José Rui Coutinho Ambrósio;

Nº 21204;

Rede *WI-FI* da Porto Digital – Expansão, controlo de acessos e criação de plataforma estatística;

Dissertação de Mestrado em Tecnologias de Informação e Comunicação Multimédia;

Trabalho realizado sob a orientação do Engº. Gil Coutinho professor no Instituto Universitário da Maia - ISMAI

Outubro 2014

Agradecimentos

Quero agradecer a todos aqueles que contribuíram para a realização deste projeto, quer a título individual quer a nível coletivo. De destacar o contributo da Associação Porto Digital (APD), que me lançou o desafio deste projeto bem como se disponibilizou no auxílio e acompanhamento de todas as suas etapas. Deixo uma palavra de apresso a todo o grupo de trabalho da APD, que ajudaram à minha integração na empresa, sendo sempre acolhedores e prestáveis.

Gostava de agradecer também ao Eng.º Gil Coutinho, meu orientador de projeto pela disponibilidade e apoio ao longo de todo o projeto.

Por fim, uma palavra de agradecimento à minha família, amigos pelo incentivo e paciência demonstrados nestes últimos meses.

Resumo

Este documento foi elaborado como forma de descrever o modo de implementação do projeto de mestrado designado por "Rede *WI-FI* da Porto Digital – Expansão, controlo de acessos e criação de plataforma estatística". O projeto em questão tem como objetivo a expansão da rede *wireless* da Associação Porto Digital (APD), bem como desenvolver um mecanismo de gestão e controlo da rede sem fios e, ainda, a criação de uma plataforma estatística que permita analisar a usabilidade da rede *Wi-Fi*.

Inicialmente, o primeiro ponto foi realizar um levantamento de necessidades existentes para melhorar a gestão da rede *wireless* já existente bem como discutir a melhor forma de proceder à sua expansão e futura monitorização.

Depois de discutida a melhor solução, de começarem a surgir as primeiras linhas mestras em relação ao projeto, foi necessário realizar, em ambiente de teste, uma prova de conceito. Este ponto permitiu verificar se, na prática, era aplicável a ideia anteriormente discutida.

Numa terceira fase, foi realizada a expansão da rede *wireless* da APD, sendo aprovisionados 15 novos *access point's* em outros tantos Bairros Socias da cidade do Porto.

Depois de colocados os AP's nos bairros sociais, foram efetuadas as devidas configurações nos diferentes equipamentos envolvidos, à imagem do que tinha ocorrido durante a prova de conceito.

Findada esta etapa, partimos para um novo desafio, a instalação de um servidor *radius* para que este possa recolher todas as informações de utilização da rede. Posteriormente, foi criado um modelo de dados normalizado para satisfazer as necessidades estipuladas.

Para finalizar foram feitas análises de dados, obtidos através da monitorização da rede.

Abstract

This document was prepared as a way to describe how the implementation of the master's project called "*WI-FI* Network of Porto Digital - Expansion, Access control and statistics platform." The project in question aims at the expansion of the *wireless* network at Associação Porto Digital (APD), as well as develop a mechanism to manage and control the wireless network and even the creation of a statistics framework that allows to analyze the usability of network Wi Fi.

Initially, the first point was to survey existing needs to improve the management of existing wireless network and discuss the best way forward to its expansion and future monitoring.

After the discussion of the best solution and the establishment of the first guidelines in relation to the project, it became necessary to implement, in a test environment, the proof of concept. This point allowed us to test if the previously discussed ideas were practicable.

In a third phase, the expansion of the APD *wireless* network took place by the procurement of fifteen new Access *points* in Social Neighborhoods of Porto.

Once the access points were placed in the Social Neighborhoods the necessary settings were made in the different equipment involved, as it had occurred during the proof of concept.

Finally, we set off for a new challenge. Installing a radius server so that it can collect all the information of network utilization. Subsequently, a normalized data model was created to meet the needs stipulated.

To complete, there were analyzes made of the data obtained through monitoring the network.

Índice

Índice de figuras

Índice de esquemas

Índice de tabelas

Lista de acrónimos

AAA – *Authentication, Authorization, Accounting*;

AEP – Associação Empresarial do Porto;

AES – *Advanced Encryption Standard*;

AMP – Área Metropolitana do Porto;

AP – *access point* (Ponto de acesso);

BD – Base de dados;

CMP – Camara municipal do porto;

DHCP – *Dynamic host Configuration Protocol*;

EAP – *Extensible Authentication Protocol*;

Eduroam – *Education Roaming*;

FDB – *Forwarding DataBase*;

GPLv2 – *GNU General Public License, version* 2;

IEEE – *Institute of Eelctrical and Electronics Engineers*;

IP – *Internet Protocol*;

IPv4 – *Internet Protocol version* 4;

LAN – *Local Area Network*;

LAP – *Lightweight access point*;

LWAPP – *Lightweight access point Protocol*;

MAC – *Media Access Control*;

MAN –*Metropolitan Area Network*;

MD5 – *Message-Digest algorithm*;

NAS – *Network-Attached Storage*;

NAT – *Network Address Tranlation*;

PEAP – *Protected Extensible Authentication Protocol*;

PSK – *Pre-Shared Key*;

PVC – *Polyvinyl chloride (policloreto de polivinila);*

radius – Remote authentication dial in user servisse;

SKIP - *Simple KeyManagement for Internet Protocol*;

SQL – *Structured Query Language*;

SSC - *Secure Services Client;*

SSC – *Secure Services Client;*

TI – *Tecnologias de informação*;

TKIP – *Temporal Key Integrity Protocol*;

TLS – *Transport Layer Security*;

TTLS – *Tunneled Transport Layer Security*;

TV – Televisão

UP – Universidade do Porto;

UTP – *Unshielded Twisted Pair*;

VID – *Virtual Local Area Network Identify*;

vlan – Virtual local área network;

VLANtag – Etiqueta *Virtual Local Area Network*;

VMPS – *vlan Management Policy Server*;

WAN – *Wide Area Network*;

WEP – *Wired Equivalent Privacy*;

wlan – wireless Local Area Network;

WLC – *wireless LAN Controller*;

WPA – *Wi-Fi Protected Access*;

1. Introdução

Neste primeiro capítulo em jeito de introdução, pretendo apresentar, de forma resumida, o enquadramento do meu projeto, os objetivos a realizar, uma vista geral sobre o projeto e, ainda, os resultados com ele obtidos.

1.1. Enquadramento

A Associação Porto Digital (APD) foi criada com o propósito de candidatar o Município do Porto ao programa "Portugal Digital". Programa, este, que tem como seu principal objetivo contribuir para a evolução da sociedade da informação e do conhecimento. Para isso foram realizadas inúmeras iniciativas e projetos, onde o meu projeto de tese se insere.

Um destes vários projetos foi a criação de uma rede metropolitana de fibra ótica na cidade do Porto, que permite a interligação de varias instituições, como instituições de ensino, de investigação, médicas, na Câmara municipal e governos locais. Esta iniciativa insere-se no programa de "cidades e regiões digitais", ao qual a Câmara Municipal do Porto (CMP) se candidatou com este propósito.

Aliado a esta rede de fibra ótica, foi também, posteriormente, criada uma rede sem fios (*wireless*), que usa os pontos de presença da fibra ótica. Esta rede *wireless*, espalhada pela cidade do Porto, permite o acesso livre e gratuito à Internet de todos os moradores e turistas que se encontrem próximos de um *hotspot*. Sendo uma rede com estas características, torna-se indispensável uma boa gestão e controlo de acessos. Desta forma torna-se extremamente necessário melhorar o controlo de acessos à rede e criar uma plataforma de armazenamento de registos e obtenção de dados estatísticos.

Tal como o nome da presente tese indica, o principal objetivo é criar essa plataforma estatística com controlo de acessos e utilização da rede *Wi-Fi* da Associação Porto Digital.

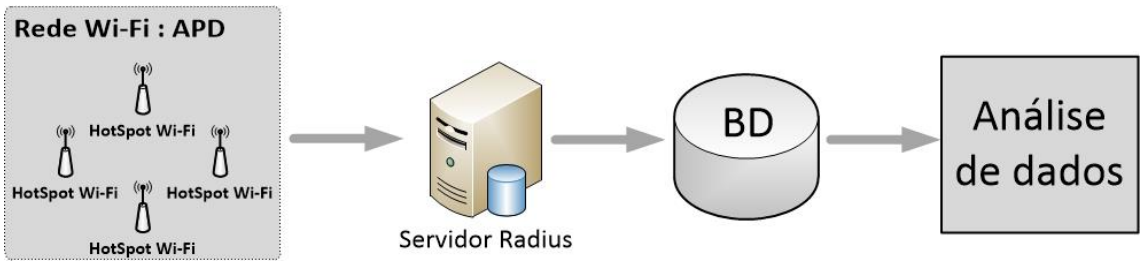
1.2. Objetivos

O objetivo deste projeto é desenvolver um mecanismo de obtenção de informações de acessos à rede, bem como informações de utilizador.

Uma vez que a rede *wireless* da Porto Digital se encontra constantemente em expansão, um dos meus objetivos será colaborar nessa mesma expansão, ajudando na tarefa de instalação de novas antenas *Wi-Fi* em cerca de quinze bairros sociais do Porto. Dito isto, e segundo o Esquema 1 - Esquema ideia base do projeto, a ordem de trabalhos a realizar será a seguinte:

Estado da arte e Levantamento de requisitos;

- ✓ Provar o conceito em ambiente teste;
- ✓ Expansão da rede *wireless*;
- ✓ Configuração dos *access point's*;
- ✓ Instalação Servidor RADIUS;
- ✓ Criação de modelo de dados;
- ✓ Análise de dados;



Esquema 1 - Esquema ideia base do projeto

1.3. Estrutura do documento

No que concerne ao capítulo 2, denominado "enquadramento", é apresentado e contextualizado o ponto de partida do projeto, bem como a descrição e definição da entidade envolvente (APD). Nesta secção são descritos de forma pormenorizada quais os seus objetivos, aquilo a que se propõe e as suas principais funções. Depois de apresentada a APD é tempo de enquadrar o meu projeto e relacioná-lo com a entidade acima referida, quais as suas motivações e objetivos.

No que diz respeito ao capítulo 3, são abordados as principais tecnologias de rede utilizadas atualmente, são dadas breves explicações do que são as redes cabladas e as redes *wireless*. São apresentados exemplos de funcionamento, assim como as suas vantagens e desvantagens.

Quanto ao capítulo 4, este diz respeito às questões de segurança indispensáveis a um bom funcionamento de uma rede. Aqui são abordadas quais as tecnologias mais utilizadas na segurança da Internet, explicados processos de funcionamento, apresentados exemplos e, ainda, esquemas de implementação. Neste capítulo é também descrito o funcionamento da tecnologia *vlan* que nos dias de hoje é indispensável quando falamos de redes. Por fim, são apresentados alguns exemplos de protocolos de segurança *wireless*. São abordados quer os protocolos de encriptação quer os protocolos de autenticação, com uma breve descrição de cada um.

O capítulo 5 corresponde à prova de conceito em ambiente de teste que faz parte dos objetivos inicialmente apresentados. No edifício da APD na Ponte Nova foi criado um ambiente o mais próximo possível do cenário que existe nos Bairros Sociais do Porto. Desta forma, foi possível testar o funcionamento na rede *wireless* dos bairros bem como a obtenção dos dados estatísticos da utilização. Terminada esta etapa com sucesso, avançamos para a instalação dos *access point's* nos bairros sociais.

No capítulo 6 é descrito o processo de montagem e configuração que foi realizado, tendo em vista a criação da rede sem fios dos bairros sociais. Neste ponto é discutida a localização dos AP's, é feito um planeamento cuidado de todos os pormenores de instalação, bem como é apresentado um orçamento indicativo acerca do investimento monetário a ser feito. Depois desta vertente mais física da instalação, as atenções voltaram-se para a configuração de todos os equipamentos e tecnologias que nos

permitirão disponibilizar Internet nos bairros sociais. O sucesso desta configuração deveu-se sobretudo à prova de conceito realizada anteriormente.

O capítulo 7 corresponde a uma mais-valia que surgiu no decorrer dos trabalhos e que não fazia parte do plano inicial do projeto. Contudo, veio acrescentar valor ao projeto e em tudo se enquadra na ideia principal. Este capítulo debruça-se sobre a rede "eduroam". Esta rede é um projeto europeu que visa disponibilizar à comunidade académica um serviço de mobilidade entre universidades. Sendo que, a APD já fazia a difusão desta rede noutros locais da cidade, achamos importante que os bairros sociais também fossem contemplados com esta rede, alargando, assim, ainda mais a área de incidência desta rede comunitária académica. Deste modo, os alunos universitários que se encontrem perto de um *access point* da APD, podem usufruir desta rede. Mais uma vez prestamos um serviço à comunidade dos bairros sociais do Porto, esperando, assim, que esta possa fomentar o ingresso no ensino superior dos habitantes locais.

O capítulo 8 relata o processo de obtenção de informações acerca da utilização da rede, não só da rede *wireless* dos bairros sociais mais também da restante rede *wireless* da APD. Aqui é abordado o tema do servidor *radius*, como se realizou a sua configuração e, ainda, os seus principais propósitos. Depois de perceber o funcionamento do *radius* e como podemos ter acesso às informações acerca dos *access point's* foram discutidas quais as informações mais relevantes a retirar e o modelo de dados a usar, de forma a satisfazer essas necessidades. Foram, ainda, criadas tabelas auxiliares com o objetivo de complementar as informações compiladas no servidor. Com isto, transformamos o modelo de dados numa base de dados relacional facilmente acessível a todos os gestores de rede da APD.

No capítulo 9 é explicado como vai ser feito o acesso à base de dados criada para o efeito e quais as principais informações a retirar da mesma. São definidos três tipos de consulta à base de dados consoante a informação pretendida, tais como: estado da rede, utilização dos equipamentos e, ainda, os dados de utilizador. O estado da rede fornece-nos informações acerca da utilização geral da rede num determinado momento como número de utilizadores e débitos de navegação. A utilização dos equipamentos indica-nos os números de utilização dos equipamentos de rede existentes. Fornece-nos informações como por exemplo, qual o controlador que tem mais tráfego, qual a *wlan* mais utilizada e qual o *hotspot* com mais utilizadores. Os dados de utilizador permitem-nos saber onde

está um determinado utilizador a uma determinada hora. Estas informações, analisadas em conjunto, permitem-nos traçar fluxos geográficos de pessoas ao longo da cidade do Porto. Por outro lado, permitem-nos retirar conclusões acerca dos utilizadores, qual o seu relacionamento com a nossa rede, e inclusive obter perfis de utilização.

No capítulo 10 são expostas as conclusões acerca do projeto realizado. Integra, também, uma opinião pessoal sobre o processo de trabalho e o estágio em si. Aproveitei, também, para expor algumas propostas de trabalho futuro a desenvolver partindo do trabalho realizado até ao momento. Estas propostas visam o melhoramento do projeto inicial, acrescentando-lhe valor e conteúdo.

2. Enquadramento

O presente relatório visa descrever a minha contribuição para a realização do Projeto de Redes *wireless* existente na Associação Porto Digital. Este projeto envolve distintas instituições que, em comunhão de interesses, procuram desenvolver e implementar uma rede sem fios comunitária na cidade do Porto.

Este capítulo debruça-se sobre as entidades participantes neste mesmo projeto e procura ilustrar as condições existentes na sua etapa inicial. Serão nomeadas as necessidades e motivações para a execução deste projeto com sucesso.

2.1. Projeto Porto Digital

Com o objetivo de candidatura ao Programa designado por Cidades Digitais, em 2004 foi formada a Associação Porto Digital (APD), com a participação da Câmara Municipal do Porto (CMP), a Universidade do Porto (UP) e a Associação Empresarial de Portugal (AEP).

Sobre a alçada da APD surgiu o projeto Porto Digital.

"O projeto Porto Digital tem como princípio orientador base a evolução para uma Sociedade da Informação e do Conhecimento e desenvolver esforços para que essa sociedade possa estar ao alcance de todos" (Digital, 2005).

O projeto Porto Digital abrange vários subprojectos, que vão sendo realizados sobe a sua orientação e estão patenteados nas seguintes categorias:

2.1.1. Subprojectos de Infraestrutura

Fornece a infraestrutura física possibilitando o acesso ao mundo digital. Permite a interligação de um conjunto de instituições da cidade, como estabelecimentos de ensino, residências universitárias, bibliotecas, museus, instituições do governo local e instituições do sector da saúde (Digital, 2005).

2.1.2. Subprojectos de Dinamização

Disponibilização de conteúdos didáticos, científicos, turísticos, lúdicos e culturais.

2.1.3. Subprojectos de Acessibilidades

Pretende espalhar pela cidade pontos de acesso à Internet, com ou sem fios, que permita o acesso aos serviços disponibilizados pela Porto Digital (Digital, 2005).

2.1.4. Subprojectos de e-Government

Abrangendo a reformulação dos processos administrativos, modernizando a prestação de serviços ao munícipe (Digital, 2005).

2.1.5. Subprojectos sectoriais

Representam uma intervenção das TIC para promover o emprego, a economia, a cultura e o turismo (Digital, 2005).

2.1.6. Subprojecto de Acompanhamento e Gestão

Pretende coordenar e gerir o projeto Porto Digital e garantir que os objetivos propostos são atingidos (Digital, 2005).

2.2. Projeto fibra ótica

O projeto de fibra ótica surgiu no seguimento da candidatura da Cidade do Porto à Medida 2.3 – Projetos Integrados: das Cidades Digitais ao Portugal Digital, do Eixo Prioritário II – Portugal Digital, renomeada recentemente por Programa Operacional Sociedade do Conhecimento.

Esta candidatura contou com o apoio da Universidade do Porto, da Câmara Municipal do Porto e da Associação Empresarial de Portugal.

Com o objetivo de promover a evolução para uma sociedade da Informação e do Conhecimento agruparam-se um conjunto de subprojectos direcionados para o Indivíduo, a Sociedade, o Mercado e a Tecnologia.

Na base desta candidatura estava a criação de uma infraestrutura de comunicação de banda larga, que melhorasse as condições de acesso à informação, quer ao nível de económico, quer ao nível de área abrangência. Desta forma pretendesse elevar o desenvolvimento económico e social de toda a cidade e região.

Os efeitos favoráveis desta, redes privadas de fibra ótica, já se fizeram notar em várias outras cidades Europeias há vários anos. Uma vez que potencia o investimento, promovendo uma sociedade do conhecimento.

Esta proposta pretende interligar instituições de ensino e bibliotecas, bem como museus. Reconheceu-se também importância na inclusão de instituições autárquicas e instituições de saúde. Desta forma todos beneficiariam das tecnologias de informação e comunicação nas suas atividades diárias, bem como promovia a modernização de alguns processos administrativos (Coutinho, 2006).

2.3. Projeto *wireless*

Depois de implementado o Subprojecto de Infraestrutura, que equipou com fibra ótica a maior parte do Grande Porto, seria interessante aliar a este projeto de fibra um projeto de rede sem fios (*wireless*). Este projeto tem como objetivo facilitar, ainda mais, o acesso à informação e abranger, ainda mais, beneficiários.

Desta forma a Porto Digital implementou uma rede *wireless*, espalhada pela cidade do Porto que permite o livre e gratuito acesso à Internet de todos os moradores e turistas que se encontrem próximos dos diversos *hotspots* espalhados pelo grande Porto. Sendo uma rede de grandes dimensões e com características comunitárias, é muito importante uma boa gestão e controlo de acessos.

Para isso, é estritamente necessário melhorar o controlo de acessos à rede e criar uma plataforma de armazenamento de registos e obtenção de dados estatísticos. Torna-se, portanto, primordial o desenvolvimento de um mecanismo de obtenção de informações de acessos à rede e informações de utilização/utilizadores.

Dada esta nova forma de gerir a rede *wireless* torna-se possível e apetecível a expansão desta rede, com a instalação de mais *hotspots* abrangendo cada vez mais áreas, nomeadamente nos Bairros Sociais do Porto, onde já existe fibra ótica instalada, no âmbito do fornecimento de sinal de TV gratuito.

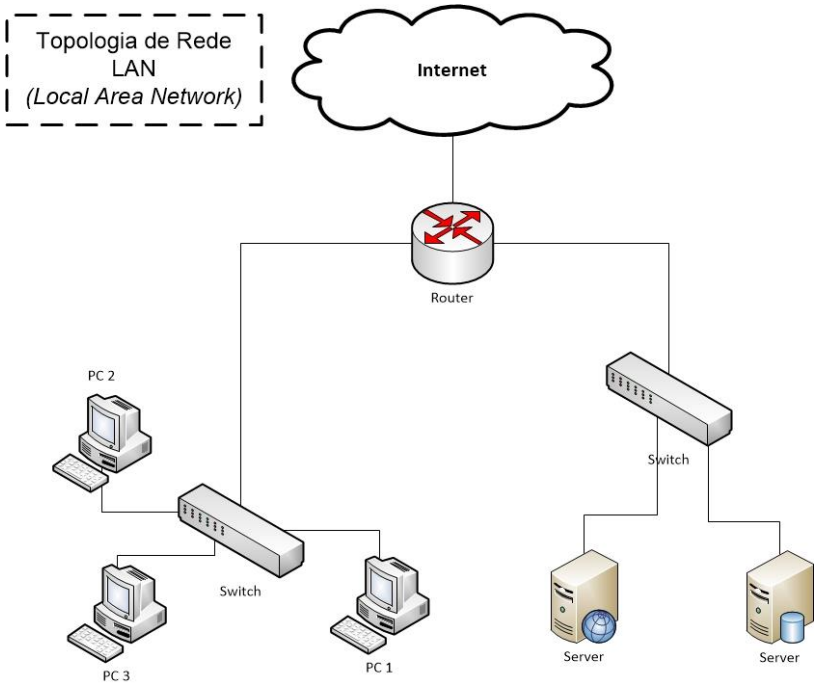
3. Tecnologias de Rede

Ao longo deste capítulo serão dadas breves explicações do que são as redes cabladas e as redes *wireless*. São apresentados exemplos de funcionamento, assim como as suas vantagens e desvantagens. Trata-se de uma descrição superficial das tecnologias mais relevantes, presentes no decorrer do meu projeto.

3.1. Redes Cabladas

As Redes cabladas são utilizadas para interligar diversos equipamentos entre si de forma a permitir a troca de dados, ou seja, é um conjunto de Hardware e Software que permite a diversos computadores estabelecerem comunicações entre si, partilhando informações e recursos. Este tipo de Redes tem vindo a sofrer melhorias ao longo dos tempos, quer ao nível de débito, quer ao nível da fiabilidade das comunicações. Estas redes de interligação de equipamentos têm diferentes nomenclaturas segundo a sua área de cobertura.

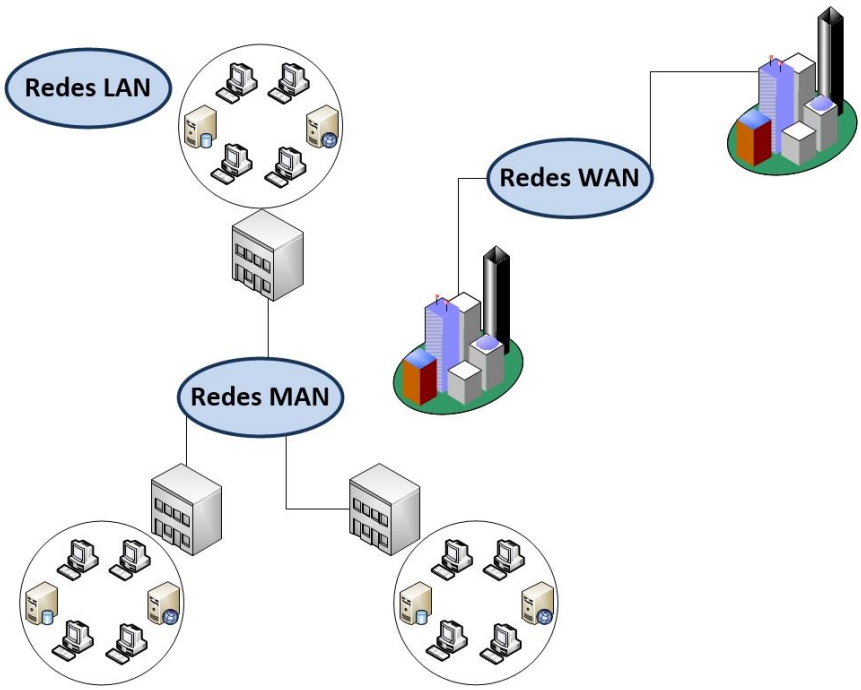
As Redes LAN (Local Area Network) são denominadas de redes locais por apenas cobrem uma área limitada de aproximadamente um quilómetro (ver Esquema 2).



Esquema 2 - Tipologias de Redes LAN

As Redes MAN (*Metropolitan Area Network*) são redes Metropolitanas de maior escala que necessitam de tecnologias mais sofisticadas, uma vez que os seus nós se encontram fisicamente mais distantes. Quanto maior a distância entre os nós da rede, maior a taxa de erros devido à degradação do sinal. (Dictionary of Networking, 2000)

As Redes WAN (*Wide Area Network*) são redes de interligação que abrangem uma enorme área geográfica como Países ou Continentes (ver Esquema 3). (Dictionary of Networking, 2000)



Esquema 3 – Tipologias de rede

Nos dias de hoje é cada vez mais frequente uma empresa usar tecnologias de informação e a Internet, como forma de facilitar processos e otimizar o trabalho. A presença das TI é bastante importante, pois facilita o trabalho em grupo, bem como desenvolve mecanismos automáticos para que o trabalho seja mais eficiente e a gestão mais rigorosa.

Consequentemente, é natural uma empresa possuir uma rede de computadores estruturada, quer no seu edifício sede, usando uma LAN, quer ligando-se a várias outras filiais usando as MAN ou WAN. Desta forma, mantém todos os postos de trabalho mais próximos e um fluxo de informação atualizado e fiável.

Uma das arquiteturas de rede mais utilizadas nas empresas é a arquitetura Cliente-Servidor. Nesta situação, toda a informação encontra-se centrada num ou mais servidores e todos os trabalhadores (clientes) podem aceder a essa informação, seja através de aplicações desenvolvidas à medida da empresa seja apenas na utilização de um *browser*. Com uma estrutura de rede bem estruturada é possível ligar todos os departamentos de uma empresa, ou até mesmo vários edifícios da empresa, mesmo estando no outro lado do planeta, e tudo funciona em rede instantaneamente. Este é um fator fundamental nos dias de hoje já que vivemos numa Era em que a informação é o bem mais precioso.

3.2. Redes wireless

A rede *wireless* refere-se a uma rede sem fios, ou seja, é uma comunicação feita por equipamentos que usam ondas de rádio. Este tipo de comunicação não necessita o uso de cabo sejam eles telefónicos, coaxiais ou óticos.

A utilização mais frequente desta tecnologia é em redes de computadores, permitindo-lhes o acesso à Internet através de ondas rádio. Normalmente, a rede *wireless* está integrada numa rede cablada potenciando essa mesma rede, quer a nível de facilidade de expansão, quer a nível de mobilidade do utilizador.

Esta tecnologia baseada no padrão IEEE 802.11 é uma das grandes inovações dos últimos anos. Prova disso é o número crescente de *hotspots* existentes, bem como a normalização dos computadores portáteis, telemóveis e *tablets* equipados originalmente com interfaces IEEE 802.11.

Este padrão atua em baixas frequências de rádio e não necessita de licença para a utilização, sendo apenas necessário estar no raio de ação ou numa área abrangida por um ponto de acesso. (Gast, 2002).

No entanto, para tirar partido das vantagens das Redes *wireless*, estas necessitam que os equipamentos *wireless* estejam ligados entre si através de uma rede cablada estruturada, permitindo a integração perfeita entre a rede cablada e a rede *Wi-Fi*. Desta forma torna-se indiferente para o utilizador estar ligado através de cabo ou *wireless*, diferenciando apenas a capacidade de débito dessas ligações.

Outra grande vantagem das redes *wireless* é a possibilidade de expandir uma rede sem obrigar a grandes investimentos em infraestruturas, sendo apenas necessário a instalação de um ponto de acesso. Dependendo do fabricante um ponto de acesso que permite o ingresso à rede de cerca de trinta e dois utilizadores ao mesmo tempo, tal coisa não acontece numa rede cablada que exige um ponto de rede para cada utilizador (Barbosa, 2009).

No entanto, as redes *wireless* apresentam algumas desvantagens, tais como a baixa capacidade de débito, a suscetibilidade a interferências externas na propagação no sinal radio, bem como problemas da segurança uma vez que não é uma comunicação orientada podendo ser intercetada por outra pessoa.

O problema da baixa capacidade de débito é causada pela forma como os dados são transmitidos. Numa rede *wireless* os dados são transmitidos por ondas rádio, ou seja, andam espalhadas pelo ar e são bastantes suscetíveis a interferências. Estas interferências podem ser causadas pelo excessivo número de utilizadores ligados ao mesmo tempo ao mesmo AP. Ou então pode resultar de fatores externos como por exemplos colisão de ondas rádio emitidas na mesma frequência uma vez que usa uma banda não licenciada, exemplo disto é o micro-ondas que deteriora o sinal *wireless* pois emite ondas eletromagnéticas na mesma frequência.

Outra desvantagem é a forma de transmissão de dados, pois é efetuada em vários sentidos correndo o risco de ser intercetada por terceiros, pondo em risco a segurança da informação. Neste caso, é imprescindível que os dados sejam transmitidos de uma forma encriptada aumentando assim a segurança das comunicações. No entanto estes protocolos de encriptação diminuem o débito nas transmissões. (Lowe, 2005)

4. Segurança

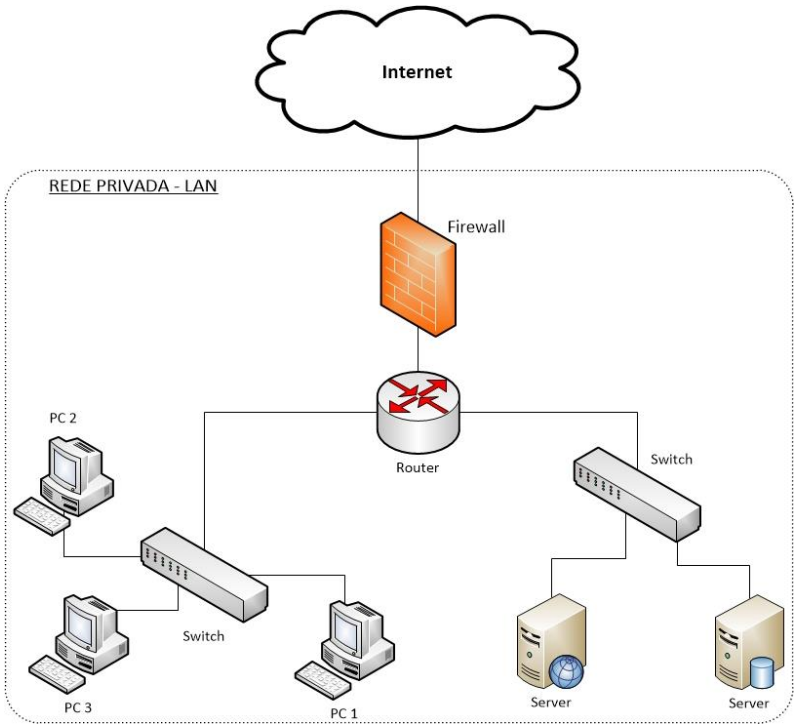
Em todas as topologias de rede existentes é necessário existirem elementos que garantam a segurança das comunicações, pois circulam na rede muitos dados pessoais e confidenciais.

Como forma de combater este problema ao longo do tempo foram desenvolvidas várias tecnologias que tentam aumentar a segurança nas comunicações. Tal como em todas as áreas, os sistemas de segurança foram evoluindo acompanhando a evolução das pessoas que o tentam quebrar. Desta forma assistimos a uma contante evolução tecnológica por parte de quem pretende atacar as redes, bem como uma resposta de quem as defende de forma a provar a sua fiabilidade e promover o aumento da sua utilização.

4.1. Firewall

A *Firewall* é a tecnologia mais utilizada para garantir a segurança das comunicações. Esta, consiste na análise de todos os pacotes de dados existentes na rede e permite ou inibe a sua propagação. Esta permissão ou inibição é dada através de um conjunto de regras implementadas previamente. Este conjunto de regras é definido por cada empresa de acordo com as suas necessidades, sendo recomendável que apenas permita o tráfego estritamente necessário para o funcionamento da mesma com o objetivo da não sobrecarga da rede (Dictionary of Networking, 2000).

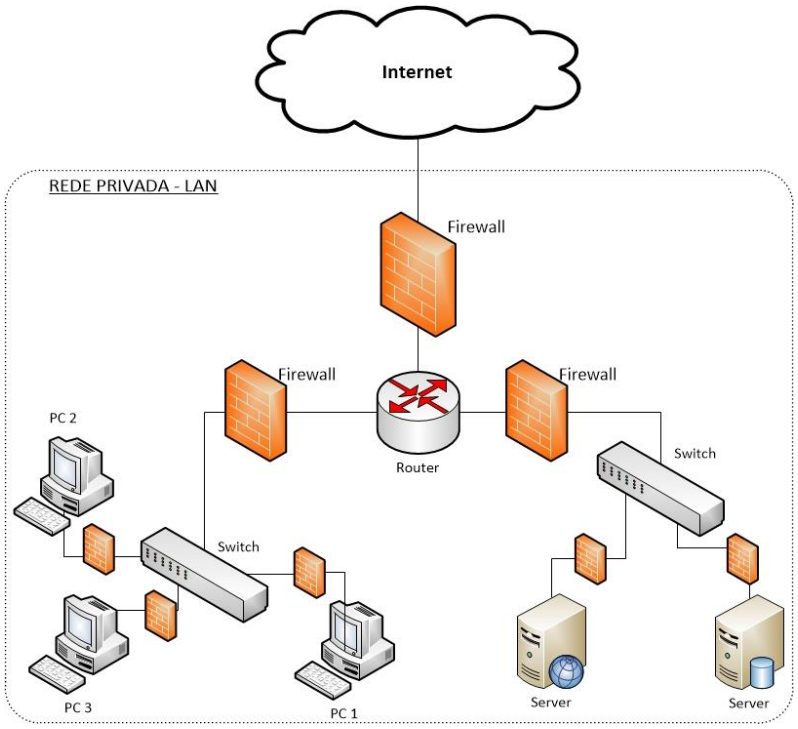
Geralmente a *Firewall* é implementada entre fronteira da rede da empresa e da rede pública, de forma a garantir que na rede da empresa exista somente tráfego já filtrado pela *Firewall*, tal como ilustra o Esquema 4.



Esquema 4 – Exemplo da utilização da firewall

Contudo, ao longo do tempo, as empresas implementam cada vez mais *Firewall*, quer nos vários sectores da empresa, quer mesmo no próprio posto de trabalho de cada funcionário (ver Esquema 5). Esta prática permite a utilização de diversos filtros que vão restringindo cada vez mais o tráfego que existe na rede privada da empresa, e desta forma, aumenta a segurança da mesma.

.



Esquema 5 – Exemplo da utilização de várias firewall

4.2. NAT

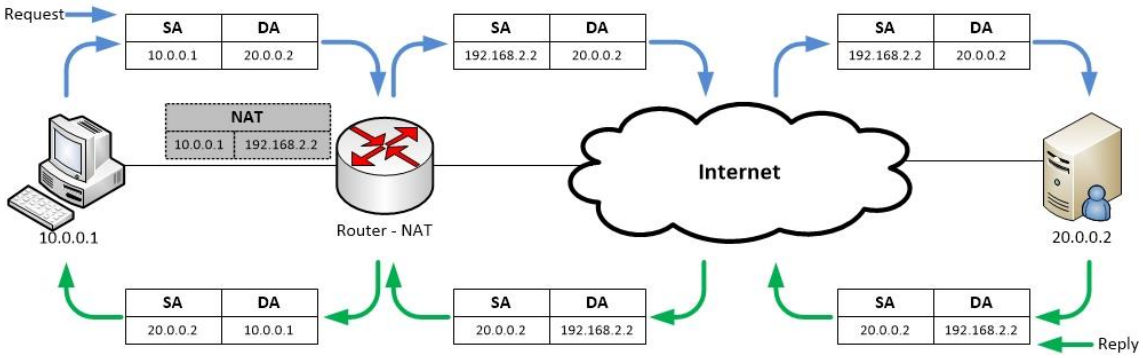
Ao longo dos tempos assistimos a um aumento exponencial do número de computadores e outros dispositivos com ligação à Internet. Este aumento aproximou-nos do número máximo de endereços de rede IPv4 (*Internet Protocol version 4*) disponíveis para tal (Briere, R. Bruce III, & Hurley, 2003).

Desta forma era importante encontrar uma alternativa a esta intrínseca necessidade de aumentar o número de dispositivos conectados. Assim sendo foi implementada a tecnologia NAT (*Network Address Tranlation*) que consiste em cada rede privada apenas necessitar de um endereço IP, designado por IP público.

Sempre que um computador de uma rede privada aceder à Internet usa a sua *gateway* da rede que possui a tecnologia NAT. Desta forma a *gateway*, substitui o endereço IP privado por um IP público, guardando numa tabela NAT, o IP privado juntamente com um porto, atribuído aleatoriamente. Quando o tráfego viaja no sentido inverso, ou seja, com destino ao computador, a tecnologia NAT vai efetuar o processo inverso substituindo o endereço IP público pelo privado e o respetivo porto, encaminhando o tráfego para a máquina interna correta (ver Esquema 6) (Alcatel-Lucent, 2008).

Os IP's presentes na tabela de NAT apenas são guardados quando o tráfego viaja da rede privada em direção à Internet. Desta forma, sempre que em pacote chegue da Internet com destino a uma máquina ao chegar à geteway não encontrará nenhuma correspondência na tabela NAT, sendo automaticamente descartado. Isto impossibilita a entrada de tráfego indesejado e o NAT acaba por funcionar como uma *Firewall*. Ao esconder para o exterior, a rede privada existente, aumenta a segurança da rede privada.

Para além disso, esta tecnologia permite, na maioria dos casos, ligar cerca de 65536 máquinas de uma rede privada usando apenas um endereço público o que permite reter o esgotamento total de endereços IP (Barbosa, 2009).



Esquema 6 – Funcionamento da tecnologia NAT

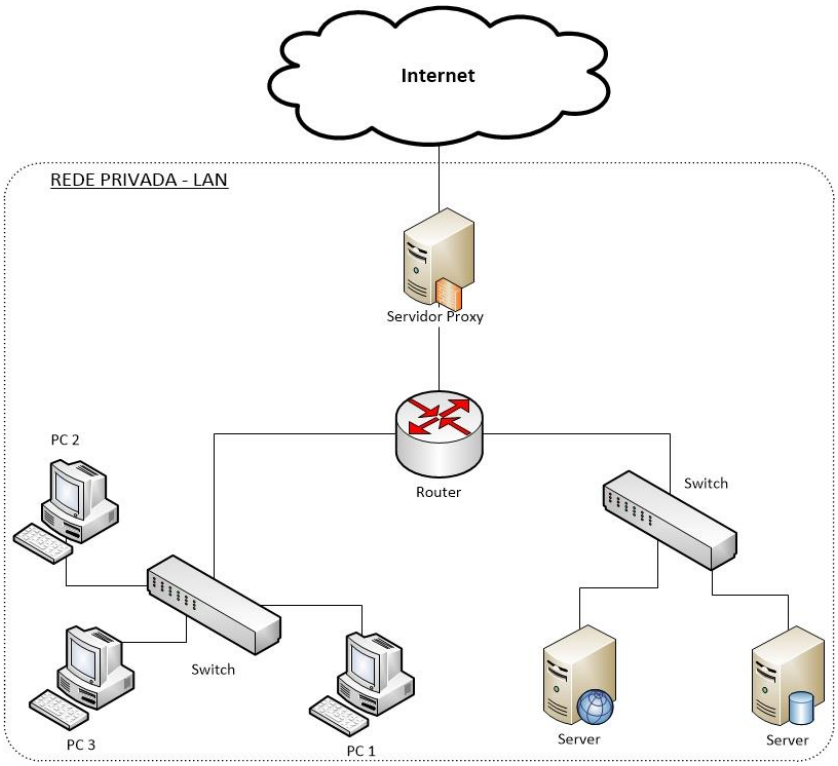
4.3. *Proxy*

O servidor *Proxy* funciona como um o intermediário entre o cliente e a rede, ou seja, quando um cliente requisita um determinado serviço à rede este pedido é processado pelo *Proxy*. Caso o *Proxy* contenha esse pedido em *cache* entrega-o ao cliente instantaneamente, caso contrário, o *Proxy* consulta a rede e reencaminha para o cliente, guardando uma cópia do mesmo na sua *cache* (ver Esquema 7). Caso exista, posteriormente, um novo pedido deste serviço por parte de este ou de outro cliente, os dados vão ser reencaminhado imediatamente pois já se encontra na *cache* do *Proxy*. Este mecanismo aumenta a velocidade de navegação, reduzindo o tráfego gerado na rede e o uso de banda.

Esta funcionalidade é também vista como uma medida de segurança uma vez que é o servidor *Proxy* que efetua os pedidos à rede, assim sendo a rede não conhece qual o equipamento que requereu o pedido, apenas que foi solicitado pelo servidor *Proxy*.

No entanto o *Proxy* é usado principalmente pela sua capacidade de limitar o acesso dos clientes a determinados *sites* e serviços que vão contra a política da empresa. Tais como, excesso de consumo de largura de banda, visita a *sites* de entretenimento ou redes sociais, como por exemplo o *facebook* ou o *Youtube*, bem como sites de conteúdo malicioso e duvidosos.

Outra vantagem é a possibilidade de monitorização de cada máquina individualmente, por outras palavras, é possível a análise de relatórios acerca do tráfego que cada máquina utiliza individualmente (Dictionary of Networking, 2000).

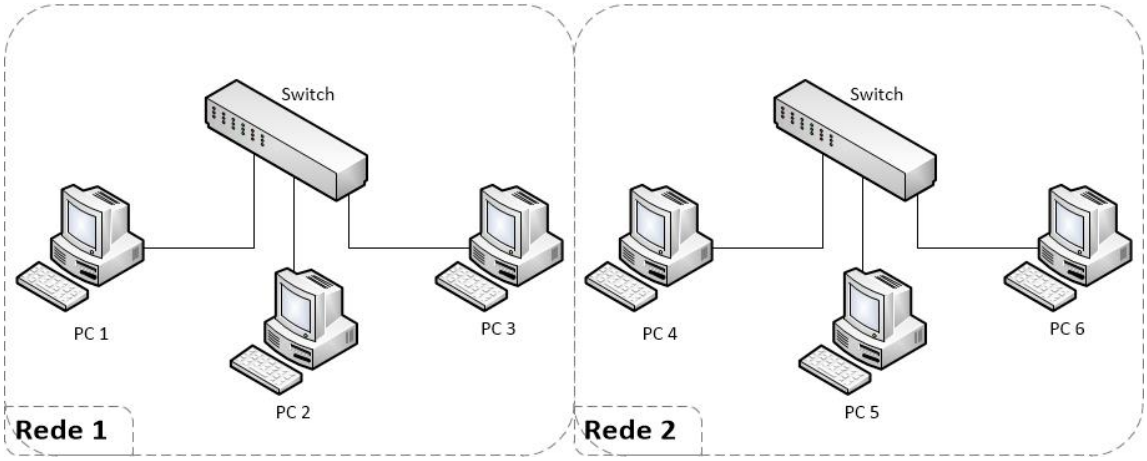


Esquema 7 – Esquema de utilização do servidor Proxy

4.4. vlans

Com a constante evolução das redes e o aumento da extensão das redes LAN os custos de implementação bem como as preocupações com a segurança tornaram-se fatores fundamentais a ter em conta. Por estas razões, a tecnologia *vlan* assumiu um papel de destaque sendo usada com muita frequência. Esta tecnologia permite não só a economia de equipamentos e consequente diminuição de custos de implementação mas também proporciona uma gestão mais inteligente e equilibrada das redes, diminuindo assim os domínios de colisão e consequente perda de pacotes. Por outro lado aumenta consideravelmente a segurança devido à divisão das grandes redes em pequenas redes lógicas distintas.

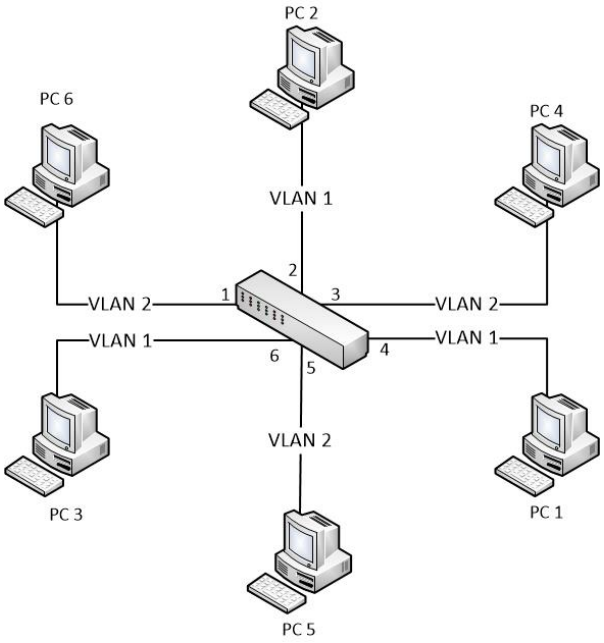
Para fazer divisão de uma rede empresarial em varias outras pequenas redes, sem o uso das *vlans*, exige a instalação de diferentes equipamentos para cada uma das pequenas redes, como ilustra o Esquema 8.



Esquema 8 - Divisão de uma rede empresarial sem vlans

Como é evidente, é necessário a implementação de dois *switch*es para dividir as duas redes representadas. De salientar, que não existe conectividade entre as duas redes, uma vez que não existe qualquer equipamento de ao nível 3 (*Network*) como é o caso de um *router*, que permita o roteamento entre as duas redes. Desta forma é possível usufruir de todas as vantagens adjacentes à divisão de redes num ambiente empresarial, tais como: diminuição de tráfego, menor número de domínios de colisão e aumento da segurança. No entanto, é necessário a instalação de vários equipamentos para este efeito, solução algo dispendiosa a nível monetário e trabalhosa a nível técnico.

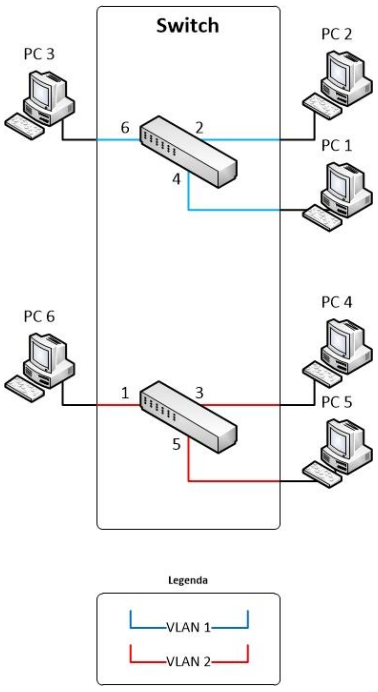
Com o aparecimento da tecnologia de *vlans*, nomeadamente o padrão IEEE 802.1Q, a divisão de uma rede tornou-se mais simples, pois é possível dividir o tráfego das diferentes redes usando os mesmos equipamentos. Seguindo o exemplo apresentado no Esquema 9, com esta tecnologia apenas é necessário um *switch*es que tenha capacidade de interpretar *vlans*. Desta forma, a quantidade de equipamentos reduz e a fiabilidade da rede mantém-se. Tal como demostrado no seguinte esquema.



Esquema 9 - Divisão de uma rede empresarial com recurso a vlans

O tráfego de uma *vlan* é completamente separado do tráfego da outra, como se fossem redes separadas fisicamente, tal como demostra o Esquema 10, onde podemos ver a existência de um *switch* virtual para cada *vlan*.

Nesta tecnologia, é atribuída a cada porta do *switch* uma determinada *vlan*, desta forma apenas existe comunicação entre portas pertencentes à mesma *vlan*. Assim sendo, cada *vlan* representa um domínio de difusão.

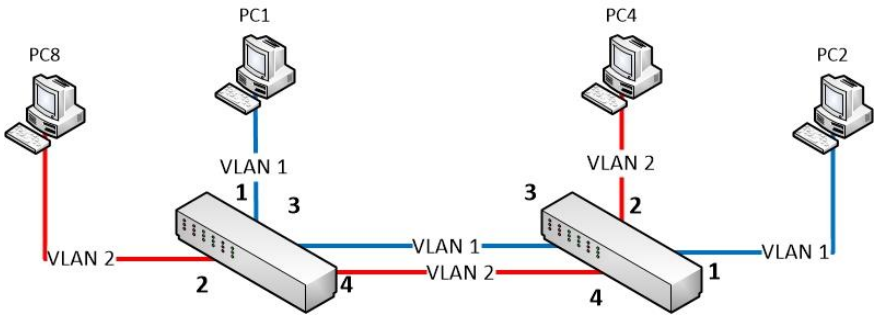


Esquema 10 - Funcionamento de um switch com vlans

Imaginemos que o PC3 decide enviar um pacote *broadcast*. Apenas o PC1 e o PC2 vão receber esse *broadcast* uma vez que são os únicos que tem registo na FDB (*forwarding database*). Os registos da FDB comportam-se da mesma forma como num *switch* convencional, ou seja, são atualizados com base no endereço de origem, desta forma a FDB do PC 3 só tem conhecimento dos endereços do PC1 e o PC2. Concluindo, num ambiente de *vlans*, existe uma FDB diferente para cada *vlan*. Neste caso, isto significa que a *vlan* 2 nunca vai aprender sobre o PC1, PC2 ou PC3 (Alcatel-Lucent, 2008).

4.4.1. *Vlan* Trunking

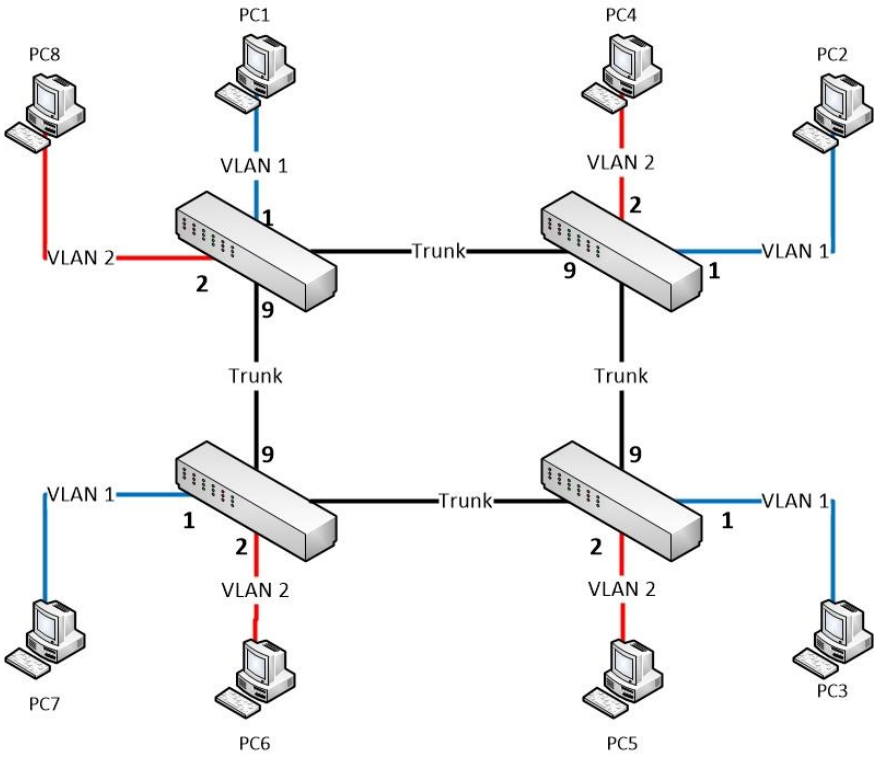
Na maioria das vezes, é importante que uma ou várias *vlans* se espalhem por mais do que um *switch*, dessa forma, como cada porta pertence a uma *vlan*, seria necessários existir, entre os *switch*es, pelo menos uma ligação física, para cada *vlan*. Só assim poderíamos estabelecer ligação entre os vários *switch*es de determinada *vlan*. No entanto isto é bastante dispendioso implementar (Esquema 11).



Esquema 11 - Interligação entre switches sem uso a trunk

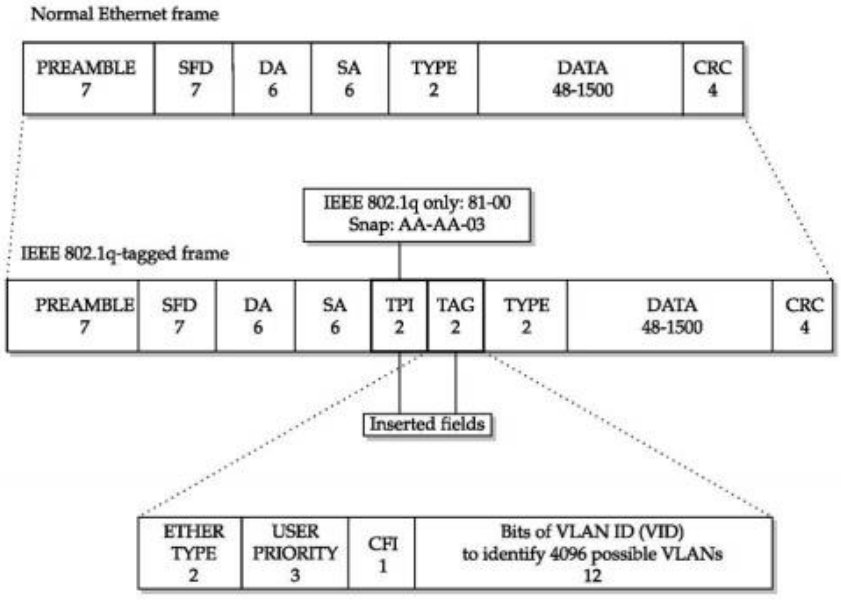
Como forma de resolver este problema, é possível atribuir às portas dos *switch*es um dos dois tipos de configuração: modo *access* e modo *trunk*.

Uma porta em modo *access* está atribuída apenas a uma *vlan*, e numa porta em modo *trunk* passa tráfego de várias *vlans*. Esta porta em modo *trunk* é usada para fazer a ligação entre os vários *switch*es da rede sem haver necessidade de usar múltiplos cabos. Tal como ilustra no Esquema 12, onde a porta as portas 9 de cada *switch* estão configuradas em modo *trunk* enquanto que as restantes portas estão em modo *access* pois fazem a interligação entre o *host* e o *switch*es (Alcatel-Lucent, 2008).



Esquema 12 - Interligação entre switches com portas trunk

Quando um *switch* recebe uma trama vinda de uma porta *trunk*, esta pode ser de qualquer uma das *vlans*, logo, é imprescindível existir um mecanismo de identificação de *vlans*. Para tal, nas tramas que viajam entre ligações *trunk* é inserido um cabeçalho com uma etiqueta *vlans* (*vlantag*). Nas portas em modo *trunk* o encapsulamento das tramas é feito de uma forma diferente do que as tramas de Ethernet normais. Tal diferença pode ser constatada no Esquema 13.



Esquema 13 - Encapsulamento ethernet normal e vlantag

Assim sendo, podemos concluir que, na maioria dos casos, para a comunicação entre *switch*es, configuramos as interfaces como *trunk* (*tagged*). Para comunicação entre *switch*es e *host*s, servidores, impressoras, entre outros, configuramos as interfaces como *access* (*untagged*). As interfaces configuradas como *tagged* vão encapsular as tramas *Ethernet* segundo a norma IEEE 802.11Q, ou seja com a *tag* que possui a *vlan* ID (Alcatel-Lucent, 2008).

4.5. Protocolos de autenticação *wireless*

As redes *wireless* são a topologia de rede mais propícia a ser alvo de ataques, pois apenas é necessário estar ao alcance do sinal de radio para tentar ingressar indevidamente na rede. Sendo este o principal fator negativo quando pensamos em implementar uma rede *wireless* (Gast, 2002).

Por este motivo, a segurança nestas redes tornou-se um fator muito importante quando pensamos na sua implementação. Como forma garantir a segurança nas redes, foram, ao longo do tempo, desenvolvidos protocolos de autenticação à rede, que visa limitar e proteger o acesso às redes *wireless* (Barbosa, 2009).

O Padrão IEEE 802.1x é uma camada de autenticação padronizada pelo IEEE baseada em portas de aceso através do *RADIUS*. Este padrão utiliza o protocolo EAP usando vários métodos de autenticação, tais como:

4.5.1. EAP-TLS *(Transport Layer Security)*

- ✓ Usa o certificado SSL (Secure Sockets Layer);
- ✓ Criptografia PKI (*Public Key Infrastructure*);

4.5.2. EAP-TTLS (*Tunneled Transport Layer Security*)

- ✓ É uma extensão do protocolo TLS;
- ✓ Criar um túnel encriptado;
- ✓ Autenticação do cliente feita por *username* e *password*;

4.5.3. EAP-PSK (Pre-Shared Key)

- ✓ Usa uma chave pré partilhada;
- ✓ Exige a troca de quatro mensagens (*four-way handshake*);

4.5.4. EAP-MD5 (*Message-Digest algorithm 5*)

- ✓ Extremamente vulnerável a ataques;
- ✓ Não suporta a geração de chaves;
- ✓ Não suporta autenticação mútua;

4.5.5. PEAP (*Protected Extensible Authentication Protocol*)

- ✓ Criado como padrão aberto;
- ✓ Criptografia PKI;
- ✓ Criar um túnel encriptado;

4.6. Protocolos de encriptação *wireless*

Como forma garantir a segurança nas redes foram desenvolvidos protocolos de encriptação de conteúdo. A criptografia apareceu por volta de 1900 a.C. exatamente com o mesmo objetivo que hoje é utilizada nas redes de computadores.

O seu objetivo é transformar algo original numa outra forma ilegível, de forma que apenas o seu destinatário consiga recolocá-la na forma original conseguindo interpretar o seu conteúdo. Em teoria apenas o detentor da chave de descodificação consegue tal feito, o desconhecimento dessa chave torna impossível a leitura.

Em concordância com a criptografia dos nossos antepassados, criptografar dados significa codificá-los, utilizando um algoritmo e uma chave secreta, de tal forma que somente o destinatário, aquele que possua a chave secreta possa decodificá-los (Vilela & Ribeiro, 2007).

Por norma as opções para o tipo de criptografia que podem ser usadas são:

4.6.1. WEP - *Wired Equivalent Privacy*

Este protocolo foi dos primeiros a ser usado nas redes sem fios, apesar de ainda ser utilizado nos dias de hoje, possuiu muitas vulnerabilidade e falhas que colocam em causa a segurança, quer nas comunicações quer na autenticação na rede. Apresenta vulnerabilidade ao nível da troca de chaves, pois é feita de forma manual, bem como o vetor de inicialização, que é relativamente pequeno. Hoje é considerado totalmente inútil face às ferramentas existentes para efetuar ataque as redes (Lewis & T. Davis, 2004).

4.6.2. WPA - *Wi-Fi Protected Access*

Devido às falhas existentes no protocolo WEP foi desenvolvido o WPA, com a intenção de corrigir as falhas existentes anteriormente. Deste modo, podemos dizer que o WPA é um WEP melhorado. A troca de chaves pode ser feita manualmente como acontece no WEP, no entanto permite a autenticação de utilizadores, usando o padrão 802.1x e EAP (*Extensible Authentication Protocol*), podendo ser configurado para utilizar um servidor RADIUS para autenticação de utilizadores. Atualmente, já é considerado inútil devido ao aumento das ameaças.

No entanto, já existe um WPA2 que possui um nível de segurança mais elevado, suficiente para ser usado em ambientes governamentais e institucionais (Lewis & T. Davis, 2004).

4.6.3. Comparação de protocolos

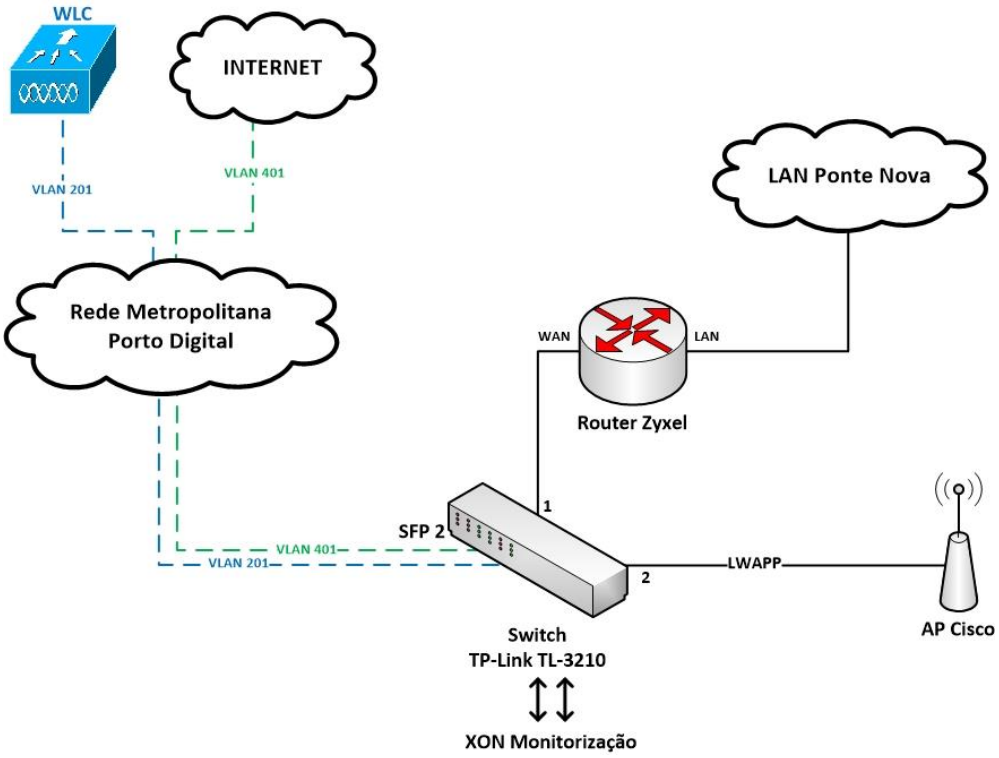
	WEP	***WPA***
Encriptação	Facilmente quebrada	Sem falhas de segurança
	Chaves estáticas de 64 e 128 bits	Chaves dinâmicas de 128 bits com Login
	Distribuição de chaves manual	Distribuição de chaves automática
Autenticação	Autenticação baseada no dispositivo	Autenticação baseado no utilizador usando 802.1x e EAP

Esquema 14 - Comparação protocolo WEP/WPA

5. Prova de conceito

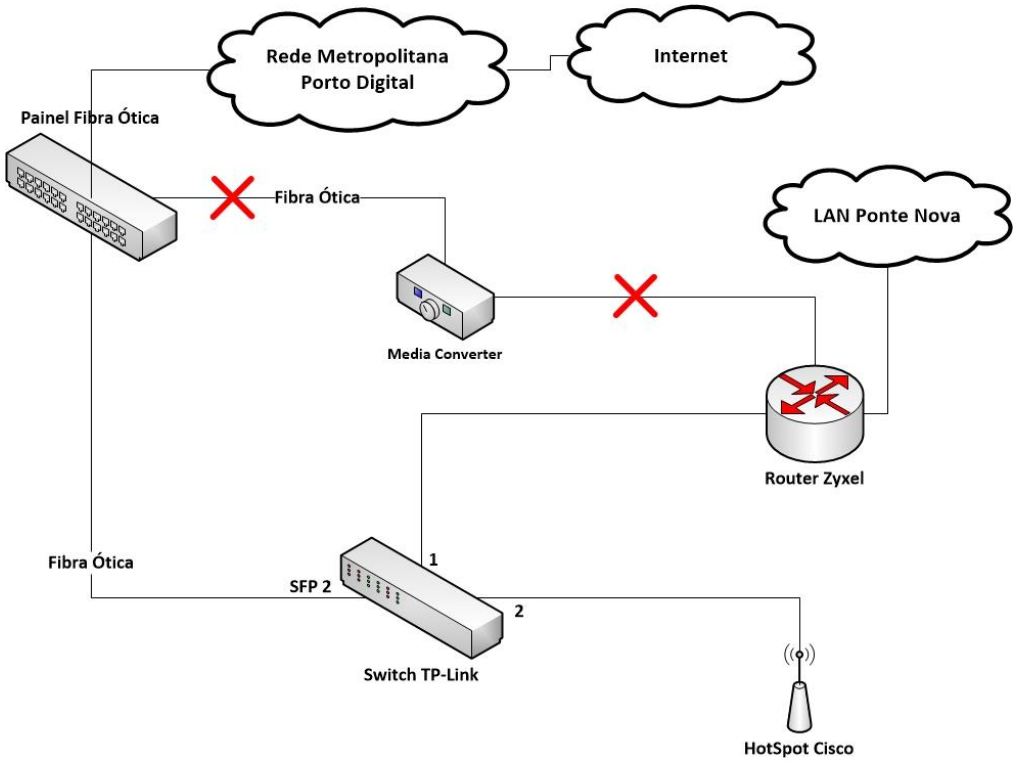
5.1. Camada Física

Como forma de testar o funcionamento dos *access point's* que futuramente vão ser instalados nos bairros sociais foi colocado um exemplar Cisco Aironet 1200 nas instalações da APD na Ponte Nova, para efeitos de prova de conceito. O conceito inicial é o apresentado no Esquema 15, de notar que a única diferença entre esta prova de conceito e o cenário existente nos Bairros Sociais é a utilização de um *switch* TP-Link no nosso edifício e nos bairros o equipamento presente é um XON de monitorização com capacidades de *switching*.



Esquema 15 - Conceito a implementar

Para esse efeito foi necessário proceder a algumas alterações na topologia de rede existente neste edifício. Nestas instalações, existia um *Media Converter* que era responsável pela conversão do sinal de fibra ótica em sinal elétrico. No entanto este equipamento foi substituído por um *switch* que para além de ter também essa funcionalidade permite a distribuição do sinal para vários elementos de rede como por exemplo o *router* e o AP *cisco* (ver Esquema 16).



Esquema 16 - Alteraçoes fisicas na APD-PonteNova

5.2. Configuração do AP

Em seguida foi necessário converter o modo de funcionamento do AP para o modo *Lightweight* de forma a ser possível a sua integração num Controlador LAN (WLC- *wireless LAN Controller*) existente na rede. Este modo de funcionamento é usado quando os AP's são controlados por uma controladora central que possui todas as configurações necessárias, ou seja, é retirada a maior parte da inteligência aos AP's.

Lightweight AP

O LAP (*Lightweight access point*) é um equipamento projetado para ser conectado a um controlador (WLC) que apenas possui funcionalidade MAC, ou seja, apenas interpreta *Layer* 2. Este equipamento funciona em IEEE 802.11a/b/g, não possuindo capacidade para agir de forma autónoma pois é o WLC que fornece todas as configurações e os *firmeware* necessário. O WLC controla os LAP's a si ligados. A comunicação entre os LAP's e o seu controlador WLC é feita através do protocolo LWAPP (*Lightweight access point Protocol*) que permite ao LAP fazer o *download* do *firmeware* e configurações necessárias, bem como o encaminhamento de todo o tráfego de cliente (Cisco Systems, 2007).

Fat AP

Os FAP (*Fat access point*) são AP's que funcionam individualmente e são geridos através de protocolos como o SNMP ou o HTTP ou então diretamente através da CLI. Para fazer a gestão dos FAP é necessários efetuar as configurações individualmente através de um destes sistemas de gestão. Cada FAP é visto na rede como um nó separadamente.

5.2.1. Servidor DHCP

Sempre que é feito um *reset* as configurações AP Cisco Aironet 1200 este assume um IP dinâmico, pelo que nos obriga a criação de um servidor DHCP como forma lhe atribuir um endereço IP ao AP. Para tal efeito foi usada a ferramenta TFTPd32 apenas com o objetivo de atribuir um endereço IP ao AP Cisco.

Configurei a carta de rede da minha máquina com um IP fixo (ver Figura 1).

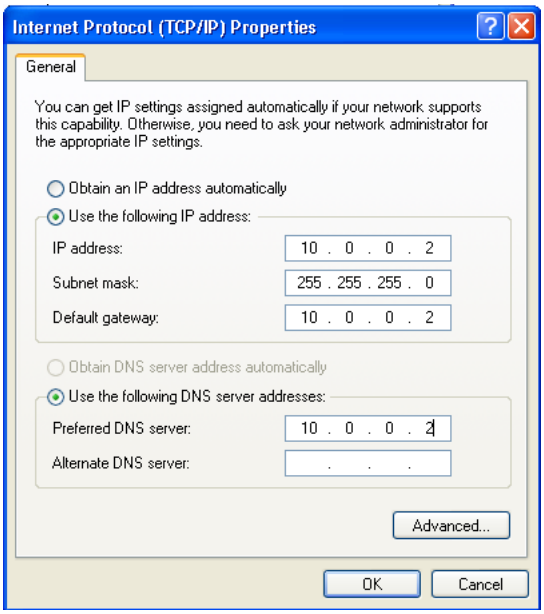


Figura 1 - Configuração carta de rede do PC

Configuração do TFTPd32 de forma a funcionar como servidor DHCP (ver Figura 2).

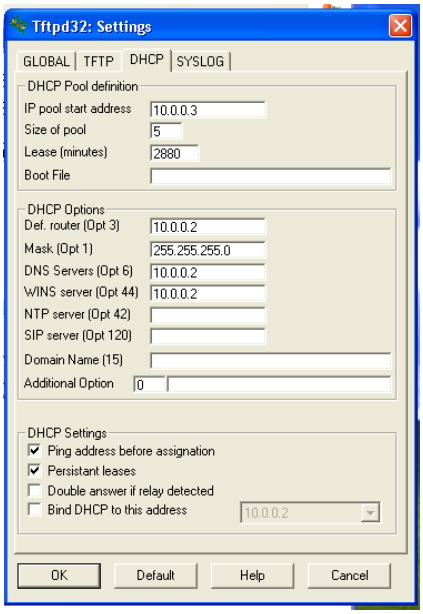


Figura 2 - Criação do servidor DHCP

Assim que é feito o *reset* nas configurações do AP este entra em contanto com o servidor DHCP instalado na máquina. Este servidor é responsável pela atribuição de um IP fixo, neste caso o endereço IP 10.0.0.3 (ver Figura 3).

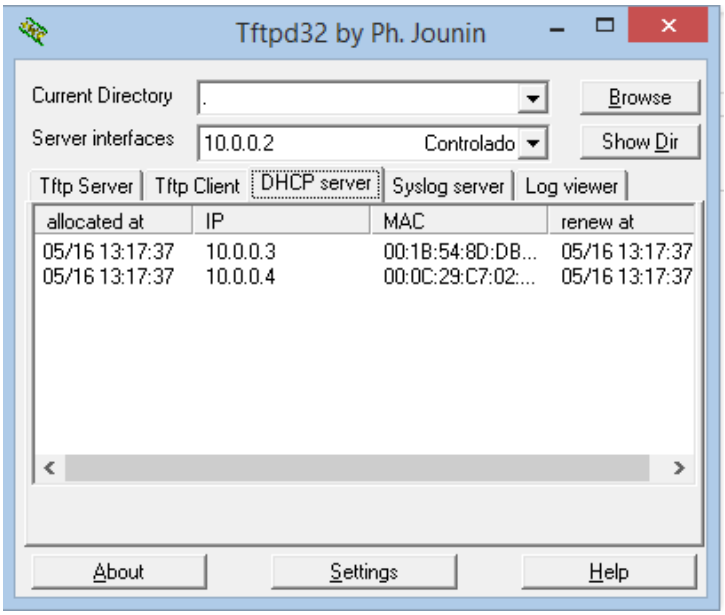


Figura 3 - Funcionamento do servidor DHCP

5.2.2. AP Cisco Upgrade

Para atribuir as funcionalidades de LAP (*Lightweight access point*) foi necessário efetuar um *upgrade* ao AP Cisco usando a ferramenta *Cisco Upgrade Tool*. No entanto, esta ferramenta apenas funciona em ambiente Windows XP logo, foi essencial a criação de uma máquina virtual usando o VMware com o sistema operativo XP. A esta máquina virtual foi atribuído o endereço IP 10.0.0.4 tal como se pode verificar na figura a cima.

Finalizado o *upgrade*, o AP ficou em modo *Lightweight* à espera de se ligar a um controlador, WLC (Cisco Systems, 2013).

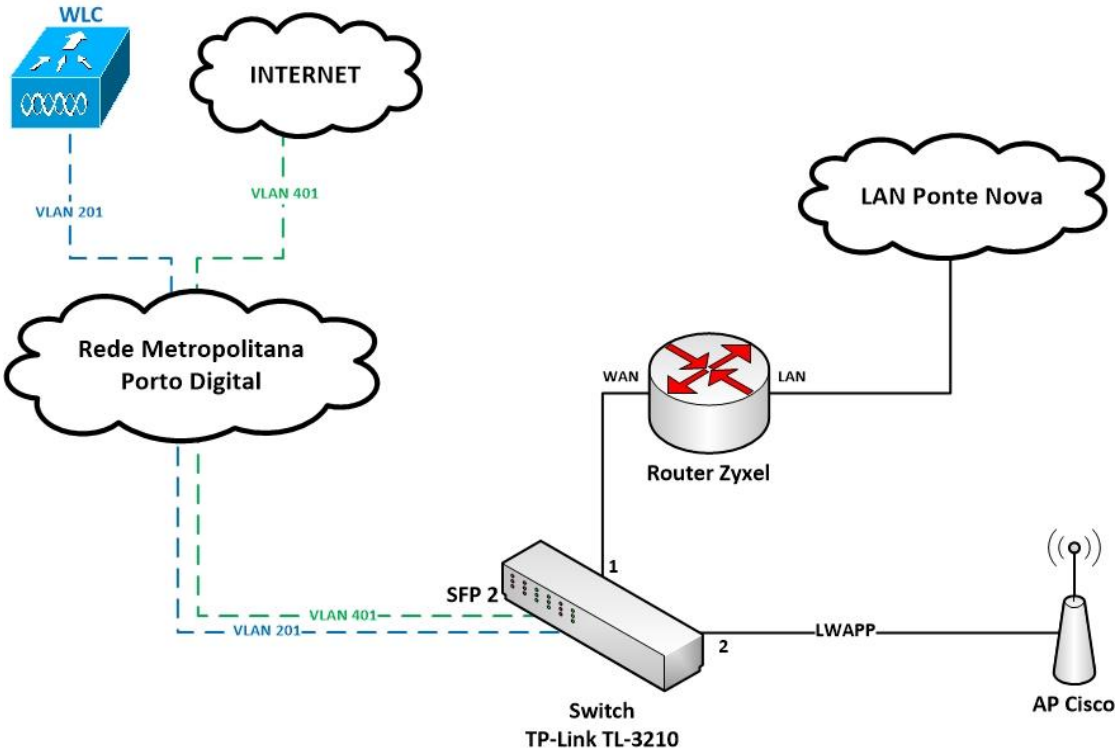
5.3. Configuração do *switch*

Tal como sugere o Esquema 17, foi necessário configurar um *switch* TP-Link de forma a tratar o diferente tráfego que por ele passa. Este *switch* tem a particularidade de falar *vlans* o que permite ter diferentes *vlans* em outras tantas portas.

Neste caso, a porta 1 está ligada à porta WAN do *router Zyxel*, que permite a conectividade à LAN do edifício. Esta porta recebe pacotes da *vlan* 401e funciona em modo *untagged*, ou seja, remove as etiquetas *vlans*.

A porta 2 liga ao AP Cisco, onde viaja tráfego LWAPP. Esta porta recebe tráfego da *vlan* 201 vinda do controlador WLC. Funciona também em modo *untagged*.

A porta 10 agrega estas duas *vlans*, por isso funciona em modo *tagged*. Esta porta permite a ligação à rede metropolitana de fibra ótica da Associação Porto Digital. Esta porta leva a *vlan* 401 até uma f*irewall* com acesso à Internet e a *vlan* 201 até ao WLC. Desta forma assume um modo *tagged*, pois todo o tráfego é marcado com as respetivas etiqueta *vlans*.



Esquema 17 - Esquema de rede APD-PonteNova com vlans

5.4. Configuração WLC

O passo seguinte passa pela configuração do controlador a fim de adicionar o AP cisco ao WLC para que seja configurado e gerido.

A configuração do WLC é bastante simples, sendo apenas necessário estar na mesma gama de endereçamento IP que o *access point* recebeu do servidor DHCP.

Assim que tal acontece o AP adiciona-se automaticamente ao WLC descarregando o *firmware* de configuração ficando gerivel através do WLC, tal como ilustra a Figura 4.

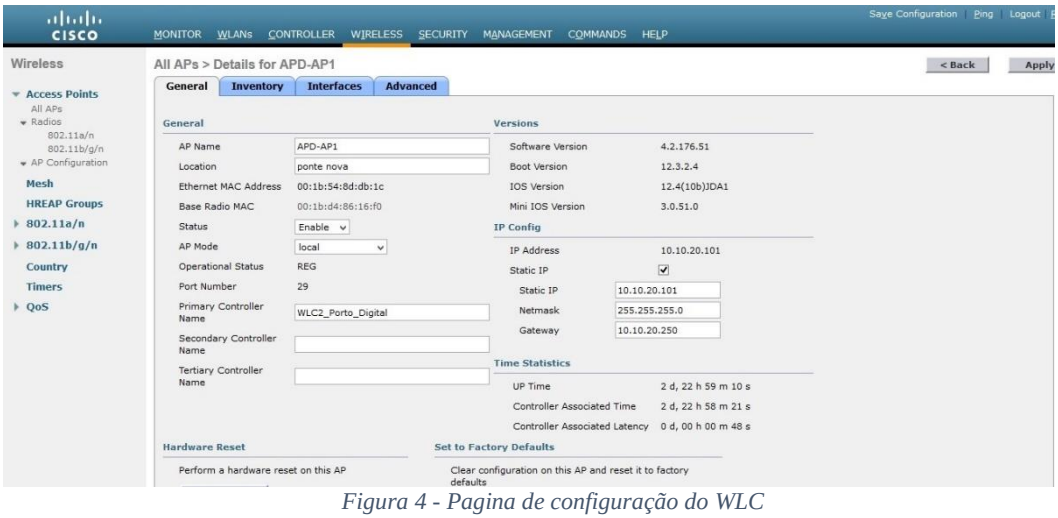


Figura 4 - Pagina de configuração do WLC

5.4.1. Configurar Interface

Antes da criação de *wlan*'s devemos indicar por qual das interfaces vão ser enviados os respetivos dados de navegação. Estas interfaces têm correspondências às *vlans* existentes. Ou seja, cada *vlan* está associada a uma interface. A Figura 5 apresenta as diferentes interfaces existentes no WLC e a sua respetiva *vlan* ID bem como o seu endereço IP.

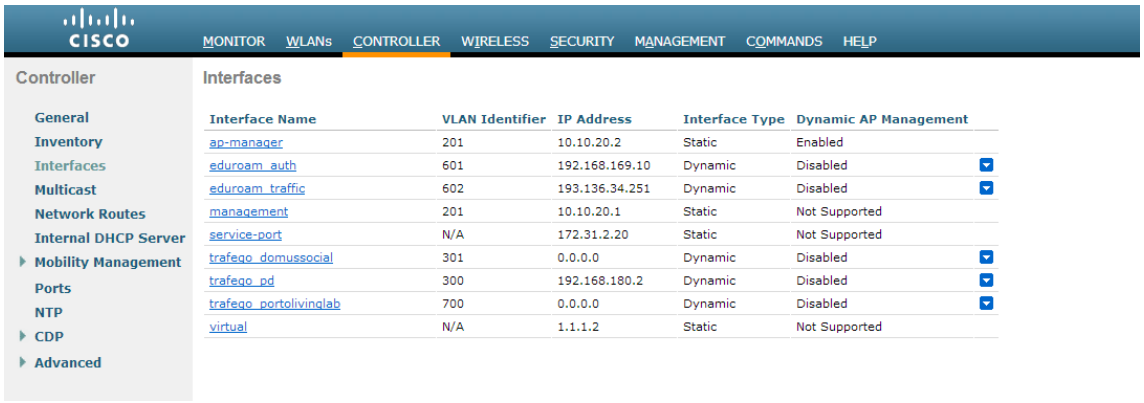


Figura 5 - Configuração das interfaces

5.4.2. Configuração *wlan*'s

Cada WLC tem a capacidade de possuir diferentes *wlan*'s (*Wireless* LANs) e assim sempre que é adicionado um novo AP as diferentes *wlan*'s são publicitadas por estes. Na prática o mesmo AP pode disponibilizar diferentes redes de acesso com características distintas e objetivos diferentes.

Dito isto, foi criada uma *wlan* com o intuito de satisfazer a proposta inicial do meu projeto que é disponibilizar Internet aos bairros sociais da CMP. Desta forma, a *wlan* "DomusSocial" vem satisfazer este requisito estando o seu nome associado a DomusSocial, entidade que gere e regula os condomínios dos bairros sociais da CMP e que trabalha neste projeto em parceria com a APD. De realçar que a nível de acesso não contêm qualquer tipo de restrição de utilização tal como se pode verifica na Figura 6.

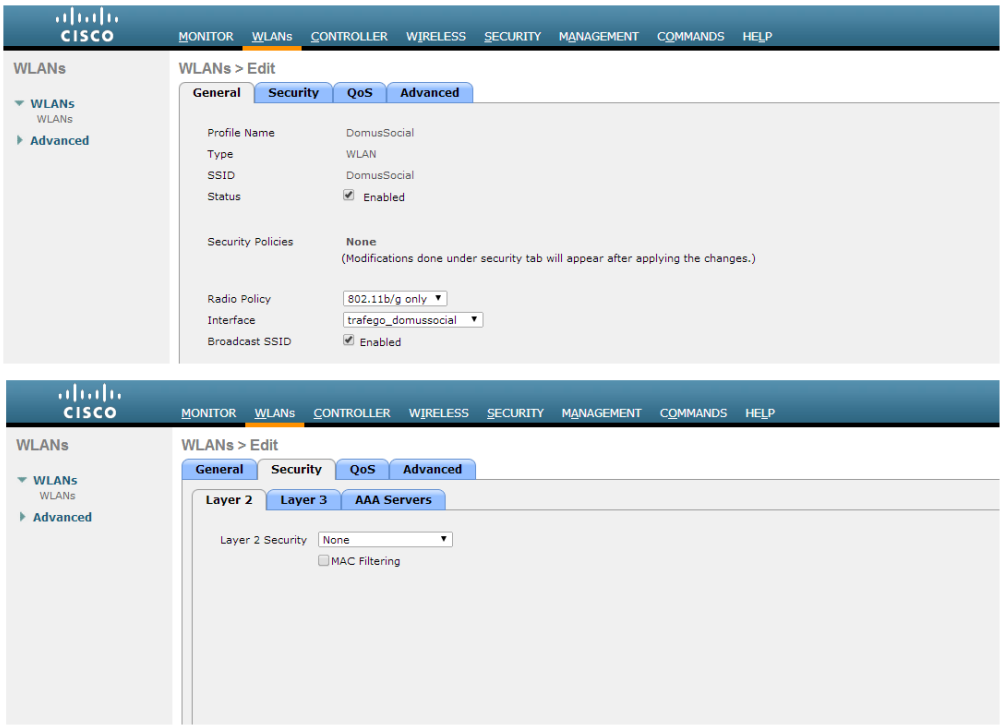


Figura 6 - WLAN DomusSocial

6. Expansão da rede *Wi-Fi*

Com referido anteriormente o objetivo deste projeto é expansão da rede *wireless* da APD, recorrendo a instalação de *access point's* nos bairros sociais da cidade do Porto. Desta forma foram realizadas algumas diligências para a concretização deste projeto com sucesso.

Visto que a Associação Porto Digital está presente com fibra ótica em 15 bairros sociais do Porto foram estes os bairros sociais escolhidos para esta intervenção e desta forma potenciar a existência de fibra ótica nestes locais. Na Figura 7estão representados os bairros sociais que receberam os *access point's*, bem como informações acerca da sua localização geográfica, incluindo o nome do bairro, bloco e entrada onde estes foram instalados.

Figura 7 - Localização geográfica dos Bairros Sociais

6.1. Localização

Desde o início deste projeto que nos deparamos com alguns problemas sobre a escolha do local ideal onde colocar os equipamentos *wireless*. Uma das condicionantes é a obrigatoriedade de estes estarem no interior dos edifícios do bairro, visto serem *access point* de interiores que não podem estar sujeitos a condições climatéricas adversas como a chuva. Por outro lado, era importante assegurar que esta localização pudesse atingir o maior número de utilizadores possível, pelo que a sua localização teria de ser num local aberto e amplo que permitisse uma propagação considerável do sinal.

Por outro lado, era importante ter em consideração a acessibilidade ao equipamento. Esta teria de ser restrita, difícil de aceder, visto que este equipamento ter um valor comercial considerável é importante mante-lo num local que não seja de fácil acesso. Desta forma pretendemos prevenir a intervenção de estranhos no equipamento ou em casos mais extremos, o furto do mesmo. Este fator foi preponderante na instalação, sendo que, em cada bairro foi tomado isso em consideração de uma forma individual. Para aumentar a segurança foram adquiridas caixas protetoras, com fechadura, de forma a inibir qualquer intervenção nos equipamentos por indivíduos não autorizados.

Foram usadas caixas de PVC apropriadas para equipamento de telecomunicações, de forma a minimizar o seu impacto na propagação do sinal. Sendo o PVC um material plástico, reduz significativamente o impacto negativo quando delimitamos um equipamento protetor. No sentido de minimizar o impacto da caixa protetora na propagação do sinal, foram tomados alguns cuidados desde logo no material usado para o fabrico das caixas. Optamos por utilizar caixas em PVC, pois são de material plástico que não interfere com a propagação das ondas radio *WI-FI*. Estas caixas de PVC foram perfuradas, permitindo a circulação do ar no seu interior e assim obter um refrigeração mais eficiente, visto este fator ser bastante importante quanto à durabilidade do equipamento em questão.

6.2. Instalação

Depois de uma visita a todos os bairros sociais da cidade do Porto com presença de fibra ótica, foram identificados os Blocos e as entradas para a instalação do AP. Assim sendo, em cada bairro social foi selecionada apenas uma entrada que receberá o AP. Esta seleção teve como condicionante a presença de XON's de monitorização[1].

6.2.1. Planeamento e requisitos

No âmbito de um outro projeto da Associação Porto Digital, os referidos 15 bairros sociais, foram equipados com fibra ótica que transporta, entre outras coisas, sinal analógico de televisão. Este projeto tinha como objetivo continuar a fornecer à população dos bairros socias a possibilidade de assistir aos 5 canais de televisão públicos em modo analógico mesmo depois

[1] Equipamento que para além de converter o sinal de fibra em sinal ótico tem a também a capacidade de *switching*, possuindo 4 entradas LAN

de transição total para sinal digital. Neste projeto foram instalados em cada entrada dos vários blocos dos bairros sociais um XON. Este XON tem a capacidade de transformar o sinal de TV presente na fibra num canal analógico que se propaga por um cabo coaxial ate casa dos habitantes. No entanto, em algumas entradas foram instalados XON's de monitorização que permitem fazer uma leitura da potência da fibra, bem como a potência do sinal de televisão, permitindo assim a sua monitorização em tempo real. Estes XON's de monitorização têm a particularidade de funcionarem como um *switch* convencional. Desta forma, foram aproveitados estes equipamentos para fornecer conectividade aos *access point's*.

Evidentemente, a instalação dos AP's foi efetuada naquelas entradas que estão equipadas com XON's de monitorização. Desta forma, reduzimos o custo de implementação do projeto bem como rentabilizamos um equipamento já existente, que não estava a ser potencializado nas suas máximas valências.

6.2.2. Montagem

Antes de iniciar a montagem, foram realizadas deslocações aos locais que vão receber os *access point*, foram feitas fotografias e medições com o objetivo de estudar cada caso específico. Foram elaborados croquis que posteriormente foram apresentados à DomusSocial, entidade camarária responsável pela gestão dos bairros sociais do Porto, a fim de obtermos autorização para a realização da intervenção (ver Figura 8). Depois de algumas normas a respeitar por indicação da DomusSocial, procedeu-se ao início da montagem.

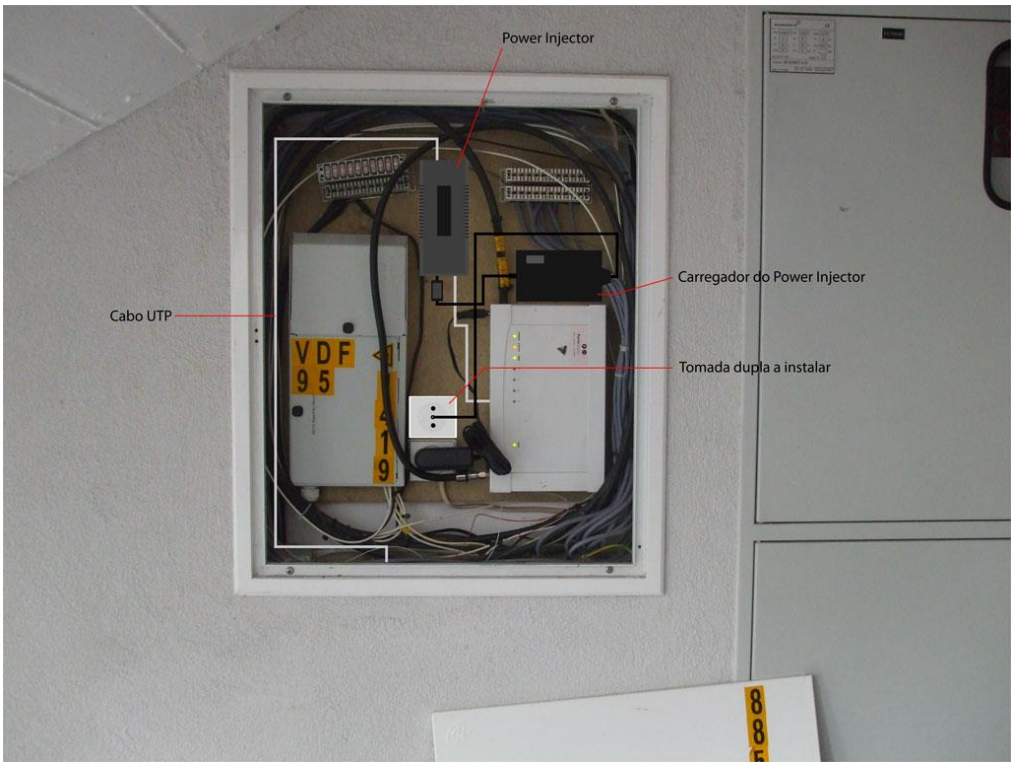


Figura 8 - Croqui da caixa de telecomunicações

Para explicar o processo de montagem foi escolhido o bairro de Aldoar. A escolha do exemplo recaiu sobre este bairro pois, a maior parte dos bairros sociais, que vão receber a nossa intervenção, tem uma infraestrutura muito similar a esta. São exceções a esta realidade os bairros do Carvalhido, Lordelo, Parceria Antunes e Lagarteiro. Todos estes bairros foram tratados de formas variadas e adequadas à situação real e específica de cada um.

A figura a cima demonstra a caixa de telecomunicações presente no piso zero no bloco 10 na entrada 120 do bairro de Aldoar. Esta caixa de telecomunicações é de acesso livre a todos os operadores de telecomunicações que pretenderem fornecer serviço, desta forma é normal existir equipamento de diferentes operadores de telecomunicações. Por tal motivo um dos problemas a ter em atenção é a ocupação do espaço, que na maioria das situações é bastante reduzido.

Nesta caixa de telecomunicações já existe o XON da APD a fazer a difusão do sinal de televisão para todo o prédio. Como referido anteriormente vamos usar este XON de monitorização como *switch* para oferecer conectividade ao nosso AP. Usamos um *Power Injector* com a objetivo de reduzir o número de cabos no exterior, visíveis. Esta tecnologia permite injetar energia elétrica num cabo UTP e, desta forma num só cabo fornecer ao AP conectividade e energia. Assim sendo, apenas é necessára a existência de um cabo UTP a ligar o XON ao AP.

Esta solução apresentou uma contrapartida na instalação, pois com a inclusão do *Power Injector* tornou-se indispensável a presença de dois pontos elétricos na caixa de telecomunicações. Cenário que não existia, portanto faz parte do processo de montagem dos AP a instalação de uma tomada elétrica dupla que fornecesse energia elétrica quer ao XON de monitorização quer ao *Power Injector* do AP.

Assim sendo, vamos usar a coluna montante para atingir a varanda do primeiro piso. Nesta localização o AP terá uma área de abrangência mais alargada pois permite a conectividade quer aos pisos superiores do prédio, como também à área exterior circundante do prédio. Ou seja, é usada a coluna montante do prédio para atingir o primeiro piso e dai é feita a ligação ao AP como ilustra a figura a baixo. Recordo que esta ligação é feita com o cabo UTP que possui dados e energia que vai ser encaminhada ate ao AP, fazendo-o funcionar difundindo a rede *wireless* da DomusSocial.

Como ilustrado na Figura 9, será colocada uma calha para efeitos de proteção no cabo UTP bem como uma caixa com fechadura para proteção do AP tal como referido anteriormente. Desta forma o AP fica fixo num ponto relativamente elevado e de acesso reservado para segurança do equipamento.

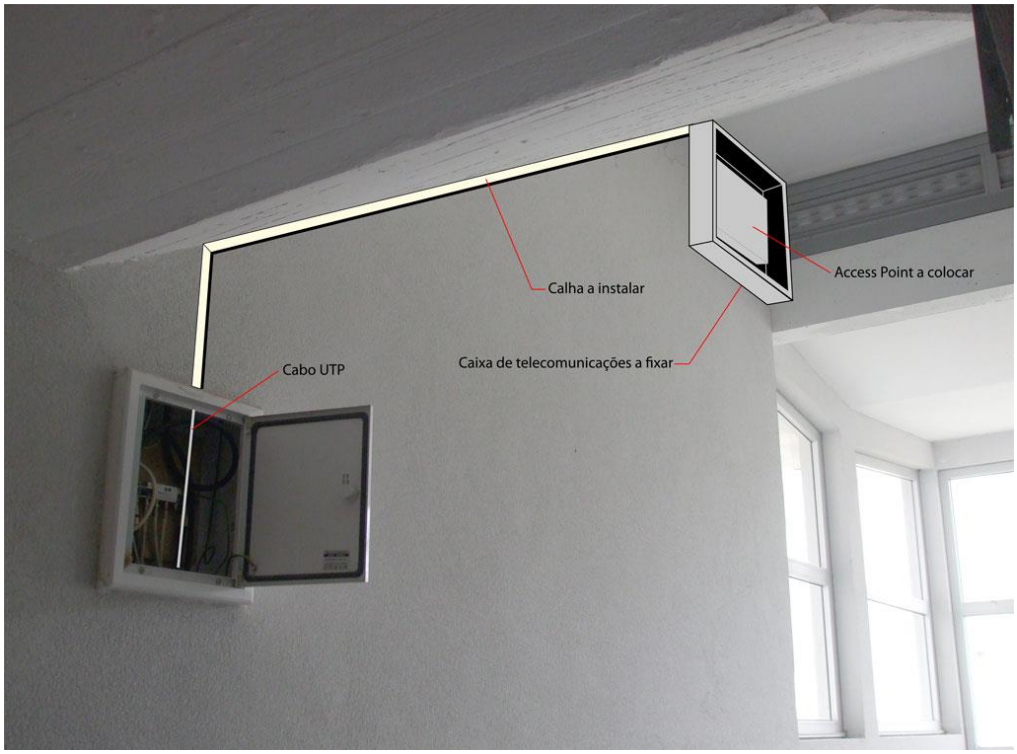


Figura 9 - Croqui da caixa de distribuição de piso1

6.2.3. Situação real da montagem

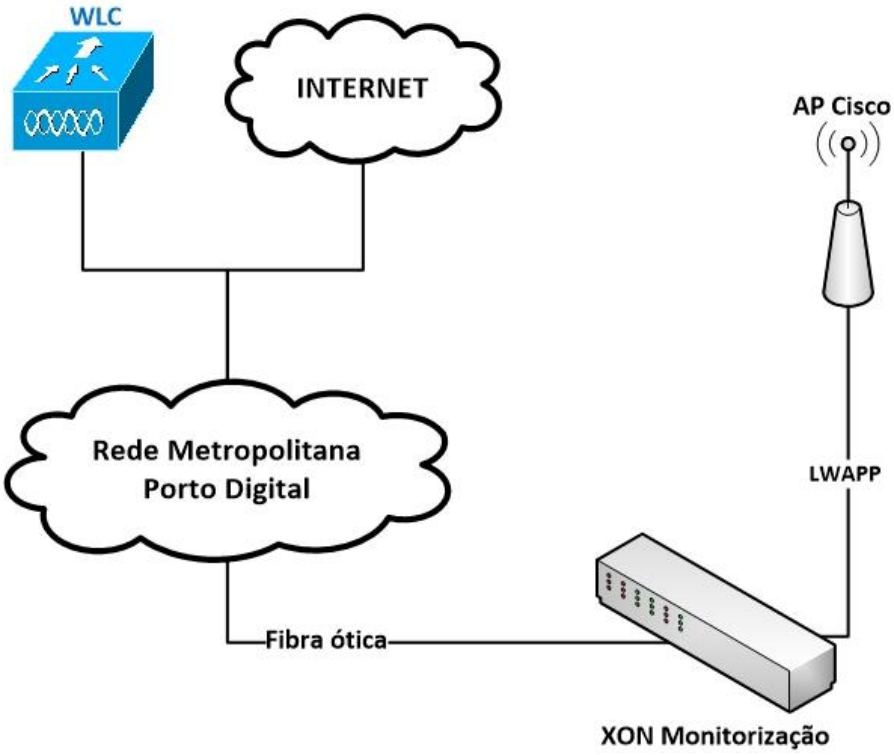
Depois do planeamento cuidado de todas as particularidades que podíamos encontrar em cada bairro social foi percetível que tudo correu como planeado. Sendo que os croquis realizados, foram em quase todas as situações, aplicados à risca. Relembro que para cada um dos quinze bairros sociais foram tiradas fotografias e feito um croqui de instalação individual com uma pequena descrição e legenda do esquema. Em todos eles esse croqui correspondeu à realidade na hora de montagem, sinal de que o planeamento foi feito com rigor. Deste modo, é natural que as fotografias tiradas depois de efetuada a intervenção sejam em tudo idênticas aos croquis acima apresentados. Tal com aconteceu com os croquis de montagem deixo o exemplo do bairro de Aldoar como forma de comparação dos croquis com as fotografias do trabalho final (ver Figura 10 e Figura 11).

Figura 10 - Cenário real caixa de entrada Aldoar

Figura 11 - Cenário real caixa de piso1 Aldoar

6.3. Configuração

Posteriormente à instalação do equipamento físico, iniciou-se uma nova etapa, a configuração dos vários elementos da rede para ser possível a conectividade entre o utilizador e a Internet. Tendo como base de funcionamento a prova de conceito já previamente realizada. O Esquema 18 ilustra como se pretende oferecer a conectividade entre os AP's distribuídos pela cidade do Porto e o WLC responsável pela sua gestão e controlo.



Esquema 18 - Esquema de ligação entre o AP ate ao WLC

6.3.1. Configuração do AP

À imagem do que aconteceu na instalação do AP de teste nas instalações da APD (situação descrita na Prova de conceito) a configuração necessária para o bom funcionamento dos AP's instalados é simples, uma vez que a toda a engenharia do processo se localiza no Controlador WLC. Desta forma apenas teremos que configurar o AP para funcionar em modo *Lightweight*. Assim o AP fica à espera de se adicionar a um controlador presente na rede. Assim que conseguir conectividade com o WLC presente na rede vai receber dele todo o *firmware* necessário ao seu funcionamento.

6.3.2. Configuração do XON

Como foi afirmado anteriormente o XON de monitorização é o ponto de entrada da fibra ótica no edifício, fornecendo 4 portas LAN. Usaremos uma dessa portas para ligar o nosso AP e, assim, permitir que este obtenha conectividade à rede da APD a fim de poder difundir sinal de Internet.

É importante referir que é nesta porta de rede que serão colocadas e retiradas as etiquetas *vlan*, ou seja, quando um pacote chega a esta porta vindo do AP, vai ser etiquetado com a *vlan* criada para o tráfego da rede DomusSocial. Quando chegar um pacote vindo da rede da APD

com destino ao AP vai ser removida a etiqueta *vlan*, para ser devolvida a trama Ethernet original ao cliente ligado ao AP.

Como podemos constatar o XON de monitorização vai fazer o mesmo trabalho do que o *switch* TP-Link que usamos na Prova de conceito.

6.3.3. Configuração do WLC

A próxima etapa passa pela configuração do controlador a fim de permitir o controlo dos vários AP´s Cisco instalados nos bairros sociais. Para efeitos de organização foi configurado um novo controlador com o nome de WLC2 que se destina à gestão apenas dos AP's dos bairros, sendo que o WLC fica responsável pela gestão de todos os outros AP's já existentes na APD espalhados pela cidade.

A primeira medida a tomar é adicionar o MAC dos AP's instalados à lista de autenticação do certificado SSC, como é ilustrado na Figura 12.

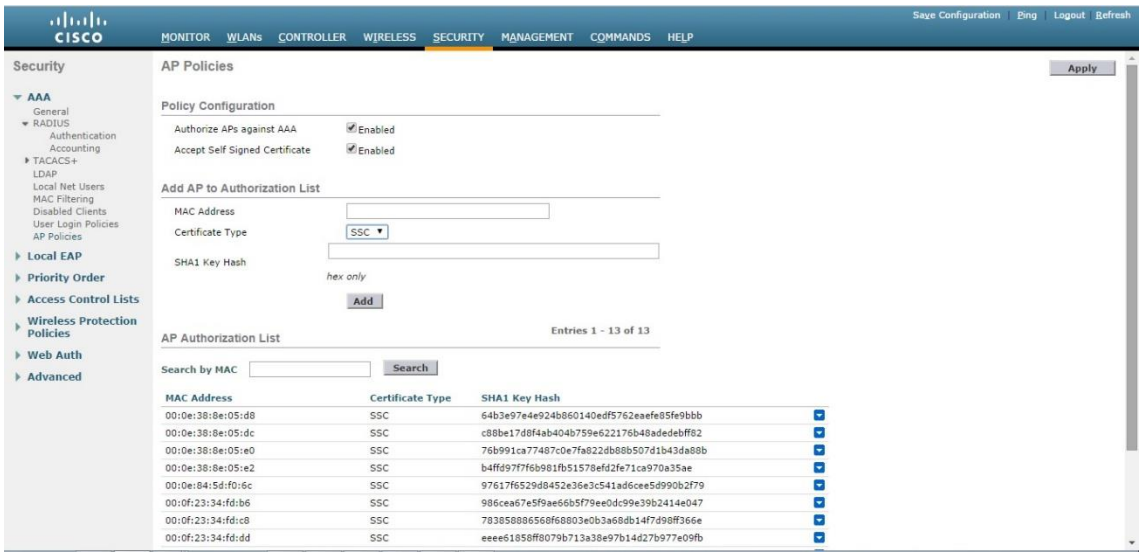


Figura 12 – Configuração AP Polocies

Assim que é aceite o certificado SSC o AP adiciona-se ao controlador, neste caso ao WLC2, e fica gerivel a partir neste momento.

Assim que o AP passa a integrar a lista de AP's do controlador é possível injetar em cada AP uma determinada configuração e *firmware* de funcionamento (Figura Nº 14).

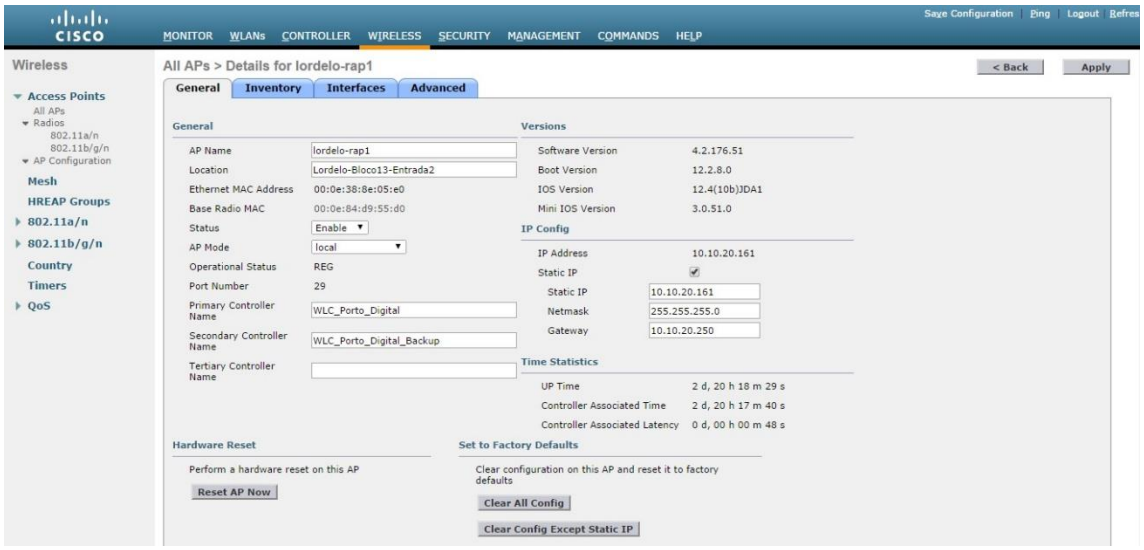


Figura 13 - Exemplo de configuração AP bairros

6.3.3.1. Certificado SSC

O certificado SSC - *Secure Services Client* é um *software* de autenticação que possibilita a integração de um AP com o controlador. Foi através deste certificado que adicionamos ao nosso controlador todos os AP's instalados nos bairros socias. O controlador possui uma lista de AP's que estão autorizados a adicionar-se a ele. Para adicionar um AP a esta lista usando o certificado SSC necessitamos de fornecer ao controlador o MAC do AP e o SHA1 Key Hash (ver Figura 14). Assim que o controlador fornecer o *firmware* ao AP este fica gerivel sendo adicionado à lista de AP geridos pelo WLC (Cisco Systems, 2007).

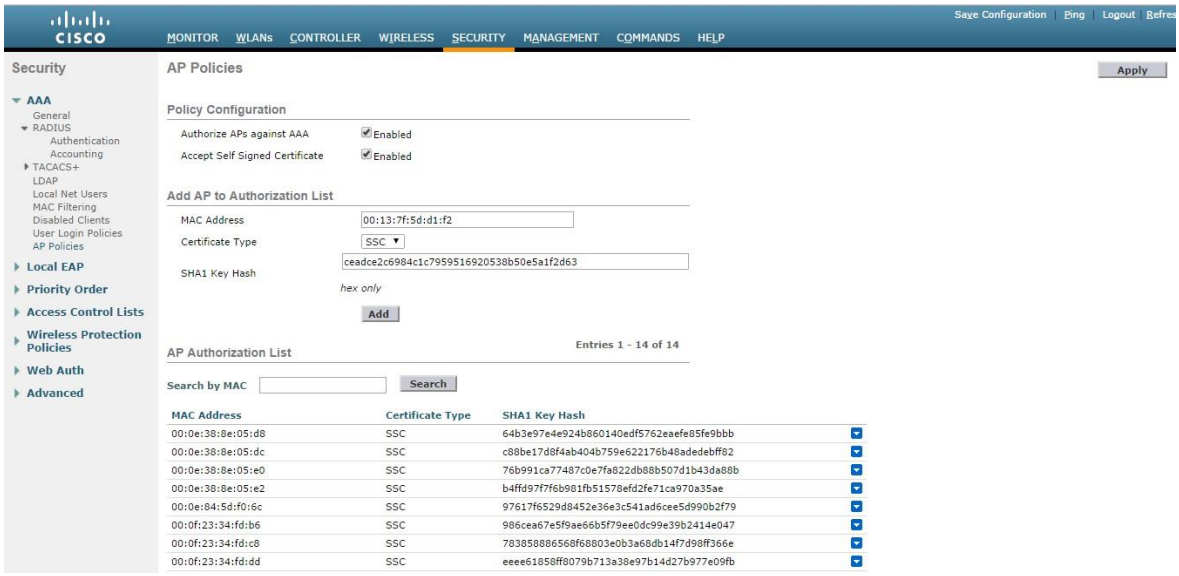


Figura 14 - Adicionar AP à controladora ussando SSC

6.3.3.2. Criação Interface

Tal como aconteceu na prova de conceito é necessário criar as interfaces por onde será enviado o tráfego gerado em cada *wlan*. A estas interfaces é associada uma *vlan* responsável pelo roteamento do tráfego no interior da nuvem da APD. Ou seja, cada *wlan* necessita de uma interface por onde envia o seu tráfego, ao mesmo tempo cada interface está associada a uma *vlan*. A Figura 15 apresenta as diferentes interfaces existentes no WLC e a sua respetiva *vlan* ID bem como o seu endereço IP.

Figura 15 – Interfaces existentes no WLC2

6.3.3.3. Criação WLANs

Figura 16 - Configuração de wlans

Como é possível constatar na Figura 16, o WLC2 possui quatro *wlan*'s diferentes e por consequência o AP Cisco, recentemente instalado, publicita essas mesmas *wlan*'s, já existentes noutros AP's da APD. Uma delas, a *wlan* "*Wi-Fi* Porto Digital" que permite um acesso livre e gratuito sem qualquer tipo de restrição, serve de expansão à rede de fibra ótica disponibilizada pela APD (Figura 17).

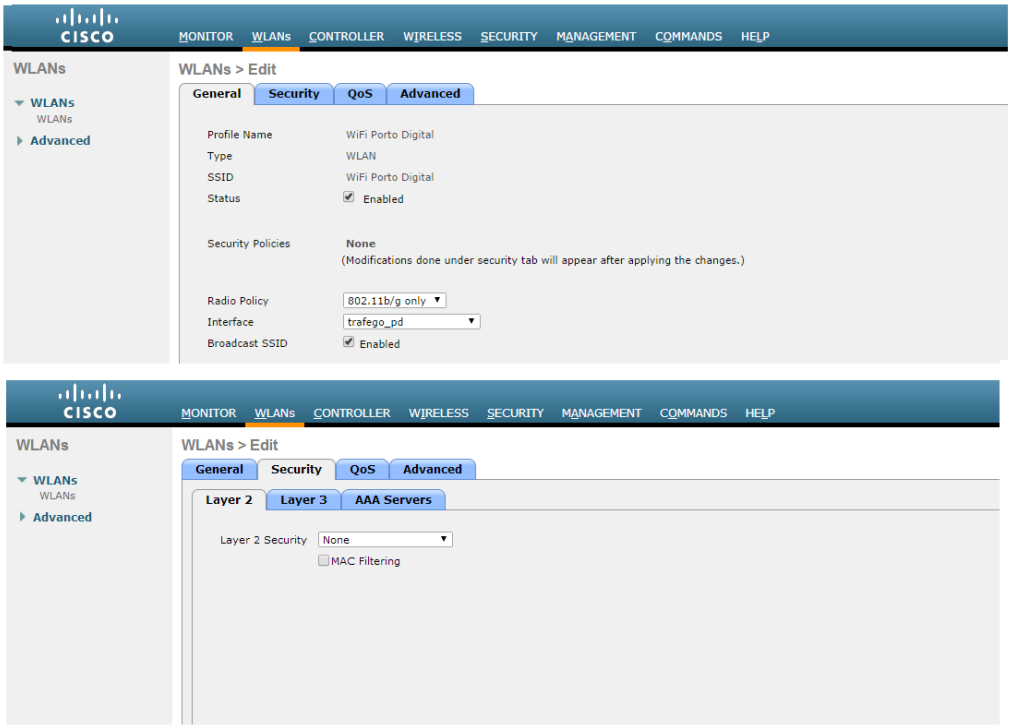


Figura 17 - WLAN WIFI PortoDigital

Outra das redes que o AP publicita é a *wlan* "eduroam", pois, é de todo o interesse a expansão desta rede universitária a fim de proporcionar cada vez mais mobilidade e serviços aos estudantes da comunidade académica nacional e europeia. Esta rede possui algumas especificações de segurança exigidas pela entidade que tutela este projeto Figura 18.

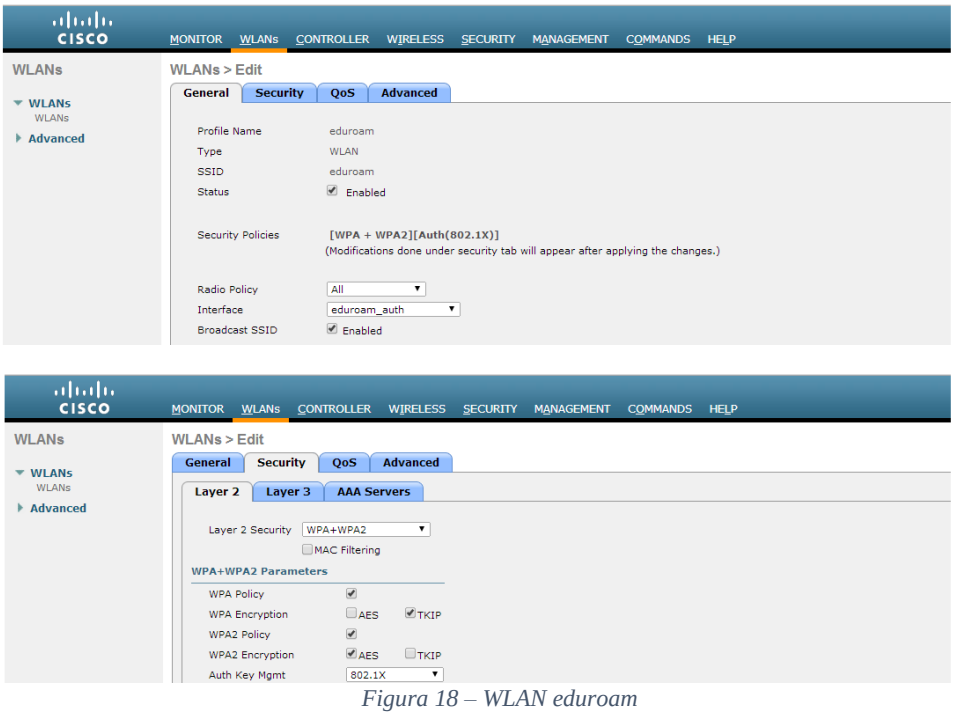


Figura 18 – WLAN eduroam

A terceira rede com o nome "portolivinglab" advém de uma projeto de parceria entre a APD e outras entidades. Esta rede tem como finalidade fornecer conectividade à Internet de sensores e outros dispositivos de domótica, inserido num projeto de cidades inteligentes que está a ser desenvolvido na cidade do Porto.

Para cumprir este requisito criei a quarta *wlan* com o nome "DomusSocial" sem qualquer tipo de necessidade de autenticação, tal como se pode verificar na Figura 19. Desta forma, a *wlan* "DomusSocial" vem satisfazer este requisito, estando o seu nome associado a DomusSocial, entidade que gere e regula os condomínios dos bairros sociais da CMP e que trabalha neste projeto em parceria com a APD. De realçar que o tráfego gerado por esta *wlan* usa a interface "trafego_domussocial" que foi criada explicitamente para este efeito como já foi referido anteriormente.

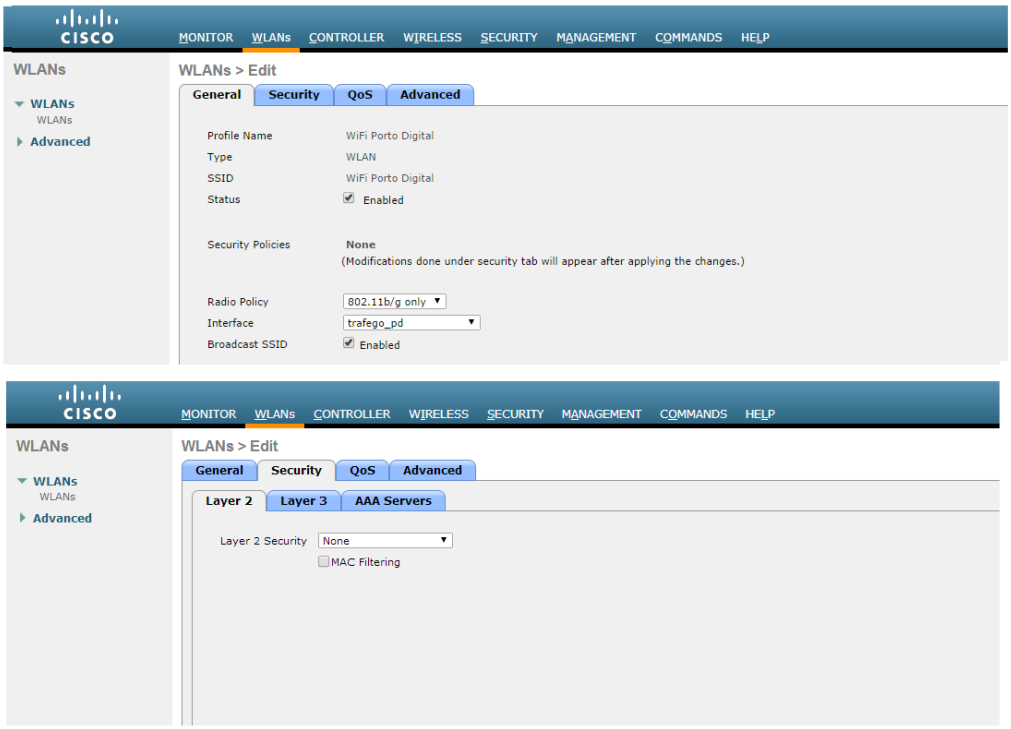


Figura 19 - WLAN DomusSocial

6.3.3.4. *Wlan* Override

Depois da criação das *wlan* acima mencionadas, um novo paradigma se levantou. O AP que se encontra nas instalações da APD não pode estar a publicitar a rede Wi- Fi da domus social, tal como não faz sentido os APs dos bairros estarem a publicitar a rede *Wi-Fi* da APD muito menos a rede do portolivinglab. Desta forma, é importante que o AP das instalações publicite as wlans "*Wi-Fi* Porto Digital", "eduroam" e "portolivinglab" ao mesmo tempo que os AP's presentes nos bairros socias apenas publicitam as wlans "eduroam" e "DomusSocial". Para isso usamos o *wlan* override. Esta tecnologia permite selecionar quais as wlans que vão ser publicitadas em cada um dos vários AP's do controlador WLC2. Assim sendo, já conseguimos controlar em que AP's vão ser difundidas determinadas *vlans*. Podemos verificar esta situação analisando a Figura Nº 21 e a Figura Nº 22. (Cisco Systems, 2007).

WLAN Override

WLAN Override: Enable

ID	WLAN profile	WLAN SSID	Select
1	WiFi Porto Digital	WiFi Porto Digital	☑
2	DomusSocial	DomusSocial	☐
3	portolivinglab	portolivinglab	☑
4	eduroam	eduroam	☑

Figura 20 - Configuração da WLAN Override do AP PonteNova

WLAN Override

WLAN Override: Enable

ID	WLAN profile	WLAN SSID	Select
1	WiFi Porto Digital	WiFi Porto Digital	☐
2	DomusSocial	DomusSocial	☑
3	portolivinglab	portolivinglab	☐
4	eduroam	eduroam	☑

Figura 21 - Configuração da WLAN Override do AP dos bairros sociais

6.4. Finalização e teste

Depois de concluída a instalação e configuração de todos os quinze *access* points correspondentes ao projeto foram realizadas visitas a todos os locais a fim de atestar o funcionamento real da rede *wireless*. Dessas visitas foram feitos testes de cobertura bem como teste de velocidade de navegação. Desta forma deixo aqui um exemplo de um teste de velocidade feito no bairro de Aldoar. Foi usado o *site* http://speedmeter.fccn.pt/ para realizar este teste. (ver Figura 22).

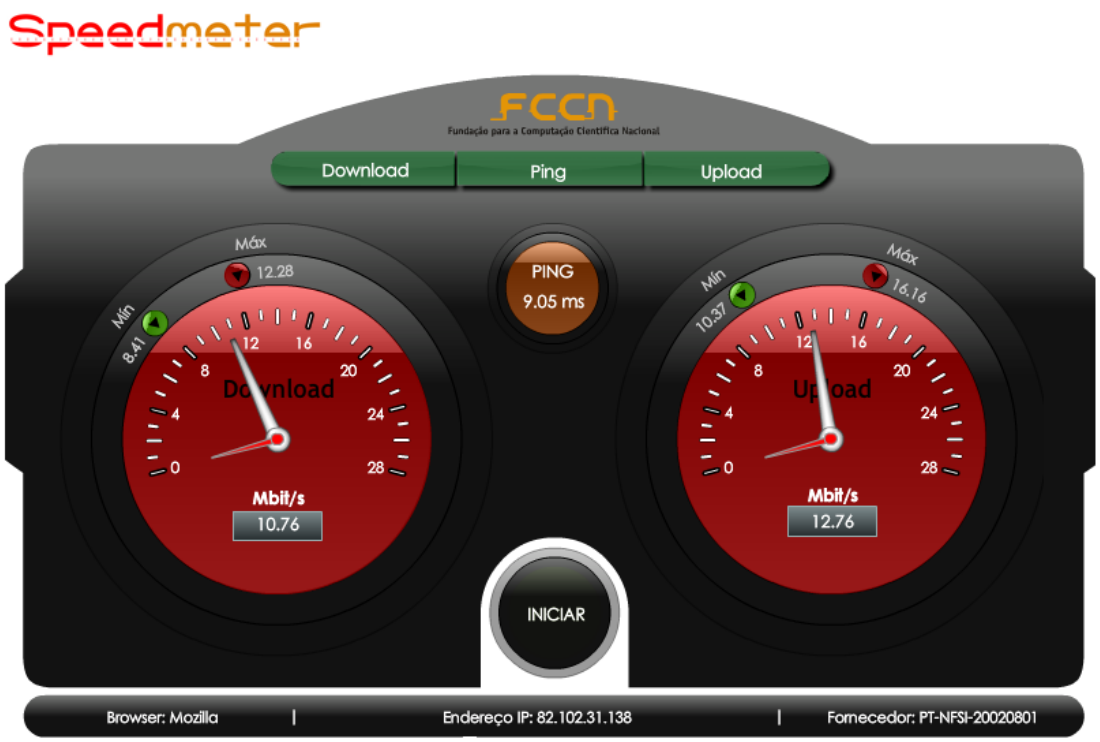


Figura 22 - Teste de velocidade AP Aldoar

7. Rede “eduroam”

Todos os AP’s instalados nos 15 bairros sociais do Porto têm a capacidade de publicitar várias redes *wireless*. Desta forma, para além de publicitarmos a rede da DomusSocial, que é o nosso principal objetivo, achei de todo pertinente e interessante publicitar também a rede “eduroam”. A rede “eduroam” é um projeto europeu que visa disponibilizar à comunidade académica um serviço de mobilidade entre universidades. Como membro da União Europeia, Portugal esta incluído neste projeto que tem vindo a ser tratado no âmbito da iniciativa da “e-U Campus Virtual” com participação ativa do Governo Português entre outras entidades ligadas à área das Tecnologias de informação (TI). Esta iniciativa visa agregar todas as redes de todas as instituições de ensino da Europa, permitindo, assim, criar uma rede do tipo “anytime, anywhere”. Ou seja promover a mobilidade dos estudantes e professores, em qualquer altura, incentivando e facilitando a produção, acesso e partilha de conhecimento. Esta iniciativa revelou-se bastante interessante ao ponto de suscitar o interesse na sua expansão a outras comunidades não europeias.

Sendo que a Associação Porto Digital tem ligações privilegiadas não só com a Câmara Municipal do Porto, mas também com a Universidade do Porto, tem um papel bastante importante na difusão desta rede universitária na cidade do Porto. Em todos os pontos de presença da APD é feita a difusão da rede “eduroam” alargando em muito a mobilidade dos estudantes e professores pela cidade do porto.

Aliando isto tudo, tornou-se descabido não usarmos os novos pontos de acesso *wireless* para expandir ainda mais a presença da rede “eduroam” na cidade. Desta feita, nos 15 bairros socias, alvos da nossa intervenção, para além da rede *wireless* da DomusSocial vão ter também acesso à rede *wireless* “eduroam”, podendo usufruir de todos os serviços e aplicações que esta rede lhes oferece como se tivessem no seu estabelecimento de ensino.

Esta rede tem as condicionantes de utilização definidas pelas entidades Europeias completamente alheias à APD. Querendo com isto referir que a sua utilização requer uma autenticação específica e restrições de utilização definidas previamente. A APD apenas a publicita nos seus AP’s. Ficando totalmente desresponsabilizada com os seus termos de acesso e utilização.

Esta medida vem, uma vez mais valorizar o projeto dos *hotspots* nos bairros socias, tornando-o num projeto cada vez mais credível e proveitoso para a comunidade.

Quanto à rede *wireless* da DomusSocial, esta, tem um cariz comunitário e é livre e gratuita, não sendo necessário qualquer autenticação ou identificação. É uma rede de nova geração completamente aberta à comunidade (ver Figura 21).

8. Plataforma estatística

Depois de configurado o segundo WLC, iniciamos o processo de obtenção de estatísticas de utilização da rede. Para tal, utilizamos uma versão gratuita de um servidor *radius*, *freeradius*.

8.1. Servidor *radius*

O *radius* é um protocolo de AAA (*authentication, authorization, accounting*) que permite fazer o controlo de acessos e gestão da utilização de todos os equipamentos que se ligam a uma rede. Este servidor tem a capacidade de fazer a autenticação de todos os equipamentos que se ligam à rede, definir restrições de acessos a cada utilizador e ainda fazer a contabilização da utilização da rede para fins estatísticos.

Há vários servidores *radius* no mercado, mas neste caso foi escolhido o *Freeradius* (Paquet, 2009).

8.1.1. *Freeradius*

O *freeradius* é um servidor *radius* desenvolvido e distribuído com uma licença GPLv2 (*GNU General Public License, version 2*) pelo que pode ser usado gratuitamente. O *freeradius* é o servidor *radius* mais conhecido e implementado no mundo das redes. Tem a capacidade de suportar todos os protocolos de autenticação e tem a particularidade de ser rápido, modular e amplamente escalável, sendo compatível com a maioria dos dispositivos NAS.

8.2. Modelo de dados

Os APs Cisco espalhados por toda a Cidade do Porto permitem enviar o seu Accounting para um servidor *radius* e desta forma termos acesso a um vasto leque de informações acerca dos AP bem como dos utilizadores que se ligam diariamente a eles. Estas informações são todas compiladas e normalizadas numa tabela chamada *radacct* do servidor *freeradius*. Cada máquina que se liga a qualquer um dos AP's da rede *wireless* provoca uma nova entrada na tabela *radacct* permitindo, assim, ter um histórico de toda a utilização da rede.

Como forma de complementar toda esta informação e obter estatísticas fidedignas acerca da utilização da rede foram criadas algumas tabelas de apoio, tal como ilustra o Figura 23. A tabela *radacct* pertence ao servidor *freeradius*, sendo que todas as outras foram criadas de forma a retirar informações de dados existentes nesta.

Figura 23 - Diagrama da Base de Dados

8.3. Descrição das tabelas

As tabelas auxiliares criadas tem como funcionalidade tirar o melhor partido possível de todos os dados adquiridos pelo servidor *radius*, e vão ao encontro das necessidade apresentadas pela APD para melhor e mais eficazmente gerir todos os seus pontos de acesso *wireless*. Assim sendo, apresento uma descrição mais pormenorizada de cada uma destas tabelas da base de dados.

8.3.1. Tabela ap

A tabela "ap" tem como objetivo listar todos os AP's presentes na rede, não só os instalados neste projeto dos bairros sociais, mas também todos os outros AP's da APD já existentes dispersos pela cidade do Porto. Possui informações importantes à cerca dos AP's, informações estas explícitas na Tabela 1.

Tabela: ap	Descrição	Tipo
ap_ehter_mac	Mac address da placa ethernet do ap	varchar(15)
ap_radio_mac	Mac address da placa rádio do ap	varchar(15)
ap_nserie	Número de serie do ap	varchar(11)
ap_nome	Nome atribuído ao ap	varchar(15)
ap_modelo	Modelo do ap	varchar(18)

ap_descricao	Descrição do ap	varchar(50)
ap_hsid	Identificação do *hotspot* a que o ap pertence	varchar(2)
ap_localizacao	Localização geográfica do ap	varchar(41)
ap_ipaddr	Endereço de sistema do ap	varchar(12)
ap_gps	Coordenadas gps da localização do ap	varchar(0)

Tabela 1 - Descrição da tabela ap

8.3.2. Tabela hs

A tabela "hs" refere-se a *hotspots*. Os *hotspots* são os pontos de presença da rede *wireless* na cidade do porto. Os *hotspots* são espaços físicos que necessitam da presença de mais do que um AP para cobrir a área, ou seja um *hotspot* é um AP ou um conjunto de AP's que cobrem uma determinada área ou edifício. No entanto a sua análise é feita como um todo. Exemplo disso são os vários AP's existentes no Edifício do IPO do Porto, todos eles pertencem ao *hotspot* IPO e tem uma análise estatística como um todo (ver Tabela 1Tabela 2).

Tabela: hs	Descrição	Tipo
hs_id	Identificação do *hotspot*	varchar(2)
hs_nome	Nome atribuído ao *hotspot*	varchar(255)

Tabela 2 - Descrição da tabela hs

8.3.3. Tabela nas

A tabela "nas" refere-se ao controlador que gere o AP. Como forma de separar os AP's já existentes na rede da APD e os novos AP's instalados nos bairros existem dois controladores WLC. O WLC gere os AP's já existentes e o WLC2 gere os novos AP's. para efeitos de consultas esta é uma forma de dividir as estatísticas entre os AP's dos bairros e os AP's já espalhados pela cidade. Para além desta função possui também algumas informações acerca destes controladores (ver Tabela 3).

Tabela: nas	Descrição	Tipo
nas_id	Identificação no servidor NAS	varchar(15)
nas_ip	Endereço IP do servidor NAS	varchar(15)

nas_nome	Nome do servidor NAS	varchar(255)
nas_soft	Versão do software existente no servidor Nas	varchar(255)
nas_servicip	Endereço de sistemas do servidor NAS	varchar(50)
nas_description	Descrição do servidor NAS	varchar(50)

Tabela 3 - Descrição da tabela nas

8.3.4. Tabela wlcwlan

A tabela "wlcwlan" refere-se à *wlan*. Como já referido anteriormente, cada AP possui várias *wlan*'s, neste caso temos a "eduroam", a "*Wi-Fi*_Portodigital" e agora o "DomusSocial". Para efeitos de gestão é interessante perceber de onde é gerado o tráfego e qual a *wlan* mais usada em determinados locais da cidade. Esta tabela tem também a particularidade de fazer a interligação com a tabela de interface (ver Tabela 4).

Tabela: wlcwlan	Descrição	Tipo
nas_ip	Endereço IP do servidor NAS	varchar(15)
***wlan*_id**	Identificação da *wlan*	varchar(50)
***wlan*_nome**	Nome da *wlan*	Varchar(255)
***wlan*_interfaceid**	Identificação da interface correspondente à *wlan*	int

Tabela 4 - Descrição da tabela wlcwlan

8.3.5. Tabela interface

A tabela "interface" tem como objetivo apresentar todas as interfaces existentes nos controladores WLC, bem como descrever as suas características mais importantes, como se pode constatar na Tabela 5.

Tabela: interface	Descrição	Tipo
int_id	Identificação da interface	int
int_nome	Nome atribuído à interface	varchar(255)
int_vlanid	Identificação da VLANScorrespondente à interface	varchar(255)
int_ipadd	Endereço IP da interface	varchar(255)
int_type	Tipo de interface	varchar(255)

Tabela 5 - Descrição da tabela interface

8.3.6. Tabela *radacct*

A tabela "*radacct"* é o centro de toda a base de dados criada. É construída pelo servidor *radius* e é simplesmente completada com as tabelas anexas criadas para traduzir algumas das informações que se revelaram interessantes para a gestão e controlo de rede. Esta tabela, para além de informações acerca do utilizador e do AP usado, tem também informações acerca da ligação estabelecida, tais como data, hora e tráfego gerado quer de *download* quer de upload. Todas estas informações existentes foram analisadas e discutidas de forma a serem trabalhadas segundo o interesse da APD. De notar que nem todos os campos foram esmiuçados pelo facto de, neste momento, não apresentam aparentemente mais-valias, situação esta, que se pode alterar com a utilização ou inclusive mudanças do paradigma de análise estatísticos. Dito isto, podemos dizer que esta tabela tem ainda mais potencialidade do que as já apresentadas (ver Tabela 6).

Tabela: radacct	Descrição	Tipo
radacctid	Identificação	int
acctsessionid	Identificação da seção iniciada	varchar
acctuniqueid		varchar
username	Nome de utilizador (*email*)	varchar
groupname		varchar
realm		varchar
nasipaddress	Endereço ip do servidor NAS	varchar
nasportid	Identificação do porto NAS	varchar
nasporttype	Tipo de porto do NAS	varchar
acctstarttime	Data e hora de inicio da ligação	datetime
acctstoptime	Data e hora o fim da ligação	datetime
acctsessiontime	Duração da ligação (segundos)	int
acctauthentic	Tipo de autenticação	varchar
connectinfo_start	*wlan* que iniciou a ligação	varchar
connectinfo_stop	*wlan* que finalizou a ligação	varchar

acctinputoctets	Quantidade de Upload (bits)	int
acctoutputoctets	Quantidade de Download (bits)	int
calledstationid	Endereço Mac do AP de ligação	varchar
callingstationid	Endereço Mac da máquina do utilizador	varchar
acctterminatecause	Motivo de finalização da secção	varchar
servicetype		varchar
framedprotocol		varchar
framedipaddress		varchar
acctstartdelay		int
acctstopdelay		int
xascendsessionsvrkey		varchar

Tabela 6 - Descrição da tabela radacct

9. Análise de dados

9.1. SQL

SQL (*Structured Query Language*) é a linguagem padrão de pesquisa declarativa para bases de dados relacionais. Tem a particularidade de ser simples, de fácil uso, permitindo fazer pesquisas inteligentes nas bases de dados apresentando rapidamente os resultados solicitados pelo utilizador. Tem a capacidade de inserir, eliminar, alterar e consultar dados. Neste caso em particular a consulta de dados é a função mais utilizada.

Esta ferramenta é essencial na análise dos dados existentes no servidor *radius* permitindo fazer inúmeras consultas sobre as mais variadas informações.

Como forma de tirar partido de todas estas funcionalidades do SQL foi necessário reunir consensos acerca das estatísticas mais importantes a retirar da extensa lista de dados gerada pelo *accouting* dos AP's. Para cada uma destas necessidades básicas de consulta foi construída uma *querie* de consulta. Através destas *queries* é possível obter instantaneamente os resultados pretendidos. A linguagem usada nas *queries* é apenas de carácter de consulta de dados de forma a responder as pesquisas previamente selecionadas como essenciais.

9.2. Consultas à BD

As consultas à base de dados foram divididas em 3 tipo de pesquisa. São elas; estado da rede, utilização do equipamento e dados do utilizador. Essencialmente, a primeira apresenta informações acerca do número de utilizadores existentes, a segunda corresponde à utilização dos nossos equipamentos de rede e a terceira, informações concretas acerca dos nossos utilizadores.

9.2.1. Estado da rede

É necessário ter uma perceção do número de utilizadores ligados a nossa rede *wireless* num determinado momento, bem como ter uma ideia do tráfego que está a ser gerado por essa utilização. Deste modo, foram elaboradas as seguintes consultas à base de dados.

9.2.1.1. *Online* agora

É sempre interessante saber o número de utilizadores da nossa rede ligados no momento da nossa consulta, por isso, foi criada uma pesquisa de forma a obter informações do estado real da rede neste momento. Ou seja, no momento da pesquisa ter a possibilidade de saber o número de utilizadores *online* bem como ter a perceção dos débitos praticados nesse momento (upload/download).

Para tal, foi desenvolvida a *querie* ilustrada na Figura 24, sendo que o objetivo desta consulta é apresentar por cada *hotspot* existente, o número de utilizadores e os débitos efetuados no dia 21 (dia da consulta) e que ainda estão com a secção ativa logo tem o "*radacct*.acctstoptime" nulo. Esta pesquisa inclui os *hotspots* ligados ao controlador 1 ou ao controlador 2.

```
1 SELECT hotspot.hs_nome,
2    count(distinct(callingstationid)) as contagem_dif_utilizadores,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5 FROM radacct
6 left join ap on radacct.calledstationid = ap.ap_radio_mac
7 left join hotspot on ap.ap_hsid = hotspot.hs_id
8 WHERE radacct.acctstarttime > '2014-09-21'
9       and radacct.acctstoptime is null
10      and (radacct.nasipaddress = '10.10.20.1' or radacct.nasipaddress = '10.10.10.1')
11 GROUP BY hotspot.hs_nome
```

hotspot (4×17)

hs_nome	contagem_dif_user	upload_GB	download_GB
Aliados	49	0.0019	0.0235
BairrosSociais	19	0.0150	0.2297
BMAG	8	0.0002	0.0001
Bonjoia	7	0.0020	0.0009
BPMP	13	0.0713	0.3407
Casa da musica	12	0.0020	0.0175
FCP - Dragao	8	0.0000	0.0001
FCP- Vitalis	2	0.0008	0.0092
Feira Park	4	0.0000	0.0000
IAPMEI	1	0.0000	0.0000
IPO	144	0.0453	0.2822
Monte Aventino	6	0.0053	0.0500
Outros	35	0.0017	0.0089
Reitoria	39	0.0058	0.0320
Serralves	2	0.0000	0.0000

Figura 24 – Querie por hotspot

No entanto, visto que existem locaias com vários AP's e pode ser interessente conhecer ao pormenor a utilização de um AP específico, foi desenvolvida uma pesquisa idêntica mas que apresenta os resultados por *Access Point*, como demostrado na Figura 25.

```
1 SELECT ap.ap_descricao,
2    count(distinct(callingstationid)) as contagem_dif_user,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5 FROM radacct
6 left join ap on radacct.calledstationid = ap.ap_radio_mac
7 WHERE radacct.acctstarttime > '2014-09-21'
8       and radacct.acctstoptime is null
9       and (radacct.nasipaddress = '10.10.20.1' or radacct.nasipaddress = '10.10.10.1')
10 GROUP BY ap.ap_descricao
```

ap (4×57)

ap_descricao	contagem_dif_user	upload_GB	download_GB
APD-Ponte Nova	7	0.0001	0.0000
BMAG	1	0.0000	0.0000
BMAG Regie	3	0.0000	0.0000
Bonfim	2	0.0000	0.0000
bonjoia-rap2	5	0.0016	0.0002
bonjoia-rap3	8	0.0005	0.0003
Bonjoia-SalaFormacao	5	0.0043	0.0104
bpmp-catalogo	4	0.0211	0.0638
bpmp-claustros	2	0.0000	0.0001
bpmp-livre acesso	2	0.0106	0.1397
bpmp-reservados	1	0.0000	0.0000
Camara do Porto	27	0.0003	0.0006
Carvalhido-BlocoM-EntradaDIREITA	3	0.0000	0.0000
Casa da Musica	17	0.0008	0.0038
Casa do Infante	6	0.0470	0.0054

Figura 25 - Querie online por AP

9.2.1.2. Intervalo de tempo

Com o objetivo de perceber a utilização da rede *wireless* num determinado intervalo de tempo, a *querie* da Figura 26 indica os dados de utilização da rede no último mês de Setembro. No entanto, esta pesquisa pode ser feita durante um espaço de tempo a determinar pelo gestor de rede. De realçar que os AP's instalados nos bairros sociais estão todos agrupados no mesmo *hotspot* "BairrosSociais".

```
1 SELECT hotspot.hs_nome,
2    count(distinct(callingstationid)) as contagem_dif_utilizadores,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5 FROM radacct
6 left join ap on radacct.calledstationid = ap.ap_radio_mac
7 left join hotspot on ap.ap_hsid = hotspot.hs_id
8 WHERE radacct.acctstarttime BETWEEN '2014-09-1' AND '2014-09-30'
9       and (radacct.nasipaddress = '10.10.20.1' or radacct.nasipaddress = '10.10.10.1')
10
11 GROUP BY hotspot.hs_nome
```

hotspot (4×17)

hs_nome	contagem_dif_utilizadores	upload_GB	download_GB
Aliados	29708	159.6126	719.7962
BairrosSociais	4852	76.6079	772.9735
BMAG	2286	648.6126	3678.2964
Bonjoia	126	75.2246	883.6744
BPMP	2598	340.4349	1974.6463
Casa da musica	8399	50.0075	197.2120
FCP - Dragao	8718	44.3807	411.6782
FCP- Vitalis	609	20.3600	214.3415
Feira Park	30	33.6526	92.3054
IAPMEI	32	2.0285	42.5532
IPO	6090	675.1606	3799.5957
Monte Aventino	3465	13.5475	144.0456
Outros	17151	189.6040	643.2671
Reitoria	25229	526.9349	2544.1807
Serralves	2247	306.8175	1288.8991

Figura 26 - Querie online no mês de Setembro

9.2.2. Utilização dos equipamentos

Destas consultas à base de dados, pretende-se adquirir conhecimento sobre a utilização dos nossos equipamentos de rede, saber essencialmente qual o wlc que é mais utilizado e, ainda, perceber qual a *wlan* mais frequentada. Desta forma, foram elaboradas as seguintes *queries* de pesquisa.

9.2.2.1. WLC

Como forma de saber qual o controlador de rede mais usado, foi construída uma *querie* para obter informações acerca da utilização da rede tendo em conta o controlador usado. Assim, podemos ter uma estimativa de utilização dos AP's dos bairros sociais em comparação com os AP's do resto da cidade do Porto. A Figura 27 mostra os dados acerca da utilização do WLC2 ou seja dos AP's dos bairros sociais. De realçar que o AP com o nome "PonteNova" foi o *access point* usado para realizar a prova de conceito e encontra-se localizado na Rua da Ponte Nova nas instalações da APD. Esta rua é muito frequentada, quer pelos portuenses quer por turistas, daí se justificar a disparidade de utilização em comparação com os AP's dos bairros socias. Estes valores apenas são medidos a partir de dia 15 de setembro de 2014 visto ser o primeiro dia de funcionamento correto de todos os AP's.

```
1 SELECT ap.ap_localizacao,
2    count(distinct(callingstationid)) as contagem_dif_users,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5
6 FROM radacct
7 left join ap on radacct.calledstationid = ap.ap_radio_mac
8
9 WHERE radacct.acctstarttime > '2014-09-15'
10       and radacct.nasipaddress = '10.10.20.1'
11 GROUP BY ap.ap_localizacao
12
```

ap (4×16)

ap_localizacao	contagem_dif_users	upload_GB	download_GB
Aldoar	11	1.0086	6.5577
Campinas	13	0.8617	15.9597
Carrical	11	0.4385	6.4571
Carvalhido	33	8.5355	163.4272
FMagalhaes	9	0.2072	3.7683
FMoura	9	3.6872	30.1926
Francos	31	8.8857	117.8377
Lagarteiro	61	9.0986	107.0740
Lordelo	18	0.9715	17.4198
Outeiro	37	2.9353	38.3814
PAntunes	16	0.0114	0.1030
pioXII	5	0.0808	0.4601
Ponte Nova	2070	11.9413	44.4833
Ptorres	21	4.6379	48.5676
Regado	20	0.1794	0.7500

Figura 27 - Querie WLC2

Com o objetivo de obter um paralelismo com a utilização e o tráfego gerado pelos restantes AP's da APD foi realizada uma consulta semelhante à anterior mas desta vez pedindo à base de dados apenas informações acerca da utilização do WLC, ou seja, todos os AP's dos APD exceto os presentes nos bairros sociais, Figura 28.

```
1 SELECT ap.ap_localizacao,
2    count(distinct(callingstationid)) as contagem_dif_users,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5
6 FROM radacct
7 left join ap on radacct.calledstationid = ap.ap_radio_mac
8
9 WHERE radacct.acctstarttime > '2014-09-15'
10       and radacct.nasipaddress = '10.10.10.1'
11 GROUP BY ap.ap_localizacao
12
```

ap (4×80)

ap_localizacao	contagem_dif_users	upload_GB	download_GB
BMAG - Unicer	503	82.9466	620.0202
BMAG-Sala de Leitura	990	201.9540	1127.9944
Bonjoia	93	10.1028	94.2326
Bonjoia-SalaFormacao	50	33.4068	161.6598
bpmp-catalogo	282	26.4543	264.7205
bpmp-claustros	223	6.8535	96.7753
bpmp-leitura geral	233	26.6187	117.3412
bpmp-livre acesso	897	163.0477	482.8640
bpmp-reservados	525	2.5566	29.2102
Casa da Musica - Cobertura	590	0.7183	0.5697
Casa da Musica - map2	1345	0.5880	4.0393
Casa da Musica - map3	3171	5.4392	76.4319
Casa da Musica - map4	308	2.5845	12.7165

Figura 28 - Querie WLC

Para a obtenção de uma comparação geral entre os dois controladores existentes na rede *wireless*, foi feita a consulta à base de dados ilustrada na Figura 29.

```
1  SELECT nas.nas_nome,
2     count(distinct(callingstationid)) as contagem_dif_utilizadores,
3     SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4     SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5     FROM radacct
6  left join nas on radacct.nasipaddress = nas.nas_ip
7
8  WHERE radacct.acctstarttime > '2014-09-15'
9
10 GROUP BY nas.nas_nome
```

nas (4×6)

nas_nome	contagem_dif_utilizadores	upload_GB	download_GB
WLC2_Porto_Digital	1131	21.6824	290.8251
WLC_Porto_Digital	21945	539.1612	3081.2687

Figura 29 - Querie de comparação WLC

9.2.2.2. *WLAN*

Todos os AP's distribuídos possuem várias wlans que podem ser utilizadas e que podem traduzir informações acerca dos interesses de cada utilizador. Desta forma, foi feito um levantamento acerca dos dados de utilização tendo em conta a *wlan* que é usada, assim obtemos o número de utilizadores ligados a cada *wlan* bem como os débitos realizados. A consulta foi realizada tendo em consideração os dados recolhidos a partir de dia 15 de setembro, primeiro dia em que todos os AP's se encontravam operacionais. De notar que com esta consulta podemos não só ter conhecimento qual a *wlan* usada, mas também, a que wlc esta pertence (Figura 30).

```
1 select wlcwlan.wlan_nome, nas.nas_description,
2    count(distinct(callingstationid)) as contagem_dif_utilizadores,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5 from radacct
6 left join wlcwlan on radacct.connectinfo_start = wlcwlan.wlan_id and radacct.nasipaddress = wlcwlan.nas_ip
7 left join nas on radacct.nasipaddress = nas.nas_ip
8
9 WHERE radacct.acctstarttime > '2014-09-15'
10 group by wlcwlan.nas_ip, wlcwlan.wlan_id, wlcwlan.wlan_nome
11
```

Result #1 (5×9)

wlan_nome	nas_description	contagem_dif_utilizadores	upload_GB	download_GB
WiFi Porto Digital	WLC 1	18344	543.1648	3139.6742
eduroam	WLC 1	4762	5.8258	30.7471
Opo_Lab	WLC 1	22	24.8224	114.7642
UFCHP	WLC 1	14	4.8168	4.0343
WiFi Porto Digital	WLC 2	717	1.9880	3.2980
DomusSocial	WLC 2	239	19.9364	290.9613
portolivinglab	WLC 2	2	0.0181	0.2844
eduroam	WLC 2	213	0.0799	0.2603

Figura 30 - Querie wlan e wlc

9.2.2.3. *Hotspot*

Sendo a localização geográfica dos AP's bastante dispersa pela cidade do Porto torna-se interessante saber qual das zonas da cidade tem mais utilizadores. Assim, esta *querie* permite ter uma noção dos locais principalmente usados para os clientes terem acesso à nossa rede *wireless*. Recordo que um *hotspot* pode estar equipado com mais do que um *access point*. Esta consulta foi feita consoante os valores recolhidos a partir de dia 15 de Setembro (Figura 31).

```
1 SELECT hotspot.hs_nome,
2    count(distinct(callingstationid)) as contagem_dif_users,
3    SUM(radacct.acctinputoctets)/1073741824 as upload_GB,
4    SUM(radacct.acctoutputoctets)/1073741824 as download_GB
5
6 FROM radacct
7 left join ap on radacct.calledstationid = ap.ap_radio_mac
8 left join hotspot on ap.ap_hsid = hotspot.hs_id
9
10 WHERE radacct.acctstarttime > '2014-09-15'
11       and (radacct.nasipaddress = '10.10.10.1' or radacct.nasipaddress = '10.10.20.1')
12 GROUP BY hotspot.hs_nome
```

hotspot (4×17)

hs_nome	contagem_dif_users	upload_GB	download_GB
Aliados	16147	87.9781	404.1334
BairrosSociais	2515	64.3869	763.9075
BMAG	1338	332.4713	1961.9124
Bonjoia	117	43.6260	259.4956
BPMP	1575	229.7054	999.6743
Casa da musica	4624	13.8995	116.6269
FCP - Dragao	6711	27.3272	251.3932
FCP- Vitalis	331	9.5985	97.5331
Feira Park	27	72.4935	96.5805
IAPMEI	34	1.2050	18.8585
IPO	4534	454.4369	2247.7768
Monte Aventino	2427	14.7975	199.6816
Outros	8844	122.3322	412.2814
Reitoria	12817	288.0740	1605.4208
Serralves	1166	129.4708	436.2912

Figura 31 –Querie por Hotspot

9.2.3. Dados de utilizador

Como forma de traçar rotas geográficas e fluxos de utilização achamos importante a obtenção de um histórico de uso de um determinado cliente. Como tal, esta pesquisa permite saber por onde determinado cliente se movimenta, o tempo de utilização da nossa rede e os débitos efetuados bem como a *wlan* utilizada em cada ligação. Desta forma, tornou-se possível tirar algumas conclusões acerca dos nossos clientes e da sua interação com a nossa rede *wireless*, permitindo traçar perfis de utilização baseados em dados reais de utilização.

9.2.3.1. Pesquisa por *email*

Esta pesquisa histórica pode ser feita através de um endereço *email* com que o cliente se autentica na rede, mostrado todos ligações à rede que este cliente efetuou bem como algumas informações acerca dessa ligação, exemplo disso é a Figura 32.

```
1 select radacct.calledstationid as AP_MAC,
2       ap.ap_localizacao,
3       radacct.callingstationid as User_MAC,
4       radacct.username,
5       radacct.acctinputoctets as upload,
6       radacct.acctoutputoctets as download,
7       radacct.acctstarttime as hora_inicio,
8       radacct.acctstoptime as hora_fim
9 from radacct
10 left join ap on radacct.calledstationid = ap.ap_radio_mac
11       where radacct.username =   'a024789@edu.ismai.pt'
12          order by radacct.acctstarttime
```

Result #1 (8×7)

AP_MAC	ap_localizacao	User_MAC	username	upload	download	hora_inicio	hora_fim
00-0b-85-98-97-40	Dragao - MonteAventino	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	10849	14800	2014-07-01 21:05:00	2014-07-01 21:11:06
00-0b-85-95-bb-00	Monte Aventino - Velasquez	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	26745	34529	2014-08-04 17:43:41	2014-08-04 17:53:43
00-0b-85-95-bf-20	Dragao - Nascente - Sul	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	70707	471582	2014-08-30 18:07:24	2014-08-30 18:09:30
00-0b-85-95-bf-20	Dragao - Nascente - Sul	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	120222	329829	2014-08-30 18:21:03	2014-08-30 18:29:59
00-0b-85-98-e6-f0	Dragao - Poente - Sul	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	25685	24600	2014-08-30 18:34:52	2014-08-30 18:43:09
00-0b-85-98-e6-f0	Dragao - Poente - Sul	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	40714	47866	2014-08-30 18:49:30	2014-08-30 18:59:11
00-0b-85-95-bb-b0	Dragao - Alameda	3c-e0-72-8d-33-cb	a024789@edu.ismai.pt	17312	81871	2014-09-13 16:43:05	2014-09-13 16:49:46

Figura 32 - Querie pesquisa por email

9.2.3.2. Pesquisa por mac

Esta pesquisa histórica pode ser feita através de um endereço MAC da máquina usada pelo cliente, mostrado todas ligações à rede que este equipamento efetuou bem como algumas informações acerca dessa ligação, temos como exemplo a Figura 33.

```
1 select radacct.calledstationid as AP_MAC,
2       ap.ap_localizacao,
3       radacct.callingstationid as User_MAC,
4       radacct.username,
5       radacct.acctinputoctets as upload,
6       radacct.acctoutputoctets download,
7       radacct.acctstarttime as hora_inicio,
8       radacct.acctstoptime as hora_fim
9 from radacct
10 left join ap on radacct.calledstationid = ap.ap_radio_mac
11    where radacct.callingstationid = 'a4-9a-58-0a-15-0f'
12    order by radacct.acctstarttime
```

Result #1 (8×8)

AP_MAC	ap_localizacao	User_MAC	username	upload	download	hora_inicio	hora_fim
00-0b-85-98-97-90	Rotunda Anemona	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	383323	945830	2014-09-05 21:29:42	2014-09-05 21:49:34
00-0b-85-98-97-00	Pr D. Joao I - Semaforo	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	19440	18791	2014-09-07 02:37:05	2014-09-07 02:43:29
00-0b-85-98-97-00	Pr D. Joao I - Semaforo	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	86200	227485	2014-09-07 04:49:50	2014-09-07 04:58:47
00-0b-85-98-97-90	Rotunda Anemona	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	151185	211386	2014-09-08 21:31:26	2014-09-08 21:47:24
00-0f-8f-22-54-10	IPO - sala tratamentos Nefrologia	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	30584	33643	2014-09-09 16:19:19	2014-09-09 16:26:37
00-0b-85-98-97-90	Rotunda Anemona	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	213214	368140	2014-09-12 21:39:31	2014-09-12 21:49:34
00-0b-85-95-bd-d0	CMP-Pacos	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	31892	56627	2014-09-13 16:46:59	2014-09-13 16:57:16
00-0b-85-98-97-60	CMP - Aliados	a4-9a-58-0a-15-0f	mimed11264@med.up.pt	11638	50877	2014-09-13 20:33:41	2014-09-13 20:43:30

Figura 33 - Querie pesquisa por MAC

10. Conclusão e trabalho futuro

Este capítulo final pretende exibir algumas conclusões que subjazem ao projeto realizado até então. Almeja, ainda, refletir a opinião pessoal acerca de todo o processo de trabalho e do estágio em si. Apresentar-se-ão, para além disso, propostas de trabalho futuro a desenvolver a partir do trabalho realizado até ao momento. Estas propostas visam o melhoramento do projeto inicial, capacitando-o para abranger cada vez mais zonas de interesse.

10.1. Conclusão

Após a realização do projeto de expansão da rede *wireless* nos bairros sociais da cidade do Porto, posso concluir que tal projeto serviu, não só para equipar os bairros sociais com rede gratuita, mas também para potencializar o investimento feito, a priori, pela APD aquando do projeto de transmissão de TV. Pudemos, assim, dar utilidade aos XONs de monitorização presentes nos bairros acimas referidos, aproveitando-os para alimentar os *access point*s com sinal de Internet.

O mesmo projeto oferece aos moradores destas zonas, habitualmente associadas a carência social, a oportunidade de usufruir de um serviço de Internet gratuito e de qualidade. Isto permite-lhes um acesso à informação e ao conhecimento, capaz de incentivar ao estudo e formação profissional, potencializando uma maior igualdade de oportunidades.

Aliado a estes fatores, surge a oportunidade de aumentar o raio de ação da rede metropolitana da APD na cidade do Porto, proporcionando um maior reconhecimento do trabalho realizado por esta associação. Tornando-a numa empresa de referência e prestígio na área das TI na cidade.

10.2. Trabalho Futuro

Enumeram-se de seguida as propostas de trabalho futuro a realizar bem como outras vertentes de utilização dos resultados obtidos com a realização do projeto - plataforma estatística.

Primeiramente, deveria ser aumentada a área de cobertura do ponto de acesso de cada bairro, usando APs de exterior com maior potência de sinal, bem como aumentar o número de APs por bairro, possibilitando o acesso em toda a área.

Testemunhado o sucesso deste projeto, faria, a meu ver, todo o sentido expandi-lo à totalidade dos bairros sociais da cidade e não somente aos selecionados, bem como a algumas áreas de interesse na cidade do Porto.

Em relação a trabalhos mais técnicos, seria pertinente desenvolver um mecanismo de autenticação de modo a precaver abusos da utilização, quer a nível de tempo de acesso, quer a conteúdos acedidos. Seguidamente, reconheço a necessidade do desenvolvimento de uma plataforma de pesquisas interativas e de fácil utilização para que não sejam necessários grandes conhecimentos técnicos para aceder aos dados estatísticos. Para tal, torna-se indispensável melhorar o desempenho da máquina onde está instalado o servidor *radius*.

No que concerne à usabilidade dos resultados do projeto para outros fins, seria interessante a criação de relatórios estatísticos de utilização para futura análise e tratamento. Estes relatórios tornar-se-iam numa poderosa arma de marketing e controlo populacional, isto, porque seria possível identificar os fluxos de movimentação dos utilizadores. Outra vantagem seria a criação de perfis de pessoas numa determinada área.

11. Bibliografia

11.1. Referências

Alcatel-Lucent. (2008). *Alcatel-Lucent Scalable IP Networks Guide.* Alcatel-Lucent.

Barbosa, A. C. (2009). *Projecto de um Hotspot, com uso controlado, para uma rede de empresa.* Faculdade de Engenharia da Universidade do Porto. Obtido em 2013/14, de http://repositorio-aberto.up.pt/handle/10216/60225

Briere, D., R. Bruce III, W., & Hurley, P. (2003). *Wireless Home Networking For Dummies.* New York: Wiley Publishing, Inc. Obtido em 2013/14

Cisco Systems. (2013). *Cisco Wireless LAN Controller Configuration Guide, Release 7.4.* San Jose: Cisco Systems, Inc.

Cisco Systems, I. (2007). *Cisco Wireless LAN Controller Configuration Guide.* California: Cisco Systems, Inc. Obtido em 2013/2014

Coutinho, G. (2006). *Estudo para uma Rede Metropolitana Comunitária.* Dissertação, Faculdade de Engenharia da Universidade do Porto, Departamento de Engenharia Electrotécnica e de Computadores, Porto. Obtido em Jan de 2014, de http://repositorio-aberto.up.pt/bitstream/10216/12013/2/Texto%20integral.pdf

Dictionary of Networking. (2000). USA: SYBEX Inc.

Digital, P. (2005). *Porto Digital - O projecto*. Obtido em Dezembro de 2013, de Porto Digital.pt: http://www.portodigital.pt/

Gast, M. (2002). *802.11® Wireless Networks: The Definitive Guide.* O'Reilly.

Lewis , B., & T. Davis, P. (2004). *Wireless Networks For Dummies®.* Indiana: Wiley Publishing, Inc.

Lowe, D. (2005). *Networking For Dummies* (7th ed.). New Jersey: Wiley Publishing, Inc.

Paquet, C. (2009). *Implementing Cisco IOS Network Security.* USA: Cisco Systems, Inc.

Vilela, R., & Ribeiro, D. (2007). *SEGURANGA EM REDES WIRELESS.* Brasil: Universidade Federal de Mato Grosso.

11.2. Outra bibliografia

Poelker, C. & Nikitin, A. (2009). Storage Area Networks For Dummies®. Indiana: Wiley Publishing, Inc.

Ivens, K. (2007). Home Networking For Dummies®. Indiana: Wiley Publishing, Inc.

Beaver, K. & T. Davis, P. (2005). Hacking *Wireless* Networks For Dummies®. Indiana: Wiley Publishing, Inc.

Grayson, M., Shatzkamer, K. & Wainner, S. (2009). IP Design for Mobile Networks. Indianapolis: Cisco Systems, Inc.

Boger, P. (2010). CCNA Exploration Course Booklet Routing Protocols and Concepts. Indianapolis: Cisco Systems, Inc.

Wheat, J., Hiser, R., Tucker, J., Neely, A. & McCullough, A. (2001). Designing a *Wireless* Network. USA: Syngress Publishing, Inc.

Mukherjee, A., Bandyopadhyay, S. & Saha, D. (2003). Location Management and Routing in Mobile *Wireless* Networks. USA: Artech House.

Yacoub, M. (2002). *Wireless* Technology: Protocols, Standards, and Techniques. USA: CRC Press LLC.

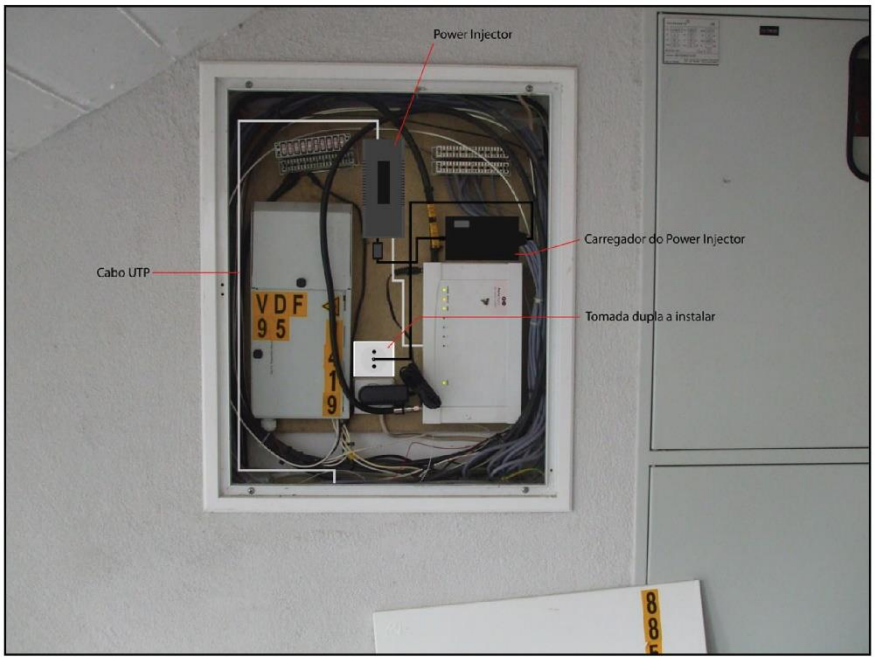
http://speedmeter.fccn.pt

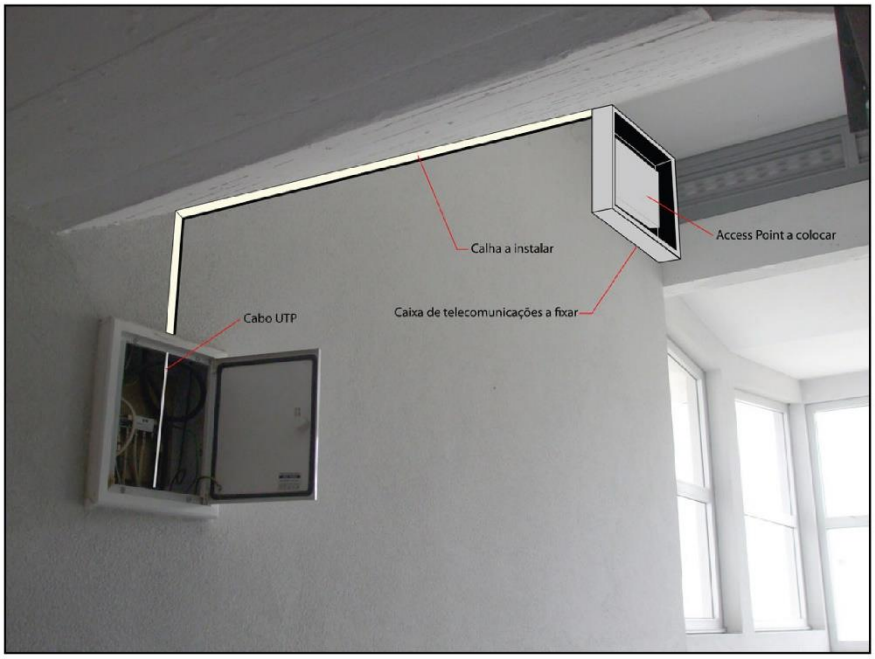
https://www.google.com/earth

12. Anexo

1 Bairro de Aldoar
bloco 10 entrada 120

Projetado $\frac{1}{2}$





PortoDigital

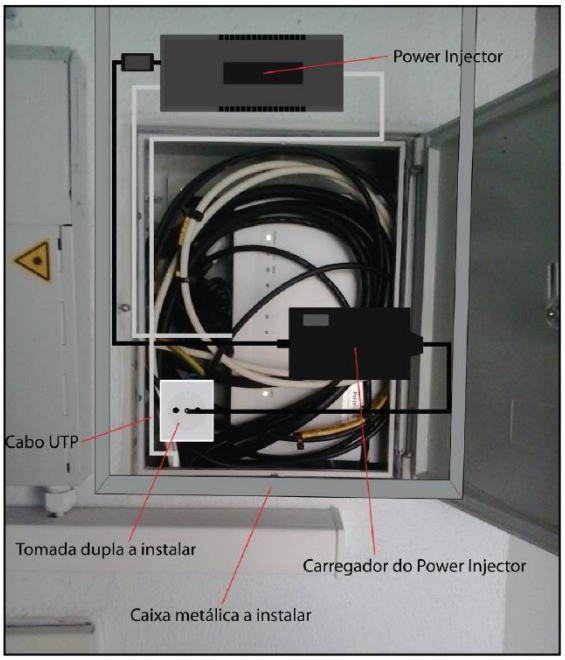
1 Bairro de Aldoar
bloco 10 entrada 120

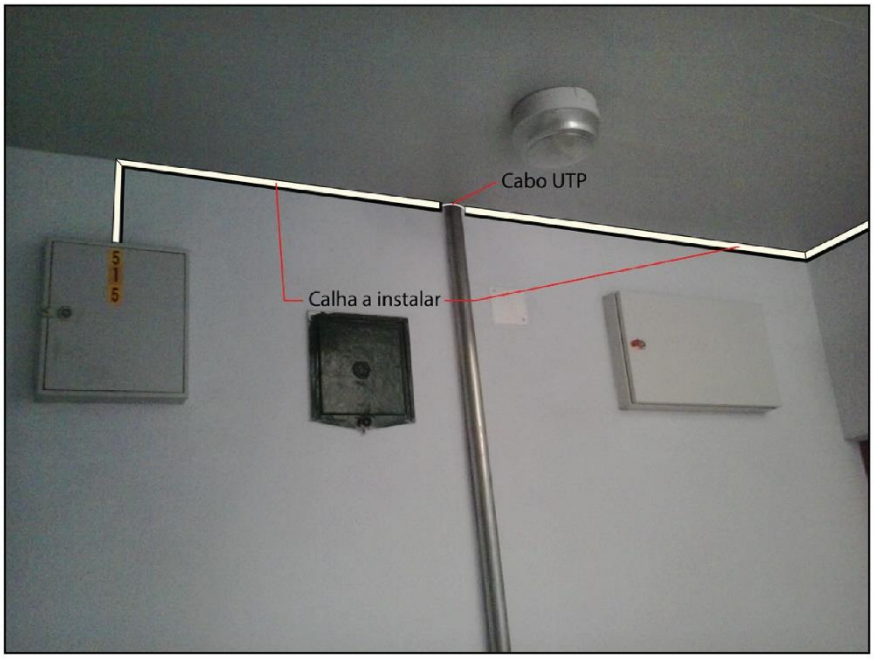
Finalizado $\frac{2}{2}$

PortoDigital

❷ Bairro de Fonte da Moura
bloco 27 entrada 613

Projetado $\frac{1}{4}$

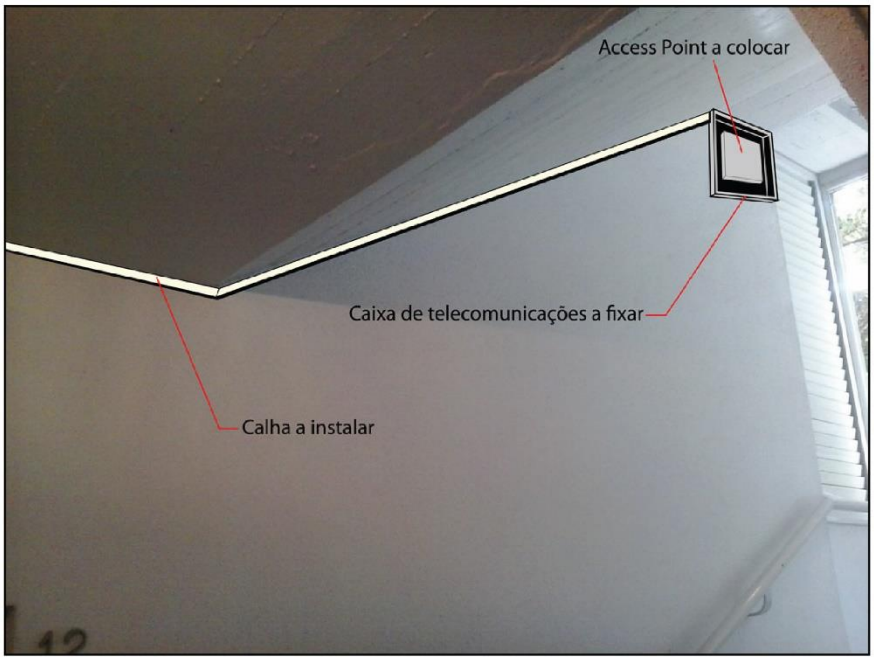




PortoDigital

❷ Bairro de Fonte da Moura
bloco 27 entrada 613

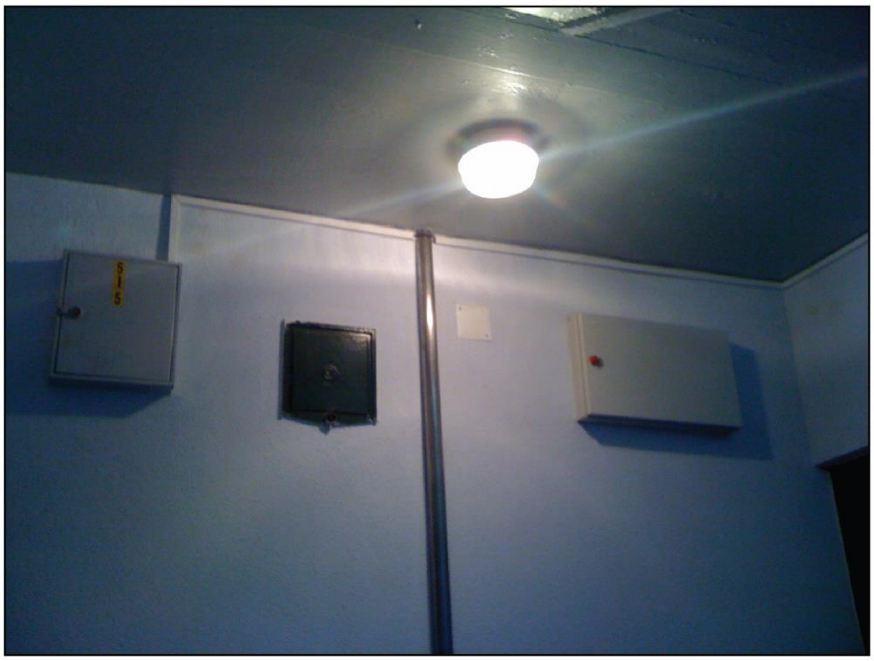
Projetado $\frac{2}{4}$



PortoDigital

2 Bairro de Fonte da Moura
bloco 27 entrada 613

Finalizado $\frac{3}{4}$



PortoDigital

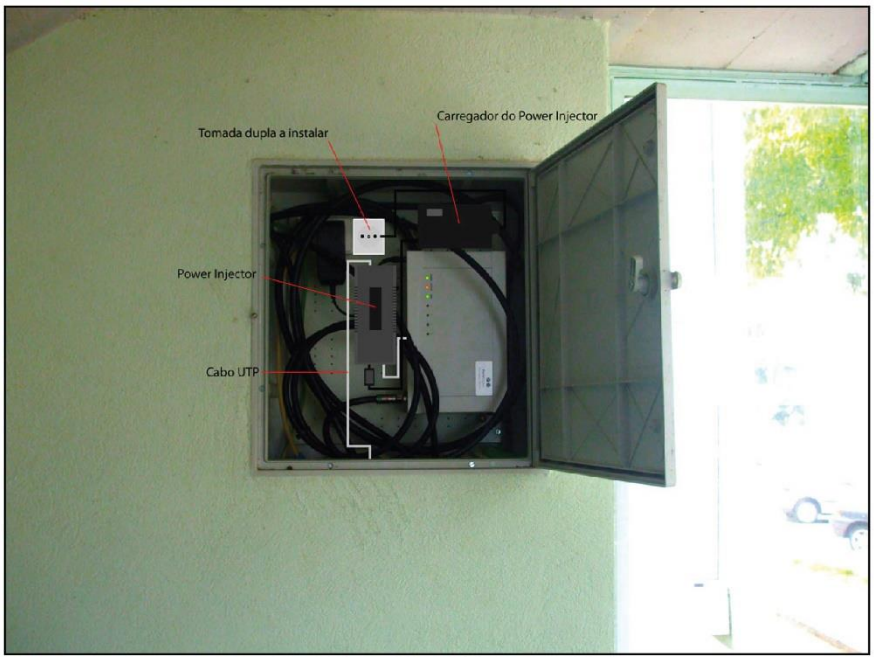
2 Bairro de Fonte da Moura
bloco 27 entrada 613

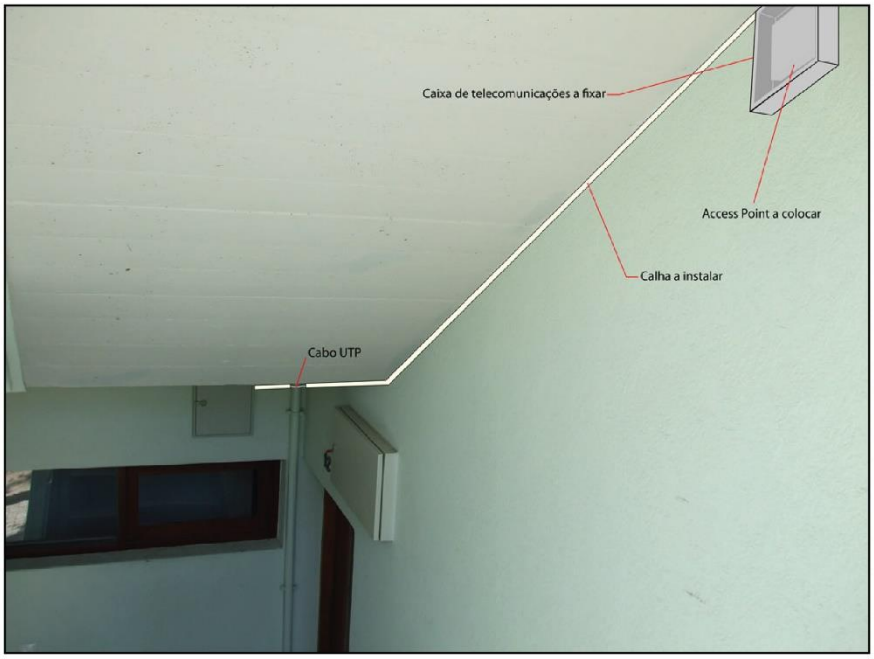
Finalizado $\frac{4}{4}$

PortoDigital

❸ Bairro de Campinas
bloco 8 entrada 163

Projetado $\frac{1}{3}$





PortoDigital

3 Bairro de Campinas
bloco 8 entrada 163

Finalizado $\frac{2}{3}$

PortoDigital

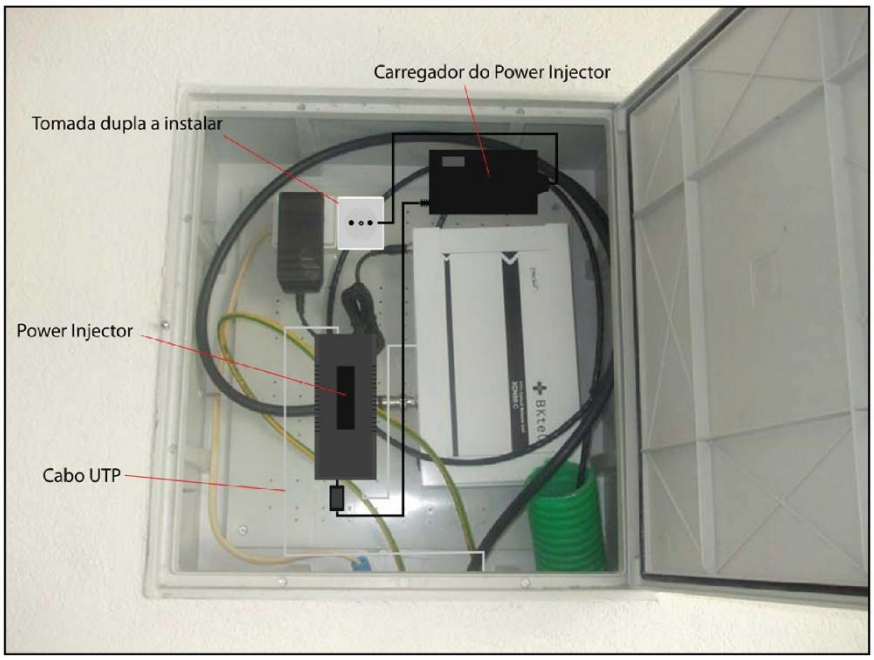
3 Bairro de Campinas
bloco 8 entrada 163

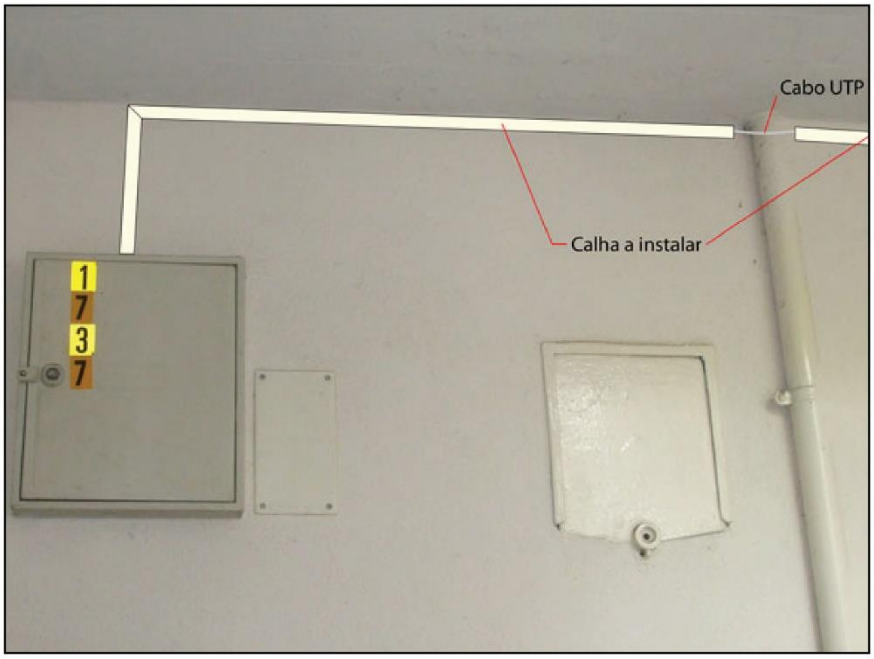
Finalizado $\frac{3}{3}$

PortoDigital

4 Bairro de Dr. Pinheiro Torres
bloco 8 entrada 399

Projetado $\frac{1}{4}$

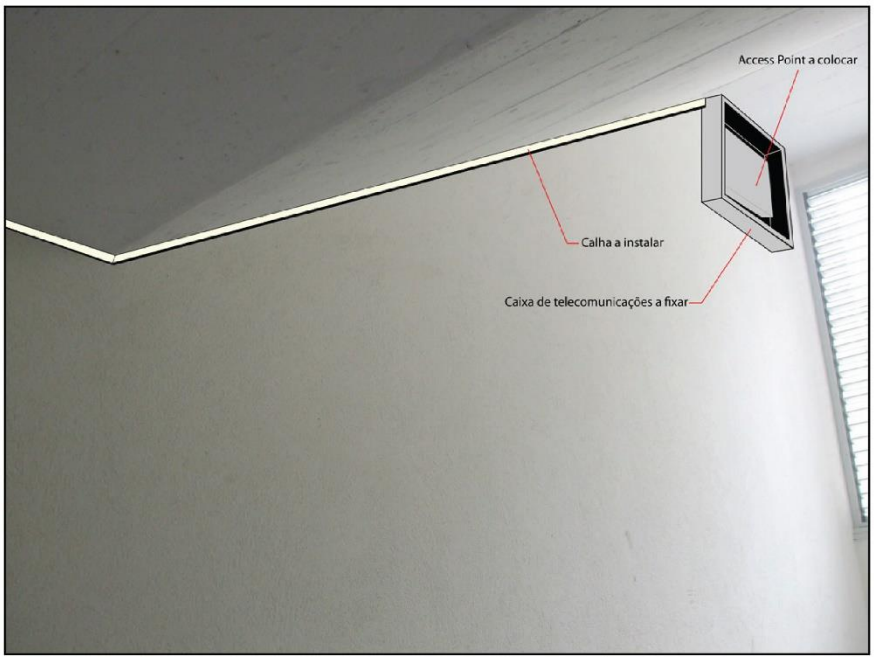




PortoDigital

4 Bairro de Dr. Pinheiro Torres
bloco 8 entrada 399

Projetado $\frac{2}{4}$



PortoDigital

4 Bairro de Dr. Pinheiro Torres
bloco 8 entrada 399

Finalizado $\frac{3}{4}$

PortoDigital

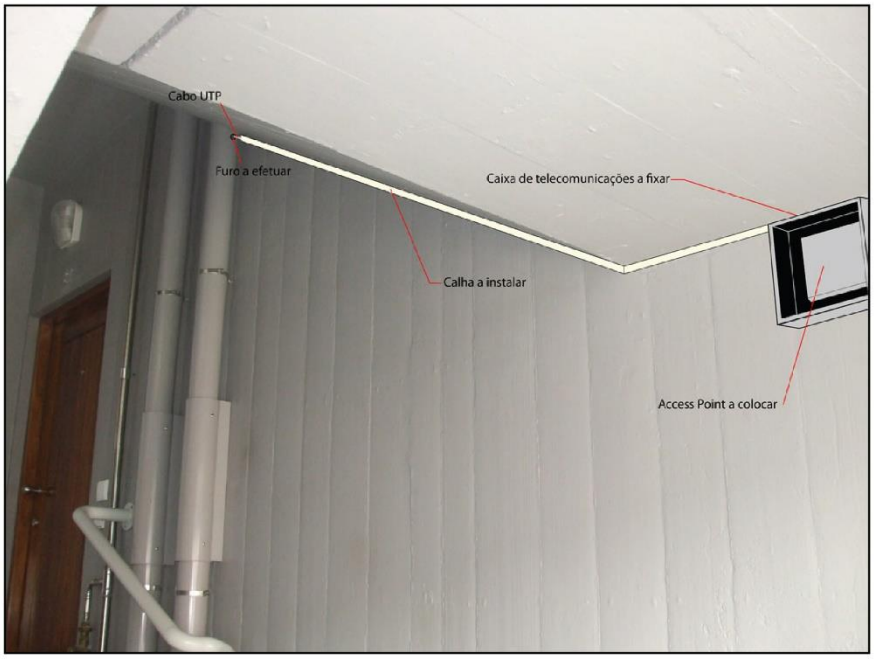
4 Bairro de Dr. Pinheiro Torres
bloco 8 entrada 399

Finalizado $\frac{4}{4}$

PortoDigital

5 Bairro de Lordelo do Ouro
bloco 13 entrada 2

Projetado $\frac{1}{2}$



PortoDigital

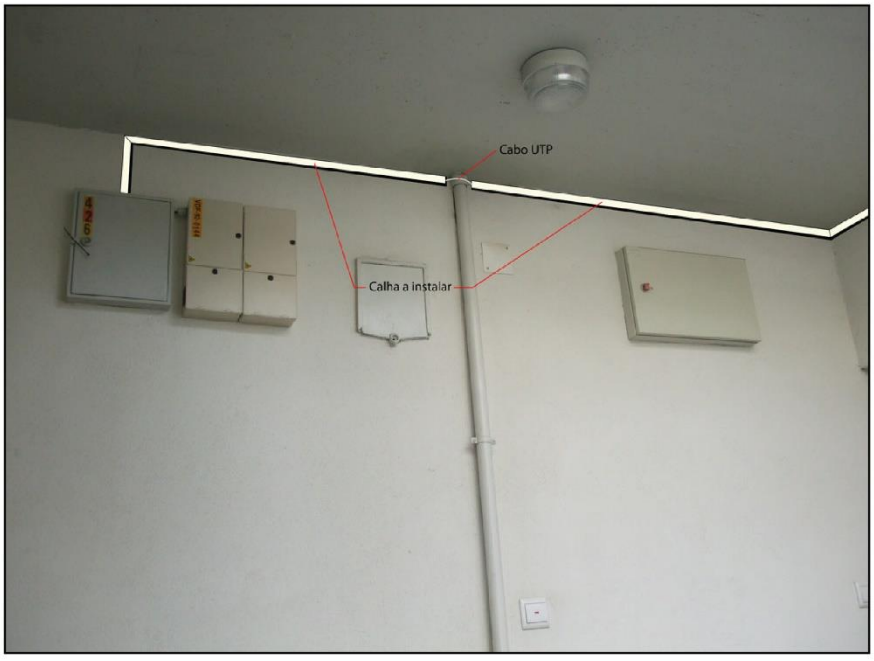
5 Bairro de Lordelo do Ouro
bloco 13 entrada 2

Finalizado $\frac{2}{2}$

PortoDigital

6 Bairro de Francos
bloco 12 entrada 189

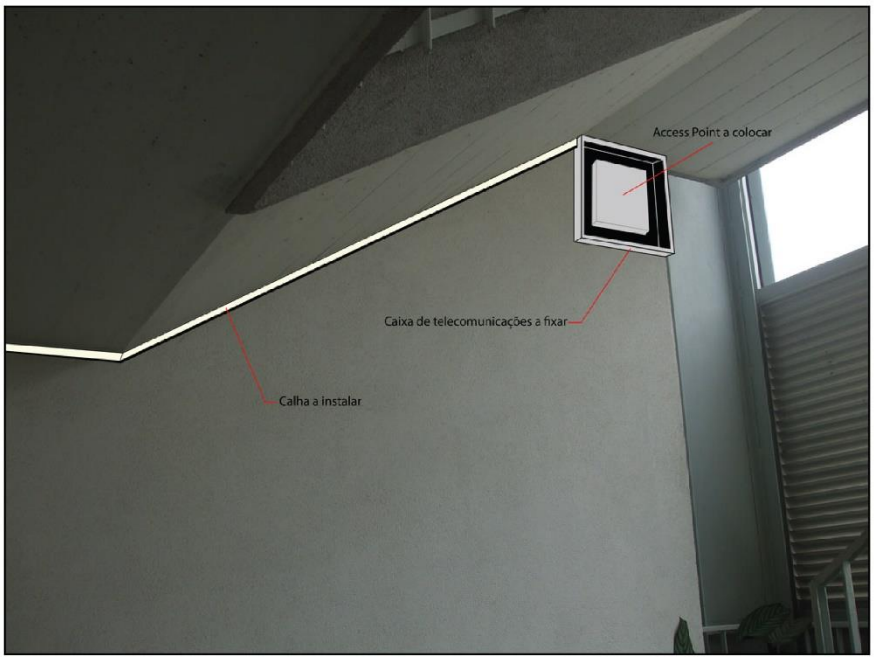
Projetado $\frac{1}{4}$



PortoDigital

6 Bairro de Francos
bloco 12 entrada 189

Projetado **2/4**



PortoDigital

6 Bairro de Francos
bloco 12 entrada 189

Finalizado $\frac{3}{4}$

PortoDigital

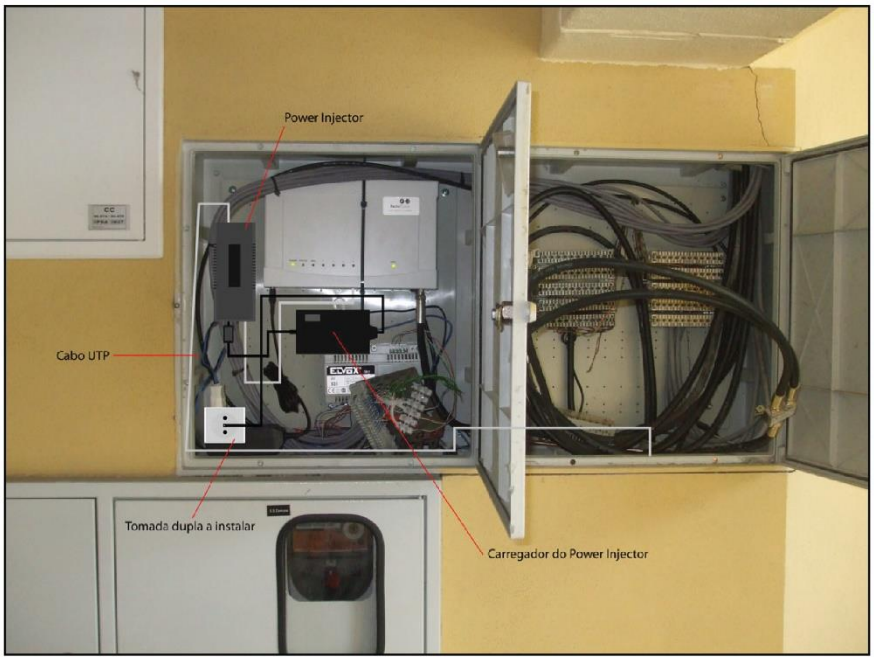
6 Bairro de Francos
bloco 12 entrada 189

Finalizado $\frac{4}{4}$

PortoDigital

7 Bairro do Carvalhido
bloco M entrada Direita

Projetado $\frac{1}{2}$



PortoDigital

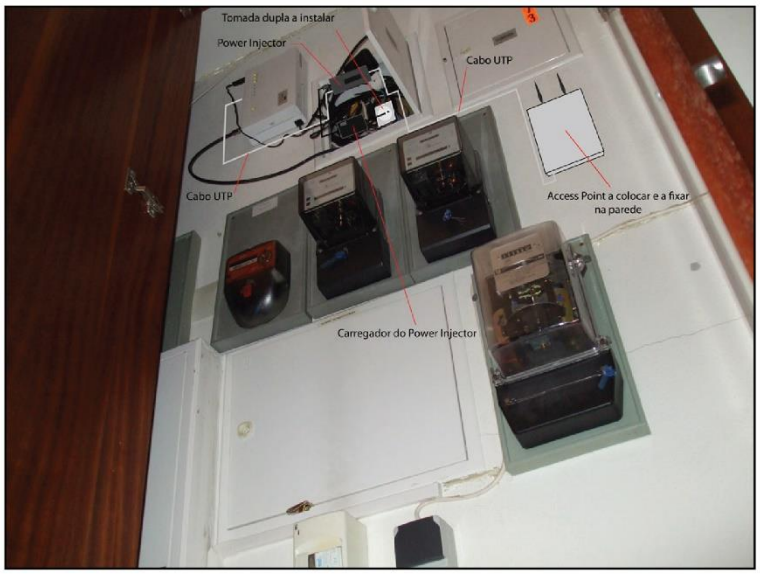
7 Bairro do Carvalhido
bloco M entrada Direita

Finalizado $\frac{2}{2}$

PortoDigital

8 Conjunto Habitacional Parceria Antunes
bloco 4 entrada 7

Projetado $\frac{1}{1}$

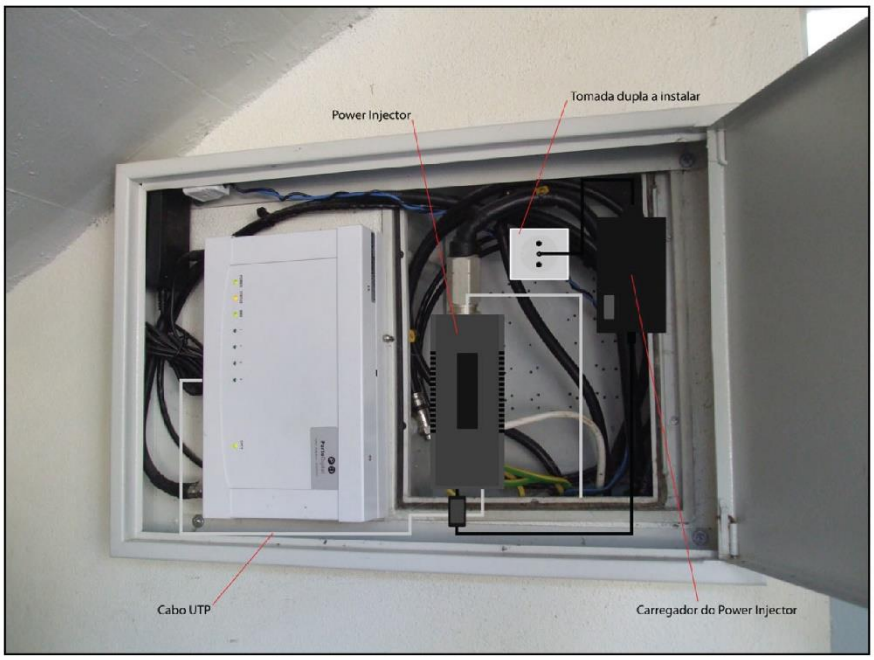


Finalizado

PortoDigital

9 Bairro do Regado
bloco 22 entrada 58

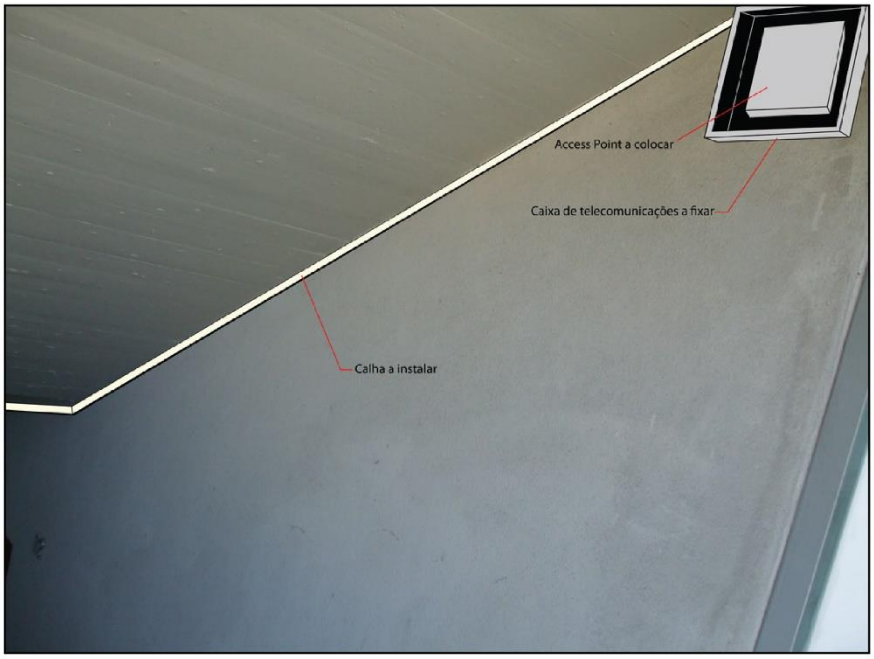
Projetado $\frac{1}{4}$



PortoDigital

9 Bairro do Regado
bloco 22 entrada 58

Projetado $\frac{2}{4}$



PortoDigital

9 Bairro do Regado
bloco 22 entrada 58

Finalizado $\frac{3}{4}$

PortoDigital

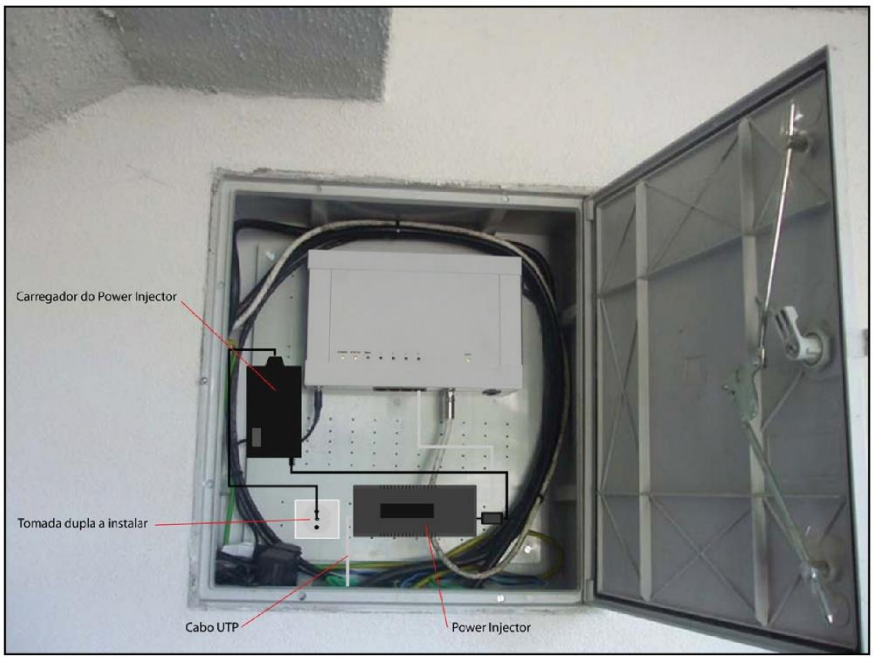
9 Bairro do Regado
bloco 22 entrada 58

Finalizado **4/4**

PortoDigital

10 Bairro do Carriçal
bloco 11 entrada 106

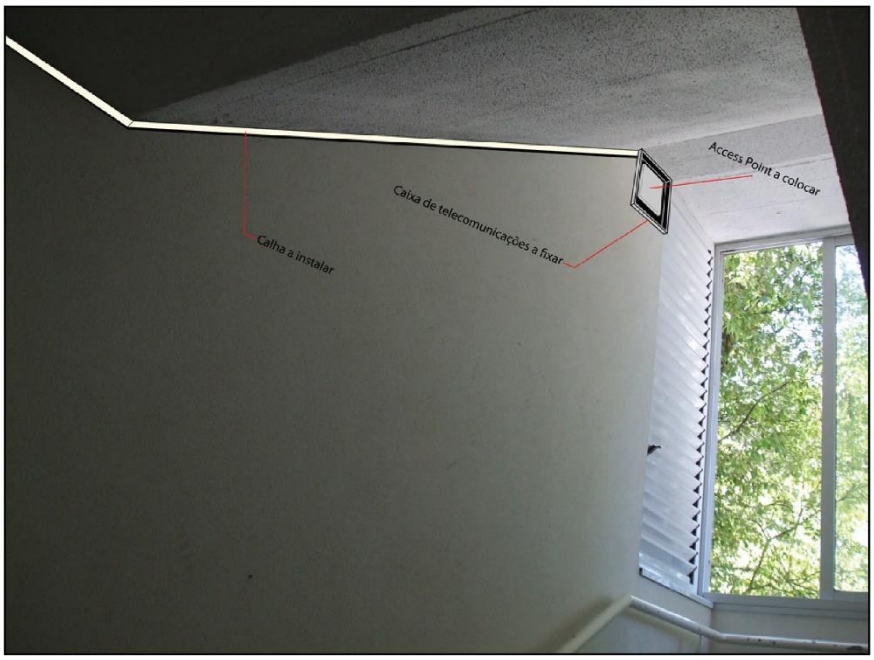
Projetado $\frac{1}{4}$



PortoDigital

10 Bairro do Carriçal
bloco 11 entrada 106

Projetado $\frac{2}{4}$



PortoDigital

10 Bairro do Carriçal
bloco 11 entrada 106

Finalizado $\frac{3}{4}$

PortoDigital

10 Bairro do Carriçal
bloco 11 entrada 106

Finalizado $\frac{4}{4}$

PortoDigital

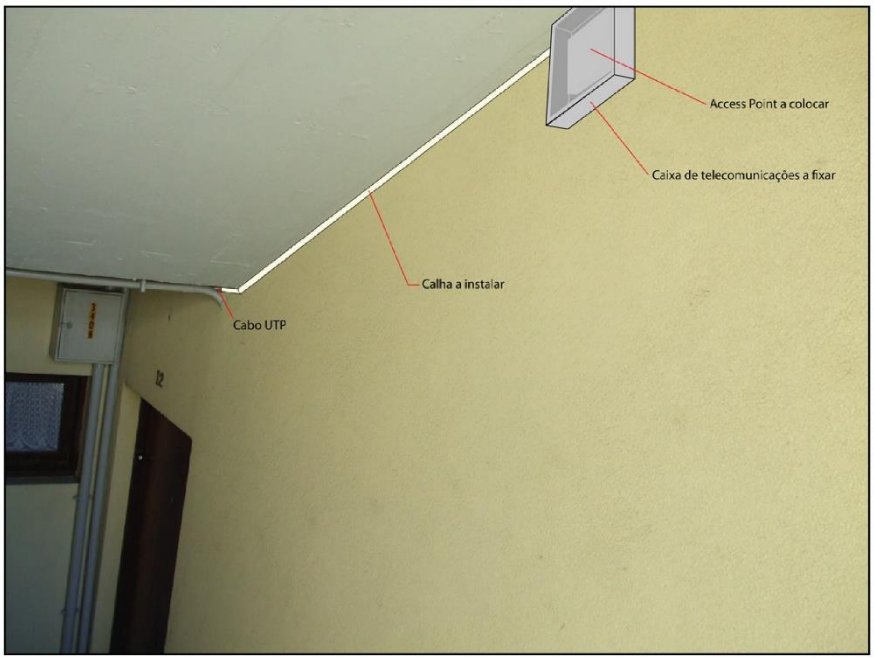
11 Bairro do Outeiro
bloco M entrada 41

Projetado $\frac{1}{4}$

PortoDigital

11 Bairro do Outeiro
bloco M entrada 41

Projetado $\frac{2}{4}$



PortoDigital

11 Bairro do Outeiro
bloco M entrada 41

Finalizado $\frac{3}{4}$

PortoDigital

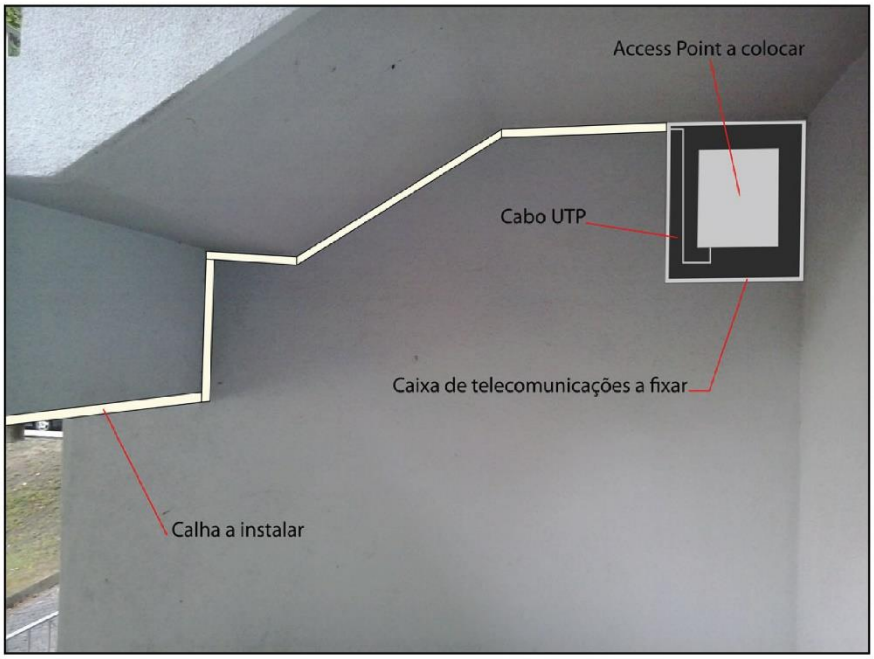
11 Bairro do Outeiro
bloco M entrada 41

Finalizado $\frac{4}{4}$

PortoDigital

⓬ Bairro de Fernão de Magalhães
bloco 13 entrada 105

Projetado $\frac{1}{3}$



PortoDigital

⓬ Bairro de Fernão de Magalhães
bloco 13 entrada 105

Finalizado $\frac{2}{3}$

PortoDigital

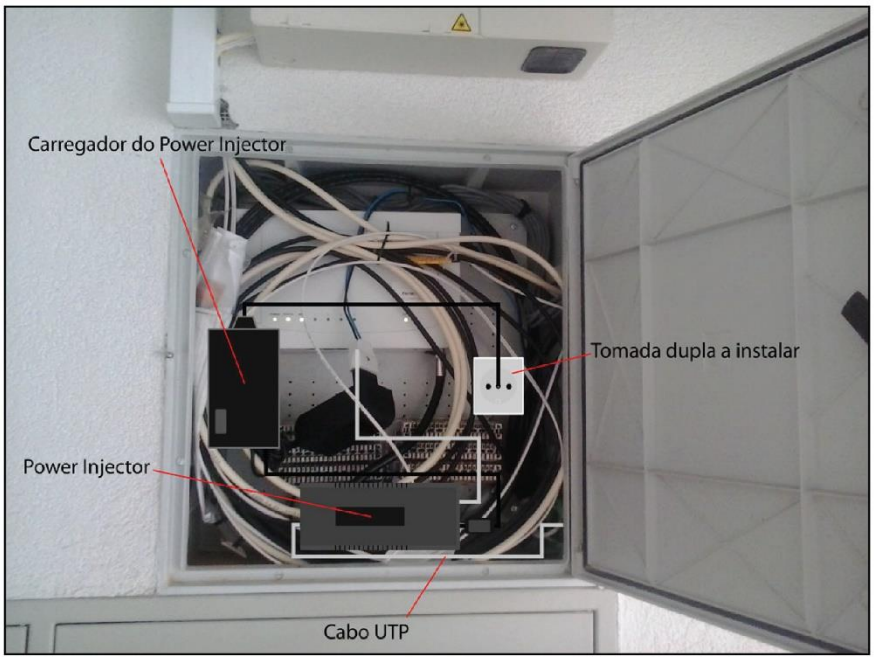
⓬ **Bairro de Fernão de Magalhães**
bloco 13 entrada 105

Finalizado $\frac{3}{3}$

PortoDigital

13 Bairro do Pio XII
bloco E entrada Direita

Projetado $\frac{1}{2}$



PortoDigital

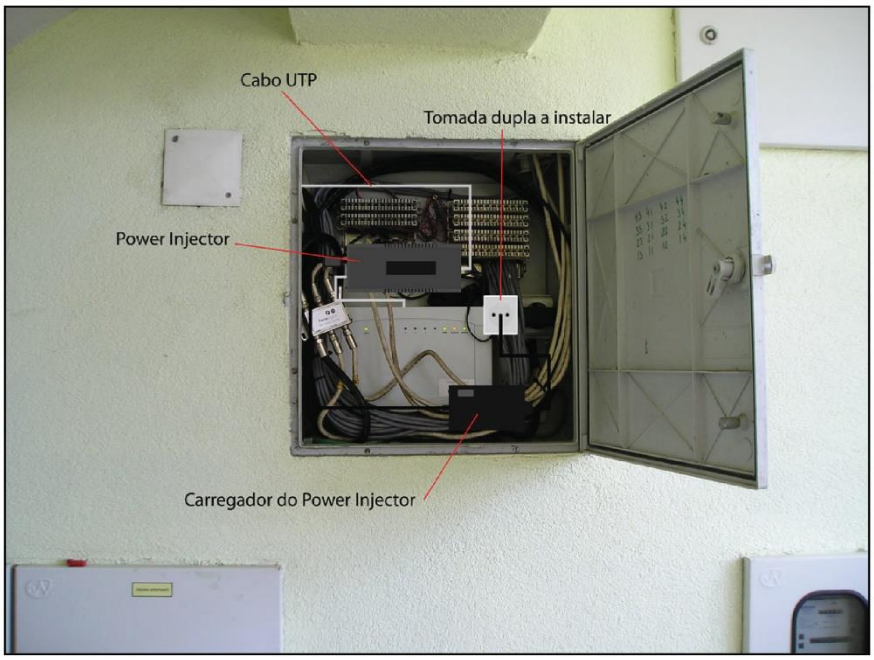
13 Bairro do Pio XII
bloco E entrada Direita

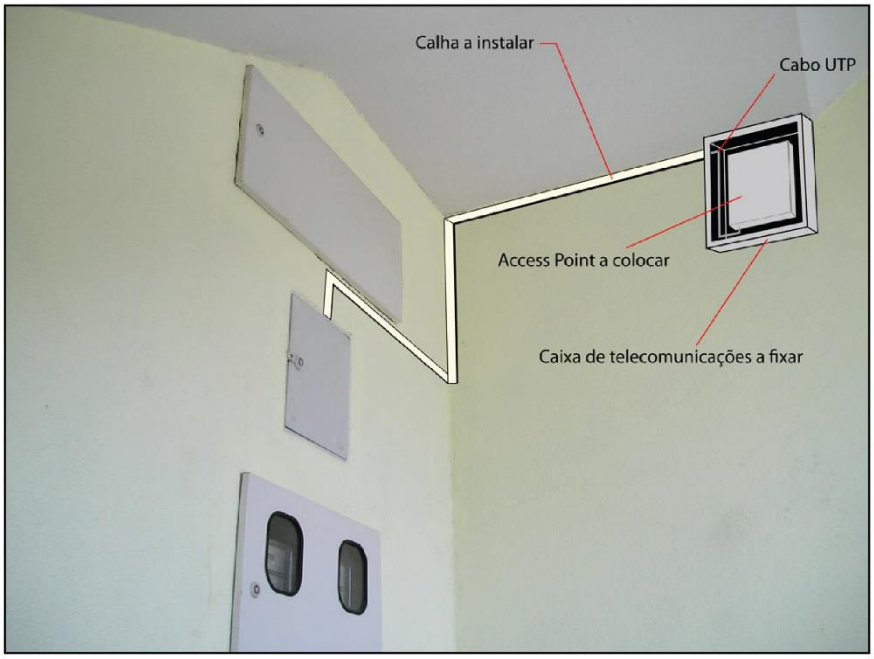
Finalizado $\frac{2}{2}$

PortoDigital

⓮ Bairro de S.Roque da Lameira
bloco 20 entrada 181

Projetado $\frac{1}{2}$





PortoDigital

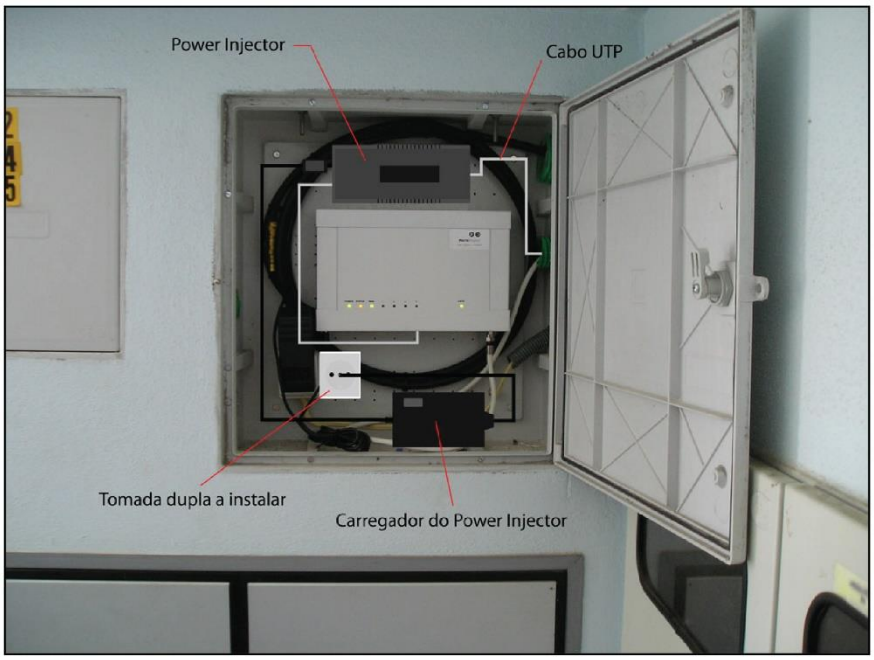
⓮ Bairro de S.Roque da Lameira
bloco 20 entrada 181

Finalizado $\frac{2}{2}$

PortoDigital

⓯ Bairro do Lagarteiro
bloco 6 entrada 73

Projetado $\frac{1}{2}$



PortoDigital

15 Bairro do Lagarteiro
bloco 6 entrada 73

Finalizado $\frac{2}{2}$

PortoDigital