Millora d'una xarxa inalàmbrica passant de bridging a routing

Juan Francisco Cano Ruiz

Resum– Crear una xarxa per una empresa que es dedica a oferir connexió a Internet tant a particulars com empreses no és una tasca fàcil, doncs s'han de tenir en compte molts paràmetres i coneixement suficient de molts conceptes i protocols relacionats amb les xarxes i s'han d'aplicar i configurar de la manera correcta. El disseny d'una xarxa d'aquest estil ha de tenir en compte moltes més casuístiques que una xarxa normal, la disponibilitat i escalabilitat són fundamentals, ja que ha de ser capaç de minimitzar les caigudes, a poder ser de forma automàtica (ja sigui amb un avís a temps o amb una ruta alternativa), i de crèixer sense que això presenti un problema (com per exemple que el manteniment es faci inviable o el tràfic de control de la mateixa xarxa provoqui problemes). En aquest projecte es tracta una xarxa que presenta els problemes descrits i com a objectiu es planteja solucionar aquests problemes amb el mínim impacte possible sobre els clients existents, doncs els problemes que es puguin haver acumulat no són culpa d'ells.

Paraules clau– bridging, enrutament, xarxa inalàmbrica, lan virtual, OSPF, redundància, broadcast, PPPoE, monitorització.

Abstract– Creating a network for a company that its business consists in providing Internet connection to individuals and companies is not an easy task, many parameters must be taken into account and knowledge of many network-related concepts and protocols are needed, they must be applied and configured in the right way. The design of a network of this style must take into account many more casuistic than a normal network, the availability and scalability are fundamental, since it must be able to minimize the falls in an automatic way (maybe with a warning just in the right time or habilitating an alternative route for the traffic), and to grow without this being a problem (such as the maintenance becomes unfeasible or the traffic control of the same network causes problems). This project addresses a network that presents the problems described and aims to solve these problems with the least possible impact on existing customers, because the problems that may have accumulated are not their fault.

Keywords– bridging, routing, wireless network, virtual lan, OSPF, redundancy, broadcast, PPPoE, monitorization.

1 Introducció

ACTUALMENT la connexió a Internet és més que una necessitat en la nostra societat, tant en l'àmbit personal com en el professional i com a servei que s'ha de pagar, tota persona o empresa que disposa d'una connexió a Internet espera que funcioni de manera adequada i que si falla sigui per una causa justificada i hagi una ràpida resposta per part del proveïdor. Meswifi SL és una empresa que entra en aquest àmbit i actua com a proveïdor de serveis d'Internet per radiofreqüència, també conegut com a *Wireless Internet Service Provider (WISP)*, això significa que pot arribar a zones on altres proveïdors no arriben, però també significa que hi ha altres elements a tenir en compte a l'hora de mantenir la xarxa de la que disposa, com poden ser els agents atmosfèrics o inclús la natura (d'un mes a l'altre les fulles d'un arbre poden fer que empitjori la senyal d'un enllaç inalàmbric), per això necessita tenir especial cura en l'estat de la xarxa.

Aquest projecte li servirà a la empresa per millorar la seva xarxa, que en un principi es va idear sense previsió pel fu-

• E-mail de contacte: joancano@kingstudio.es
• Mención realitzada: Tecnologies de la Informació
• Treball tutoritzat per: Joan Serra-Sagristà (Departament d'Enginyeria de la Informació i de les Comunicacions)
• Curs 2016/17

tur i no s'esperava un creixement tant gran durant els últims mesos. Això, a part de descuidar altres aspectes, ha fet que el rendiment de la xarxa empitjori degut a que tots els paquets de *broadcast* (és a dir, aquells que arriben a tot un segment de xarxa) arribin a tots els punts de la xarxa, independentment del lloc on es trobin. Meswifi té nodes inalàmbric situats des de Vic fins Salou i tots estan connectats a la mateixa xarxa sense fils i fins a data d'avui ja superen els 700. Aquests estaven administrats de forma manual, sense poder veure en directe en quin estat es trobava cada node, cosa que feia que l'empresa no se n'adonés de la caiguda d'un node fins que un dels clients truqués enfadat o es decidís entrar de forma manual a l'administració d'un d'aquests nodes.

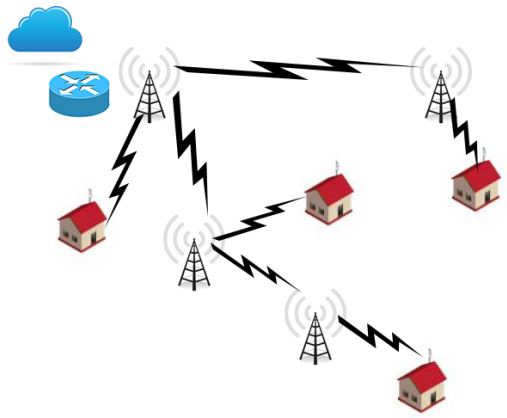

Fig. 1: Domini de broadcast, cada paquet de broadcast arriba a tots els punts de la xarxa

Així doncs, el projecte proposa, amb el mínim impacte possible, fer un canvi necessari a la xarxa que permeti la segmentació en subxarxes més petites (evitant així el problema de *broadcast*), el control de cada un dels més de 700 nodes en directe per anticipar-se als problemes que puguin sorgir en el futur i la millora tant en el rendiment com en la disponibilitat i escalabilitat de la xarxa.

Aquest document s'organitza en diferents apartats, sent aquest el de introducció, on s'explica la motivació del projecte que es realitza en l'empresa Meswifi SL, el segon apartat, que explica els objectius a aconseguir al final del projecte, el tercer, on podem llegir sobre l'estat de l'art de les diferents tecnologies que porten alguna relació amb aquest projecte, al quart apartat està explicada la metodologia feta servir, el cinquè apartat explica la planificació del projecte, amb el temps dedicat a cada part, al sisè el desenvolupament de les diferents etapes del projecte, separades en diferents subseccions, en el setè es poden llegir les conclusions obtingudes sobre els resultats i per últim i després de les conclusions els corresponents agraïments i la bibliografia.

2 Objectius

L'objectiu principal d'aquest projecte és aconseguir una millora de la xarxa de la empresa de tal forma que aquesta quedi totalment redundada, sense problemes de congestió de tràfic i permeti la seva gestió i el seu manteniment d'una forma eficient. Per poder assolir aquest objectiu, s'han proposat els següents subobjectius:

1. Analitzar què és el que es pot millorar de la xarxa i quines manances té, per tal de saber què és el que s'ha de fer per arribar a l'objectiu principal.

2. Implementació de tots els sistemes necessaris causant el mínim impacte sobre la xarxa actual, de manera que els clients no se n'adonin dels canvis realitzats i no tinguin cap tall al servei, o que aquest sigui mínim.

3. Observar una millora sobre l'estat actual de la xarxa en general, tant en estabilitat com en el seu manteniment i escalabilitat.

3 Estat de l'art

Avui en dia no existeix una única manera de dissenyar una xarxa que sigui escalable i redundant sobretot degut a la gran quantitat de protocols que es poden escollir i a les necessitats i capacitats de cada empresa.

Primer de tot parlarem dels protocols d'enrutament existents, que es divideixen en tres tipus[1]:

1. *Interior Gateway Protocol type 1 (IGP)*, Protocol de Passarel·la Interior de tipus 1: són els protocols que es basen en Enllaç-Estat, com *OSPF* o *IS-IS*.

2. *Interior Gateway Protocol type 2 (IGP)*, Protocol de Passarel·la Interior de tipus 2: són els protocols que es basen en Vector-Distància, com *RIP*, *RIPv2* o *IGRP*.

3. *External Gateway Protocols (EGP)*, Protocols de Passarel·la Exterior: són els protocols encarregats de l'intercanvi d'informació entre Sistemes Autònoms (*AS*), com *EGP* o *BGP*.

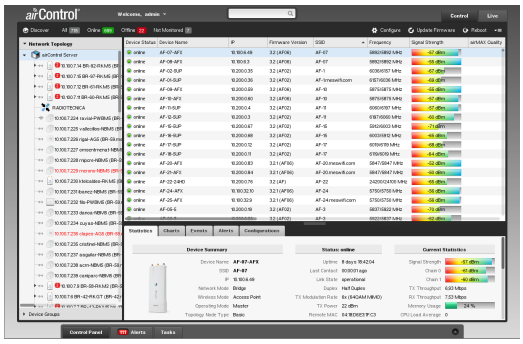

Fig. 2: AirControl 2

Per aquest projecte el tipus de protocol d'enrutament que es farà servir serà un *IGP* de tipus 1, ja que tractarà de millorar la part de la xarxa interna i no s'encarregarà de les comunicacions amb l'exterior com a objectiu principal, a part d'haver de tenir en compte l'estat dels enllaços per escollir la ruta que han de seguir els paquets, en concret *OSPF (Open Shortest Path First)*[2][3], que farà passar els paquets pel camí disponible més curt.

A més dels protocols d'enrutament, també hem de tenir en compte altres tecnologies de vanguàrdia per la realització d'aquest projecte.

Els proveïdors de serveis de connexió a Internet han de guardar els logs de quin usuari ha estat fent servir la connexió en qualsevol moment, així que per realitzar aquesta tasca és necessari un sistema que permeti això, però tornem

al mateix que al principi d'aquesta secció, no hi ha un sol sistema vàlid i s'ha d'escollir un segons les preferències del projecte. En trobem sistemes com *graylog2*, *ossec*, *LogAnalyzer*, etc. Encara que tots funcionen fent servir la base de l'estàndard *syslog*[4].

Aquesta secció acabarà parlant del sistemes de monitorització[5], però tornem a entrar a la mateixa premissa de que no hi ha un únic sistema vàlid. Existeixen sistemes com *Smokeping*, *Nagios*, *PRTG*, *Splunk*, etc. Però en el cas de la empresa, s'utilitzarà el sistema propietari de la marca dels equips (*Ubiquiti*), *airControl2*, aquest permet controlar tota la informació dels equips i consultar un històric de senyals, amples de banda, etc.

4 Metodologia

Per aquest projecte s'ha seguit la metodologia corresponent a un procés iteratiu-incremental[6], que consta de les fases de planificació, requeriments, anàlisi i disseny, proves, evaluació i finalització (sent úniques la primera i la última i les altres quatre fent-se iterativament. Això permet que el projecte pugui anar avançant per parts independents entre elles obtenint la funcionalitat esperada sense que afecti a les demés.

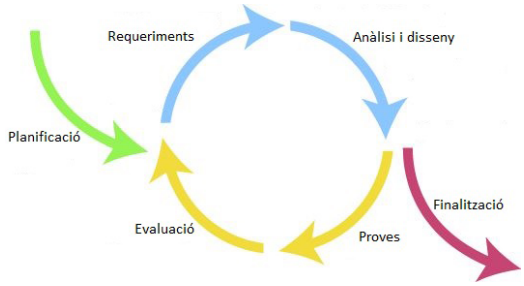

Fig. 3: Procés iteratiu-incremental

S'ha decidit escollir aquesta metodologia perquè és la que més s'adapta al projecte, doncs els objectius permeten que la implementació de les diferents parts siguin independents i tinguin el seu propi cicle, cosa important degut a que la afectació sobre el servei ha de ser la mínima possible.

5 Planificació

El projecte s'ha hagut de planificar adequament per saber quines són les tasques a fer, ordenades per prioritat i amb un temps assignat a cadascuna.

Aquestes tasques són les següents (veure Fig. 4 per la planificació en el temps):

1. Planificar les accions a realitzar sobre la xarxa i decidir l'ordre
2. Aplicar un sistema d'autenticació
3. Aplicar un sistema de logs
4. Posar en marxa el protocol *OSPF* i activar els enllaços per la redundància
5. Aplicar un sistema de monitorització
6. Comprovar que el sistema funciona correctament, i si cal, solucionar els problemes provocats
7. Extreure'n conclusions i observar si el sitema ha millorat

6 Desenvolupament

6.1 Estat inicial

La xarxa de Meswifi, en un primer moment, presenta problemes que s'han de sol·lucionar, però aquests venen d'una planificació dolenta i una configuració que no s'ha canviat durant el pas del temps.

6.1.1 VLANs i bridging

Una VLAN (xarxa d'àrea local virtual)[7] fa referència a una o més xarxes d'àrea local que es comporten com si estiguessin al mateix segment de xarxa físic, el que permet també tenir més d'una xarxa separada en el mateix segment físic i per tant, el domini de *broadcast*[8] (un paquet de *broadcast* és aquell que arribarà a tot el segment de xarxa en el que es trobi, en el nostre cas, a tota la mateixa VLAN).

La xarxa es divideix principalment en tres VLANs distintes, una per l'administració (VLAN 100), i les altres dues per la connexió a Internet (950 i 2000), però a diferència de la primera no estan presents a tota la xarxa de manera global, sinó que estan truncades (és a dir, tots els dispositius pertanyen a aquestes 3 VLANs però hi ha un punt de la xarxa on es separen, com podem observar a la Fig. 5). Aquesta diferència d'VLANs per les dades ve donada per la existència de diferents sortides a Internet per diferents proveïdors, de manera que només existeix un router per a cada proveïdor.

Per entendre millor com arribem a aquesta distribució de xarxa, hem de saber què és un bridge. Quan parlem d'un bridge en la terminologia de xarxes, parlem d'aquell dispositiu que interconnecta segments de xarxa fent que aquests formin part del mateix. La xarxa disposa de dispositius (switchos) que permeten activar o desactivar la funció de bridge per cada VLAN, així arriba la xarxa a tenir interconnectats al mateix domini de *broadcast* més de 700 nodes de manera inalàmbrica. Tots aquests també pertanyen a la mateixa subxarxa, la 10.32.40.0/22.

6.1.2 Autenticació

Meswifi fa ús del protocol *PPPoE*[9] per l'autenticació dels clients i per fer la entrega d'IPs públiques a les antenes. Aquest protocol (*Point-to-Point Protocol over Ethernet*) s'encarrega d'encapsular una connexió *PPP* sobre la capa Ethernet. El protocol *PPP* serveix per establir una connexió directa entre nodes, proveïnt (no necessàriament) de:

- autenticació de connexió
- xifrat de la transmissió (*ECP*)
- compressió

En el cas d'aquesta xarxa només s'utilitza la primera opció, però per cada client, encara que la IP assignada sigui dinàmica, té un perfil dedicat amb un usuari i una contrasenya, això comporta un cost afegit innecessari al manteniment d'aquest aspecte. A més, en comptes de fer servir

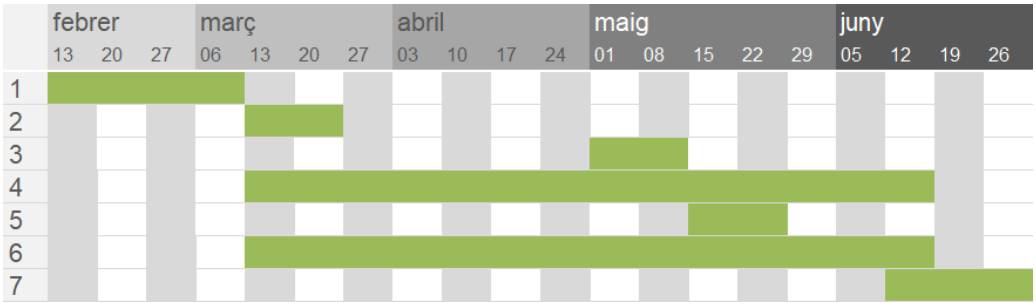

Fig. 4: Planificació

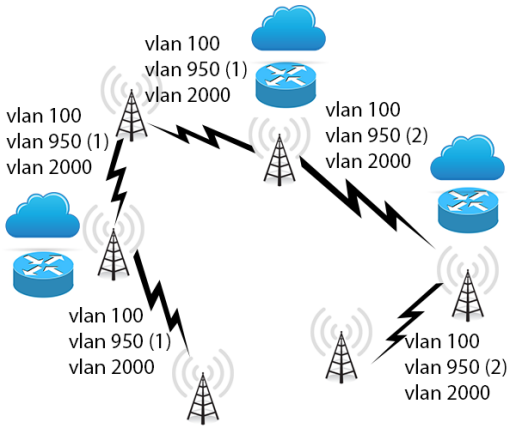

Fig. 5: Configuració xarxa antiga

un sistema centralitzat on estigui tota la relació d'usuaris, aquesta està present distribuïda entre diferents punts de la xarxa, encara que en qualsevol d'aquests no es disposa de tota la relació, si no només de part d'aquesta.

El sistema tampoc ha estat dissenyat de manera que cada cop que un usuari s'autentica quedi gravada la informació de la seva sessió amb les dades necessàries (IP pública entregada, adreça física del dispositiu, usuari utilitzat, data d'entrega i data de finalització de la sessió), aquest és un problema que també s'ha de sol·lucionar.

6.1.3 Redundància inexistent i sense monitorització

Degut a la naturalesa de la configuració de la xarxa no pot existir cap tipus de redundància, doncs en el cas de connectar un enllaç que permetés la sortida del tràfic per una ruta alternativa això no portaria més que problemes ja que provocaria un *bridge loop* i tot seguit un *broadcast storm* (un *broadcast storm* apareix a causa del tràfic de *broadcast*, aquest és dirigit a tots els dispositius del mateix segment de xarxa i un switch el tracta de forma que enviarà aquest tràfic per totes les boques que pertanyin a aquest segment, si existeix un bucle aquest tràfic es reenviarà de manera indefinida per tots els ports i haurà de ser processat per tots els dispositius, provocant inclús reinicis dels nodes de la xarxa), això significa una caiguda total de la xarxa ja que tota pertany al mateix segment i l'afectació seria del 100%.

A més, per la decisió de no embrutar més la xarxa amb tràfic de *broadcast* es va decidir no implementar cap tipus de sistema de monitorització, no obstant, un sistema d'aquest tipus és vital per tenir el control sobre una xarxa on saber quin és el node que provoca la caiguda d'una part pot fer que una caiguda que es pot sol·lucionar en 5 minuts duri hores.

6.1.4 Equipació disponible

Per complir amb els objectius d'aquest projecte l'empresa disposa de la següent equipació:

- 3 x Router MikroTik CCR1036-12G-4S
- 1 x Servidor SunFire X2250 (Sun Microsystems), 2 x Intel Xeon L5420 @ 2.5GHz (4 cores), 16GB RAM, 2 x 1TB (raid 1)

Aquests dispositius permeten la sol·lució dels problemes que presenta la xarxa, els routers permeten posar en marxa la redundància que tant necessària és i el servidor és d'utilitat per allotjar les aplicacions que calen pel sistema d'autenticació centralitzat, un sistema de logs lligat al sistema d'autenticació i el sistema de monitorització. Com a pas previ s'ha instal·lat un sistema de virtualització per a poder allotjar els sistemes necessaris. Un sistema de virtualització permet instal·lar diversos sistemes operatius en una mateixa màquina física i que aquests siguin totalment independents els uns dels altres, amb la seva configuració de xarxa i diferent programari instal·lat. La decisió ha estat instal·lar *Proxmox VE*[10], un entorn de virtualització de codi lliure amb administració via web, que permet la migració de màquines en calent i la pogramació de còpies de seguretat.

Dins del sistema de virtualització s'han instal·lat tres màquines virtuals amb les següents característiques:

- Ubuntu Server 16.04 LTS, 1 x 2 cores, 3GB RAM, 20GB HDD, IP 10.100.1.100/24
- Ubuntu Server 16.04 LTS, 2 x 4 cores, 8GB RAM, 500GB HDD, IP 10.100.1.101/24
- Ubuntu Server 16.04 LTS, 2 x 2 cores, 4GB RAM, 400GB HDD, IP 10.100.1.102/24

El primer servidor anirà destinat a allotjar el sistema d'autenticació, el segon servirà pel sistema de logs i el tercer per monitoritzar la xarxa. Per entendre la configuració de xarxa, veure la secció 6.4.

6.2 Sistema d'autenticació

Per posar en marxa el sistema d'autenticació s'ha decidit instal·lar *FreeRADIUS* amb *daloRADIUS* per la seva administració. *FreeRADIUS* és un servidor del protocol *RADIUS*

(acrònim de *Remote Authentication Dial-In User Service*), aquest es fa servir per comprobar que la informació d'autenticació demanada en el sistema d'enregistrament (en aquest cas *PPPoE*) sigui correcta i donar una autorització que pot portar diferents recursos de xarxa, com pot ser una direcció IP. *daloRADIUS* és una interfície web per l'administració dels diferents paràmetres del servidor *RADIUS*.

Per instal·lar el sistema d'autenticació a la màquina virtual corresponent, s'han executat les següents comandes[11][12]:

```
apt-get update
apt-get upgrade
apt-get install php5-common php5-gd php-pear php-
    db libapache2-mod-php5 php-mail
apt-get install php7.0 libapache2-mod-php7.0 php7
    .0-mysql php7.0-gd php-pear php-db
service apache2 restart
apt-get install freeradius freeradius-mysql
mysql -u root -p
        mysql> create database radius;
        mysql> create user raduser@localhost
            identified by "*****";
        mysql> grant all on raddb.* to
            raduser@localhost;
        mysql> quit
vim /etc/freeradius/sql.conf
        > login = "raduser"
        > password = "*****"
        > radius_db = "raddb"
vim /etc/freeradius/clients.conf
        > secret = "*****"
        > client 10.100.0.0/16 {
                secret = Adam-Wisp23
                shortname = meswifi-internal
        }
service freeradius restart
wget https://github.com/lirantal/daloradius/
    archive/master.zip
unzip master.zip
cp -r daloradius-master/* /var/www/html/
chown -R www-data:www-data /var/www/html/
mysql -u raduser -p raddb < /var/www/html/contrib
    /db/mysql-daloradius.sql
vim /var/www/html/library/daloradius.conf.php
        > \$configValues['CONFIG_DB_USER'] = '
            raduser';
        > \$configValues['CONFIG_DB_PASS'] =
            '*****';
        > \$configValues['CONFIG_DB_NAME'] = '
            raddb';
```

Amb aquesta configuració s'especifica l'usuari i contrasenya de la base de dades a utilitzar i es permet l'accés de totes les peticions que vinguin de la xarxa 10.100.0.0/16. S'accedeix a la interfície web de *daloRADIUS* a través de l'adreça http://10.100.1.100/login.php (el primer cop permet crear una contrasenya d'administració). A través de la interfície web es crea un usuari que servirà per a tots els clients particulars, que disposaran d'una IP dinàmica, per fer això es segueixen els següents passos:

1. Mangament → New User
2. Username: meswifippp Password: ******
3. Attributes → Vendor: dictionary-rfc2869 Attribute: Framed-Pool[13] → Add Attribute
4. Value: meswifi Op: = Target: reply → Apply

Per crear un usuari amb IP estàtica, s'han de seguir els següents passos:

1. Management → New User - Quick Add
2. Username: usuari Password: ***** Framed-IP-Address[14]: adreça-IP
3. Apply

Els routers *MikroTik* fan servir el sistema operatiu *RouterOS*, que està basat en Linux però que implementa funcionalitats pròpies de les *ISPs*, com poden ser els protocols d'enrutament per routers frontera. Aquest sistema operatiu permet l'ús (segons llicència) com a servidor *PPPoE*, utilitzat per l'entrega d'IPs als dispositius connectats a la xarxa però a través d'una autenticació d'usuari i contrasenya. Per defecte *RouterOS* consulta una base de dades local per la relació usuari-contrasenya, que es pot omplir sempre que es tingui accés a aquest dispositiu, però a més també permet la configuració d'un servidor *RADIUS* extern per la consulta i autorització de les dades corresponents.

El que s'ha fet en aquest projecte per sol·lucionar els problemes que comporta mantenir una relació d'usuaris per cada router existent és centralitzar-ho tot en una sola base de dades i realitzar les peticions a través d'el client *RADIUS* incorporat a cada router *MikroTik*, per fer això, amb el sistema de *FreeRADIUS + daloRADIUS* instal·lat, es configura cada router executant les següents comandes amb una connexió per SSH:

```
/radius add address=10.100.1.100 secret=******
    service=ppp src-address=<IP-del-router>
/ppp aaa set use-radius=yes
```

Fent servir aquesta configuració els routers, en el cas de no tenir cap coincidència a la seva base de dades local a l'hora d'autenticar un usuari pel protocol *PPP*, farà la consulta d'autenticació al servidor *RADIUS* especificat.

6.3 Sistema de logs

Per guardar tots els intents, siguin acceptats o denegats, de connexió al nostre sistema d'autenticació, es necessita un sistema de logs per dur a terme la tasca. S'ha decidit fer servir *graylog2*[15], en aquest cas s'ha instal·lat fent servir la tecnologia oferida per *Docker*[16], que és una plataforma de contenidors (semblant a les màquines virtuals, però en comptes de sistemes operatius, aplicacions) que permet la execució, independentment del sistema on estiguin corrent, de l'aplicació que s'ha preparat amb anterioritat de manera eficient i lleugera. Per fer la instal·lació de tot el sistema, s'han executat les següents comandes:

```
mkdir /graylog
cd /graylog
wget https://raw.githubusercontent.com/Graylog2/
    graylog2-images/2.1/docker/config/graylog.
    conf
wget https://raw.githubusercontent.com/Graylog2/
    graylog2-images/2.1/docker/config/log4j2.xml
curl -L "https://github.com/docker/compose/
    releases/download/1.9.0/docker-compose-$(
    uname -s)-$(uname -m)" -o /usr/local/bin/
    docker-compose
ln -s /usr/local/bin/docker-compose /usr/bin/
    docker-compose
vim /graylog/docker-compose.yml
        version: '2'
        services:
          mongo:
            image: "mongo:3"
```

```
      volumes:
        - /graylog/data/mongo:/data/db
    elasticsearch:
      image: "elasticsearch:2"
      command: "elasticsearch -Des.cluster.
          name='graylog'"
      volumes:
        - /graylog/data/elasticsearch:/usr/
            share/elasticsearch/data
    graylog:
      image: graylog2/server:2.1.2-1
      volumes:
        - /graylog/data/journal:/usr/share/
            graylog/data/journal
        - /graylog/config:/usr/share/
            graylog/data/config
      environment:
        GRAYLOG_PASSWORD_SECRET: *****
        GRAYLOG_ROOT_PASSWORD_SHA2: *****
        GRAYLOG_WEB_ENDPOINT_URI: http
            ://10.100.1.101:9000/api/
      depends_on:
        - mongo
        - elasticsearch
      ports:
        - "9000:9000"
        - "12201/udp:12201/udp"
        - "1514/udp:1514/udp"
docker-compose up
```

Per fer la instal·lació més senzilla, s'ha fet servir *docker-compose*[17], que permet crear un arxiu de configuració (*docker-compose.yml*) a través del qual s'especifiquen els diferents contenidors que s'han d'executar, les carpetes que s'han de poder veure des de fora dels contenidors, quin port podrà ser accedit des de fora dels contenidors, etc.

Un cop aixecats els contenidors es pot accedir a la interfície web de *graylog2* a través de la url http://10.100.1.101:9000/. Per fer que els routers enviïn els seus logs cap el nou servidor, s'han d'executar les següents comandes a cadascun d'ells[18]:

```
/system logging action add bsd-syslog=yes name=
    graylog remote=10.100.1.101 remote-port=1514
    target=remote
/system logging
add action=graylog topics=pppoe,info
add action=graylog topics=pppoe,ppp,info,account
add action=graylog topics=pppoe,ppp,error
```

D'aquesta forma quedaran enregistrats tant els intents de connexió fallits com els que s'efectuin de manera correcta, amb la informació suficient per identificar la pertinença d'una IP específica en un temps determinat.

6.4 Redundància a la xarxa

El problema principal de la xarxa ve degut a la falta de redundància, i aquesta falta apareix perque tota la xarxa pertany al mateix domini de *broadcast*, separat en diferentes VLANs per dades de client i administració, com s'ha explicat a l'apartat 6.1.1.

La nova estructura de la xarxa es fa possible gràcies a la incorporació de diferents routers en punts específics. Aquests routers permeten eliminar el *bridging* de les VLANs de dades i administració, fent-se càrrec ells mateixos de gestionar el *PPPoE* i d'enrutar la xarxa d'administració, creant així diferents subsegments de xarxa cadascun amb el seu domini de *broadcast*. Es creen llavors, per cada router, una subxarxa per l'administració, a la VLAN 123, una altra VLAN, la 800, per on es realitzaran les peticions *PPPoE* i una subxarxa per cada enllaç de troncal que existeixi en aquell punt. Les subxarxes per cada enllaç permeten la connexió IP directa entre els routers que siguin veïns, requeriment necessari per poder aplicar el protocol *OSPF*, que serà el que s'encarregui d'afegir la redundància a la xarxa. A més, com Meswifi disposa de diferentes sortides a Internet, s'han de crear les regles necessàries d'enrutament per a cada rang d'IPs, doncs així es pot entregar qualsevol de les IPs de les que es disposa independentment del lloc on es trobi el client dins de la xarxa.

S'ha escollit la xarxa 10.100.0.0/16 per dividir-la en diferents subxarxes per fer servir com a part d'administració, es creen així una subxarxa del tipus 10.100.X.0/24 per a cada repetidor, que com s'ha dit abans, pertany a la VLAN 123 del router present en el repetidor específic. Es reserven les IPs des de la 10.100.X.50 fins la 10.100.X.254 per muntar un servidor *DHCP* que s'encarregarà d'oferir les IPs d'administració als equips de clients. La IP 10.100.X.1 correspondrà al router, la 10.100.X.2 al switch i des de la 10.100.X.3 fins la 10.100.X.49 es faran servir pels equips de repetició, que tindran les IPs assignades de forma estàtica i manual.

Per fer aquesta configuració s'han d'executar les següents comandes a cada router:

```
/ip address add address=10.100.X.1/24 interface=
    vlan123 network=10.100.X.0
/interface vlan add interface=ether12 name=
    vlan123 vlan-id=123
/interface bridge add name=vlan123
/interface bridge port add bridge=vlan123
    interface=vlan123_ether12
/ip pool add name=dhcp123 ranges=10.100.X
    .50-10.100.X.254
/ip dhcp-server network add address=10.100.X.0/24
     dns-server=8.8.8.8,8.8.4.4 gateway=10.100.X
    .1 netmask=24
/ip dhcp-server add address-pool=dhcp123 disabled
    =no interface=vlan123 lease-time=23h59m59s
    name=dhcp123 src-address=10.100.X.1
```

Per la part de les subxarxes dedicades als enllaços de troncal, s'ha escollit la xarxa 10.200.0.0/24, que en aquest cas s'ha hagut de dividir en subxarxes del tipus 10.200.0.X/29 (cada /29 correspon a un rang de 8 IPs, 6 d'elles utilitzables), ja que existeixen 4 equips amb IP, ambdós routers i els dos equips inalàmbrics. Per poder fer servir el protocol *OSPF* i evitar problemes futurs, ja que aquest depen de l'estat físic d'una interfície, a més, s'ha de crear una interfície virtual que per aquest projecte s'anomenarà *loopback* i serà del tipus *bridge*, aquesta tindrà una IP del rang 10.255.255.0/24, i cada router tindrà una IP d'aquest rang, és aquest rang el que serveix realment per la comunicació entre routers, doncs fa possible l'enrutament encara que un dels enllaços estigui caigut. Es creen també regles específiques d'enrutament per no crear bucles per quan s'intenti accedir des de una IP pública cap a una altra que estigui present a la xarxa de Meswifi.

S'executen les següents comandes a cada router per complir amb la configuració:

```
/interface bridge add name=loopback
/ip address
add address=10.255.255.X interface=loopback
    network 10.255.255.X
add address=10.200.0.X/29 comment="troncal 1"
    interface=ether1 network=10.200.0.X
```

```
add address=10.200.0.X/29 comment="troncal 2"
    interface=ether2 network=10.200.0.X
/routing ospf instance set [ find default=yes ]
    redistribute-connected=as-type-1 router-id
    =10.255.255.X
/routing ospf network
add area=backbone network=10.200.0.0/24
add area=backbone network=10.255.255.0/24
/ip route
add distance=1 gateway=10.255.255.1 routing-mark=
    jazztel scope=10 target-scope=20
add distance=1 gateway=10.255.255.4 routing-mark=
    ono scope=10 target-scope=20
add distance=1 gateway=10.255.255.8 routing-mark=
    airenetworks scope=10 target-scope=20
add distance=1 dst-address=10.100.1.0/24 gateway
    =10.255.255.1 routing-mark=adm scope=10
    target-scope=20
/ip route rule
add dst-address=10.100.1.0/24 table=adm
add dst-address=62.14.146.0/24 table=main
add dst-address=62.14.148.0/24 table=main
add dst-address=5.40.92.0/24 table=main
add dst-address=62.175.244.0/24 table=main
add dst-address=5.40.253.0/24 table=main
add dst-address=5.154.45.0/24 table=main
add dst-address=84.236.155.0/24 table=main
add dst-address=10.255.255.0/24 table=main
add src-address=62.14.146.0/24 table=jazztel
add src-address=62.14.148.0/24 table=jazztel
add src-address=5.40.92.0/24 table=ono
add src-address=62.175.244.0/24 table=ono
add src-address=5.40.253.0/24 table=ono
add src-address=5.154.45.0/24 table=airenetworks
add src-address=84.236.155.0/24 table=
    airenetworks
```

Pel que fa a la part del servidor *PPPoE* de cada router, s'ha de crear la VLAN 800 i especificar, com hem vist a l'apartat 6.2, el nom que correspon al *pool* d'adreces IP que farà servir el perfil *meswifippp*, aquest *pool* a més, s'ha d'ajustar segons quines IPs públiques dinàmiques es volen entregar en el router específic. Es té en compte també la configuració ja realitzada a l'apartat 6.2 que fa referència al *RADIUS*.

S'han d'executar, per tant, les següents comandes:

```
/interface vlan add interface=ether12 name=
    vlan800 vlan-id=800
/ip pool add name=meswifi ranges
    =62.14.148.220-62.14.148.254
/ppp profile add dns-server=8.8.8.8,8.8.4.4 local
    -address=10.23.45.67 name=meswifi remote-
    address=meswifi
/interface pppoe-server server add default-
    profile=meswifi disabled=no interface=vlan800
     max-mru=1480 max-mtu=1480 mrru=1600 service-
    name=MESWIFI
```

Aplicades aquestes configuracions, la xarxa ara disposa de redundància a més d'un manteniment molt més fàcil, havent-se de preocupar de menys coses i amb un rendiment millorat, ja que ara es pot escollir el camí més curt o menys saturat fins la sortida a Internet que el client estigui fent servir gràcies al protocol *OSPF*.

6.5 Sistema de monitorització

Tota xarxa mitjanament gran hauria de tenir un sistema de monitorització per saber en qualsevol moment l'estat en el que es troben els dispositius que pertanyen a aquesta i fer més ràpida la resposta en cas que algun node provoqui una caiguda. En una empresa que es dedica a oferir connexió a Internet al seus clients tenir un sistema de monitorització és vital.

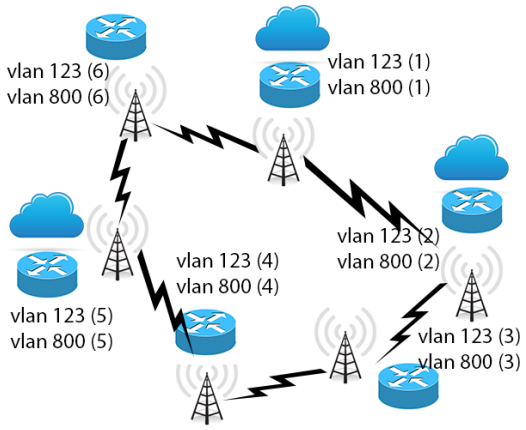

Fig. 6: Configuració xarxa nova

En el cas de Meswifi, els equips que utilitza són de la marca *Ubiquiti* (tant els repetidors com les antenes de client), i aquest fabricant ofereix la seva pròpia solució quant a la monitorització dels seus dispositius, anomenada *airControl2*[19]. Aquesta eina, un cop afegits els equips mitjançant el programari de client, mostra totes les dades que interessen per a poguer mantenir la xarxa, com són les senyals inalàmbriques, si el dispositiu està connectat, el temps de funcionament i de connexió, etc. a més també ofereix un sistema d'avisos configurables a través de correu electrònic, per exemple si un dispositiu baixa d'una senyal preestablerta, si es desconnecta del sistema, etc.

Per instal·lar aquest sistema a la tercera màquina virtual, s'han executat les següents comandes:

```
apt-get update
apt-get upgrade
apt-get install default-jdk iperf
wget http://www.ubnt.com/downloads/aircontrol2/
    aircontrol-v2.1-Beta4.2212.170323.1619-unix64
    .bin
chmod u+x aircontrol-v2.1-Beta4.2212.170323.1619-
    unix64.bin
./aircontrol-v2.1-Beta4.2212.170323.1619-unix64.
    bin
```

Un cop instal·lat, cal descarregar el programari de client (disponible per Linux, Mac OS X i Windows) i entrar a través de la IP 10.100.1.102 amb l'usuari i contrasenya configurats durant la instal·lació. Ara només cal afegir els equips a monitoritzar i configurar els avisos, que per aquest cas han estat dos, un que avisi quan qualsevol repetidor passi a estat desconnectat i un altre que ho faci quan torni a connectar-se, tots dos enviaran un correu electrònic a una adreça electrònica destinada a rebre aquests avisos.

7 Conclusions

Durant aquest projecte s'ha hagut de idear una nova xarxa per la empresa Meswifi tenint en compte la xarxa que ja tenia, aquestes dues han hagut de conviure durant la fase de conversió d'una a l'altre perque els clients no tinguessin cap tall i evitar els problemes que això comporta, doncs no han de ser afectats per un disseny dolent que ha deixat de tenir en compte aspectes fundamentals a l'hora de realitzar-lo, si es que s'ha arribat a realitzar desde el primer moment.

L'objectiu principal del projecte era solucionar el problema de la xarxa sense afectar als usuaris, cosa que s'ha pogut realitzar amb èxit.

Un cop aplicats tots els canvis i millores a la xarxa s'observa una millora considerable respecte a com estava la xarxa en un principi. Es passa de tenir una xarxa mal configurada amb problemes de rendiment degut a la gran quantitat de tràfic de tipus *broadcast* provocat per tants nodes que pertanyien a la mateixa subxarxa, a més de no tenir redundància per la naturalesa de la mateixa xarxa, amb un sistema d'autenticació difícil de mantenir perque la relació d'usuaris-contrasenyes estava repartida per tota la xarxa sense cap tipus de logs i un sistema de monitorització inexistent a una xarxa totalment remodelada on si cau un enllaç de troncal el tràfic sortirà per un altre, sempre i quan existeixi la sortida alternativa, amb una monitorització amb avisos automàtics de caigudes, un sistema de logs eficient que a més proporciona informació valuosa a l'empresa i un sistema d'autenticació centralitzat que fa l'alta i el manteniment de nous usuaris molt més fàcil.

Així doncs, es considera que tots els objectius han estat assolits, remarcant el de que els usuaris no s'hagin donat compte del canvi pel que fa a les possibles caigudes de xarxa que s'haguessin pogut ocasionar durant la transició.

7.1 Futur després del projecte

El futur de la xarxa de la empresa, ara que ja està dissenyada pensant en l'escalabilitat i disponibilitat, passa per fer sortir tot el tràfic d'Internet per un sol punt, suficientment redundat. En el moment d'aquest projecte Meswifi ja es troba fent els tràmits necessaris per donar-se d'alta a RIPE (Réseaux IP Européens)[20], l'organisme encarregat d'assignar rangs d'IPs públiques a les empreses que ho demanin, a Europa. A part també està fent les negociacions corresponents per tenir un lloc on disposar d'un rack per la interconnexió amb diferents proveïdors i la sortida principal a Internet. Això significa una simplificació encara més gran de l'administració de la xarxa, doncs ja no s'han de tenir regles específiques d'enrutament a cada router, i, en el cas d'arribar a aconseguir un altre punt de sortida a Internet es podria triar la ruta més curta, mantenint el mateix rang d'IPs assignat per RIPE.

AGRAÏMENTS

A la meva dona, per el suport que m'ha donat durant la realització del projecte i tot el que ha fet per aconseguir-me el temps necessari per dedicar al desenvolupament d'aquest treball. Al meu tutor, Joan Serra-Sagristà, per guiar-me i resoldre els meus dubtes durant aquests mesos de treball. Al coordinador de grau, Jordi Pons Aróztegui, per animar-me a completar el projecte i preocupar-se per fer possible la realització de la meva carrera. Al meu antic cap de feina i company, Adam Marsal Llobet, ja que gràcies a ell he pogut realitzar aquest projecte a la seva empresa i he pogut aprendre molt durant el temps que he treballat per ell. Al meu amic, Ismael Hernández Bernabeu, graduat en enginyeria informàtica a la Escuela Politécnica Superior de Alcoy de la Universidad Politécnica de Valencia, per aconsellar-me en diferents aspectes del treball i donar-me suport.

REFERÈNCIES

[1] Choosing a Common IGP for the IP Internet (The IESG's Recommendation to the IAB), 1992. https://tools.ietf.org/html/rfc1371 [Últim accés abril de 2017]

[2] OSPF Version 2, 1991. https://tools.ietf.org/html/rfc1247 [Últim accés maig de 2017]

[3] Manual:OSPF Case Studies - MikroTik Wiki.https://wiki.mikrotik.com/wiki/Manual:OSPF_Case_Studies [Últim accés maig de 2017]

[4] What is Syslog? Linux & Windows Syslog Server Options. http://www.networkmanagementsoftware.com/what-is-syslog/ [Últim accés abril de 2017]

[5] Top 10 Reasons to use Network Monitoring Solutions. https://techtalk.gfi.com/top-10-reasons-network-monitoring-solutions/ [Últim accés febrer de 2017]

[6] Iterative and incremental development - Wikipedia. https://en.wikipedia.org/wiki/Iterative_and_incremental_development [Últim accés febrer de 2017]

[7] Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, 1999. https://www.ietf.org/rfc/rfc2674.txt [Últim accés abril de 2017]

[8] What is a Broadcast Storm? - Definition from Techopedia. https://www.techopedia.com/definition/6270/broadcast-storm [Últim accés maig de 2017]

[9] A Method for Transmitting PPP Over Ethernet (PPPoE), 1999. https://www.ietf.org/rfc/rfc2516.txt [Últim accés febrer de 2017]

[10] Installation - Proxmox VE. https://pve.proxmox.com/wiki/Installation [Últim accés març de 2017]

[11] Install FreeRADIUS and DaloRADIUS - VPN Integration with WHMCS. http://vpn.whmcssmarters.com/install-freeradius-and-daloradius/ [Últim accés març de 2017]

[12] Servidor FreeRADIUS + MySQL y gestión Web "DaloRADIUS". http://elcajondelelectronico.com/freeradius/ [Últim accés març de 2017]

[13] RADIUS Extensions, 2000. https://www.ietf.org/rfc/rfc2869.txt [Últim accés març de 2017]

[14] Remote Authentication Dial In User Service (RADIUS), 2000. https://tools.ietf.org/html/rfc2865 [Últim accés març de 2017]

[15] Graylog — Open Source Log Management. https://www.graylog.org/features [Últim accés abril de 2017]

[16] What is Docker? https://www.docker.com/what-docker [Últim accés maig de 2017]

[17] Docker - Graylog 2.2.1 documentation. http://docs.graylog.org/en/2.2/pages/installation/docker.html [Últim accés maig de 2017]

[18] Manual:System/Log - MikroTik Wiki. https://wiki.mikrotik.com/wiki/Manual:System/Log [Últim accés abril de 2017]

[19] airControl - How to Install airControl on Ubuntu Server - Ubiquiti Networks Support and Help Center. https://help.ubnt.com/hc/en-us/articles/218279908-airControl-How-to-Install-airControl-on-Ubuntu-Server [Últim accés maig de 2017]

[20] RIPE Network Coordination Centre. https://www.ripe.net/ [Últim accés juny de 2017]