UNIVERSITAT POLITÈCNICA DE CATALUNYA

Estudi de la implantació de IPv6 a la xarxa *guifi·net*

13 de juliol de 2017

Memòria del projecte que presenta Jordi Masip
sota la direcció del Dr. Eng. Francisco Del Águila
per assolir el grau d'Enginyer en Sistemes TIC.

Agraeixo el suport i l'ajuda de la Qiwei, el meu tutor Paco, els membres de l'Associació Guifibages, i a totes aquelles persones que m'han ajudat.

Índex

Abstract

In this document we'll explain how *guifi·net* network works with IPv4 and propose how it could be the IPv6 network. Finally, we'll set up a proof of concept.

Resum

En aquest treball s'explicarà com funciona la xarxa *guifi·net* IPv4 i es farà una proposta de com podria ser la xarxa amb IPv6. Finalment, es realitzarà una prova per verificar la proposta.

Part I.

Context històric

1. Introducció

Aquest projecte consisteix en planificar la implantació de IPv6 a la xarxa *guifi·net*. Per implantar IPv6 a *guifi·net* s'ha de fer un pla d'adreçament per decidir quines IPs destinarem a cada regió, zona i aparell de la xarxa.

A més, com que *guifi·net* és una xarxa de transport que permet que proveïdors d'Internet ofereixin un servei a la xarxa, s'ha de buscar la millor manera perquè els proveïdors puguin treballar sobre la xarxa, sense imposar gaires restriccions, amb una solució que maximitzi el rendiment i l'escalabilitat i no resulti en un cost desorbitat.

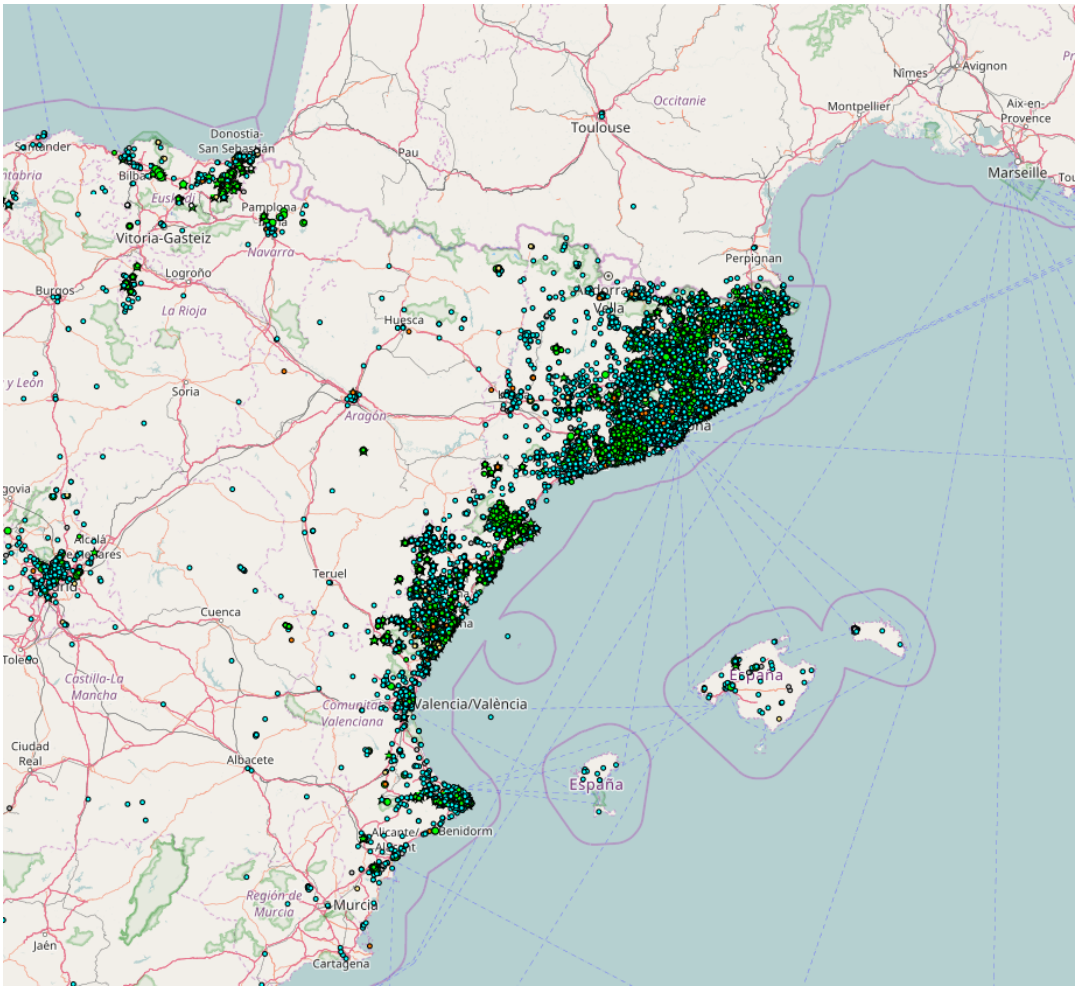

Figura 1.1.: Nodes que trobem als Països Catalans

2. Internet al llarg dels anys

2.1. Als inicis

> I, finalment, perquè ningú podia decidir-se i jo estava assegut allà al Departament de Defensa tractant d'aconseguir que aquest programa avancés, vaig dir: és de 32 bits. Això és. Anem a fer alguna cosa. I aquí estem, culpa meva.
>
> — Dr. Vinton G. Cerf

Cap al 1997, quan va escollir 32 bits per l'adreçament de l'*Internet Protocol* (IP), a Vint Cerf li hauria costat creure's que en un parell de dècades, una xarxa global amb bilions de màquines hauria revolucionat les comunicacions. Al cap i a la fi, en aquella època el número de màquines de la xarxa ARPANET era tan sols d'unes 100.

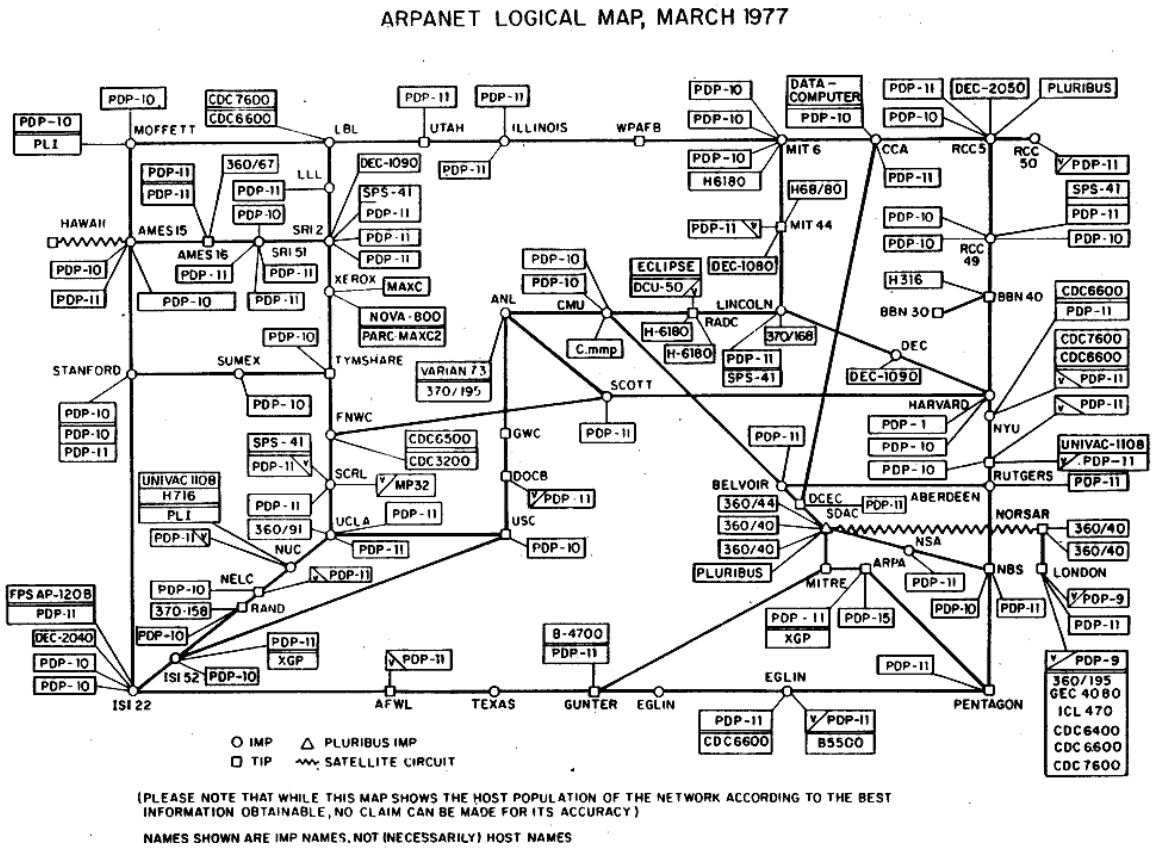

Figura 2.1.: Mapa lògic d'ARPANET, març 1977

2.2. Internet Protocol

IPv6 és la versió més recent de *Internet Protocol*[17g; 17h; 17i], el protocol de comunicacions que permet retransmetre datagrames (paquets de dades) entre xarxes. La seva funció d'encaminament permet la interconnexió de xarxes. La feina del protocol IP és entregar paquets des d'una màquina d'origen a una màquina de destí, basant-se en l'adreça IP que es troba definida a la capçalera del paquet. Amb aquest objectiu, el protocol IP defineix l'estructura del paquet per encapsular les dades que s'han d'entregar conjuntament amb la informació d'origen i destí. Assegurar l'entrega, la integritat de les dades o la seqüenciació és feina de les capes superiors, com ara el protocol TCP (Transmission Control Protocol).

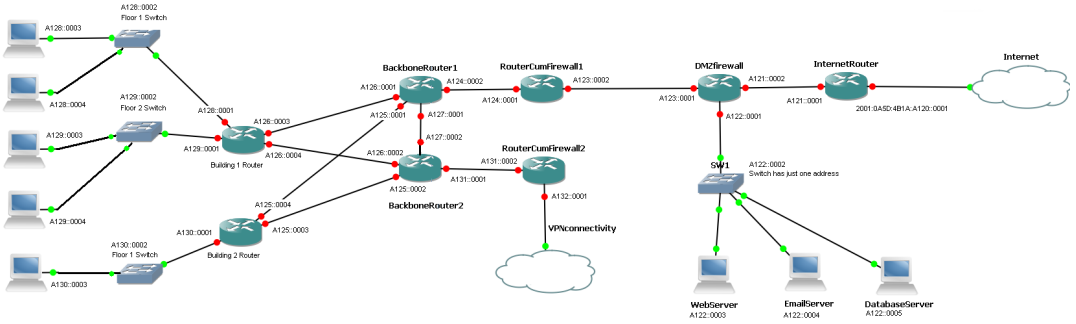

Figura 2.2.: Exemple de xarxa

La primera gran versió va ser IPv4, descrita a la publicació RFC 791 (setembre de 1981) de IETF. IPv4 utilitza adreces de 32 bits, limitant l'espai d'adreces a 4.294.967.296 (2^{32}). D'aquests 4 bilions d'adreces es reserven uns 18 milions per adreces especials (veure la taula 2.1).

Rang	Descripció
`0.0.0.0/8`	Current network (only valid as source address)
`10.0.0.0/8`	Private network
`100.64.0.0/10`	Shared Address Space
`127.0.0.0/8`	Loopback
`169.254.0.0/16`	Link-local
`172.16.0.0/12`	Private network
`192.0.0.0/24`	IETF Protocol Assignments
`192.0.2.0/24`	TEST-NET-1, documentation and examples
`192.88.99.0/24`	IPv6 to IPv4 relay (includes 2002::/16)
`192.168.0.0/16`	Private network
`198.18.0.0/15`	Network benchmark tests
`198.51.100.0/24`	TEST-NET-2, documentation and examples
`203.0.113.0/24`	TEST-NET-3, documentation and examples
`224.0.0.0/4`	IP multicast (former Class D network)
`240.0.0.0/4`	Reserved (former Class E network)
`255.255.255.255`	Broadcast

Taula 2.1.: Blocs d'adreces reservades

La notació més comuna d'expressar una adreça IPv4 és amb 4 octets separats per punts (`.`), per exemple, `192.168.1.100`. Una adreça IP està formada per dues parts: el **prefix** de la xarxa i l'**identificador de la interfície** ("màquina de destí")[17f].

2.2.1. Classful Network

L'any 1981 es van començar utilitzar l'arquitectura *Classful Network*[17j]. Consisteix en dividir les adreces IPv4 en 5 rangs de classes (veure la taula 2.2).

Classes	bits inicials	Número de xarxes	Adreces per xarxa	Adreça d'inici
Class A	0	128 (2^7)	16,777,216 (2^{24})	0.0.0.0
Class B	10	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0
Class C	110	2,097,152 (2^{21})	256 (2^8)	192.0.0.0
Class D (multicast)	1110	not defined	not defined	224.0.0.0
Class E (reserved)	1111	not defined	not defined	240.0.0.0

Taula 2.2.: Classificació de les xarxes per classes

A l'hora d'assignar blocs d'adreces IP, s'utilitzava l'arquitectura anterior. El principal problema que va suposar aquesta arquitectura és que moltes organitzacions que sol·licitaven un bloc d'adreces IP rebessin un de classe B (a causa del nombre reduït d'adreces que ofereix la classe C). Això va produir que amb poc temps s'exhaurissin el nombre de xarxes d'aquesta classe B[17k].

El novembre de 1991 es va crear *Routing and Addressing Group* (ROAD) per intentar resoldre els problemes que estava generant l'arquitectura d'adreçament *Classful Network*. Es van començar a adoptar noves tecnologies per frenar l'esgotament d'adreces IP. Es van començar a adoptar tecnologies com *Network Address Translation* (NAT) i *Classless Inter-Domain Routing* (CIDR).

2.2.2. Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR[17l]) és un mètode d'assignació d'adreces IP i d'encaminament d'IP. Va ser introduït l'any 1993 (amb l'especificació de IETF[17b] i[17c]) per substituir l'anterior arquitectura, *Classful Network*. L'objectiu era que disminuís el creixement de les taules d'encaminament[1][17m] del *routers* que trobem a Internet i per frenar l'esgotament de les adreces IP. A la taula 2.3 trobem un exemple de taula d'encaminament d'una xarxa domèstica.

[1] són taules de dades que emmagatzemen els *routers* o un ordinador de xarxa que llista les rutes cap a destinacions de xarxa, en alguns casos, les distàncies associades a aquestes rutes

Destinations	Gateway	Interface
0.0.0.0 (default)	192.168.1.1	eth0
192.168.1.0/24	link	eth0
255.255.255.255/32	link	eth0
127.0.0.0/8	127.0.0.1	lo0

Taula 2.3.: Exemple de taula d'encaminament d'un ordinador en una xarxa domèstica

Les adreces IP les podem disseccionar en dos grups: els bits més significatius (els de més a l'esquerra) són els bits que indiquen el prefix de xarxa mentre que els bits menys significatius són els d'identificador de host (identificador d'una interfície d'una màquina final).

CIDR també defineix *Variable-Length Subnet Masking* (VLSM), una tècnica per definir la longitud dels prefixes de xarxa d'una adreça IP. Es representa utilitzant CIDR *notation* i consisteix a escriure l'adreça IP acompanyada del nombre de bits que formen el prefix de xarxa, per exemple: `192.168.1.0/24` o bé `2001:db8::/32`.

Un conjunt d'adreces IP s'anomena **rang** d'IPs o **bloc** d'IPs. La mida d'un bloc s'indica acompanyant l'adreça IP amb una barra obliqua (`/`) i el nombre de bits del bloc. En el bloc `192.168.1.0/24` tenim 2^8 (2^{32-24}) adreces. Com més petit és el número que acompanya la barra obliqua més adreces hi ha al bloc.

Abans de la notació CIDR s'utilitzava la notació de les *Subnet Masks*. En IPv4, la *Subnet Mask* consisteix a definir una cadena formada per 32 bits que si realitzem l'operació lògica `AND` amb la IP ens permet obtenir el prefix de xarxa. Per expressar que tenim una subxarxa amb el prefix `192.168.1.x`, utilitzaríem la notació CIDR `192.168.1.0/24`, que és equivalent a escriure la IP `192.168.1.0` amb una màscara de subxarxa `255.255.255.0`. Per exemple, per conèixer si l'adreça IPv4 `192.168.1.33` pertany a una subxarxa `192.168.1.0/24` realitzem les següents operacions:

```
192.168.1.0 ⇒ 0b11000000 10101000 00000001 00000000
192.168.1.33 ⇒ 0b11000000 10101000 00000001 00100001
255.255.255.0 ⇒ 0b11111111 11111111 11111111 00000000
```

Tot seguit fem l'operació AND entre l'adreça IP i la màscara,

```
0b11000000 10101000 00000001 00100001
0b11111111 11111111 11111111 00000000
-----------------------------------
0b11000000 10101000 00000001 00000000
```

Convertim el resultat binari a decimal...

```
0b11000000 10101000 00000001 00000000 ⇒ 192.168.1.0
```

...i verifiquem que l'adreça `192.168.1.33` pertany a `192.168.1.0/24`.

L'any 1993 es va crear el grup *Address Lifetime Expectations* (ALE). Aquest grup va predir que l'esgotament de les adreces IPv4 seria un fet entre el 2005 i 2011. Al febrer del 2011 IANA (*Internet Assigned Numbers Authority*) va donar els cinc últims blocs `/8` als RIRs (*Regional Internet Registries*). El febrer de 2011 l'adopció de IPv6 a nivell mundial era només d'un 0.25% mentre que el febrer de 2017 l'adopció és de 17%.

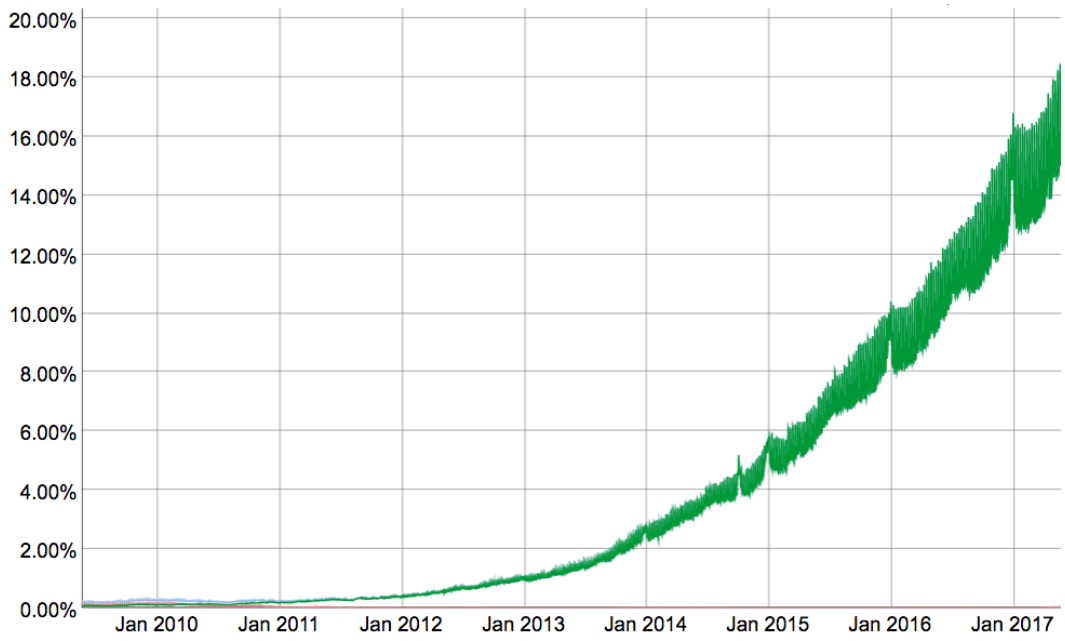

Figura 2.3.: Adopció de IPv6

2.2.3. NAT

Amb molta probabilitat les adreces IPv4 s'haurien esgotat abans si no fos per l'adopció de NAT. La proposta inicial de NAT va ser que les xarxes corporatives compartissin i reutilitzessin un rang d'IPs per tota la seva xarxa privada, fent una traducció de la IP privada a una IP públic a l'extrem de la xarxa. Aquesta proposta va ser atractiva per diverses raons. La principal raó era perquè ajudaria a frenar l'esgotament d'adreces IPv4. També permetia que les empreses guanyarien flexibilitat a l'hora d'administrar i planificar les seves xarxes, per exemple, en cas de canviar d'ISP (*Internet Service Provider*), canviaria la IP pública però no haurien de canviar tot l'adreçament privat. Per altra banda, també té els seus inconvenients. El principal problema és que NAT trenca el principi del model *end-to-end* d'Internet. La traducció d'adreces fa que la comunicació *end-to-end* no sigui possible, trencant el funcionament d'algunes aplicacions de xarxa i presentant problemes de rendiment.

2.3. IPv6

L'any 1998 l'IETF havia formalitzat IPv6. IPv6 (o simplement IP) utilitza adreces de 128 bits, proporcionant un espai de 2^{128} adreces:

$$340.282.366.920.938.463.463.374.607.431.768.211.456$$

Equival a prop de $6,7 \times 10^7$ adreces per cada mil·limetre quadrat de la Terra. IPv6 no és (directament) compatible amb IPv4 i això ha dificultat l'adopció de l'última versió del protocol IP, tot i que s'han desenvolupat de mecanismes de transició com NAT64, *6to4*, *6in4* i d'altres.

IPv6 no només es va dissenyar per oferir un espai d'adreces més extens que IPv4 sinó que satisfés els següents principis fonamentals de disseny:

- **Adreçament únic**: cada màquina, node o interfície d'una xarxa s'ha de poder adreçar únicament.
- **Gestionables**: les xarxes s'han de poder gestionar, la metodologia i tasques necessàries per construïr i mantenir la xarxa han de ser fàcils de reproduir i s'han de basar en protocols ben coneguts.
- **Escalables**: perquè una xarxa s'adapti a les necessitats d'empreses o organitzacions, ha de ser relativament senzill afegir i gestionar nous usuaris, aplicacions i serveis.
- **Rendible**: tots els dissenys de xarxa han de ser rendibles econòmicament. Tal com diu el proverbi: *ràpid, fiable, barat: escull-ne dos*. Sovint estem obligats a escollir *barat*, i després "ràpid" o "fiable".
- **Flexibilitat**: una xarxa s'hauria de poder configurar per satisfer tant una gran empresa com una petita organització. La dificultat en assolir aquesta flexibilitat amb els protocols de xarxa tradicionals ha estat un dels reptes pels enginyers de xarxes i ha portat a desenvolupar tecnologies com *Software-defined Networking* (SDN).
- **Elasticitat**: totes les xarxes han de tenir un cert grau de tolerància a fallades. En casos on la missió de la xarxa és simplement millorar la productivitat d'un negoci, un bon disseny de la xarxa és suficient. Per altra banda, les conseqüències d'un tall a la xarxa pot ser una perdua de beneficis i el disseny de la xarxa ha de contemplar aquest fet.
- **Simplicitat**: un disseny de xarxa ha de reflectir la bellesa de les matemàtiques, ciència i tecnologia. Aquesta bellesa premia l'elegància de la solució més simple per qualsevol problema complex.

3. Què és i com funciona guifi·net?

3.1. Introducció

guifi·net[17a] és una xarxa de telecomunicacions de comuns, oberta, lliure i neutral. Amb una forta presència a Catalunya, País Valencià i d'altres localitats a la península Ibèrica. La xarxa està subdividida en zones, per exemple, el Bages. Les zones estan formades per nodes i supernodes que tot ells formen un **sistema autònom**. Un node és un punt de connexió a la xarxa. Un supernode ofereix un punt de connexió a la xarxa a diversos nodes i estableix enllaços amb altres supernodes per formar la xarxa. Els nodes i supernodes acostumen a ser enllaços sense fils (amb equips que utilitzen l'espai radioelèctric), però també hi ha alguns trams de fibra òptica.

3.2. Sistemes Autònoms

Un sistema autònom (en anglès, *Autonomous System*, AS) és una col·lecció de xarxes IP que està sota el control d'un o més operadors de xarxa que actua com a una sola entitat administrativa i que presenta una política d'encaminament comuna a Internet. Originalment, el control de l'AS només podia recaure sobre una única entitat, normalment, el proveïdor d'Internet (ISP) o empreses molt grans. La nova definició *"Guidelines for creation, selection, and registration of an Autonomous System"* permet que múltiples organitzacions puguin utilitzar números d'AS privats cap a un ISP que connecta totes les organtizacions a Internet. La Fundació *guifi·net* és un proveïdor d'Internet i està registrat com a entitat administrativa `GUIFINET-AS`, amb número `AS49835`, i és responsable d'encaminar els prefixes IP de les taules 3.1 i 3.2.

5.10.200.0/24	185.41.99.0/24	109.69.8.0/24
5.10.201.0/24	185.41.98.0/24	109.69.9.0/24
5.10.202.0/24	185.41.97.0/24	109.69.10.0/24
5.10.203.0/24	185.41.96.0/24	109.69.11.0/24
5.10.204.0/24	185.32.19.0/24	109.69.12.0/24
5.10.205.0/24	185.32.18.0/24	109.69.13.0/24
5.10.206.0/24	185.32.17.0/24	109.69.14.0/24
5.10.207.0/24	185.32.16.0/24	109.69.15.0/24
		149.6.203.0/24

Taula 3.1.: Blocs d'IPv4 sota el control de `GUIFINET-AS`

2a01:57a0::/32
2a00:1508::/32

Taula 3.2.: Blocs d'IPv6 sota el control de `GUIFINET-AS`

Els sistemes autònoms utilitzen *Border Gateway Protocol* (BGP)[17n] per intercanviar les rutes (els prefixes que encaminen) i informació d'accessibilitat entre sistemes autònoms. Quan s'intercanvia informació dins d'un sistema autònom s'utilitza el protocol *internal BGP* (iBGP) o *Open Shortest Path First* (OSPF)[17o] mentre que entre sistemes autònoms d'Internet s'utilitza *external BGP* (eBGP).

Els *routers* es configuren perquè estableixin connexions TCP amb els sistemes autònoms veïns (també anomenats *peers*) per intercanviar informació. La versió més recent, BGP4 (publicada l'any 2006), conté correccions d'errors, suporta CIDR i utilitza agregació de rutes per fer disminuir la mida de les taules d'encaminament.

Dins de *guifi·net* trobem sistemes autònoms privats, que coincideixen en regions geogràfiques.

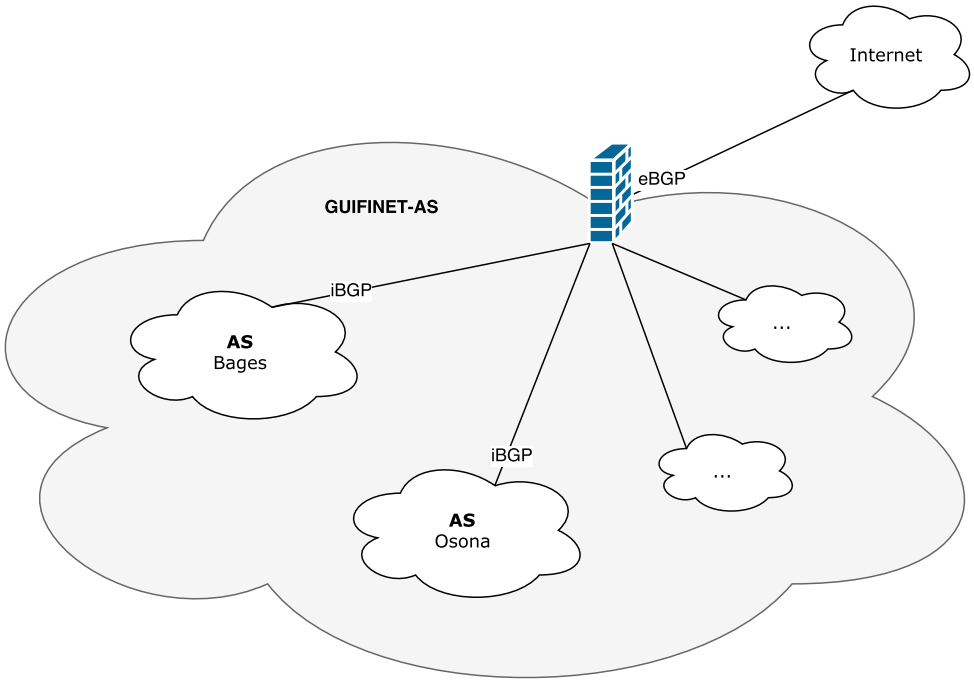

Figura 3.1.: `GUIFINET-AS` i els AS privats

Guifi·net és una xarxa de transport amb adreçament privat (`10.0.0.0/8`) i que no forma part d'Internet, tot i que hi ha punts de la xarxa que permeten sortir Internet. Els usuaris de la xarxa que volen una connexió a Internet utilitzen un protocol de túnel per connectar-se a la màquina que permet sortir a Internet (*gateway*). Aquesta màquina assigna una adreça IPv4 per cada túnel. S'utilitza una idea semblant a *Carrier Grade NAT*[17p], però en comptes de tenir una màquina que fa les traduccions d'IPs públiques a privades (que presenta desavantatges com ara trencar amb el principi d'*end-to-end*), hi ha una màquina que assigna una IP pública a un extrem del túnel del client (veure la figura 3.2).

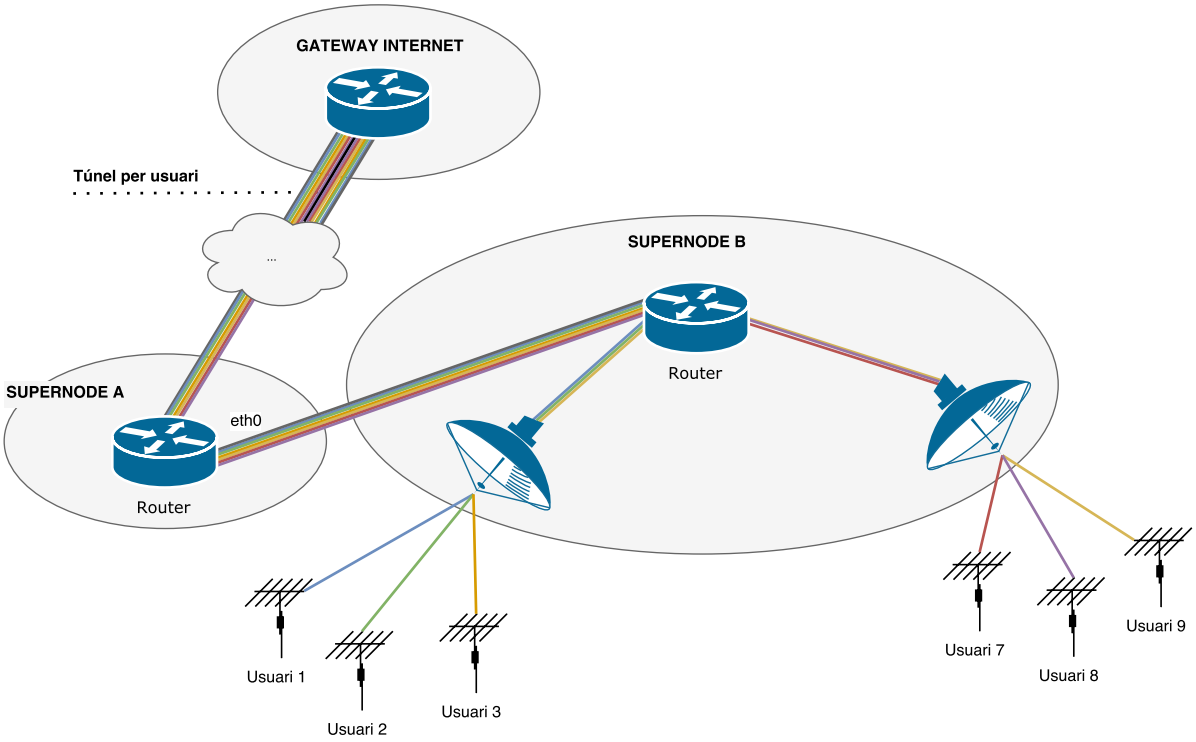

Figura 3.2.: Túnel sobre la xarxa *guifi·net* per oferir connectivitat a Internet als usuaris

3.3. Adreçament IPv4

Des de la fundació *guifi·net* s'ha assignat la subxarxa `10.228.0.0/17` per tot el Bages. Amb una sola subxarxa teòricament podríem configurar 2^{15} (32.768) màquines però segons la topologia de la xarxa hi ha la necessitat de definir una subxarxa per cada punt de cobertura. Cada punt de cobertura ofereix connectivitat a pocs usuaris, aproximadament uns 10 usuaris de mitjana, és per això que creant subxarxes de 4 bits ($2^4 - 1$ màquines) o 5 bits ($2^5 - 1$ màquines) és suficient. Com que *guifi·net* és una xarxa que creix amb la gent del carrer, no es pot predir quin serà el creixement de la xarxa. Es va optar per subdividir el `/27` en petites subxarxes i assignar-les a mesura que un supernode creixés. És per això que en un mateix supernode podem trobar subxarxes que no comparteixen el mateix prefix entre elles. D'aquesta manera es garanteix que no es desaprofitin subxarxes massa grans, però no permet fer agregació de rutes.

L'agregació de rutes[17e] en una xarxa IP consisteix en ajuntar diverses rutes per fer un únic anunci. Per altra banda, trobem la no-agregació de rutes, on cada ruta és un registre únic a la taula d'encaminament[1]. Un cas real d'agregació de rutes és el següent.

[1] A l'inici del 2017, els *routers* del sistema autònom del Bages tenen una taula d'encaminament d'uns 3000 registres.

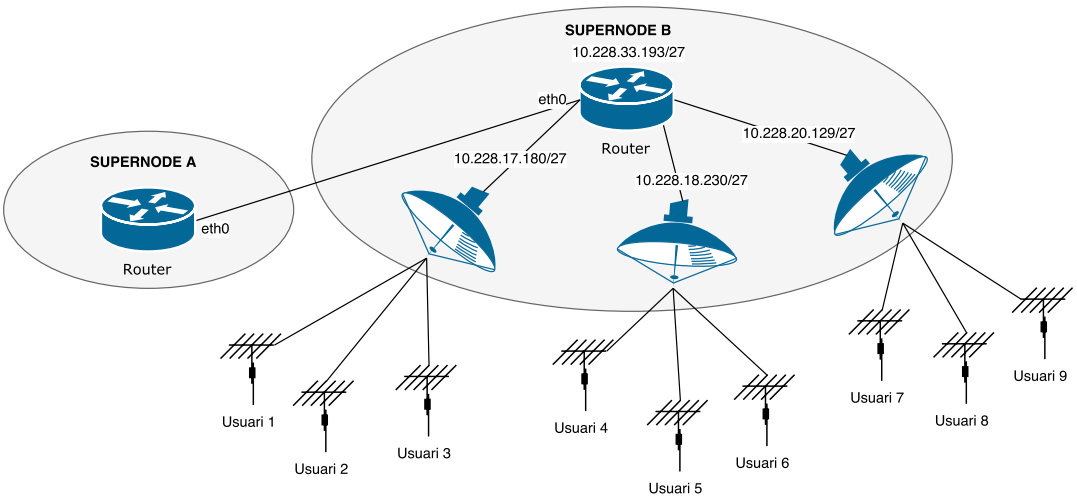

Figura 3.3.: Exemple de les subxarxes que trobem en un supernode

A l'exemple anterior trobem que el *router* del Supernode A i qualsevol *router* que es troba a la mateixa zona ha de tenir 4 rutes a la taula d'encaminament per poder arribar al Supernode B:

Rang	Interfície
10.228.33.193/27	eth0
10.228.17.180/27	eth0
10.228.18.230/27	eth0
10.228.20.129/27	eth0

Taula 3.3.: Rutes que han de tenir tots els router per arribar al Supernode B

En canvi, si es disposes d'un rang més ampli que un `/17` per a tot el Bages, per exemple un `/15`, el supernode B podria tenir una subxarxa `/24` que permetria crear $2^3 - 1$ (`/27 - /24` = 3) subxarxes de mida `/27` (que permetrien adreçar $2^5 - 1$ màquines cada una), aconseguint disminuir la taula d'encaminament en una sola línia sense limitar el creixement de la xarxa. En total podríem crear 2^9 (`/24 - /15` = 9) subxarxes de mida `/24` i tindríem un espai d'adreces molt més ampli que garantiria que la xarxa pogués créixer i tenint agregació de rutes. Tot seguit trobem una variació de la figura anterior suposant que tenim un `/24` per supernode.

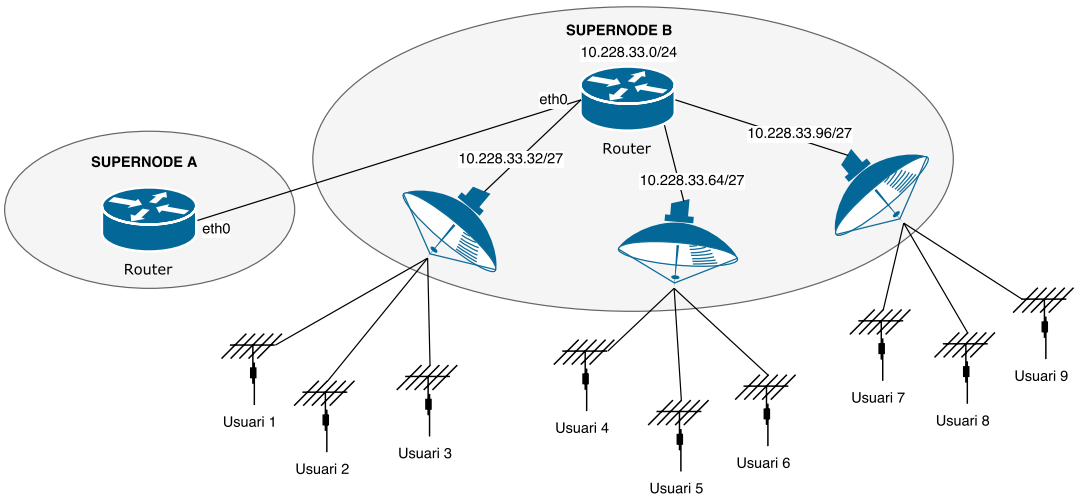

Figura 3.4.: Exemple de les subxarxes que trobem en un supernode

D'aquesta manera, la taula d'encaminament del *router* del supernode A i qualsevol *router* que es troba a la mateixa zona seria:

Rang	Interfície
10.228.33.0/24	eth0

Taula 3.4.: Rutes que han de tenir tots els router per arribar al Supernode B

Aquest canvi implicaria que tots els *routers* del Bages haurien de conèixer tots els supernodes. Actualment hi ha menys de 50 supernodes a la zona, de manera que la taula d'encaminament disminuiria de 3000 entrades a 50.

Part II.

Desenvolupament tècnic

4. Mètodes de planificació de l'adreçament IPv6

En aquest capítol explicarem les diferents tècniques que existeixen per planificar l'adreçament d'una xarxa. Planificar un adreçament significa, principalment, decidir quants bits reservarem a les subxarxes.

Com s'ha explicat a capítols anteriors, IPv6 (d'ara en endavant IP) utilitza adreces de 128 bits. Això significa que podem donar una adreça a aproximadament 2^{128}. Com que IP té un espai d'adreces d'aproximadament 7×10^{28} vegades més que IPv4, s'utilitzen uns criteris diferents a l'hora de planificar un adreçament per una xarxa IPv4. El més important és no deixar-se endur per la por de quedar-se sense adreces si es sobredimensionen massa les subxarxes.

La notació de les IP consisteix en dividir els 128 *bits* en grups de 16 *bits* (2 *bytes*) amb dos punts (`:`) com a separador. Quan una IP té zeros consecutius, es poden agrupar amb un parell de dos punts (`::`). Per exemple, la IP de *loopback* és `::1` (equival a la IPv4 `127.0.0.1`) i la podem escriure sense agrupar de la següent manera:

`0000:0000:0000:0000:0000:0000:0000:0001`

En canvi, la IP

`2001:0000:0000:0000:0000:0111:0000:0000`

la podem expressar com `2001::0111:0000:0000` o bé `2001:0000:0000:0000:0000:0111::` però mai podem agrupar zeros consecutius més d'un cop (`2001::111::`) perquè no seríem capaços de conèixer quants zeros hi havia a cada agrupació. Si que és vàlid obviar els zeros a l'esquerra `2001::0111:0000:0000` → `2001::111:0000:0000`.

Els mètodes d'assignació que disposem són[Cof15]:

- *Best-fit*
- *Sparse*
- *N+1*
- *Random*
- per lloc o funcionalitat

4.1. Assignació Best-Fit

És un mètode molt eficient des del punt de vista de no malgastar adreces. El mètode que s'aplica és el següent:

1) Es busca el bloc sense assignar més petit del total de blocs disponibles.

2) Si és possible, es parteix el bloc per la meitat successivament fins que encaixa amb les nostres necessitats.

3) S'assigna el bloc.

Per exemple, si tenim el bloc `2001:0db8:cafe::/48` i volem 375 subxarxes `/64` anirem subdividint el `/48` fins tenir el primer `/55` ($2^{64-55} \rightarrow 512$):

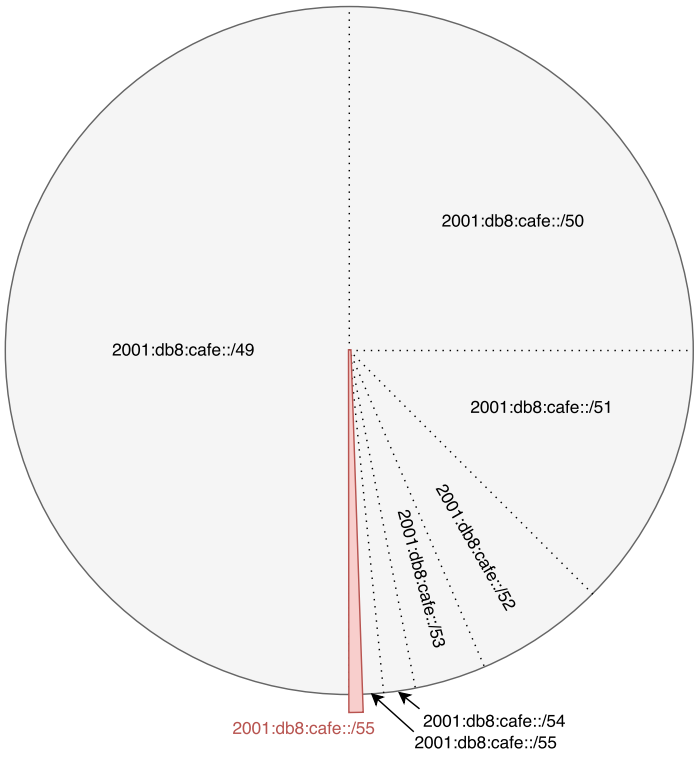

Figura 4.1.: Exemple d'assignació *Best-fit*

Val a dir que aquest sistema a l'hora de fer una planificació inicial és pobre, perquè l'adreçament resultant no seguirà cap criteri com agrupar els blocs per zona geogràfica i la mida de les subxarxes no serà múltiple de 4 (en parlarem més endavant).

4.2. Assignació Sparse

El mètode *Sparse* (en català, escàs) consisteix a deixar molt espai entre assignacions de blocs. Comparteix la idea de *best-fit*, partir el bloc per la meitat successivament, però agafem el bloc a la vora de cada nova meitat. Permet que futures subxarxes que pertanyen a una mateixa zona o que formen, conceptualment, part de la mateixa jerarquia, tinguin una subxarxa consecutiva.

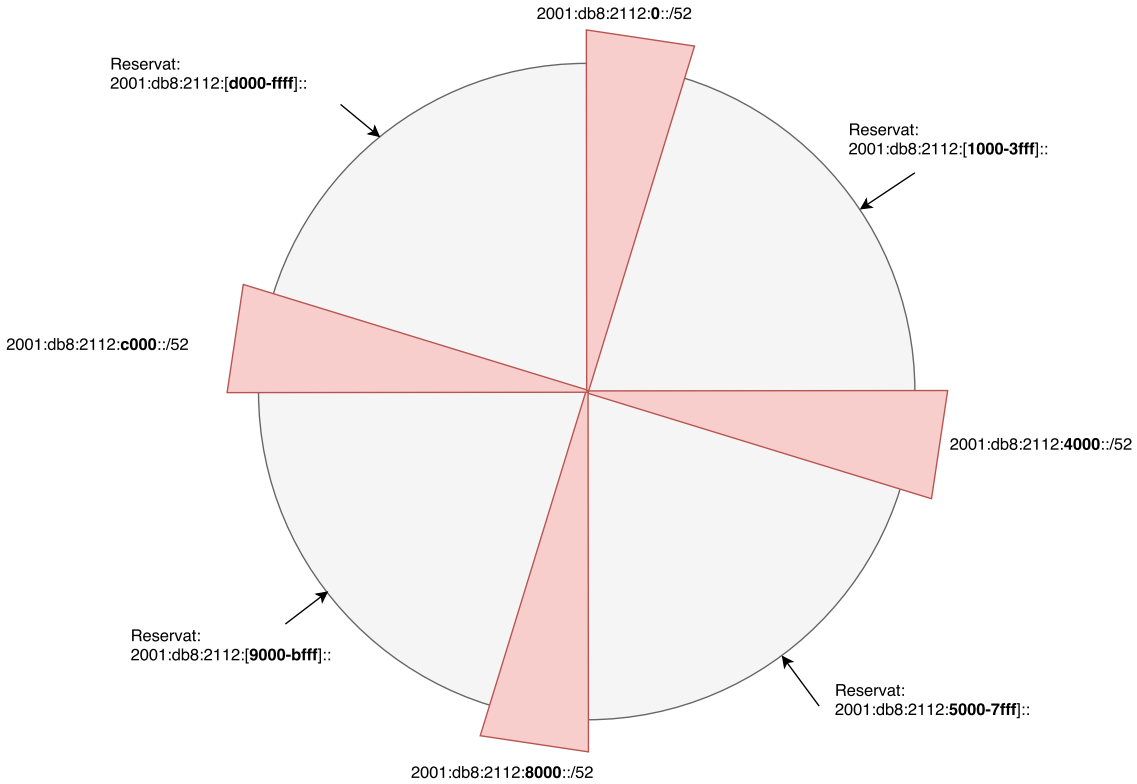

Figura 4.2.: Exemple d'assignació *Sparse*

4.3. Assignació N+1

L'assignació *N+1* també coneguda com assignació seqüencial consisteix a subdividir un bloc en petites subxarxes de la mateixa mida i es s'assignen per ordre numèric. De manera que no es deixa espai entre subxarxes per futures assignacions. Com a resultat, si la xarxa va creixent i a una zona s'esgoten totes les IP de la subxarxa, s'haurà d'assignar una altra subxarxa. Aquesta altra subxarxa s'hauria de poder agrupar amb l'actual (idealment haurien de compartir el prefix) però amb aquest mètode d'assignació no seria possible.

4.4. Assignació Random

L'assignació *Random* (en català, aleatòria) consisteix en subdividir el bloc en petites subxarxes, però en comptes d'assignar-los en ordre, com es fa a l'assignació *N+1*, es fa aleatòriament. Aquest mètode pot ser d'utilitat quan les assignacions són més dinàmiques, ja que es podria utilitzar com a una mínima capa de seguretat amagant la lògica d'assignació.

4.5. Assignació per lloc o funcionalitat

L'assignació per lloc normalment correspon a una localització geogràfica, on una organització té part de la seva xarxa: edificis, pisos, departaments, ... L'assignació per funcions pot ser qualsevol entitat lògica o administrativa, que normalment està relacionada amb usuaris (p.e.:

estudiants, convidats), *hosts* (p.e.: dispositius mòbils), servidors (p.e.: desenvolupament, financs)...

4.6. Aspectes a l'hora de planificar

4.6.1. Com agrupar els bits

Un dels aspectes a tenir en compte a l'hora de planificar una xarxa en IPv6 és que el núermo de *bits* que s'agafen per crear una subxarxa sigui un *nibble*. Un *byte* són 8 *bits* i un *nibble* són 4 *bits*. Quan representem un número en hexadecimal (el `255` → `0b11111111` → `0xFF`), cada *byte* està format per dos caràcters (p.e.: `FF`) i cada caràcter (`F`) és un *nibble*. Agrupar les subxarxes per caràcters ens facilita a identificar ràpidament quina part de l'adreça és el prefix de la xarxa i quin és el sufix de la subxarxa, sense haver de convertir la representació hexadecimal a binària per aplicar la màscara.

Per il·lustrar l'explicació anterior: si disposem del bloc `2001::/16` i necessitem 256 subxarxes, obtindríem 256 `/24`.

- `2001:0000::/24` → `0010 0000 0000 0001 :` **`0000 0000`** `0000 0000::`
- `2001:0100::/24` → `0010 0000 0000 0001 :` **`0000 0001`** `0000 0000::`
- `2001:0200::/24` → `0010 0000 0000 0001 :` **`0000 0010`** `0000 0000::`
- `...`
- `2001:A000::/24` → `0010 0000 0000 0001 :` **`1010 0000`** `0000 0000::`
- `2001:A100::/24` → `0010 0000 0000 0001 :` **`1010 0001`** `0000 0000::`
- `...`
- `2001:FD00::/24` → `0010 0000 0000 0001 :` **`1111 1101`** `0000 0000::`
- `2001:FE00::/24` → `0010 0000 0000 0001 :` **`1111 1110`** `0000 0000::`
- `2001:FF00::/24` → `0010 0000 0000 0001 :` **`1111 1111`** `0000 0000::`

En canvi, si necessitem 300 subxarxes i volem maximitzar el màxim de bits per subxarxa, hauríem de fer servir un `/25` i no pas un `/28`:

- `2001:0000::/25`
- `2001:0080::/25`
- `2001:0100::/25`
- `2001:0180::/25`
- `2001:0200::/25`
- `2001:0280::/25`

- ...

Com es pot observar, és molt més difícil de saber una adreça a quina subxarxa pertany. Si analitzem els blocs anteriors expressant les adreces IP en binari veurem que és més fàcil de llegir:

- `2001:0000::/25` → `0010 0000 0000 0001 : 0000 0000 0000 0000::`
- `2001:0080::/25` → `0010 0000 0000 0001 : 0000 0000 1000 0000::`
- `2001:0100::/25` → `0010 0000 0000 0001 : 0000 0001 0000 0000::`
- `2001:0180::/25` → `0010 0000 0000 0001 : 0000 0001 1000 0000::`
- `2001:0200::/25` → `0010 0000 0000 0001 : 0000 0010 0000 0000::`
- `2001:0280::/25` → `0010 0000 0000 0001 : 0000 0010 1000 0000::`
- ...

Conclusió, agrupar les subxarxes en *nibbles* per tenir un adreçament més clar, sempre que sigui possible.

4.6.2. Agregació de rutes

L'agregació de rutes i la mida de la taula d'encaminament ha estat un factor destacat a diversos capítols i seccions d'aquest treball. L'agregació de rutes és important per dos motius:

- **Tècnic**: una taula d'encaminament petita ocupa menys memòria RAM en els encaminadors i altres dispositius que treballin a la capa 3 model OSI. També és menys costosa la operació de buscar la ruta més restrictiva que compleixi amb l'adreça de destí d'un pàquet, per decidir cap a on s'ha de d'encaminar. Per tant, com menys rutes hi hagi, més ràpida és la decisió.
- **Gestió**: si les adreces IP s'assignen jeràrquicament per zones geogràfiques, és més fàcil memoritzar-les i de treballar-hi. Per exemple (veure la proposta d'adreçament de l'Associació d'Usuaris Guifibages 5.1), donat el rang `2a00:1508:5104::/48` sabem que pertany a un supernode de Manresa perquè la zona de Manresa té assignat `2a00:1508:510::/44`.

5. Proposta tècnica per implantar IPv6 a guifi·net

5.1. Proposta des de l'Associació d'Usuaris Guifibages

L'Associació d'Usuaris Guifibages (o simplement "Guifibages") va fer (entre el 2013 i 2014) un pla d'adreçament i una proposta de com hauria de ser la xarxa amb IPv6. Guifibages és un proveïdor d'Internet que només opera al Bages. La fundació *guifi·net* ha assignat el rang `2a00:1508:5100::/40` a l'associació. El pla d'adreçament consisteix en:

- Crear 16 zones que s'assignaran geogràficament: Manresa, Sallent, ...
- Cada zona (és un `/44`) pot tenir 16 supernodes (`/48`).
- A cada supernode es poden connectar un màxim de 256 clients.
- Cada client rebrà un `/56`.

5.1.1. Pla d'adreçament per zona

Els supernodes que pertanyen al municipi de Manresa tenen els rangs assignats:

- `2a00:1508:5100::/44`

Rang	Supernode
`2a00:1508:5100::/48`	MNBufalvent
`2a00:1508:5101::/48`	MNSantaCaterina
`2a00:1508:5102::/48`	MNPuigBerenguer
`2a00:1508:5103::/48`	MNAigüesDeManresa
`2a00:1508:5104::/48`	MNVergeAngusties
`2a00:1508:5105::/48`	MNPalauFiral
`2a00:1508:5106::/48`	MNPauMiralda
`2a00:1508:5107::/48`	MNPuigTerrà
`2a00:1508:5108::/48`	MNStIgnasi
`2a00:1508:5109::/48`	PADesguas
...	
`2a00:1508:510f::/48`	MNViladordisSalut

Taula 5.1.: Supernodes Manresa

Els supernodes que pertanyen al municipi de Sallent tenen els rangs assignats:

- 2a00:1508:51**a**0::/44
- 2a00:1508:51**c**0::/44

Rang	Supernode
2a00:1508:51**a0**::/48	SLLTorreTel
2a00:1508:51**a1**::/48	SLLCampanarST1
2a00:1508:51**a2**::/48	SLLCampanarST2
2a00:1508:51**a3**::/48	SLLAjuntament
2a00:1508:51**a4**::/48	SLLVerdura
...	
2a00:1508:51**c0**::/48	CABDepuradora
2a00:1508:51**c1**::/48	CABCampanar
2a00:1507:51**c2**::/48	CABHostalDelCamp
...	
2a00:1508:51**c8**::/48	CORCornet

Taula 5.2.: Supernodes Sallent

Els supernodes que pertanyen a altres poblacions tenen els rangs assignats:

- 2a00:1508:51**d**0::/44
- 2a00:1508:51**e**0::/44
- 2a00:1508:51**f**0::/44

Rang	Supernode
2a00:1508:51**d0**::/48	CTDCampanar
...	
2a00:1508:51**e0**::/48	SMdBCalFranch
...	
2a00:1508:51**f0**::/48	SFBDipositSanmarti

Taula 5.3.: Supernodes d'altres poblacions

5.1.2. Mètode utilitzat per fer l'adreçament

L'adreçament anterior es basa en el mètode d'assignació *sparse*, però en comptes de dividir els blocs per la meitat successivament i realitzar l'assignació de blocs uniformement, s'ha optat per predefinir la mida de la primera divisió en 4 bits (/44) i assignar-ho a una zona.

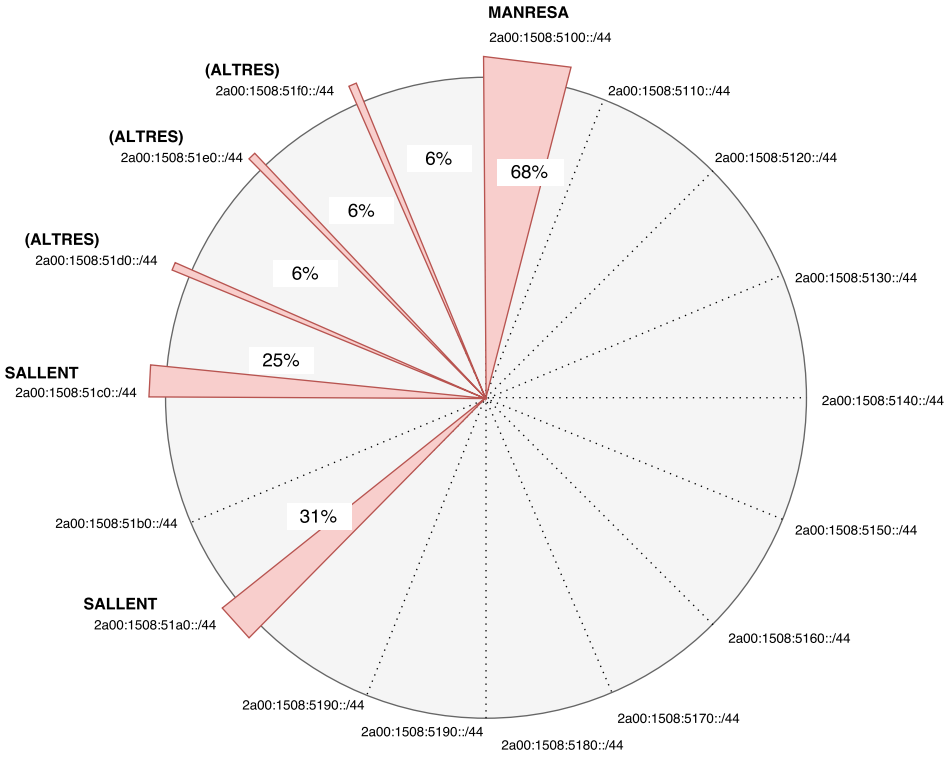

Figura 5.1.: Exemple d'assignació *Best-fit*

Si una zona es queda sense cap `/48`, com per exemple Manresa, podem assignar el següent bloc `2a00:1508:5110::/44`. Assignant aquest bloc consecutiu aconseguiríem que les taules d'encaminament en comptes de tenir aquestes dues rutes poguessin agregar en una sola ruta:

Rang	Interfície
`2a00:1508:5100::/44`	eth0
`2a00:1508:5110::/44`	eth0

Taula 5.4.: Taula sense agregació

Rang	Interfície
`2a00:1508:5100::/43`	eth0

Taula 5.5.: Taula amb agregació

Actualment només s'han assignat 6 dels 16 blocs de zona. Amb l'assignació que s'ha fet als supernodes existents, només s'està utilitzant un 8.875% de tots els `/48` disponibles, de manera que aquesta planificació garanteix el creixement de la xarxa sense comprometre aspectes com l'agregació.

$$\frac{68 + 31 + 25 + 3 * 6}{16} = 8.875\%$$

5.1.3. Connectivitat a Internet

La connectivitat a Internet és un punt pendent de resoldre per l'associació Guifibages i per la Fundació *guifi·net*. Hi ha diverses opinions: continuar utilitzant túnels perquè cada operador treballi amb el seu rang IP o bé trobar alguna altra solució que no necessiti afegir cap capa.

Actualment s'utilitzen túnels PPTP[17q], un mètode obsolet d'implementar VPNs (*Virtual Private Networks*), i OpenVPN[17r], un protocol obert, modern i segur, però que no deixa de tenir un cost en rendiment.

5.2. Proposta que es fa en aquest treball

La proposta que es fa en aquest treball es basa en la planificació que ha fet l'Associació d'Usuaris Guifibages i aprofundeix en detalls que per ara la fundació *guifi·net* encara no ha acabat d'especificar:

- Com haurien d'encaixar els diferents proveïdors d'Internet a la xarxa?
- Quin seria el millor mecanisme per oferir *guifi·net* com a xarxa de transport sense sobrecarregar amb túnels del tipus OpenVPN o PPTP?
- Com es podria comptabilitzar el trànsit segons operador?
- Cada operador tindria les seves IP? La xarxa tindria un adreçament públic sense connexió a Internet i per accedir-hi s'hauria de fer un túnel per obtenir una IP del proveïdor d'Internet?

5.2.1. Primeres idees...

Guifi·net com a xarxa de transport tindrà un adreçament IPv6 públic que permetrà adreçar les màquines de xarxa com *routers*, antenes i d'altres. Per altra banda, cada proveïdor d'Internet tindrà un rang IPv6 que l'utilitzarà per assignar als clients a qui ofereix el servei d'Internet. El proveïdor d'Internet haurà de complir l'adreçament de les màquines de xarxa perquè la xarxa sigui coherent i fàcil de mantenir.

5.2.2. Desenvolupament d'una possible solució tècnica

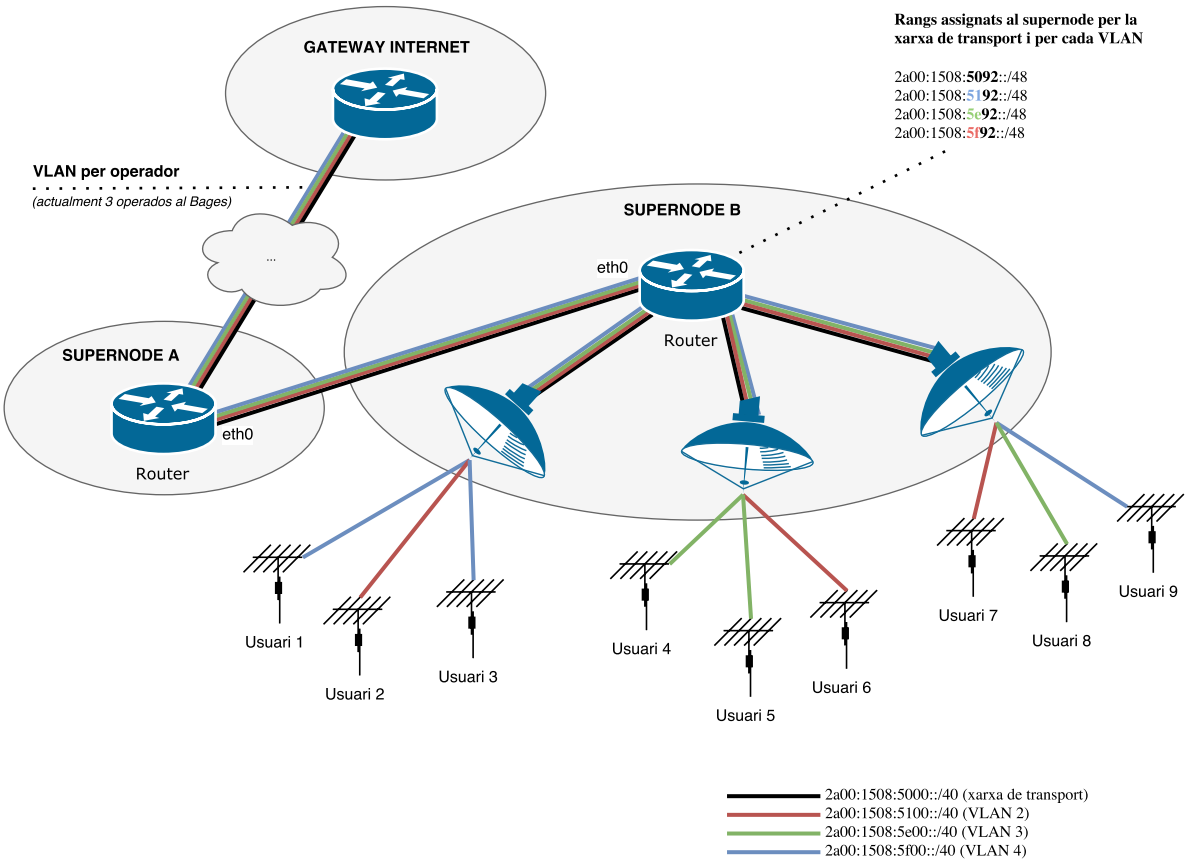

Figura 5.2.: Mapa de *guifi·net* conceptual amb la xarxa física i 3 xarxes lògiques (VLAN) amb l'adreçament IPv6 que correspondria a cada xarxa física i lògica

Per aconseguir que cada operador pugui treballar amb el seu rang IP, cada operador tindrà una *Virtual LAN* (VLAN)[17s] perquè pugui oferir serveis sobre la xarxa *guifi·net*. Una VLAN és un mètode per crear xarxes lògiques independents en una mateixa xarxa física. La VLAN permet utilitzar diferents subxarxes IP sobre la **capa d'enllaç** del model OSI.

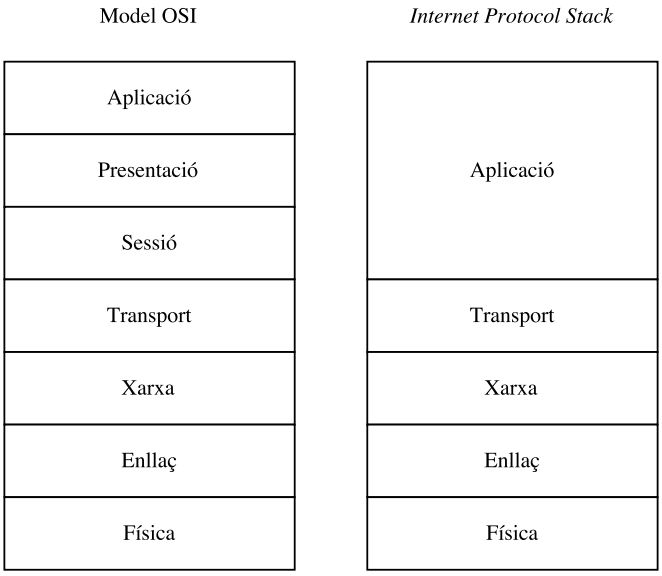

Figura 5.3.: Model OSI vs *Internet Protocol Stack*

La capa d'enllaç, *link layer* o L2 és la capa que transporta trames (*frames*) que contenen paquets de xarxa (IP). El protocol IEEE 802.1Q és una extensió del protocol IEEE 802.3 que afegeix una capçalera de 32 bits que inclou el camp *VLAN identifier* (VID) de 12 bits que permet crear 2^{12} subxarxes a una LAN.

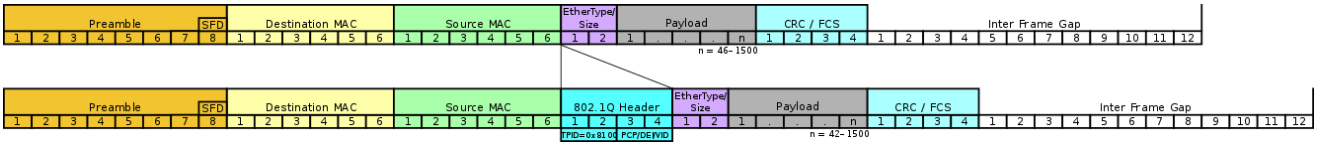

Figura 5.4.: format d'una trama de la capa d'enllaç

Amb aquesta solució, els encaminadors hauran de mantenir una instància de taula d'encaminament per cada VLAN. Des del punt de vista lògic, cada proveïdor d'Internet tindrà un encaminador per la seva xarxa i, per tant, cada VLAN no intercanviarà paquets amb cap altra VLAN dels altres proveïdors (no hi haurà *InterVLAN Routing*). La comunicació entre altres xarxes esfarà al *PE Router* (*Provider Edge Router*).

La utilització de VLAN a favor d'alternatives com MPLS[17t] (*Multiprotocol Label Switching*) conjuntament amb VRF[17u] (*VPN Routing and Forwarding*) ha estat degut a l'ampli suport que trobem als dispositius de xarxa, tant els més quotidians com els més professionals.

Actualment a la xarxa *guifi·net* s'utilitzen *routers* de la marca *Mikrotik* i antenes de la marca *Ubiquiti* i s'ha pogut verificar que suporten les VLAN.

La solució tècnica que acabem de descriure té un seguit d'avantatges i inconvenients:

- **Avantatges**:
  - Permet "multiplexar" la xarxa física en n xarxes virtuals, una per cada operador.
  - Cada xarxa és independent a la capa de xarxa, per tant, el comportament que obtenim és que cada operador podria configurar la xarxa com volgués, tot i que no

es recomanaria.

- **Inconvenients**:
  - Per cada interfície física, tenim n interfícies virtuals. Si en un encaminador volem fer un *bridge* d'unes quantes interfícies físiques haurem de configurar n *bridges* per cada interfície virtual.
  - Configurar la xarxa n vegades dificulta el manteniment.
  - Podria dificultar la implantació d'IPv6 la necessitat de mantenir en paral·lel la xarxa IPv4 en funcionament.
  - *A priori*, no existeix cap mètode per autentificar els usuaris. Un usuari malintencionat podria suplantar a un altre usuari de la xarxa.

5.2.3. Desenvolupament de la solució definitiva

Seguint amb la filosofia de l'anterior solució tècnica:

- Una xarxa IP per cada proveïdor d'Internet.
- Utilitzar una tecnologia que tingui el mínim d'impacte a la xarxa i sigui econòmic.

Amb aquesta proposta decidim "multiplexar" la xarxa però a la **capa de xarxa** (*network layer* o L3) en comptes de la capa d'enllaç. D'aquesta manera, tenim una sola xarxa física (i lògica), i utilitzem IP *aliasing* per assignar més d'una adreça IP o subxarxa a una mateixa interfície.

- **Avantatges**:
  - Permet transportar la informació de diverses subxarxes en una mateixa interfície física.
  - Només hem de configurar les interfícies un sol cop a la capa d'enllaç i no pas n.
  - Configurar una sola xarxa permet que el manteniment sigui més senzill.
  - Els canvis es fan a L3, de manera que facilitaria la posada en marxa mantenint en paral·lel IPv4.
- **Inconvenients**:
  - Cada operador no podrà gestionar les interfícies ni els *bridge* com ell vulgui perquè la interfície física és compartida entre tots.
  - *A priori*, no existeix cap mètode per autentificar els usuaris. Un usuari malintencionat podria suplantar a un altre usuari de la xarxa.

Un cop valorats els avantatges i inconvenients, decidim que aquesta és la millor solució per implantar IPv6 a *guifi·net*.

5.2.4. Connectivitat a Internet

Com que cada proveïdor d'Internet tindrà el seu adreçament públic a la xarxa, per oferir Internet els usuaris només hauràn de demanar una adreça IP al proveïdor i configurar el *router*. Si els proveïdors volen implementar un mètode que garanteixi que qualsevol usuari de la xarxa no pot suplantar l'adreça IP de qualsevol altre usuari, poden utilitzar qualsevol dels següents mètodes:

- Continuar utilitzant túnels OpenVPN.
- Implementar IPsec per autentificar els paquets IP i, de forma opcional, encriptar-los.

OpenVPN ofereix el mode de funcionament túnel. Permet encriptar i autentificar els paquets a la capa d'aplicació per oferir confidencialitat.

IPsec[17v] ofereix dos modes de funcionament:

- **Mode transport**: normalment només s'autentifica o encripta el *payload* (la informació del paquet). Però si s'utilitza l'*Authentication Header*, l'adreça IP s'autentifica.
- **Mode túnel**: el paquet sencer s'autentifica i s'encripta. Els paquets autentificats i encriptats s'encapsulen en un altre paquet IP. Aquest mode ofereix confidencialitat.

En aquest treball es recomana la utilització d'IPsec en mode transport amb *Authentication Header* perquè permet autentificar que l'adreça d'origen dels paquets IP provenen d'un usuari legítim. Es considera que és "responsabilitat de la xarxa" garantir que un usuari no pugui suplantar un altre, mentre que gaudir de confidencialitat és responsabilitat de l'usuari (utilitzant protocols segurs a la capa d'aplicació com HTTPS, SSH, ...).

6. Procediment per fer la transició a IPv6

El diumenge 3 de setembre de 1967, conegut com **Dagen H** (El dia H), a les 5:00 de la matinada es va canviar el sentit de la circulació del trànsit, passant de conduir per l'esquerra per fer-ho a la dreta. L'"H" prové de *höger*, "dreta" en suec.

Figura 6.1.: Carrer de Suècia el dia del canvi de direcció

Escollir un dia al calendari per deixar d'utilitzar IPv4 i migrar a IPv6 no és una opció viable. La migració s'ha de fer sense comprometre el funcionament de la xarxa ni forçar als usuaris de la xarxa a fer grans canvis (a curt termini) que podríen produir problemes.

Afortunadament, IPv6 pot conviure en paral·lel amb IPv4 (utilitzant el mecanisme de transició *dual stack*). Es pot configurar IPv6 progressivament sense necessitat que els usuaris facin una migració forçada. Els passos per fer la transició de la xarxa a IPv6 podrien ser els següents:

1) Fer una prova pilot sobre una zona de la xarxa, per exemple, la més propera al *firewall* (que dóna accés a Internet), per haver de configurar el mínim de dispositius de xarxa.

2) Configurar IPv6 a una zona de la xarxa

3) Configurar els nodes (els *routers* dels usuaris finals) perquè tinguin una connexió IPv6 amb el seu proveïdor, afavorint que totes les connexions a Internet que sigui possibles fer amb IPv6 no es facin amb IPv6.

4) Configurar els túnels que ofereixen una IPv4 als usuaris finals perquè viatgin a través de la xarxa IPv6.

5) Deixar la xarxa IPv4 en funcionament per mantenir compatibilitat, però adoptar la xarxa IPv6 com a xarxa per defecte.

6) Quan IPv6 tingui un percentatge important d'adopció a escala global i IPv4 es percebi com una tecnologia obsoleta llesta per abandonar, es podrà començar a abandonar IPv4 a la xarxa *guifi·net* però mantenint una IPv4 pública per donar compatibilitat.

7. Prova de concepte

Aquest capítol està dedicat a verificar que la proposta escollida és viable tècnicament. El procés per verificar el funcionament de la proposta tècnica consta de les següents parts:

1) Preparar un entorn de proves similar a *guifi·net*.

2) Configurar les antenes i els *router* amb adreçament IPv4.

3) Configurar el protocol OSPF per intercanviar les rutes.

4) Configurar les antenes i els *router* amb adreçament IPv6.

5) Configurar el protocol OSPFv3 per intercanviar les rutes IPv6.

6) Configurar dues màquines finals per establir connexions entre si.

7.1. Preparació d'un entorn de proves

Primer de tot hem muntat una petita xarxa de proves amb una topologia semblant a la que trobem a *guifi·net*: dos supernodes que entre ells es comuniquen per ràdio i cada supernode té un *bridge* (equivalent a una antena de cobertura) on es connecten els usuaris. Cada supernode té un encaminador *Mikrotik* (`RB951Ui`) i una antena amb una ràdio WiFi *Ubiquiti* (`PowerBeam AC`).

Com que per configurar les antenes cal una xarxa IPv4, la primera implantació de la solució es farà en IPv4, tal com es mostra a la següent figura:

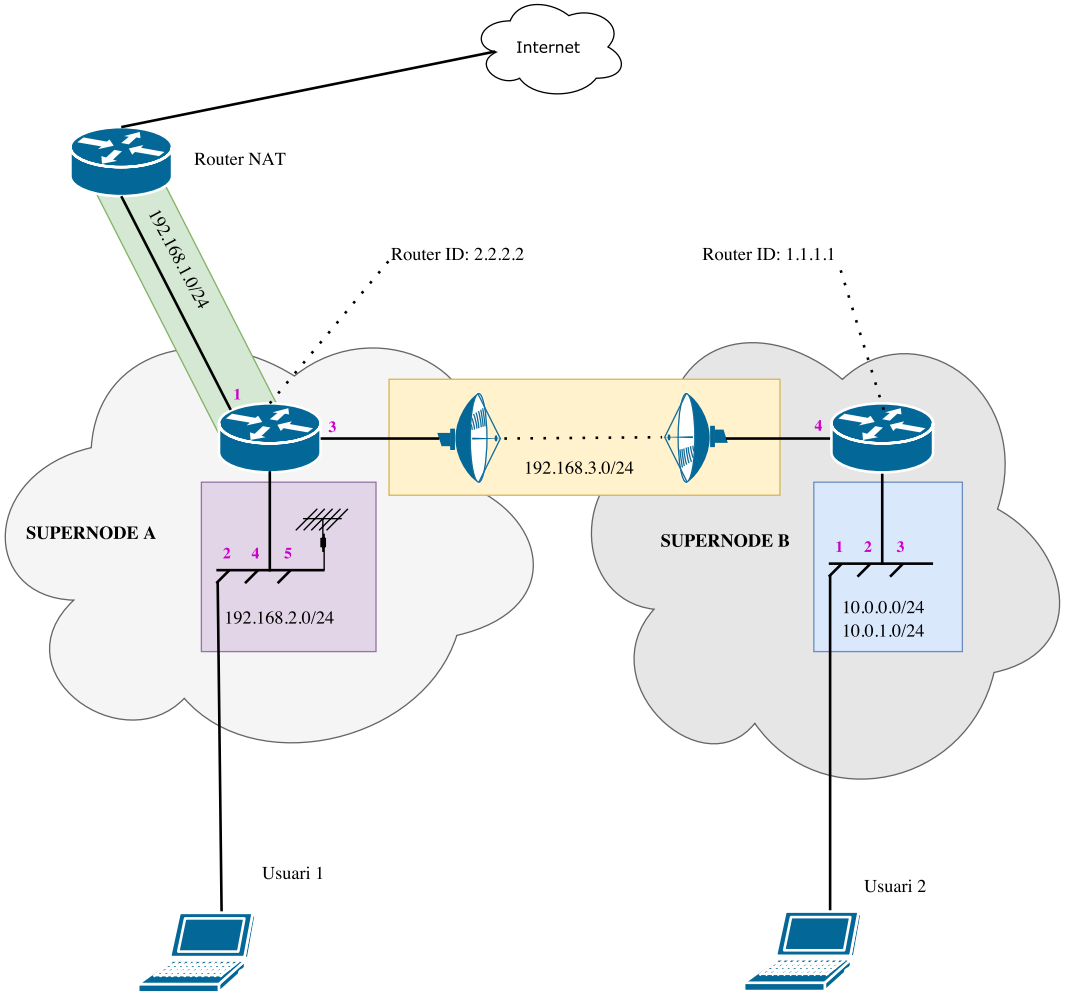

Figura 7.1.: Xarxa de proves per verificar la viabilitat tècnica

7.1.1. Enllaç a través de ràdio

Primer de tot hem configurat les antenes per crear un enllaç ràdio. Per fer-ho s'han deixat les antenes amb la configuració de fàbrica, hem connectat un ordinador a l'antena per *ethernet* i ens hem connectat des del navegador de l'ordinador a la pàgina de configuració. La primera antena la configurem amb el mode sense fils `Access Point` i la segona en mode sense fils `Station`. La interfície *ethernet* i la interfície *wireless* de l'antena estarà configurat com a *bridge*, de manera que aquest enllaç de xarxa sigui a través de ràdio és totalment transparent per la resta de dispositius de xarxa. Cal que l'opció WDS (*Wireless Distribution System*) estigui activa perquè ofereix el mode *transparent bridging*. Assignem una adreça IPv4, la màscara de xarxa i el prefix de xarxa. En aquest cas configurem la xarxa `192.168.3.0/24` perquè no entri en conflicte amb altres xarxes que hi ha actualment a l'entorn de proves. Assignem l'adreça `192.168.3.80/24` i `192.168.3.90/24` a cada antena. Les adreces `192.168.3.1/24` i `192.168.3.2/24` les assignarem a les interfícies *ethernet* dels dos *routers* al següent pas.

El resum de la configuració és la següent:

Antena supernode B

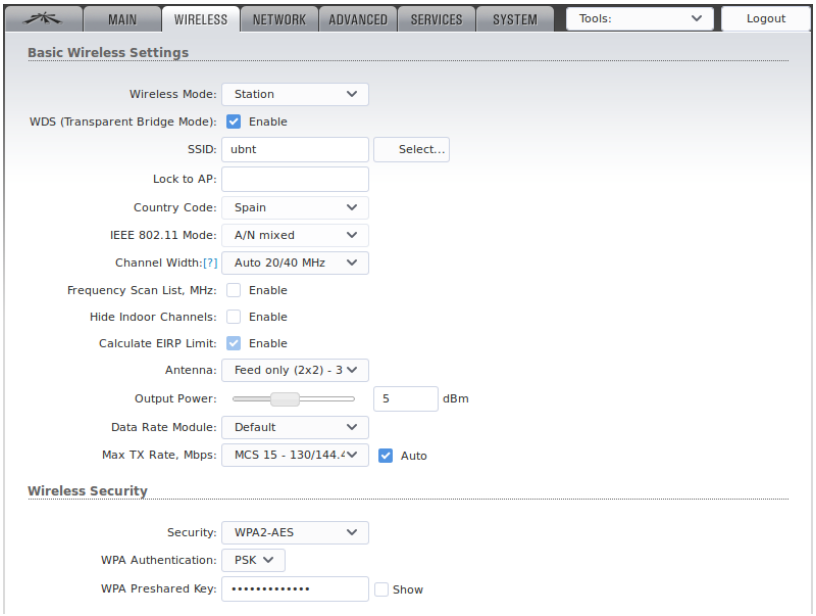

Figura 7.2.: Pestanya de la configuració *Wireless*

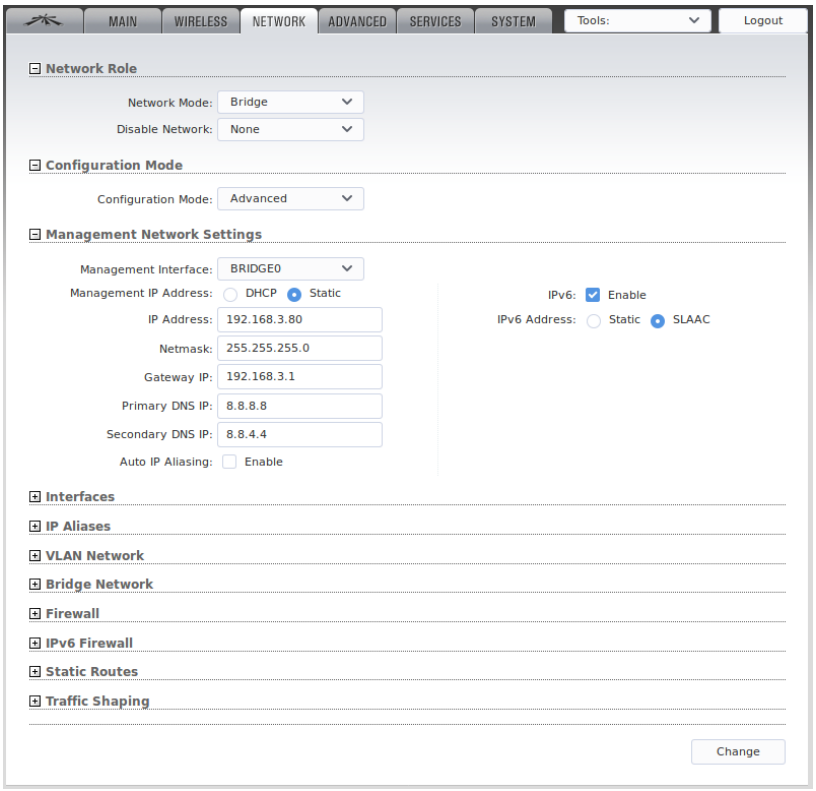

Figura 7.3.: Pestanya de la configuració *Network*

Antena supernode A

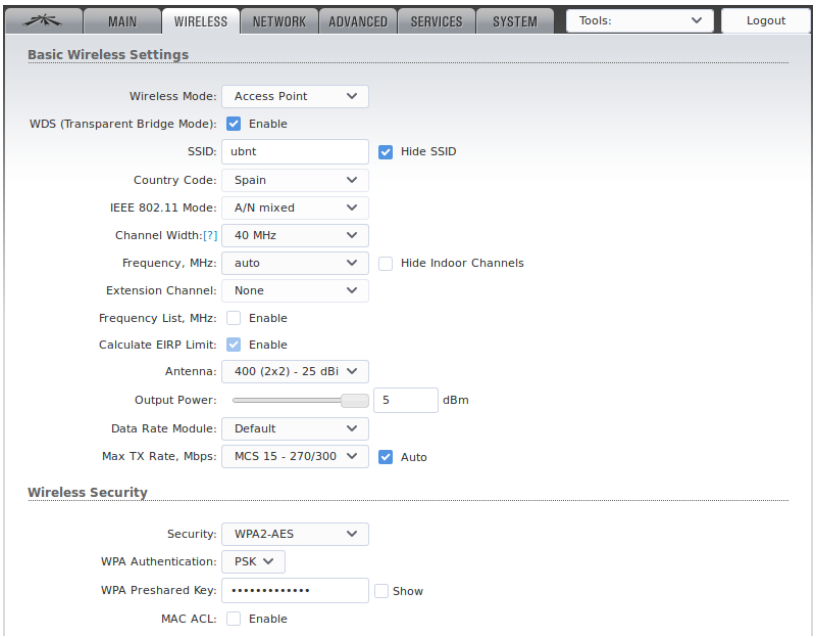

Figura 7.4.: Pestanya de la configuració *Wireless*

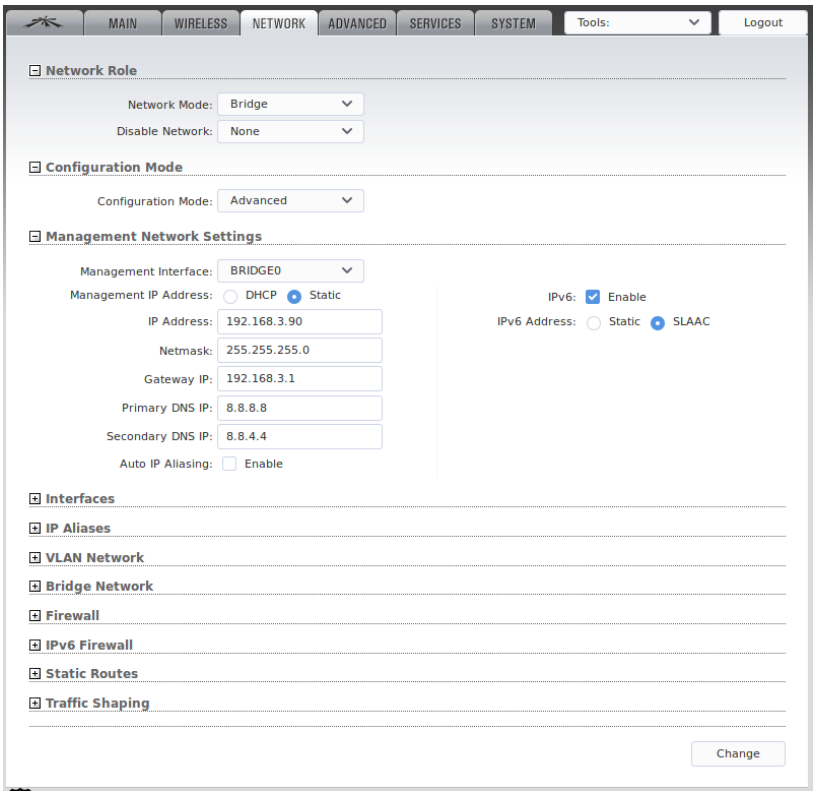

Figura 7.5.: Pestanya de la configuració *Network*

7.1.2. Configuració dels encaminadors

Per posar en marxa la xarxa de proves s'ha utilitzat part de la xarxa domèstica que actualment hi ha casa, ja que es necessiten dos *routers* per realitzar la prova i només s'ha aconseguit a través de l'Associació Guifibages un encaminador més.

La xarxa domèstica abans de començar les proves és la següent:

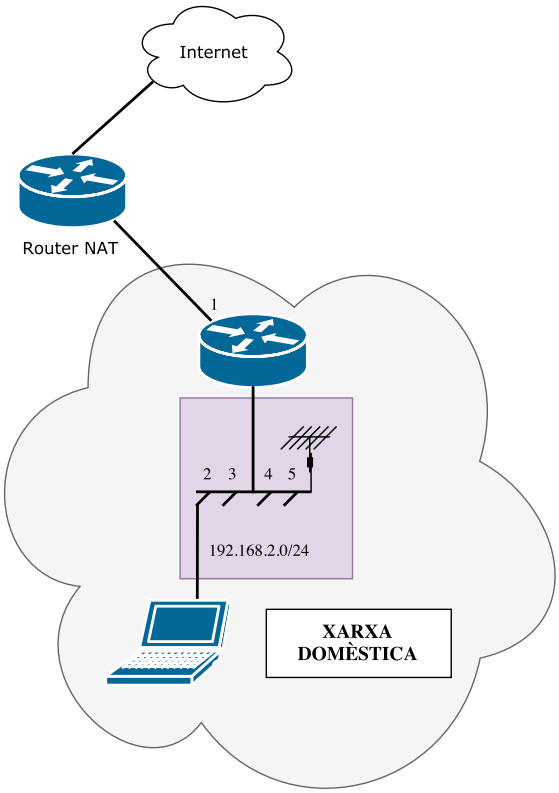

Figura 7.6.: Xarxa domèstica que s'aprofitarà per muntar la xarxa de proves

Configuració del supernode B

El primer pas ha estat deixar l'encaminador del supernode B (situat a la dreta a l'esquema anterior) amb la configuració de fàbrica. Tot seguit s'ha configurat la subxarxa `10.0.0.0/24` del *router* utilitzant les opcions de *Quick Setup* (veure captura).

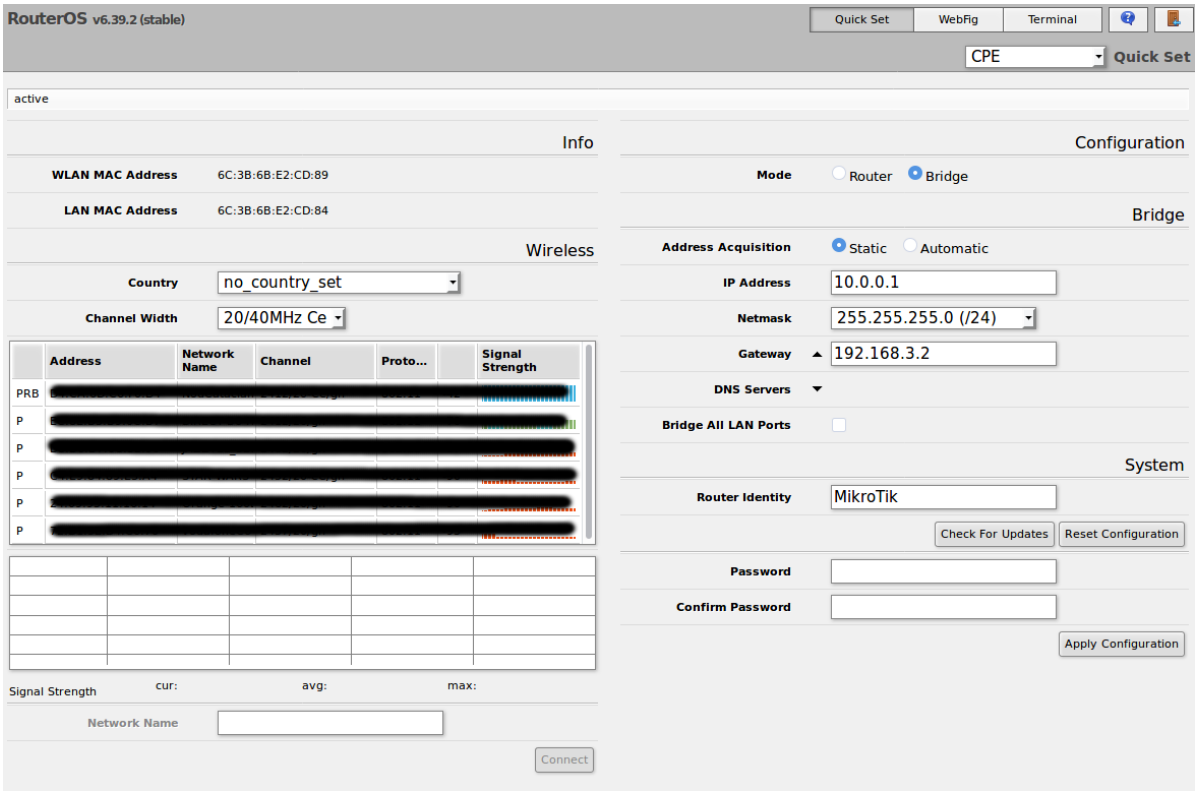

Figura 7.7.: Captura de *Quick Setup*

Tot seguit "s'ha desconnectat" la interfície *ether4* del *switch*, per poder configurar la xarxa `192.168.3.1/24` a la interfície. Les taules d'encaminament generades pel *router* són les esperades:

		Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
D	AS	0.0.0.0/0	192.168.3.2 reachable ether4	1		
	DAC	10.0.0.0/24	bridge reachable	0		10.0.0.1
	DAC	10.0.1.0/24	bridge reachable	0		10.0.1.1
	DAC	192.168.3.0/24	ether4 reachable	0		192.168.3.1

Figura 7.8.: Taula d'encaminament del *router* del supernode B

En aquest punt, des de l'ordinador connectat al *router* fem un *ping* a `192.168.3.1`, `192.168.3.80` i `192.168.3.90` i es verifica que l'enllaç ràdio funciona correctament.

Configuració del supernode A

Continuem, amb la configuració del *router* del supernode A perquè la interfície *ether3* (la interfície que queda lliure) no formi part del *switch*. Seguidament es configura que la interfície *ether3* amb la subxarxa `192.168.3.2/24` i es connecta l'antena. Repetim els pasos anteriors per verificar el correcte funcionament. Les taules d'encaminament generades pel *router* són les esperades:

		Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
-	DAS	0.0.0.0/0	192.168.1.1 reachable bridge-1/24	0			
-	DAC	192.168.1.0/24	bridge-1/24 reachable	0		192.168.1.96	
-	DAC	192.168.2.0/24	bridge reachable	0		192.168.2.1	
-	DAC	192.168.3.0/24	ether3 reachable	0		192.168.3.2	

Figura 7.9.: Taula d'encaminament del *router* del supernode A

Tot seguit es fa un *ping* a `192.168.3.1`, `192.168.3.80` i `192.168.3.90` i verifiquem que l'enllaç ràdio funciona correctament des de l'altre extrem.

7.1.3. Configuració del protocol OSPF

Com es pot veure a les taules d'encaminament dels *routers* del supernode A (figura 7.9) i del supernode B (figura 7.8), cada *router* només coneix les seves rutes però no les dels seus veïns. Com que coneixem físicament com estan connectats els *routers* podríem afegir les rutes manualment a la taula d'encaminament, però podem utilitzar el protocol OSPFv2 perquè faci aquesta feina per nosaltres automàticament.

S'ha de configurar cada encaminador perquè cadascun anunciï les xarxes que formen part de la seva subxarxa. L'encaminador del supernode B ha d'anunciar les següents subxarxes als seus veïns:

- `10.0.0.0/24`
- `10.0.1.0/24`
- `192.168.3.0/24`

L'encaminador del supernode A ha d'anunciar les subxarxes:

- `192.168.1.0/24`
- `192.168.2.0/24`
- `192.168.3.0/24`

Passats uns 10s, revisem les taules d'encaminament dels dos *routers*:

		Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
- D	AS	0.0.0.0/0	192.168.3.2 reachable ether4	1			
-	DAC	10.0.0.0/24	bridge reachable	0		10.0.0.1	
-	DAC	10.0.1.0/24	bridge reachable	0		10.0.1.1	
-	DAo	192.168.1.0/24	192.168.3.2 reachable ether4	110			
-	DAo	192.168.2.0/24	192.168.3.2 reachable ether4	110			
-	DAC	192.168.3.0/24	ether4 reachable	0		192.168.3.1	

Figura 7.10.: Taula d'encaminament del *router* del supernode B

		Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
-	DAS	0.0.0.0/0	192.168.1.1 reachable bridge-1/24	0			
-	DAo	10.0.0.0/24	192.168.3.1 reachable ether3	110			
-	DAo	10.0.1.0/24	192.168.3.1 reachable ether3	110			
-	DAC	192.168.1.0/24	bridge-1/24 reachable	0		192.168.1.96	
-	DAC	192.168.2.0/24	bridge reachable	0		192.168.2.1	
-	DAC	192.168.3.0/24	ether3 reachable	0		192.168.3.2	

Figura 7.11.: Taula d'encaminament del *router* del supernode A

La llegenda dels *flags* que trobem al costat de cada ruta és:

- **D** *dynamic*
- **A** *active*
- **C** *connected*
- **S** *static*
- **o** *OSPF*

7.2. Configuració amb adreces IPv6

7.2.1. Configuració de les adreces IP de les interfícies dels encaminadors

Per configurar els encaminadors *Mikrotik* s'ha hagut d'instal·lar el paquet IPv6. Permet configurar les adreces IPv6 per cada interfície, DHCP, *Firewall*, *Neighbor Discovery*, *Pool* d'adreces i veure les rutes.

Les antenes Ubiquiti inclouen per defecte IPv6 desactivat i per activar-ho només cal marcar una casella i escollir si volen configurar una adreça IP estàtica o bé utilitzar SLAAC.

S'ha escollit *Stateless Address Autoconfiguration*[17d] (SLAAC) perquè utilitza EUI-64 (*Extended Unique Identifier*) per autoassignar-se una IPv6 a partir del prefix de xarxa i l'adreça MAC. Només ens cal definir la subxarxa (una subxarxa privada `fe80::/64`) de l'enllaç ràdio (en el *Mikrotik*) i automàticament les antenes s'assignen una IP.

Les interfícies del supernode B rebran els següents rangs:

- *ether4*: (SLAAC) `fe80::/64`
- *bridge*: `2001::1/64` i `2004::1/64`

Les interfícies del supernode A rebran els següents rangs:

- *ether3*: (SLAAC) `fe80::/64`
- *bridge*: `2002::1/64`

7.2.2. Configuració del protocol OSPFv3

El protocol OSPFv2 es configura indicant la llista de subxarxes que s'han d'anunciar. En canvi, el protocol OSPFv3 configurem quins son els enllaços (interfícies) que s'han d'anunciar.

L'encaminador del supernode B ha d'anunciar les següents interfícies als seus veïns:

- *ether4*
- *bridge*

L'encaminador del supernode A ha d'anunciar les interfícies:

- *ether3*
- *bridge*

Passats uns 10s, revisem les taules d'encaminament dels dos *routers*:

		Dst. Address	Gateway	Distance
-	DAo	2002::/64	fe80::d6ca:6dff:fec6:f0d1%ether4 reachable	110
-	DAC	2001::/64	bridge reachable	0
-	DAC	2004::/64	bridge reachable	0

Figura 7.12.: Taula d'encaminament del *router* del supernode B

		Dst. Address	Gateway	Distance
-	DAo	2004::/64	fe80::6e3b:6bff:fee2:cd87%ether3 reachable	110
-	DAC	2002::/64	bridge reachable	0
-	DAo	2001::/64	fe80::6e3b:6bff:fee2:cd87%ether3 reachable	110

Figura 7.13.: Taula d'encaminament del *router* del supernode A

7.2.3. Configuració de la Raspberry Pi amb diferents alias IPv4 i IPv6

S'ha utilitzat una *Raspberry Pi* com a ordinador connectat al supernode B.

```
auto lo
iface lo inet loopback

auto eth0:1
iface eth0:1 inet6 static
    address 2001::314
    network 64
    gateway 2001::1

auto eth0:2
iface eth0:2 inet6 static
    address 2001:1::314
    network 64
    gateway 2001:1::1
```

```
auto eth0:3
iface eth0:3 inet static
    address 10.0.0.10
    netmask 255.255.255.0
    gateway 10.0.0.1
    dns-nameservers 8.8.8.8 8.8.4.4

auto eth0:4
iface eth0:4 inet static
    address 10.0.1.10
    netmask 255.255.255.0
    gateway 10.0.1.1
```

Un cop configurada la *Raspberry Pi*, des de l'ordinador del supernode A (que s'ha autoassignat una IP utilitzant SLAAC, `2002::fabc:12ff:fe92:96f1`) s'ha fet *ping* (`ping6 2001::314`) per verificar que l'encaminament funciona correctament i finalment i s'ha establert comunicació per SSH (`ssh pi@2001::314`) per verificar el funcionament de IPv6 a la capa d'aplicació.

8. Conclusions

Aquest treball final de grau l'he enllestit amb una satisfacció personal important que prové d'haver gaudit fent el treball i del coneixement que he obtingut. El projecte m'ha enriquit professionalment; estudiant com és la xarxa *guifi·net*, buscant quins solucions oferirien una millora i, finalment, realitzar una proposta que millori el model actual.

Des del punt de vista de les tecnologies utilitzades, aquest treballar ha sigut el primer contacte seriós que he tingut amb IPv6 i amb dispositius de xarxa professionals (*routers* i antenes). També m'ha permès conèixer i aprendre dels professionals que formen part de l'Associació Guifibages i que voluntàriament fan créixer la xarxa *guifi·net*.

Bibliografia

[17a] *Guifi·net. Què és Guifi·net?* Mar. de 2017. URL: https://guifi.net/ca/que_es.

[17b] *IETF. RFC 1518*. Abr. de 2017. URL: https://tools.ietf.org/html/rfc1518.

[17c] *IETF. RFC 1519*. Abr. de 2017. URL: https://tools.ietf.org/html/rfc1519.

[17d] *IETF. RFC 4862*. Jul. de 2017. URL: https://tools.ietf.org/search/rfc4862.

[17e] *Juniper. Understanding Route Aggregation*. Abr. de 2017. URL: https://www.juniper.net/documentation/en_US/junos/topics/concept/policy-aggregate-routes.html.

[17f] *RIPE. Understanding IP Addressing and CIDR Charts*. Jun. de 2017. URL: https://www.ripe.net/about-us/press-centre/understanding-ip-addressing.

[17g] *Viquipèdia. Internet Protocol (IP)*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/Internet_Protocol.

[17h] *Viquipèdia. Internet Protocol version 4*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/IPv4.

[17i] *Viquipèdia. Internet Protocol version 6*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/IPv6.

[17j] *Viquipèdia. Classful Network*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/Classful_network.

[17k] *Viquipèdia. IPv4 Address Exhaustion*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/IPv4_address_exhaustion.

[17l] *Viquipèdia. Classless Inter-Domain Routing*. Mar. de 2017. URL: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing.

[17m] *Viquipèdia. Routing table*. Abr. de 2017. URL: https://en.wikipedia.org/wiki/Routing_table.

[17n] *Viquipèdia. BGP*. Abr. de 2017. URL: https://en.wikipedia.org/wiki/Border_Gateway_Protocol.

[17o] *Viquipèdia. OSPF*. Abr. de 2017. URL: https://en.wikipedia.org/wiki/Open_Shortest_Path_First.

[17p] *Viquipèdia. Carrier-grade NAT*. Abr. de 2017. URL: https://en.wikipedia.org/wiki/Carrier-grade_NAT.

[17q] *Viquipèdia. Point-to-Point Tunneling Protocol*. Mai. de 2017. URL: https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol.

[17r] *Viquipèdia. OpenVPN*. Mai. de 2017. URL: https://en.wikipedia.org/wiki/OpenVPN.

[17s] *Viquipèdia. VLAN*. Abr. de 2017. URL: https://en.wikipedia.org/wiki/Virtual_LAN.

[17t] *Viquipèdia. MPLS*. Mai. de 2017. URL: https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching.

[17u] *Viquipèdia. Virtual routing and forwarding*. Jun. de 2017. URL: https://en.wikipedia.org/wiki/Virtual_routing_and_forwarding.

[17v] *Viquipèdia. IPsec*. Jun. de 2017. URL: https://en.wikipedia.org/wiki/IPsec.

[Cof15] Tom Coffeen. *IPv6 Address Planning*. First release. CA, USA: O'Reilly, 2015.