executados os seguintes testes:

- Envio de um e-mail para a conta mclaren@peer-link.net. Verificar os LOGS no servidor TUX e verificar o caminho percorrido pela mensagem quando chega à caixa de correiro do utilizador mclaren.
    - Mensagens de LOG registadas no servidor TUX:

```
Jun  4 11:02:43 tux postfix/smtpd[5805]: connect from unknown[94.23.43.221]
Jun  4 11:02:43 tux postfix/smtpd[5805]: 956029EA03: client=unknown[94.23.43.221]
```

```
Jun  4 11:02:43 tux postfix/cleanup[5809]: 956029EA03: message-
id=<4A279BBA.9070506@fe.up.pt>
Jun  4 11:02:43 tux postfix/qmgr[5636]: 956029EA03: from=<maia.luis@fe.up.pt>,
size=1337, nrcpt=1 (queue active)
Jun  4 11:02:43 tux postfix/smtpd[5805]: disconnect from unknown[94.23.43.221]
Jun  4 11:02:43 tux postfix/smtp[5810]: 956029EA03: to=<mclaren@peer-link.net>,
relay=192.168.129.11[192.168.129.11]:25, delay=0.25, delays=0.09/0.01/0.01/0.14,
dsn=2.6.0, status=sent (250 2.6.0 <4A279BBA.9070506@fe.up.pt> Queued mail for delivery)
Jun  4 11:02:43 tux postfix/qmgr[5636]: 956029EA03: removed
```

- Caminho percorrido pela mensagem:

```
Received: from tux.peer-link.net (192.168.129.3) by exchange.peer-link.net
(192.168.129.11) with Microsoft SMTP Server id 8.1.240.5; Thu, 4 Jun 2009 11:02:33 +0100
Received: from email.peer-link.net (unknown [94.23.43.221]) by
 tux.peer-link.net (Postfix) with ESMTP id 956029EA03       for
 <mclaren@peer-link.net>; Thu,  4 Jun 2009 11:02:43 +0100 (WEST)
Received: from smtp.fe.up.pt (smtp.fe.up.pt [193.136.28.30])       by
 email.peer-link.net (Postfix) with ESMTP id 7AEC6124082    for
 <mclaren@peer-link.net>; Thu,  4 Jun 2009 11:19:56 +0100 (WEST)
```

- Envio de um e-mail a partir da conta mclaren@peer-link.net. Verificar os LOGS no servidor TUX e verificar caminho percorrido pela mensagem quando chega ao destino.
  - Mensagens de LOG registadas no servidor TUX:

```
Jun  4 11:09:12 tux postfix/smtpd[5814]: connect from unknown[192.168.129.11]
Jun  4 11:09:12 tux postfix/smtpd[5814]: 268A39EA03: client=unknown[192.168.129.11]
Jun  4 11:09:12 tux postfix/cleanup[5817]: 268A39EA03: message-
id=<A79079C08BE6F04EB965D18CBD4B20230240814F@exchange.peer-link.net>
Jun  4 11:09:12 tux postfix/qmgr[5636]: 268A39EA03: from=<mclaren@peer-link.net>,
size=883, nrcpt=1 (queue active)
Jun  4 11:09:12 tux postfix/smtpd[5814]: disconnect from unknown[192.168.129.11]
Jun  4 11:09:13 tux postfix/smtp[5818]: 268A39EA03: to=<maia.luis@fe.up.pt>,
relay=relay1.fe.up.pt[193.136.28.33]:25, delay=1, delays=0.05/0.01/0.84/0.11, dsn=2.0.0,
status=sent (250 2.0.0 Ok: queued as A25B224940DA)
Jun  4 11:09:13 tux postfix/qmgr[5636]: 268A39EA03: removed
```

  - Caminho percorrido pela mensagem. Como se pode observar o caminho percorrido entre o servidor EXCHANGE e o servidor TUX é ocultado.

```
Received: from mx2.fe.up.pt ([127.0.0.1])
        by localhost (mx2.fe.up.pt [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id ymh4uWDBAooj for <maia.luis@fe.up.pt>;
        Thu,  4 Jun 2009 10:55:05 +0100 (WEST)
Received: from tux.peer-link.net (51-238.dial.nortenet.pt [212.13.51.238])
        by mx2.fe.up.pt (Postfix) with ESMTP id A25B224940DA
        for <maia.luis@fe.up.pt>; Thu,  4 Jun 2009 10:55:05 +0100 (WEST)
```

- Desligar servidores EXCHANGE, DC1 e DC2. Recuperar a caixa de correio dos utilizadores no servidor EXCHANGED.

  Foram executados os seguintes comandos na Exchange Management Shell do servidor EXCHANGED [50]:

```
# Cria Storage Group "Recover" à qual ficarão associados os utilizadores
new-StorageGroup -Server EXCHANGED -Name Recover -LogFolderPath
'C:\EXCHANGE\Mailbox\Recover\logs' -SystemFolderPath 'C:\EXCHANGE\Mailbox\Recover\data'
# Cria uma Mailbox Database dentro da Storage Group "Recover"
new-mailboxdatabase -StorageGroup 'EXCHANGED\Recover' -Name 'RecoverMailbox' -
EdbFilePath 'C:\EXCHANGE\Mailbox\Recover\data\RecoverMailbox.edb'
mount-database -Identity Recover\RecoverMailbox
dismount-database -Identity Recover\RecoverMailbox
# Inicia o processo de activação da funcionalidade SCR
restore-storagegroupcopy exchange\peerlink -standbymachine exchanged –force
# Verificar o Estado da base de dados
eseutil /MH c:\exchange\mailbox\peerlink\mailbox.edb
```

```
# Se base de dados estiver no estado Dirty Shutdown executar os 2 comandos seguintes
eseutil /R E00 /l c:\exchange\mailbox\peerlink /S c:\exchange\mailbox\peerlink
eseutil /R E00 /l c:\exchange\mailbox\peerlink /S c:\exchange\mailbox\peerlink /a
# Move conteúdo dos LOGS enviados pela funcionalidade SCR para a Storage Group "Recover"
move-storagegrouppath exchanged\Recover -systemfolderpath c:\exchange\mailbox\peerlink -
logfolderpath c:\exchange\mailbox\peerlink –ConfigurationOnly
move-databasepath exchanged\Recover\RecoverMailbox -edbfilepath
c:\exchange\mailbox\peerlink\MAILBOX.edb –configurationonly
set-mailboxdatabase exchanged\recover\recovermailbox -allowfilerestore:$true
# Activa nova Mailbox Database
mount-database exchanged\recover\recovermailbox
# Altera a localização caixa de correio dos utilizadores
get-mailbox -database exchange\peerlink\mailbox | where {$_.ObjectClass -NotMatch
'(SystemAttendantMailboxExOleDbSystemMailbox)'} | Move-mailbox -configurationonly -
targetdatabase exchanged\recover\recovermailbox
```

Após a execução dos passos apresentados foi possível aceder à conta de correio do utilizador mclaren através do servidor EXCHANGED sem perca de mensagens. Assim, os testes apresentados nesta secção permitem validar o correcto comportamento do serviço de e-mail assim como o seu funcionamento de acordo com a arquitectura desenhada.

4.2.3 Conclusões

Os resultados da simulação parcial da infra-estrutura proposta na fase de desenho revelaram que, o que foi desenhado teórica e logicamente apresenta o comportamento esperado quando aplicado na prática.

A infra-estrutura de interligação dos sites, constituída através de túneis GRE com mecanismos criptográficos baseados na suite de protocolos IPSEC, revelou-se funcional, permitindo a ligação entre os vários sites de forma segura, mesmo quando os dados viajam numa rede pública como a Internet. O protocolo OSPF funcionou também de forma estável sobre esta arquitectura, permitindo gerir dinamicamente o encaminhamento do tráfego entre as diferentes redes dos diversos sites.

Os testes efectuados aos serviços abrangidos nesta simulação apresentaram resultados positivos. O serviço de autenticação dos utilizadores, configurado logicamente para suportar os 3 sites que constituem a infra-estrutura, Porto, Lisboa e DRS funcionou correctamente, sendo possível controlar a frequência da replicação de informação entre sites e fazer com que cada site funcione de forma autónoma em caso de falha da ligação à restante infra-estrutura. Em caso de desastre será possível recuperar toda a informação com base no servidor DCD. O serviço de partilha de ficheiros revelou-se eficaz, optimizando bastante a transferência de informação entre servidores para garantir a redundância dos dados no Porto e no DRS. O serviço de e-mail comportou-se conforme previsto, garantindo a segurança do servidor onde são armazenadas as caixas de correio dos utilizadores e resistindo ao desaparecimento do servidor do Porto, através da configuração do serviço SCR que mantém no DRS uma cópia das caixas de correio dos utilizadores, que foi activada com êxito nos testes executados.

Finalmente é importante referir o relevo das ferramentas de virtualização de Sistemas Operativos (Vmware) e de emulação de *Routers* Cisco (Dynamips) que permitiram, sem investir em vários *Routers* e Servidores, simular uma grande parte da infra-estrutura proposta possibilitando a execução de diversos testes de forma a validar a arquitectura e prever eventuais problemas que possam surgir na fase de implementação.

Capítulo 5

Implementação

Neste capítulo são descritas as actividades já efectuadas para a implementação da solução proposta, assim como previstas as actividades a executar para concluir a implementação. A contratação a um ISP dos serviços que permitirão estabelecer a interligação entre os vários sites, colocar em funcionamento o serviço de e-mail e aceder à Internet, constituiu a primeira actividade a realizar na fase de implementação. Por isso, serão aqui apresentados os requisitos mínimos para os serviços a contratar e de seguida analisadas tecnicamente as várias propostas recebidas. No final é apresentado um plano sucinto das actividades a realizar para a implementação da solução proposta.

5.1 Concurso e Avaliação das Propostas

Para seleccionar o ISP a contratar para o fornecimento dos serviços dos circuitos de interligação e acesso à Internet foi preparado e lançado um concurso a vários ISP's. Assim, para esse concurso foram definidos os requisitos mínimos dos serviços a contratar e após o concurso, foram avaliadas e classificadas as várias propostas recebidas, com o objectivo de seleccionar a melhor tendo em vista as necessidades do IGC.

5.1.1 Requisitos mínimos para os serviços a contratar a ISP

Com base no estudo executado nas fases anteriores e tendo em conta a primeira análise de mercado efectuada face ao orçamento disponibilizado pelo IGC foram definidos os requisitos mínimos para os serviços a contratar a um ISP que são apresentados de seguida:

Acesso Internet Porto:

- Circuito Ethernet, dedicado e simétrico
- Velocidade: 10 Mbit/s
- Disponibilidade: 99,8%
- Nº endereços IP públicos: 4 endereços da mesma rede

Acesso Internet Lisboa:

- Circuito assimétrico
- Taxa de contenção mínima: 1:10
- Velocidade *downstream*: 10 Mbit/s
- Velocidade *upstream*: 1 Mbit/s
- Endereço IP fixo
- Disponibilidade: 99,5%

Serviço de E-mail *Relay*:

- Reencaminhamento de todas as mensagens destinadas ao domínio "igc.pt" para um servidor do IGC
- Armazenamento temporário das mensagens até serem entregues ao servidor do IGC
- Filtragem automática das mensagens recebidas através de sistemas de anti-vírus e anti-spam

Serviço de *Housing*:

- Espaço para 3 U's a serem ocupados por 2 equipamentos: 1 *router* e 1 servidor
- Pontos de fornecimento de alimentação: 3
- Circuito Ethernet, dedicado e simétrico de acesso à Internet
- Velocidade de acesso: 10 Mbit/s
- Disponibilidade: 99,8%

Serviço de alojamento e administração do domínio "igc.pt"

Como critérios preferenciais de adjudicação valoriza-se:

- Valorização técnica da proposta
- Menor custo de exploração
- Prazo de instalação após a adjudicação

5.1.2 Avaliação técnica das propostas apresentadas pelos ISP's

O IGC convidou 5 entidades a apresentar propostas, que por motivos de confidencialidade serão aqui denominadas por: ISP1, ISP2, ISP3, ISP4, ISP5. Todas as entidades aceitaram responder ao convite e apresentaram propostas, que são descritas sumariamente a seguir.

ISP1

A proposta apresentada pelo ISP1 destaca-se por não cumprir o requisito mínimo de uma taxa de contenção mínima de 1:10, no circuito de acesso à Internet em Lisboa. Para este circuito de acesso o ISP1 propõe uma taxa de contenção 1:20, razão suficiente para a sua exclusão.

ISP2

A proposta apresentada pelo ISP2 destaca-se pelo facto de prever a ligação à Internet dos vários sites (Porto, Lisboa e DR) com circuitos dedicados e simétricos, assentes na sua

infra-estrutura de fibra óptica, de 10 Mbit/s e com a maior disponibilidade garantida apresentada pelas várias propostas, 99,99%.

- **Serviço de e-mail *Relay***

  Relativamente ao serviço de e-mail *relay* é importante referir os limites impostos para o funcionamento:

  - Tempo máximo de armazenamento das mensagens: 7 dias
  - Tamanho máximo de cada mensagem: 42 MB
  - Número máximo de caixas do correio: 50

  Relativamente ao tempo máximo em que as mensagens serão armazenadas é referido que em situações especiais (por exemplo, no caso de uma grande quantidade de SPAM ser endereçado ao cliente) não é garantido que todos os e-mails do cliente possam ser armazenados por esse período de tempo. Tais restrições não parecem fazer sentido, dado ser um requisito a filtragem automática das mensagens recebidas através de sistemas de anti-vírus e anti-spam.

  Outro ponto que não é claro na proposta é a limitação de 50 caixas do correio. Embora não estejam previstas tantas caixas do correio no domínio 'igc.pt' tal é irrelevante pois estas não vão ser alojadas no servidor do fornecedor do serviço. Apenas se pretende contratar o *relaying* e a filtragem do e-mail.

- **Circuitos de Acesso**

  Relativamente aos circuitos de acesso à Internet, é proposto para o acesso de Lisboa um circuito simétrico de 10 Mbit/s, o que valoriza localmente a capacidade de *upload*. No entanto, tendo em consideração os serviços previstos a disponibilizar, o aumento da qualidade da infra-estrutura não será perceptível do ponto de vista dos utilizadores locais, mas beneficiará significativamente o serviço de *backup* de Lisboa para o Porto. Um acesso em Lisboa com estas características permite considerar a implementação futura entre os dois escritórios de novos serviços exigentes no tráfego de *download* e *upload*, tal como alguns serviços multimédia.

ISP3

A proposta do ISP3 satisfaz os requisitos mínimos e destaca-se pela ligação proposta para o escritório de Lisboa.

- **Serviço de e-mail *Relay***

  Relativamente ao serviço de e-mail *relay* é importante referir o limite imposto no tempo máximo em que as mensagens são armazenadas, 7 dias. Quanto às restantes funcionalidades de filtragem automática das mensagens recebidas através de sistemas de anti-vírus e anti-spam, a proposta do ISP3 satisfaz completamente os requisitos.

- **Circuitos de Acesso**

  A proposta do ISP3 prevê para o acesso em Lisboa um circuito ADSL a 16/2 Mbit/s, com uma taxa de contenção de 1:10. Estas características poderão permitir, em função da contenção, uma boa capacidade de *download*, o que no ponto de vista dos utilizadores se traduz num melhor acesso à Internet. Também dependendo da contenção, a capacidade de *upload* poderá ser relevante ao permitir aumentar a quantidade de dados enviados no sentido Lisboa para o Porto, reduzindo assim o tempo de transferência da informação dos *backups*.

ISP4

A proposta apresentada pelo ISP4 destaca-se pelo facto de ligar os vários sites (Porto, Lisboa e DR) à Internet a 10 Mbit/s com ligações dedicadas e simétricas, em Ethernet e interfaces de acesso com capacidade de 100 Mbit/s, com disponibilidade de 99,8% para Porto e Lisboa, e 99,9% para o DRS.

- **Serviço de e-mail *Relay***

  Relativamente ao serviço de e-mail *relay* e comparando com as restantes propostas esta é a que apresenta maiores limitações. Assim,

  - Tempo máximo de armazenamento das mensagens: 4 dias
  - Tamanho máximo de cada mensagem: 20 MB
  - Número máximo de destinatários: 100

Analisando, por exemplo, o tempo máximo de armazenamento das mensagens verifica-se que apesar de não ser explícito nos requisitos mínimos é realista considerar cenários muito excepcionais em que o servidor do IGC esteja indisponível mais do que 4 dias. Embora sejam cenários improváveis, a aceitação à partida desta limitação implica admitir a eventual perda de e-mail. Quanto à limitação do tamanho das mensagens, considerando o tamanho médio actual de um documento ou conjunto de documentos em arquivo é muito provável ultrapassar o limite de 20 MB, pelo que esta limitação é um factor negativo. Também não parece ser aceitável a limitação do número de destinatários de uma mensagem, principalmente por que esta limitação afecta a recepção de mensagens de eventuais remetentes não conhecedores da restrição.

- **Circuitos de Acesso**

  Relativamente aos circuitos de acesso à Internet, a proposta de circuitos simétricos em Ethernet a 10 Mbit/s, configura uma boa solução perante as necessidades identificadas, sendo que no escritório de Lisboa valoriza a capacidade de *upload*. Tendo em consideração os serviços previstos a disponibilizar, o aumento da qualidade da infra-estrutura não será francamente perceptível do ponto de vista dos utilizadores em Lisboa, mas beneficiará significativamente o serviço de *backup* de Lisboa para o Porto e o acesso interactivo a ficheiros.

  Uma infra-estrutura de comunicações com estas características permite ao IGC considerar a implementação futura entre os dois escritórios de novos serviços exigentes no tráfego de *download*/*upload* e atraso, tal como por exemplo o serviço de vídeo-conferência.

ISP5

A proposta ISP5 inclui uma proposta base e seis propostas variantes. Tanto a proposta base assim como as variantes caracterizam-se por satisfazer todos os requisitos mínimos. Pela qualidade de serviço intrínseca da tecnologia, é um factor importante de valorização das várias propostas a 10 Mbit/s, 20 Mbit/s e 50 Mbit/s, a oferta de circuitos dedicados em fibra óptica, simétricos e entregues em Ethernet.

Todas as propostas do ISP5 são avaliadas, por serem tecnicamente válidas, embora pareça ser dimensionado por excesso circuitos de acesso a 50 Mbit/s tendo em consideração o número de sistemas, utilizadores e aplicações planeados para a rede do IGC.

- **Serviço de e-mail *Relay***

É importante referir que o serviço de e-mail *relay* proposto pelo ISP5, que é comum a todas as suas variantes, apresenta as melhores características uma vez que:

- Armazena as mensagens por um tempo a definir pelo IGC
- Não impõe qualquer limite sobre o tamanho máximo das mensagens
- Relativamente às mensagens filtradas possibilita a sua cópia para uma pasta especial para uma análise posterior

É, portanto, a melhor solução para o serviço de e-mail *relay*.

- **Circuitos de Acesso**

  A proposta base é valorizada pela velocidade de *download* e taxa de contenção garantida no circuito de acesso à Internet em Lisboa, 16 Mbit/s e 1:1, assim como pela disponibilidade garantida no circuito de acesso no Porto, 99,9%. Em contrapartida apenas propõe oferecer a 99,8% de disponibilidade no circuito de ligação à Internet do DRS. As propostas variantes apresentam do ponto de vista técnico e da qualidade de serviço que permite disponibilizar aos utilizadores do IGC, uma valorização considerável. Essa valorização é muito acentuada nas variantes com circuitos dedicados de 20 Mbit/s e 50 Mbit/s quer no Porto quer no DRS.

  Os aspectos importantes de valorização são os seguintes:

  - Maior velocidade de acesso à Internet para os utilizadores do Porto;
  - Maior velocidade de acesso remoto aos serviços localizados no escritório do Porto, quer para os utilizadores do escritório de Lisboa quer através de VPN;
  - Disponibilização de capacidade e qualidade de serviço excepcional para serviços interactivos;
  - Possibilidade do aumento do volume de dados a ser enviado para o DRS.

5.1.2.1 Ordenação das Propostas

Neste capítulo será apresentada uma ordenação das propostas consideradas, tendo em conta os parâmetros apresentados na tabela 11, perante os requisitos identificados para o IGC na fase de Preparação e Planeamento.

Tabela 11 Resumo dos parâmetros técnicos das propostas apresentadas pelos ISP's

	Ligação Porto		**Ligação Lisboa**				**E-mail *Relay***	***Housing***	
	Velocidade (Mbit/s)	Disponibilidade (%)	*Download* (Mbit/s)	*Upload* (Mbit/s)	Contenção (Rácio)	Disponibilidade (%)	Armazenamento (Dias)	Velocidade (Mbit/s)	Disponibilidade (%)
ISP1	10	99,8	12	1	0,05	99,5	7	20	99,99
ISP2	10	99,99	10	10	1	99,99	7	10	99,99
ISP3	10	99,8	16	2	0,1	99,5	7	10	99,8
ISP4	10	99,8	10	10	1	99,8	4	10	99,9
ISP5	10	99,9	16	1	1	99,5	Personalizável	10	99,8
ISP5(21)	20	99,9	24	1	1	99,5	Personalizável	10	99,8
ISP5(12)	10	99,9	24	1	1	99,5	Personalizável	20	99,8
ISP5(2)	20	99,9	24	1	1	99,5	Personalizável	20	99,8
ISP5(51)	50	99,9	24	1	1	99,5	Personalizável	10	99,8
ISP5(15)	10	99,9	24	1	1	99,5	Personalizável	50	99,8
ISP5(5)	50	99,9	24	1	1	99,5	Personalizável	50	99,8

É apresentado na tabela 12 a ordenação das propostas avaliando apenas as suas características técnicas. A cada proposta está associada uma apreciação numa escala normalizada de 0 a 10. A apreciação atribuída a cada proposta baseia-se num Sistema de Apoio à Decisão construído para o efeito e que pesa as características dos vários serviços a contratar pela seguinte ordem (1 = Maior Peso; 4 Menor Peso):

1. Ligação Porto
2. Ligação Lisboa
3. Ligação DR
4. E-Mail *Relay*

Tabela 12 Ordenação e apreciação das propostas

Proposta	**Apreciação (0 – 10)**
ISP5 (2)	10,00
ISP5	7,55
ISP5 (21)	7,38
ISP2	6,72
ISP5 (5)	6,66
ISP5 (12)	6,00
ISP3	5,31
ISP4	4,31
ISP5 (51)	1,38
ISP5 (15)	0,00

O sistema construído para a apreciação técnica das propostas teve em especial consideração os seguintes aspectos:

- Relação da velocidade da ligação no Porto com a do escritório de Lisboa e com a velocidade no DRS pelo facto de, um aumento de velocidade no Porto, dever ser mais valorizado quando os restantes sites possuem ligações que aproveitem o débito disponibilizado no site principal (Porto);
- Dimensionamento dos serviços propostos tendo em conta os requisitos e dimensão do IGC.

5.1.2.2 Conclusões

Pela ordenação apresentada a proposta que se destaca e se conclui ser a melhor, tendo em conta as suas características técnicas e adaptação à dimensão do IGC, é a variante (2) do ISP5. Esta proposta apresenta as seguintes vantagens:

- Maior velocidade de acesso à Internet para os utilizadores do Porto (acesso até 20 vezes mais rápido que o actual);
- Possibilidade do aumento do volume de dados a ser enviado para o DRS. Por exemplo, será possível enviar aproximadamente 60 GB de informação para o DRS numa janela temporal de 8 horas;
- Maior velocidade de acesso remoto aos serviços localizados no escritório do Porto, quer para os utilizadores do escritório de Lisboa quer através de VPN. Por exemplo, a possibilidade de descarregar um ficheiro de 20 MB a partir do escritório de Lisboa em apenas, aproximadamente, 10 segundos;

- Em caso de desastre aceder aos serviços críticos de forma mais rápida por parte dos utilizadores;
- Grande capacidade para utilizar o circuito do Porto para serviços multimédia, por exemplo voz e vídeo;
- Serviço de e-mail *relay* sem limitações e parametrizável pelo IGC.

Por último, há um aspecto que poderá ser importante dependendo do contrato de fidelização que for assinado, pois geralmente os proponentes excluem os custos de instalação no caso de ser contratada uma fidelização de dois ou mais anos. É reconhecido pela evolução tecnológica dos últimos anos que as necessidades de largura de banda de acesso ao exterior de uma rede vão aumentando anualmente [51]. Portanto, os requisitos de hoje muito provavelmente serão insuficientes no prazo de um ano ou dois anos.

5.2 Plano de Tarefas

Nesta secção são apresentadas, de forma bastante sucinta, as tarefas identificadas para a implementação da infra-estrutura proposta e para aquelas que se encontrem já concluídas será apresentada alguma informação adicional relevante. De acordo com a abordagem feita nas fases anteriores, seguir-se-ão ordenadamente as camadas física, lógica, de rede e aplicacional.

Ao nível da camada física procedeu-se à instalação de um novo sistema de ar condicionado, colocação de chão com características anti-estátitcas, instalação dos equipamentos adquiridos e reorganização de toda a cablagem do Pólo Técnico do Porto. A implementação ao nível da camada física encontra-se concluída e a figura 78 ilustra o aspecto do Pólo Técnico do Porto após as alterações.

Figura 78 Pólo técnico do Porto remodelado

Ao nível lógico foram configuradas as ligações entre *switches* através de EtherChannel's, tecnologia que foi também utilizada na ligação entre os *switches* e servidores evitando assim a

utilização de protocolos que necessitem de tráfego de *broadcast* para o seu funcionamento. Foram também configuradas as diversas *VLAN*'s previstas assim como o protocolo VTP para a sua divulgação entre os vários *switches*. A implementação ao nível da camada lógica encontra-se concluída.

A nível da rede será necessário configurar os vários *routers* para o acesso à Internet. Serão configurados mecanismos de Network Address Translation (NAT) para a tradução entre endereços privados e públicos, o CBAC como forma de protecção, os túneis GRE para a comunicação entre sites e o OSPF para a troca de informações de routing. As tarefas do nível da Rede não foram ainda executadas pelo facto de os circuitos de acesso à Internet não terem sido ainda disponibilizados pelo ISP contratado.

O nível aplicacional incluirá a configuração dos novos servidores com os serviços previstos, a migração dos actuais servidores e das estações de trabalho dos colaboradores e configuração dos serviços de DR assim com a execução de testes. Das tarefas associadas ao nível aplicacional apenas foi instalado e configurado o servidor DC1. Estima-se que a duração das restantes tarefas será de cerca de 2 meses estando a sua conclusão dependente da disponibilização dos circuitos de acesso à Internet, contratados ao ISP escolhido.

5.3 Conclusões

A implementação da infra-estrutura proposta está dependente da disponibilização dos circuitos de interligação entre os vários sites. Por essa razão a escolha do ISP a contratar constitui a primeira actividade desta fase. Foram então definidos os requisitos mínimos dos serviços a contratar, contactados vários ISP's e finalmente avaliadas e comparadas as propostas recebidas.

A negociação com vários ISP's possibilitou a contratação de diversos serviços que permitirão a constituição de uma infra-estrutura com as seguintes vantagens:

- Maior velocidade de acesso à Internet para os utilizadores do Porto (20 Mbit/s);
- Possibilidade de envio de um grande volume de dados para o DRS (cerca de 60 GB de numa janela temporal de 8 horas);
- Grande velocidade de acesso remoto aos serviços localizados no escritório do Porto, quer para os utilizadores do escritório de Lisboa quer através de VPN;
- Em caso de desastre aceder aos serviços críticos de forma mais rápida por parte dos utilizadores;
- Grande capacidade para utilizar o circuito do Porto para serviços multimédia, por exemplo voz e vídeo;
- Serviço de e-mail *relay* sem limitações e parametrizável pelo IGC

Além da escolha do ISP a contratar, a implementação da infra-estrutura proposta encontra-se já concluída ao nível físico, através do melhoramento das condições físicas no Pólo técnico do Porto (instalação de chão com características anti-estáticas e novo equipamento de ar condicionado), instalação do equipamento adquirido (*Routers* e Servidores) e reorganização de toda a cablagem de interligação dos equipamentos. Ao nível lógico encontra-se já concluída a configuração dos equipamentos de nível 2 (*switches*). Para os restantes níveis, de rede e aplicacional foram previstas sumariamente as actividades a realizar.

Capítulo 6

Conclusões e Trabalho Futuro

O trabalho levado a cabo ao longo deste projecto e que se encontra aqui documentado resultou numa infra-estrutura de rede de comunicações de suporte ao negócio construída através de uma actividade lógica, reproduzível e defensável.

A solução construída poderá ser utilizada como alicerce fiável para as ferramentas e recursos informáticos de suporte ao negócio do IGC, uma vez que foi dotada de diversos mecanismos de redundância e segurança que permitem garantir a sua disponibilidade, fiabilidade e confiança. Mesmo que uma catástrofe atinja e destrua a sede do IGC, é garantida a continuidade do funcionamento dos serviços críticos, através da manutenção de sistemas redundantes, configurados com uma arquitectura *Hot Standby*, alojados em *Housing* nas instalações de um ISP, podendo por isso ser acedidos em qualquer local do mundo tendo como única exigência um acesso à Internet. A solução proposta permite também o acesso rápido a novas aplicações e serviços de suporte ao funcionamento da organização, através de uma infra-estrutura de rede escalável.

A construção de uma solução à medida do IGC teve por base uma análise profunda feita aos sistemas e serviços informáticos, o que permitiu conhecer os problemas que afectam actualmente o negócio da instituição assim como as suas necessidades específicas de funcionamento. Este conhecimento permitiu a construção fundamentada de uma nova infra-estrutura onde foram analisados diversos cenários possíveis e onde foi escolhida a melhor solução tendo em conta as necessidades e dimensão do IGC. A solução escolhida foi ainda sujeita a um processo de *Proof of Concept* onde através de ferramentas de virtualização e emulação de sistemas operativos foi possível simular parcialmente a infra-estrutura proposta validando a sua arquitectura e prevendo eventuais problemas que pudessem surgir na fase de implementação.

De seguida será então avaliada a satisfação dos objectivos propostos para este projecto e feita uma previsão do trabalho futuro associado à solução desenhada.

6.1 Satisfação dos Objectivos

Os objectivos deste projecto foram referidos na secção 1.1.4, são aqui reescritos e para cada um serão referidas as actividades principais assim como uma avaliação qualitativa da forma como foram atingidos.

- *Caracterização e identificação dos requisitos da rede, sistemas e serviços que suportam o negócio do IGC*;

  Este objectivo foi atingido com sucesso sendo o seu resultado apresentado no capítulo 3, correspondente à Abordagem ao Problema. A realização das tarefas associadas à fase de Preparação e de Planeamento permitiram, através de uma análise detalhada dos sistemas e serviços que suportam o negócio do IGC, especificar e fundamentar os requisitos da infra-estrutura a desenhar. Sem a realização deste objectivo, o desenho de uma infra-estrutura que cumprisse todos os requisitos do IGC seria uma actividade pouco ou nada fundamentada.

- *Avaliação e proposta de soluções para garantir a disponibilidade, a possibilidade da infra-estrutura de rede ser utilizada como alicerce fiável no negócio do IGC e o suporte de uma plano que garanta a continuidade do funcionamento das TI/SI críticas em caso de catástrofe na sede do IGC*;

  Este objectivo foi concluído com sucesso sendo o seu resultado apresentado no capítulo 4, correspondente ao Desenho da Solução. Neste capítulo é descrita detalhadamente a solução desenhada tendo em conta os dados recolhidos nas fases de preparação e planeamento. Para a escolha de uma solução em concreto foram analisados diversos cenários, envolvendo diversas tecnologias, com custos de implementação diversificados e características distintas. Escolhida a solução a propor para a resolução do problema do IGC, é feita uma simulação parcial, recorrendo a ferramentas de virtualização e emulação, com o objectivo de validar a sua arquitectura e prever eventuais problemas que possam surgir na fase de implementação, constituindo assim um *Proof of Concept* da solução proposta. Os testes levados a cabo permitiram concluir o funcionamento da solução desenhada de acordo com o previsto.

- *Iniciar a implementação da infra-estrutura proposta*;

  O resultado deste objectivo é apresentado no capítulo 5, correspondente à Implementação. São assim descritas as actividades efectuadas para a implementação da solução proposta, assim como previstas as actividades a executar para concluir a implementação. A contratação a um ISP dos serviços que permitirão estabelecer a interligação entre os vários sites, colocar em funcionamento o serviço de e-mail e aceder à Internet, constituíram a primeira actividade a realizar, sendo por isso apresentados os requisitos mínimos para os serviços a contratar e de seguida analisadas tecnicamente as várias propostas recebidas. A implementação da infra-estrutura apenas poderá ser concluída quando os serviços contratados forem disponibilizados. A escolha destes serviços constituirá a base de expansão de toda a infra-estrutura tendo por isso havido o cuidado de seleccionar a proposta que não constrangerá a curto e médio prazo, a expansão da infra-estrutura de rede de comunicações do IGC.

- *Criação de um caso de estudo que coloca em prática uma metodologia que acompanha o ciclo de vida de uma infra-estrutura de rede de comunicações*.

Este objectivo foi igualmente concluído com sucesso sendo o seu resultado comprovado através deste documento que pretende assim constituir uma ajuda para o desenho de infra-estruturas de rede no futuro. Neste projecto, foi seguida uma metodologia bem definida e bem documentada e ao longo das várias fases foram utilizadas diversas ferramentas, formas de análise e comparadas várias tecnologias e cenários possíveis que poderão servir de exemplo para casos futuros. Desta forma, foi possível validar que a metodologia utilizada foi uma ferramenta extremamente importante para o sucesso do projecto, uma vez que através de uma forma sistemática de análise e desenho da rede ajudou a garantir que os requisitos da organização fossem cumpridos.

6.2 Trabalho Futuro

Uma vez que neste relatório apenas são abordadas as fases de Preparação, Planeamento, Desenho e Implementação, embora esta última apenas parcialmente, fica a faltar assim a sua conclusão, que se prevê, como já foi referido, demorar cerca de 2 meses. Na restante implementação a fase mais crítica será a migração dos utilizadores e actuais servidores de produção para a nova infra-estrutura, sem causar paragens nos serviços críticos do IGC. Esta migração terá que ser feita através da criação de uma ligação entre as duas infra-estruturas que permitirá que os utilizadores da nova infra-estrutura utilizem serviços da antiga conseguindo desta forma migrar gradualmente os actuais servidores de produção.

Concluída a fase de Implementação surgem então as fases de Operação e Optimização onde o servidor dedicado à monitorização e gestão da rede, com todas as ferramentas necessárias, desempenhará um papel fundamental ajudando a controlar eventuais erros ou falhas, através da análise dos dados do servidor SYSLOG que receberá os registos de todos os equipamentos da rede e através da análise da estatística gerada. Estas ferramentas ajudarão a verificar se a infra-estrutura responde ou não as necessidades do IGC, a solidificar a sua segurança e a resolver problemas pontuais que possam surgir. A fase de optimização contemplará eventuais reestruturações da infra-estrutura de rede.

Relativamente à implementação de novos serviços estima-se que a curto prazo, perante o dimensionamento dos circuitos de acesso ao exterior, se poderão implementar serviços de Voz e Vídeo nomeadamente para reduzir custos nas ligações telefónicas e possibilitar o estabelecimento de vídeo-conferências entre os escritórios de Lisboa e Porto. A implementação destes novos serviços deverá ter em atenção os requisitos de Qualidade de Serviço (Quality of Service – QoS) do tráfego de Voz e Vídeo que necessitam de atraso (delay), variação do atraso (jitter) e perda de pacotes (packet loss) determinados.

Referências

[1] Instituto Gestor de Capital. *Relatório e Contas* 2007.

[2] James D. Mccabe. *Network Analysis, Architecture, and Design*, *3rd Edition*. Morgan Kaufmann Publishers, 2007.

[3] Diane Theare. *Authorized Self-Study Guide – Designing for Cisco Internetwork Solutions (DESGN), 2nd Edition*. Cisco Press, 2008.

[4] Wendell Odom. *CCNA Self-Study – CCNA INTRO – Exam Certification Guide*. Cisco Press, 2004.

[5] José Ruela. *Arquitecturas de Rede – Modelos Arquitectónicos*. FEUP/DEEC, 2008/2009. [Em linha; consultado em Março de 2009] http://paginas.fe.up.pt/~jruela/redes/teoricas/6_arquitect_v0809_mieec.pdf

[6] Andrew S. Tanenbaum. *Computer Networks, 4th Edition.* Pearson Education, 2003

[7] Paul Simoneau. *Expert Reference Series of White Papers– The OSI Model: Understanding the Seven Layers of Computer Networks*. Global Knowledge, 2006. [Em linha; consultado em Março de 2009] http://whitepapers.techrepublic.com.com/abstract.aspx?docid=236912

[8] Priscilla Oppenheimer. *Top-Down Network Design Second Edition*. Cisco Press, 2004

[9] Cisco Systems. *White Paper: Creating Business Value and Operational Excellence with the Cisco Systems Lifecycle Services Approach*. 2005. [Em linha; consultado em Março de 2009] http://www.cisco.com/warp/public/437/services/lifecycle/LifecycleServicesWhitePaper.pdf

[10] Gan Chee-Syong. *Introduction to Business Continuity Planning*. SANS Institute, InfoSec Reading Room, 2003. [Em linha; consultado em Março de 2009] http://www.sans.org/reading_room/whitepapers/recovery/introduction_to_business_continuity_planning_559

[11] Klaus Schmidt. *High Availability and Disaster Recovery: Concepts, Design, Implementation.* Springer, 2006

[12] Chad Bahan. *The Disaster Recovery Plan*. SANS Institute, InfoSec Reading Room, 2003. [Em linha; consultado em Março de 2009] http://www.sans.org/reading_room/whitepapers/recovery/the_disaster_recovery_plan_1164

[13] J. Nicholas Hoover. *Reader Survey: Top Networking Vendors*. Network Computing. 2006. [Em linha; consultado em Fevereiro de 2009] http://www.networkcomputing.com/showArticle.jhtml?articleID=177104916

[14] Mike Gilmore. *White Paper: Cabling Performance vs. Component Conformance*. EXCEL, Excellence in Networking, 2009. [Em linha; consultado em Maio de 2009] http://www.excelnetworking.com/case/documents/Excel_Whitepaper_CB_vs_CC.pdf

[15] Fluke Networks. *DTX Series CableAnalyzer, User Manual*. Fluke Corporation, 2004

[16] OPENXTRA. *Network Cable Testing What Causes Data Loss?* 2009 [Em linha; consultado em Abril de 2009] http://www.openxtra.co.uk/articles/network_cable_testing_causes_data_loss

[17] Cisco Systems. *White Paper: Cisco StackWise and StackWise Plus Technology*. 2006 [Em linha; consultado em Abril de 2009] http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/prod_white_paper09186a00801b096a.pdf

[18] Cisco Systems. *White Paper: Cisco EtherChannel Technology*. 2003 [Em linha; consultado em Abril de 2009] http://www.cisco.com/warp/public/cc/techno/lnty/etty/fsetch/tech/fetec_wp.pdf

[19] Howard Frazier. *IEEE 802.3ad Link Aggregation (LAG) – what it is, and what it is not*. IEEE 802.3 HSSG, 2007. [Em linha; consultado em Maio de 2009] http://www.ieee802.org/3/hssg/public/apr07/frazier_01_0407.pdf

[20] Intel. *White Paper: Intel Advanced Network Services Software*. 2004. [Em linha; consultado em Maio de 2009] http://support.dell.com/support/edocs/software/Inteladv/17092_ANS_WP_r04.pdf

[21] Broadcom. *White Paper: Broadcom NexXtreme Gigabit Ethernet Teaming*. 2003

[22] Cisco Systems. *Configuring SPAN and RSPAN*. 2008. [Em linha; consultado em Março de 2009] http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_44_se/configuration/guide/swspan.pdf

[23] NexantiS Corporation. *SecureScout - Microsoft-DS*. 2007. [Em linha; consultado em Março de 2009] http://descriptions.securescout.com/glossary/255

[24] Microsoft MSDN. *BITS Upload Protocol*. 2009 [Em linha; consultado em Março de 2009] http://msdn.microsoft.com/en-us/library/aa362828.aspx

[25] Wikipedia. *Distributed Component Object Model*. 2009. [Em linha; consultado em Março de 2009] http://en.wikipedia.org/wiki/Distributed_Component_Object_Model

[26] Kennedy Clark. *CCIE Professional Development series - Cisco LAN Switching*. Cisco Press, 1999

[27] Shon Harris. *ALL-IN-ONE: CISSP Exam Guide*. McGrawHill Osborne, 2008

[28] Cisco Systems. *Understanding VLAN Trunk Protocol (VTP)*. 2007. [Em linha; consultado em Maio de 2009] http://www.cisco.com/application/pdf/paws/10558/21.pdf

[29] Yakov Rekhter. *Internet Best Current Practices*: *Address Allocation for Private Internets*. IETF, 1996

[30] Cisco Systems. *OSPF Design Guide*. 2005 [Em linha; consultado em Maio de 2009] http://www.cisco.com/application/pdf/paws/7039/1.pdf

[31] Cisco Systems. *Configuring IP Access Lists*. 2008 [Em linha; consultado em Maio de 2009] http://www.cisco.com/application/pdf/paws/23602/confaccesslists.pdf

[32] Cisco Systems. Configuring Context-based Access Control. 2007 [Em linha; consultado em Maio de 2009] http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_content_ac.pdf

[33] William Stanek. *Microsoft Windows Server 2003 – Administrator's Pocket Consultant, 2nd Edition*. Microsoft Press, 2006

[34] Dan Shearer. *MTA Comparison.* 2007. [Em linha; consultado em Maio de 2009] http://shearer.org/MTA_Comparison

[35] Microsoft Technet. *Standby Continuous Replication*. 2008 [Em linha; consultado em Maio de 2009] http://technet.microsoft.com/en-us/library/bb676502.aspx

[36] Vmware. *White Paper: Why choose Vmware*. Vmware, 2008

[37] Microsoft Technet. *Overview of the Distributed File System Solution in Microsoft Windows Server 2003 R2.* 2005 [Em linha; consultado em Maio de 2009] http://technet.microsoft.com/en-us/library/cc787066(WS.10).aspx

[38] Ashish Ray. *Oracle Data Guard – Disaster Recovery for Enterprise*. Oracle Corporation, 2003

[39] Microsoft Techhnet. *Log Shipping in SQL Server 2000 - Part 1*. 2002 [Em linha; consultado em Maio de 2009] http://technet.microsoft.com/en-us/library/cc966381.aspx

[40] Yu Gu. *GRE Encapsulated Multicast Probing: A Scalable Technique for Measuring One-Way Loss*. IEEE Communications Society, 2008

[41] John Moy. *RFC2328 - OSPF Version 2*. The Internet Society, 1998.

[42] C. Sanchez-Avila. The *Rijndael Block Cipher (AES Proposal): A Comparison with DES*. IEEE, 2001

[43] Mark Lewis. *Comparing, Designing, and Deploying VPNs*. Cisco Press, 2006

[44] Xipeng Xiao. *Internet QoS: A Big Picture.* IEEE, 1999. [Em linha, consultado em Maio de 2009] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.28.1487&rep=rep1&type=pdf

[45] Bruce Davie. *MPLS: Multiprotocol Label Switching Technology and Applications*. Morgan Kaufmann Publishers, 2000

[46] Cisco Systems. *Point-to-Point GRE over IPSec Design Guide*. 2006. [Em linha; consultado em Maio de 2009] http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008073a0c5.pdf

[47] Postfix. *Postfix Basic Configuration*. 2009. [Em linha; consultado em Maio de 2009] http://www.postfix.org/BASIC_CONFIGURATION_README.html

[48] nixCraft. *Postfix Hide Client (MUA) System IP Address / Hostname*. 2009. [Em linha; consultado em Maio de 2009] http://www.cyberciti.biz/faq/postfix-remove-hide-hostnames-ip-addresses/

[49] Tony Redmond. *Microsoft Exchange Server 2007 with SP1 - Tony Redmond's Guide to Successful Implementation*. SYNGRESS, 2008

[50] Exchange-Genie. Standby Continuous Replication (SCR). 2007. [Em linha; consultado em Maio de 2009] http://www.exchange-genie.com/2007/08/standby-continuous-replication-scr/

[51] ANACOM. *Informação Estatística do Serviço de Acesso à Internet - 1º Trimestre de 2009*. 2009. [Em linha; consultado em Junho de 2009] http://www.anacom.pt/render.jsp?contentId=952048

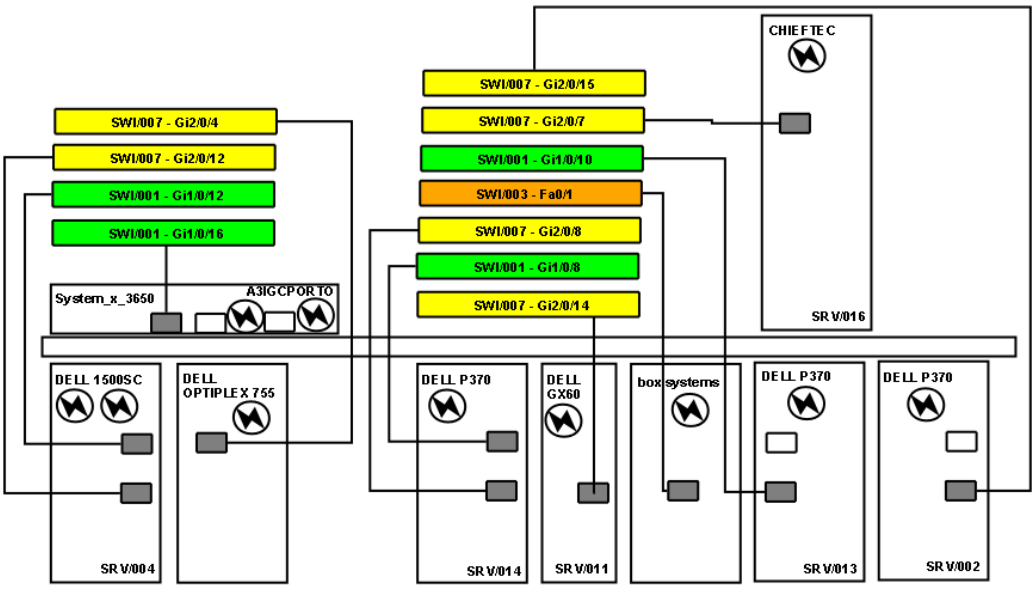
Anexo A

Estatísticas de tráfego na Rede

Este anexo contém as estatísticas recolhidas da quantidade de tráfego na rede do IGC.

A.1 Porto

Em cada gráfico de tráfego de rede apresentado, é indicado a que servidor se refere através da inserção da sua imagem correspondente a uma das duas figuras apresentadas de seguida, que representam o esquema como estão dispostos fisicamente no pólo técnico do Porto.

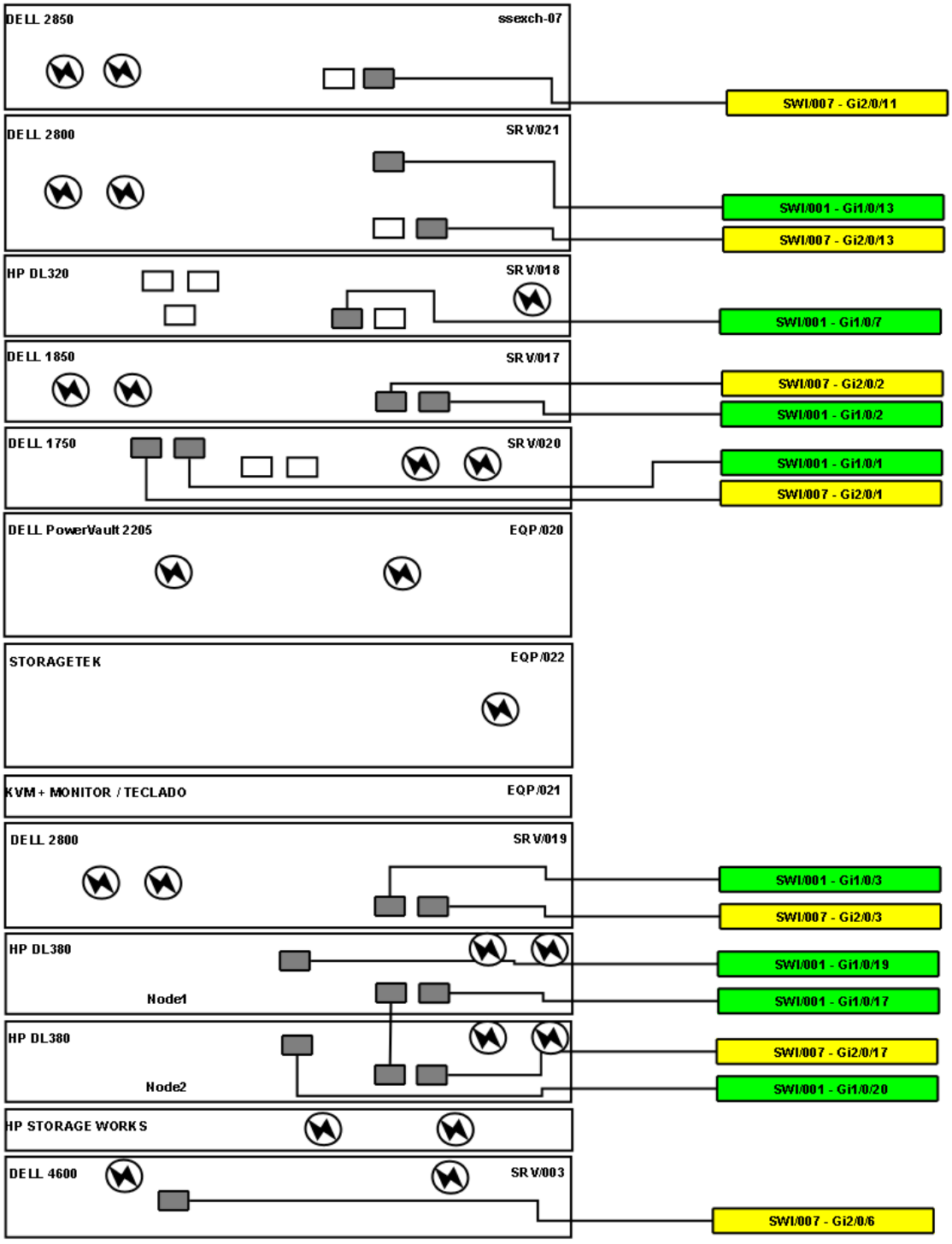


Legenda:

Ligação eléctrica

Ligação de rede não utilizada

Ligação de rede utilizada



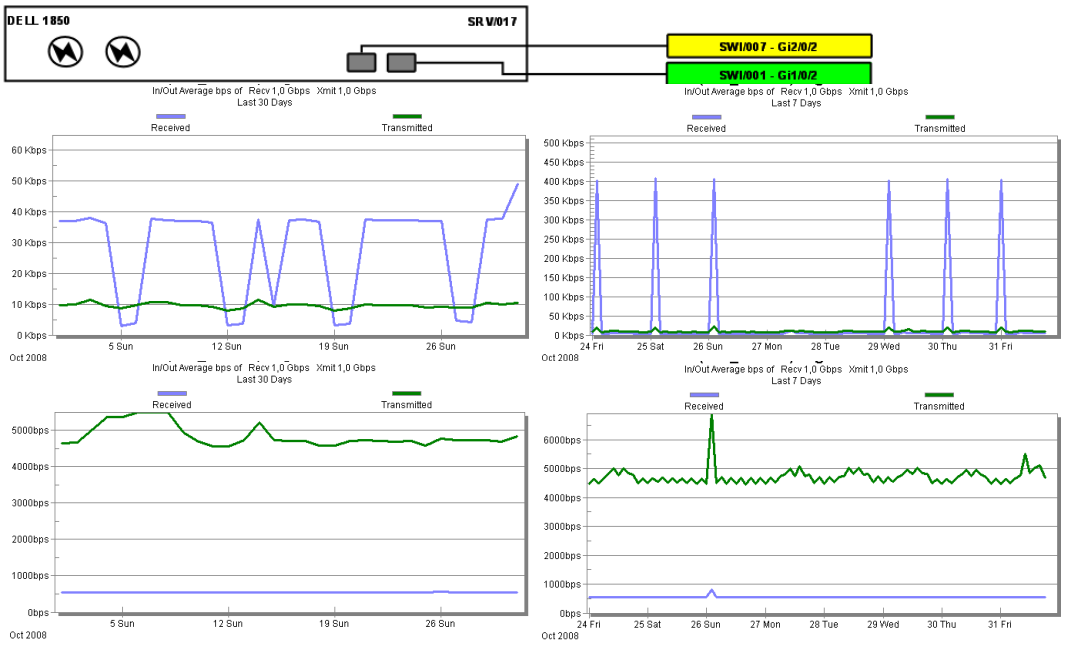
Legenda:

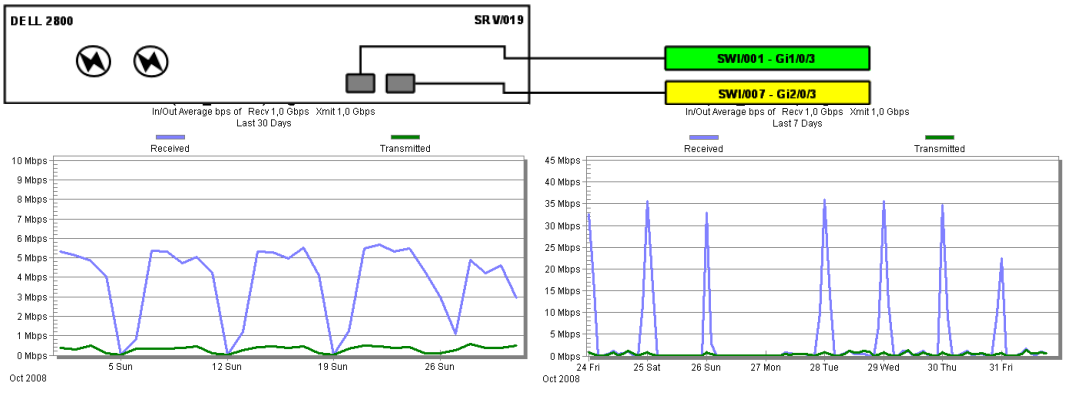
Ligação eléctrica

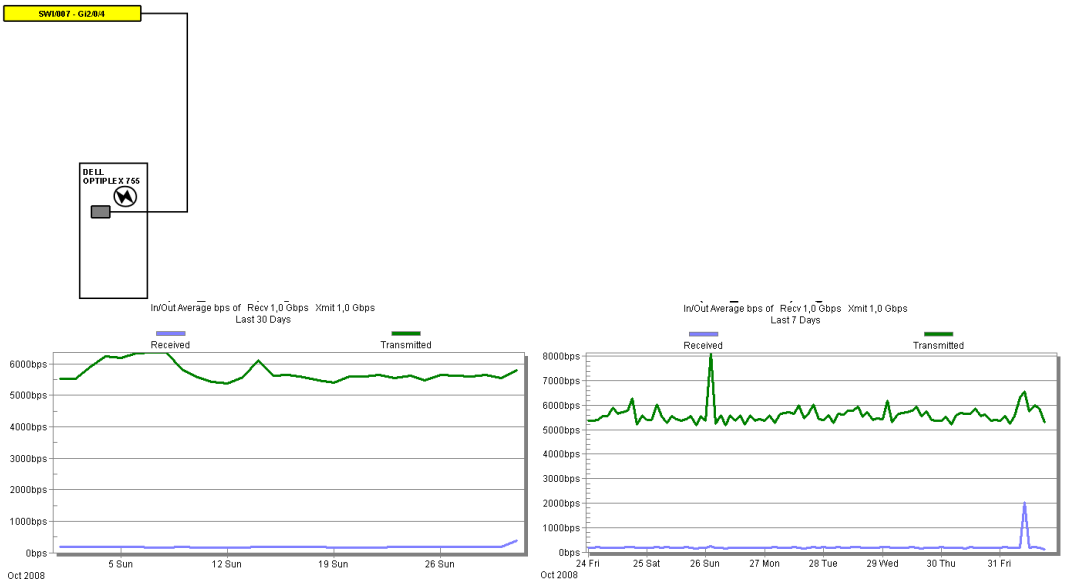
Ligação de rede não utilizada

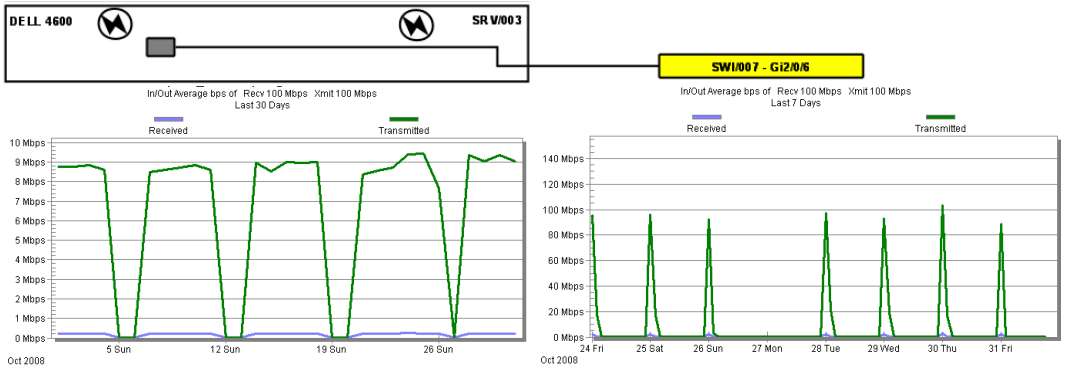
Ligação de rede utilizada


DELL 1750
SRV/020
SWI/001 - Gi1/0/1
SWI/007 - Gi2/0/1
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

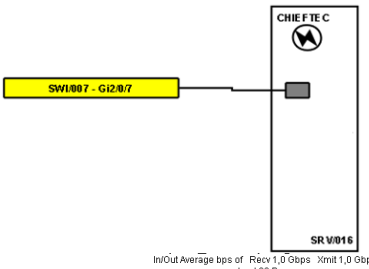

DELL 1850
SRV/017
SWI/007 - Gi2/0/2
SWI/001 - Gi1/0/2
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
60 Kbps
50 Kbps
40 Kbps
30 Kbps
20 Kbps
10 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

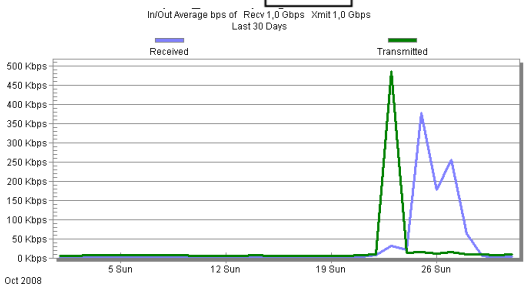

DELL 2800
SRV/019
SWI/001 - Gi1/0/3
SWI/007 - Gi2/0/3
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
45 Mbps
40 Mbps
35 Mbps
30 Mbps
25 Mbps
20 Mbps
15 Mbps
10 Mbps
5 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

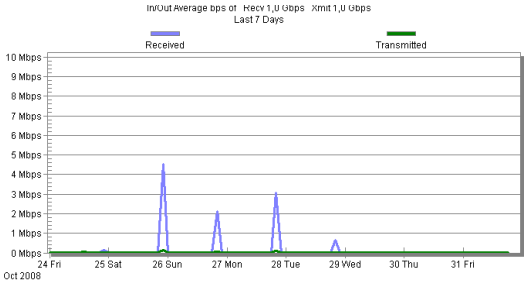

SWI/007 - Gi2/0/4
DELL OPTIPLEX 755
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
8000bps
7000bps
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

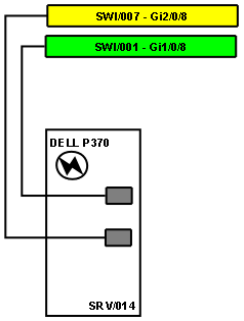

DELL 4600
SRV/003
SWI/007 - Gi2/0/6
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 30 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 7 Days
Received
Transmitted
140 Mbps
120 Mbps
100 Mbps
80 Mbps
60 Mbps
40 Mbps
20 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

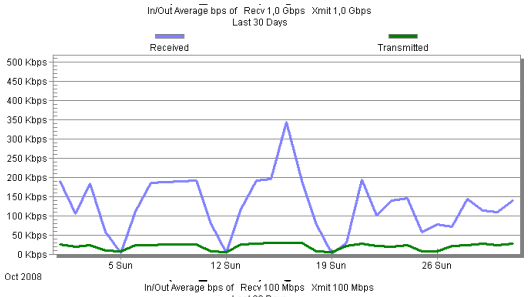

HP DL320
SRV/018
SWI/001 - Gi1/0/7
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

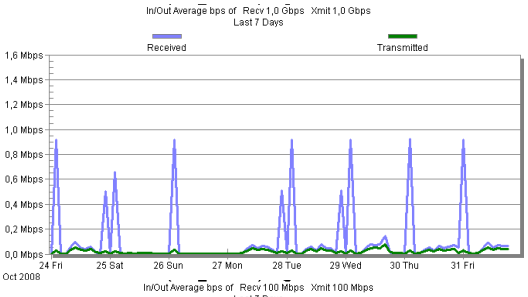

CHIEFTEC
SWI/007 - Gi2/0/7
SRV/016

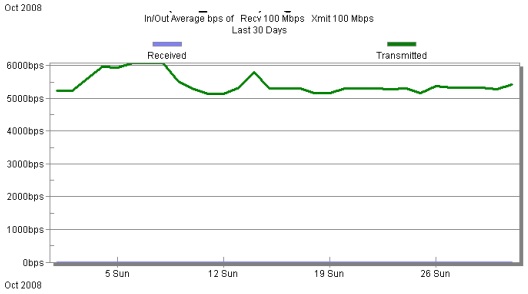

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

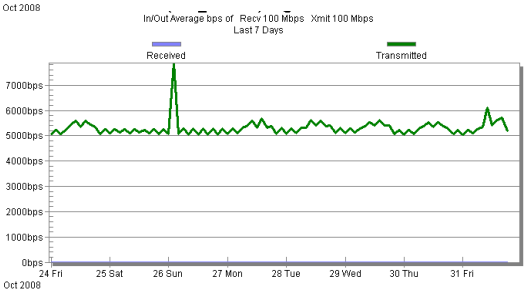

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

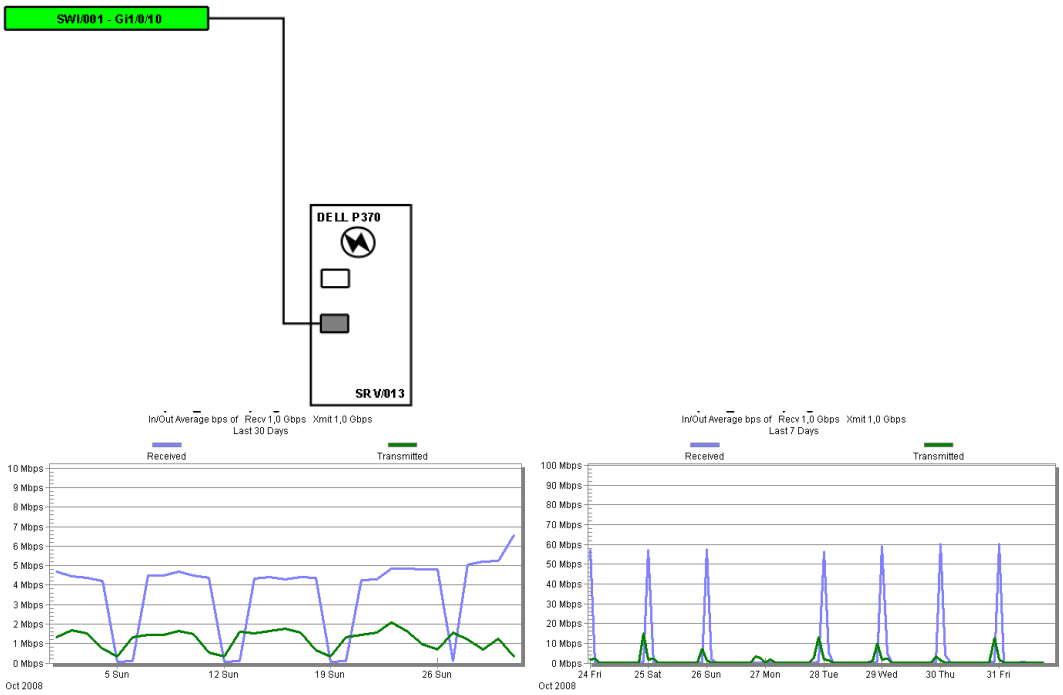

SWI/007 - Gi2/0/8
SWI/001 - Gi1/0/8
DELL P370
SRV/014


In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

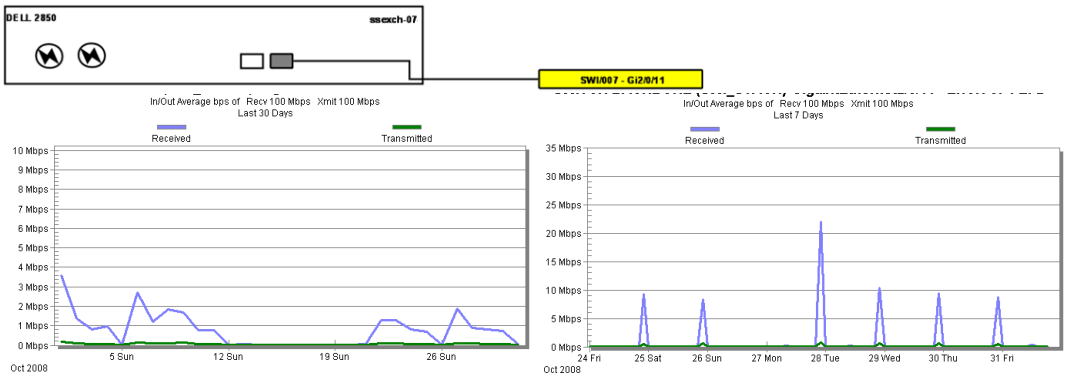

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008


In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 30 Days
Received
Transmitted
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

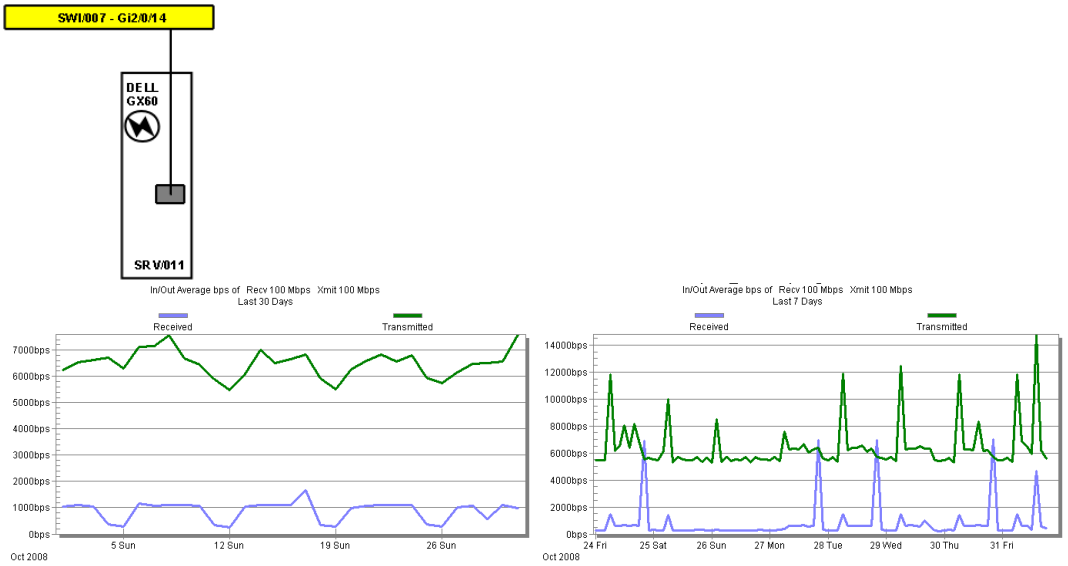

In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 7 Days
Received
Transmitted
7000bps
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

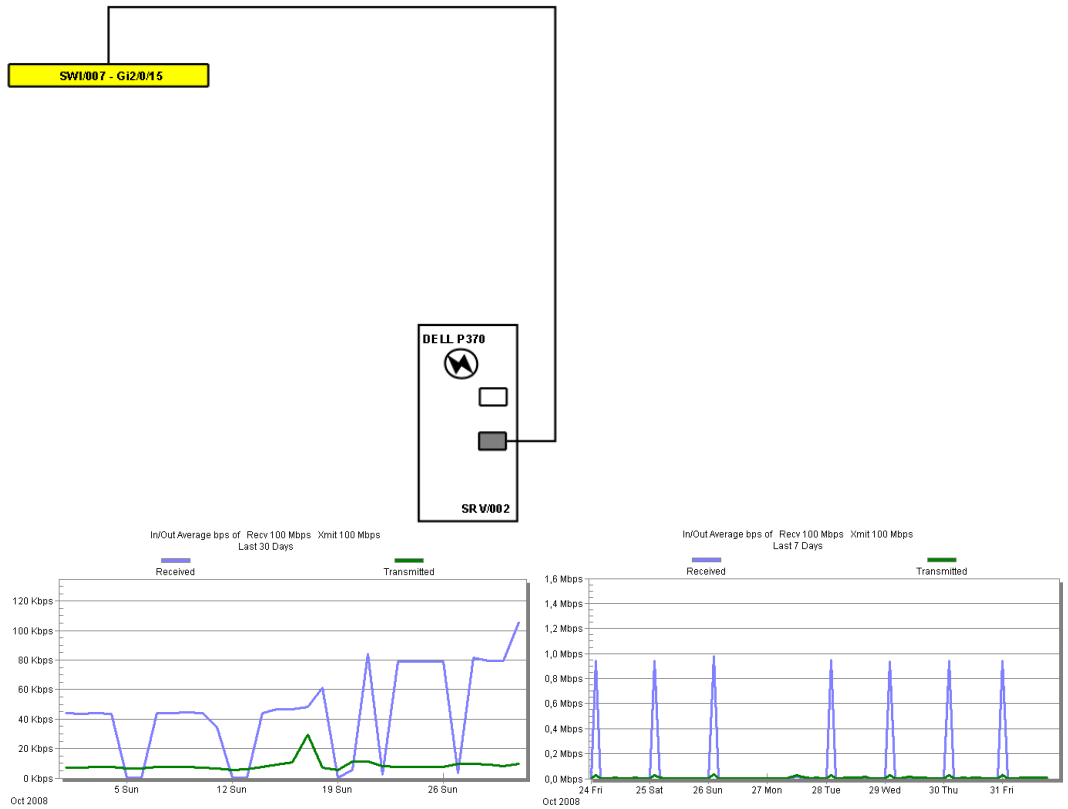


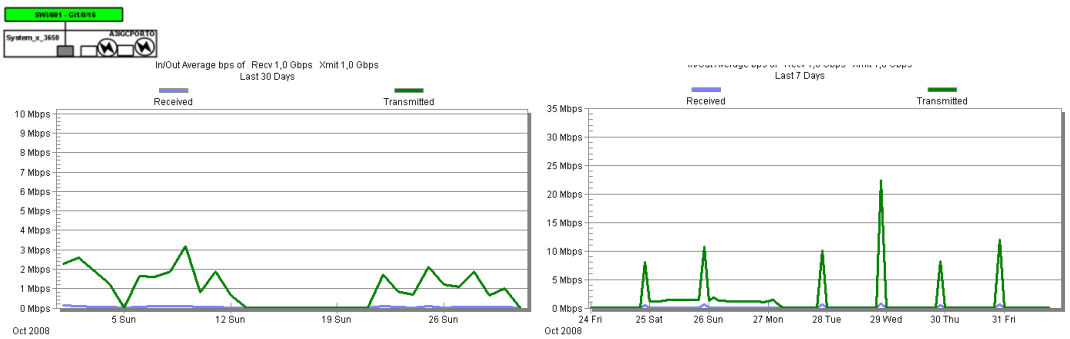
Terminal Controlo de Acessos (POLO TÉCNICO)

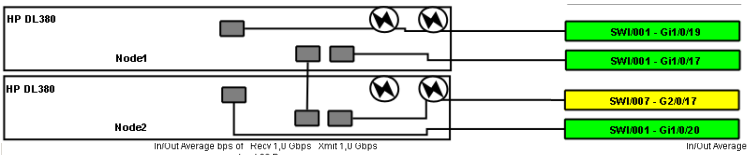


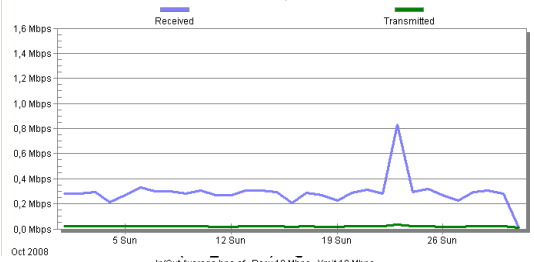

SWI/007 - Gi2/0/12
SWI/001 - Gi1/0/12
DELL 1500SC
SRV/004
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 30 Days
Received
Transmitted
14000bps
12000bps
10000bps
8000bps
6000bps
4000bps
2000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 7 Days
Received
Transmitted
60 Kbps
50 Kbps
40 Kbps
30 Kbps
20 Kbps
10 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
DELL 2800
SRV/021
SWI/001 - Gi1/0/13
SWI/007 - Gi2/0/13
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 30 Days
Received
Transmitted
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 7 Days
Received
Transmitted
7000bps
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

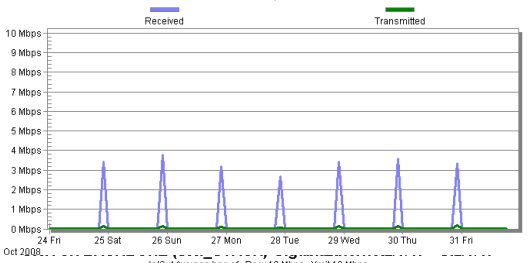

SWI/007 - Gi2/0/14
DELL GX60
SRV/011
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 30 Days
Received
Transmitted
7000bps
6000bps
5000bps
4000bps
3000bps
2000bps
1000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 7 Days
Received
Transmitted
14000bps
12000bps
10000bps
8000bps
6000bps
4000bps
2000bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

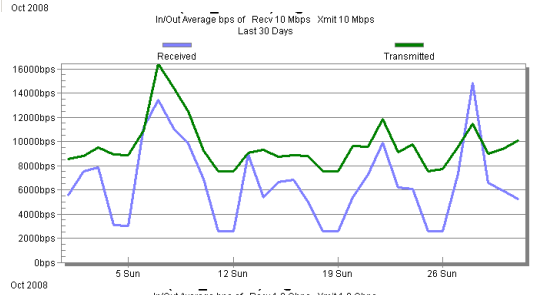

SWI/007 - Gi2/0/15
DELL P370
SRV/002
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 30 Days
Received
Transmitted
120 Kbps
100 Kbps
80 Kbps
60 Kbps
40 Kbps
20 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 100 Mbps Xmit 100 Mbps
Last 7 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

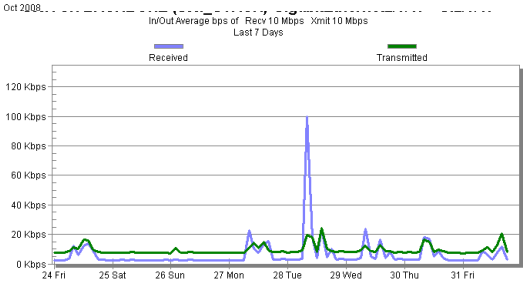

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
Last 7 Days
Received
Transmitted
35 Mbps
30 Mbps
25 Mbps
20 Mbps
15 Mbps
10 Mbps
5 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

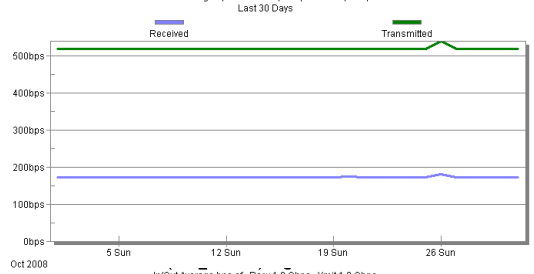

HP DL380
Node1
HP DL380
Node2
SWI001 - Gi1/0/19
SWI001 - Gi1/0/17
SWI007 - G2/0/17
SWI001 - Gi1/0/20

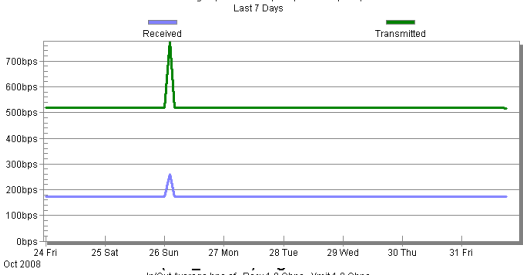

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008


In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

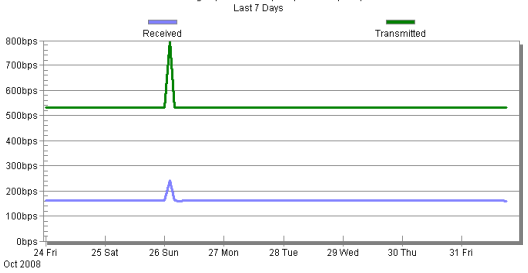

In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 30 Days
Received
Transmitted
16000bps
14000bps
12000bps
10000bps
8000bps
6000bps
4000bps
2000bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

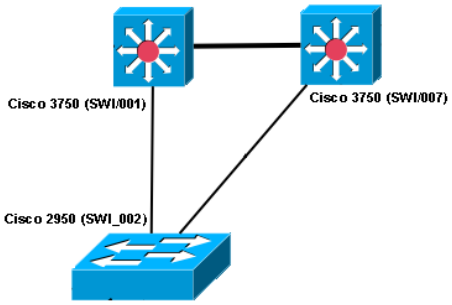

In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 7 Days
Received
Transmitted
120 Kbps
100 Kbps
80 Kbps
60 Kbps
40 Kbps
20 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

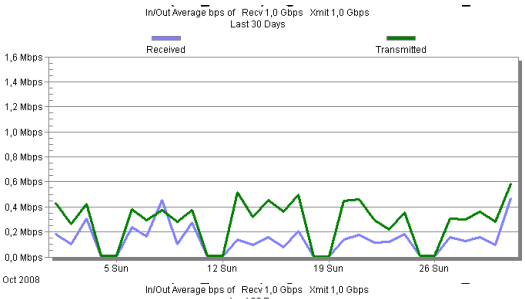

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
500bps
400bps
300bps
200bps
100bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

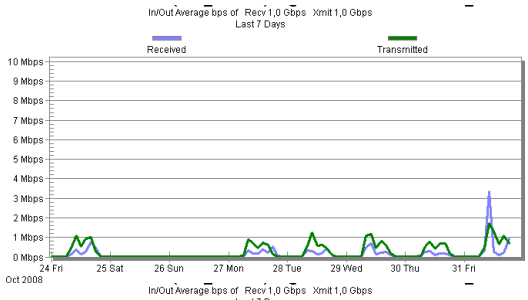

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
700bps
600bps
500bps
400bps
300bps
200bps
100bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

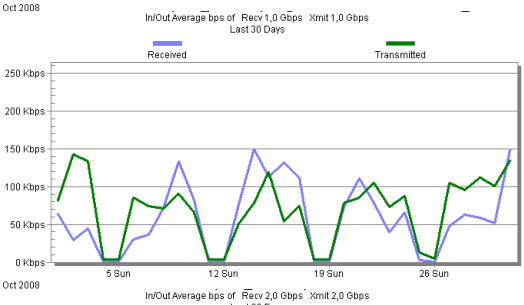

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
500bps
400bps
300bps
200bps
100bps
0bps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

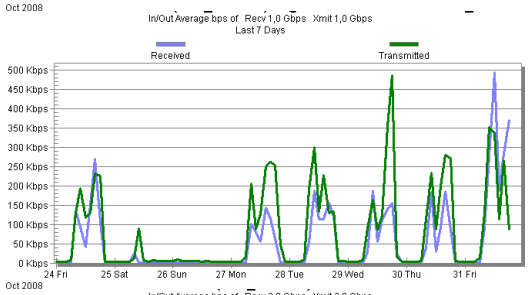

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
800bps
700bps
600bps
500bps
400bps
300bps
200bps
100bps
0bps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

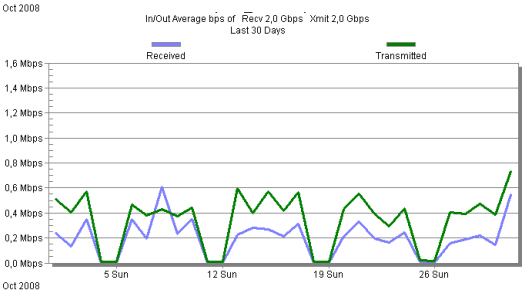

Cisco 3750 (SWI/001)
Cisco 3750 (SWI/007)
Cisco 2950 (SWI_002)

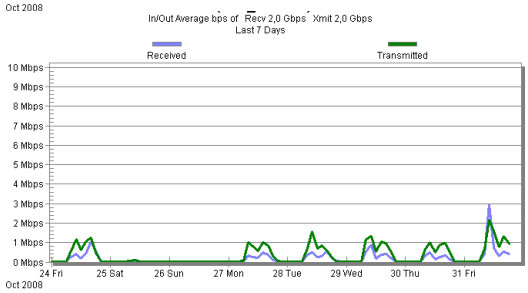

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

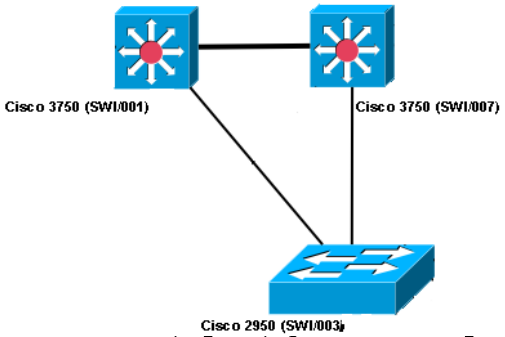

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

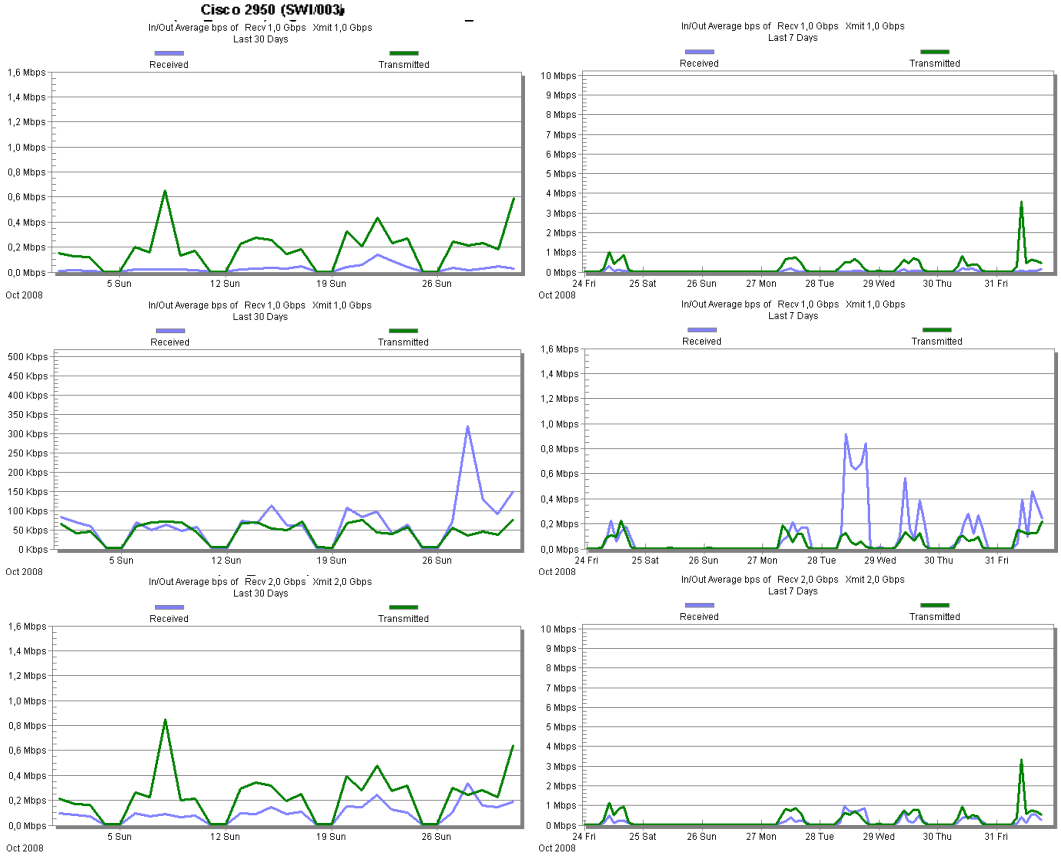

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 30 Days
Received
Transmitted
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008

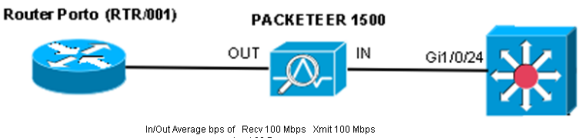

In/Out Average bps of Recv 1,0 Gbps Xmit 1,0 Gbps
Last 7 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

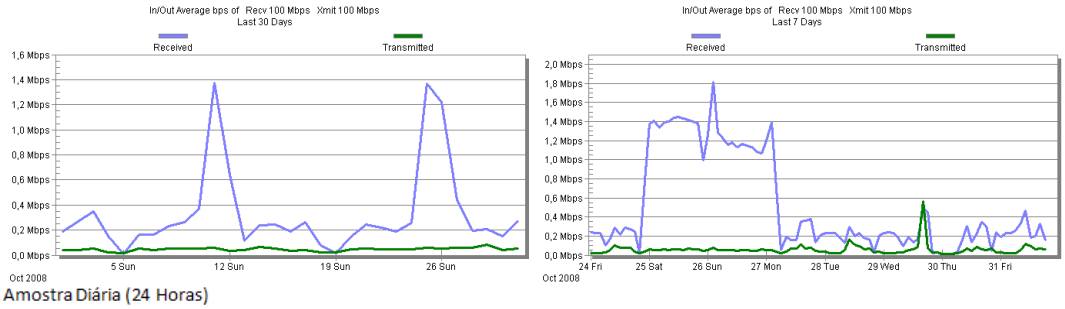

In/Out Average bps of Recv 2,0 Gbps Xmit 2,0 Gbps
Last 30 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008


In/Out Average bps of Recv 2,0 Gbps Xmit 2,0 Gbps
Last 7 Days
Received
Transmitted
10 Mbps
9 Mbps
8 Mbps
7 Mbps
6 Mbps
5 Mbps
4 Mbps
3 Mbps
2 Mbps
1 Mbps
0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

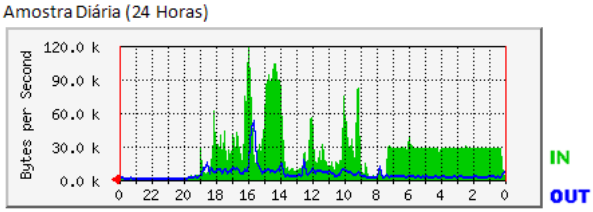


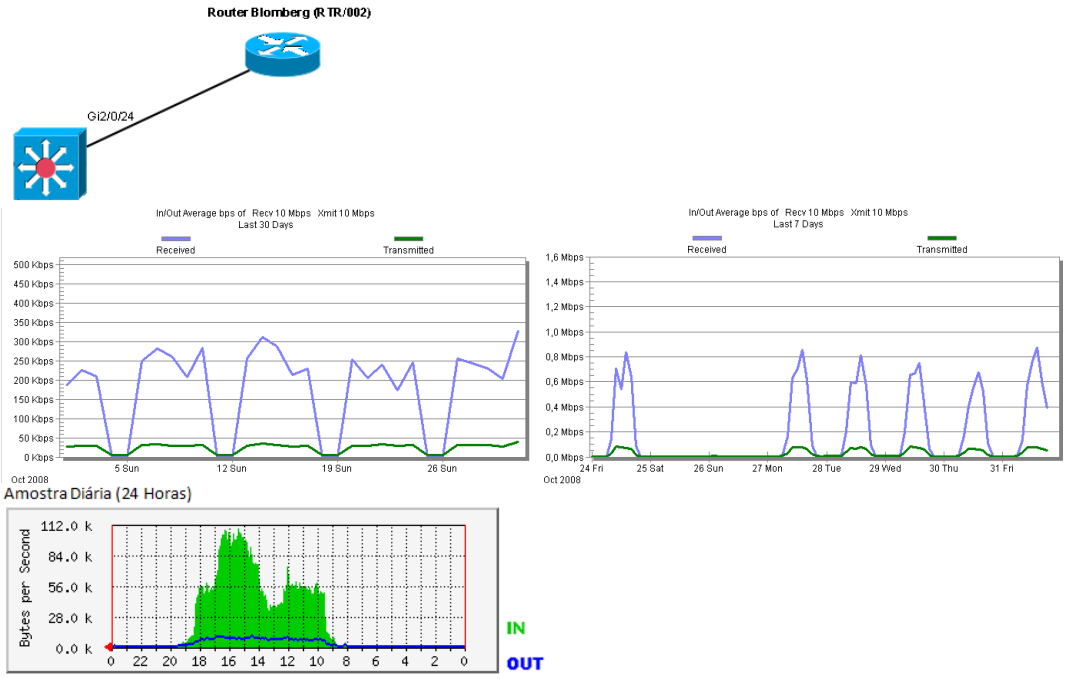




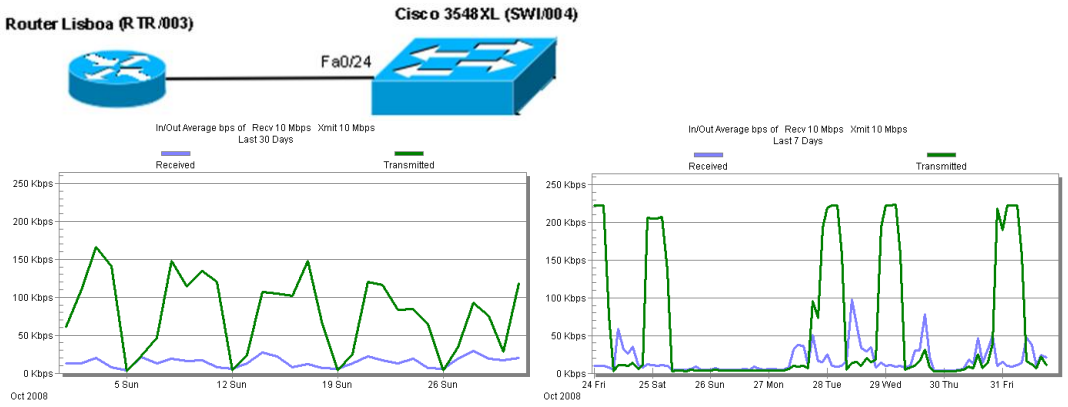


Amostra Diária (24 Horas)




Router Blomberg (RTR/002)
Gi2/0/24
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 30 Days
Received
Transmitted
500 Kbps
450 Kbps
400 Kbps
350 Kbps
300 Kbps
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 7 Days
Received
Transmitted
1,6 Mbps
1,4 Mbps
1,2 Mbps
1,0 Mbps
0,8 Mbps
0,6 Mbps
0,4 Mbps
0,2 Mbps
0,0 Mbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008
Amostra Diária (24 Horas)
Bytes per Second
112.0 k
84.0 k
56.0 k
28.0 k
0.0 k
0 22 20 18 16 14 12 10 8 6 4 2 0
IN
OUT

A.2 Lisboa

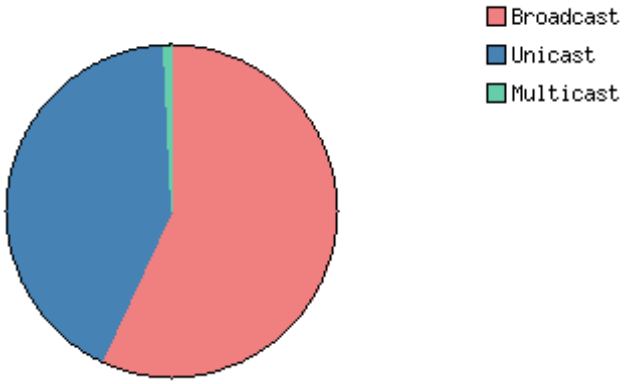

Router Lisboa (RTR/003)
Cisco 3548XL (SWI/004)
Fa0/24
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 30 Days
Received
Transmitted
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
5 Sun
12 Sun
19 Sun
26 Sun
Oct 2008
In/Out Average bps of Recv 10 Mbps Xmit 10 Mbps
Last 7 Days
Received
Transmitted
250 Kbps
200 Kbps
150 Kbps
100 Kbps
50 Kbps
0 Kbps
24 Fri
25 Sat
26 Sun
27 Mon
28 Tue
29 Wed
30 Thu
31 Fri
Oct 2008

Anexo B

Características dos fluxos de tráfego

Este anexo contém as estatísticas recolhidas sobre as características dos principais fluxos de tráfego na rede do IGC.

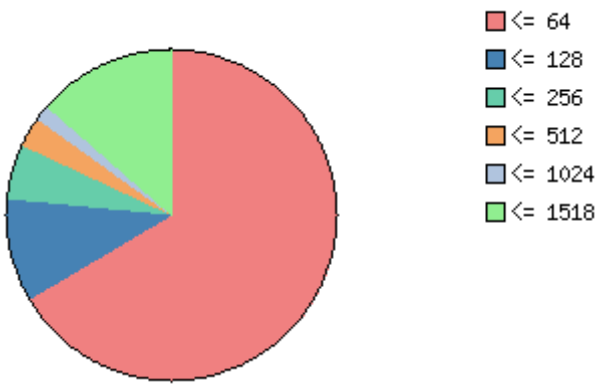
D.1 SRV/020 – IGCDC1 (172.20.8.10)



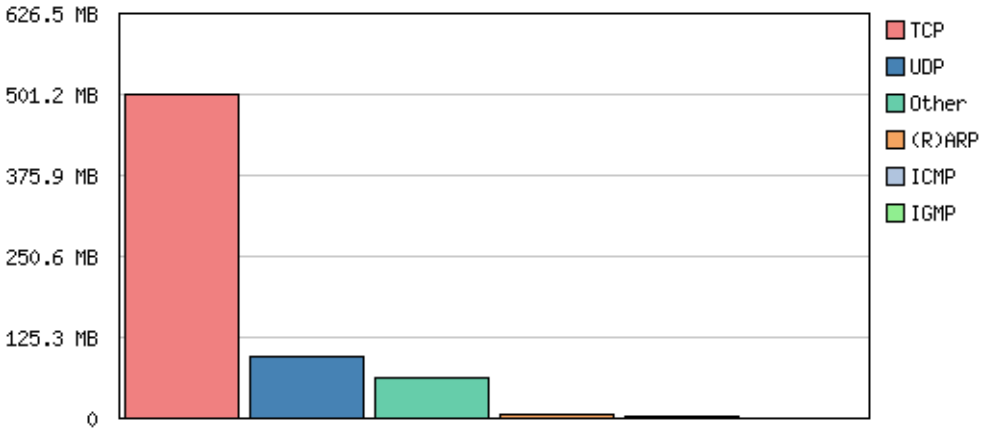
Unicast	42.5%
Broadcast	57.0%
Multicast	0.6%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SRV/020 – IGCDC1 (172.20.8.10)

<= 64 bytes	66.6%
64 to 128 bytes	10.4%
129 to 256 bytes	5.5%
257 to 512 bytes	3.1%
513 to 1024 bytes	1.6%
1025 to 1518 bytes	12.7%
> 1518 bytes	0.0%

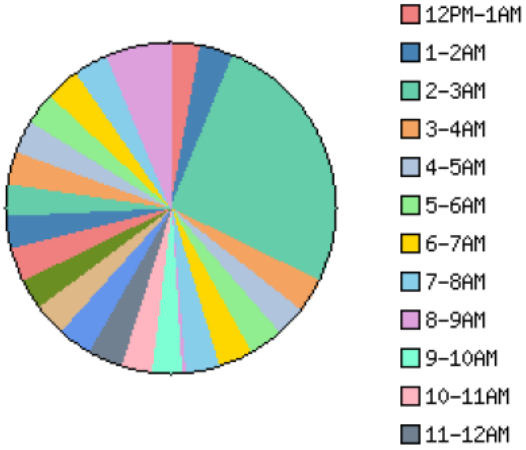
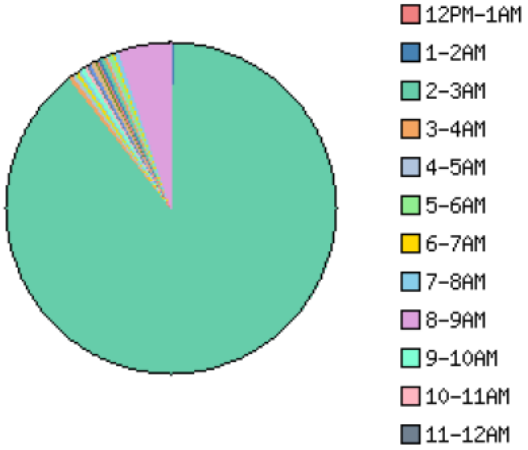


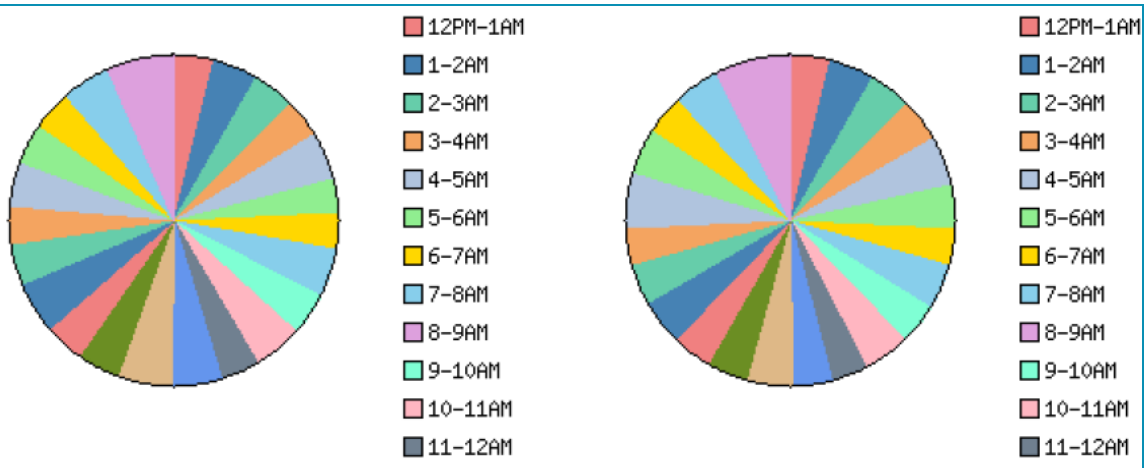
Distribuição do tamanho dos pacotes em SRV/020 – IGCDC1 (172.20.8.10)



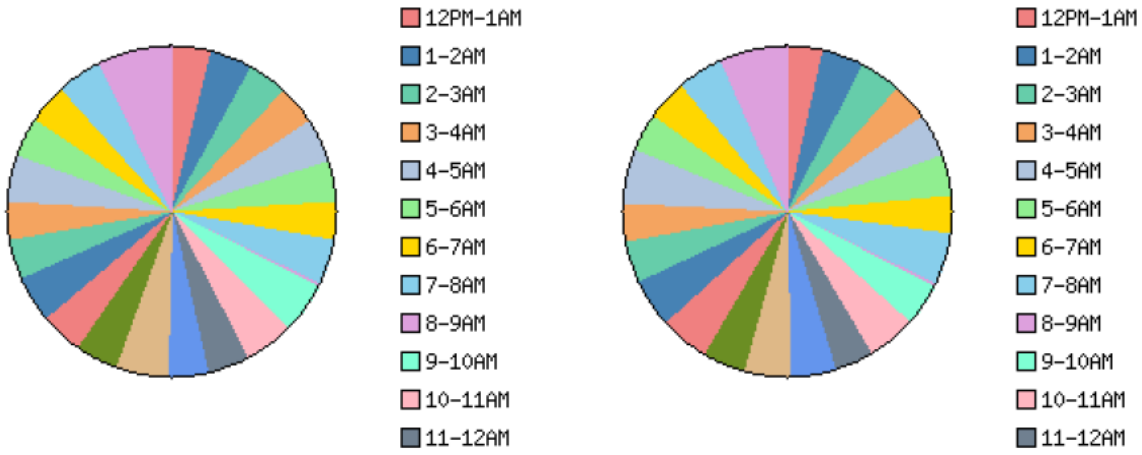
Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SRV/020 – IGCDC1 (172.20.8.10)

A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

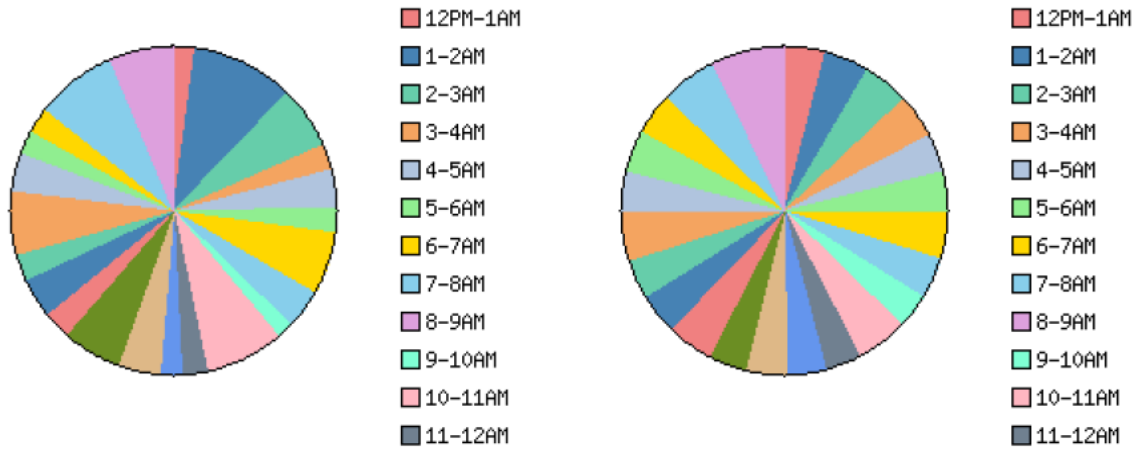
Parceiro Comunicação	**Quantidade de Dados**
igc-bck.igc.isi.pt	430.0 MB
Enviado	**Recebido**
	
Parceiro Comunicação	**Quantidade de Dados**
igc-fslx.igc.isi.pt	32.2 MB
Enviado	**Recebido**



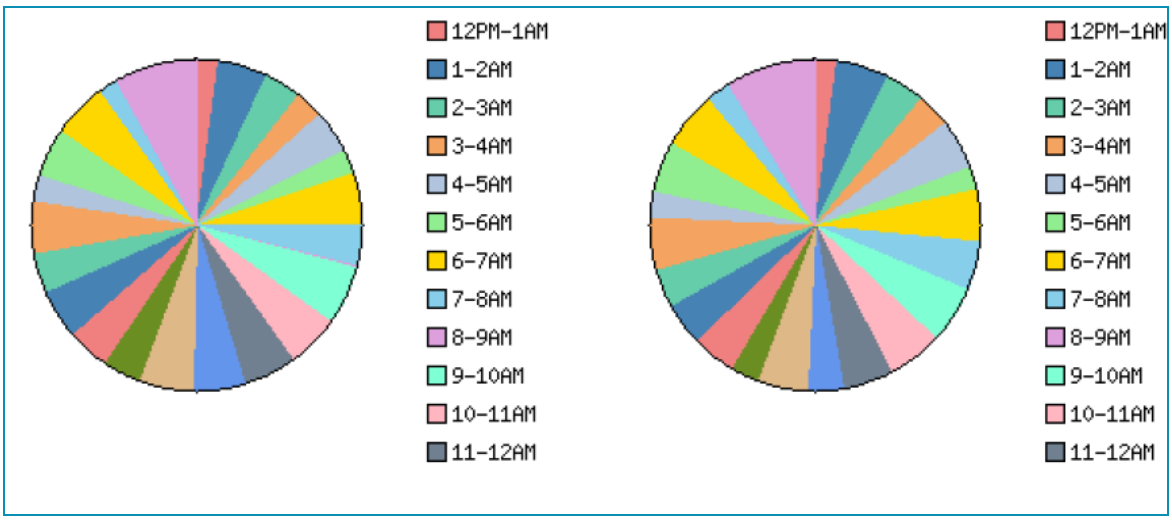
Parceiro Comunicação	**Quantidade de Dados**
igcdc2.igc.isi.pt	31.9 MB
Enviado	**Recebido**



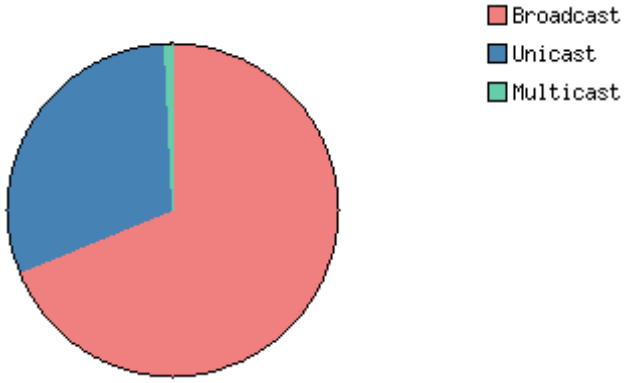
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	12.0 MB
Enviado	**Recebido**



Parceiro Comunicação	**Quantidade de Dados**
igc-fs.igc.isi.pt	4.8 MB
Enviado	**Recebido**

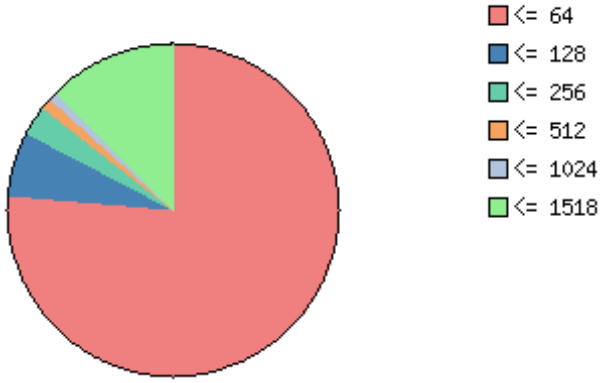


D.2 SRV/017 – IGCDC2 (172.20.8.18)



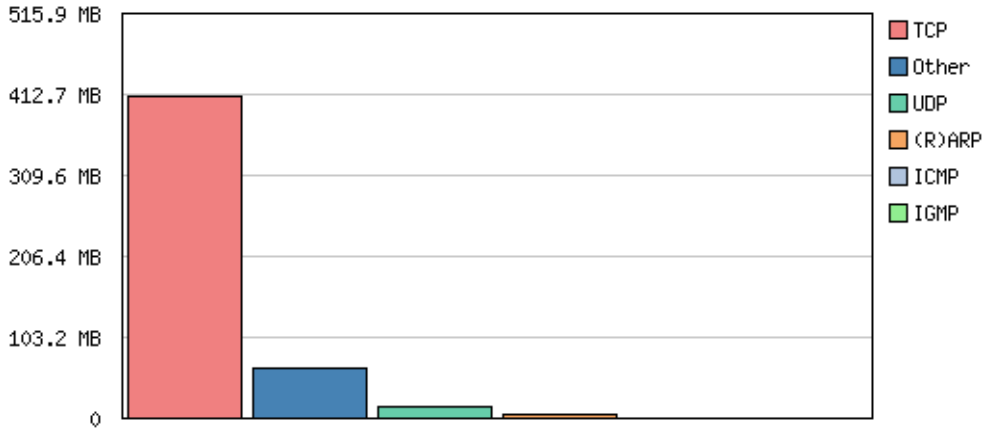
Unicast	30.4%
Broadcast	69.0%
Multicast	0.7%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SRV/017 – IGCDC2 (172.20.8.18)

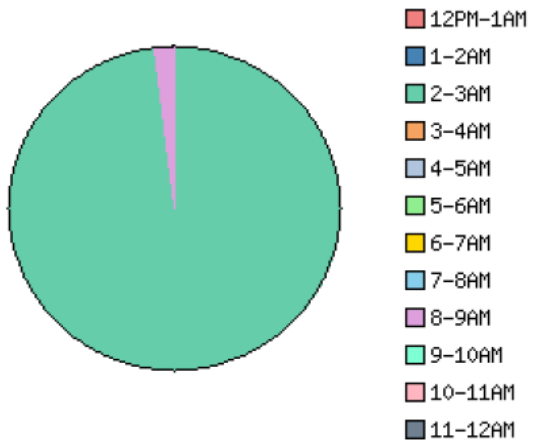
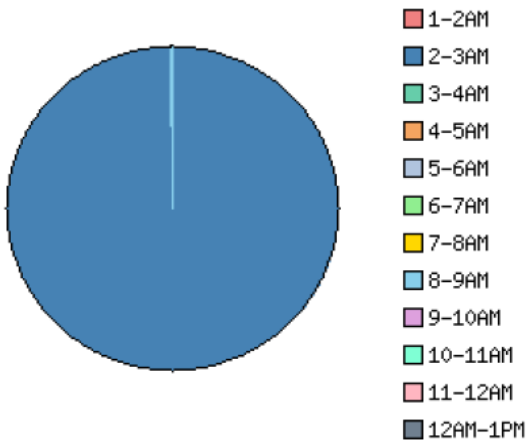


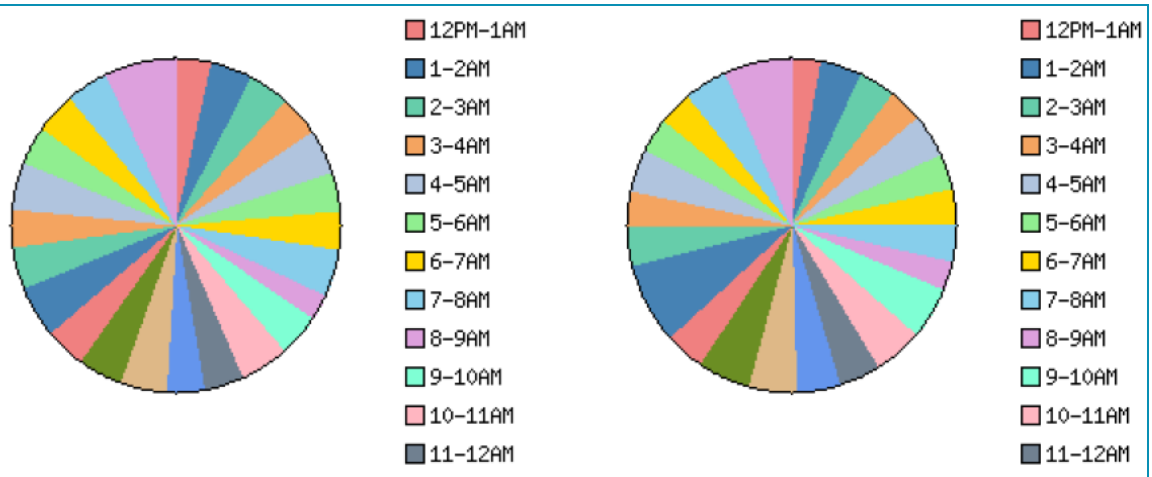
<= 64 bytes	76.6%
64 to 128 bytes	6.4%
129 to 256 bytes	2.9%
257 to 512 bytes	1.4%
513 to 1024 bytes	0.9%
1025 to 1518 bytes	11.7%
> 1518 bytes	0.0%

Distribuição do tamanho dos pacotes em SRV/017 – IGCDC2 (172.20.8.18)

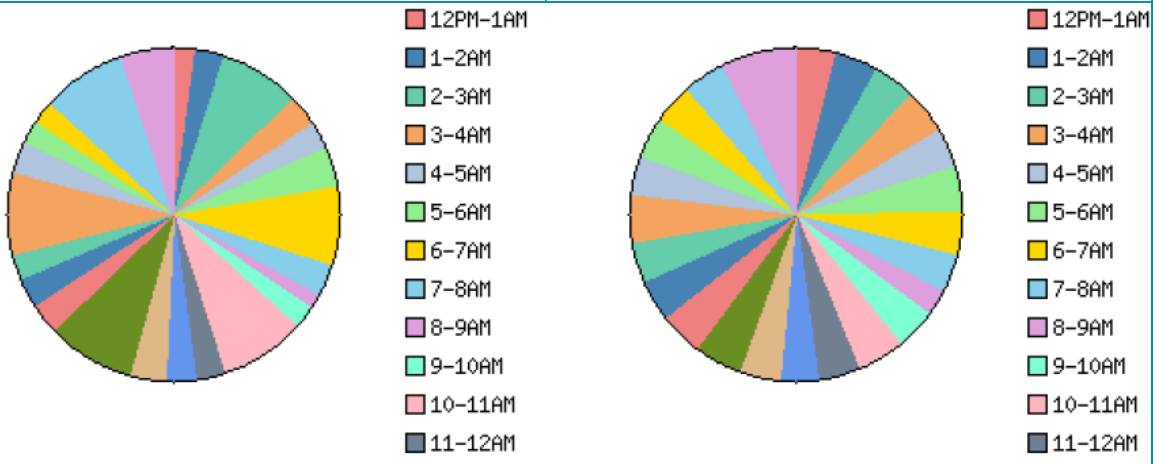


Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SRV/017 – IGCDC2 (172.20.8.18)
A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

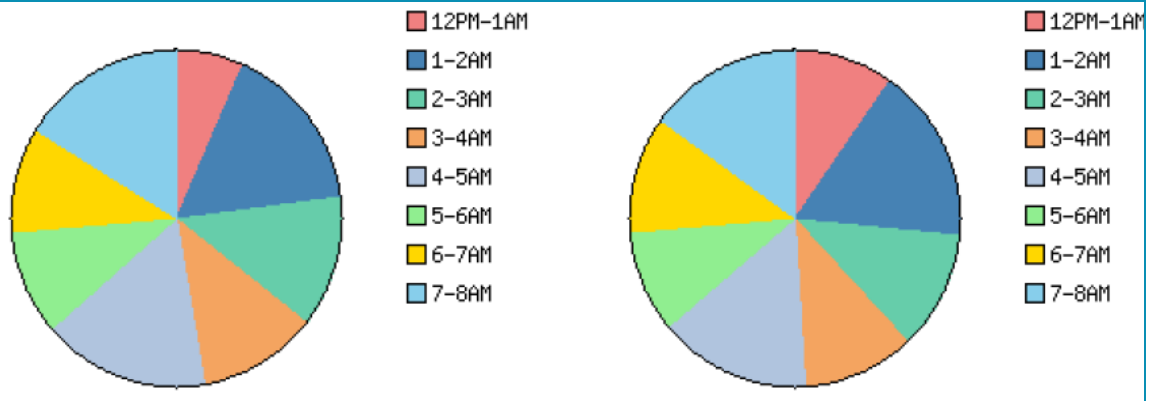
Parceiro Comunicação	**Quantidade de Dados**
igc-bck.igc.isi.pt	344.9 MB
Enviado	**Recebido**
	
Parceiro Comunicação	**Quantidade de Dados**
igcdc1.igc.isi.pt	32.7 MB
Enviado	**Recebido**



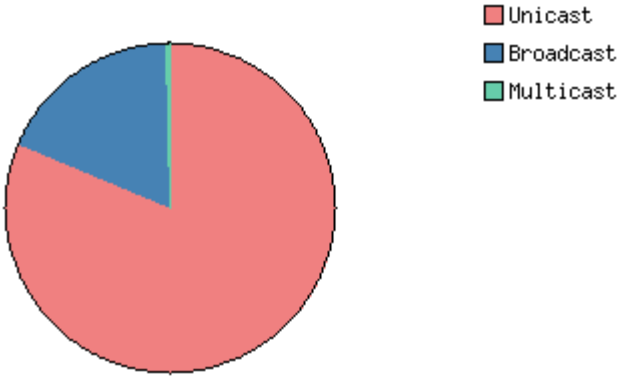
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	6.7 MB
Enviado	**Recebido**



Parceiro Comunicação	**Quantidade de Dados**
igc-fslx.igc.isi.pt	3.8 MB
Enviado	**Recebido**

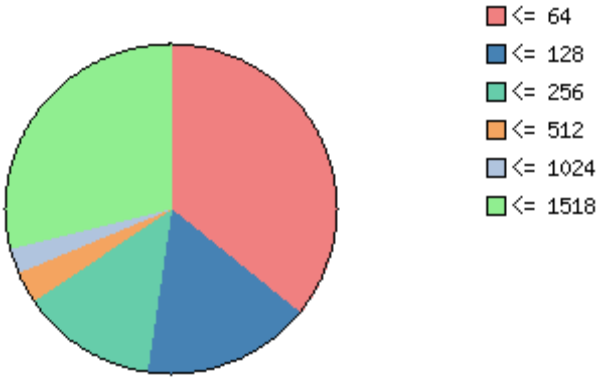


D.3 SRV/021 – IGC-SQL (172.20.8.13)



Unicast	81.6%
Broadcast	18.2%
Multicast	0.2%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SRV/021 – IGC-SQL (172.20.8.13)

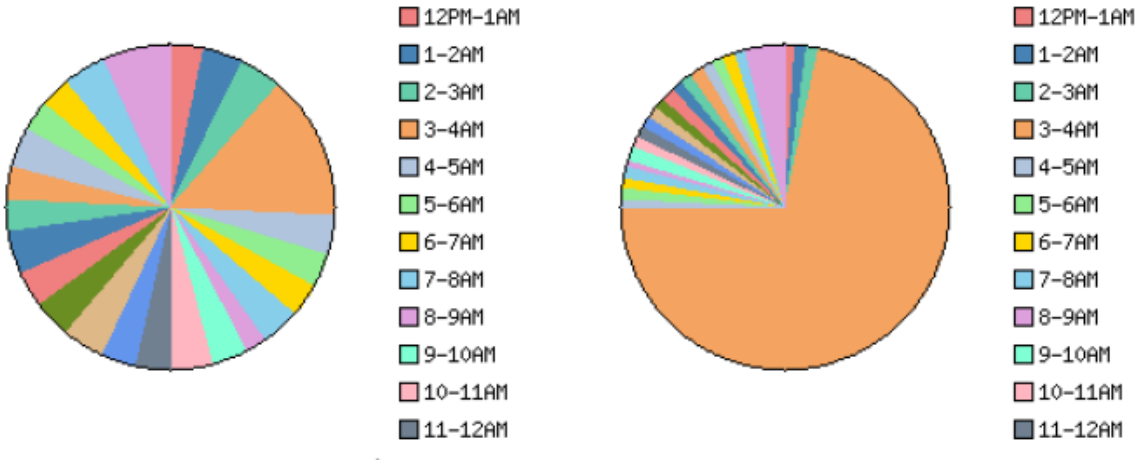


<= 64 bytes	36.1%
64 to 128 bytes	16.8%
129 to 256 bytes	13.2%
257 to 512 bytes	3.2%
513 to 1024 bytes	2.7%
1025 to 1518 bytes	27.9%
> 1518 bytes	0.0%

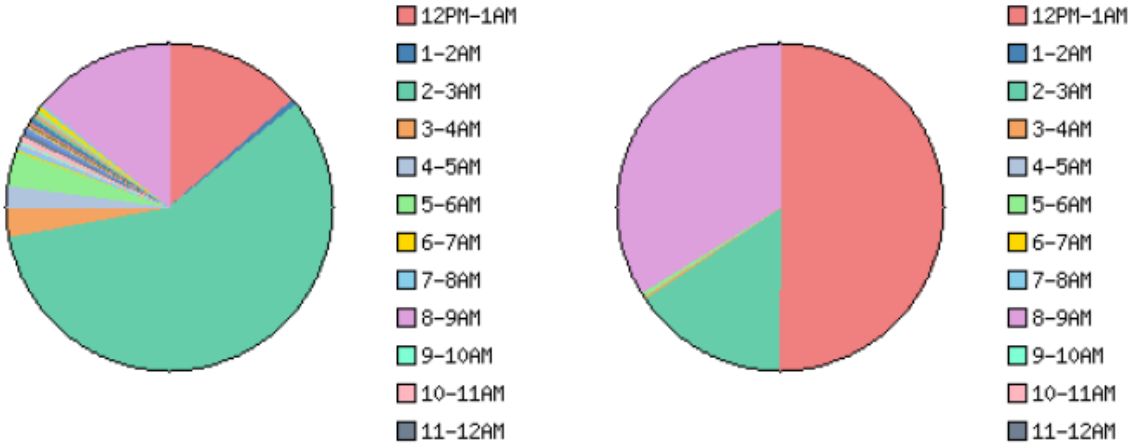
Distribuição do tamanho dos pacotes em SRV/021 – IGC-SQL (172.20.8.13)

Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SRV/021 – IGC-SQL (172.20.8.13)
A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

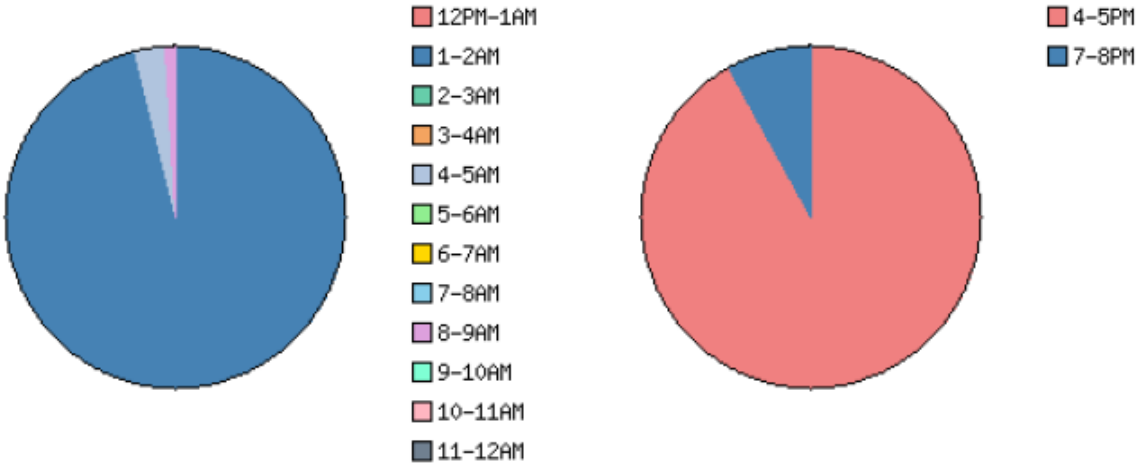
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	2.4 GB
Enviado	**Recebido**



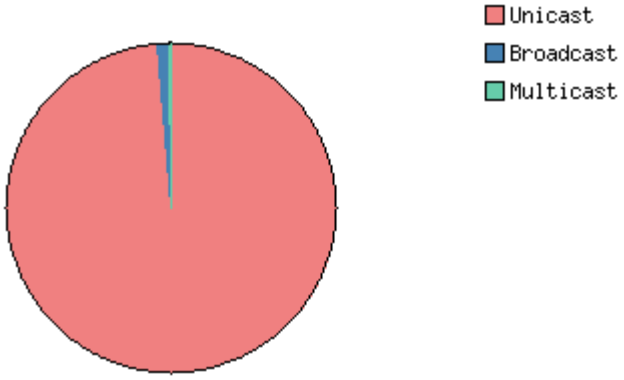
Parceiro Comunicação	**Quantidade de Dados**
igc-bck.igc.isi.pt	1.4 GB
Enviado	**Recebido**



Parceiro Comunicação	**Quantidade de Dados**
node1-vip.igc.isi.pt	12.8 MB
Enviado	**Recebido**

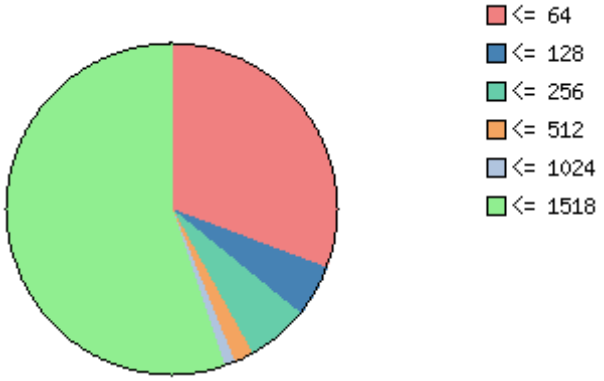


D.4 SRV/019 – IGC-FS (172.20.8.12)



Unicast	98.8%
Broadcast	1.2%
Multicast	0.0%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SRV/019 – IGC-FS (172.20.8.12)



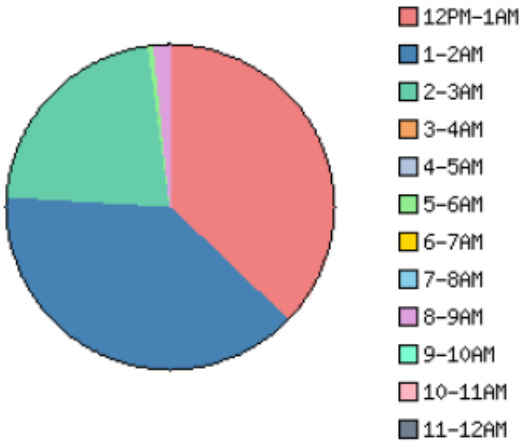
<= 64 bytes	30.9%
64 to 128 bytes	5.1%
129 to 256 bytes	6.3%
257 to 512 bytes	2.1%
513 to 1024 bytes	1.0%
1025 to 1518 bytes	54.5%
> 1518 bytes	0.0%

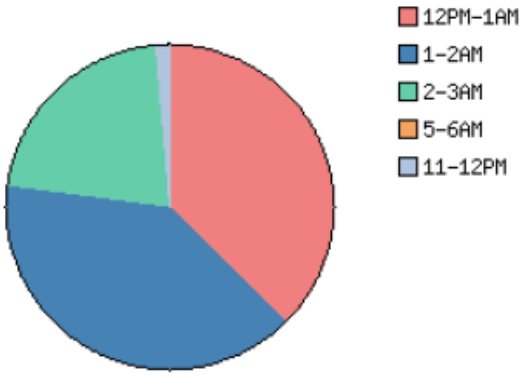
Distribuição do tamanho dos pacotes em SRV/019 – IGC-FS (172.20.8.12)

Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SRV/019 – IGC-FS (172.20.8.12)

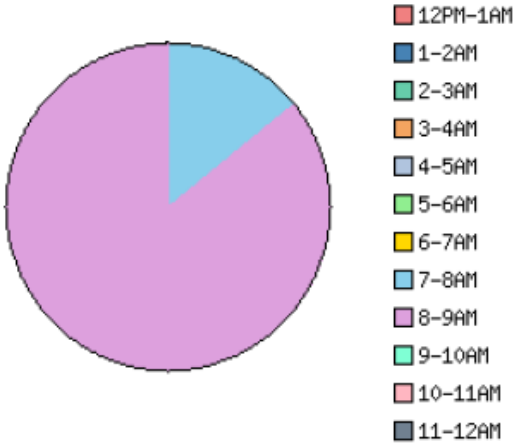
A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

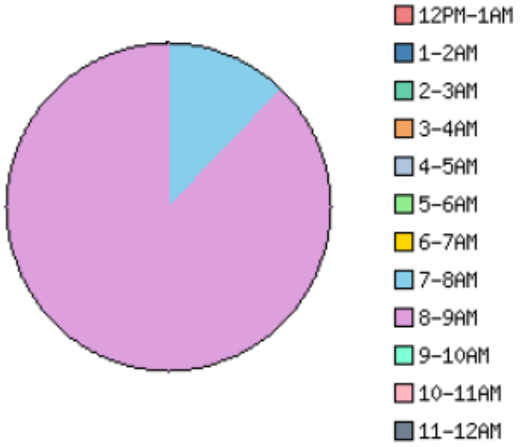
Parceiro Comunicação	**Quantidade de Dados**
igc-bck.igc.isi.pt	43.0 GB
Enviado	**Recebido**



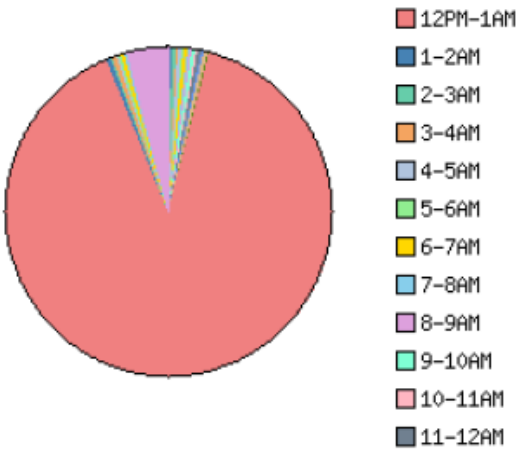


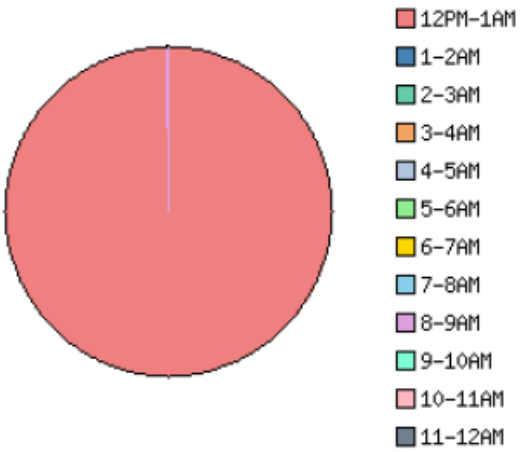
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	8.3 GB
Enviado	**Recebido**



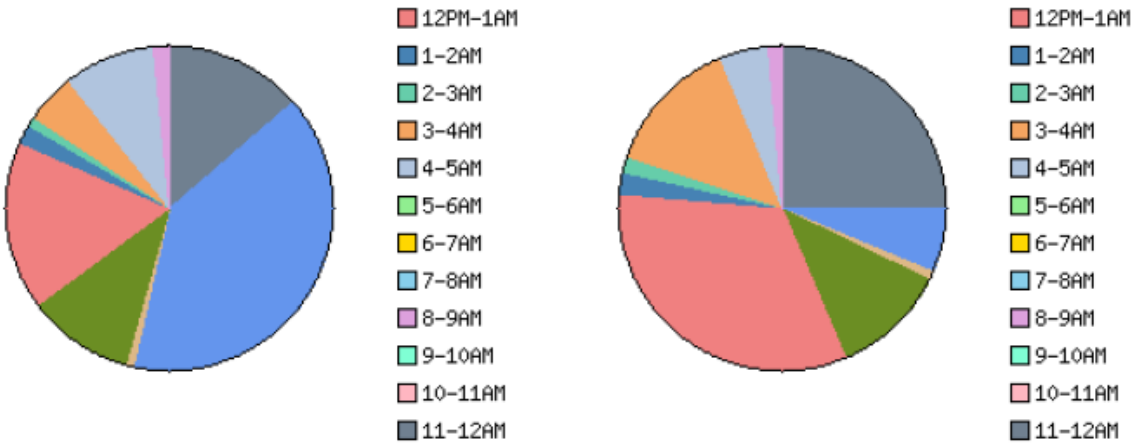


Parceiro Comunicação	**Quantidade de Dados**
igcdc2.igc.isi.pt	920.0 MB
Enviado	**Recebido**

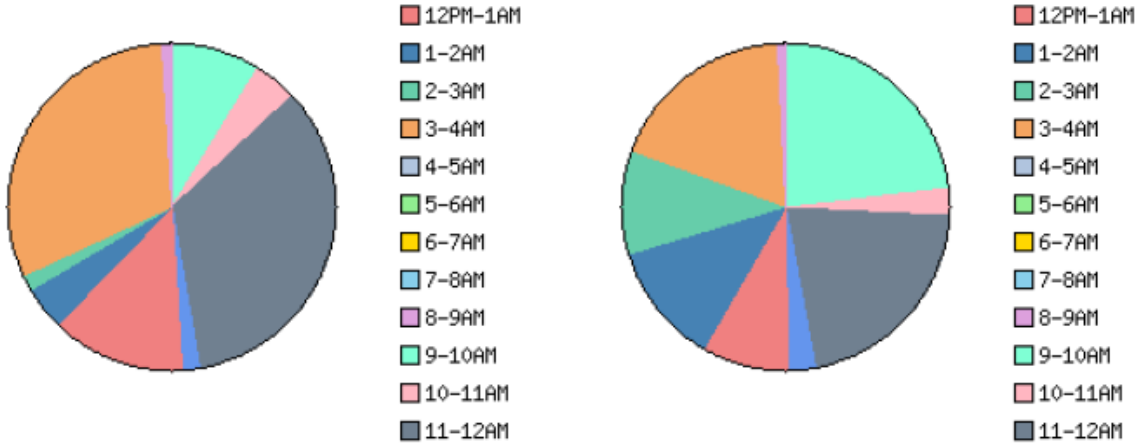




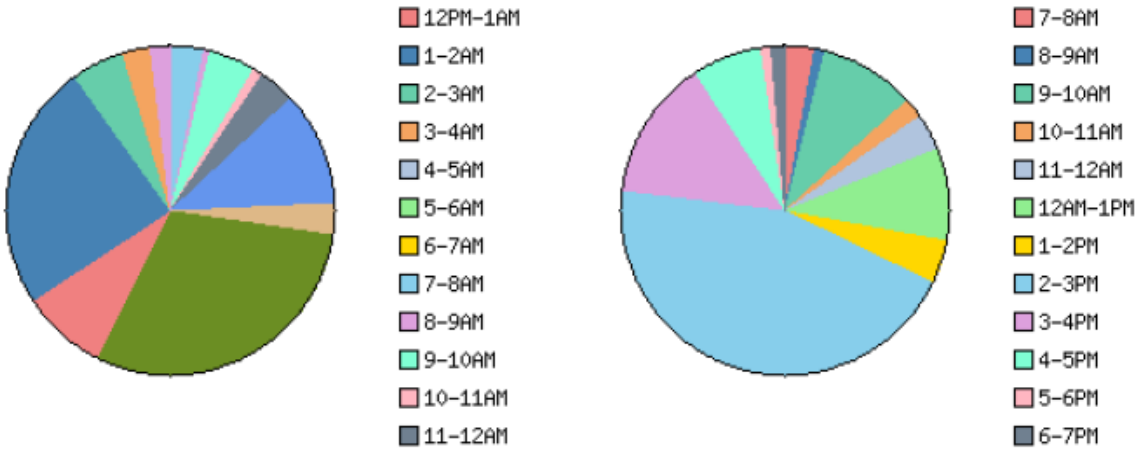
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.186	228.8 MB
Enviado	**Recebido**



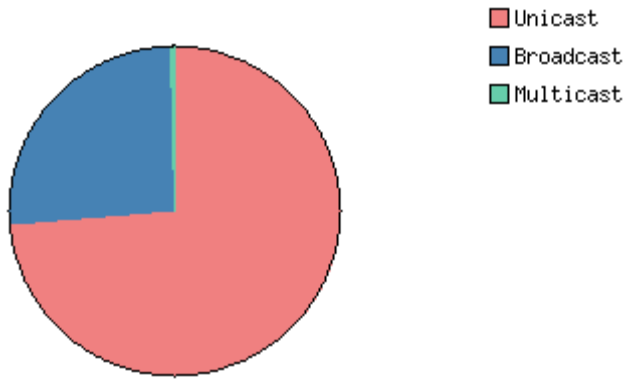
Parceiro Comunicação	**Quantidade de Dados**
di-fefroliveira.igc.isi.pt	174.0 MB
Enviado	**Recebido**



Parceiro Comunicação	**Quantidade de Dados**
depc-fefjvidrag.igc.isi.pt	67.1 MB
Enviado	**Recebido**

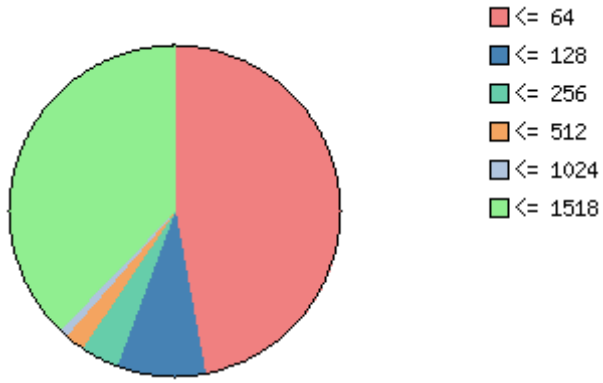


D.5 NODE1+NODE2



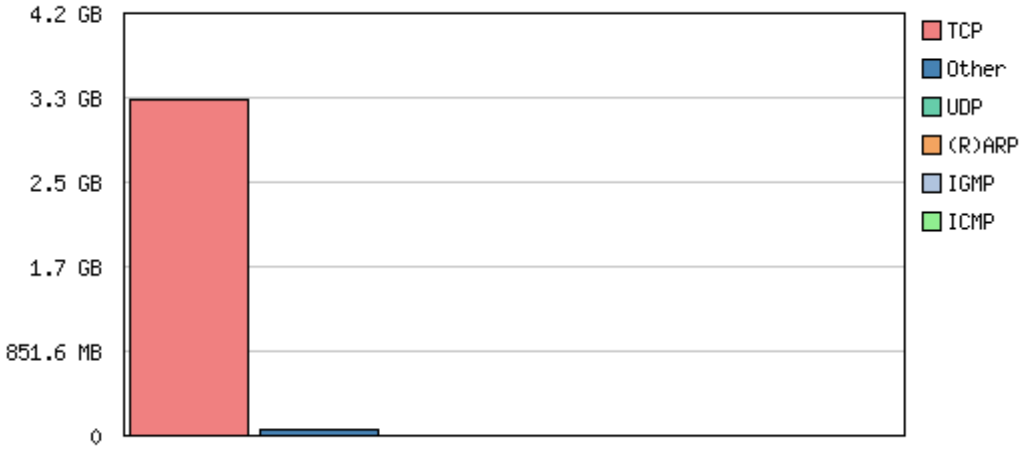
Unicast	73.7%
Broadcast	26.0%
Multicast	0.3%

Distribuição do tráfego em Unicast, Broadcast e Multicast em NODE1+NODE2



<= 64 bytes	47.2%
64 to 128 bytes	9.1%
129 to 256 bytes	3.7%
257 to 512 bytes	2.1%
513 to 1024 bytes	0.9%
1025 to 1518 bytes	37.1%
> 1518 bytes	0.0%

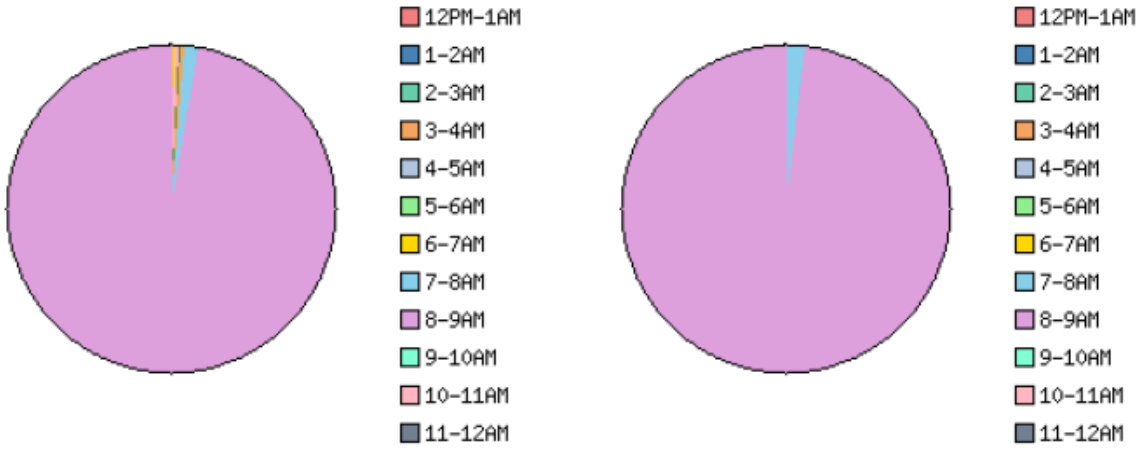
Distribuição do tamanho dos pacotes em NODE1+NODE2



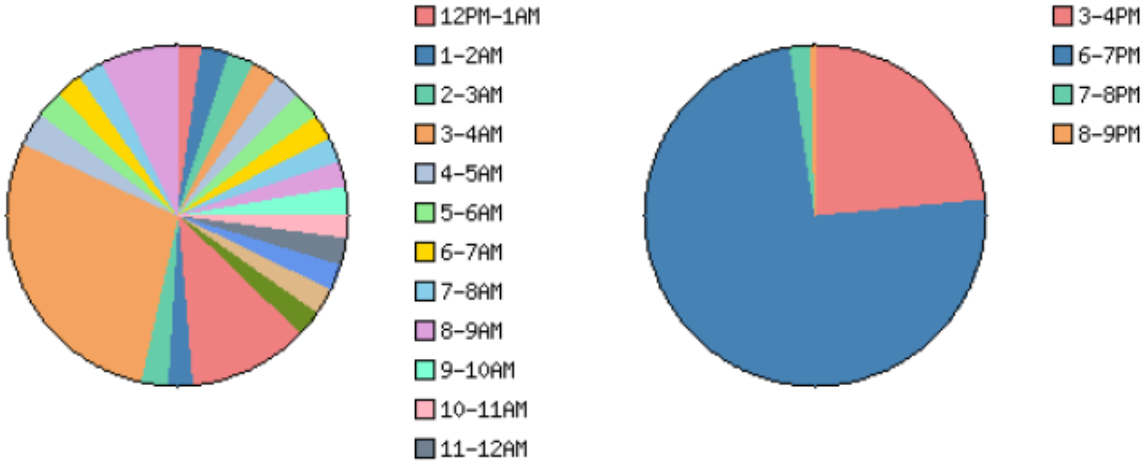
Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em NODE1+NODE2

A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

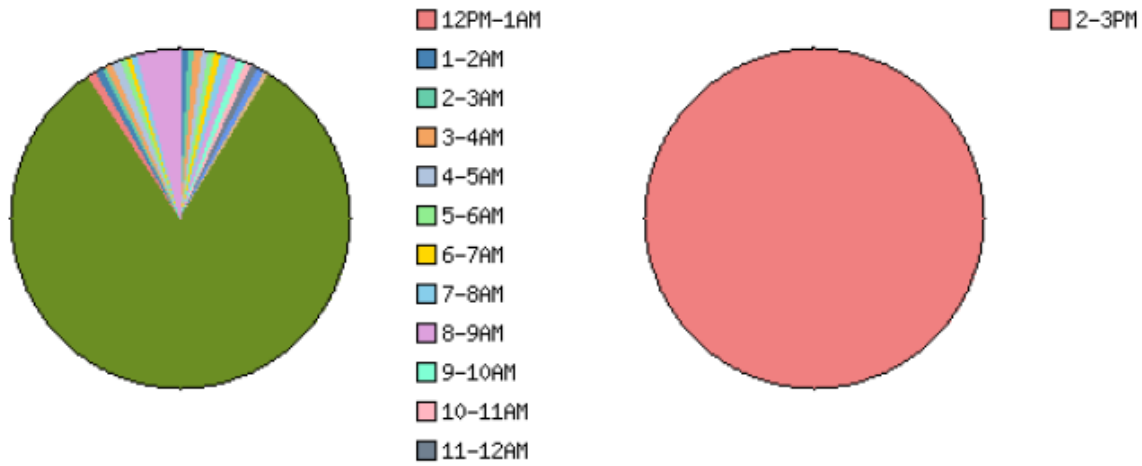
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	3.1 GB
Enviado	**Recebido**



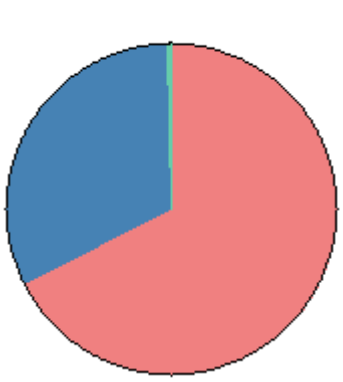
Parceiro Comunicação	**Quantidade de Dados**
igc-sql.igc.isi.pt	63.9 MB
Enviado	**Recebido**



Parceiro Comunicação	**Quantidade de Dados**
172.20.8.74	14.1 MB
Enviado	**Recebido**

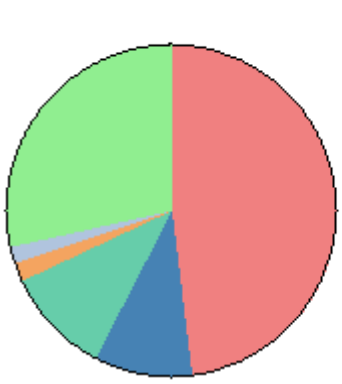


D.6 SRV/014 – IGC-IIS (172.20.8.16)



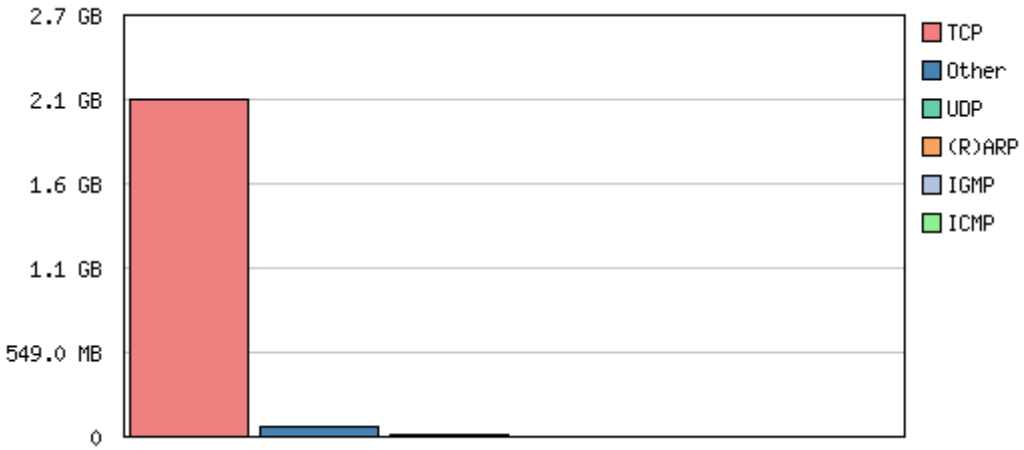
Unicast	67.7%
Broadcast	32.0%
Multicast	0.3%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SRV/014 – IGC-IIS (172.20.8.16)



<= 64 bytes	48.3%
64 to 128 bytes	9.8%
129 to 256 bytes	10.4%
257 to 512 bytes	1.9%
513 to 1024 bytes	1.9%
1025 to 1518 bytes	27.7%
> 1518 bytes	0.0%

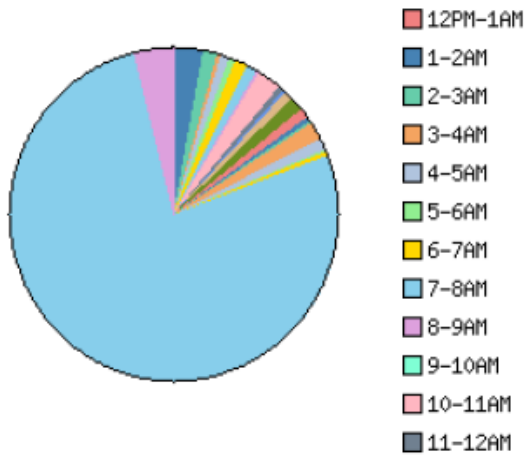
Figura 1 Distribuição do tamanho dos pacotes em SRV/014 – IGC-IIS (172.20.8.16)

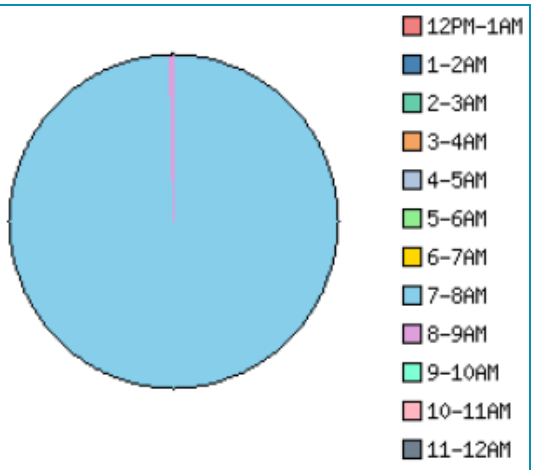


Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SRV/014 – IGC-IIS (172.20.8.16)

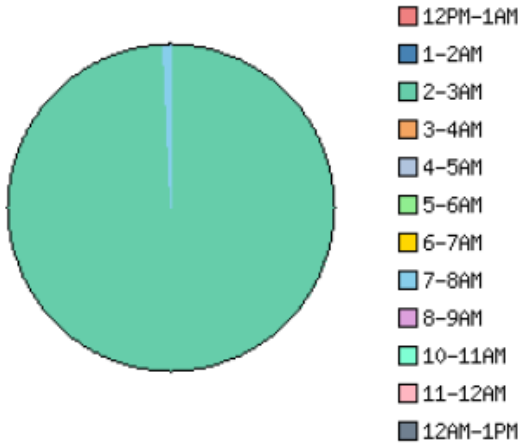
A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

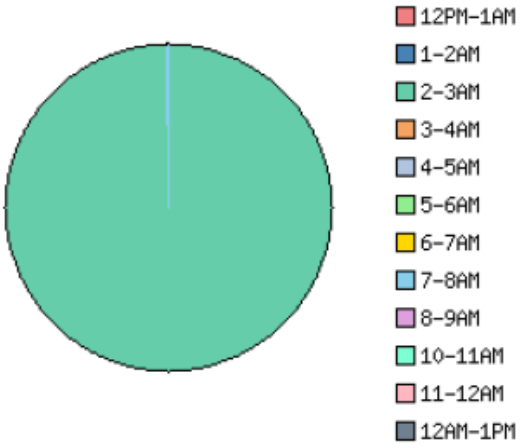
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	876.1 MB
Enviado	**Recebido**



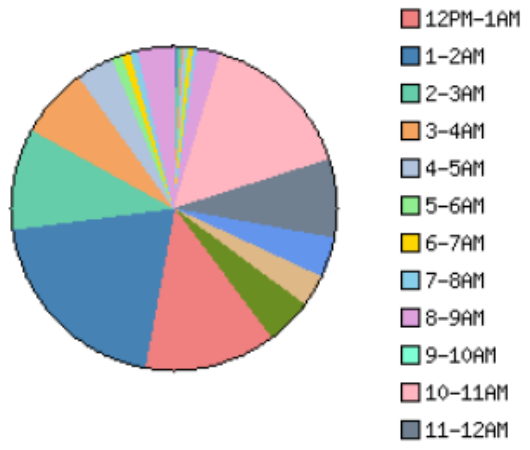


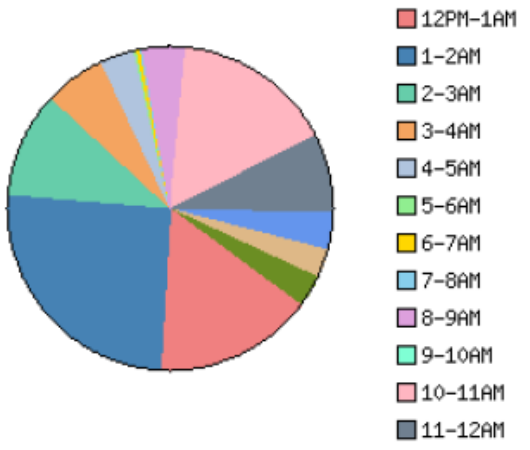
Parceiro Comunicação	**Quantidade de Dados**
igc-bck.igc.isi.pt	794.3 MB
Enviado	**Recebido**



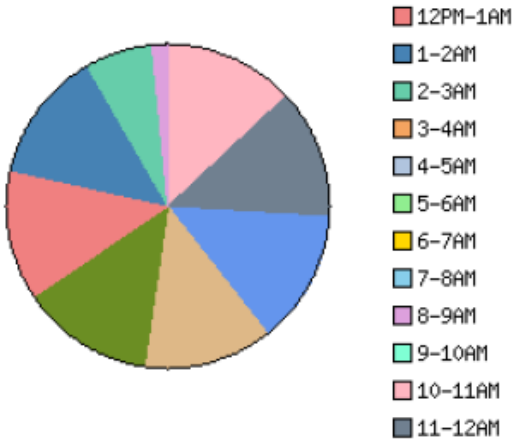


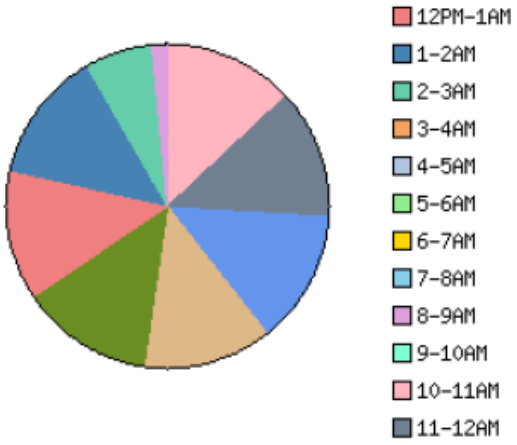
Parceiro Comunicação	**Quantidade de Dados**
igc-sql.igc.isi.pt	155.6 MB
Enviado	**Recebido**



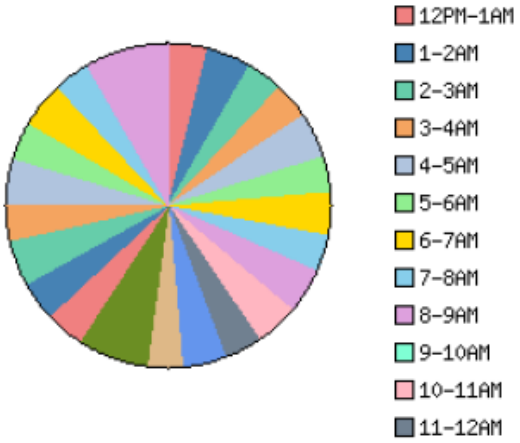


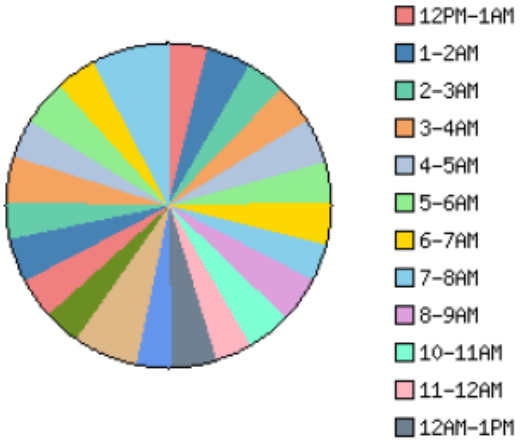
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.196	43.1 MB
Enviado	**Recebido**



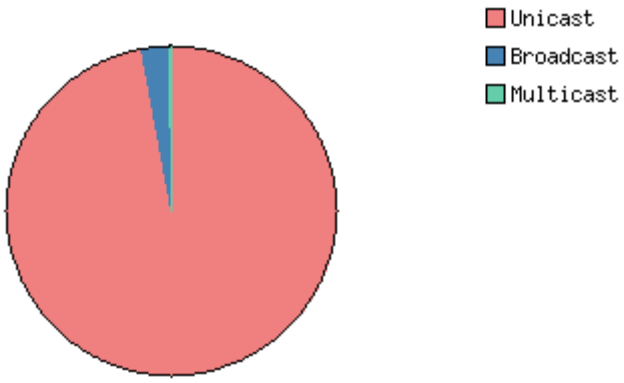


Parceiro Comunicação	**Quantidade de Dados**
172.20.8.68	19.0 MB
Enviado	**Recebido**





D.7 SSEXCH-07 (172.20.8.22)

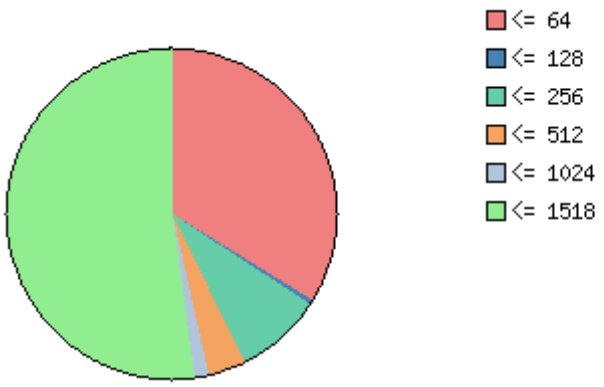


Unicast	97.0%
Broadcast	2.9%
Multicast	0.0%

Distribuição do tráfego em Unicast, Broadcast e Multicast em SSEXCH-07 (172.20.8.22)

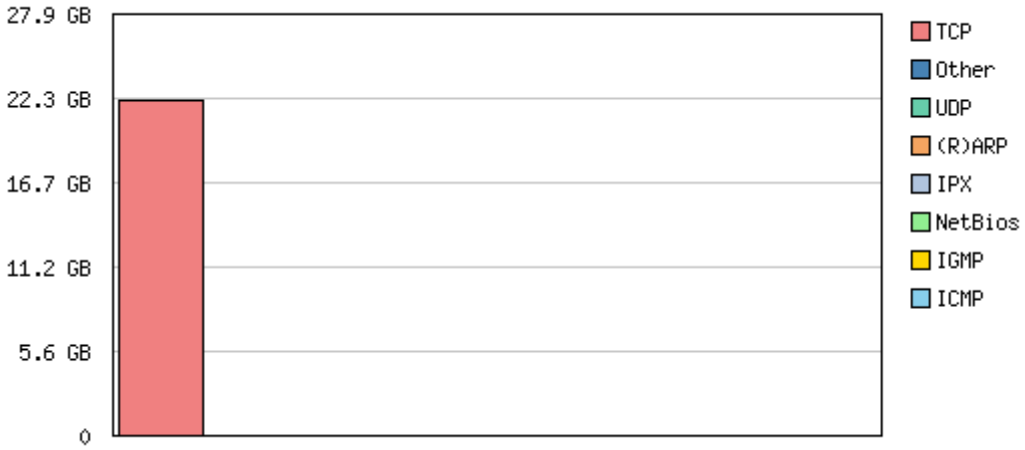
<= 64 bytes	33.9%
64 to 128 bytes	0.5%

Características dos fluxos de tráfego



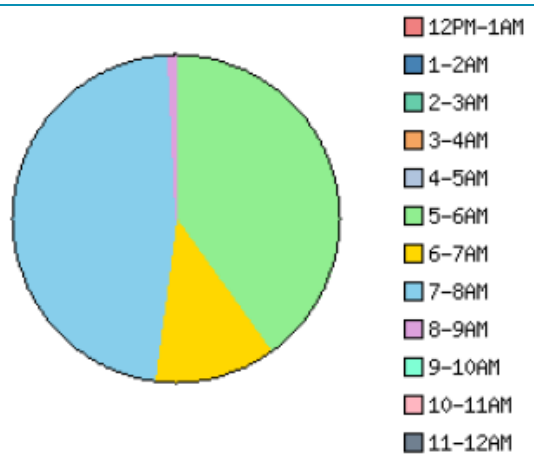
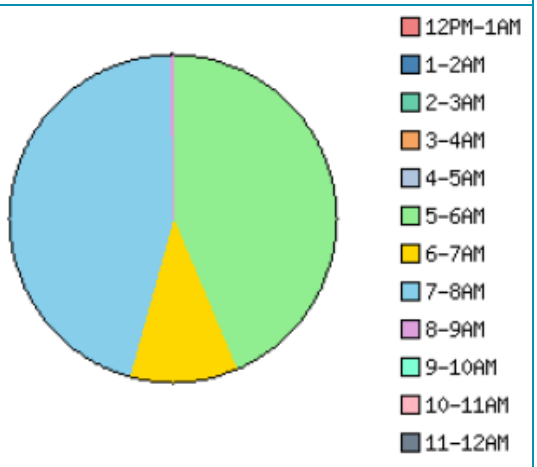
129 to 256 bytes	8.7%
257 to 512 bytes	3.9%
513 to 1024 bytes	1.4%
1025 to 1518 bytes	51.5%
> 1518 bytes	0.0%

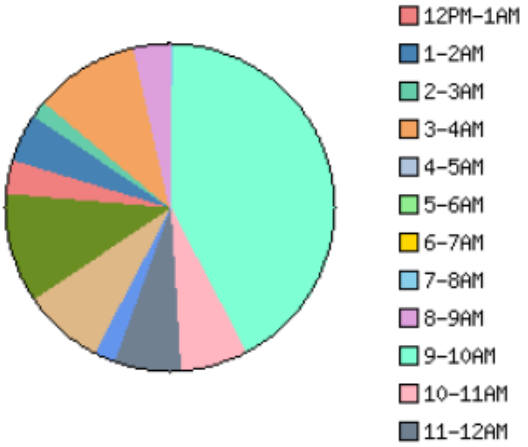
Distribuição do tamanho dos pacotes em SSEXCH-07(172.20.8.22)

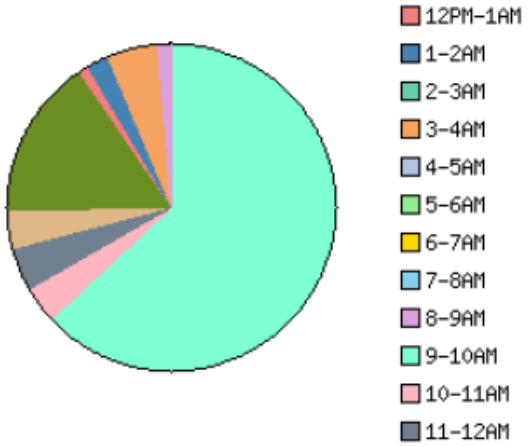


Distribuição do tráfego em TCP, UPD, (R)ARP e outros, em SSEXCH-07 (172.20.8.22)

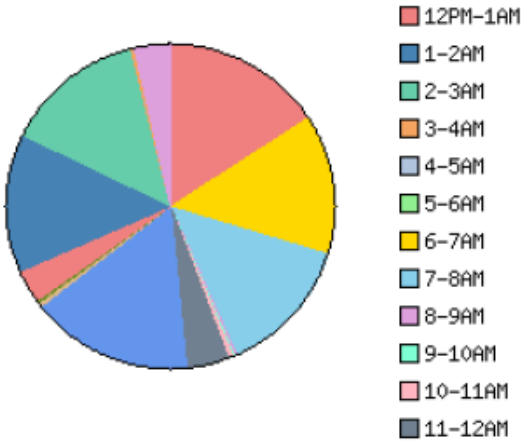
A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

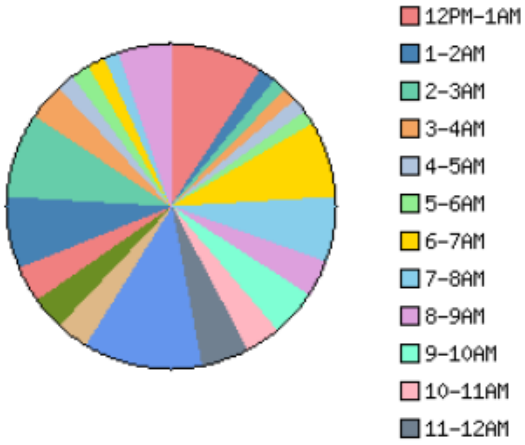
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.24	21.8 GB
Enviado	**Recebido**
	
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.184	28.7 MB
Enviado	**Recebido**



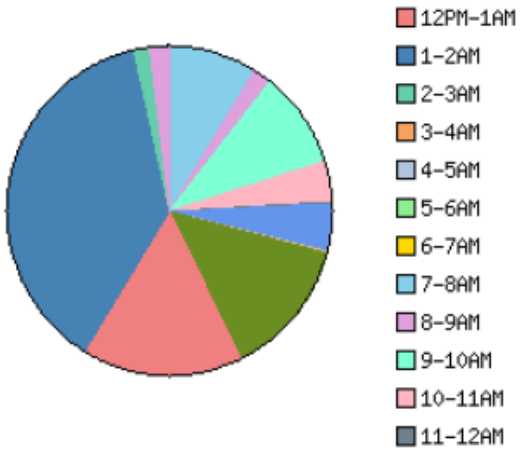


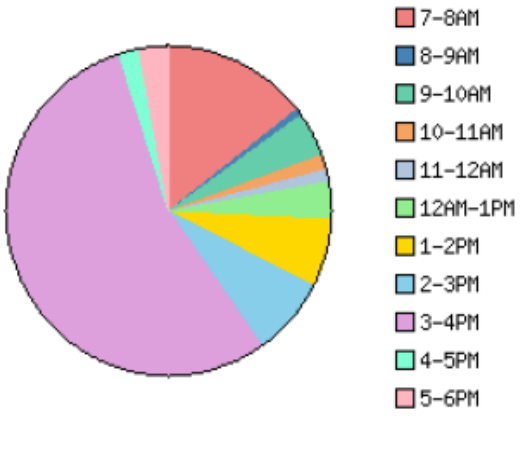
Parceiro Comunicação	**Quantidade de Dados**
ssexch-00-001	22.9 MB
Enviado	**Recebido**



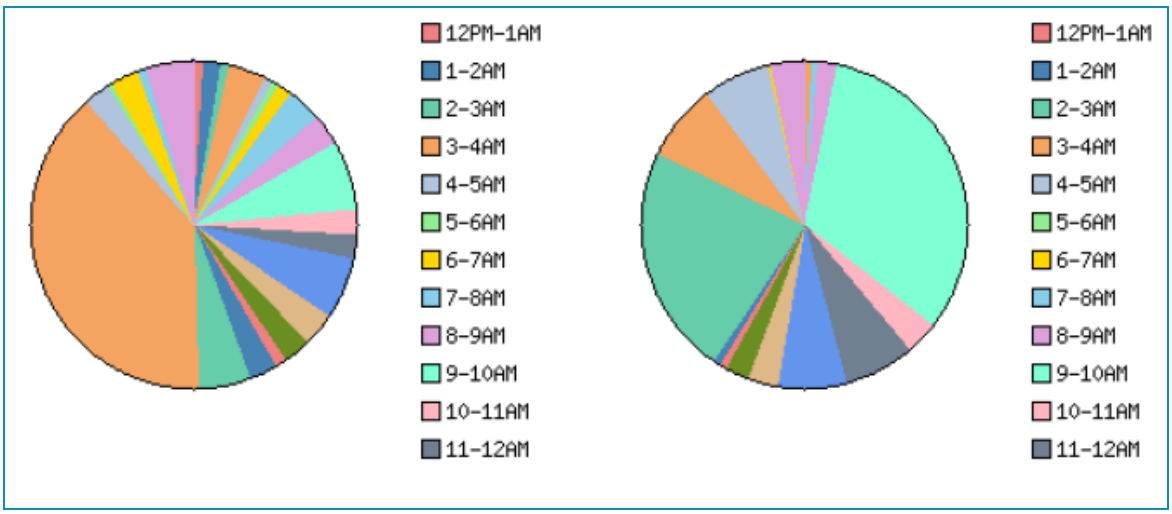


Parceiro Comunicação	**Quantidade de Dados**
172.20.8.74	22.2 MB
Enviado	**Recebido**

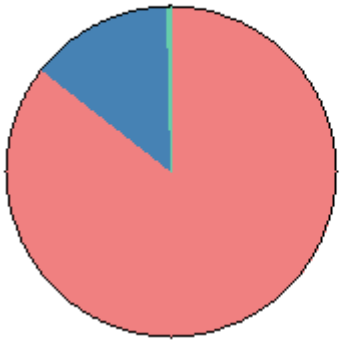




Parceiro Comunicação	**Quantidade de Dados**
172.20.8.68	11.8 MB
Enviado	**Recebido**

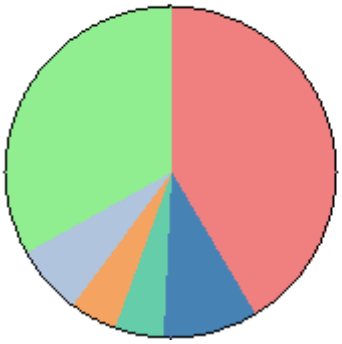


D.8 RTR/001 - Router Porto ISI (172.20.8.2)



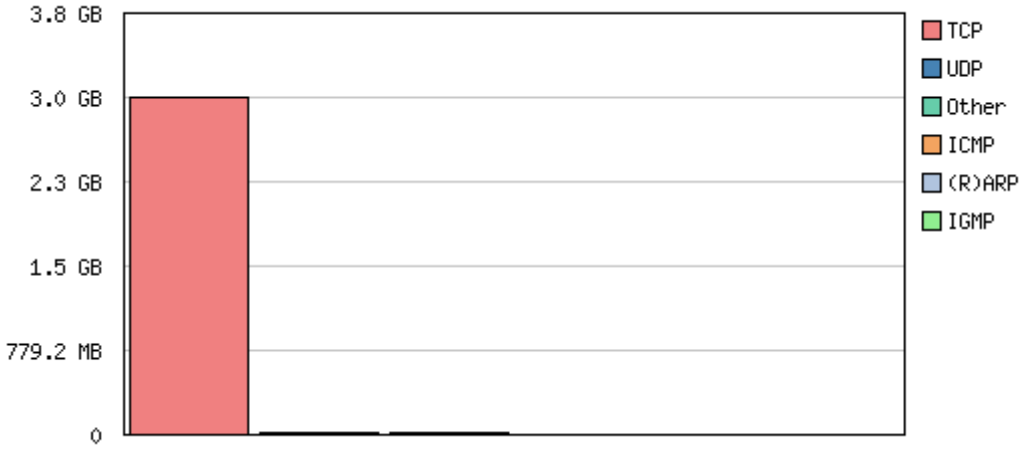
Unicast	85.8%
Broadcast	14.1%
Multicast	0.1%

Distribuição do tráfego em Unicast, Broadcast e Multicast no RTR/001 - *Router* Porto ISI (172.20.8.2)



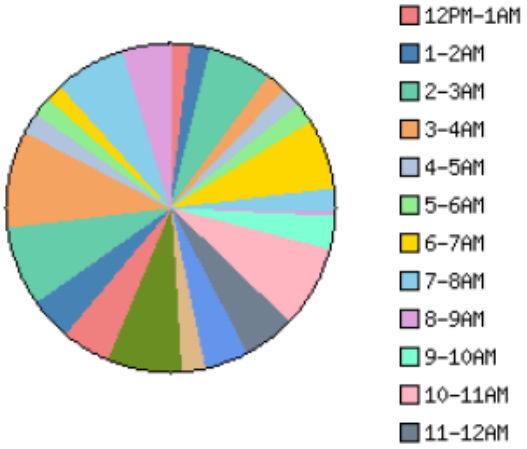
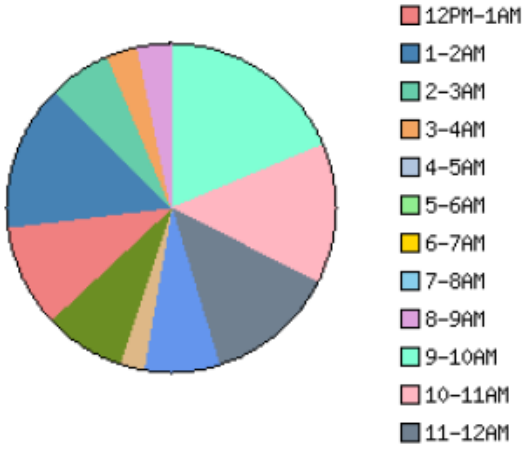
<= 64 bytes	41.5%
64 to 128 bytes	9.5%
129 to 256 bytes	5.0%
257 to 512 bytes	4.8%
513 to 1024 bytes	6.9%
1025 to 1518 bytes	32.3%
> 1518 bytes	0.0%

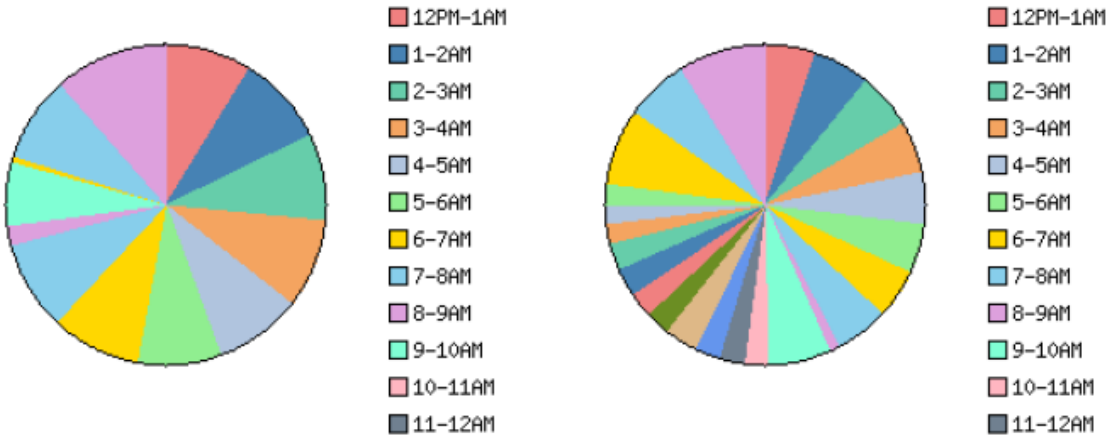
Distribuição do tamanho dos pacotes no RTR/001 - *Router* Porto ISI (172.20.8.2)



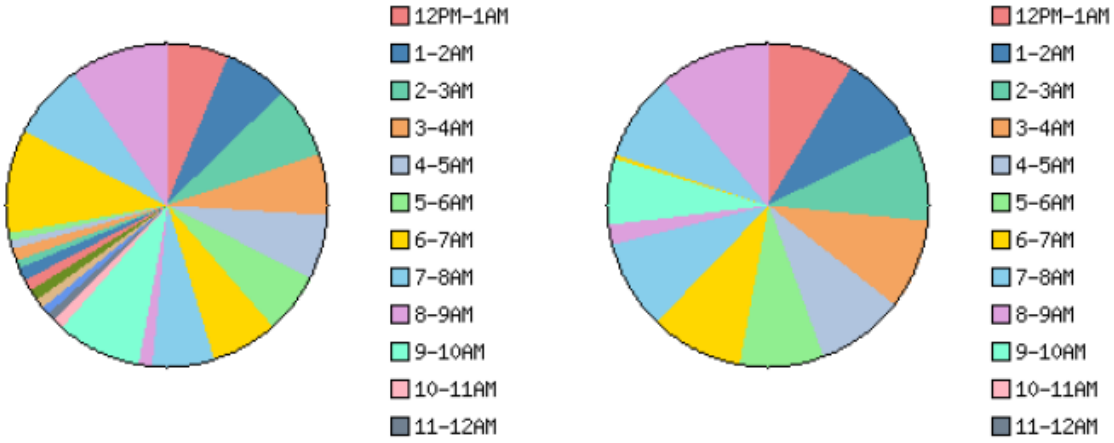
Distribuição do tráfego em TCP, UPD, (R)ARP e outros, no RTR/001 - *Router* Porto ISI (172.20.8.2)

A tabela seguinte mostra com quem se transfere maior quantidade de informação assim como a distribuição horária desse tráfego.

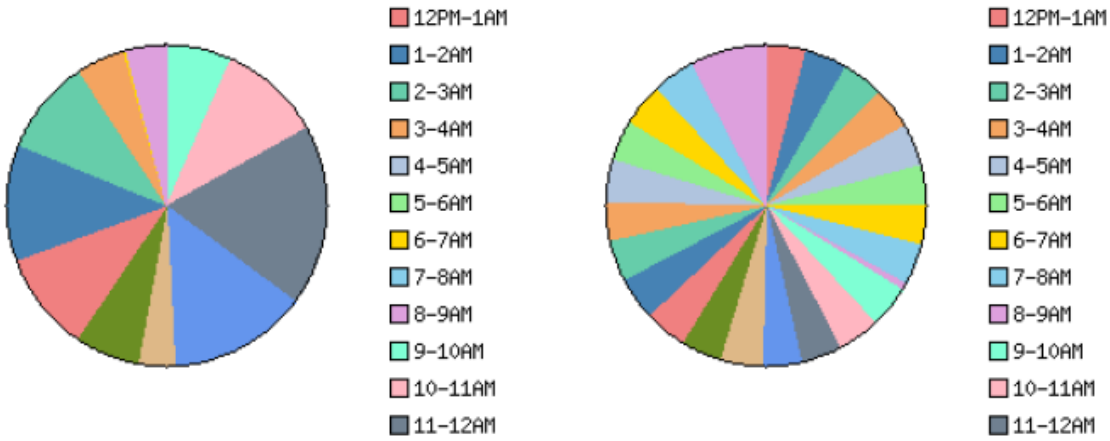
Parceiro Comunicação	**Quantidade de Dados**
igc-fw.igc.isi.pt	1.5 GB
Enviado	**Recebido**
	
Parceiro Comunicação	**Quantidade de Dados**
igc-fslx.igc.isi.pt	1.2 GB
Enviado	**Recebido**



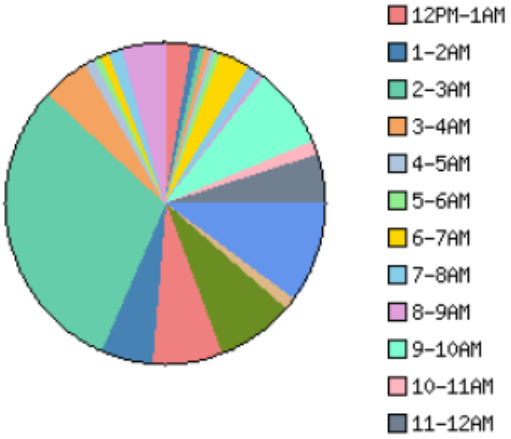
Parceiro Comunicação	**Quantidade de Dados**
igc-mon.igc.isi.pt	1.1 GB
Enviado	**Recebido**

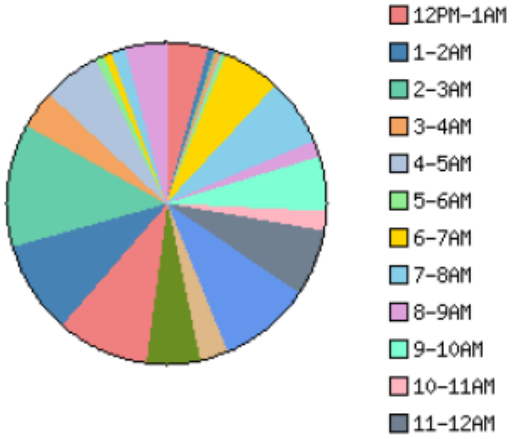


Parceiro Comunicação	**Quantidade de Dados**
172.20.8.1	198.2 MB
Enviado	**Recebido**

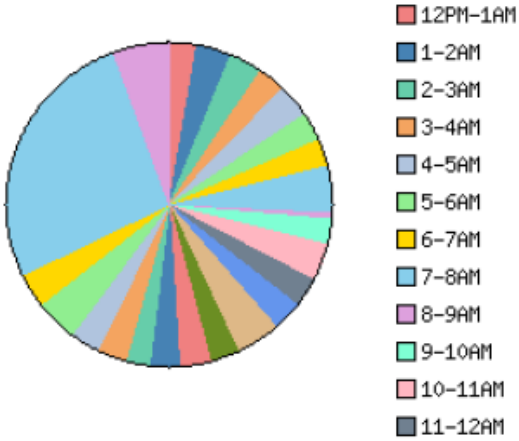


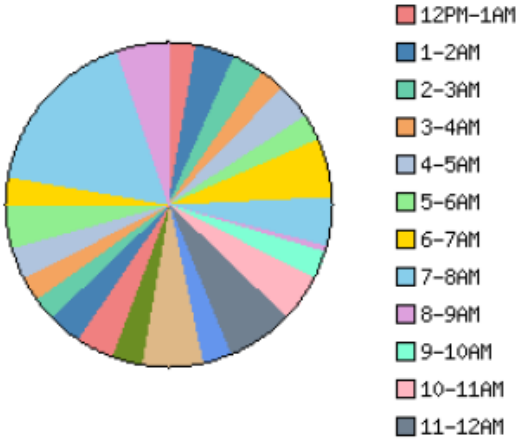
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.22	169.8 MB
Enviado	**Recebido**



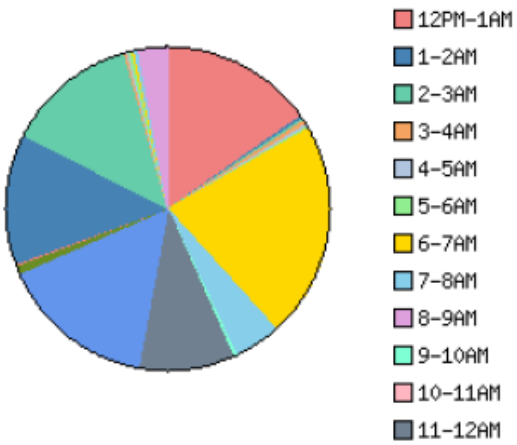


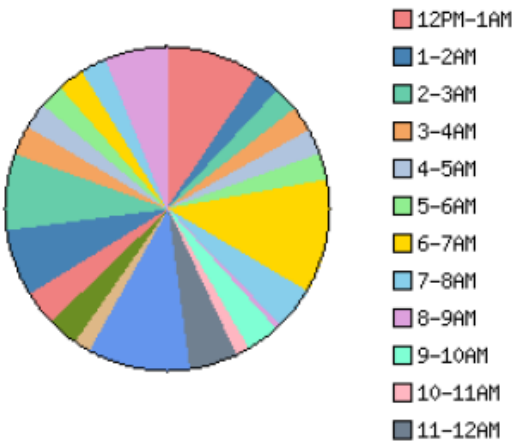
Parceiro Comunicação	**Quantidade de Dados**
172.20.8.10	70.4 MB
Enviado	**Recebido**





Parceiro Comunicação	**Quantidade de Dados**
ssexch-00-001	24.2 MB
Enviado	**Recebido**





Inbound

Inbound Link Utilization: 0%

Average Rate	Average Rate (bps)	% of Total
Microsoft-ds	80.6k	32%
BITS	68.9k	27%
HTTP	67.8k	27%
MSN-Messenger	17.0k	7%
DCOM	9983	4%
NetBIOS-IP	2594	1%
Default	2095	1%
WinMedia	1319	1%
DiscoveredPorts/TCP_Port_1025	1261	0%
SNMP	565	0%
All other classes	1855	1%

Outbound

Outbound Link Utilization: 8%

Average Rate	Average Rate (bps)	% of Total
HTTP	15.2k	39%
DCOM	4366	11%
Default	3388	9%
Protocol_886D	3260	8%
Microsoft-ds	2378	6%
DiscoveredPorts/TCP_Port_1025	2111	5%
NetBIOS-IP	2055	5%
MSN-Messenger	1844	5%
BITS	1501	4%
SNMP	799	2%
All other classes	1771	5%

Distribuição protocolar em termos de largura de banda requerida no acesso ao exterior no Porto

Inbound

Inbound Link Utilization: 0%

Total Bytes	Total Bytes	% of Total
Microsoft-ds	26.1G	32%
BITS	22.3G	27%
HTTP	21.9G	27%
MSN-Messenger	5.5G	7%
DCOM	3.2G	4%
NetBIOS-IP	839.2M	1%
Default	677.9M	1%
WinMedia	426.8M	1%
DiscoveredPorts/TCP_Port_1025	408.0M	0%
SNMP	182.7M	0%
All other classes	599.6M	1%

Outbound

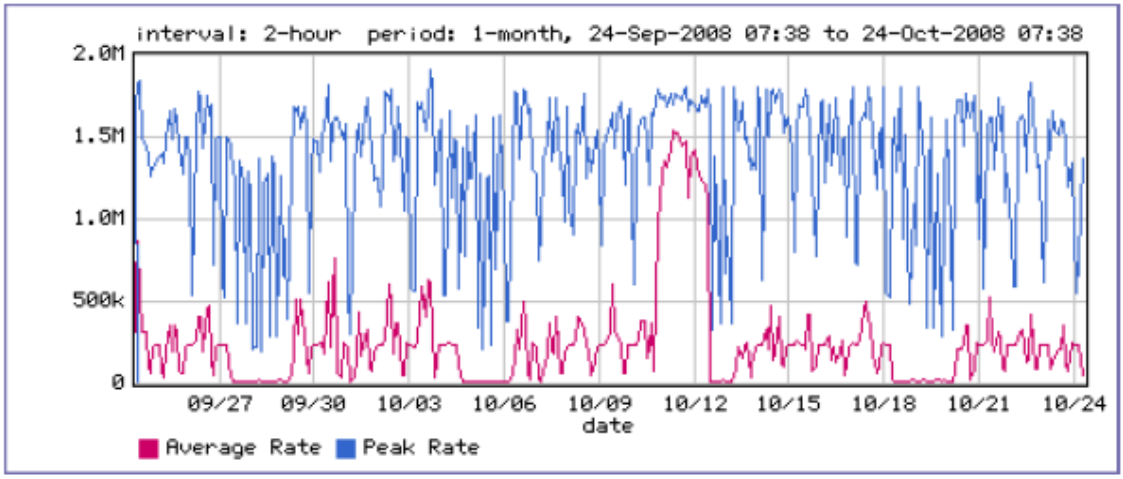
Outbound Link Utilization: 8%

Total Bytes	Total Bytes	% of Total
HTTP	4.9G	39%
DCOM	1.4G	11%
Default	1.1G	9%
Protocol_886D	1.1G	8%
Microsoft-ds	769.5M	6%
DiscoveredPorts/TCP_Port_1025	682.9M	5%
NetBIOS-IP	665.1M	5%
MSN-Messenger	596.5M	5%
BITS	485.6M	4%
SNMP	258.6M	2%
All other classes	572.3M	5%

Distribuição protocolar em termos de quantidades de tráfego de acesso ao exterior no Porto

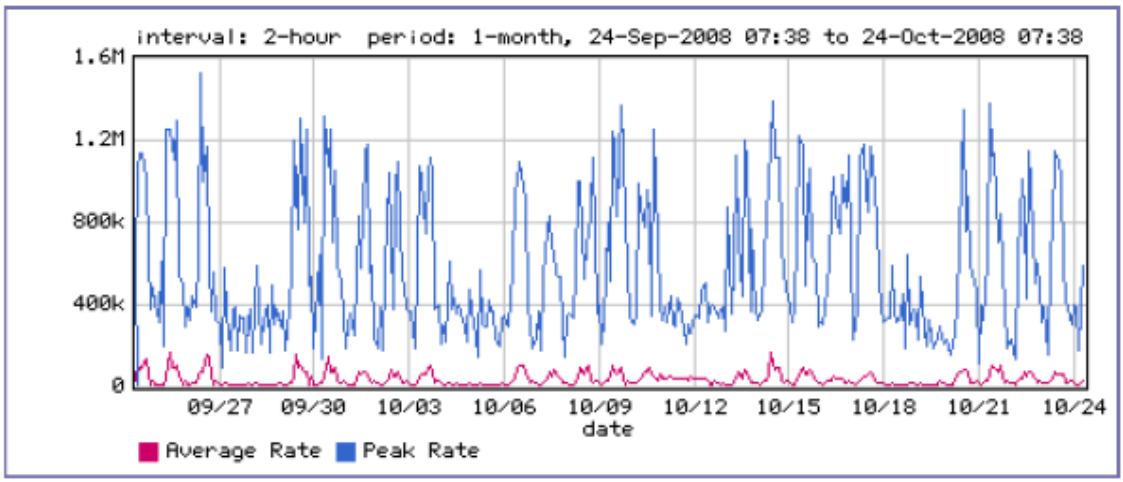
Inbound

Utilization



Outbound

Utilization



Anexo C

Políticas de Grupo da Active Directory

Este anexo contém o resultado do levantamento das políticas de grupo actualmente em efeito no domínio "igc.isi.pt".

C.1 CD

Nome: CD

Grupos em que é aplicada: CD

Data Criação: 23/11/2005

Data Modificação: 1/8/2008

ID: {A086E215-E105-47A3-82F6-C808AE2DAF7C}

Logon Script:

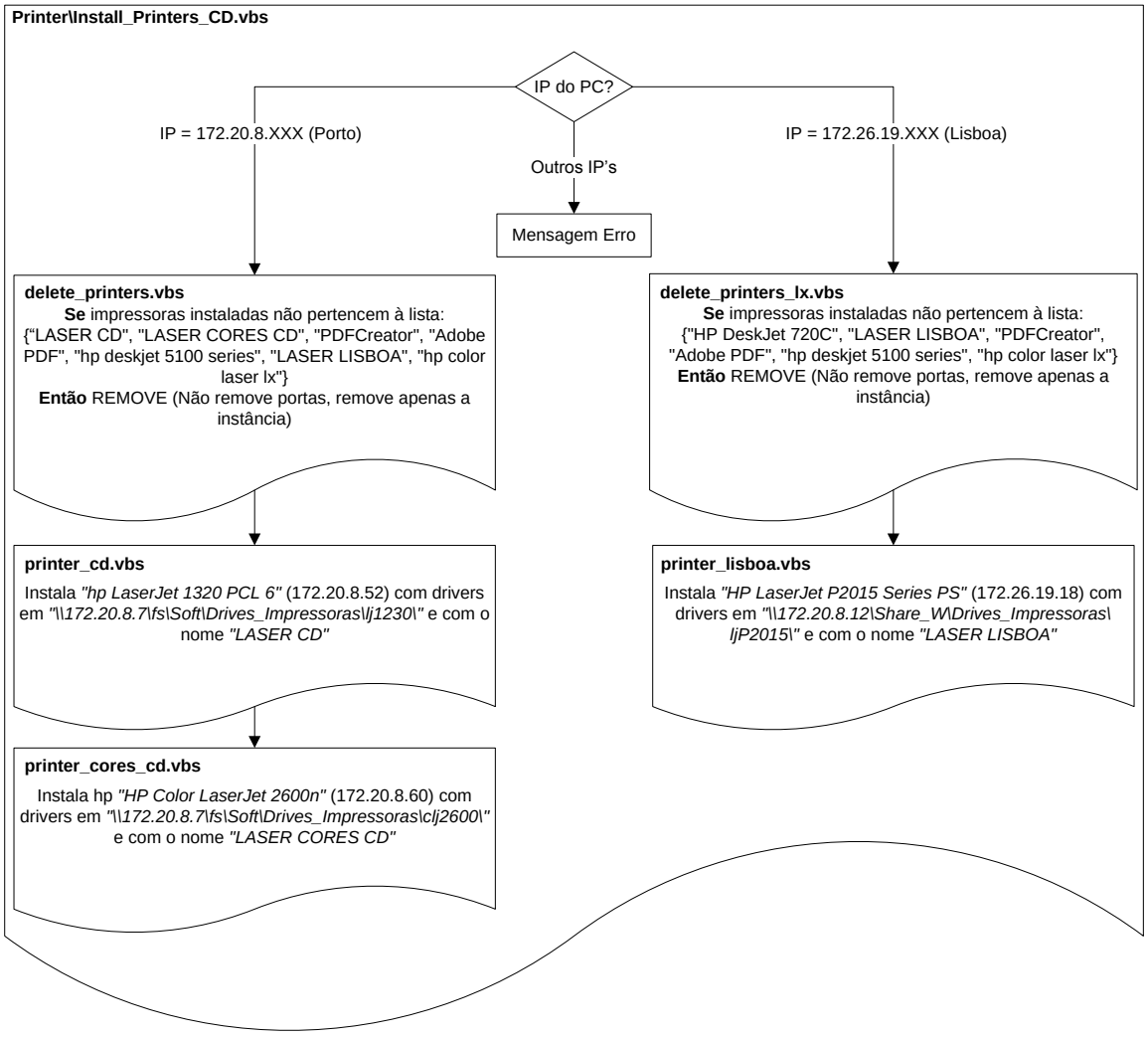


Figura 79 Fluxograma do Logon Script da política CD

C.2 DAG

Nome: DAG
Grupos em que é aplicada: DAGSI
Data Criação: 7/10/2005
Data Modificação: 28/3/2008
ID: {20C0BF69-977C-469B-843D-ED0FF62D7EF0}
Logon Script:

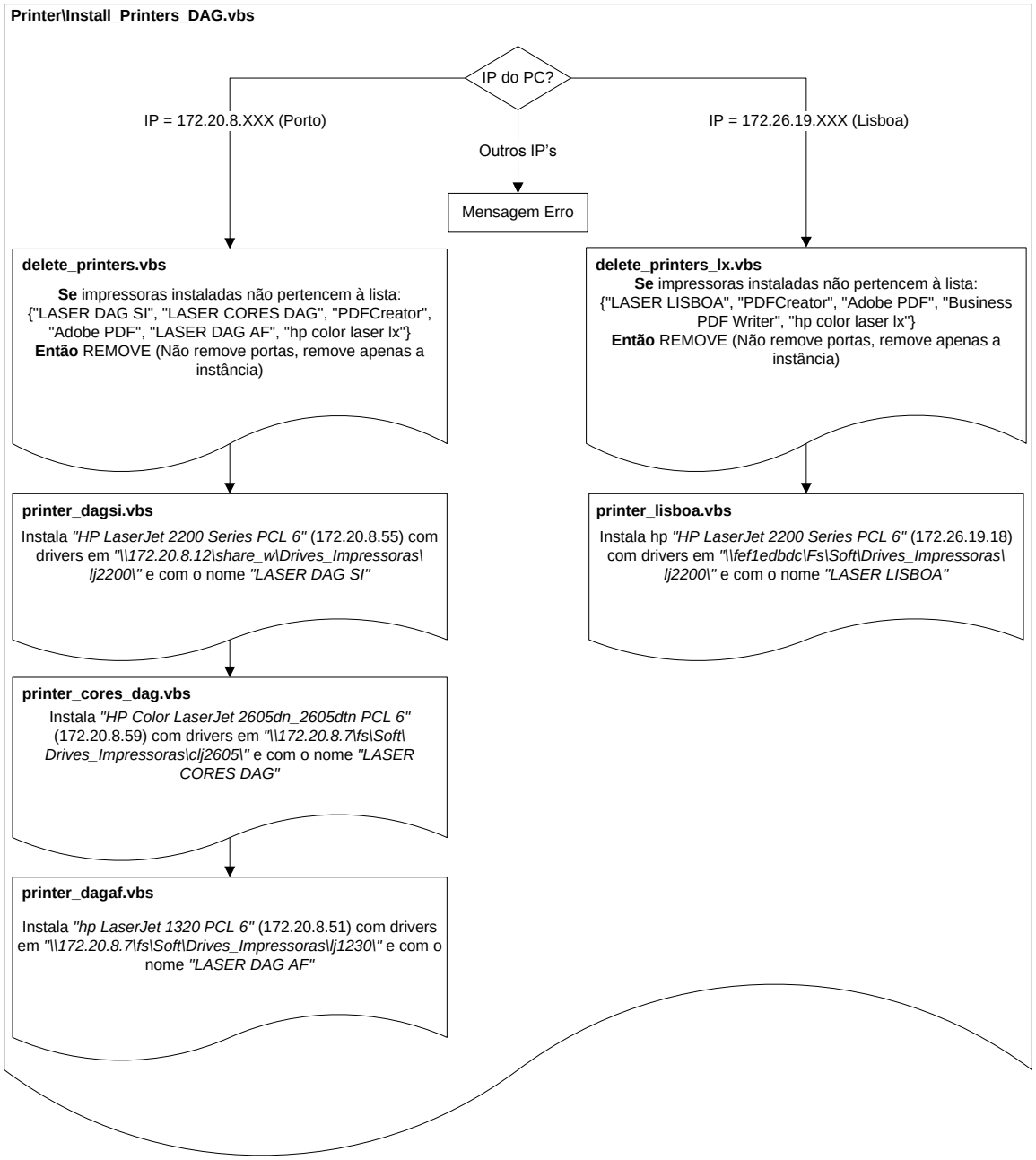
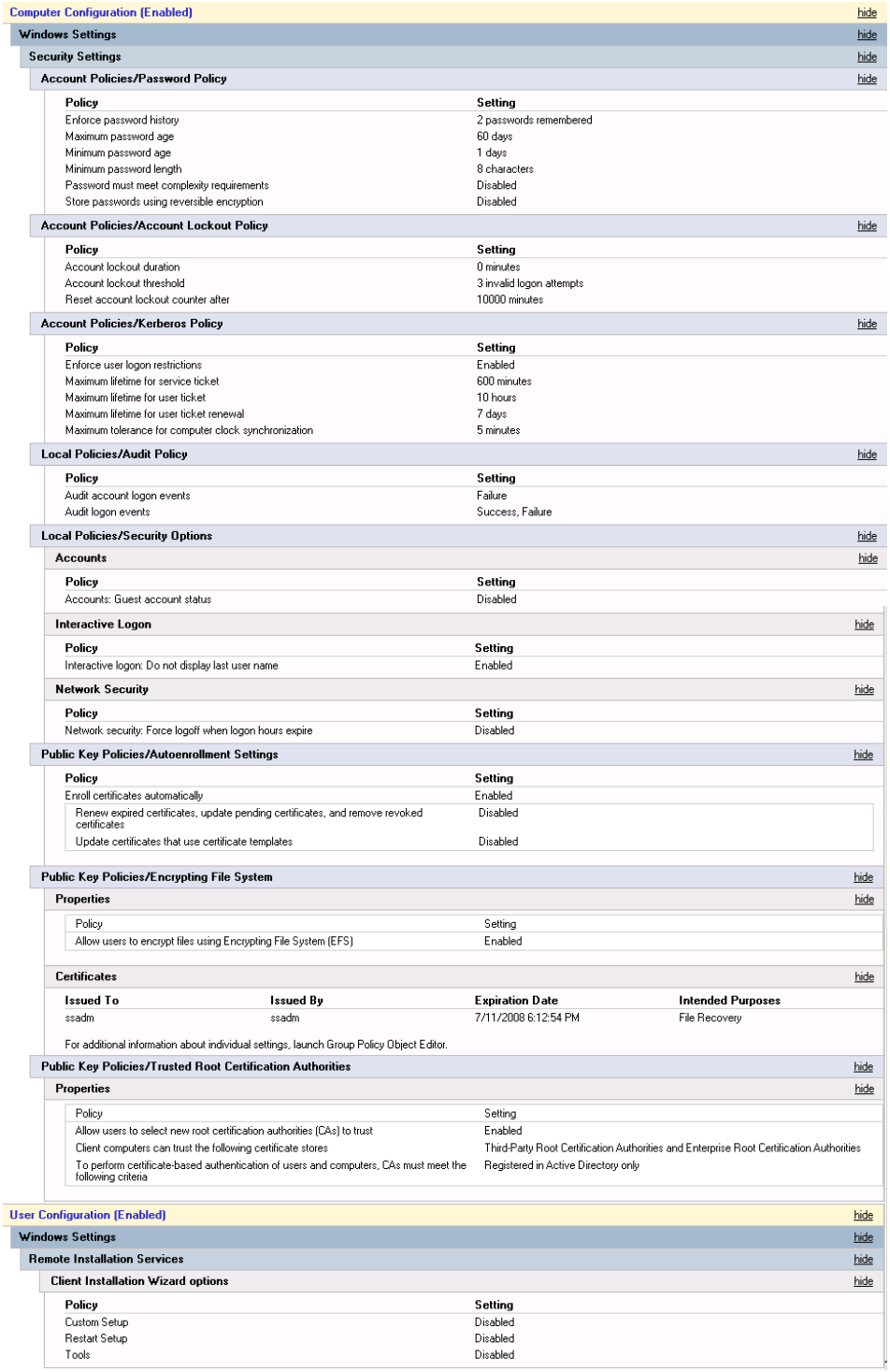


Figura 80 Fluxograma do Logon Script da política DAG

C.3 *Default Domain Policy*

Nome: Default Domain Policy
Grupos em que é aplicada: Authenticated Users
Data Criação: 12/7/2005
Data Modificação: 26/10/2006
ID: {31B2F340-016D-11D2-945F-00C04FB984F9}
Definições:



Computer Configuration (Enabled) hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	2 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout duration	0 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	10000 minutes

Account Policies/Kerberos Policy hide

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy hide

Policy	Setting
Audit account logon events	Failure
Audit logon events	Success, Failure

Local Policies/Security Options hide

Accounts hide

Policy	Setting
Accounts: Guest account status	Disabled

Interactive Logon hide

Policy	Setting
Interactive logon: Do not display last user name	Enabled

Network Security hide

Policy	Setting
Network security: Force logoff when logon hours expire	Disabled

Public Key Policies/Autoenrollment Settings hide

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Public Key Policies/Encrypting File System hide

Properties hide

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Certificates hide

Issued To	Issued By	Expiration Date	Intended Purposes
ssadm	ssadm	7/11/2008 6:12:54 PM	File Recovery

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities hide

Properties hide

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and computers, CAs must meet the following criteria	Registered in Active Directory only

User Configuration (Enabled) hide

Windows Settings hide

Remote Installation Services hide

Client Installation Wizard options hide

Policy	Setting
Custom Setup	Disabled
Restart Setup	Disabled
Tools	Disabled

Figura 81 Definições de segurança da política Default Domain

C.4 DEPC

Nome: DEPC
Grupos em que é aplicada: DEPC
Data Criação: 28/10/2005
Data Modificação: 26/03/2008
ID: {F1E827C4-3C5C-492E-889C-346A2EF832E6}
Logon Script:

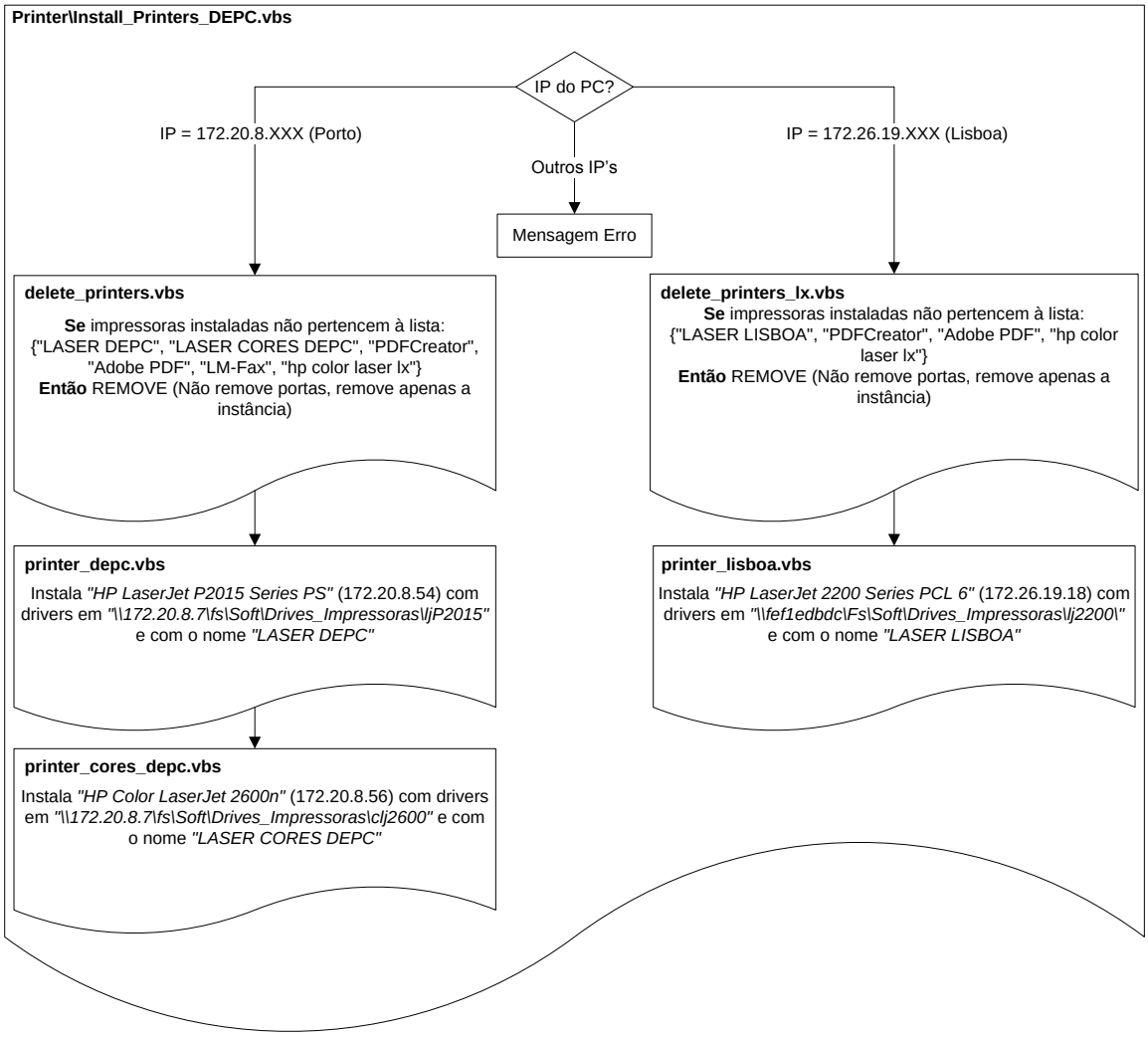


Figura 82 Fluxograma do Logon Script da política DEPC

C.5 DEPC

Nome: DI

Grupos em que é aplicada: DI

Data Criação: 28/10/2005

Data Modificação: 26/03/2008

ID: {FA416692-3213-4D03-B50C-27D43A44901A}

Logon Script:

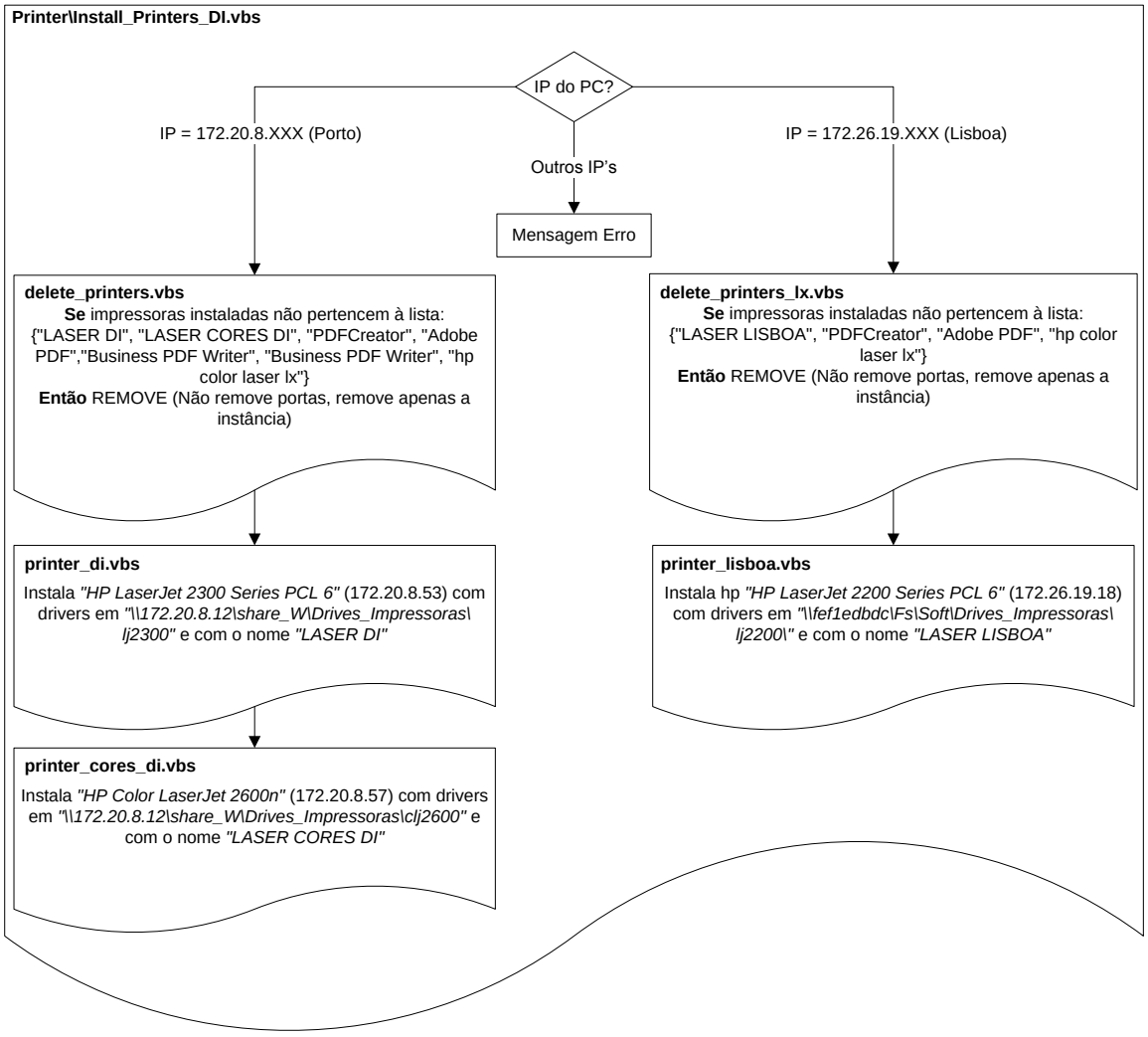


Figura 83 Fluxograma do Logon Script da política DI

C.6 Unat7

Nome: Unat7
Grupos em que é aplicada: Authenticated Users
Data Criação: 03/10/2008
Data Modificação: 3/10/2008
ID: {EE94226F-DE18-4D5A-9B95-1C9B22D6FDFC}
Definições:

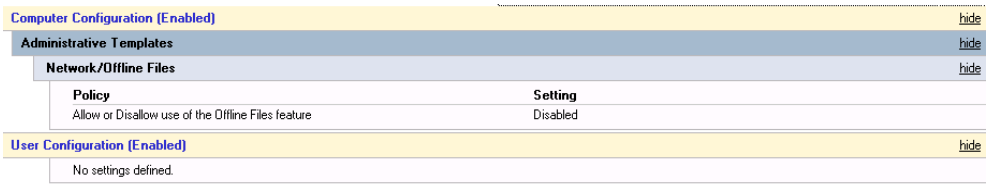


Figura 84 Definições de segurança da política Unat7

C.7 Geral

Nome: GERAL
Grupos em que é aplicada: CD, DAF, DEPC, DI, DSI
Data Criação: 01/09/2005
Data Modificação: 30/11/2007
ID: {CC70B1C0-2ABB-4F56-837D-90B79289B863}
Definições:

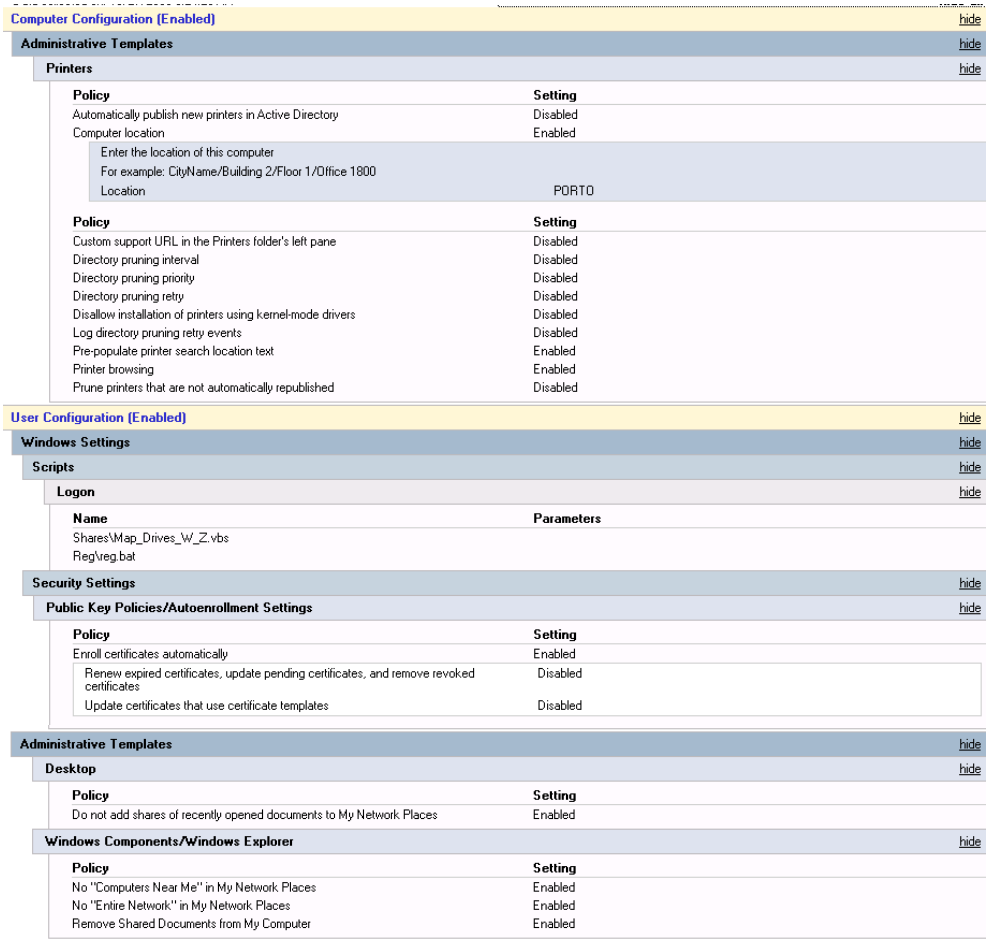


Figura 85 Definições de segurança da política GERAL

Shares\Map_Drives_W_Z.vbs

- Cria unidade de rede W: correspondente ao caminho "\\172.20.8.12\Share_W" com a descrição " Pasta de Software" e o atalho correspondente no Ambiente de Trabalho
- Cria unidade de rede Z: correspondente ao caminho "\\172.20.8.12\Share_Z" com a descrição " Pasta Partilhada" e o atalho correspondente no Ambiente de Trabalho

Reg\reg.bat

- Regista as definições do ficheiro igc.reg no registo das máquinas;
- Copia \\igc-fs\Share_W\ActiveX_Intranet\BlobMgmt.dll para c:\windows\BlobMgmt.dll;
- Regista c:\windows\BlobMgmt.dll.

C.8 IE7 Policy

Nome: IE7 policy
Grupos em que é aplicada: Authenticated Users
Data Criação: 03/10/2008
Data Modificação: 03/10/2008
ID: {CE6A6990-8C96-4FAC-A491-14C2FAE61425}
Definições:

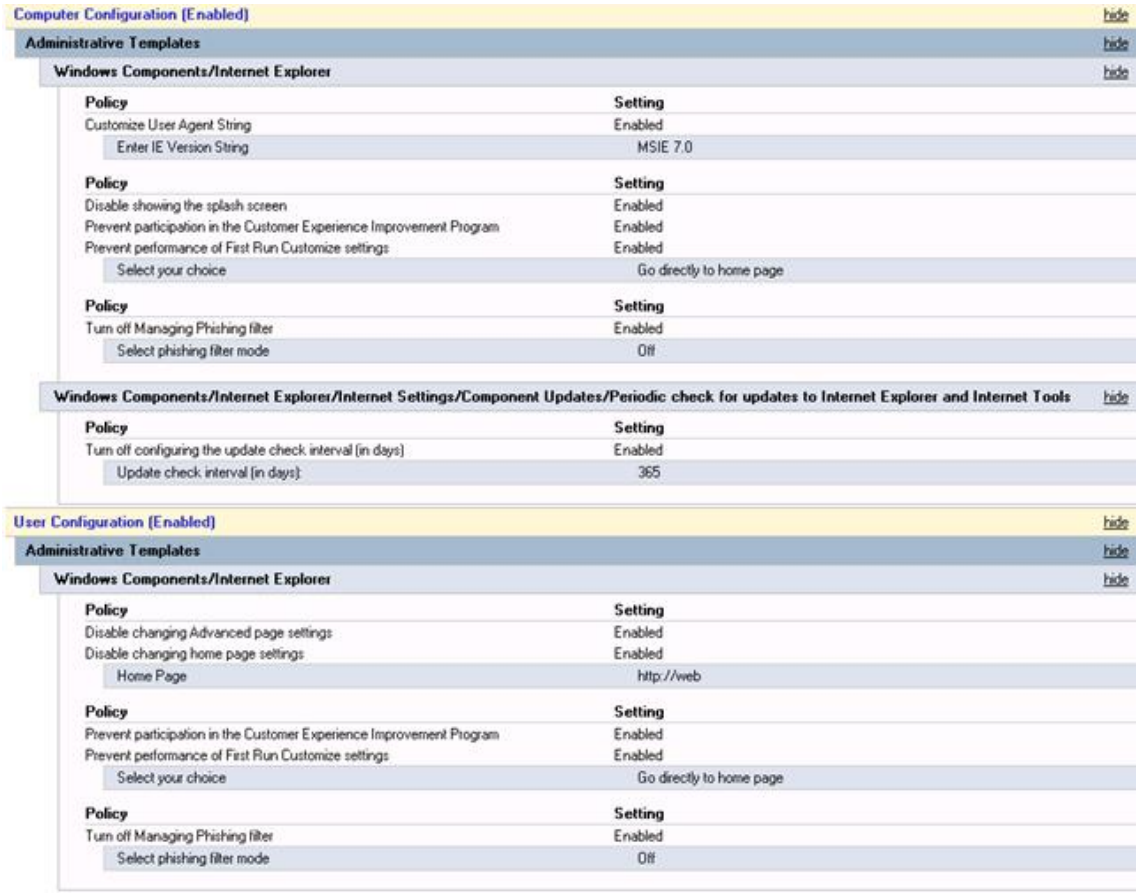


Figura 86 Definições de segurança da política IE7 policy

C.9 Lisboa

Nome: LISBOA
Grupos em que é aplicada: LX
Data Criação: 12/04/2007
Data Modificação: 12/04/2007
ID: {62D427E6-9836-4A18-99F2-69AF311B5E9C}
Logon Script:

Shares\Map_Drive_Y_LX.vbs: cria unidade de rede Y: correspondente ao caminho "\\172.26.19.5\Share_Y" com a descrição "Pasta Pessoal" e o atalho correspondente no Ambiente de Trabalho

C.10 NetOP_LX

Nome: NetOP_LX
Grupos em que é aplicada: LX
Data Criação: 12/09/2005
Data Modificação: 27/06/2007
ID: {DAE059D2-BE7F-4FCB-89AB-FDDD6F360B30}
Logon Script:
netopLX.bat: instala NetOP a partir de \\172.26.19.5\install\Netop\setup

C.11 NetOP_OPO

Nome: NetOP_OPO
Grupos em que é aplicada: PT_Users
Data Criação: 09/09/2005
Data Modificação: 7/03/2008
ID: {B3ED4B3F-2CBF-4F19-B4AF-2755E9542B6D}
Logon Script:
netop.bat: instala NetOP a partir de \\igc-fs\Share_W\NetOP\setup

C.12 Porto

Nome: PORTO
Grupos em que é aplicada: PT
Data Criação: 12/04/2007
Data Modificação: 12/04/2007
ID: {9B2A7297-7F50-4B36-8E20-7C46-A82B22DB}
Logon Script:
Shares\Map_Drive_Y_PT.vbs – cria unidade de rede Y: correspondente ao caminho \\172.20.8.12\Share_Y" com a descrição "Pasta Pessoal" e o atalho correspondente no Ambiente de Trabalho

Anexo D

Detalhes dos Custos Envolvidos na Implementação

Este anexo contém os detalhes dos custos associados à implementação da infra-estrutura proposta, face à necessidade de aquisição de novos servidores, *routers*, *software* e contratação de serviços a ISP's.

D.1 Servidores

De seguida é indicado o custo aproximado, sem IVA, obtido através de uma consulta de mercado, para a aquisição dos servidores necessários:

- **MON** – Características de referência:
  - Processador: 1 X Xeon Quad Core E5420 2.5Ghz /2x6MB Cache 1333Mhz FSB
  - Memória: 4GB Single Rank DDR2 Memory (2x2GB)
  - Discos: 2 x 146GB 15k SAS Hard Drive
  - Interface de rede: duplo
  - Fonte de alimentação: redundante
  - Assistência: Next Business Day (NBD)
  - **PREÇO APROXIMADO: 2300€**

- **DC1** – Características de referência:
  - Processador: 1 X Xeon Quad Core E5420 2.5Ghz /2x6MB Cache 1333Mhz FSB
  - Memória: 4GB Single Rank DDR2 Memory (2x2GB)
  - Discos: 2 x 146GB 15k SAS Hard Drive
  - Interface de rede: duplo
  - Fonte de alimentação: redundante

- Assistência: Next Business Day (NBD)
- **PREÇO APROXIMADO: 2300€**

- **TUX** – Características de referência:
  - Processador: 1 X Xeon Quad Core E5420 2.5Ghz /2x6MB Cache 1333Mhz FSB
  - Memória: 4GB Single Rank DDR2 Memory (2x2GB)
  - Discos: 2 x 146GB 15k SAS Hard Drive
  - Interface de rede: duplo
  - Fonte de alimentação: redundante
  - Assistência: Next Business Day (NBD)
  - **PREÇO APROXIMADO: 2300€**

- **EXCHANGE** – Características de referência:
  - Processador: 1 X Xeon Quad Core E5450 3.0Ghz /2x6MB Cache 1333Mhz FSB
  - Memória: 8GB Single Rank DDR2 Memory (4x2GB)
  - Discos: 6 x 146GB 15k SAS Hard Drive
  - Interface de rede: duplo
  - Fonte de alimentação: redundante
  - Assistência: 4 Horas
  - **PREÇO APROXIMADO: 4000€**

- **DRS** – Características de referência:
  - Processador: 2 X Xeon Quad Core E5450 3.0Ghz /2x6MB Cache 1333Mhz FSB
  - Memória: 16GB Single Rank DDR2 Memory (4x4GB)
  - Discos: 6 x 1TB 7.2k SAS Hard Drive
  - Interface de rede: duplo
  - Fonte de alimentação: redundante
  - Assistência: Next Business Day (NBD)
  - **PREÇO APROXIMADO: 5600€**

D.2 Routers

De seguida é indicado o custo aproximado, sem IVA, obtido através de uma consulta de mercado, para a aquisição dos *routers* necessários para os vários sites, sendo apresentadas 3 gamas de modelos, mínimo, médio e melhor, que diferem a nível de preço, desempenho e de expansibilidade.

Porto:

Mínimo	CISCO2811 (AC PWR,2FE,4HWICs,2PVDMs,1NME,2AIMS,IP BASE,64F/256D)	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**3400 €**
Médio	CISCO2821 (AC PWR,2GE,4HWICs,3PVDM,1NME-X,2AIM,IP BASE,64F/256D)	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**4100 €**
Melhor	CISCO3825 (AC PWR, 2GE,1SFP, 2NME, 4HWIC, IP Base, 64F/256D)	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	S382AISK9-12421 - Cisco 3825 ADVANCED IP SERVICES	
	Total Aproximado	**7500 €**

Lisboa:

Mínimo	CISCO1801/K9 - ADSL/POTS Router with Firewall/IDS and IPSEC 3DES	
	Total Aproximado	**800 €**
Médio	CISCO2811 (AC PWR,2FE,4HWICs,2PVDMs,1NME,2AIMS,IP BASE,64F/256D)	
	HWIC-1ADSL - 1-port ADSLoPOTS HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**2700 €**
Melhor	CISCO2821 (AC PWR,2GE,4HWICs,3PVDM,1NME-X,2AIM,IP BASE,64F/256D)	
	HWIC-1ADSL - 1-port ADSLoPOTS HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**3500 €**

DRS:

Mínimo	CISCO1811/K9 - Dual Ethernet Security Router with V.92 Modem *Backup*	
	Total Aproximado	**700 €**
Médio	CISCO2811 (AC PWR,2FE,4HWICs,2PVDMs,1NME,2AIMS,IP BASE,64F/256D)	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**2700 €**
Melhor	CISCO2821 (AC PWR,2GE,4HWICs,3PVDM,1NME-X,2AIM,IP BASE,64F/256D)	
	HWIC-1FE - 1-port 10/100 Routed Port HWIC	
	S28NAISK9-12421 - Cisco 2800 ADVANCED IP SERVICES	
	Total Aproximado	**3500 €**

D.3 Software

De seguida é indicado o custo aproximado, sem IVA, obtido através de uma consulta de mercado, para a aquisição do licenciamento do *software* necessário:

- **Licenças para Sistema Operativo Microsoft Windows 2003 R2**
  - Novos Sistemas:
    - DC1
    - EXCHANGE
    - MON
    - DCD
    - FSD
    - EXCHANGED
    - TRADERD
    - SQLD
    - IISD
  - **Custo Total: 600€ x 9 = 5400€**
- **Licenças para servidor de E-mail Microsoft Exchange 2007**
  - Sistemas:
    - EXCHANGE
    - EXCHANGED
  - Licença para 40 utilizadores
  - **Custo Total: 600€ x 2 + 55€ x 40 = 3400€**

D.4 Serviços dos ISP's

De seguida são indicados os custos aproximados, para os vários cenários avaliados, obtidos através de uma consulta de mercado a vários fornecedores, para a contratação dos circuitos de interligação dos vários sites e acesso à Internet. Nas tabelas apresentadas, serão utilizadas as seguintes abreviaturas:

- **CD** – Circuito Dedicado
- **DSL** – Ligação baseada na tecnologia Digital Subscriber Line (DSL), com taxas de contenção implícitas

Algumas notas prévias relativamente aos valores apresentados:

- Nos casos em que os ISP's não facultaram os preços de *Housing* será utilizado um preço estimado de 200 €. Este valor será associado a um identificador denominado "H?";
- Nos casos em que os ISP's não facultaram os preços para uma ligação DSL em Lisboa serão utilizados os preços apresentados pelo ISP1, sendo esse valor associado a um identificador denominado "ISP1";
- Nos casos em que os ISP's não facultaram os preços para o serviço de E mail *Relay* usou-se um valor estimado de 100 € para a mensalidade deste servido, sendo essa informação identificada com "MR?";
- Todos os preços apresentados não incluem o IVA.

Cenário A1H

- Ligação Internet Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação Internet Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
- Ligação Internet *Housing*: 4 Mbit/s (down) / 4 Mbit/s (up)

ISP1	ISP2	ISP3	ISP4
1) CD Porto (4/4 Mbit/s): 2509€ 2) CD Porto (6/6 Mbit/s): 3458€ 3) CD Porto (10/10 Mbit/s): 5358€ DSL Lisboa (16/1 Mbit/s): 73€ CD *Housing* (5/5 Mbit/s): 737€ Housing 3 U's: 249€ E-Mail *Relay*: 214,9€	1) CD Porto (4/4 Mbit/s): 770€ 2) CD Porto (6/6 Mbit/s): 840€ 3) CD Porto (8/8 Mbit/s): 910€ 4) CD Porto (10/10 Mbit/s): 970€ DSL Lisboa (24/1 Mbit/s): 90€ Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: INCLUÍDO	1) CD Porto (4/4 Mbit/s): 936,54€ 2) CD Porto (6/6 Mbit/s): 1028,85€ 3) CD Porto (8/8 Mbit/s): 1121,15€ 4) CD Porto (10/10 Mbit/s): 1213,46€ DSL Lisboa (16/1 Mbit/s): 73€ (**ISP1**) Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)	CD Porto (10/10 Mbit/s): 1000€ DSL Lisboa (2/2 Mbit/s): 350€ Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)
Total: 3782,9€ (1) **Total: 4731,9€ (2) Total: 6631,9€ (3)**	**Total: 1060€ (1)** **Total: 1130€ (2)** **Total: 1200€ (3)** **Total: 1260€ (4)**	**Total: 1309,54€ (1)** **Total: 1401,85€ (2)** **Total: 1494,15€ (3)** **Total: 1586,46€ (4)**	**Total: 1650€**

Cenário A1L

- Ligação Internet Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação Internet Lisboa:
  - 4 Mbit/s (down) / 1 Mbit/s (up) (obriga deslocação física - ODF)
  - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente - PTR)

ISP1	ISP2	ISP3	ISP4
1) CD Porto (4/4 Mbit/s): 2509€ 2) CD Porto (6/6 Mbit/s): 3458€ 3) CD Porto (10/10 Mbit/s): 5358€ ODF) DSL Lisboa (16/1 Mbit/s): 73€ PTR) CD Lisboa (4/4 Mbit/s): 2509€ E-Mail *Relay*: 214,9€	1) CD Porto (4/4 Mbit/s): 770€ 2) CD Porto (6/6 Mbit/s): 840€ 3) CD Porto (8/8 Mbit/s): 910€ 4) CD Porto (10/10 Mbit/s): 970€ ODF) DSL Lisboa (24/1 Mbit/s): 90€ PTR) CD Lisboa (4/4 Mbit/s): 770€ E-Mail *Relay*: INCLUÍDO	1) CD Porto (4/4 Mbit/s): 936,54€ 2) CD Porto (6/6 Mbit/s): 1028,85€ 3) CD Porto (8/8 Mbit/s): 1121,15€ 4) CD Porto (10/10 Mbit/s): 1213,46€ ODF) DSL Lisboa (16/1 Mbit/s): 73€ (**ISP1**) PTR) CD Lisboa (4/4 Mbit/s): 936,54€ E-Mail *Relay*: 100€ (**MR?**)	Não foram fornecidas informações
Total: 2796,9€ (1/ODF) Total: 3745,9€ (2/ODF) **Total: 5645,9€ (3/ODF)** **Total: 5232,9€ (1/PTR) Total: 6181,9€ (2/PTR)** **Total: 8081,9€ (3/PTR)**	**Total: 860€ (1/ODF)** **Total: 930€ (2/ODF)** **Total: 1000€ (3/ODF)** **Total: 1060€ (4/ODF)** **Total: 1540€ (1/PTR)** **Total: 1610€ (2/PTR)** **Total: 1680€ (3/PTR)** **Total: 1740€ (4/PTR)**	**Total: 1109,54€ (1/ODF)** **Total: 1201,85€ (2/ODF)** **Total: 1294,15€ (3/ODF)** **Total: 1386,46€ (4/ODF)** **Total: 1973,08€ (1/PTR)** **Total: 2065,39€ (2/PTR)** **Total: 2158,69€ (3/PTR)** **Total: 2250€ (4/PTR)**	

Cenário A2H

- Ligação Internet Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
- Ligação Internet Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
- Ligação Internet Housing: 4 Mbit/s (down) / 4 Mbit/s (up)

ISP1	ISP2	ISP3	ISP4
1) CD Porto (2/2 Mbit/s): 583€ 2) CD Porto (4/4 Mbit/s): 2509€ 3) CD Porto (6/6 Mbit/s): 3458€ 4) CD Porto (10/10 Mbit/s): 5358€ DSL Lisboa (16/1 Mbit/s): 73€ CD Housing (5/5 Mbit/s): 737€ Housing 3 U's: 249€ E-Mail *Relay*: 214,9€	1) CD Porto (2/2 Mbit/s): 600€ 2) CD Porto (4/4 Mbit/s): 770€ 3) CD Porto (6/6 Mbit/s): 840€ 4) CD Porto (8/8 Mbit/s): 910€ 5) CD Porto (10/10 Mbit/s): 970€ DSL Lisboa (24/1 Mbit/s): 90€ Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: INCLUÍDO	1) CD Porto (2/2 Mbit/s): 844,23€ 2) CD Porto (4/4 Mbit/s): 936,54€ 3) CD Porto (6/6 Mbit/s): 1028,85€ 4) CD Porto (8/8 Mbit/s): 1121,15€ 5) CD Porto (10/10 Mbit/s): 1213,46€ DSL Lisboa (16/1 Mbit/s): 73€ (**ISP1**) Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)	Não foram fornecidas informações
Total: 1119,9€ (1) **Total: 3045,9€ (2)** **Total: 3994,9€ (3)** **Total: 6894,9€ (4)**	**Total: 890€ (1)** **Total: 1060€ (2)** **Total: 1130€ (3)** **Total: 1200€ (4)** **Total: 1260€ (5)**	**Total: 1217,23€ (1)** **Total: 1309,54€ (2)** **Total: 1401,85€ (3)** **Total: 1494,15€ (4)** **Total: 1586,46€ (5)**	

Cenário A2L

- Ligação Internet Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
- Ligação Internet Lisboa:
  - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física - ODF)
  - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente - PTR)

ISP1	ISP2	ISP3	ISP4
1) CD Porto (2/2 Mbit/s): 583€ 2) CD Porto (4/4 Mbit/s): 2509€ 3) CD Porto (6/6 Mbit/s): 3458€ 4) CD Porto (10/10 Mbit/s): 5358€ ODF) DSL Lisboa (2/2 Mbit/s): 160€ PTR) CD Lisboa (4/4 Mbit/s): 2509€ E-Mail *Relay*: 214,9€	1) CD Porto (2/2 Mbit/s): 600€ 2) CD Porto (4/4 Mbit/s): 770€ 3) CD Porto (6/6 Mbit/s): 840€ 4) CD Porto (8/8 Mbit/s): 910€ 5) CD Porto (10/10 Mbit/s): 970€ ODF) DSL Lisboa (2/2 Mbit/s): 160€ (**ISP1**) PTR) CD Lisboa (4/4 Mbit/s): 770€ E-Mail *Relay*: INCLUÍDO	1) CD Porto (2/2 Mbit/s): 844,23€ 2) CD Porto (4/4 Mbit/s): 936,54€ 3) CD Porto (6/6 Mbit/s): 1028,85€ 4) CD Porto (8/8 Mbit/s): 1121,15€ 5) CD Porto (10/10 Mbit/s): 1213,46€ ODF) DSL Lisboa (2/2 Mbit/s): 160€ (**ISP1**) PTR) CD Lisboa (4/4 Mbit/s): 936,54€ E-Mail *Relay*: 100€ (**MR?**)	CD Porto (10/10 Mbit/s): 1000€ DSL Lisboa (2/2 Mbit/s): 350€ Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)
Total: 957,9€ (1/ODF) Total: 2883,9€ (2/ODF) **Total: 3832,9€ (3/ODF)** **Total: 5732,9€ (4/ODF)** **Total: 3306,9€ (1/PTR) Total: 5232,9€ (2/PTR)** **Total: 6181,9€ (3/PTR)** **Total: 8081,9€ (4/PTR)**	**Total: 760€ (1/ODF)** **Total: 930€ (2/ODF)** **Total: 1000€ (3/ODF)** **Total: 1070€ (4/ODF)** **Total: 1130€ (5/ODF)** **Total: 1370€ (1/PTR)** **Total: 1540€ (2/PTR)** **Total: 1610€ (3/PTR)** **Total: 1680€ (4/PTR)** **Total: 1740€ (5/PTR)**	**Total: 1104,23€ (1/ODF)** **Total: 1196,54€ (2/ODF)** **Total: 1288,85€ (3/ODF)** **Total: 1381,15€ (4/ODF)** **Total: 1473,46€ (5/ODF)** **Total: 1880,77€ (1/PTR)** **Total: 1973,08€ (2/PTR)** **Total: 2065,39€ (3/PTR)** **Total: 2157,69€ (4/PTR)** **Total: 2250€ (5/PTR)**	**Total: 1650€ (ODF)**

Cenário B1H

- Ligação MPLS Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação MPLS Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
- Ligação MPLS Housing: 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação Internet Centralizada: 2 Mbit/s (down) / 2 Mbit/s (up)

ISP1	ISP2	ISP3	ISP4
Não foram fornecidas informações	1) MPLS Porto (4/4 Mbit/s): 550€ 2) MPLS Porto (6/6 Mbit/s): 570€ 3) MPLS Porto (8/8 Mbit/s): 660€ 4) MPLS Porto (10/10 Mbit/s): 690€ MPLS Lisboa (2/2 Mbit/s): 520€ (**ISP1**) a) Internet Centralizada (2/2 Mbit/s): 500€ b) Internet Centralizada (4/4 Mbit/s): 750€ Housing 3 U's: 60€ E-Mail *Relay*: INCLUÍDO	1) MPLS Porto (4/4 Mbit/s): 936,54€ 2) MPLS Porto (6/6 Mbit/s): 1028,85€ 3) MPLS Porto (8/8 Mbit/s): 1121,15€ 4) MPLS Porto (10/10 Mbit/s): 1213,46€ MPLS Lisboa (2/2 Mbit/s): 186,67€ Internet Centralizada: Ligação Porto Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)	MPLS Porto (10/10 Mbit/s) MPLS Lisboa (2/2 Mbit/s) Internet Centralizada (10 Mbit/s) Housing 3 U's E-Mail *Relay*: + 100€ (**?**)
	Total: 1630€ (1 a): **Total: 1880€ (1 b)** **Total: 1650€ (2 a)** **Total: 1900€ (2 b)** **Total: 1740€ (3 a)** **Total: 1990€ (3 b)** **Total: 1770€ (4 a)** **Total: 2020€ (4 b)**	**Total: 1423,21€ (1)** **Total: 1515,52€ (2)** **Total: 1607,82€ (3)** **Total: 1700,13€ (4)**	**Total: 1700€**

Cenário B1L

- Ligação MPLS Porto: 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação MPLS Lisboa:
  - 4 Mbit/s (down) / 4 Mbit/s (up)
- Ligação Internet Centralizada:
  - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física - ODF)
  - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente - PTR)

ISP1	ISP2	ISP3	ISP4
Não foram fornecidas informações	1) MPLS Porto (4/4 Mbit/s): 550€ 2) MPLS Porto (6/6 Mbit/s): 570€ 3) MPLS Porto (8/8 Mbit/s): 660€ 4) MPLS Porto (10/10 Mbit/s): 690€ MPLS Lisboa (4/4 Mbit/s): 550€ (**ISP1**) ODF) Internet Centralizada (2/2 Mbit/s): 500€ PTR) Internet Centralizada (4/4 Mbit/s): 750€ E-Mail *Relay*: INCLUÍDO	Não foram fornecidas informações	Não foram fornecidas informações
	Total: 1600€ (1 ODF) **Total: 1850€ (1 PTR)** **Total: 1620€ (2 ODF)** **Total: 1870€ (2 PTR)** **Total: 1710€ (3 ODF)** **Total: 1960€ (3 PTR)** **Total: 1740€ (4 ODF)** **Total: 1990€ (4 PTR)**		

Cenário B2H

- Ligação MPLS Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
- Ligação MPLS Lisboa: 2 Mbit/s (down) / 1 Mbit/s (up)
- Ligação MPLS Housing: 2 Mbit/s (down) / 2 Mbit/s (up)
- Ligação Internet Centralizada: 2 Mbit/s (down) / 2 Mbit/s (up)

ISP1	ISP2	ISP3	ISP4
Não foram fornecidas informações	1) MPLS Porto (2/2 Mbit/s): 520€ 2) MPLS Porto (4/4 Mbit/s): 550€ 3) MPLS Porto (6/6 Mbit/s): 570€ 4) MPLS Porto (8/8 Mbit/s): 660€ 5) MPLS Porto (10/10 Mbit/s): 690€ MPLS Lisboa (2/2 Mbit/s): 520€ a) Internet Centralizada (2/2 Mbit/s): 500€ b) Internet Centralizada (4/4 Mbit/s): 750€ Housing 3 U's: 60€ E-Mail *Relay*: INCLUÍDO	1) MPLS Porto (2/2 Mbit/s): 844,23€ 2) MPLS Porto (4/4 Mbit/s): 936,54€ 3) MPLS Porto (6/6 Mbit/s): 1028,85€ 4) MPLS Porto (8/8 Mbit/s): 1121,15€ 5) MPLS Porto (10/10 Mbit/s): 1213,46€ MPLS Lisboa (2/2 Mbit/s): 186,67€ Internet Centralizada: Ligação Porto Housing 3 U's: 200€ (**H?**) E-Mail *Relay*: 100€ (**MR?**)	MPLS Porto (10/10 Mbit/s) MPLS Lisboa (2/2 Mbit/s) Internet Centralizada (10 Mbit/s) Housing 3 U's E-Mail *Relay*: + 100€ (**MR?**)
	Total: 1600€ (1 a) **Total: 1850€ (1 b)** **Total: 1630€ (2 a)** **Total: 1880€ (2 b)** **Total: 1650€ (3 a)** **Total: 1900€ (3 b)** **Total: 1740€ (4 a)** **Total: 1990€ (4 b)** **Total: 1770€ (5 a)** **Total: 2020€ (5 b)**	**Total: 1330,9€ (1)** **Total: 1423,21€ (2)** **Total: 1515,52€ (3)** **Total: 1607,82€ (4)** **Total: 1700,13€ (5)**	**Total: 1700€**

Cenário B2L

- Ligação MPLS Porto: 2 Mbit/s (down) / 2 Mbit/s (up)
- Ligação MPLS Lisboa:
    - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física - ODF)
    - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente - PTR)
- Ligação Internet Centralizada:
    - 2 Mbit/s (down) / 2 Mbit/s (up) (obriga deslocação física – "a")
    - 4 Mbit/s (down) / 4 Mbit/s (up) (permite trabalhar remotamente – "b")

ISP1	ISP2	ISP3	ISP4
Não foram fornecidas informações	1) MPLS Porto (2/2 Mbit/s): 520€ 2) MPLS Porto (4/4 Mbit/s): 550€ 3) MPLS Porto (6/6 Mbit/s): 570€ 4) MPLS Porto (8/8 Mbit/s): 660€ 5) MPLS Porto (10/10 Mbit/s): 690€ ODF) MPLS Lisboa (2/2 Mbit/s): 520€ PTR) MPLS Lisboa (4/4 Mbit/s): 550€ a) Internet Centralizada (2/2 Mbit/s): 500€ b) Internet Centralizada (4/4 Mbit/s): 750€ E-Mail *Relay*: INCLUÍDO	1) MPLS Porto (2/2 Mbit/s): 844,23€ 2) MPLS Porto (4/4 Mbit/s): 936,54€ 3) MPLS Porto (6/6 Mbit/s): 1028,85€ 4) MPLS Porto (8/8 Mbit/s): 1121,15€ 5) MPLS Porto (10/10 Mbit/s): 1213,46€ MPLS Lisboa (2/2 Mbit/s): 186,67€ Internet Centralizada: Ligação Porto E-Mail *Relay*: 100€ (**MR?**)	Não foram fornecidas informações
	Total: 1540€ (1 a) **Total: 1790€ (1 b)** **Total: 1820€ (1 b PTR)** **Total: 1570€ (2 a)** **Total: 1820€ (2 b)** **Total: 1850€ (2 b PTR)** **Total: 1590€ (3 a)** **Total: 1840€ (3 b)** **Total: 1870€ (3 b PTR)** **Total: 1680€ (4 a)** **Total: 1930€ (4 b)** **Total: 1960€ (4 b PTR)** **Total: 1710€ (5 a)** **Total: 1960€ (5 b)** **Total: 1990€ (5 b PTR)**	**Total: 1130,9€ (1 ODF)** **Total: 1223,21€ (2 ODF)** **Total: 1315,52€ (3 ODF)** **Total: 1407,82€ (4 ODF)** **Total: 1500,13€ (5 ODF)**	