Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels
UNIVERSITAT POLITÈCNICA DE CATALUNYA

# PROJECTE DE FI DE CARRERA

**TÍTOL DEL PFC: Estudi d'implantació de la IPv6 al CTTC**

**TITULACIÓ: Enginyeria de Telecomunicació (segon cicle)**

**AUTOR: Jordi Escoda Ramon**

**DIRECTOR: Roc Meseguer Pallarès**

**SUPERVISOR: David Company i Estall**

**DATA: 20 de febrer de 2017**

**Títol:** Estudi d'implantació de la IPv6 al CTTC

**Autor:** Jordi Escoda Ramon

**Director:** Roc Meseguer Pallarès

**Data:** 20 de febrer de 2017

**Resum**

Durant els últims anys, el creixement del nombre de dispositius amb necessitats de connexió a Internet ha crescut de forma exponencial. Aquest fet es preveu que segueixi sent així en un futur. Quan es va crear el protocol IPv4, no s'imaginaven la seva evolució. Amb el pas dels anys han anat observant deficiències, entre elles l'escalabilitat i el creixement no sostenible de les taules d'encaminament dels *routers*. Aquesta situació, fa que es definís el protocol IPv6 a finals dels anys 90 per resoldre aquests problemes i afegir noves funcionalitats. En l'actualitat, l'esgotament de l'assignació d'adreces IPv4, la demanda de connectivitat creixent dels dispositius i les notícies que arriben de la necessitat de suportar IPv6, provoquen que el Centre Tecnològic de Telecomunicacions de Catalunya (CTTC) hagi proposat afegir a la seva xarxa el nou protocol. Per altre banda, des de RedIris i el CSUC s'està animant i donant suport a les institucions afiliades com el CTTC perquè implementin IPv6 a la seva xarxa de comunicacions.

El projecte es realitza dins de les activitats del Centre de Serveis Informàtics (CSI), que és el departament encarregat de les TIC al CTTC.

La finalitat d'aquest projecte és analitzar i conèixer les característiques principals del protocol IPv6 i veure quines són les diferències amb IPv4. També es pretén implementar de forma nativa el protocol IPv6 a la xarxa del CTTC. Per altre banda, sorgeix la necessitat de donar suport IPv6 en alguns dels serveis bàsics com el DNS i el web. Per últim, es vol comparar el rendiment dels dos protocols a la xarxa del CTTC.

Per avaluar la implementació, s'analitzen en detall els equips i la topologia de la xarxa per tal de proposar una solució que suporti IPv6. Això provoca la substitució d'alguns elements de la infraestructura de xarxa del CTTC. Per integrar IPv6 de forma progressiva, s'escull una estratègia perquè convisquin els protocols IPv4 i IPv6, anomenada doble pila. Amb l'adaptació del servidors DNS i web, es donen els primers passos per a la integració total dels serveis del CTTC al nou protocol. Un cop implementada l'IPv6 a la xarxa del centre, plantegem uns escenaris de proves per fer una avaluació comparativa d'aquest protocol amb IPv4. S'executen un seguit de tests per mesurar el rendiment d'IPv6 en front d'IPv4 a través dels paràmetres *Round-Trip Time* (RTT), *throughput* i *Time To First Byte* (TTFB).

A l'entorn de la xarxa del CTTC, els resultats obtinguts en els test, no mostren diferències significatives entre l'ús d'un o altre protocol a nivell de percepció d'usuari. Si els comparem, observem que el valor de RTT és més gran a IPv6, que el *throughput* és més gran a IPv4 i que el cost de carregar el primer byte (TTFB) varia si l'escenari és amb doble pila o si només hi ha implementat un dels dos protocols. La latència de la xarxa és menor amb IPv6 en front IPv4 amb la configuració de la doble pila. En canvi, quan només hi ha un dels protocols configurats és a l'inrevés. També podem concloure que la distància entre l'origen i el destí d'una comunicació és rellevant i repercuteix en la latència de la connexió. Això és causa de la influència del nombre de salts fins al destí, el tipus de xarxes i el proveïdor de serveis. En un altre dels escenaris de prova comparem NAT (*Network Address Translation*) amb IPv6 com a solució alternativa per mitigar la manca d'adreces. A nivell dels paràmetres mesurats no notem grans diferències de rendiment.

**Title:** Estudi d'implantació de la IPv6 al CTTC

**Author:** Jordi Escoda Ramon

**Director:** Roc Meseguer Pallarès

**Date:** February, 20th 2017

**Overview**

In recent years, the number of devices connected to Internet has increased exponentially and in fact, it is estimated that the demand keep on increasing. When IPv4 protocol was introduced, this evolution was not expected. Over the years several limitations have arosen, including scalability and the unsustainable growth of the Internet routing table. In the late 90s, IPv6 protocol was defined to solve these issues and add new features. Currently, the *Centre Tecnològic de Telecomunicacions de Catalunya* (CTTC) has been forced to propose IPv6 deployment on its network mainly caused by the IPv4 address depletion, the increasing demand for devices connectivity and the need to support IPv6. RedIris and CSUC are encouraging and supporting the affiliated institutions like CTTC to deploy IPv6.

This project is carried out by the IT department of CTTC, the *Centre de Serveis Informàtics* (CSI).

The purpose of this project is, on the one hand, to analyse and acknowlege the main features of IPv6 protocol and show the differences with IPv4. It also aims to implement native IPv6 network in CTTC. On the other hand, the CTTC needs to give support with IPv6 in some basic services like DNS and web services. Finally, it is thought to compare IPv6 and IPv4 performance on the CTTC network.

We analysed the network equipment and the network topology before proposing an IPv6 compatible solution. This causes the replacement of some network equipment. To gradually integrate IPv6 in the CTTC network we have chosen the dual-stack deployment. IPv6 is deployed in parallel with IPv4 on all infrastructure and services. We are adapting the DNS and the website service to IPv6 requests. In this project we are measuring the performance of IPv6 versus IPv4. We are running some tests to evaluate the performance through the calculation of the Round-Trip Time (RTT), throughput and Time To First Byte (TTFB) parameters.

The results of the performance tests in the CTTC network are not showing important differences between the two protocols. The RTT is larger in IPv6, the throughput is higher in IPv4 and the TTFB depends on if the dual stack is enabled. The network latency is lower in IPv6 on a dual stack scenario. However, when there is only one protocol set the result is opposite. The

distance between the origin and the destination of communications is relevant because this affects the latency of the connection. This is due to the number of hops to destination, the network type and the service provided. In another test, we are comparing IPv6 with NAT (Network Address Translation) to evaluate this alternative method as a solution to the IPv4 address depletion. The results obtained in the comparison are quite similar.

Voldria agrair especialment al Roc Meseguer la seva dedicació i la paciència que ha tingut amb aquest projecte, ja que s'ha estès molt en el temps des del seu inici fins a la seva presentació.

També voldria agrair al David Company, als meus companys del CSI i del CTTC i al mateix centre el suport donat en la realització d'aquest projecte.

Per últim també voldria agrair a la meva família el suport donat durant tot aquest temps.

# ÍNDEX

# ÍNDEX DE FIGURES I TAULES

# INTRODUCCIÓ

## Marc del projecte

El **Centre Tecnològic de Telecomunicacions de Catalunya** (CTTC) és un centre públic d'R+D sense ànim de lucre fundat l'any 2001 amb el suport de la Generalitat de Catalunya. El CTTC rep finançament de la Generalitat de Catalunya, dels projectes d'R+D amb fons competitius en els que hi participa i dels contractes de transferència de tecnologia amb empreses.

Les activitats de recerca bàsica i aplicada que es duen a terme al CTTC es centren en tecnologies relacionades amb els nivells físic, d'enllaç i de xarxa de la torre OSI de protocols de comunicacions. A nivell organitzatiu, l'activitat d'R+D es realitza en quatre divisions d'investigació: Sistemes de Comunicacions, Xarxes de Comunicacions, Tecnologies de Comunicacions i Geomàtica. Les activitats del CTTC estan tutelades per un comitè extern, el Comitè Científic.

El projecte "Estudi d'implantació de la IPv6 al CTTC" es realitza dins de les activitats del Centre de Suport Informàtic (CSI), departament transversal encarregat de donar suport als usuaris, gestionar, implementar i mantenir tots els serveis i equipaments TIC del centre.

## Raó i oportunitat del projecte

La raó fonamental de la necessitat d'un nou protocol d'Internet es basa en que durant els últims anys, el nombre de dispositius connectats a Internet, l'aparició de noves tecnologies i serveis que necessiten connectivitat IP ha crescut de forma exponencial perquè les necessitats de comunicació entre persones, són un factor important en l'actualitat. Aquest creixement es preveu que segueixi la tònica que porta ja que les tecnologies i les necessitats van en augment i estan en constant desenvolupament. L'espai d'adreces de 32 bits d'IPv4 compost per $2^{32}$ adreces està pràcticament esgotat. Cada host a Internet necessita una adreça única, tot i que hi han tècniques que permeten compartir adreces com pot ser NAT (*Network Address Translation*) o els servidors virtuals, només són un pal·liatiu i impliquen l'aparició d'altres problemes a un sistema que es queda petit. Aquest creixement també provoca que les taules d'encaminament dels routers troncals d'Internet tinguin un creixement no sostenible a causa del seu sistema de jerarquia en l'adreçament, que fa que siguin ineficients i augmentin els temps de resposta.

Els creadors de IPv4, a principis dels anys 70, no van predir l'èxit, el creixement i l'aplicació del protocol. Aquest fet provoca que la IETF (*Internet Engineering Task Force*) es plantegi als anys 90 la creació d'un nou protocol d'Internet per fer front a la falta d'adreces IPv4. El protocol IPv6 va ser definit l'any 1996 per

l'IETF a partir del document RFC 2460 [1]. IPv6 aporta un espai de $2^{128}$ adreces.

El creixement d'Internet també ha provocat que s'hagin tingut de fer modificacions i protocols complementaris a IPv4, per adaptar-lo a les necessitats. Aquests canvis han produït que es perdés el principi de connectivitat punt a punt amb el que estava dissenyat IPv4. El protocol IPv4 presenta altres problemes que IPv6 soluciona o millora com la Qualitat de Servei (QoS), la Seguretat (IPsec) i la Mobilitat (MIPv6) bàsicament.

El CTTC està connectat a l'Anella Científica, la xarxa acadèmica de Catalunya, on el CESCA (CSUC) és el seu gestor i el que ens dona servei. A la vegada, l'Anella Científica forma part de RedIRIS, la xarxa acadèmica i d'investigació espanyola. Des de RedIRIS i del CESCA també s'està promocionant, animant i donant suport a que les institucions afiliades implementin IPv6 a la seva xarxa de comunicacions.

El CTTC al ser un centre de recerca en telecomunicacions té l'obligació moral de donar els primers passos i estar al dia tecnològicament. La xarxa de comunicacions del centre està basada en el protocol IPv4 com a protocol de transport. Donats els problemes d'escalabilitat d'aquest protocol causats pel creixement dels dispositius connectats a la xarxa i a les noticies que ens arriben de la necessitat de suportar IPv6, el CTTC s'ha proposat afegir a la seva xarxa el suport IPv6.

El desenvolupament d'aquest projecte neix com a resposta a aquestes necessitats i consisteix en analitzar, conèixer i implementar de forma nativa el protocol IPv6 a la xarxa del CTTC. La implantació de IPv6 no implica la desaparició de IPv4, serà un procés progressiu, això significa que serà poc agressiu amb els actors.

En el projecte d'estudi d'implantació del protocol IPv6 hi té un paper rellevant l'anàlisi comparatiu d'aquest amb el protocol IPv4. D'aquesta manera podem conèixer i entendre les motivacions, els canvis i les funcionalitats introduïdes per IPv6. Un altre aspecte remarcable per a la implantació és analitzar la situació actual de la xarxa del CTTC i prendre les decisions oportunes per tal d'adaptar-la perquè suporti ambdós protocols IPv4/IPv6 (doble pila). Les decisions que sorgeixin en la implantació del protocol IPv6 al CTTC es prendran de forma consensuada al CSI, valorant i sospesant l'afectació als serveis i usuaris de la institució perquè aquesta no suposi un greuge.

Els recursos disponibles de maquinari i programari per la implantació de la IPv6 al CTTC són la seva infraestructura i recursos actuals. En cas que hi hagi una necessitat de realitzar algun canvi en algun d'aquests aspectes, el CSI ho valorarà en funció dels seus criteris.

A nivell econòmic, les decisions i accions que s'hagin de prendre derivades de l'estudi d'implantació de IPv6, seran a càrrec del CTTC en funció dels seus criteris. El responsable de les TIC del CSI és l'encarregat de transmetre els resultats i valorar-los amb la direcció del centre.

La xarxa IPv6 al CTTC donarà servei als actuals equips de servidors i d'usuaris a nivell de proves. La implementació permetrà al centre estar preparats per a futures necessitats que es puguin esdevenir en relació amb el nou protocol i obre les portes a possibles línies de recerca i desenvolupament entorn al protocol IPv6 i les tecnologies. Aquest treball i els seus resultats representen el primer pas per a una futura migració de tots els serveis oferts al centre a IPv6.

La realització d'aquest projecte no té un impacte ambiental negatiu. Es procura reutilitzar l'equipament existent, i en el cas que s'hagi adquirit nou maquinari, reaprofitar el que substituïm. En la implementació de la xarxa IPv6, els equips canviats s'han acabat reutilitzant en segments de la xarxa que no tenien aquests requeriments o per proves. Els equips utilitzats per realitzar els tests del banc de proves ja es disposaven al centre o s'han utilitzat màquines virtuals aprofitant la infraestructura de virtualització existent.

## Objectius i estructura del projecte

Els objectius principals que es proposen en aquest projecte són:

- L'objectiu principal d'aquest projecte és dissenyar i implementar IPv6 de forma nativa al CTTC amb connectivitat exterior.
- Analitzar i conèixer les característiques principals del protocol IPv6 i veure quines són les diferencies amb IPv4.
- Elaborar un banc de proves per avaluar el rendiment del protocol IPv6 i comparar-lo amb IPv4 a la xarxa el CTTC.

Sorgeixen altres objectius més específics:

- Avaluar i adaptar la infraestructura de xarxa del CTTC per tal de suportar la doble pila de protocols IPv4/IPv6.
- Crear un pla d'adreçament IPv6 al CTTC.
- Configurar els serveis bàsics en IPv6.
    - Adaptar el web principal del CTTC perquè respongui a IPv6 (ipv6.cttc.cat i www.cttc.cat).
    - Configurar el DNS perquè respongui les peticions en ambdós protocols.

Aquest document s'estructura per capítols. En els següents capítols, s'estudien les característiques, les diferències amb el protocol IPv4, l'adreçament, les funcionalitats i els mecanismes de migració i coexistència del protocol IPv6. En el capítol 2, es realitza un anàlisis de l'estat actual de la xarxa del CTTC i en funció d'aquest, en el capítol 3, es realitza la proposta de disseny que s'implementarà a la xarxa perquè suporti IPv6. En el capítol 4, es realitza un banc de proves per comprovar i experimentar amb les funcionalitat del nou protocol d'Internet. En capítol 5, es recullen les principals conclusions que s'han obtingut de l'estudi i s'analitzen els aspectes a tenir en compte pel futur. Finalment, en l'últim capítol hi trobem les referències bibliogràfiques, el glossari i els annexos.

# CAPÍTOL 1. EL PROTOCOL IPv6

El principal motiu de la creació del protocol IPv6 és l'esgotament de les adreces disponibles IPv4 provocat pel creixement d'Internet. Per això sorgeix la necessitat de conèixer i implementar IPv6. Aquest capítol està centrat en explicar les principals característiques del protocol IPv6: analitzem el format de la capçalera IPv6 i la comparem amb la capçalera IPv4; expliquem l'adreçament IPv6 i les seves característiques; mostrem les diferències amb l'adreçament IPv4; presentem algunes de les funcionalitats introduïdes per IPv6 com les que fan referència als protocols d'encaminament, el protocol de control de missatges, el protocol de descobriment de nodes veïns, l'autoconfiguració d'adreces i la seguretat; indiquem quins són els mecanismes de migració i coexistència de xarxes IPv4 a IPv6. D'aquesta forma coneixem el seu funcionament i els podem comparar amb la tècnica de doble pila que és la que ens proposem implementar.

## 1.1. Estructura d'IPv6

### 1.1.1. Format de la capçalera IPv6

La capçalera IPv6 té un nou format que està dissenyat per reduir al mínim la sobrecarrega d'informació. Elimina els camps que no són essencials d'IPv4. Veure **Annex A. Camps capçalera IPv4**. La figura **Fig. 1.1** mostra, com a referència, la estructura de la capçalera d'un paquet IPv4.

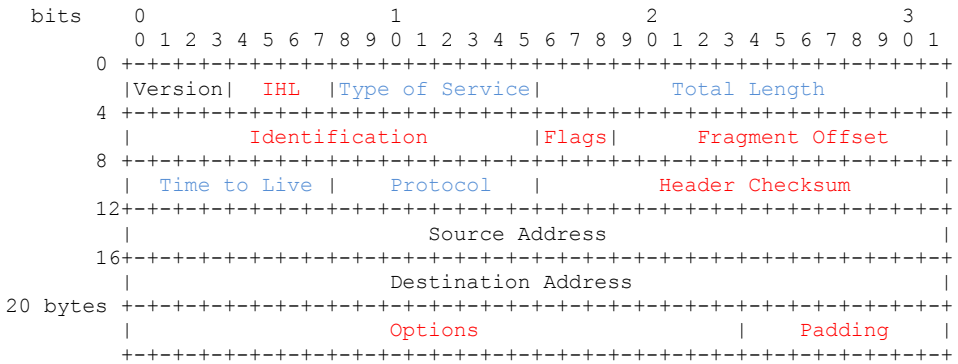



**Fig. 1.1** Format de la capçalera IPv4 [2]

En les figures **Fig. 1.1** i **Fig. 1.3**, apareixen marcats de color vermell els camps que desapareixen. Els que es modifiquen estan marcats de color blau, els que estan de color negre es mantenen i els de color verd són nous camps en IPv6 (veure figura **Fig. 1.2**). La capçalera passa de 12 camps a IPv4, a 8 camps a IPv6.

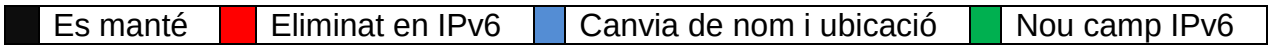



**Fig. 1.2** Llegenda comparativa capçalera IPv4 i IPv6

La figura **Fig. 1.3** mostra la estructura de la capçalera d'un paquet IPv6.


**Fig. 1.3** Format de la capçalera IPv6 [3]

Aquesta intenta millorar els principals problemes de la capçalera IPv4 a través de:

- Mida fixa de la capçalera. Sempre de 40 bytes, el doble de la longitud mínima de la capçalera IPv4. Això afavoreix el poder processar-la de forma més ràpida perquè els *routers* poden buscar les direccions origen i destí de forma més eficient. Les funcionalitats que tenia IPv4 a través del camp de mida variable, *Options,* ara les obtindrem a través de les extensions de la capçalera, veure **Annex B. Extensions de capçalera IPv6**.
- La fragmentació deixa de tenir sentit ja que a través del PMTU *discovery,* els *routers* ajusten la mida de les trames per tal de que no hi hagi fragmentació en els paquets. No s'admet la fragmentació de paquets més grans que la MTU. Per aquest motiu, desapareixen els camps de control que apareixien a la capçalera IPv4 per suportar la fragmentació *Identification*, *Flags*, i *Fragment Offset*.
- Les comprovacions de la capçalera (*header checksums*) s'eliminen. Aquesta tasca es deixa per les capes superiors.

La capçalera d'IPv6 consta dels camps següents:

- **Version** (4 bits) versió del protocol IP, valor fixe a 6. Es manté com a primer camp del datagrama per mantenir la compatibilitat amb el mateix camp que la capçalera IPv4.
- **Traffic Class** (8 bits) fa referència a la prioritat del datagrama. Inclou

informació que permet als *routers* classificar el tipus de tràfic al que pertany el paquet. Té les mateixes funcionalitats que el camp *Type of Service*[1] (ToS) d'IPv4.

- **Flow Label** (20 bits) a través d'aquest camp identifiquem un flux de paquets, informant al *router* que els següents 'n' paquets seran iguals a aquest, i per tant, es poden tractar de la mateixa manera. Aquesta informació es fixa a l'origen del paquet i no la poden modificar els *routers* [4].
- **Payload Lengh** (16 bits) és la longitud de la càrrega útil, pot ser de més de 65535 bytes. Les extensions de la capçalera es consideren part de les dades. Equivalent al camp *Total Length* d'IPv4.
- **Next Header** (8 bits) Identifica el tipus d'extensió de la capçalera que segueix a la capçalera bàsica. Empra els mateixos valors que el camp *Protocol* d'IPv4 [5].
- **Hop Limit** (8 bits) Indica el nombre màxim de salts que pot realitzar el paquet fins arribar al seu destí. Disminueix en una unitat aquest valor per cada node que envia el paquet. El paquet es descarta si el límit de salts arriba a zero. És l'equivalent al camp *TTL* d'IPv4.
- **Source Address** (128 bits) Adreça origen IPv6 del node que ha generat el paquet.
- **Destination Address** (128 bits) Adreça destí IPv6 del paquet.

Els camps *Flow Label* i *Traffic Class* són els camps que ens permeten una de les característiques fonamentals i intrínseques d'IPv6: Qualitat de Servei (QoS) i Classe de Servei (CoS). Són un mecanisme de control de flux i d'assignació de prioritats en funció del tipus de servei.

### 1.1.2. Capçaleres opcionals d'IPv6

A IPv6, la informació opcional és codificada en capçaleres diferents a la principal, aquestes poden ser col·locades entre la capçalera IPv6 i la capçalera dels protocols de capes superiors, i ocupen un espai destinat a la càrrega útil del paquet bàsic. Això és degut a que aquestes opcions en IPv4 estaven a la capçalera principal, provocant un impacte en el rendiment perquè els encaminadors les han de processar.

Com ja hem mencionat en l'apartat anterior, IPv6 no suporta la fragmentació de paquets ens els nodes intermedis. Aquesta funció es realitza ens els extrems. Quan es requereix fragmentació d'un paquet de dades, s'introdueix una capçalera d'extensió que es referencia a la capçalera del paquet principal.

Les capçaleres opcionals [6], s'utilitzen per a donar les funcions que es donaven en IPv4 a través del camp Options, de mida variable i màxim de 40 bytes. En IPv6 podem fer aquestes extensions de capçalera tant grans com ens interessin, sempre que respectem la mida màxima del paquet.

[1]**Type of Service** (ToS) identificador usat en QoS per tal de poder classificar els paquets segons la prioritat que li volem donar.

Hi ha varies *Extension Headers* [7], que s'identifiquen amb un valor diferent al camp *Next Header* de la capçalera IPv6. Els tipus de capçaleres estandarditzats són: *Hop-by-Hop Options header, Destinations Options header, Routing header, Fragment header, Authentication header, Encapsulating Security Payload header, Mobility header, No next header i Upper-layer header.* (Veure **Taula B.1 a l'Annex B** i **B.2 Capçaleres d'Extensió més usades**).

De forma general només es processen les capçaleres en els nodes destí i origen, excepte *Hop-by-Hop Options* que es processa per a tots els encaminadors intermedis.

## 1.2. Adreçament IPv6. RFC 4291 [8]

IPv6 aporta un espai de $2^{128}$ adreces, això equival a 3,40E38 (340282366920938463374607431768211456). Les adreces IPv6 són identificadors de 128 bits per interfícies i conjunts d'interfícies. Aquestes adreces es classifiquen en tres tipus:

- ***Unicast*** [9]*:* Identificador per a una única interfície. Un paquet enviat a una adreça unicast s'entrega només a la interfície identificada amb l'adreça. Equivalent a les adreces IPv4.
- ***Anycast*** [10]: Identificador per a un conjunt d'interfícies (normalment pertanyents a diferents nodes). Un paquet enviat a una adreça *anycast* és lliurat a una de les interfícies identificades amb aquesta adreça (la més propera, d'acord amb les mesures de distància del protocol d'encaminament emprat).
- ***Multicast*** [11]: Identificador per a un grup d'interfícies (normalment pertanyents a diferents nodes). Quan un paquet s'envia a una adreça multicast és entregat a totes les interfícies del grup identificades amb aquesta adreça.

### 1.2.1. Diferències amb IPv4

Hi ha algunes diferències importants en l'adreçament d'IPv6 respecte el d'IPv4:

- L'assignació d'adreces IPv6 es realitza a cada interfície, no per node. Qualsevol de les adreces *unicast* de les interfícies del node pot servir per identificar-lo.
- No hi ha adreces *broadcast*, la seva funció és substituïda per les adreces *multicast*.
- Totes les interfícies poden tenir assignades qualsevol tipus d'adreça (*unicast*, *anycast* o *multicast*) però, com a mínim, han de tenir assignada una adreça *unicast link-local* (enllaç local).

En la **Taula C.1 de l'Annex C. Diferències adreçament IPv4 i IPv6** observem les principals diferències entre l'adreçament IPv4 i IPv6.

### 1.2.2. Representació de les adreces IPv6

El RFC 5952 [12] dona recomanacions per l'escriptura de les adreces IPv6. La representació de les adreces IPv6 segueix el següent esquema:

- **x:x:x:x:x:x:x:x**, on "x" és un grup de 4 dígits hexadecimals de 16 bits. No és necessari escriure els zeros a l'esquerra de cada camp. Les següents adreces són equivalents:
  2001:40b0:7c22:6020:0000:0000:0005:0145
  2001:40b0:7c22:6020:0:0:5:145
- **Abreviació**. Poden existir adreces IPv6 que tinguin una llarga cadena de zeros. Per simplificar-les i comprimir-les es permet l'escriptura de la seva abreviació per mitjà de "::". Aquest símbol representa múltiples grups consecutius de 16 bits zero. Aquest símbol només pot aparèixer un cop en una adreça IPv6. Les següents adreces són equivalents:
  2001:40b0:7c22:6020:0000:0000:0005:0145 ≡
  2001:40b0:7c22::5:145
  0:0:0:0:0:0:0:1 ≡ ::1
  0:0:0:0:0:0:0:0 ≡ ::
- **Minúscules**. És aconsellable que els caràcters hexadecimals ("a","b","c","d","e" i "f") en una adreça IPv6 estiguin representats en minúscules.
- **Adreces IPv4**. Una forma alternativa, útil en entorns compartits amb IPv4, és el format x:x:x:x:x:x:d.d.d.d, on "x" té el significat anterior i "d" són els valors decimals que representen l'adreça IPv4. Aquest tipus d'adreces estan desaprovades pel RFC 4291 [8] perquè els mecanismes actuals de transició IPv6 ja no utilitzen aquest tipus d'adreces. Les següents adreces són equivalents:
  0:0:0:0:0:0:84.88:25.4 ≡ ::84.88.25.4
  2001:0:0:0:0:2a:84.88.76.13 ≡ 2001::2a:84.88.76.13
- **Literal**. Les adreces uri s'escriuen als navegadors web amb els següent format:
  [2001:40b0:7c22::4:201c]
  http://[ff01::43]:80/index.html

### 1.2.3. Representació dels prefixos de xarxa de les adreces IPv6

Les adreces IPv6 estan formades per un prefix de xarxa seguit d'un identificador d'interfície i de la longitud del prefix de xarxa. La longitud del prefix de xarxa és un valor decimal que indica quants bits contigus de la part esquerra de l'adreça formen el prefix. S'utilitzen els mateixos principis del CIDR. La representació dels prefixes IPv6 segueix la següent notació:

<adreça IPv6>/<longitud del prefix>

El següent exemple mostra les representacions vàlides d'un prefix 48 bits :

2001:0000:0c22:0000:0000:0000:0000:0000/48
2001::c22:0:0:0:0:0/48
2001:0:c22::/48

Una adreça completa IPv6 amb la seva subxarxa seria:
2001:7c01:c22::6020:cade/48

### 1.2.4. Àmbits de les adreces IPv6

Les adreces IPv6 tenen un àmbit (*scope*) que determina en quines parts de la xarxa són vàlides:

- **Enllaç (*link-local*):** Vàlida dins de l'enllaç en el que està connectat la interfície de xarxa (per exemple, una LAN).
- **Local (*site-local*):** Vàlida dins d'un lloc, que pot estar format per una o vàries xarxes interconnectades per mitjà de *routers* (per exemple, un campus universitari).
- **Global:** Vàlida a tot Internet.

La unicitat de les adreces només es garanteix dins del seu àmbit.

### 1.2.5. Tipus d'adreces

A IPv6 els primers bits de l'adreça identifiquen el tipus d'adreces. En la **taula 2.2 de l'Annex D. Tipus d'adreces Ipv6** i en la figura **Fig. 1.4** observem un resum amb l'assignació d'adreces IPv6.

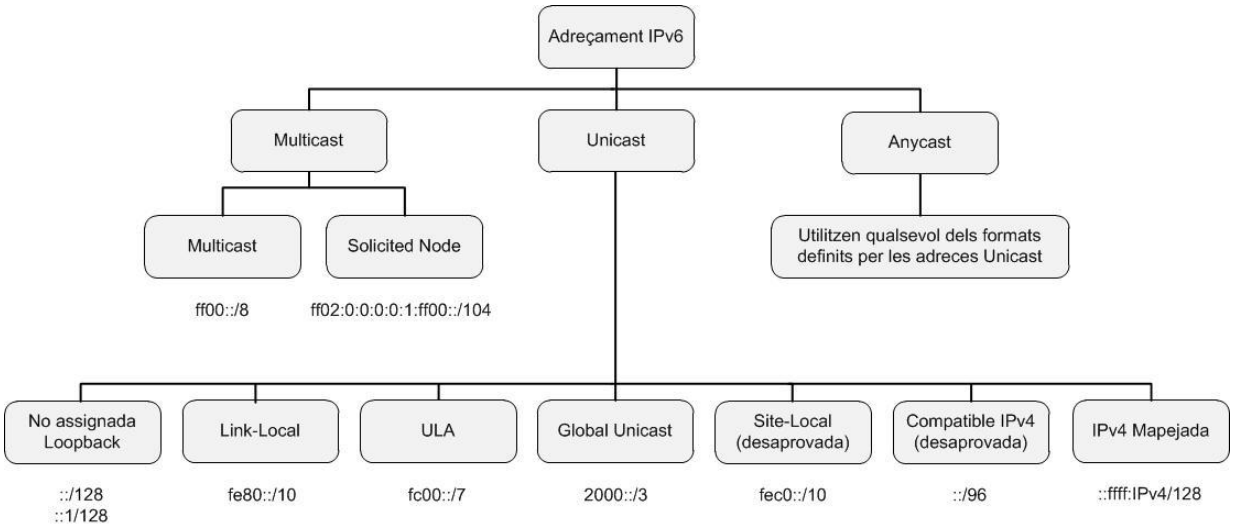



**Fig. 1.4** Classificació de les adreces IPv6

### 1.2.6. Adreces Unicast

Les adreces *unicas*" identifiquen a una sola interfície. Això permet donar connectivitat punt a punt entre els nodes d'aquesta xarxa. A aquest grup pertanyen:

- Global Unicast Addresses
- Link-Local
- Site-Local (desaprovades)
- Unique Local Addresses (ULA)
- Adreces especials

Veure **Annex D.1 Tipus d'adreces IPv6 Unicast**.

Cal destacar les adreces *Global Unicast* que estan definides per tal de connectar els usuaris a Internet. Són l'equivalent a les adreces públiques IPv4. Aquestes segueixen un model d'adreçament públic basat en una política coordinada de distribució d'adreces. Amb aquesta distribució jeràrquica s'aconsegueix una gran eficàcia en els aspectes d'encaminament, ja que disminueix les grans taules que suporten els principals *routers* d'Internet amb IPv4.

#### *1.2.6.1. Identificadors d'Interfície (IID) RFC4291 [13]*

Els identificadors d'interfície de les adreces IPv6 *Unicast*, s'utilitzen per a identificar les interfícies d'un enllaç. Han de ser únics dins del mateix prefix de subxarxa. El mateix IID pot ser utilitzat en múltiples interfícies d'un únic node, sempre que estiguin associats a diferents xarxes. Totes les adreces *Unicast*, excepte les que comencen amb el prefix 000, utilitzen un IID de 64 bits (veure figura **Fig. 1.5**) anomenat *Modified EUI-64*.

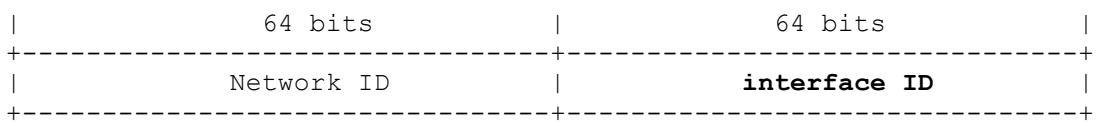



**Fig. 1.5** Format dels IID

A part del EUI-64 hi ha dos formes més per determinar l'IID:

- Un IID generat aleatòriament que canvia periòdicament per a donar un cert nivell d'anonimat (configuració *Stateless*).
- Un IID assignat durant l'autoconfiguració d'adreces, com per exemple durant DHCPv6 (configuració *Stateful*).

### 1.2.7. Adreces anycast RFC 2526 [10]

Una adreça IPv6 *anycast* és una adreça que s'assigna a més d'una interfície (normalment pertanyent a diferents nodes), amb la propietat que un paquet enviat a una adreça *anycast* s'encamina a la interfície més "propera" que tingui aquella adreça, d'acord amb els protocols de routing implementats.

Les adreces *anycast* estan incloses dins l'espai d'adreçament de les adreces *unicast*, per la qual cosa són sintàcticament indistingibles. Quan una adreça *unicast* s'assigna a més d'una interfície, esdevé una adreça *anycast*. Tot i això, cal dir que els nodes que tenen una adreça *anycast* han de ser explícitament configurats per a reconèixer les adreces *anycast* com a tals.

Una adreça *anycast* té un prefix que identifica la regió topològica en què hi ha les adreces *anycast.* Dins de la regió definida per aquest prefix, cada membre del grup *anycast* ha de ser identificat com una entrada diferent en la informació de *routing*. Fora de la regió identificada pel prefix, l'adreça *anycast* ha de ser agregada dins de la informació de *routing* del prefix en qüestió.

Un dels usos de les adreces *anycast* és, per exemple, el servei DNS, ja que aquest pot estar replicat en diversos servidors, amb una sola IP anycast. Les peticions s'encaminen al servidor més proper a l'origen. L'experiència en l'ús d'aquestes adreces encara no té gran fonament i, per tant, poden sorgir problemes quan s'usen.

### 1.2.8. Adreces multicast RFC 2375 [11]

Una adreça *multicast* és un identificador per a un grup de nodes. Hi ha dos avantatges principals amb l'ús d'aquest tipus d'adreces respecte a les adreces *unicast*. Les adreces *multicast* permeten enviar una mateixa informació a diferents usuaris finals creant un únic flux de dades, és a dir, sense haver de repetir el missatge per cada destí. Respecte a les adreces *broadcast*, les adreces *multicast* eviten haver d'enviar la informació a tots els nodes d'un mateix grup, millorant l'eficiència i la seguretat de la xarxa, ja que només reben les dades el conjunt d'usuaris als quals va dirigida la informació.

Tot i això, els nodes i encaminadors de la xarxa han d'utilitzar un marge específic d'adreces IP per rebre els beneficis del *multicasting*. Algunes de les utilitats del *multicasting* en IPv6 són l'anunciament de prefixos, la detecció d'adreces duplicades, els seu ús en els missatges de resolució d'adreces MAC, el renombrament automàtic de prefixos i l'ús en aplicacions de retransmissió múltiple (*broadcast*). Les adreces IPv6 *multicast* tenen el format que s'observa en la figura **Fig. 1.6**. Veure l'**Annex D.2 Tipus d'adreces multicast** per veure els tipus d'adreces *multicast*.

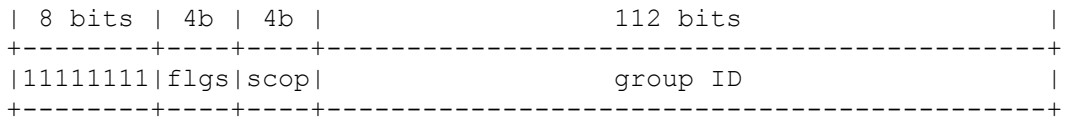



**Fig. 1.6** Format de les adreces IPv6 *multicast* [13]

Descripció dels camps:

- 11111111(binari): ff Hexadecimal. Identifica l'adreça *multicast*
- *Flags*: Són un conjunt de 4 *flags*: |0|R|P|T|
  El flag de major pes està reservat i inicialitzat a zero.
  T=0 indica una assignació permanent ("*well-know*") d'adreça *multicast*, assignada per l'autoritat de numeració global d'Internet (IANA). Té un sentit global a tota la xarxa. [14]
  T=1 indica una adreça *multicast* temporal ("transitòria o dinàmica")
  Els *flags* R [15] i P [16] són emprats en el protocol de construcció de l'arbre *multicast* de tipus *Sparce Mode* (dominis que no són densament poblats i dispersos) i PIM-SM.
- *Scope* (Àmbit): És un valor de 4 bits que defineix l'abast del grup *multicast*. Aquest restringeix l'enviament de paquets a certes seccions de xarxa. Els valors permesos són els detallats en la **Taula 1.1**.

**Taula 1.1** Significat dels bits d'àmbit (*scope*)

| | | | |
|---|---|---|---|
| 0 | Reservat | 8 | Àmbit local d'organització<br>*Organization-Local scope* |
| 1 | Àmbit local d'interfície/node<br>*Interface-Local scope* | 9 | Sense assignar |
| 2 | Àmbit local d'enllaç<br>*Link-Local scope* | A | Sense assignar |
| 3 | Reservat | B | Sense assignar |
| 4 | Àmbit local d'administració<br>*Admin-Local scope* | C | Sense assignar |
| 5 | Àmbit local de lloc<br>*Site-Local scope* | D | Sense assignar |
| 6 | Sense assignar | E | Àmbit Global<br>*Global scope* |
| 7 | Sense assignar | F | Reservat |

- *Group ID*: Identifica el grup *multicast*, tant permanent com transitori, dins d'un determinat àmbit. Veure **Annex D.2.1. Exemple del camp Group ID en les adreces multicast permanents i transitòries.**

Les adreces *multicast* no han de ser utilitzades com adreces origen en un paquet IPv6 o aparèixer en qualsevol capçalera d'encaminament.

### 1.2.9. Adreces necessàries per qualsevol node

Tots els nodes, en el procés d'identificació, a l'unir-se a la xarxa, han de reconèixer com a mínim, les següents adreces:

- Les seves adreces *link-local* (locals d'enllaç) per cada interfície.
- Les adreces *unicast* assignades (*ULA* o *global*).
- L'adreça de *loopback* (::1).
- Les adreces *multicast* que identifiquen tots els nodes, tant la de *node-local* (ff01::1) com la de *site-local* (ff02::1).
- Les adreces *multicast solicited-node* associades a cadascuna de les seves adreces *unicast* o *anycast*.
- Les adreces *multicast* de tots els grups als que pertany el *host*.

A part d'aquestes, els *routers*, han de reconèixer també:

- L'adreça *anycast* del *router* de la sub-xarxa, per les interfícies en les que està configurat per actuar com a *router*.
- Totes les adreces *anycast* amb les que el *router* ha estat configurat.
- Les adreces *multicast* de tots els *routers*.
- Les adreces *multicast* de tots els grups als que el *router* pertany.

Tots els dispositius amb IPv6, han de tenir predefinits els següents prefixos:

- Adreça no especificada.
- Adreça de *loopback.*
- Prefix *multicast* (ff)
- Prefixos d'ús local (local d'enllaç i local de lloc).
- Adreces *multicast* predefinides.
- Prefixes compatibles IPv4.

S'ha d'assumir que tota la resta d'adreces són *unicast* a no ser que siguin configurades específicament (per exemple les adreces *anycast*).

## 1.3. Funcionalitats d'IPv6

### 1.3.1. Encaminament a IPv6

L'ús d'IPv6 no implica canvis significatius en la forma d'operar dels protocols d'encaminament en les xarxes IP. Per tal d'aprofitar les noves característiques d'IPv6, s'han desenvolupat noves versions o complements als protocols d'encaminament utilitzats en IPv4 (RIP, EIGRP, OSPF, IS-IS i BGP). Hi ha dos tipus de rutes, les estàtiques, configurades manualment i les dinàmiques, que modifiquen les taules de rutes de forma automàtica.

Hi ha dos tipus de protocols:

- *Interior Gateway Protocol* (IGP), utilitzat per intercanviar la informació d'encaminament dels *routers* dins de sistemes autònoms. Utilitzen vector-distància i *link-state*. Exemple: IS-ISv6, RIPng, EIGRP i OSPFv3
- *Exterior Gateway Protocol* (EGP), utilitzat per determinar les rutes entre sistemes autònoms. Exemple: MP-BGP4.

Veure **Annex E1 Protocols d'encaminament IPv6**, amb les característiques d'aquests.

### 1.3.2. Taules d'encaminament

El procés de selecció de rutes és idèntic que en IPv4, però les taules de rutes són independents. Els equips que treballin amb ambdós protocols mantindran dues taules d'encaminament separades, una per a cada protocol de nivell 3.

### 1.3.3. ICMPv6 RFC4443 [17][18][19]

Com IPv4, IPv6 per si mateix no proporciona cap utilitzat per informar sobre errors. IPv6 utilitza una versió actualitzada del Protocol de Missatges de Control d'Internet (*Internet Control Message Protocol*) per IPv4 [20], ICMPv6. Els paquets ICMPv6 s'encapsulen dins de paquets IPv6, identificats amb el valor 58 en el camp "Next Header".

El protocol ICMPv6 incorpora dues noves funcions a realitzar, *Multicast Listener Discovery (MLD)* i *Neighbor Discovery (ND)*.

*Multicast Listener Discovery*, és un conjunt de tres missatges ICMPv6 que reemplacen la versió 2 del protocol IGMP *(Internet Group Management Protocol)* d'IPv4 per gestionar els membres d'un grup *multicast*.

*Neighbor Discovery* és un conjunt de cinc missatges ICMPv6 que gestionen la comunicació node a node en un enllaç. El ND reemplaça els protocols ARP, *ICMPv4 Router Discovery* i el *ICMPv4 Redirect*.

El format genèric dels missatges ICMPv6 és el de la figura **Fig. 1.7**:

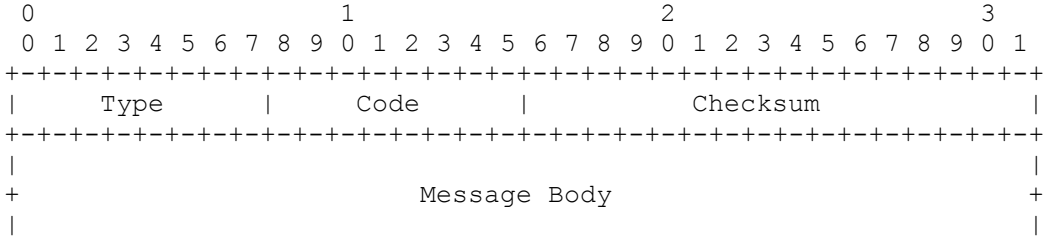



**Fig. 1.7** Format genèric dels missatges ICMPv6 [17]

Els camps del paquet ICMPv6 són:

- El camp *Type* indica el tipus de missatge i el seu valor determina el format de la capçalera.
- El camp *Code* depèn del tipus de missatge, s'utilitza per a crear un nivell addicional de jerarquia per a la classificació del missatge.
- El camp *Checksum* permet detectar errors en el missatge ICMPv6.
- El camp *Message Body* conté les dades del missatge ICMPv6.

Els missatges ICMPv6 s'agrupen en dos tipus: missatges d'error i missatges informatius. Els missatges d'error tenen el bit de major pes del camp *Type* igual a zero. Els seus valors es situen entre 0 i 127 i s'utilitzen per reportar errors en l'entrega de paquets IPv6. Els valors dels missatges informatius oscil·len entre 128 i 255. A la **Taula E.1** de **l'Annex E.2. Format dels missatges ICMPv6** observem els missatges definits per la especificació bàsica.

### 1.3.4. Neighbor Discovery RFC4861 [21][18][19]

El protocol *Neighbor Discovery* (ND) d'IPv6 és el mecanisme que utilitza un node per incorporar-se a la xarxa, descobrir la presència d'altres nodes en el mateix enllaç, determinar les seves adreces de la capa d'enllaç i IPv6, localitzar els *routers* disponibles, i per mantenir la informació actualitzada de connectivitat (*reachability*) sobre les rutes als nodes veïns actius.

ND es correspon a la combinació dels següents protocols d'IPv4: ARP, *ICMPv4 Router Discovery* i *ICMPv4 Redirect*. Per l'intercanvi d'informació utilitza els missatges ICMPv6.

*Neighbor Discovery* soluciona problemes d'interacció entre nodes connectats al mateix enllaç i defineix els mecanismes per solucionar els següents problemes:

- *Router Discovery*: com els hosts localitzen els *routers* connectats als seus enllaços.
- *Prefix Discovery*: com els hosts descobreixen quins prefixos d'adreça hi ha als enllaços on estan connectats.
- *Parameter Discovery*: com un node aprèn els paràmetres de l'enllaç (p.e: *link MTU*).
- *Address Autoconfiguration*: com els nodes configuren les adreces de les interfícies de xarxa.
- *Address Resolution*: com els nodes determinen la correspondència entre adreces IP i adreces de nivell d'enllaç.
- *Next-hop determination*: com els hosts poden trobar els *routers* del següent salt per un destí.
- *Neighbor Unreachability Detection (NUD)*: com els nodes determinen que no es pot arribar a un veí.

- *Duplicate Address Detection (DAD)*: com els nodes poden comprovar si una adreça ja s'està fent servir.
- *Redirect*: com un *router* informa a un host d'un millor node de sortida per dirigir el tràfic cap a un cert destí.

*Neighbor Discovery* defineix cinc nous tipus de paquet ICMPv6 per solucionar els anterior problemes. Es poden observar a la **Taula E.2** de l'**Annex E.3 Tipus de missatge ICMPv6 del protocol Neighbor Discovery.**

### 1.3.5. Autoconfiguració RFC4861 [21][18][19]

L'autoconfiguració és un mecanisme en el qual un host d'un segment afegeix la seva adreça física, en el format EUI-64, a l'adreça *unicast* IPv6 que ha obtingut mitjançant algun mecanisme. Això permet el *plug and play,* la connexió de dispositius a la xarxa sense la necessitat de configurar els seus paràmetres de xarxa. Els *routers* no poden tenir autoconfiguració, s'han de configurar manualment.

El procés d'autoconfiguració inclou la creació d'una adreça *link-local*, la verificació que no està duplicada en aquest determinat enllaç i l'obtenció de la informació necessària per a la configuració.

Hi ha tres tipus d'autoconfiguració [22]:

- *Stateless* (autoconfiguració automàtica)
- *Stateful* (DCPv6)
- Ambdues

L'autoconfiguració *stateless,* configura les adreces sense cap tipus de protocol. Es basa en els *Router Advertisements*. Aquest mode de configuració permet obtenir una adreça *unicast* IPv6 a partir d'informació anunciada per part del *router* del mateix segment.

L'autoconfiguració *stateful*, es basa en l'ús de protocol de configuració d'adreces, com DHCPv6, per obtenir adreces i altres opcions de configuració. Aquesta opció s'utilitza quan no hi ha *routers* en l'enllaç local o quan aquests no generen *Router Advertisements*.

L'autoconfiguració que utilitza totes dues es basa tant en missatges *Router Advertisements* com configuracions *stateful*.

### 1.3.6. Seguretat

Una de les principals avantatges d'IPv6 és la seguretat, es va aprofitar per integrar els mecanismes de seguretat, autenticació i encriptació, dins del nucli del protocol. Es realitza a través d'IPsec, a IPv4 el seu ús és opcional però amb

IPv6 és una part obligatòria.

La seguretat a nivell d'IPsec es dona a través dels següents protocols de la capçalera: Autenticació, AH (*Autentication Header*) i encriptació, ESP (*Encapsulation Security Payload*). A l'**Annex B.2.2.3** per l'AH i a l'**Annex B.2.2.3** per l'ESP trobem les característiques d'aquestes capçaleres d'extensió.

## 1.4. Mecanismes de migració i coexistència de xarxes IPv4 a IPv6. RFC4213 [23]

IPv6 està dissenyada per facilitar la transició i la coexistència amb IPv4. Per la implementació de xarxes IPv6 sobre xarxes que funcionen en IPv4 i viceversa, existeixen tres tècniques. Es preveu que el seu ús serà prolongat, o fins i tot, indefinit en moltes ocasions.

- Doble pila, permet la coexistència IPv4 i IPv6 en el mateix dispositiu i xarxes. [24]
- Túnels IPv6 sobre IPv4, encapsulat de paquets IPv6 dins de paquets IPv4. [24]
- Mecanismes de traducció, permeten la comunicació entre dispositius que són només IPv6 i dispositius que són només IPv4.[26]

### 1.4.1. Doble Pila

La tècnica doble pila o *dual stack* executa paral·lelament els protocols IPv4 i IPv6 en els nodes d'una xarxa. Cada node té assignades adreces d'ambdós protocols. L'avantatge d'aquesta implementació és que assegura la connectivitat dels nodes de la xarxa, quan no poden utilitzar IPv6 utilitzen IPv4. La doble pila de forma nativa no requereix mecanismes de tunneling (apartat 1.4.2) en les xarxes internes.

Les aplicacions que no suporten IPv6 podran coexistir amb les que si ho suporten. Aquestes triaran la pila en funció de les DNSs. Per contrapartida, disminueixen les prestacions dels equips de xarxa perquè han de mantenir taules de direccions i rutes independents per cada un d'ells. La següent figura **Fig. 1.8** mostra les diferències entre la pila IPv4 i la doble pila.

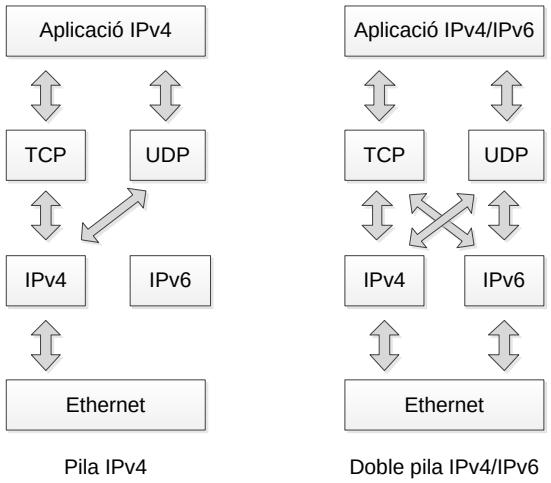



**Fig. 1.8** Doble pila IPv4/IPv6 en relació amb la pila IPv4

### 1.4.2. Túnels IPv6 sobre IPv4

La tècnica de túnels IPv6 sobre IPv4 (*tunneling 6over4*) consisteix en encapsular paquets IPv6 dins de paquets IPv4 perquè aquests puguin ser transportats a través de xarxes IPv4, figura **Fig. 1.9**.

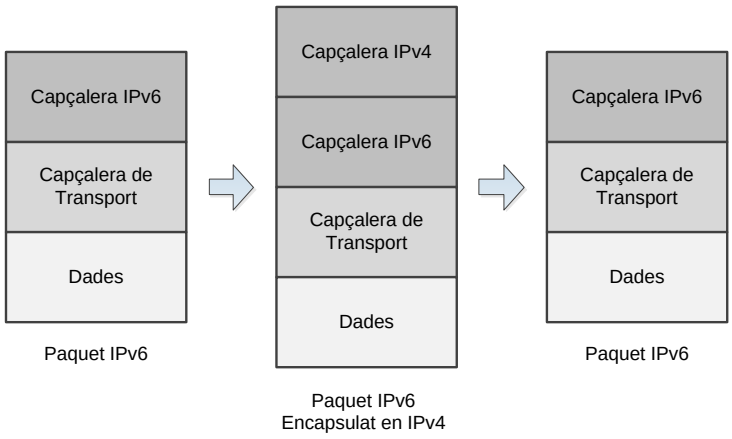



**Fig. 1.9** Encapsulament i desencapsulament d'IPv6 sobre IPv4.

Els extrems finals del túnel són els encarregats de realitzar el procés d'encapsulació i extracció de paquets IPv6 sobre IPv4. Els túnels ofereixen una manera d'utilitzar una infraestructura d'encaminament IPv4 existent que no permet la implementació de IPv6 per transportar el tràfic IPv6.

Els *routers* o *hosts* de cada extrem del túnel han de ser de doble pila. Els túnels poden ser emprats en escenaris diferents:

- Entre dos *host* IPv6 de doble pila

- Entre dos *routers* IPv6 de doble pila
- Entre en *host* i un *router* IPv6 de doble pila

Existeixen varies tècniques de *tunneling*: 4in6, *6in4*; *6over4*; *6to4*; 6rd; IPv6 túnel *Broker*; túnel TEREDO; túnel ISATAP; *Dual Stack Lite; Softwires*.

El principal inconvenient de l'ús de túnels és que empitjora la latència. Els túnels poden presentar problemes de seguretat ja que molts usuaris tenen IPv6 perquè tenen serveis que els configuren automàticament. Poden tenir problemes de privacitat i traçabilitat quan es configuren contra altres entitats.

### 1.4.3. Mecanismes de traducció

Aquesta tècnica permet la comunicació entre zones IPv4 i IPv6 aïllades, sense connexió directa. Realitza una "traducció" similar a la que realitza el NAT, on es modifica la capçalera IPv4 a una capçalera IPv6 i viceversa, figura **Fig. 1.10**.

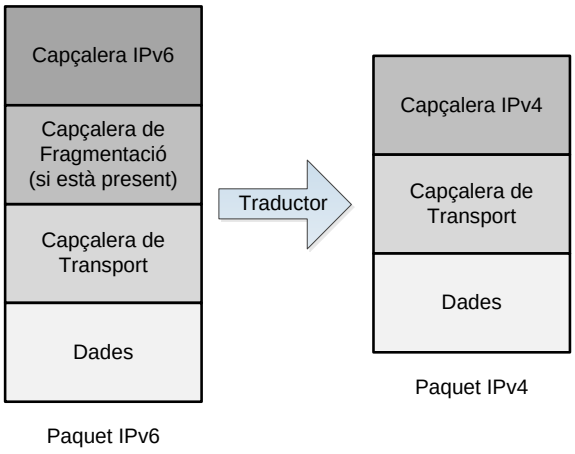



**Fig. 1.10** Mecanisme de traducció IPv6 a IPv4.

Les tècniques de traducció més emprades són: *Stateless IP/ICMP Translation; DNS64; NAT64; Stateless NAT64; Translator (TRT); NAT-PT* (el·liminat RFC 4966).

## 1.5. Resum del protocol IPv6

Les característiques principals d'IPv6 que el diferencien d'IPv4 són:

- L'espai d'adreces és més gran que a IPv4, disposa de $2^{128}$ adreces.
- Protocol escalable.
- Paquets IP eficients i extensibles, sense que hi hagi fragmentació als encaminadors i amb una capçalera de mida fixe que agilitza el seu processat pels routers.

- Introdueix Qualitat de Servei (QoS) i Classe de Servei (CoS).
- Millor suport per opcions addicionals:
    - Les capçaleres opcionals no estan codificades a la capçalera, sinó en el cos del paquet IP.
    - Permet introduir noves opcions en el futur.
- Nous tipus d'adreces per millorar l'eficiència de certes comunicacions.
    - Adreces multicast: Enviament d'un mateix paquet a un grup de receptors creant un únic flux de dades.
    - Adreces anycast: Enviament d'un paquet a un receptor dins d'un grup.
- Les adreces tenen àmbit (Global, Local i Enllaç).
- Encaminament més eficient en el troncal de la xarxa a causa de l'adreçament jeràrquic basat en prefixes.
- Possibilitat d'autoconfiguració d'adreces (*Plug & Play*). Permet la connexió de dispositius a la xarxa sense necessitat de configurar els seus paràmetres de xarxa.
- Seguretat intrínseca en el nucli del protocol (IPsec).
- Característiques de mobilitat.

Existeixen tres tècniques de migració i coexistència de xarxes IPv4 a IPv6:

- Doble Pila, permet la coexistència d'IPv4 i d'IPv6 en els mateix dispositiu i xarxes.
- Túnels IPv6 sobre IPv4, encapsulat de paquets IPv6 dins de paquets IPv4.
- Mecanismes de traducció d'adreces, permeten la comunicació entre dispositius que són només IPv6 i dispositius que són només IPv4.

# CAPÍTOL 2. ANÀLISIS DE LA XARXA DEL CTTC

En aquest capítol analitzem l'estat actual de la xarxa del CTTC per a veure quina és la seva topologia, quins són els elements que la formen, com estan configurats i quin adreçament utilitzen. Avaluem quins són els requeriments perquè aquesta pugui suportar de forma nativa el protocol IPv6 i, a més a més, que coexisteixi amb IPv4. De l'estudi obtenim un seguit d'accions a emprendre per tal d'implementar IPv6 a la xarxa del CTTC.

## 2.1. Xarxa del CTTC

La xarxa de dades del CTTC (veure figura **Fig. 2.1**) està formada per dos *Firewalls* Cisco ASA 5510 en alta disponibilitat, de forma que siguin resistents en cas de fallada. Per darrera del *Firewall* hi han dos *switchos* (SUN) Cisco WS-C3750G-12S-E en stack que formen el *core* de la xarxa. Aquets equips actuen d'encaminadors.

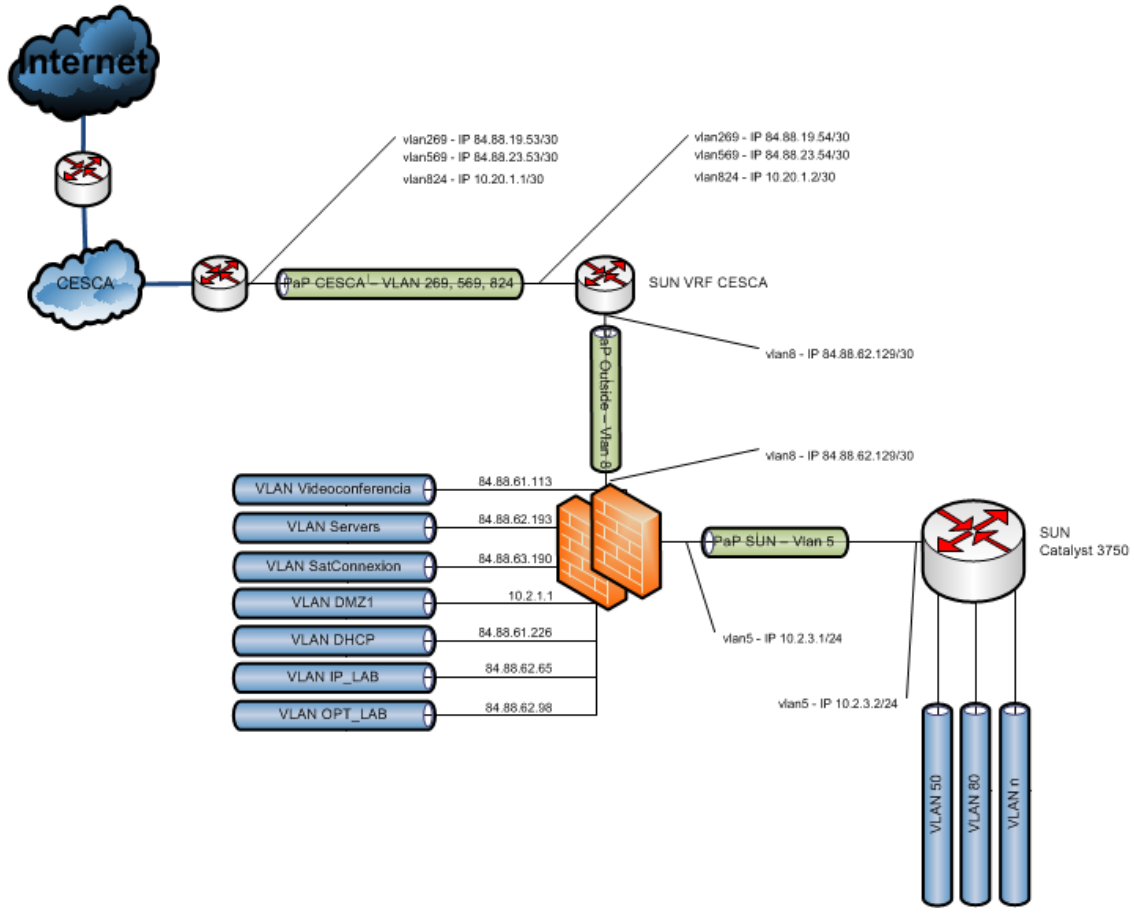



**Fig. 2.1** Esquema lògic de la xarxa de dades del CTTC

Les principals xarxes són l'accés a Internet proporcionades pel CESCA[2] (des del 2013 CSUC[3]) de forma nativa per mitja de dues VLANs amb rutes redundades obtingudes per BGP a 100 Mbps, i la xarxa de servidors entre d'altres.

La xarxa del CTTC està segmentada en VLANs. Les VLANs de connexió externes són cap a un node del Campus Nord (principal) i cap a un node Telvent (secundari) (veure figura **Fig. 2.2**). També disposa d'una connexió a UPCNET a través de fibra (2 VLANs) a 1Gbps.

A la figura **Fig F.1 de l'Annex F. Anàlisis de la xarxa del CTTC** podem observar la topologia de la xarxa del CTTC. Bàsicament a cada planta hi ha commutadors que serveixen per a la connexió d'usuaris i *Access Points*. Aquests equips són NEPTUNE, URANUS i SATURN, són commutadors que treballen a nivell 3 de la capa OSI [26] i SW-R1-1 i SW-2-PEIX-N que donen connexió a usuaris.

JUPITER dona connexió als laboratoris i alguns usuaris. Els equips MARS, TRITON, DEIMOS i VENUS, són emprats per les connexions dels centres de càlcul (CPDs) i PANDORA és un equip per a connexions de prova.

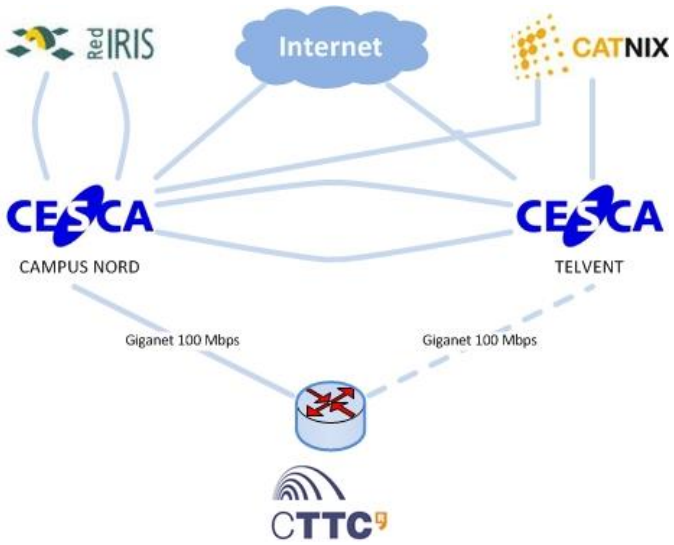



**Fig. 2.2** Topologia de la Anella Científica i el CTTC

El CTTC disposa de tres rangs d'adreces IPv4 públiques de classe C, no es fa NAT:

- 84.88.61.0/24
- 84.88.62.0/24
- 84.88.63.0/24

[2] **CESCA** (Centre de Serveis Científics i Acadèmics de Catalunya) és el proveïdor d'accés a internet per a les institucions de l'Anella Científica. www.cesca.cat
[3] **CSUC** (Consorci de Serveis Universitaris de Catalunya) és el proveïdor d'accés a internet per a les institucions de l'Anella Científica. www.csuc.cat

## 2.2. Anàlisis del suport d'IPv6 a la xarxa del CTTC

L'objectiu d'aquest anàlisis és la implementació d'una xarxa que funcioni nativament amb IPv6 i que en la xarxa del CTTC coexisteixin IPv4 i IPv6 utilitzant la tècnica de doble pila (*dual stack*). D'aquesta forma es dona suport IPv6 als usuaris de la Institució sense perdre la connectivitat IPv4.

L'ús de la tècnica *dual stack* té el requeriment que els equips que participen en la connexió han de tenir habilitat el suport per IPv6. A la **Taula F.1 de l'Annex F.2** es presenta un anàlisis dels equips existents a la xarxa del CTTC amb les accions necessaries que s'han d'aplicar perquè tinguin suport IPv6.

De l'anàlisi observem que el *core* de la xarxa SUN, encarregat del *routing*, s'ha d'actualitzar la versió del sistema operatiu (IOS) perquè pugui implementar IPv6.

Els equips que hi ha al centre de càlcul de la planta 2 MARS, TRITON i DEIMOS, i JUPITER no disposen de cap actualització de la IOS per implantar IPv6. Cal destacar que aquests equips s'utilitzen com a commutadors (*switch*), és a dir, funcionen a nivell 2 de la capa OSI i podrien ser utilitzats amb les mateixes funcionalitats amb IPv6. El motiu de la seva substitució és que deixen de tenir suport de Cisco i arriben a la fi del seu cicle de vida [27]. L'equip PANDORA té el mateix problema que els anteriors, però al ser un equip de connexions de prova, no es programa cap actuació.

Els commutadors de planta NEPTUNE, URANUS i SATURN, i VENUS no accepten IPv6 en la versió de la IOS instal·lada. Seria necessari una actualització d'aquesta per a poder suportar el nou protocol.

A la **Taula 2.1** observem un resum de les acción a realitzar sobre els equips de xarxa per tal de que donguin suport a IPv6.

**Taula 2.1** Resum de les accions a realitzar sobre els equips de xarxa perquè la xarxa del CTTC suporti IPv6

| Acció a realitzar | Equips |
|---|---|
| Actualitzar IOS | Neptune, Saturn, Sun1, Sun2, Uranus, Venus |
| Substituïr/Reutilitzar | Deimos, Jupiter, Mars, Pandora, Triton |
| No requereix cap canvi | Firewall1, Firewall2, sw-r2-peix-n, sw-r1-1 |

# CAPÍTOL 3. DISSENY I IMPLEMENTACIÓ DE LA XARXA IPv6

En aquest capítol s'explica el procés d'implementació d'IPv6 al CTTC arran de l'anàlisi fet al capítol anterior. Presentem l'equipament que conforma la xarxa amb suport IPv6, alguns d'aquets equips són nous i substitueixen al mencionats anteriorment. També expliquem el procés de petició del nou adreçament i realitzem un pla de distribució de les adreces IPv6 al CTTC. Mostrem el procés d'activació de la connectivitat IPv6 al centre amb la configuració i actualització dels equips implicats. Durant la implementació sorgeixen incidències que resoldrem en aquest capítol. Decidim implementar alguns serveis basics amb suport IPv6, el servei DNS i web. Per últim, exposem un seguit de recomanacions a tenir en compte per la migració/coexistència del protocol IPv4 i IPv6 fruit d'aquesta implementació i presentem un resum dels passos seguits en el procés d'implantació d'IPv6.

## 3.1 Topologia proposada de la xarxa del CTTC

A l'apartat 2.2 observem que hi ha una sèrie d'equips a substituir. El motiu d'aquest canvi no és principalment la implementació d'IPv6, sinó que queden obsolets. No entrem en gaires detalls al respecte ja que no és la finalitat d'aquest projecte.

Per l'elecció del nou equipament s'ha tingut en compte que tinguin suport IPv6. Actualment tots els equips de xarxa ja ho inclouen. Els principals avantatges [28] de la substitució dels tres primers equips de la **Taula 3.1**, que estan ubicats en el mateix CPD són:

- Redundància i manteniment: es poden *stackar*, de manera que els 3 commutadors es veuen i es controlen com un de sol. En cas de fallada d'un d'ells, els restants poden assumir les seves funcions.
- Velocitat: els seus ports treballen a *GigaEthernet*. Comunicacions entre ells a 20Gbps (*FlexStack protocol*).

L'equip JUPITER es substitueix per un de similars prestacions amb els ports a *GigaEthernet*. Es treballa amb equips Cisco ja que hi ha una certa experiència acumulada al centre amb aquest model d'equipaments, Cisco ofereix un gran suport i hi ha molta documentació disponible. En la figura **Fig. F.2** de l'**Annex F.3** podem observar la topologia proposada de la xarxa del CTTC.

**Taula 3.1** Equipament proposat.

| Nom d'equip | Equip de xarxa a substituir | Equip de xarxa proposat | Nom d'equip |
|---|---|---|---|
| TRITON | Cisco WS-C2950G-24-EI | Cisco WS-C2960S-24TS-L | HIPERION |

| | | | |
|---|---|---|---|
| MARS | Cisco WS-C2970G-24TS-E | Cisco WS-C2960S-24TS-L | |
| DEIMOS | Cisco WS-C3550-24-SMI | Cisco WS-C2960S-24TS-L | |
| JUPITER | Cisco WS-C2970G-24TS-E | Cisco WS-C2960S-24TC-L | GANIMEDES |

## 3.2 Petició del rang d'adreces IPv6

El proveïdor d'accés a internet del CTTC és el CESCA, tal i com em esmentat en l'apartat 2.1. Aquest actua coma registre local (LIR) i assigna blocs d'adreces IP de RIPE NCC (Europa), registre regional (RIR) al que pertany.

El CESCA és l'encarregat de tramitar la sol·licitud amb l'organisme RIPE NCC. Aquest assigna un rang d'adreces IPv6 /48 per a les institucions connectades a l'Anella Científica. Per a realitzar la sol·licitud, cal complimentar els formularis disponibles al web del CESCA [29]. Veure **Annex G. Petició del rang d'adreces IPv6**.

En el procés d'assignació es descobreix que el CTTC té un rang d'adreces IPv6 assignat, el 2001:720:b1c::/48 que pertany a RedIRIS i va ser assignat el gener del 2003 per realitzar un túnel amb el CESCA. Es retorna aquest rang a RedIRIS perquè no s'utilitza i es demana un rang d'adreces que pertanyi al CESCA. Aquest ens assigna el rang d'adreces IPv6 **2001:40b0:7C22::/48** al desembre del 2011.

## 3.3 Adreçament

El prefix 2001:40b0:7c22::/48 implica que el CTTC disposa de 65536 subxarxes /64 [30], que representen un total de $2^{80}$ (1208925819614629174706176) adreces IPv6.

Per a realitzar la distribució del rang d'adreces i el disseny dels nivells de xarxa, ens basarem en el memoràndums d'assignació d'adreces de la IETF [31][32][33]. En la **Taula 3.2** observem la distribució del rang IPv6 al CTTC.

Les principals recomanacions que s'han seguit són:

- Evitar la sensació que s'han d'emprar tècniques de conservació d'adreces (pe: Translació d'adreces IPv6 a IPv6).
- Per a realitzar subxarxes es recomana assignar més d'un /64, per cobrir les necessitats futures dels llocs de tenir múltiples subxarxes.
- Facilitar l'administració assignant prefixes /48, /56 i /64.
- Ús de prefixos /127 entre enllaços punt-a-punt (*routers*).
- L'ús d'un prefix de xarxa diferent a un /64 trencarà moltes característiques d'IPv6, com autoconfiguració, descobriment de veïns (ND), parts de MIPv6, entre d'altres.

- L'assignació d'un prefix més curt que un /64. Normalment es considera una mala pràctica.

**Taula 3.2** Distribució del rang d'adreces IPv6 al CTTC.

| | CTTC | Divisions R+D | Subxarxes | Enllaços punt-a-punt | Interfícies |
|---|---|---|---|---|---|
| Prefix de xarxa | /48 | /56 | /64 | /127 | /128 |

S'ha considerat en el disseny dels nivells de xarxa:

- Creació de 4 subxarxes /56 per a les 4 divisions de recerca del centre
  - Cada àrea disposarà de 256 /64.
- Creació de 2 subxarxes /56 per a ús del Centre de Serveis Informàtics (CSI),
  - Integració de les subxarxes existents. Es redissenyarà la numeració actual de les VLANs per facilitar la gestió en IPv6.
  - Creació de 10 subxarxes /64 d'inici per fer noves assignacions dintre del rang del CSI.
  - Creació de 10 subxarxes /127 per fer noves assignacions dins del rang del CSI.

A l'**Annex H** podem observar la distribució d'adreces al CTTC.

L'assignació d'adreces *unicast* globals als dispositius es realitzarà manualment. Per simplificar en una primera fase, es deixa per a futures línies la implementació de l'autoconfiguració (apartat 1.3.5).

## 3.4 Procés d'activació de la connectivitat IPv6 i configuració dels equips

Un cop obtingut el rang d'adreces IPv6, es procedeix a activar la connectivitat IPv6 del CTTC. Per activar IPv6, primerament es procedeix a l'actualització de la IOS dels equips necessaris segons l'apartat 2.2 amb l'ús de la comana **3.1** i, seguidament, s'habilita el *template "dual-ipv4-and-ipv6"* en els equips per tal de que coexisteixin IPv4 i IPv6 utilitzant la tècnica de doble pila (comana **3.2**). En la **Taula 3.3** observem els *templates* activats a cada equip de xarxa del CTTC per establir la connectivitat IPv6.

```
#archive download-sw /leave-old-sw tftp://IP/nom_IOS
```
**(3.1)**

```
#sdm prefer dual-ipv4-and-ipv6 {default/routing/vlan}
```
**(3.2)**

**Taula 3.3** *Templates* activats als equips de xarxa del CTTC per habilitar IPv6.

| Nom d'equip | SUN | NEPTUNE | URANUS | SATURN | VENUS | SW-R1-1 | SW-2-PEIX-N | GANIMEDES | HIPERION |
|---|---|---|---|---|---|---|---|---|---|
| *Template* | *aggregator IPv4 and IPv6 routing* | *desktop IPv4 and IPv6 default* | | | *dual IPv4 and IPv6 default* | | | | *default* |

El CESCA crea als seus encaminadors dues VLANs IPv6 per establir connexió amb el CTTC, una al node del Campus Nord (CN) i una altre al node Telvent (TV):

- vlan 479 (CN): 2001:40B0:1::F0A1/125
- vlan 779 (TV): 2001:40B0:1::F4A1/125

Observem que un cop actualitzat SUN, no podem activar IPv6 amb VRF [34] en aquest equip. Al *stack* de *switchos* SUN, que fan la funció d'encaminador, tenim una instància amb VRF amb la que realitzem BGP-4 [35] i el CESCA ens fa arribar les IPv4 i les IPv6 que tenim assignades. La versió de la IOS instal·lada i les altres versions per aquest equip, no suporten aquesta funcionalitat. Per tant, no hi ha possibilitat d'implementar IPv6 amb VRF [36] i BGP-4.

La solució proposada consisteix en portar les VLANs IPv6 del CESCA al *firewall*, darrera del *router* (SUN) i definir en aquest equip les interfícies. L'inconvenient d'aquesta solució és que impedeix la possibilitat d'activar IPv6 amb encaminament dinàmic utilitzant BGP, per les raons ja mencionades i perquè el *firewall* no suporta BGP [37].

La connectivitat IPv6 proporcionada pel CESCA es realitza de forma nativa per les mateixes línies i amb els mateixos cabdals disponibles que per la connexió a Internet per IPv4. El Cesca habilita les rutes estàtiques. El tràfic anirà cap al node del Campus Nord per la connexió IPv6. S'implementaria de la següent forma, figura **Fig 3.1**:

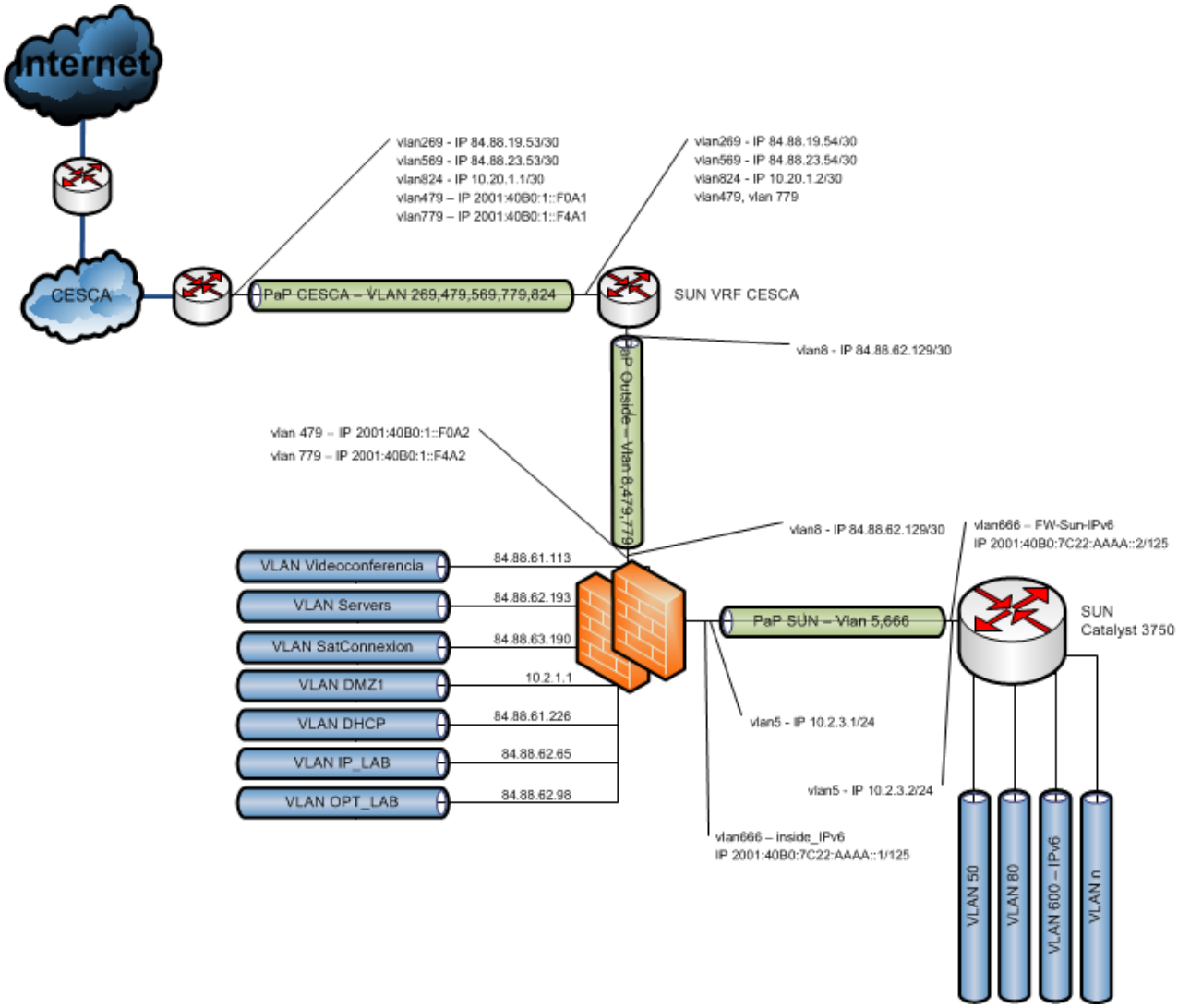



**Fig. 3.1** Esquema lògic de la xarxa de dades del CTTC amb connectivitat IPv4 i IPv6

A SUN (Nivell 2 capa OSI): Es permet que les VLANs 479 I 779 (enllaç IPv6 cap al Cesca) passin cap al *firewall* (comana **3.3**) tal i com s'observa en la figura **Fig. 3.2.**

```
interface Port-channel8
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779

interface Port-channel9
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779

interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779

interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779

interface GigabitEthernet2/0/2
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
```

```
interface GigabitEthernet2/0/4
 switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
```

**(3.3)**

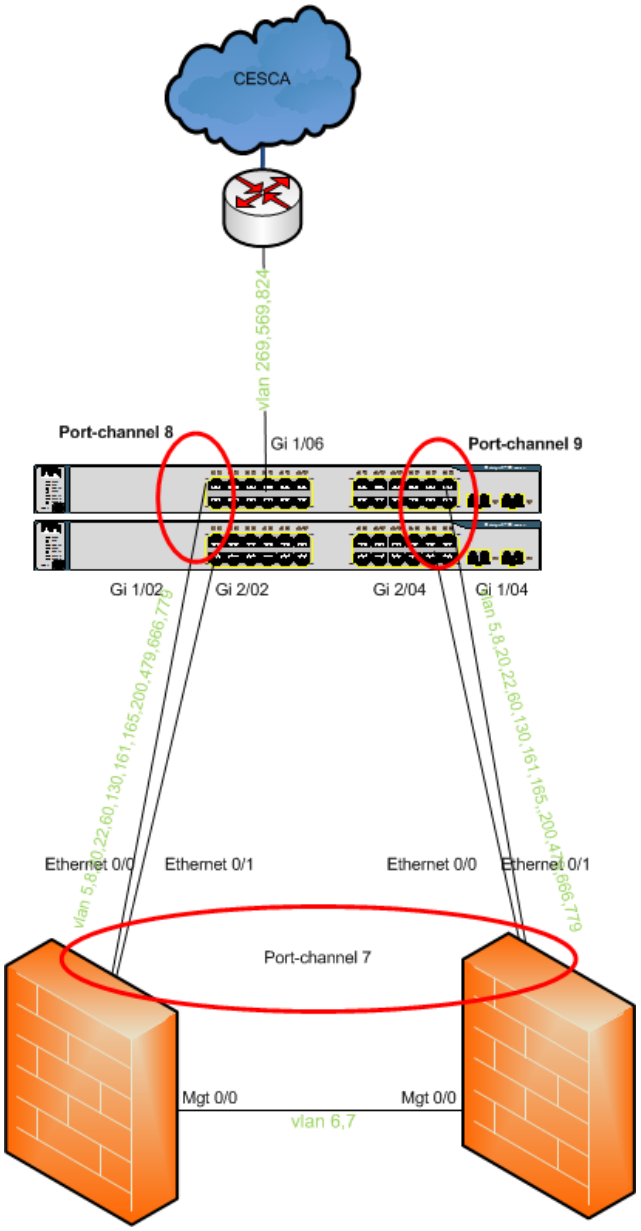



**Fig. 3.2** Esquema físic del *firewall* CTTC

Al *Firewall* es creen les VLANs (nivell 2 de la capa OSI) del Cesca i es defineixen les interfícies (nivell 3) amb les IPv6 corresponents (comana **3.4**).

```
interface Port-channel7.479
 description Cesca_IPv6
 vlan 479
 nameif Cesca_IPv6
 security-level 5
 no ip address
```

```
 ipv6 address 2001:40B0:1::F0A2/125
 ipv6 enable


interface Port-channel7.779
 description Telvent_IPv6
 vlan 779
 nameif Telvent_IPv6
 security-level 5
 no ip address
 ipv6 address 2001:40b0:1::f4a2/125
```
**(3.4)**

A SUN, en un primer moment per prudència, es crea la VLAN 666 que té la funció d'enllaçar amb IPv6 aquest equip amb el *Firewall.* D'aquesta forma són independents les dues vlans. Finalment s'aprofita la VLAN 5 que enllaça aquests equips amb IPv4 per enllaçar-los també amb IPv6 (configuració **(3.5)**).

```
interface Vlan5
 description enllac_firewall
 ip address 10.2.3.2 255.255.255.0
 ipv6 address  2001:40B0:7C22:AAAA::2/125
 ipv6 enable
```
**(3.5)**

Modifiquem al *firewall* la interfície corresponent amb IPv6 de la VLAN 5 (nivell 3 capa OSI) (comana **(3.6)**).

```
interface Port-channel7.5
 vlan 5
 nameif inside
 security-level 100
 ip address 10.2.3.1 255.255.255.0 standby 10.2.3.3
 ipv6 address 2001:40B0:7C22:AAAA::1/125
 ipv6 enable
```
**(3.6)**

A SUN (Nivell 2): Comprovem que la VLAN 5 passi entre SUN i el *firewall* (comana (**3.7**)). Veure figura **Fig. 3.1.**

```
interface Port-channel8
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
interface Port-channel9
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
interface GigabitEthernet2/0/2
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
interface GigabitEthernet2/0/4
switchport trunk allowed vlan 5,8,20,22,60,130,161,165,200,479,779
```
**(3.7)**

A SUN (Nivell 3), afegim la ruta per defecte, el *gateway* és el *firewall* (comana (**3.8**)).

```
ipv6 route ::/0 2001:40B0:7C22:AAAA::1
```
**(3.8)**

Creem una VLAN de proves (VLAN 600). La creem a nivell 2 i 3 a SUN (comana (**3.9**)). Al *firewall* afegim la ruta perquè pugui accedir a la subxarxa de la VLAN 600 (comana (**3.10**)). En aquest cas el *gateway* és SUN.

```
vlan 600
interface Vlan600
 description IPv6
 no ip address
 ipv6 address 2001:40B0:7C22:1::1/64
 ipv6 enable
```
**(3.9)**

```
ipv6 route inside_IPv6 2001:40B0:7C22:1::1/64 2001:40B0:7C22:AAAA::2
```
**(3.10)**

Al *firewall* s'activen una sèrie de regles d'accés entrant IPv6 a les interfícies, per tal de permetre un determinat tràfic de dades. Veure **Annex I. Regles d'accés entrant IPv6 del *Firewall***.

## 3.5 Incidències en l'activació

- Descripció:

S'ha detectat que la connexió IPv6 cap a Internet es talla periòdicament, provocant que les màquines no puguin sortir a Internet.

- Detecció del problema:

Des de SUN no s'obté un *ping* satisfactori al *gateway* del Cesca (Campus Nord) (comana (**3.11**)).

```
Sun#ping 2001:40b0:1::f0a1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:40B0:1::F0A1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```
**(3.11)**

El problema apareix degut a que la taula IPv6 *Neighbor Discovery Cache (apartat 1.3.4)*, que s'omple de forma dinàmica, no incorpora la ruta al *gateway* del Cesca, a no ser que s'iniciï el *ping* cap al *gateway* del Cesca des del propi *firewall*. D'aquesta forma el *ping* des de SUN fracassa si l'entrada de la taula dinàmica no hi és, i torna a funcionar quan realitzem un *ping* des del *firewall*, ja que es torna a omplir (comana (**3.12**)).

```
fw# show ipv6 neighbor
```

```
IPv6 Address                              Age Link-layer Addr State
Interface
2001:40b0:1::f0a1                           0 -               INCMP
Cesca_IPv6
fe80::e25f:b9ff:fe6d:b802                   0 e05f.b96d.b802  STALE
Cesca_IPv6
fe80::207:7dff:fe9a:169e                    0 0007.7d9a.169e  REACH
servers
fe80::213:c4ff:fe3e:39c1                    0 0013.c43e.39c1  STALE
inside                                                        (3.12)
```

- Solució:

Per evitar el problema, s'afegeix una entrada estàtica dins la taula IPv6 Neighbor Discovery Cache, d'aquesta manera l'entrada mai s'esborra i no es perd la connectivitat (comana (**3.13**) i (**3.14**)).

```
fw(config)# ipv6 neighbor 2001:40b0:1::f0a1 Cesca_IPv6 e05f.b96d.b802
fw# show ipv6 neighbor
IPv6 Address                              Age Link-layer Addr State
Interface
2001:40b0:1::f0a1                           - e05f.b96d.b802  REACH
Cesca_IPv6
fe80::215:17ff:fea8:1f1c                    0 0015.17a8.1f1c  DELAY
servers
2001:40b0:7c22:6020:215:17ff:fea8:1f1c      0 0015.17a8.1f1c  REACH
servers                                                       (3.13)
```

```
Sun#ping 2001:40b0:1::f0a1
Type escape sequence to abort.Sending 5, 100-byte ICMP Echos to
2001:40B0:1::F0A1, timeout is 2 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms
                                                              (3.14)
```

- Possibles Inconvenients de la solució:

El problema d'aquesta solució és que si per la part del Cesca canvien l'adreça MAC de l'encaminador, això provocarà un tall que s'haurà de corregir afegint la nova adreça MAC.

## 3.6 Serveis implementats amb IPv6

Decidim implementar alguns serveis amb suport IPv6 al CTTC per tenir desenvolupat una primera integració, el DNS i el servidor web.

El protocol de DNS "Sistema de Noms de Domini" (*Domain Name Server*) tradueix noms de domini a adreces de xarxa tant d'IPv4 com d'IPv6. És un mecanisme fonamental a Internet. El servidor DNS estarà configurat en doble pila, així podrà resoldre peticions DNS ambdós protocols. Assegurem la compatibilitat amb els servidors ja existents. Veure **Annex J.1 Servei DNS**.

Activem IPv6 al servidor web on s'allotja el web de CTTC per tenir visibilitat exterior amb aquest. El servidor web configurat amb Apache funciona amb la doble pila de protocols. Veure **Annex J.2 Servei web**.

## 3.7 Recomanacions a tenir en compte

Hi ha diversos aspectes relacionats amb la migració/coexistència del protocol IPv4 i IPv6 a tenir en compte. S'ha de tenir en consideració que aquest procés serà gradual, conviuran els dos protocols durant uns quants anys. Les recomanacions següents són el resultat de la implementació realitzada al CTTC. Per tant, es pot donar el cas que no siguin útils de forma genèrica, ja que es tracta d'un escenari en concret.

- És crucial realitzar un estudi de la xarxa i de l'equipament que la forma, per veure les necessitats i les particularitats que pot tenir.
- Escollir el mecanisme de transició/coexistència (veure capítol 1.4) més indicat en funció de l'escenari en qüestió. En el cas del CTTC s'ha escollit implementar IPv6 per mitjà del mecanisme de doble pila, perquè l'equipament ho permet. No introdueix latència en comparació als túnels i permet la coexistència d'ambdós protocols.
- Planificar detalladament les actualitzacions de SO dels equips de xarxa. Tenir en compte que l'actualització no implica necessàriament l'activació d'IPv6. Pot requerir l'ús d'altres funcions per activar el nou protocol. Aquest punt és crític perquè implica talls de xarxa.
- Seguir les recomanacions de la IETF alhora de realitzar la distribució de l'adreçament, per tal d'evitar una xarxa poc organitzada i amb limitacions (veure apartat 3.3 Adreçament).

## 3.8 Resum de la implantació d'IPv6

Podem resumir la implementació de la xarxa IPv6 al CTTC de la següent forma:

- L'activació d'IPv6 provoca la substitució d'alguns equips per altres que tinguin suport IPv6.
- El CESCA ens assigna el rang d'adreces IPv6 2001:40b0:7c22::/48.
    - Això suposa 256 subxarxes /56 o 65536 subxarxes /64 i un total de $2^{80}$ adreces IPv6.
- El disseny de l'adreçament, s'ha realitzat assignant subxarxes /56 als departaments. Això suposa 256 subxarxes /64.
- Habilitem el template *dual-ipv4-and-ipv6* als equips de xarxa per habilitar la doble pila de protocols.
- Configurem la connectivitat IPv6 al firewall, perquè el nucli de la xarxa (Sun) no suporta IPv6 amb VRF i BGP-4.
- S'implementen els serveis bàsics del DNS i web amb suport IPv6.

# CAPÍTOL 4. BANC DE PROVES I RESULTATS

Un cop implementat l'adreçament IPv6 al CTTC plantegem un sèrie de proves per avaluar quin és l'efecte de la implementació de l'IPv6 a un escenari IPv4 amb el rendiment del maquinari. Compararem el rendiment d'ambdós protocols a la xarxa del CTTC per mitja d'una sèrie de paràmetres que mesuren l'experiència a nivell d'usuari com el *Round Trip Time*, el *throughtput* i el *Time To First Byte*.

Plantegem un escenari general de proves i en funció del test que realitzem, escollirem una porció d'aquest escenari. A l'**Annex K. Escenari Banc de Proves** podem veure la figura **Fig. K1** amb les màquines que el configuren (jordiserver, jordiserver2, pcjescoda, pc i jordi1) i a la **Taula K.1** les seves característiques a nivell de sistema operatiu i recursos.

També intervenen tres equips de xarxa Nayade (Cisco Catalyst WS-2960G-24TT-L) i Hiperion que actuen com a *switchos* i Helium (Cisco Catalyst WS-C3850-12S) que actua com a *router* amb moltes interfícies. Les màquines estan connectades entre elles a *Gigabit Ethernet*, excepte pcjescoda i jordi1 amb Nayade que ho fan a *Fast Ethernet*. Els enllaços no són dedicats, comparteixen el tràfic de la xarxa del CTTC. Aproximadament, el volum de tràfic que hi ha a la xarxa entre les 17h i 18h, hora de realització dels tests, és d'uns 21Mbps.

## 4.1 Round Trip Time

L'objectiu de la prova és comparar el temps d'anada i tornada RTT[1] *(round-trip time*) en funció del protocol utilitzat. Així podem observar quina és la latència a la xarxa i com influeix en aquest valor l'ús d'IPv6. Agafarem mostres d'aquest paràmetre com a indicador de QoS experimentada per l'usuari a la xarxa interna i a l'exterior de CTTC, així també podem observar com influeix la distància. Paral·lelament realitzarem mesures de memòria utilitzada i consum de cpu dels tests per comparar quin és el cost de recursos en funció del protocol utilitzat.

### 4.1.1 Escenari

En aquest test configurem dues màquines pcjescoda, jordi1 i una màquina externa al CTTC (google.com) per comparar el paràmetre RTT en ambdós protocols, tal i com observem en la figura **Fig. 4.1**. Les màquines pcjescoda i jordi1 tenen configurat l'adreçament amb doble pila. També intervenen els equips de xarxa Nayade i Helium.

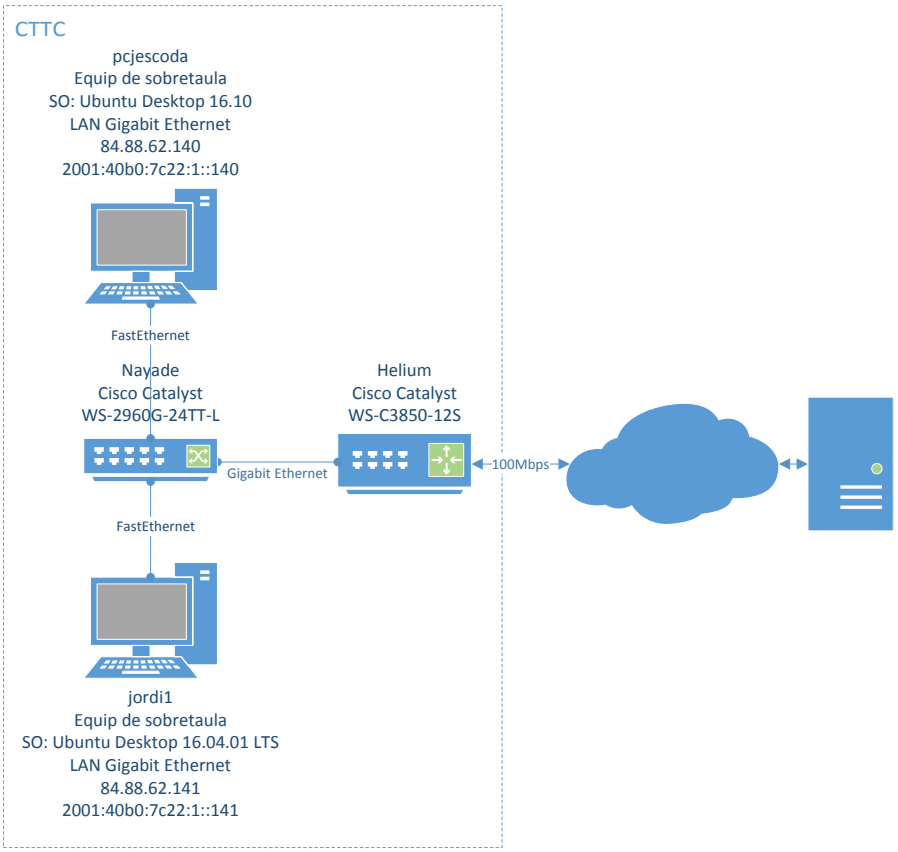



**Fig. 4.1** Escenari RTT.

El valor del paràmetre RTT el mesurem a través d'un script que executem a pcjescoda pingtest.sh (veure **Annex L.1 Script càlcul Round Trip Time**) al que l'hi passem com a paràmetre el protocol que volem mesurar (4 o 6) i l'adreça IP de l'altre màquina destí (jordi1 o google.com). L'script utilitza l'eina *ping* que mesura el temps d'anada i tornada dels paquets enviats entre un origen i un destí.

L'script executa un *ping* que envia 4 paquets seguits successivament durant una hora per tenir una finestra de mostres representativa. Guardem a l'arxiu de resultats el valor de la mitjana del RTT que presenta.

Paral·lelament, l'script calcula els paràmetres de rendiment d'ús de memòria i cpu de la màquina pcjescoda d'on s'executa l'script per tal d'avaluar com afecta l'ús d'un o altre protocol. Utilitzem l'eina *free* de Linux per obtenir la quantitat de memòria utilitzada i l'eina *top* de Linux per obtenir l'ús de cpu.

Amb el càlcul del paràmetre contra google.com podrem observar com influeix la localització i el nombre de salts en la latència de la xarxa.

### 4.1.2 Resultats i conclusions

Realitzem un test a la xarxa interna del CTTC des de la màquina pcjescoda a jordi1. Els resultats que obtenim a les figures **Fig. 4.2** i **Fig. 4.3** mostren que el RTT per IPv6 és lleugerament més gran que el RTT per IPv4. El valor mitjà de RTT per IPv6 és 326µs i per IPv4 307µs. Aquesta diferència la podríem explicar a nivell de la xarxa del CTTC relacionant-la amb el cost a nivell de recursos del processat d'un paquet IPv6 respecte un IPv4. En consum mitja de memòria durant el test és més gran en IPv6 que en IPv4. Els valors mitjans són 14,71% i 14,68% respectivament. A nivell de consum de CPU és insignificant amb els dos protocols.

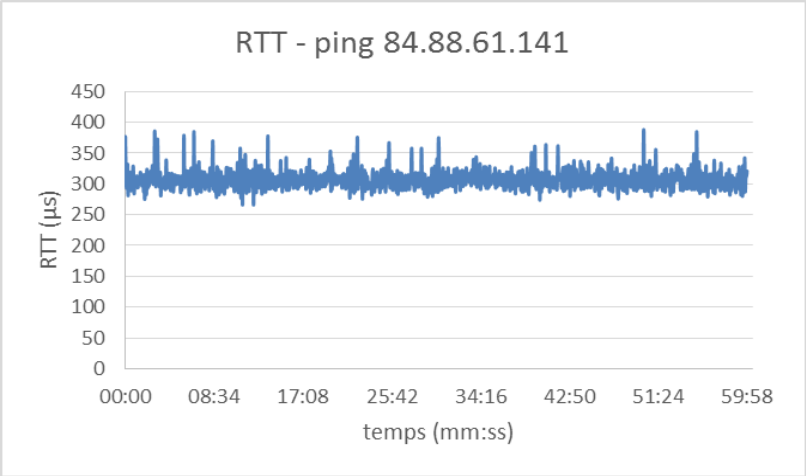



**Fig. 4.2** RTT IPv4

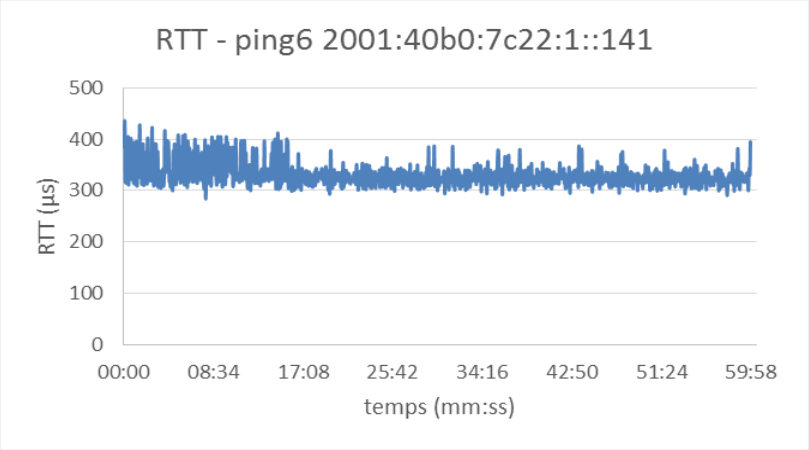



**Fig. 4.3** RTT IPv6

Realitzem el mateix test contra una màquina a l'exterior del CTTC, google.com. Els resultats que es mostren en les figures **Fig. 4.4** i **Fig. 4.5** mostren que el

RTT per IPv6 és més gran que per IPv4 igual que succeïa amb la prova a l'interior del CTTC. El valor mitja de RTT per IPv6 és 14,840ms i per IPv4 14,470 ms. Una altre explicació per justificar aquesta diferència podríem trobar-la lligada a que el nombre de nodes disponibles a IPv6 és inferior que a IPv4 i la distància entre els nodes és superior. Això implica que el RTT augmenti. Si mirem el nombre de salts que tenim des de la màquina pcjescoda a google.com amb IPv6 i IPv4, veiem que amb IPv6 és menor. Per mesurar el nombre de salts ho fem amb l'eina *traceroute*, com veiem en la figura **Fig.4.6**.

```
root@pcjescoda:~# traceroute -m 30 216.58.201.142
traceroute to 216.58.201.142 (216.58.201.142), 30 hops max
  1   84.88.62.137  2,065ms  2,090ms  2,118ms
  2   84.88.62.129  2,354ms  2,017ms  2,144ms
  3   84.88.19.53  1,899ms  3,570ms  4,991ms
  4   130.206.211.69  6,565ms  6,055ms  6,526ms
  5   130.206.245.90  13,029ms  13,220ms  12,999ms
  6   130.206.255.2  13,281ms  12,698ms  12,430ms
  7   72.14.235.18  13,463ms  12,958ms  12,938ms
  8   216.239.40.217  13,096ms  13,056ms  12,854ms
  9   216.58.201.142  13,151ms  12,800ms  12,745ms

root@pcjescoda:~# traceroute6 -m 30 2a00:1450:4003:804::200e
traceroute      to      2a00:1450:4003:804::200e      (2a00:1450:4003:804::200e)      from
2001:40b0:7c22:1::140, 30 hops max, 24 byte packets
 1  gateway (2001:40b0:7c22:1::1)  2,238 ms  1,989 ms  2,19 ms
 2  anella-cttc6.csuc.cat (2001:40b0:1::f0a1)  3,235 ms  3,083 ms  4,05 ms
 3  2001:720:1000::1:11 (2001:720:1000::1:11)  6,608 ms  6,844 ms  6,7 ms
 4  2001:720::245:92 (2001:720::245:92)  12,801 ms  12,732 ms  15,568 ms
 5  google-router.red.rediris.es (2001:720:400::1:2)  12,863 ms  12,667 ms  12,748 ms
 6  2001:4860::1:0:79db (2001:4860::1:0:79db)  13,505 ms  17,627 ms  13,677 ms
 7  2001:4860:0:1::f17 (2001:4860:0:1::f17)  13,338 ms  13,042 ms  13,094 ms
 8  mad06s25-in-x0e.1e100.net (2a00:1450:4003:804::200e)  13,146 ms  12,988 ms  12,909
ms
```

**Fig. 4.6** *Traceroute* cap a google.com amb IPv4 i IPv6.

A nivell del cost a nivell de recursos el consum mitja de memòria durant el test és més gran a IPv6 que a IPv4. Els valors mitjos són de 15,09% i 14,84% respectivament. El consum de CPU és insignificant amb els dos protocols.

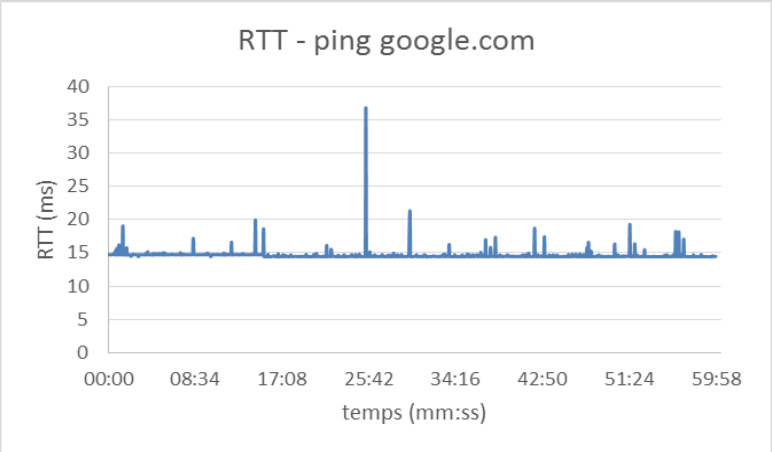



**Fig. 4.4** RTT IPv4 google.com.

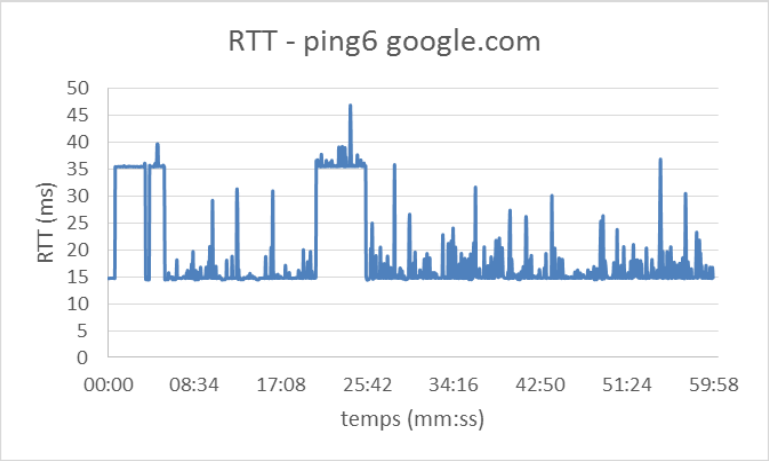



**Fig. 4.5** RTT IPv6 google.com.

## 4.2 Throughtput

L'objectiu de la prova és comparar la velocitat de transport de dades, el *throughput*[4], en funció del protocol utilitzat. Paral·lelament, realitzarem tests de rendiment dels equips de xarxa per observar com els afecta l'ús d'un protocol o altre i analitzarem el comportament del *throughput* en diferents SO.

### 4.2.1 Escenari

En aquest test intervenen quatre màquines jordiserver, jordiserver2, pc i pcjescoda. També intervenen tres equips de xarxa Nayade, Hiperion i Helium tal i com es pot observar en la figura **Fig. 4.7**.

[4]**Throughput**: velocitat real de transport de dades a través d'una xarxa telemàtica. Es mesura en Mbit/s i sempre serà inferior a l'ample de banda o bandwidth

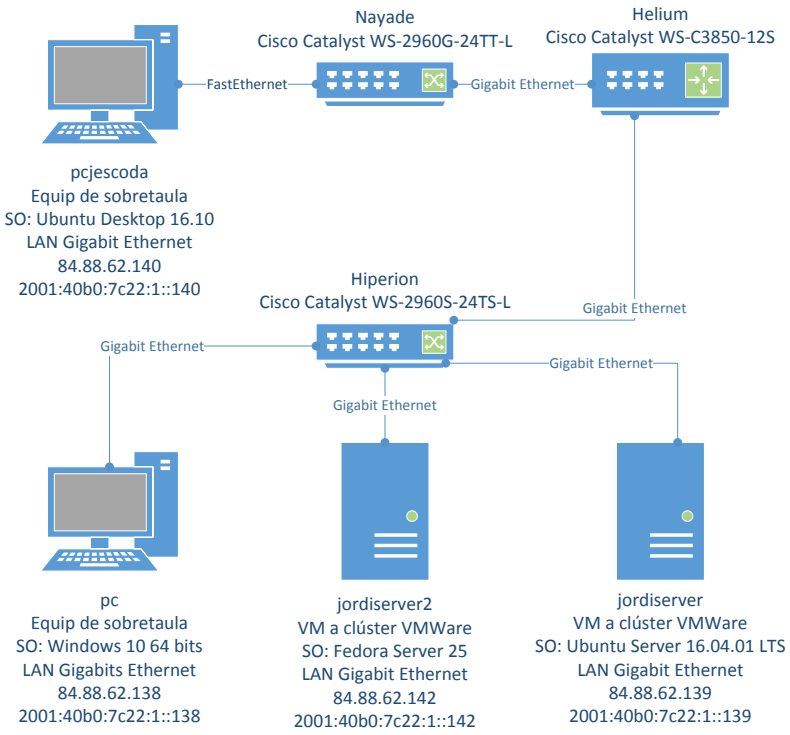



**Fig. 4.7** Escenari *throughput*

Els tres servidors (pc, jordiserver2 i jordiserver) i l'equip client pcjescoda estan configurats amb adreçament de doble pila. Cadascuna de les màquines servidor té una infraestructura LAMP o WAMP en el cas de la màquina amb Windows 10. A l'escenari hi intervenen tres equips de xarxa, Nayade, Hiperion i Helium.

Utilitzarem l'eina de Linux *wget* per enviar dades entre dos equips dins de la xarxa de doble pila i per calcular i analitzar el *throughput* mitja dels dos protocols. S'utilitzen diferents SO perquè aquests no influeixin en els resultats de la mitjana. Paral·lelament, també podem veure si aquest factor té alguna afectació. El valor del *throughput*, s'obté de les mesures de descarrega de 20 paquets de diferent mida entre 61,4kB i 1,0GB que classifiquem en grups de 5 paquets segons la seva dimensió, petits (<1MB), mitjans (1MB – 10MB), grans (10MB – 100MB) i enormes (100MB – 1GB).

Mesurarem també els paràmetres d'ús de cpu i memòria dels equips de xarxa implicats durant l'intercanvi de dades per a veure quin és l'impacte i com influeix el protocol.

Per a calcular els valors del *throughput*, ho realitzem a través de l'script descarrega.sh (veure **Annex L.2. Script càlcul throughput i recursos equips de xarxa**). Aquest programa executa l'eina *wget* i *wget6* per descarregar un darrere l'altre els 20 paquets de diferents mides dels servidors web que l'hi anem indicant. Aquest script genera uns logs d'on extraiem el valor del *throughput* per cada arxiu descarregat.

Aquest mateix script executa altres tres scripts per monitoritzar el consum de recursos dels equips de xarxa que intervenen, cisco_helium.sh, cisco_hiperion.sh i cisco_nayade.sh (veure **Annex J.2. Script càlcul throughput i recursos equips de xarxa**) durant la transferència. Aquesta dura uns 8 minuts aproximadament. Els scripts recullen dades dels equips de xarxa a través del Protocol Simple d'Administració de Xarxa (SNMP).

## 4.2.2 Resultats i conclusions

### *4.2.2.1 Throughput*

A la gràfica de la figura **Fig. 4.8** i la **Taula 4.1** podem observar que el *throughput* d'IPv4 és més gran que el d'IPv6. La diferència s'accentua en els paquets petits, mitjans i grans. En canvi, en els enormes la diferència és menor.

El *throughput* mitja d'IPv4 és de 10,76 Mb/s i el d'IPv6 és de 9,57 Mb/s. Sobre el paper hauríem de pensar que com la xarxa IPv4 està més congestionada que la xarxa IPv6 al CTTC, el *throughput* seria major en IPv6. En aquest aspecte, cal destacar que la desviació estàndard sobre la mitjana aritmètica del *throughput* a IPv6 és molt més gran que a IPv4 i podria explicar-se en aquest sentit. Per altre banda podem notar una relació amb els resultats obtinguts de RTT. A IPv6 aquest valor és superior que a IPv4. El *throughput* té una relació inversament proporcional al RTT donada per la següent fórmula **(4.1)**. Veiem que el valor de RTT afecta al valor del *throughput*.

$$Throughput = TCP\ Window\ size / RTT \qquad \textbf{(4.1)}$$

La velocitat de transport de dades a IPv6 augmenta amb la mida del paquet.

**Taula 4.1** Mitjana i desviació estàndard del *throughput* en funció de la mida del paquet

| | **Me Paquets** | | | | | |
|---|---|---|---|---|---|---|
| | Petit | Mitja | Gran | Enorme | Me | s |
| IPv4 (Mb/s) | 10,95 | 10,01 | 11,13 | 10,95 | 10,76 | 0,51 |
| IPv6 (Mb/s) | 8,12 | 9,06 | 10,52 | 10,57 | 9,57 | 1,19 |
| | **s Desviació Estàndard Paquets** | | | | | |
| | Petit | Mitja | Gran | Enorme | | |
| IPv4 | 0,581 | 1,123 | 0,150 | 0,171 | | |
| IPv6 | 1,315 | 0,635 | 0,238 | 0,386 | | |

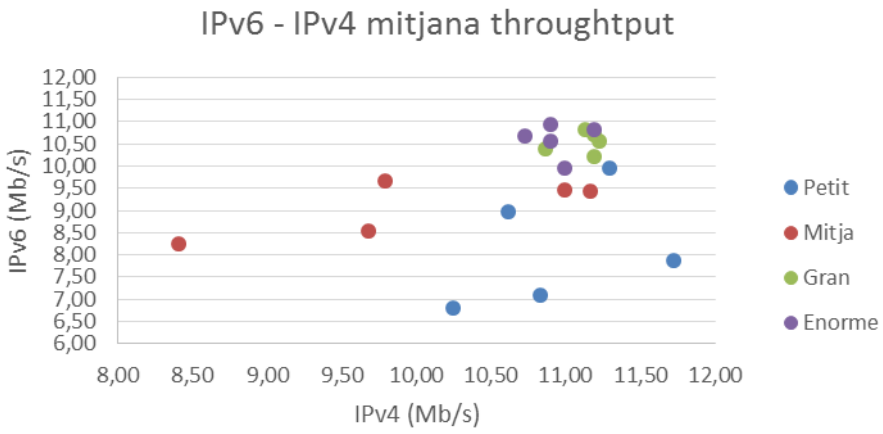



**Fig. 4.8** Mitjana del *throughput* en funció de la mida del paquet en IPv4 i IPv6.

### *4.2.2.2 Throughput en funció del SO*

De la prova realitzada anteriorment, avaluem la mitjana del *throughput* en funció dels diferents SO utilitzats amb IPv4 i IPv6. En la **Taula 4.2** podem observar que la diferència entre utilitzar IPv4 i IPv6 és petita, exceptuant Windows 10, on la diferència de l'ús d'IPv4 i IPv6 és d'un 9% aproximadament. Els resultats són similars en els diferents SO. Podem notar que amb IPv6 el servidor amb Fedora 25 té un *throughput* més elevat que la resta.

Podríem dir que la diferència d'utilitzar un servidor o un altre no és significativa.

**Taula 4.2** *Throughput* en funció del SO

| | ***Throughput* (Mb/s) - SO Servidor** | | |
|---|---|---|---|
| | Windows 10 | Fedora 25 | Ubuntu S. 16.04LTS |
| IPv4 | 11,15 | 11,20 | 10,80 |
| IPv6 | 10,18 | 11,10 | 10,40 |

### *4.2.2.3 Rendiment dels equips de xarxa*

En el mateix test de transferència de dades per mesurar el *throughput*, hem recollit mesures del consum de CPU i de la memòria utilitzada als equips de xarxa (Helium, Hiperion i Nayade) als que estan connectats les màquines que intervenen en l'escenari.

En les gràfiques de les figures **Fig. 4.9 i Fig. 4.10** observem que el consum de %CPU varia molt poc i la memòria utilitzada no varia durant el test. Entenem

que la quantitat de tràfic que hem generat durant la prova és petita per aquests equips.

Hem resumit amb el valor mig els valors de consum de recursos als equips de xarxa en funció del protocol utilitzat a la **Taula 4.3** i observem que no hi ha diferència entre el protocol utilitzat.

**Taula 4.3** Consum de recursos dels equips de xarxa en funció del SO i el protocol utilitzat

| | Helium | | Hiperion | | Nayade | |
|---|---|---|---|---|---|---|
| | % CPU | M. Utilitzada (MB) | % CPU | M. Utilitzada (MB) | % CPU | M. Utilitzada (MB) |
| IPv4 | 18 (0,95) | 172804 (42,24) | 16 (3,22) | 27496 (7,97) | 5 (1,74) | 8465 (3,06) |
| IPv6 | 18 (0,51) | 172804 (2,47) | 16 (2,38) | 27496 (3,80) | 5 (0,64) | 8465 (0,48) |

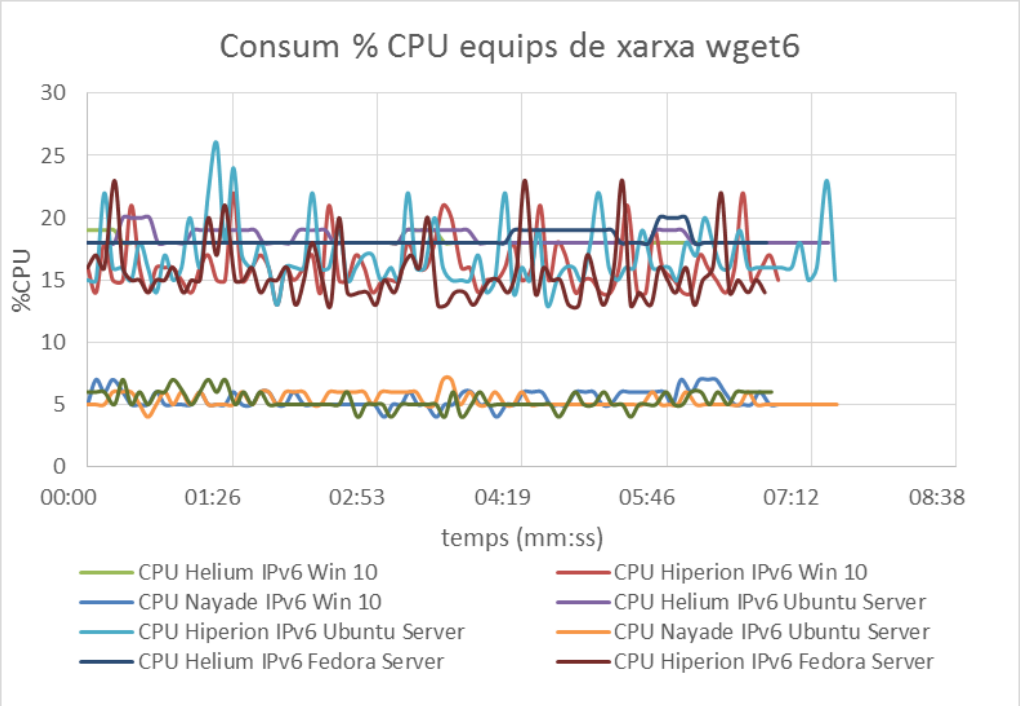



**Fig. 4.9** Consum de CPU dels equips de xarxa en IPv6

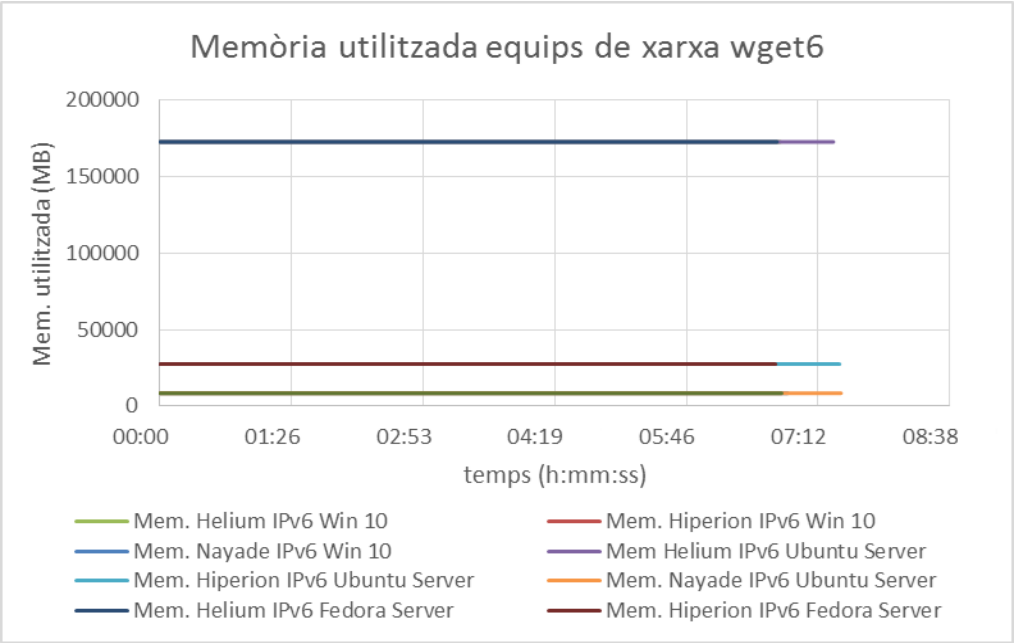



**Fig. 4.10** Consum de memòria dels equips de xarxa en IPv6

## 4.3 Time To First Byte

L'objectiu de la prova és avaluar el rendiment del protocol IPv6 respecte l'IPv4 a través de mesurar el paràmetre *Time To First Byte*[5] (TTFB). Compararem quin és el cost de carregar el primer byte en funció del protocol utilitzat. Plantegem múltiples escenaris per prendre les mesures del rendiment. A nivell intern de la xarxa del CTTC amb configuració de xarxa nativa amb doble pila i amb un dels protocols configurats i des de l'exterior del CTTC en diferents localitzacions per veure com afecta aquest factor i amb configuració IPv4 amb NAT[6] per comparar-ho amb IPv6 com alternativa a l'esgotament d'adreces.

### 4.3.1 Escenaris

Es configuren tres escenaris per comparar el paràmetre TTFB en ambdós protocols. Per calcular el temps de carregar el primer byte, necessitem que una de les màquines sigui un servidor web per poder descarregar el primer byte d'un web. En aquesta prova, l'equip jordiserver és un servidor web amb infraestructura LAMP.

[5]**Time To First Byte (TTFB):** És la quantitat de temps (segons) que hi ha després que el client enviï una petició HTTP_GET per rebre el primer byte del recurs sol·licitat al servidor. Aquest temps inclou el temps de connexió que necessita el servidor per calcular el resultat (time_pretransfer) i el temps en resoldre la petició DNS (time_namelookup).

[6]**Network Address Translation (NAT): L**a traducció d'adreces de xarxa és el procés pel qual es modifica la informació sobre adreces a la capçalera del paquet IPv4 mentre està en trànsit per un dispositiu d'encaminament

A l'escenari intervenen les màquines jordiserver (servidor web), pcjescoda (client) i un servidor extern al CTTC que també realitza la funció de client. Les màquines pcjescoda i jordiserver van variant la configuració de xarxa en funció de l'escenari. En canvi, el servidor extern només disposa d'adreçament IPv4. No podrem comparar el rendiment amb IPv6 des de l'exterior.També intervenen els equips de xarxa Nayade, Hiperion i Helium.

El valor del paràmetre, el mesurem a través d'un script ttfb.sh (veure **Annex L.3 Script càlcul Time To First Byte**) que executem a pcjescoda, al que l'hi passem com a paràmetre el nom del servidor jordiserver.cttc.es i el protocol que volem mesurar (4 o 6). El valor del *Time To First Byte* serà la mitjana aritmètica de 20 peticions, per treure un valor representatiu de varies mostres. L'script utilitza l'eina *curl* basada amb la llibreria *libcurl* i l'intèrpret de comanes *curl* orientat a la transferència d'arxius.

Per a calcular el valor del TTFB de forma remota, ho realitzem a través de l'eina online per analitzar el rendiment de pàgines web webpagetest.org, d'on obtenim el resultat de la mitjana del TTFB de 20 tests des de diferents localitzacions. Amb el càlcul del paràmetre de forma remota podrem observar com influeix la latència de la xarxa.

#### *4.3.1.1 Escenari 1: configuració de xarxa nativa*

En aquest test, l'objectiu és mesurar el paràmetre TTFB a la xarxa interna del CTTC i des de l'exterior del CTTC des de diferents localitzacions. A l'escenari intervenen les màquines jordiserver, pcjescoda i el servidor extern al CTTC webpagetest.org tal i com observem en la següent figura **Fig. 4.11**. Les màquines pcjescoda i jordiserver estan configurades amb adreçament de doble pila natiu.

Calculem el TTFB des de la xarxa interna del CTTC entre les màquines pcjescoda i jordiserver amb la configuració de xarxa en dual stack i posteriorment, només amb la configuració IPv4 i IPv6 per separat, per observar com afecta la configuració en doble pila en el rendiment.

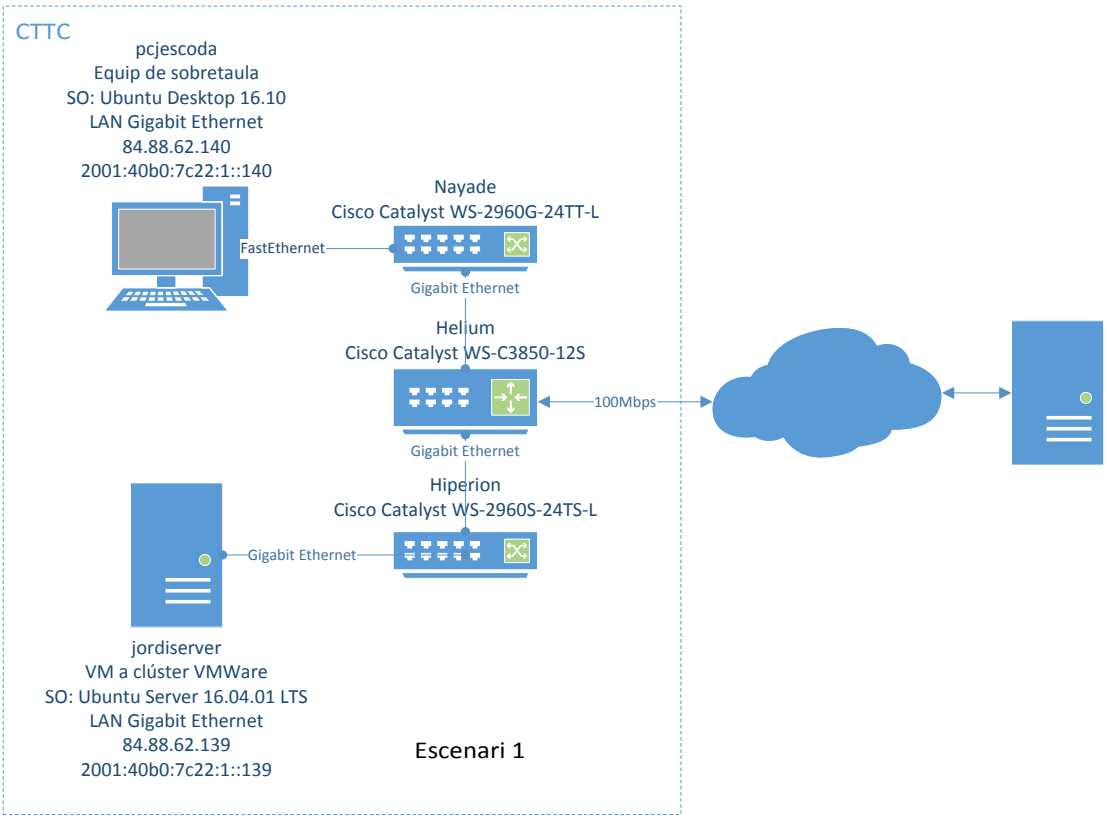



**Fig. 4.11** Escenari 1 amb configuració de xarxa nativa.

#### *4.3.1.1.1* Resultats i conclusions de l'escenari 1

Del càlcul de la mitjana del TTFB de 20 peticions obtenim els següents resultats.

A la **Taula 4.4** podem observar que el valor del TTFB quan només hi ha un dels protocols configurats tant al servidor com al client és menor amb IPv4 que amb IPv6. En canvi, quan ambdós protocols estan configurats succeeix a l'inrevés, el TTFB a IPv6 és menor que a IPv4 i inferior al calculat amb la configuració de xarxa nativa per IPv6.

**Taula 4.4** TTFB en funció de la configuració de xarxa

| | Xarxa CTTC | | | |
|---|---|---|---|---|
| | Configuració | | Dual Stack | |
| | IPV4 | IPv6 | IPv4 | IPv6 |
| Mitjana TTFB (ms) | 6,00 | 6,80 | 7,65 | 6,60 |
| Desviació estàndard (ms) | 0 | 2,46 | 3,39 | 2,04 |

Aquests resultats els podem interpretar com que la configuració amb la doble pila de protocols IPv6 té preferència davant el IPv4 i això provoca que el temps de processat d'IPv4 augmenti.

Un altre explicació és que les màquines client i servidor han de tenir les dues taules d'encaminament i com que la capçalera del paquet IPv6 és més simple i té una mida fixe amb comparació amb la d'IPv4, el processat és més senzill i això afecta el valor del TTFB.

Cal destacar que els valors de TTFB són molt similars. No hi ha massa diferència entre les variacions de configuració de xarxa a l'escenari. Això també és degut a que en la xarxa interna del CTTC aquestes màquines estan properes.

Si observem els valors del *Time To First Byte* calculats des de l'exterior del CTTC a la següent **Taula 4.5** podem notar que la localització del client que pren les mesures és rellevant, ja que el nombre de salts que té fins al destí, el tipus de xarxes i el proveïdor de serveis per les que s'estableix la comunicació, influeix en la latència de la connexió. També influeix les característiques i l'ús de les màquines en el moment de la mesura, però no tenim referències per poder remarcar-ho.

**Taula 4.5** TTFB en funció de la configuració de xarxa mesurat des de l'exterior del CTTC

| | webpagetest.org | | |
|---|---|---|---|
| | Localització | IPv4 | Desv. Estàndard (s) |
| Mitjana TTFB (s) 20 peticions | Montreal, CA | 0,358 | 1,585 |
| | Califòrnia, USA | 0,452 | 0,197 |
| | Manchester, UK | 0,302 | 0,040 |
| | Amsterdam, NL | 0,242 | 0,227 |
| | Frankfurt, GE | 0,183 | 0,024 |

#### *4.3.1.2 Escenari 2: configuració de xarxa amb NAT*

Plantegem un segon test per observar quin és el rendiment de la configuració de xarxa amb NAT. Així podem comparar NAT com a solució a la poca escalabilitat i la falta d'adreces del model IPv4 en comptes d'utilitzar IPv6.

Com observem en la figura **Fig. 4.12**, intervenen les màquines jordiserver que disposa de configuració en IPv4 amb la interfície de xarxa configurada amb NAT (10.1.16.210) i pcjescoda amb la interfície de xarxa configurada amb NAT (10.1.16.182). La interfície NAT de pcjescoda surt a Internet amb l'adreça 84.88.63.150 i la interfície IPv4 de jordiserver surt a Internet amb l'adreça 84.88.61.206.

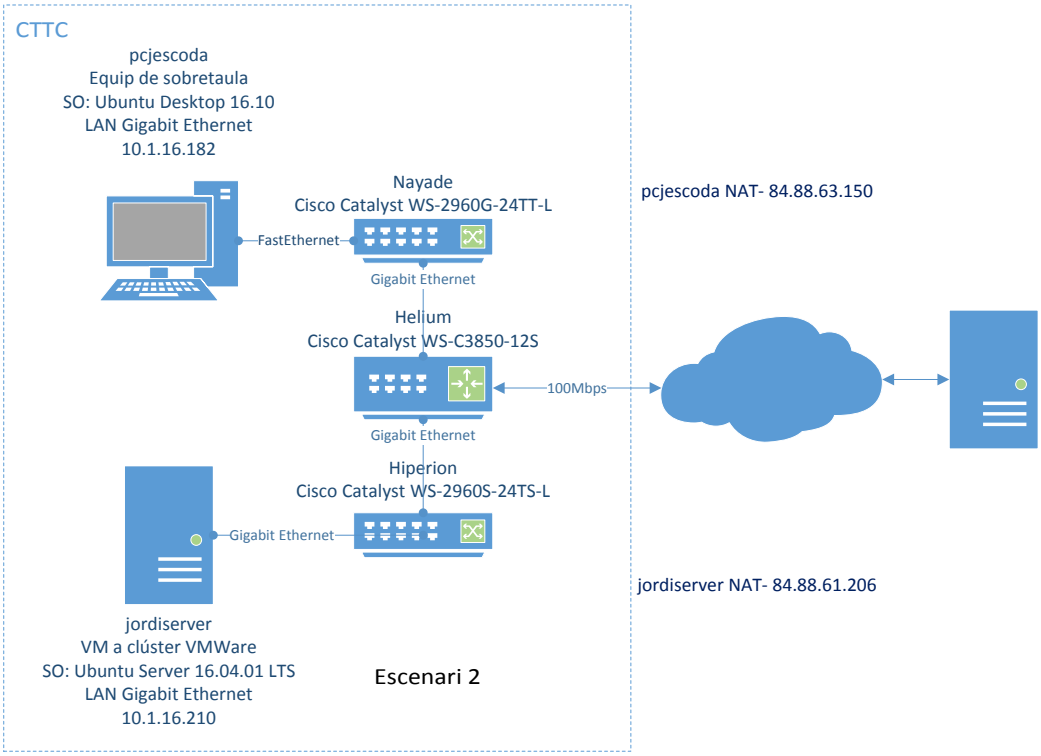



**Fig. 4.12** Escenari 2 amb configuració de xarxa amb NAT.

Calculem el valor de la mitjana aritmètica de 20 mesures del TTFB a la xarxa interna del CTTC amb l'script ttfb.sh i també ho fem de forma remota a través de l'eina web de la pàgina webpagetest.org. Amb el càlcul del paràmetre de forma remota podem observar i comparar com influeix la configuració de xarxa NAT amb el valor del TTFB mesurat amb configuració de xarxa nativa de l'escenari 1.

#### *4.3.1.2.1* Resultats i conclusions de l'escenari 2

Del càlcul de la mitjana del TTFB de 20 peticions obtenim els següents resultats.

A la **Taula 4.6** podem observar que el valor del TTFB mesurat a la xarxa del CTTC quan la configuració de xarxa de l'equip client i servidor és amb NAT, el valor del TTFB obtingut és lleugerament superior al mesurat amb la configuració nativa IPv4. Podem notar que la configuració NAT afecta negativament en el valor del paràmetre. Podríem dir que el NAT té un cost de procés més elevat a la capçalera. En el cas de la xarxa interna del CTTC tenir NAT o IPv6 no és perceptible. Això és degut a que les màquines són molt properes les unes a les altres i la latència introduïda és baixa.

La diferència d'utilitzar NAT o no, està a nivell complexitat de gestió i configuració de la xarxa interna del centre.

**Taula 4.6** TTFB amb la configuració de xarxa amb NAT

| | Xarxa CTTC |
|---|---|
| | IPV4 |
| Mitjana TTFB (ms) | 7,05 |
| Desv. Estàndard (ms) | 2,21 |

Si observem els valors del *Time To First Byte* calculats des de l'exterior del CTTC amb la configuració actual, a la **Taula 4.7** podem notar, igual que a l'escenari 1, que la localització és rellevant. En aquest cas, les mesures són molt similars. No percebem cap penalització per utilitzar NAT. Això pot ser degut a que els factors externs esmentats en l'escenari 1 hagin variat. Les mesures han estat preses en finestres temporals diferents.

**Taula 4.7** TTFB amb la configuració de xarxa amb NAT mesurat des de l'exterior del CTTC

| | webpagetest.org | | |
|---|---|---|---|
| | Localització | IPv4 | Desv. Estàndard (s) |
| Mitjana TTFB (s) 20 peticions | Montreal, CA | 0,360 | 0,012 |
| | Califòrnia, USA | 0,450 | 0,066 |
| | Manchester, UK | 0,278 | 0,009 |
| | Amsterdam, NL | 0,245 | 0,251 |
| | Frankfurt, GE | 0,183 | 0,018 |

A nivell de resultats obtinguts del *Time To First Byte* en els escenaris plantejats, tots són valors acceptables.

# CAPÍTOL 5. CONCLUSIONS I LÍNIES FUTURES

Els objectius que ens havíem proposat en la realització del PFC els hem assolit.

S'ha estudiat i dissenyat un escenari de xarxa perquè es pogués implementar de forma nativa el protocol IPv6 al CTTC. En una primera fase, s'han substituït alguns equips de xarxa perquè es pogués suportar IPv6 aprofitant que l'equipament existent tenia una edat. S'ha optat per integrar una solució que contingui la doble pila de protocols IPv4 i IPv6 de forma nativa. Així mantenim la connectivitat IPv4 i l'aconseguim amb IPv6. També s'han adaptat els serveis bàsics del CTTC, el DNS i el servei web perquè puguin rebre peticions IPv6.

La xarxa IPv6 proposada i implementada és la base de futures actualitzacions de la xarxa del CTTC perquè l'IPv6 estigui present en tots els equips finals i els serveis. El pla d'adreçament proposat, actualment cobreix amb escreix les necessitats d'adreçament del CTTC. Aquest està preparat i permet un creixement ordenat en funció de les futures necessitats que puguin sorgir amb el creixement d'Internet i els dispositius que necessiten connectivitat.

En la darrera part del projecte hem creat un banc de proves per comparar el rendiment del protocol IPv6 respecte l'IPv4. A nivell intern de la xarxa del CTTC podem concloure de forma general arran dels resultats obtinguts en els tests, que no existeixen grans diferències entre l'ús d'un protocol o altre.

Si desgranem una mica els resultats dels tests, veiem que el $RTT_{IPv6} > RTT_{IPv4}$, i paral·lelament que el *throughput* de la xarxa IPv4 és més gran que a la IPv6. Això és degut a que IPv6 consumeix més recursos en el processat dels paquets respecte IPv4 i Internet disposa de menys nodes IPv6 disponibles que IPv4 a nivell de la xarxa externa del CTTC. Els nodes IPv6 estan més distants entre ells i això fa que el temps augmenti en IPv6. Aquest paràmetre és un indicador de la QoS experimentada per l'usuari. Les diferències no són remarcables amb IPv4.

Dels sistemes operatius avaluats com a servidors, podem dir que el que disposa de Fedora 25 té un millor rendiment a nivell dels paràmetres valorats.

Hem comparat NAT amb IPv6 natiu com a solució alternativa a la manca d'adreces i al creixement d'Internet. A nivell de percepció d'usuari, no hem observat grans diferències entre ells.

Les línies futures de la implantació d'IPv6 al CTTC passen per donar connectivitat IPv6 a tots els equips i serveis del CTTC. Podem remarcar, com a servei amb més repercussió a nivell d'usuari, el servei del DHCP i paral·lelament el servei WiFi. Així podrem avaluar i comparar l'autoconfiguració *stateful* (DHCPv6) i *stateless*.

Per altre banda, podem realitzar estudis futurs que tractin i implementin la seguretat d'IPv6 (IPsec), la mobilitat d'IPv6 (MIPv6) i aspectes de qualitat de servei en IPv6.

# GLOSSARI

| | |
|---|---|
| BGP | Border Gateway Protocol |
| CIDR | Encaminament Inter-Dominis sense Classes |
| CoS | Classe de Servei |
| CPU | Unitat central de processament |
| DHCPv6 | Dynamic Host Configuration Protocol versió 6 |
| DNS | Sistema de noms de domini |
| EIGRP | Protocol d'Encaminament de Porta d'enllaç Interior Millorat |
| EUI-64 | Identificador únic d'interfície IPv6 de 64 bits |
| IGP | Protocol de Gateway Interior |
| IID | Identificadors d'Interfície |
| IOS | Internetwork Operating System |
| IP | Protocol d'Internet |
| IPsec | Protocol de Seguretat d'Internet |
| IPv4 | Protocol d'Internet versió 4 |
| IPv6 | Protocol d'Internet versió 6 |
| IS-IS | Protocol de sistema intermedi a sistema intermedi |
| LAMP | Linux, Apache, MySQL, PHP |
| LAN | Xarxa d'àrea local |
| LIR | Registre Local d'Internet |
| Me | Mitjana aritmètica |
| MIPv6 | IPv6 mòbil |
| MTU | Unitat màxima de transferència |
| NAT | Traducció d'adreces de xarxes |
| ND | Descobriment de veïns |
| OSI | Interconnexió de sistemes oberts |
| OSPF | Protocol d'encaminament de codi obert pel camí més curt |
| PIM-SM | Protocol Independent Multicast Sparse Mode |
| PMTUD | Descobriment del camí MTU |
| QoS | Qualitat de Servei |
| RIP | Protocol de Passarel·la Interna |
| RIR | Registre Regional d'Internet |
| RTT | Temps d'anada i torna d'un paquet |
| s | Desviació estàndard |
| ToS | Tipus de Servei |
| TTFB | Temps que hi ha entre que un client enviï una petició per rebre el primer byte del recurs del servidor |
| TTL | Temps de vida |
| ULA | Adreça Local Única |
| VLAN | Xarxa d'àrea local virtual |
| VRF | Encaminament i Reenviament Virtual |
| WAMP | Windows, Apache, MySQL, PHP |
| wget | Obtenir World Wide Web |
| WiFi | Fidelitat sense cable |

# BIBLIOGRAFIA

[1] Deering S.(Cisco), Hinden R. (Nokia), RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification”, December 1998, [en línia] Disponible a: https://www.ietf.org/rfc/rfc2460.txt

[2] Postel, J., RFC 791, "Internet Protocol", STD 5, USC/Information Sciences Institute, September 1981, [en línia] Disponible a: http://tools.ietf.org/html/rfc791#page-11

[3] Deering S.(Cisco), Hinden R. (Nokia), RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification”, December 1998, [en línia] Disponible a: http://tools.ietf.org/html/rfc2460#section-1

[4] Rajahalme J. (Nokia, Conta A. Transwitch B., Carpenter B (IBM), Deering S. (Cisco), RFC 3697, “IPv6 Flow Label Specification”, Març 2004, [en línia] Disponible a: https://www.ietf.org/rfc/rfc3697.txt

[5] Reynolds J, Postel J. (ISI), RFC 1700, “Assigned Numbers”, Octubre 1994, [en línia] Disponible a: https://www.ietf.org/rfc/rfc1700.txt

[6] Cisco Systems, Inc, “IPv6 extension headers”, Octubre 2006, [en línia] Disponible a: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

[7] Deering S.(Cisco), Hinden R. (Nokia), RFC 2460, “Internet Protocol, Version 6 (IPv6) Specification”, December 1998, [en línia] Disponible a: https://tools.ietf.org/html/rfc2460#section-4.1

[8] Hinden R. (Nokia), Deering S.(Cisco), RFC 4291, “IP Version 6 Addressing Architecture”, Febrer 2006, [en línia] Disponible a: https://tools.ietf.org/html/rfc4291

[9] Hinden R. (Nokia), Deering S.(Cisco), Normand E. (Sun), RFC 3587, “IPv6 Global Unicast Address Format”, Agost 2003, [en línia] Disponible a: https://tools.ietf.org/html/rfc3587

[10] Johnson D (Carnegie Mellon University), Deering S.(Cisco),RFC 2526, “Reserved IPv6 Subnet Anycast Addresses”, Març 1999, [en línia] Disponible a: https://tools.ietf.org/html/rfc2526

[11] Hinden R. (Ipsilon Networks), Deering S.(Cisco), RFC 2375,”IPv6 Multicast Address Assignments”, Juliol 1998, [en línia] Disponible a: https://www.ietf.org/rfc/rfc2375.txt

[12] Kawamura S. (NEC BIGLOBE, Ltd.), Kawashima M. (NEC AccessTechnica, Ltd.), RFC 5952, “A Recommendation for IPv6 Address Text

Representation", Agost 2010, [en línia] Disponible a: https://tools.ietf.org/html/rfc5952

[13] Hinden R. (Nokia), Deering S.(Cisco), RFC 4291, "IP Version 6 Addressing Architecture", Febrer 2006, [en línia] Disponible a: https://tools.ietf.org/html/rfc4291#section-2.5.1

[14] Hinden R. (Nokia), Deering S.(Cisco), RFC 3513, "Internet Protocol Version 6 (IPv6) Addressing Architecture", Abril 2003, [en línia] Disponible a: https://www.ietf.org/rfc/rfc3513.txt

[15] Savola P. (CSC/FUNET), Haberman B. (JHU APL), RFC3956, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", Novembre 2004, [en línia] Disponible a: https://tools.ietf.org/html/rfc3956

[16] Haberman B. (Consultant), Thaler D. (Microsoft),RFC3306, "Unicast-Prefix-based IPv6 Multicast Addresses", Agost 2002, [en línia] Disponible a: https://tools.ietf.org/html/rfc3306

[17] Conta A. (Transwitch), Deering S. (Cisco), RFC4443, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", Març 2006, [en línia] Disponible a: https://tools.ietf.org/html/rfc4443

[18] Palet Martínez J., "Tutorial IPv6 ConsulinTel", [en línia] Disponible a: www.consulintel.es/html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

[19] Corral, G., "Telemática i Xarxes d'ordinadors", 2009.

[20] Postel J. (ISI), RFC792, "INTERNET CONTROL MESSAGE PROTOCOL", Setembre 1981, [en línia] Disponible a: https://tools.ietf.org/html/rfc792

[21] Narten T. (IBM), Nordmark E. (Sun Microsystems), Simpson W. (Daydreamer), Soliman H. (Elevate Technologies), RFC 4861, "Neighbor Discovery for IP version 6 (IPv6)", [en línia] Disponible a: https://tools.ietf.org/html/rfc4861

[22] Thomson S. (Bellcore), Narten T. (IBM), RFC2462, "IPv6 Stateless Address Autoconfiguration", Desembre 1998, [en línia] Disponible a: https://tools.ietf.org/html/rfc2462

[23] Nordmark E. (Sun), Gilligan R. (Intransa), RFC 4213, "Basic Transition Mechanisms for IPv6 Hosts and Routers", Octubre 2005, [en línia] Disponible a: https://tools.ietf.org/html/rfc4213

[24] Gilligan R., Normark E. (Sun), RFC 1933, "Transition Mechanisms for IPv6 Hosts and Routers", Abril 1996, [en línia] Disponible a: https://tools.ietf.org/html/rfc1933

[25] Li X, Bao C. Chen M., Zhang H., Wu J. (CERNET Center/Tsinghua), RFC 6219, “The China Education and Research Network (CERNET) IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition”, Maig 2011, [en línia] Disponible a: https://tools.ietf.org/html/rfc6219

[26] “Model OSI: ITU-T Recommendation X.200 (07/94): Information technology - Open Systems Interconnection - Basic Reference Model: The basic model”, 1994, [en línia] Disponible a: www.itu.int/rec/T-REC-X.200-199407-I/en

[27] “Cisco products “End of Life””, [en línia] Disponible a: http://www.cisco.com/en/US/products/hw/switches/prod_category_end_of_life.html

[28] Cisco Systems, Inc, “Cisco Catalyst 2960-S FlexStack - White Paper”, Gener 2014, [en línia] Disponible a: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps6406/white_paper_c11-578928.html

[29] CSUC (CESCA), “Adreces IPv4 i IPv6”, [en línia] Disponible a: www.cesca.cat/ca/comunicacions/anella-cientifica/procediment-de-connexio/adreces-ipv4-i-ipv6

[30] “IPv6 Subnetting Card”, Gener 2011, [en línia] Disponible a: www.ripe.net/lir-services/resource-management/number-resources/ipv6/ipv6-subnetting-card

[31] Narten T. (IBM), Huston G. (APNIC), Roberts L. (Standford University), RFC 6177, “IPv6 Address Assignement to End Sites”, Març 2011, [en línia] Disponible a: https://tools.ietf.org/html/rfc6177

[32] George W. (Time Warner Cable), RFC 6547, “Using 127-Bit IPv6 Prefixes on Inter-Router Links”, Febrer 2012, [en línia] Disponible a: https://tools.ietf.org/html/rfc6547

[33] Van de Velde G., Popoviciu C. (Cisco), Chown T. (University of Southampton), Bonness O., Hahn C. (T-Systems), RFC 5375, “IPv6 Unicast Address Assignment Considerations”, Desembre 2008, [en línia] Disponible a: https://tools.ietf.org/html/rfc5375

[34] Rosen E. (Cisco), Rekhter Y. (Juniper), RFC 4364, “BGP/NPLS IP Virtual Private Networks (VPN)”, Febrer 2006, [en línia] Disponible a: https://tools.ietf.org/html/rfc4364

[35] Rekhter Y. Ed., Li T. Ed., Hares S. Ed, RFC 4271, “A Border Gateway Protocol 4 (BGP-4)”, Gener 2006, [en línia] Disponible a: https://tools.ietf.org/html/rfc4271

[36] Cisco Systems, Inc, “Catalyst 3750 Metro Switch Software Configuration Guide, 12.2(58)SE”, [en línia] Disponible a: www.cisco.com/en/US/docs/switches/metro/catalyst3750m/software/release/12

.2_58_se/configuration/guide/swipv6.html#wp1450419

[37] Cisco Systems, Inc, “Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6”, [en línia] Disponible a: http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/glossary.html#wp1027964

[38] Perkins C. Ed. (Tellabs), Johnson D. (Rice University), Arkko J. (Ericsson), RFC 6275, “Mobility Support in IPv6”, Juliol 2011, [en línia] Disponible a: https://tools.ietf.org/html/rfc6275

[39] Abley J. (Afilias), Savola P. (CS/FUNET), Neville-Neil G. (Neville-Neil Consulting), RFC 5095, “Deprecation of Type 0 Routing Headers in IPv6”, Desembre 2007, [en línia] Disponible a: https://tools.ietf.org/html/rfc5095

[40] Kent S. (BBN Technologies), RFC 4302, “IP Authentication Header”, Desembre 2005, [en línia] Disponible a: https://tools.ietf.org/html/rfc4302

[41] Kent S. (BBN Technologies), RFC 4303, “IP Encapsulating Security Payload (ESP)”, Desembre 2005, [en línia] Disponible a: https://tools.ietf.org/html/rfc4303

[42] Johnson D. (Rice University), Perkins C. (Nokia), Arkko J. (Ericsson), RFC 3775, “Mobility Support in IPv6”, Juny 2004, [en línia] Disponible a: https://tools.ietf.org/html/rfc3775

[43] Kent S. (BBN Corp), Atkinson R. (@Home Network), RFC 2402, “IP Authentication Header”, Novembre 1998, [en línia] Disponible a: https://tools.ietf.org/html/rfc2402

[44] S. Kent S, Atkinson R., RFC 2406, “IP Encapsulating Security Payload (ESP)", Novembre 1998, [en línia] Disponible a: https://tools.ietf.org/html/rfc2406

[45] Hiden R. (Nokia), Haberman B. (JHU-APL), RFC 4193, “Unique Local IPv6 Unicast Addresses", Octubre 2005, [en línia] Disponible a: https://tools.ietf.org/html/rfc4193

[46] Huston G. (Telstra), Lord A. (APNIC), Smith P. (Cisco), RFC 3849, “IPv6 Address Prefix Reserved for Documentation", Juliol 2004, [en línia] Disponible a: https://tools.ietf.org/html/rfc3849

[47] Huitema C. (Microsoft), Carpenter B. (IBM), Smith P. (Cisco), RFC 3879, “Deprecating Site Local Addresses", Septembre 2004, [en línia] Disponible a: https://tools.ietf.org/html/rfc3879

[48] IAB, IESG, RFC 3177, “IAB/IESG Recommendations on IPv6 Address Allocations to Sites", Septembre 2001, [en línia] Disponible a: https://tools.ietf.org/html/rfc3177

[49] Thomson S. (Cisco), Narten T. (IBM), Jinmei T. (Toshiba), RFC 4862, “IPv6 Stateless Address Autoconfiguration", Setembre 2007, [en línia] Disponible a: https://tools.ietf.org/html/rfc4862

[50] Malkin G. (Xylogics), Minnear R. (Ipsilon Networks), RFC2080, “RIPng for IPv6”, Gener 1997, [en línia] Disponible a: https://tools.ietf.org/html/rfc2080

[51] Malkin G. (Xylogics), RFC2081, “RIPng Protocol Applicability Statement”, Gener 1997, [en línia] Disponible a: https://tools.ietf.org/html/rfc2081

[52] Hedrick C. (Rutgers University), RFC1058, “Routing Information Protocol”, Juny 1988, [en línia] Disponible a: https://tools.ietf.org/html/rfc1058

[53] Malkin G. (Xylogics), RFC1723, “RIP Version 2 Carrying Additional Information”, Novembre 1994, [en línia] Disponible a: https://tools.ietf.org/html/rfc1723

[54] Manner J (TKK), McDonald A. (Siemens/Roke), RFC5350, “IANA Considerations for the IPv4 and IPv6 Router Alert Options”, Setembre 2008, [en línia] Disponible a: https://tools.ietf.org/html/rfc5350

[55] Bates T. (Cisco), Chandra R. (Sonoa), Katz D., Rekhter Y. (Juniper), RFC4760, “Multiprotocol Extensions for BGP-4”, Gener 2007, [en línia] Disponible a: https://tools.ietf.org/html/rfc4760

[56] Bates T. (Cisco), Chandra R. (Sonoa), Katz D., Rekhter Y. (Juniper), RFC2545, “Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing”, Març 1999, [en línia] Disponible a: https://tools.ietf.org/html/rfc2545

[57] Hopps C. (Cisco),”Routing IPv6 with IS-IS”, RFC5308, Octubre 2008, [en línia] Disponible a: https://tools.ietf.org/html/rfc5308

[58] Regis dos Santos R., M. Moreiras A., Ascenço Reis E., Soares da Rocha A. (Núcleo de Informação e Coordenação do ponto BR), "CURSO IPv6 BÁSICO", 2010, [en línia] Disponible a: http://ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf

[59] “Ripe Database Query”, [en línia] Disponible a: https://apps.db.ripe.net/search/query.html)

[60] Thomson S. (Bellcore), Huitema C. (INRIA), RFC1886, “DNS Extensions to Support IP Version 6”, Souissi M. (AFNIC), Desembre 1995, [en línia] Disponible a: https://tools.ietf.org/html/rfc1886

[61] Thomson S. (Cisco), Huitema C. (Microsoft), Ksinant V. (6WIND), Souissi M. (AFNIC), RFC3596, “DNS Extensions to Support IP Version 6”, Octubre 2003, [en línia] Disponible a: https://tools.ietf.org/html/rfc3596

[62] Cicileo G, Gagliano R., O’Flaherty C., Rocha M, Olvera Morales C, Palet Martínez J., Vives Martínez Á., “IPv6 per a tothom. Guia d’ús i aplicació per a

diversos entorns", Febrer 2001, [en línia] Disponible a: http://www.ipv6peratothom.cat

[63] Mockapetris P. (ISI), RFC1034, "DOMAIN NAMES - CONCEPTS AND FACILITIES", Novembre 1987, [en línia] Disponible a: https://tools.ietf.org/html/rfc1034

[64] Mockapetris P. (ISI), RFC1035, "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION", Novembre 1987, [en línia] Disponible a: https://tools.ietf.org/html/rfc1035

[65] BIND, Internet Systems Consortium, Inc., [en línia] Disponible a: https://www.isc.org/downloads/bind/

Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels

UNIVERSITAT POLITÈCNICA DE CATALUNYA

# ANNEXOS

**TÍTOL DEL PFC: Estudi d'implantació de la IPv6 al CTTC**

**TITULACIÓ: Enginyeria de Telecomunicació (segon cicle)**

**AUTOR: Jordi Escoda Ramon**

**DIRECTOR: Roc Meseguer Pallarès**

**SUPERVISOR: David Company i Estall**

**DATA: 20 de febrer de 2017**

# ANNEX A. CAMPS CAPÇALERA IPv4

- **Version** (4bits) Versió del protocol.
- **Header Length** (4bits) Llargada en octets de la capçalera.
- **Type of Service** (ToS) (8bits) Identificador (QoS) per classificar els paquets segons la prioritat.
- **Total length** (16bits) Llargada en octets del paquet sencer, capçalera més dades.
- **Identification** (16bits) Flags (3bits) Fragment Offset (13bits) A través d'aquests tres camps IPv4 implementa el suport de la fragmentació de paquets.
- **Time to Live** (TTL) (8bits) Número màxim de salts que pot fer un paquet abans d'arribar al seu destí.
- **Protocol Number** (8bits) Indica el codi del protocol (TCP, UDP, ICMP, etc.) que encapsula IP en la capa superior, o sigui, la capa 4.
- **Header Checksum** (16bits) Comprova la integritat de les dades de la capçalera.
- **Source IPv4 address** (32bits) Adreça IP origen.
- **Destination IPv4 Address** (32 bits) Adreça IP destí.
- **Options** (mida variable) Guarda informació necessària per interpretar les dades que transporta el paquet.
- **Padding** (mida variable) S'usa per ajustar la mida del camp Options a 32 bits totals.

# ANNEX B. EXTENSIONS DE CAPÇALERA IPv6

## B.1 Codi de les extensions de capçalera (EH) IPv6 i ordre recomanat en el paquet [6]

**Taula B.1**. Codi de les extensions de capçalera (EH) IPv6 i ordre recomanat en el paquet

| Order | Keyword | Header | Next Header number |
|---|---|---|---|
| 1 | | Basic IPv6 Header [RFC-2460][1] | - |
| 2 | HOPOPT | Hop-By-Hop Options Header [RFC-2460][1] | 0 |
| 3 | IPv6-Opts | Destination Options Header (with Routing Options) [RFC-2460][1] | 60 |
| 4 | IPv6-Route | Routing Header [RFC-2460][1] [RFC-2460 [1], RFC-6275 [38], RFC-5095 [39]] | 43 |
| 5 | IPv6-Frag | Fragment Header [RFC-2460 [1]] | 44 |
| 6 | AH | Authentication Header [RFC-4302 [40]] | 51 |
| 7 | ESP | Encapsulating Security Payload Header [RFC-4303 [41]] | 50 |
| 8 | | Destination Options [RFC-2460][1] | 60 |
| 9 | | Mobility Header [RFC-6275 [38]] | 135 |
| | IPv6-NoNxt | No Next Header | 59 |
| Upper Layer | | TCP | 6 |
| Upper Layer | | UDP | 17 |
| Upper Layer | | ICMPv6 | 58 |

# B.2 Capçaleres d'Extensió més usades

## B.2.1 Hop-by-Hop Options Header

La capçalera *Hop-by-Hop* és la única extensió de capçalera que s'ha de processar per tots els nodes del camí entre l'origen i el destí del paquet. Si aquesta capçalera està present va immediatament darrera de la capçalera IPv6. Això permet als routers al llarg del camí examinar la capçalera sense necessitat de tractar qualsevol altra capçalera d'extensió. En la figura **Fig. B.1** observem el format de la capçalera Hop-by-Hop:

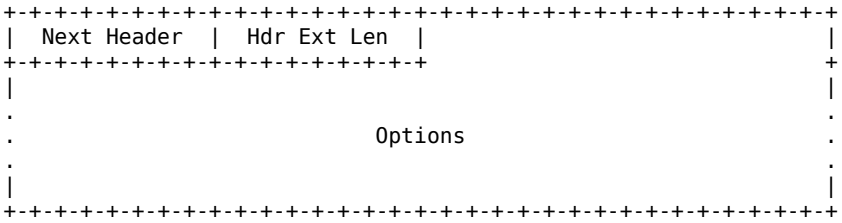



**Fig. B.1** Format de la capçalera Hop-by-Hop [1]

## B.2.2 Destination Options Header

Destination EH és utilitzada en el Mobile Internet Protocol v6 (MIPv6) així com a suport de determinades aplicacions.

### *B.2.2.1 Routing Header*

La Routing Header s'utilitza per a que un origen IPv6 indiqui els nodes intermedis que han de ser visitats en el camí del paquet cap a la seva destinació. La capçalera IPv6 conté l'adreça del primer node que visita i la Routing Header tota la resta. En la figura **Fig. B.2** es mostra el seu format:

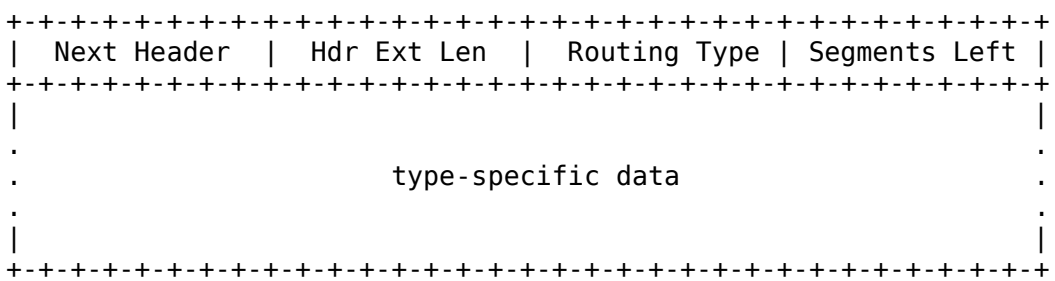



**Fig. B.2** Format de la capçalera Routing Header [1]

La capçalera *Routing Header* conté un camp de tipus (type) que permet saber amb exactitud la funcionalitat d'aquesta capçalera. Hi ha dos tipus de funcionalitats definides:

- **Type 0** [1] especifica tots els salts que ha de fer el paquet per viatjar fins al seu destí. El que faran els routers intermedis és anar canviant la direcció destí de la capçalera bàsica en funció de la capçalera estesa per forçar el salt cap al següent node. Si haguessin de fer algun salt no contemplat, aquest no modificaria la direcció destí d'aquell moment ni apareixeria ni s'afegiria a la capçalera estesa. Per tant, aquests salts no contemplats serien transparents al procés. Aquesta capçalera està obsoleta [39].
- **Type 2** [42] usat amb MIPv6.

### *B.2.2.2 Fragment Header*

La fragmentació requereix molt de procés en els nodes. Per tal d'evitar les necessitats de sobrecarregar els processadors dels nodes a IPv6 no s'admet la fragmentació de paquets més grans que la MTU. Per aquest motiu, la capçalera IPv6 no conté els camps de control que apareixen a la capçalera IPv4 per a suportar fragmentació: l'***identificador*** de paquet, ***flags*** i ***offset***. En IPv6, si la mida d'un paquet excedeix la MTU en el següent salt, es descartarà i s'enviarà un missatge ICMPv6 cap a la font. És el mateix comportament que té un paquet en IPV4 amb el bit *don't fragment* a 1.

Abans d'enviar un paquet, l'origen ha de passar per un procés de descobriment de la mida màxima acceptable que els paquets han de tenir mitjançant el procediment *Path-MTU-discovery*.

El node origen és l'encarregat de fragmentar el paquet. Els *routers* no han de controlar la fragmentació i els nodes destí han de saber re composar un paquet fragmentat. La capçalera Fragment Header té el següent format, figura **Fig. B.3**.

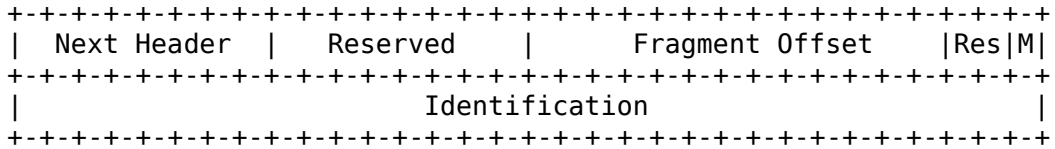



**Fig. B.3** Format de la capçalera Fragment Header [1]

### *B.2.2.3 Authentication Header (AH)*

L'Authentication Header s'utilitza en IPv6 per proporcionar serveis d'integritat de dades, autenticació de l'origen d'una transmissió i *antireplay* per IP. Aquesta capçalera s'assembla a la capçalera IPSec AH [43] usada en IPv4. El camp

*Next Header* l'identifica amb el codi 51 **(Taula B.1)**. En la figura **Fig. B.4** es mostra el seu format:

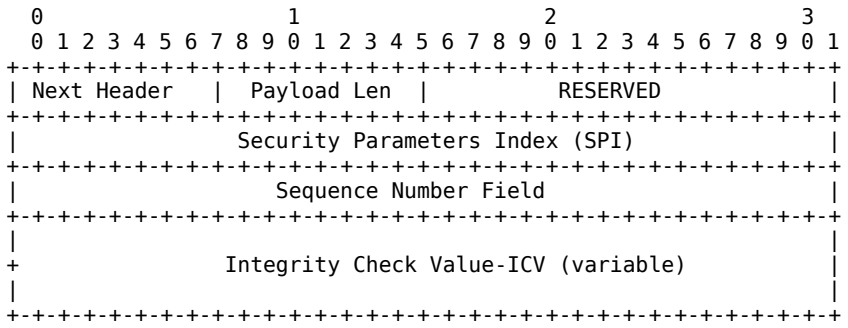



**Fig. B.4** Format de la capçalera Authentication Header [40]

### *B.2.2.4 Encapsulating Security Payload Header (ESP)*

La integritat i la confidencialitat són proporcionades per *Encapsulating Security Payload* (ESP). Es pot utilitzar l'*Authentication Header* juntament amb la ESP per proporcionar autenticació. ESP xifra les dades per a protegir-les i les col·loca en la part de dades de la capçalera ESP, figura **Fig. B.5**. Hi ha dos modes de xifrat:

- Mode Túnel: la capçalera ESP xifra el paquet IPv6 sencer, el qual és col·locat en el camp xifrat. La capçalera ESP llavors es col·loca en una nova capçalera IPv6.
- Mode Transport: la capçalera ESP xifra només els segment de la capa de transport (TCP, UDP, ICMP), col·loca aquestes dades xifrades en el seu camp de xifrat i llavors és col·locat en el paquet original.

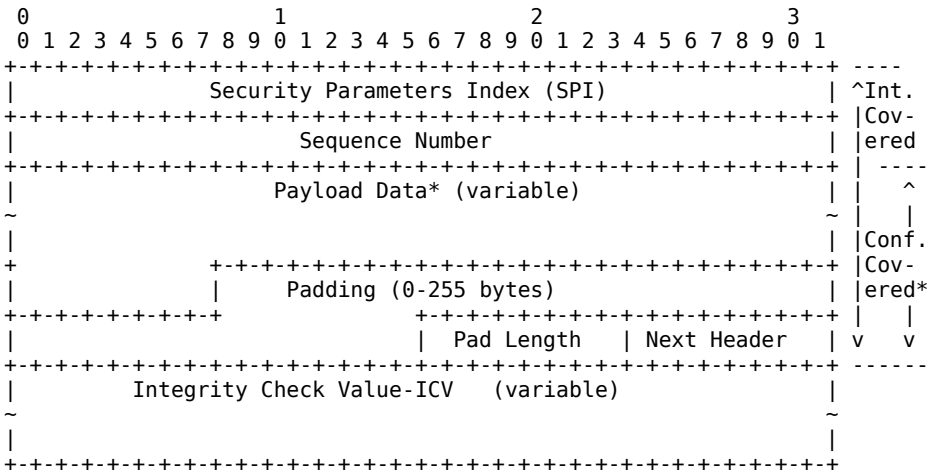



**Fig. B.5** Top-Level Format of an ESP Packet

S’assembla a la idea implementada en IPSec ESP [44] en IPv4. S'identifica amb el codi 50 al camp next header **(Taula B.1)**.

### *B.2.2.5 Mobility Header*

La capçalera *Mobylity Header* [42], és utilitzada en comunicacions entre nodes mòbils, nodes corresponents (*correspondent nodes)* i amb agents domèstics *(home agents)* en l’establiment i el control de *bindings.* S’identifica amb el codi 135 al camp *next header* **(Taula B.1)**.

### *B.2.2.6 No Next Header*

El valor 59 **(Taula B.1)** en el camp “Next Header” de la capçalera IPv6 o en qualsevol capçalera d’extensió indica que no hi ha res a partir d’aquella capçalera.

# ANNEX C. DIFERÈNCIES ADREÇAMENT IPv4 I IPv6

En la **Taula C.1** observem les principals diferències entre l'adreçament IPv4 i IPv6.

**Taula C.1** Principals diferències entre l'adreçament IPv4 i IPv6

| Adreces IPv4 | Adreces IPv6 |
|---|---|
| Classes d'adreces: A, B, C, D, E | No hi ha aquesta classificació, per suportar l'adreçament jeràrquic. |
| *Multicast* 224.0.0.0/4 | *Multicast* ff00::/8 |
| *Broadcast* | No existeixen |
| No especificades 0.0.0.0/32 | No especificades ::/128 |
| *Loopback* 127.0.0.1/32 | *Loopback* ::1/128 |
| IP públiques | *Global Unicast* |
| IP privades (10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16) | *Site-local* fec0::/10 |
| *Autoconfigured* 169.254.0.0/16 | *Link-local* fe80::/10 |
| Representació: notació decimal amb punts | Representació: dos punts amb format hexadecimal amb supressió de començament amb zeros i compressió de zeros. Les adreces compatibles amb IPv4 són expressades com notacions decimals amb punts. |
| Representació de bits de xarxa: *netmask* amb notació decimal amb punts (ex: 255.255.255.0) o com a prefix de longitud (/24) | Representació de bits de xarxa: només com a notació amb prefix de longitud (ex: /64) |
| Resolució de noms DNS: registre de recerca d'adreces de host IPv4 del tipus (A) | Resolució de noms DNS: registre de recerca d'adreces de host IPv6 del tipus (AAAA) |

# ANNEX D. TIPUS D'ADRECES IPv6

**Taula D.1** Quadre resum amb l'assignació d'adreces IPv6

| Tipus d'adreça | Prefix binari | Notació IPv6 |
|---|---|---|
| No assignada | 000...0 (128 bits) | ::/128 |
| Loopback | 000...1 (128 bits) | ::1/128 |
| Multicast | 1111 1111 | ff00::/8 |
| Unique Local Unicast RFC4193 [45] | 1111 110 | fc00::/7 |
| Link-local Unicast | 1111 1110 10 | fe80::/10 |
| Global Unicast RFC3587 [9] | 001 | 2000::/3 |
| Documentation Address RFC 3849 [46] | 2001:db8::/32 | |
| Anycast | Adreces unicast assignades a més d'una interfície | |
| IPv4-Mapped IPv6 | 00...0:1111...1111:IPv4 | ::ffff:IPv4/128 |
| 6to4 | 2002::/16 | |
| IPv4-Compatible IPv6 (desaprovada RFC 4291 [8]) | 00...0 (96 bits) | ::IPv4/128 |
| Site-local Unicast (desaprovada RFC 3879 [47]) | 1111 1110 11 | fec0::/10 |

## D.1 Tipus d'adreces IPv6 unicast

### D.1.1 EUI-64 Modificat RFC4291

El IEEE ha definit un identificador d'interfície únic de 64 bits, anomenat EUI-64 (Extended Unique Identifier), que deriva de les actuals adreces MAC (IEEE 802 MAC), però augmentant la longitud d'aquestes de 48 a 64 bits. El format de l'IDD del EUI-64 Modificat s'obté invertint el bit "u" (bit universal/local) del EUI-64, tal i com es mostra en la figura **Fig. D.1**. El bit es posa a 1 per indicar un abast universal i 0 per indicar un abast local. On "g" és el bit individual/grup. Una adreça MAC es converteix en una adreça EUI-64 de 64 bits inserint "ff:fe" al mig.

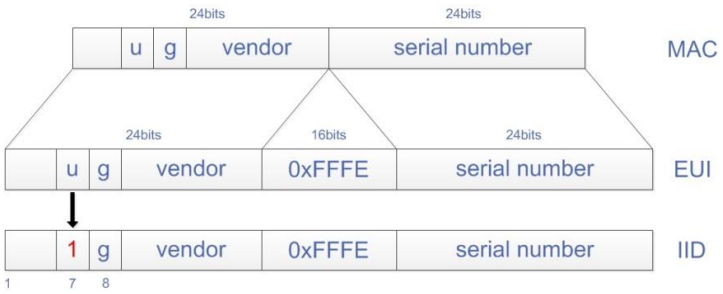



**Fig. D.1** Procés d'obtenció de l'IDD IPv6 a partir de l'adreça MAC

### D.1.2 Adreces Global Unicast RFC3587 [9]

Les adreces "Global Unicast" estan definides per tal de connectar els usuaris a Internet. Són l'equivalent a les adreces públiques IPv4. Aquestes segueixen un model d'adreçament públic basat en una política coordinada de distribució d'adreces a càrrec de les RIR (*Regional Internet Registres*). El RFC 3177 [48] i RFC 6177 [31] assigna a les RIRs les polítiques de distribució d'adreces.

Amb aquesta distribució jeràrquica s'aconsegueix una gran eficàcia en els aspectes d'encaminament, ja que disminueix les grans taules que suporten els principals *routers* d'Internet amb IPv4. El format d'adreça de les adreces "Global Unicast" és el que es mostra en la figura **Fig. D.2**:

```
|         n bits           |   m bits  |       128-n-m bits          |
+--------------------------+-----------+-----------------------------+
| global routing prefix    | subnet ID |        interface ID         |
+--------------------------+-----------+-----------------------------+
```

**Fig. D.2** Format de les adreces Global Unicast [9]

- **Global Routing Prefix:** identifiquen un site connectat a Internet. Aquests n bits són d'estructuració jeràrquica i són assignats per un proveïdor. Típicament de 48 bits.
- **Subnet ID:** aquests m bits identifiquen la subxarxa dins d'un *site* on està localitzada l'adreça. Són els que ens permetran fer el *subnetting*. Mida 16 bits.
- **Interface ID:** són els 64 bits que identifiquen la interfície, seguint el format EUI-64.

### D.1.3 Adreces Link-Local RFC4291

És una adreça unicast d'ús local, equivalent a les adreces privades de IPv4. Les adreces "Link-Local" tenen per objectiu ser usades dins d'un mateix enllaç

de dades (nivell 2) amb finalitats com l'autoconfiguració de l'adreçament, el descobriment de veïns (Neighbor Discovery [49]) o quan no hi ha routers que puguin assignar el prefix de xarxa als nodes d'aquest enllaç. El seu format es mostra en la figura **Fig. D.3**:

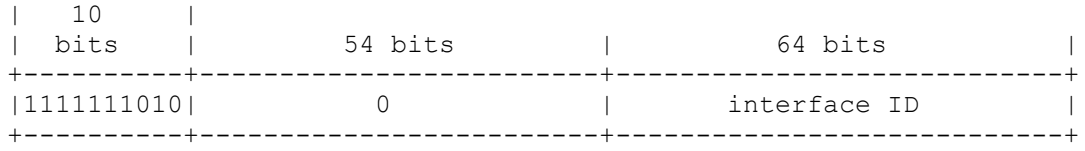



**Fig. D.3** Format de les adreces Link-Local [8]

Els routers no han d'encaminar cap paquet que contingui alguna adreça d'aquest tipus ja que només tenen sentit en un enllaç local.

Quan un node es connecta a un enllaç IPv6, automàticament una adreça Link-Local és assignada a cada interfície del node. Igualment, quan hi ha una renumeració automàtica dels prefixes de xarxa, els routers assignen automàticament adreces Link-Local a tots els nodes de l'enllaç, inclosos ells mateixos.

### D.1.4 Adreces Site-Local RFC4291

També és una adreça unicast d'ús local, equivalent a les adreces privades de IPv4. Les adreces "Site-Local" van ser dissenyades originalment per l'adreçament intern de totes les subxarxes dins d'un "site" sense la necessitat d'usar un prefix global (global unicast). Els encaminadors no poden transmetre cap paquet que contingui alguna adreça d'aquest tipus fora del "site".

Les adreces Site-Local es consideren obsoletes com es defineix en el RFC3879 [47]. El format de les adreces Site-Local es mostra en la figura **Fig. D.4**:

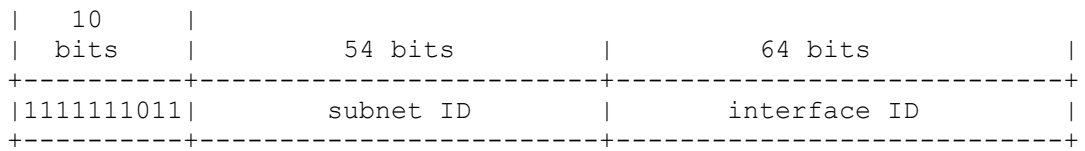



**Fig. D.4** Format de les adreces Site-Local [8]

Les implementacions existents i desplegaments podran seguir utilitzant aquest prefix.

### D.1.5 Adreces Unique-Local (ULA) RFC4193 [45]

Les adreces ULA també són una adreça unicast d'ús local, equivalent a les adreces privades de IPv4. No són adreces enrutables a Internet. Són independents de les adreces proporcionades pels ISP i es poden utilitzar per comunicacions dins d'un "site" que té connectivitat a Internet intermitent o que no en tingui. Des del punt de vista de les aplicacions, s'han d'utilitzar com adreces globals. Com comentem en l'apartat D.1.4, les adreces "Site-Local" estan obsoletes. En el seu lloc s'han d'utilitzar les adreces ULA.

Les adreces IPv6 locals ULA es creen utilitzant una assignació pseudo-aleatòria per la ID global. Aquest fet assegura que no hi ha cap relació entre les assignacions i referma que aquests prefixos no són per ser encaminats globalment. El seu format es pot observar en la figura **Fig. D.5**:

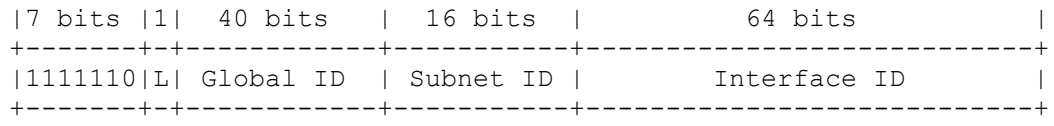



**Fig. D.5** Format de les adreces ULA [45]

On:

- L = 1 si el prefix s'assigna localment.
- L = 0 es pot definir en el futur. A la pràctica s'utilitza per especificar assignacions centrals.

La principal diferència entre les assignacions és que les assignacions centrals són adreces úniques i l'assignació es registra en una base de dades pública.

### D.1.6 Adreces especials IPv6

Hi ha definides una sèrie d'adreces per a usos especials:

- **Adreça no especificada:** L'adreça 0:0:0:0:0:0:0:0 o :: és una direcció no especificada. Indica la absència d'adreça. No es pot assignar a un node ni utilitzar-se com adreça destí. Un exemple del seu ús és, en el moment en que un host vol aconseguir la seva adreça IPv6 de forma automàtica, envia un paquet de sol·licitud en què indica que la seva adreça origen és la no especificada per mostrar que no té direcció.
- **Adreça de loopback:** L'adreça unicast 0:0:0:0:0:0:0:1 o ::1 és l'adreça loopback que té la mateixa funció que en IPv4 (127.0.0.0), enviar-se paquets a si mateix. No es pot utilitzar per enviar paquets a fora del node. No s'ha d'assignar mai a cap interfície física ja que el seu significat és lògic.
- **Adreça IPv4-compatible:** (desaprovada) Els mecanismes de transició

d'IPv6 [23].

- **Adreça IPv4-mapped:** És una adreça IPv6 que conté una adreça IPv4. Aquesta adreça s'utilitza per representar adreces IPv4 com adreces IPv6, les adreces dels nodes que no suporten IPv6. En la figura **Fig. D.6** podem veure el seu format:

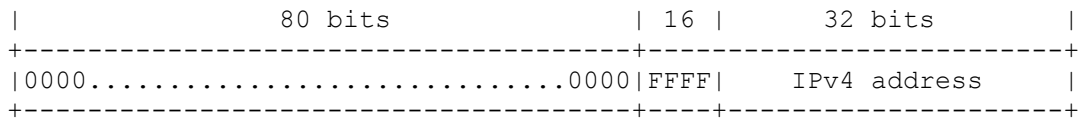



**Fig. D.6** Format de l'adreça IPv4-mapped

## D.2 Tipus d'adreces multicast

Existeixen dos tipus d'adreces *multicast*: les adreces *multicast* predefinides i l'adreça *Solicited-Node Multicast Address.*

- Adreces *multicast* predefinides ("*well-known*") [14]:

L'ús d'aquests *Group ID's* per qualsevol valor d'un altre àmbit, no està permès amb el *flag* T igual a zero.

**Taula D.2** Adreces multicast predefinides

| Adreces *multicast* | Abast | Aplicables | Descripció |
|---|---|---|---|
| ff0X:: | Reservades | Reservades | Reservades |
| ff01::1 | Node | Tots els nodes | Tots els nodes en la interfície local |
| ff02::1 | *Link-Local* | Tots els nodes | Tots els nodes en un enllaç local |
| ff01::2 | Node | Tots els routers | Tots els routers en la interfície local |
| ff02::2 | *Link-Local* | Tots els routers | Tots els routers en un enllaç local |
| ff05::2 | *Site* | Tots els routers | Tots els routers dins d'un *site* |

- Adreces *Solicited-Node Multicast Address:*

Aquesta adreça s'utilitza pel descobriment d'adreces MAC dels veïns mitjançant missatges ICMP i per al descobriment d'adreces duplicades o que ja estan en ús en l'enllaç local.

L'adreça ff02:0:0:0:0:1:ffxx:xxxx (*Solicited-Node Address*, o adreça de node sol·licitada), permet calcular l'adreça *multicast* a partir de la *unicast* o *anycast* d'un determinat node. Per això, es substitueixen els 24 bits de menor pes ("x")

pels mateixos bits de l'adreça original. Així, l'adreça 4037::01:800:200e:8c6c es convertiria en ff02::1:ff0e:8c6c.

Cada node ha de calcular i unir-se a totes les adreces *multicast* que l'hi corresponen per cada adreça *unicast* y *anycast* que té assignada.

### D.2.1 Exemple del camp Group ID en les adreces multicast permanents i transitòries

*Group ID*: Identifica el grup *multicast*, tant permanent com transitori, dins d'un determinat àmbit.

Per exemple, si assignem una adreça *multicast* permanent amb l'identificador de grup 101 (hexadecimal) al grup dels servidor de temps (NTP), llavors:

- ff01::101 significa tots els NTP en el mateix node que el paquet origen.
- ff02::101 significa tots els NTP en el mateix enllaç que el paquet origen.
- ff05::101 significa tots els NTP en el mateix lloc que el paquet origen.
- ff0E::101 significa tots els NTP a Internet.

Les adreces *multicast* transitòries, només tenen sentit en el seu propi àmbit. Per exemple, un grup identificat per l'adreça temporal *multicast* local de lloc ff15::101, no té cap relació amb un grup utilitzant la mateixa adreça en un altre lloc, ni amb un altre grup temporal que utilitzi el mateix identificador de grup (en un altre àmbit), ni en un grup permanent amb el mateix identificador de grup.

# ANNEX E. FUNCIONALITATS D'IPv6

## E.1 Protocols d'encaminament IPv6

### E.1.1 RIPng. RFC 2080 [50] i 2081 [51]) [18]

Les especificacions del Protocol d'Informació de Rutes (RIP – "Routing Information Protocol") per IPv6, recull els canvis mínims i indispensables al RFC1058 [52] i RFC1723 [53] pel seu adequat funcionament.

RIPng és un protocol pensat per petites xarxes i s'inclou en el grup de protocols de passarel·la interior (IGP – "Interior Gateway Protocol"), el qual utilitza un algoritme de vector-distància. Es basa en l'intercanvi d'informació entre encaminadors, de forma que puguin calcular les rutes més adequades de forma automàtica.

RIPng només es pot implementar als *routers* que tenen el requeriment de la mètrica o nombre de salts (entre 1 i 15) d'un paquet per arribar a un destí determinat. Cada salt suposa un canvi de xarxa, normalment travessant un nou *router*. A més de la mètrica, cada xarxa tindrà un prefix i la longitud de l'adreça destí. Aquets paràmetres els configura l'administrador de la xarxa.

El *router* incorporarà a la taula d'encaminament, una entrada per cada destí accessible pel sistema. Cada entrada tindrà com a mínim els següents paràmetres:

- El prefix IPv6 del destí.
- La mètrica.
- L'adreça IPv6 del següent *router* i una ruta per arribar a ell.
- Un indicador relatiu al canvi de ruta.
- Varis comptadors associats a la ruta.

També podran crear rutes internes (salts entre interfícies del propi *router*) o rutes estàtiques.

RIPng és un protocol basat en UDP. Cada *router* té un procés que envia i rep datagrames al port 521 (RIPng). L'inconvenient de RIPng, comú en la versió IPv4, és la seva orientació a petites xarxes (15 salts com a màxim), on la mètrica és fixe i no pot variar en funció de les circumstàncies de temps real (retards, fiabilitat, carrega, etc.).

### E.1.2 OSPFv3. RFC 5340 [54] [18]

El protocol d'encaminament OSPF (*Open Shortets Path Firts*), és un protocol IGP basat en una tecnologia d'estat d'enllaços ("link-state").
Es tracta d'un protocol d'encaminament dinàmic que detecta ràpidament camins de la topologia (com una fallada en un *router* o interfície) i calcula la

següent ruta disponible (sense bucles) després d'un curt període de convergència amb molt poc tràfic de *routing*.

Cada encaminador manté una base de dades que descriu la topologia del sistema autònom, anomenat base de dades de l'estat dels enllaços. Tots els *routers* del sistema tenen una base de dades idèntica, indicant l'estat de cada interfície i de cada destí del sistema autònom. Si hi hagués vàries rutes amb el mateix cost cap a un destí, el tràfic es distribueix equilibradament entre totes. El cost d'una ruta es descriu per una mètrica simple, sense dimensió.

Es poden crear àrees o agrupacions de xarxes (de forma jeràrquica), on la seva topologia no es retransmesa a la resta del sistema, evitant tràfic innecessari.

OSPF permet l'ús de diferents màscares per la mateixa xarxa (*variable length subnetting*), i permet l'encaminament a les millors rutes (les més llargues o més específiques). Tots els intercanvis del protocol OSPF són autentificats. Només poden participar els *routers* verificats (*trusted*).

OSPFv6 manté els mecanismes fonamentals de la versió per IPv4. S'han modificat alguns paràmetres de la semàntica del protocol, com l'increment de la mida de l'adreça. OSPFv6 s'executa basat en cada enllaç, en lloc de cada subxarxa. S'ha eliminat l'autenticació del protocol OSPFv3 perquè IPv6 incorpora aquestes característiques (AH i ESP, apartat 1.3.6).

Tot i que la longitud de les adreces IPv6 és més gran, els paquets OSPFv3 són tant compactes com amb la versió IPv4, eliminant algunes limitacions i flexibilitzant la manipulació d'adreces.

### E.1.3 MP-BGP4 (BGP4+) RFC 4760 [55] i 2545 [56] [18]

El protocol BGP (*Border Gateway Protocol*) és un protocol d'encaminament per la interconnexió de sistemes autònoms (encaminament entre diferents dominis). S'utilitza per grans corporacions i per la connexió entre proveïdors de serveis (ISP's).

La seva funció principal és l'intercanvi d'informació de disponibilitat o abast entre varis sistemes BGP. Inclou la informació dels sistemes autònoms que conté, permetent construir les rutes més adequades i evitar bucles de tràfic.

MP-BGP4 incorpora mecanismes per suportar encaminament entre dominis sense classes (*classeless interdomain routing*), com l'ús de prefixos, l'agregació de rutes i tots els mecanismes en que es basa IPv6.

BGP es basa en un dispositiu que només informa als altres dispositius que es connecten a ell sobre les rutes que ell utilitza. És una estratègia "salt a salt". L'inconvenient, és que aquest mecanisme no permet polítiques complexes.

BGP utilitza TCP com a protocol de transport a través del port 179.

MP-BGP4 afegeix a BGP, extensions multiprotocol, tant per IPv6 com per altres protocols com IPX.

### E.1.4 Integrated IS-ISv6. RFC 5308 [57] [58]

IS-IS (*Intermediate System to Intermediate System*) és un protocol IGP de tipus *link-state* que utilitza l'algoritme de Dijkistra per calcular les rutes.

IS-IS va ser originalment desenvolupat per funcionar sobre el protocol CLNS, però la versió *Integrated* IS-IS permet encaminar tant paquets de xarxa IP com OSI. Per fer-ho, utilitza un identificador de protocol, NLPID, per informar quin protocol de xarxa es fa servir.

De la mateixa forma que OSPF, IS-IS també permet treballar la xarxa de forma jeràrquica. Per tractar l'encaminament IPv6 no es va definir una nova versió d'IS-IS, sinó que es van agregar noves funcionalitats a la versió existent.

Es van agregar dues noves TLVs (*Type-Lenght-Values*):

- IPv6 *Reachability* (*type 236*). Transporta informació de les xarxes accessibles.
- IPv6 *Interface Address* (*type* 232). Indica les adreces IP de la interfície que està transmetent el paquet.

També s'ha agregat un nou identificador de la capa de xarxa.

- IPv6 NLPID. El seu valor és 142.

El procés d'establiment de veïns no varia.

## E.2 Format dels missatges ICMPv6

**Taula E.1** Format dels missatges ICMPv6.

| Missatges d'error ICMPv6 | | |
|---|---|---|
| Tipus | Descripció i Codis | |
| 1 | Destí no accessible (*Destination Unreachable*) | |
| | Codi | Descripció |
| | 0 | Sense ruta cap al destí |
| | 1 | Comunicació prohibida administrativament |
| | 2 | Sense assignar |
| | 3 | Adreça no accessible |
| | 4 | Port no accessible |
| 2 | Paquet massa gros (*Packet Too Big)* | |
| 3 | Temps excedit (*Time Exceeded*) | |
| | Codi | Descripció |

| | | |
|---|---|---|
| | 0 | Límit de salts excedit |
| | 1 | Temps de desfragmentació excedit |
| 4 | Problema de paràmetres (*Parameter Problem*) | |
| | Codi | Descripció |
| | 0 | Camp erroni a la capçalera |
| | 1 | Tipus de “capçalera següent” desconeguda |
| | 2 | Opció IPv6 desconeguda |
| Missatges informatius ICMPv6 | | |
| Tipus | Descripció | |
| 128 | Sol·licitud d’eco (*Echo Request*) | |
| 129 | Resposta d’eco (*Echo Reply*) | |

## E.3 Tipus de missatge ICMPv6 del protocol Neighbor Discovery

**Taula E.2.** Tipus de missatge ICMPv6 del protocol *Neighbor Discovery*.

| Tipus de ICMPv6 | Nom del missatge | Descripció |
|---|---|---|
| 133 | *Router solicitation (RS)* | Sol·licitud de *router* per part d’un host, espera rebre missatge *router advertisement.* |
| 134 | *Router advertisement (RA)* | Els *routers* es donen a conèixer la presència en resposta del missatge anterior. |
| 135 | *Neighbor solicitation (NS)* | Enviat per un node per determinar l’adreça a nivell d’enllaç d’un veí, o verificar que pot arribar-hi via una adreça que manté en *caché*. També s’utilitza per detecció d’adreces duplicades. |
| 136 | *Neighbor advertisement (NA)* | Resposta al missatge anterior. També es pot utilitzar sense demanda prèvia per anunciar un canvi en l’adreça de nivell d’enllaç. |
| 137 | *Redirect message* | Utilitzat pels *routers* per informar als hosts d’un millor camí de sortida cap a un destí. |

# ANNEX F. ANÀLISIS DE LA XARXA DEL CTTC

## F.1 Topologia de la xarxa del CTTC

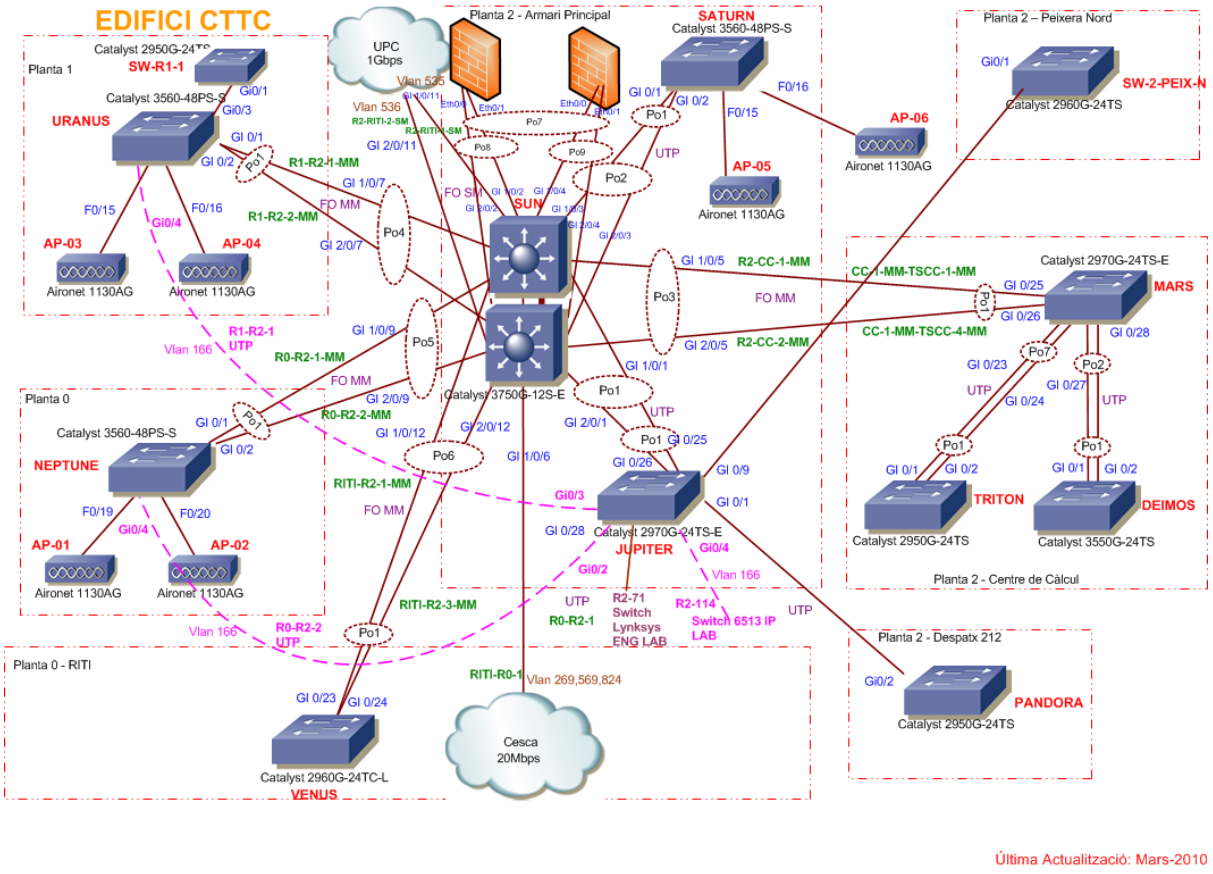



**Fig. F.1** Topologia de la xarxa del CTTC

## F.2 Anàlisis d'equips existents a la xarxa del CTTC

**Taula F.1** Anàlisis d'equips existents a la xarxa del CTTC.

| Nom equip | Model | Firmware | Soporta IPv6? | Acció a realitzar |
|---|---|---|---|---|
| Deimos | Cisco WS-C3550-24-SMI | c3550-ipbasek9-mz.122-25.SEE2 | No | Substituir l'equip |
| Firewall1 | Cisco ASA 5510 | Cisco ASA Version 8.4(2) | Si | - |

| | | | | |
|---|---|---|---|---|
| Firewall2_failover | Cisco ASA 5510 | Cisco ASA Version 8.4(2) | Si | - |
| Jupiter | Cisco WS-C2970G-24TS-E | c2970-lanbasek9-mz.122-25.SEE2 | No | Substituir l'equip |
| Mars | Cisco WS-C2970G-24TS-E | c2970-lanbasek9-mz.122-25.SEE2 | No | Substituir l'equip |
| Neptune | Cisco WS-C3560-48PS-S | c3560-advipservicesk9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(46)SE |
| Pandora | Cisco WS-C2950G-24-EI | c2950-i6k2l2q4-mz.121-22 | No | Substituir l'equip |
| Saturn | Cisco WS-C3560-48PS-S | c3560-advipservicesk9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(46)SE |
| Sun1 | Cisco WS-C3750G-12S-E | c3750-advipservicesk9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(46)SE |
| Sun2 (Master) | Cisco WS-C3750G-12S-E | c3750-advipservicesk9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(46)SE |
| sw-r2-peix-n | Cisco WS-C2960-24TT-L | c2960-lanbasek9-mz.122-46.SE | Si | - |
| sw-r1-1 | Cisco WS-C2960-24TT-L | c2960-lanbasek9-mz.122-46.SE | Si | - |
| Triton | Cisco WS-C2950G-24-EI | c2950-i6k2l2q4-mz.121-22 | No | Substituir l'equip |
| Uranus | Cisco WS-C3560-48PS-S | c3560-advipservicesk9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(46)SE |
| Venus | Cisco WS-C2960G-24TC-L | c2960-lanbasek9-mz.122-25.SEE2 | Si | Actualitzar IOS a una versió superior a la 12.2(58)SE2 |

# F.3 Topologia proposada de la xarxa del CTTC

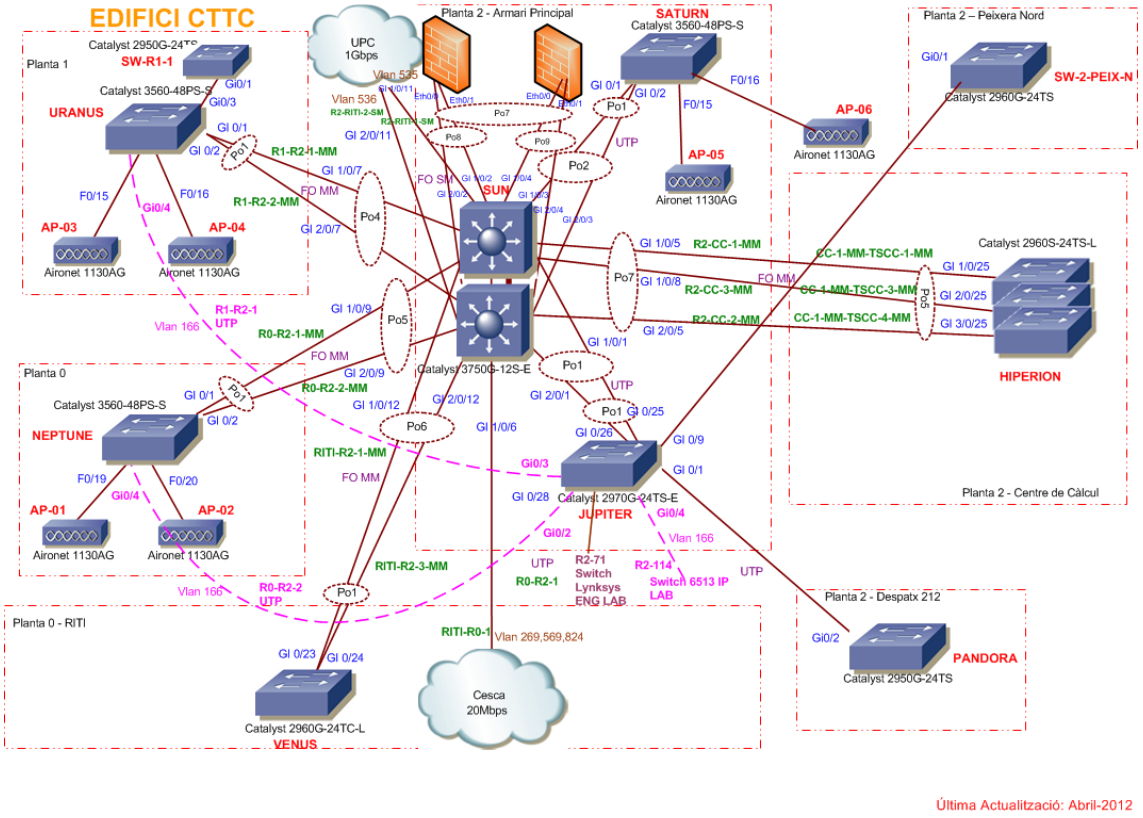



**Fig. E.2** Topologia proposada de la xarxa del CTTC

# ANNEX G. PETICIÓ DEL RANG D'ADRECES IPv6

## G.1 Formulari de petició d'adreçament IPv6 pel CTTC al CESCA.

Una institució, per demanar adreces IPv6 al CESCA, ha d'omplir els següents formularis: el formulari de petició d'adreces IPv6 perquè el CESCA tramiti la sol·licitud amb RIPE i el formulari de petició d'anunci de xarxes mitjançant el sistema autònom de l'Anella Científica per encaminar el rang d'adreces /48 que ens assignen.

### G.1.1 Formulari de petició d'adreces IPv6

```
================================================================================
                    Formulari de petició d'adreces IPv6
================================================================================

Darrera actualització: Març de 2011

L'assignació d'adreces IP requereix el registre i la publicació de les dades
personals dels representants executiu i tècnic de la Institució a la base de
dades de RIPE accessible al públic a través d'Internet, com a contacte
administratiu i tècnic respectivament. En el cas de les universitats, el
contacte administratiu es pot delegar en el Director de Serveis Informàtics.
Mitjançant l'enviament d'aquest formulari, el sol·licitant dóna el seu
consentiment tàcit per a aquesta comunicació i tractament. El CESCA es
compromet a tractar les dades personals d'acord amb la clàusula referent a
la protecció de dades personals del conveni d'adhesió a l'Anella
Científica.

Talleu per aquí, ompliu i envieu a l'adreça ac-nic@suport.cesca.cat juntament
amb un plànol de la xarxa, en cas que el tingueu disponible.


----------8<------------8<-----------8<-----------8<-----------8<----------8<

    - Tipus de connectivitat externa:
      | | Accés per RedIRIS
      | | Accés exclusiu per la connexió pròpia del CESCA


En ambdós casos les xarxes també obtindran connectivitat a través de l'Anella
Científica i el Punt Neutre d'Internet a Catalunya (CATNIX).
```

```
---·---·---·---·-- A partir d'aquí és informació per a RIPE --·---·---
·---·---

#[GENERAL INFORMATION]#

request-type: ipv6-enduser-assignment
form-version: 1.1
x-ncc-regid: es.cesca

#[REQUIRED INFORMATION]#
%
% Do you and the End User accept the IPv6 Address
% Allocation and Assignment Policy? (Yes/No)

confirmation: yes

% Why does the End User site need more than a /48?

reason: Only need a /48

#[OVERVIEW OF ORGANISATION TEMPLATE]#
%
% Who will use the requested address space?

organisation-name: Centre Tecnològic de Telecomunicacions de Catalunya
(CTTC)
organisation-location:  Av.  Carl  Friedrich  Gauss  7  -CP:08860  -
Castelldefels -Barcelona (Spain)
org-description:  The  Centre  Tecnològic  de  Telecomunicacions  de
Catalunya (CTTC) is a research institute
and  technology  center  devoted  to  physical  layer  technologies  for
communications systems.
website-if-available: http://www.cttc.es

% Will the whole organisation use this assignment? If
% another part of the organisation will request separate
% IPv6 address space, please inform us below. (Whole/Part)

for-whole-or-part-of-the-organisation: whole

#[USER TEMPLATE]#
%
% Who is the contact person for this organisation?

name: David Company Estall
phone: +34 936452926
fax-no: +34 936452901
e-mail: david.company@cttc.es
nic-hdl:

#[IPv6 ASSIGNMENT USAGE PLAN]#
%
% When will the End User use this IPv6 assignment?
%
%       Subnet       Within     Within   Within
%       size (/nn)   3 months   1 year   2 years   Purpose

subnet:  /48           x                     General purpose
subnet:
```

```
% Which netname will you use for this assignment?

netname: CTTC

#[INSERT SUPPLEMENTAL COMMENTS]#
%
% Please add more information if you think it will help us
% understand this request.

<add more information>

#[END of REQUEST]#
```

**Fig. G.1** Formulari de petició d'adreces IPv6 al CESCA

### G.1.2 Formulari de petició d'encaminament del rang d'adreces del CTTC

```
Formulari de sol·licitud d'anunci de xarxes
===========================================
mitjançant el Sistema Autònom de l'Anella Científica
====================================================


Talleu per aquí, ompliu i envieu a l'adreça ac-noc@cesca.es.


----------8<------------8<-----------8<-----------8<-----------8<-----
------8<


La institució sol·licita l'anunci al sistema autònom de l'Anella
Científica (AS13041) de la xarxa o les xarxes que es detallen a
continuació.

La institució sol·licitant es responsabilitza d'assegurar que els seus
usuaris coneguin i usin els recursos i serveis de l'Anella Científica
d'acord amb els paràmetres d'ètica i correcció descrits a
http://www.cesca.es/info/politica_ac, i és conscient i accepta que
l'incompliment dels compromisos indicats a aquest document poden
portar a una desconnexió temporal o permanent de les xarxes per a les
que sol·licita connexió.


    -   Nom de la institució sol·licitant: CENTRE TECNOLÒGIC DE
TELECOMUNICACIONS DE CATALUNYA (CTTC)


    -  Punt d'accés directe:
       |X| Nou
       | | Ja existent
           En aquest cas, indiqueu de quin punt d'accés es tracta:


    -  Adreçament:
```

```
       | | Propi de la institució? (com a proveïdor (LIR) o
independents de proveïdor (PI) dins del CESCA)
       |X| Assignat pel CESCA dins del rang de l'Anella Científica
       | | D'una altra institució?
           En aquest cas, indiqueu de quin punt d'accés es tracta:


   -  Nom, número de les xarxes per a les que es sol·licita la
inclusió? al sistema autònom de l'Anella Científica i número de
Sistema Autònom si es disposa d'aquest.

Nom de xarxa     Número de xarxa     Número de Sistema Autònom (AS)
-------------------------------------------------------------------
CTTC        2001:40B0:7C22::/48
```

**Fig. G.2** Formulari de sol·licitud d'anunci de xarxes mitjançant el Sistema Autònom de l'Anella Científica

### G.1.3 Comprovació a la BBDD RIPE

Comprovem que s'ha crear correctament l'objecte a la BBDD de RIPE [59], figura **Fig. G.3**:

```
Responsible organisation: Consorci de Serveis Universitaris de
Catalunya
Abuse contact info: eriac@csuc.cat
```

- inet6num: 2001:40b0:7c22::/48
- netname: CTTC
- descr: CTTC
- country: ES
- admin-c: MAL20-RIPE
- tech-c: DCE5-RIPE
- remarks: ----------
- remarks: spam/security incidents: eriac@cesca.cat
- remarks: ----------
- status: ASSIGNED
- mnt-by: CESCA-MNT
- mnt-irt: IRT-CESCA-CSIRT
- created: 2011-12-13T07:52:49Z
- last-modified: 2011-12-13T07:52:49Z
- source: RIPE

- person: David Company Estall
- address: CTTC
- address: Av. Carl Friedrich Gauss 7
- address: Castelldefels, Barcelona, 08860
- address: ES
- e-mail: david.company@cttc.es
- phone: +34 93 6452926
- fax-no: +34 93 6452901
- notify: admin-ripe@cesca.cat

- mnt-by: CESCA-MNT
- nic-hdl: DCE5-RIPE
- created: 2011-12-13T07:46:10Z
- last-modified: 2011-12-13T12:19:51Z
- source: RIPE

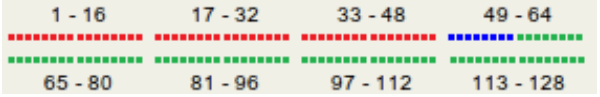
- person: Miguel A. Lagunas
- address: CTTC
- address: Av. Carl Friedrich Gauss 7
- address: Castelldefels, Barcelona, 08860
- address: ES
- phone: +34 93 6452900
- fax-no: +34 93 6452901
- notify: admin-ripe@cesca.cat
- abuse-mailbox: abuse@rediris.es
- mnt-by: CESCA-MNT
- nic-hdl: MAL20-RIPE
- created: 2003-09-18T09:41:47Z
- last-modified: 2011-12-13T12:25:04Z
- source: RIPE

- route6: 2001:40b0::/32
- descr: Anella Cientifica RREN
- origin: AS13041
- notify: admin-ripe@cesca.cat
- mnt-by: CESCA-MNT
- created: 2005-03-07T12:29:58Z
- last-modified: 2011-04-29T07:35:58Z
- source: RIPE

**Fig. G.3** Comprovació de l'adreçament IPv6 a la BBDD RIPE

# ANNEX H. DISTRIBUCIÓ DEL RANG D'ADRECES IPv6 AL CTTC

**Taula H.1** Distribució del rang d'adreces IPv6 del CTTC amb /56

| RANG CTTC | # /56 | ESQUEMA |
|---|---|---|
| 2001:40b0:7c22::/48 | 256 /56 |   |

**Taula H.2** Distribució del rang d'adreces IPv6 al CTTC

| ASSIGNACIÓ | XARXA |
|---|---|
| CSI | 2001:40b0:7c22:6000:0000:0000:0000:0000/56<br>2001:40b0:7c22:6000::/56 |
| COMMUNICATION NETWORKS | 2001:40b0:7c22:7000:0000:0000:0000:0000/56<br>2001:40b0:7c22:7000::/56 |
| COMMUNICATION SYSTEMS | 2001:40b0:7c22:7100:0000:0000:0000:0000/56<br>2001:40b0:7c22:7100::/56 |
| COMMUNICATION TECHNOLOGIES | 2001:40b0:7c22:7200:0000:0000:0000:0000/56<br>2001:40b0:7c22:7200::/56 |
| GEOMATICS | 2001:40b0:7c22:7300:0000:0000:0000:0000/56<br>2001:40b0:7c22:7300::/56 |
| CSI | 2001:40b0:7c22:aa00:0000:0000:0000:0000/56<br>2001:40b0:7c22:aa00::/56 |

# ANNEX I. REGLES D'ACCÉS ENTRANT IPv6 DEL FIREWALL

Veure esquema figura **Fig. 2.1** Esquema lògic de la xarxa de dades del CTTC amb connectivitat IPv4 i IPv6 per ubicar les interfícies de la **Taula I.1**.

**Taula I.1** Regles d'accés entrant IPv6 del Firewall aplicades a les interfícies

| Interfície | | Source | Destination | Service | Action |
|---|---|---|---|---|---|
| Cesca_IPv6 IPv6 | Telvent_IPv6 IPv6 | 2001:40b0:1::48 | any :: | Protocol: icmp6 (58) | Permit |
| | | any :: | Name: ipv6_web<br>IP: 2001:40b0:7c22:6022::dddd:198 | TCP: http (80) | Permit |
| | | any :: | any :: | ICMP6: echo-reply (129) | Permit |
| | | any :: | Name: ARIES<br>IP: 2001:40b0:7c22:6020::194 | TCP-UDP: domain (53) | Permit |
| DMZ1 IPv6 | | any :: | any :: | Protocol: ip (0) | Permit |
| dhcp IPv6 | | any :: | any :: | Protocol: ip (0) | Permit |
| inside IPv6 | | any :: | any :: | Protocol: ip (0) | Permit |
| servers IPv6 | | any :: | any :: | Protocol: ip (0) | Permit |
| Global IPv6 | | any :: | any :: | Protocol: ip (0) | Deny |

# ANNEX J. SERVEIS

En aquest apartat trobem una petita introducció al servei i la configuració bàsica aplicada en la implementació del servei DNS i del web del CTTC per tal de donar resposta a les peticions IPv6.

## J.1 Servei DNS al CTTC

### J.1.1 DNS. RFC1886 [60], RFC3596 [61], [18] i [62]

El protocol de DNS "Sistema de Noms de Domini" (Domain Name Server) tradueix noms de domini a adreces de xarxa tant d'IPv4 com d'IPv6, és un mecanisme fonamental a Internet.

Aquest mecanisme, definit per IPv4 (RFC1034 [63] i RFC1035[65]), va ser actualitzat pel (RFC1886 [60]), bàsicament introduint un nou registre AAAA per IPv6, un nou domini per suportar les localitzacions (*lookups*) basades en IPv6 i definicions actualitzades de la llista de DNS record types.

Perquè resolgui adreces de 128 bits, s'han de definir les següents extensions que acabem de mencionar:

- Un nou registre per mapejar adreces IPv6, el registre AAAA.
- Un nou domini de registres PTR per a la resolució inversa. La diferència amb el d'IPv4 és la notació utilitzada per representar les adreces IPv6 (utilitzant nibbles7) i en el nom del domini utilitzat (.IP6.ARPA).
- Redefinició de les consultes exitents (DNS record types), perquè puguin processar adreces IPv6.

Es recomana que tots els servidors DNS siguin de doble-pila, és a dir, capaços de fer peticions DNS sobre IPv4 i IPv6. S'assegura la compatibilitat amb els servidors ja existents.

### J.1.2 Servidor DNS IPv6

Hi han diversos programes de servidor DNS que funcionen amb IPv6, al CTTC tenim implementat el BIND (Berkeley Internet Name Domain) [65]. Al centre tenim un servidor DNS primari, Aries, que és visible també des de l'exterior i un servidor secundari esclau, Apolo, que només és visible a la xarxa del CTTC. A la **Taula J.1** observem les característiques del servidor Aries.

[7] **Nibbles**: són 4 bits; es sol representar en format hexadecimal separat per punts (".")

**Taula J.1** Caraterístiques del servidor DNS primari, Aries.

| | |
|---|---|
| SO del Servidor | Ubuntu 16.04.1 LTS |
| Tipus de Màquina | Màquina virtual en clúster VMWare |
| Processador | Intel Xeon CPU E5620 @ 2,4GHz |
| Mem. RAM | 500MB |
| Programari | BIND 9.10.3-P4-Ubuntu |

Per configurar el servei DNS amb suport IPv6 a les dues màquines, primer les proveïm d'adreçament IPv6, veure **Taula J.2**.

**Taula J.2** Adreçament dels servidors DNS del CTTC.

| | ARIES | APOLO |
|---|---|---|
| Adreça | 2001:40b0:7c22:6020::194 | 2001:40b0:7c22:6020::220 |
| Màscara | /64 | /64 |

- **Configuració del servidor DNS master** (Aries):

L'arxiu de configuració principal del DNS es troba a */etc/bin/named.conf*, aquest inclou la directiva *included* amb els arxius */etc/bind/named.conf.options i* /etc/bind/named.conf.local

Per habilitar l'escolta d'IPv6 del servidor s'ha d'afegir a l'arxiu /etc/bind/named.conf.options a la secció options la directiva: *listen-on-v6 { any; };*

Configurarem també els arxius hosts que contenen les màquines del domini.

A l'arxiu */etc/bind/named.conf* no hi realitzem canvis, aquests els realitzem ens el fitxers que estan referenciats.

*include "/etc/bind/named.conf.options";*
*include "/etc/bind/named.conf.local";*

A l'arxiu */etc/bind/named.conf.local d*efinim la zona interna i externa pel nostre adreçament invers IPv6 (figura **Fig. J.1**), *2.2.c.7.0.b.0.4.1.0.0.2.ip6.arpa*, la zona d'adreçament directe ja estava definida per IPv4.

```
zone "2.2.c.7.0.b.0.4.1.0.0.2.ip6.arpa" IN {
type master;
file "hosts.2001:40b0:7c22-int";
allow-update { none; };
allow-transfer { 2001:40b0:7c22:6020:220; 2001:40b0:7c22:6020::200; };
also-notify { 2001:40b0:7c22:6020:220; 2001:40b0:7c22:6020::200; };
};

zone "2.2.c.7.0.b.0.4.1.0.0.2.ip6.arpa" IN {
```

```
type master;
file "hosts.2001:40b0:7c22";
allow-update { none; };
allow-transfer { secondary-nameservers; };
also-notify        {2001:720:418:caf1::2;        2001:720:418:caf1::3;
2001:40b0:1:1122:ce5c:a000:0:5; 2001:40b0:1:1122:ce5c:a000:0:3;};
};
```

**Fig. J.1** Zona adreçament invers IPv6 interna i externa

Als arxius de configuració de les zones afegim les nostres entrades de resolució directa i inversa.

Arxius a modificar: /var/cache/bind/hosts.cttc.es, /var/cache/bind/hosts.cttc.es-int, /var/cache/bind/hosts.cttc.cat, /var/cache/bind/hosts.cttc.cat-int, hosts.2001:40b0:7c22 i hosts.2001:40b0:7c22-int, veure figures **Fig. J.2** i **Fig J.3**.

### *hosts.cttc.cat, hosts.cttc.es, hosts.cttc.cat-int i hosts.cttc.es-int*

```
$TTL 86400
@ 1D IN SOA aries.cttc.es. csi.cttc.es. (
2017020801 ; serial YYYYmmddss
86400 ; refresh
3600 ; retry
2592000 ; expiry
172800 ) ; minimum

IN NS aries.cttc.cat.

... ... ...

www IN A 84.88.61.199
IN AAAA 2001:40b0:7c22:6022::dddd:199
networks IN A 84.88.61.199
IN AAAA 2001:40b0:7c22:6022::dddd:199
systems IN A 84.88.61.199
IN AAAA 2001:40b0:7c22:6022::dddd:199
technologies IN A 84.88.61.199
IN AAAA 2001:40b0:7c22:6022::dddd:199
geomatics 1 IN A 84.88.61.199
IN AAAA 2001:40b0:7c22:6022::dddd:199
ipv6 IN AAAA 2001:40b0:7c22:6022::dddd:199
```

**Fig. J.2** Arxiu de configuració de les zones internes i externes dels dominis cttc.es i cttc.cat

### *hosts.2001:40b0:7c22 i hosts.2001:40b0:7c22-int*

```
$TTL 86400 ; 1D
@ IN SOA aries.cttc.es. csi.cttc.es. (
2017020801 ;serial (YYYYMMdd##)
86400 ;refresh
7200 ;retry
2592000 ;expire
```

```
172800 ) ;ttl

4.9.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.6 IN PTR aries.cttc.es.
... ... ...
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR ipv6.cttc.es.
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR www.cttc.es.
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR technologies.cttc.es.
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR systems.cttc.es.
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR networks.cttc.es.
9.9.1.0.d.d.d.d.0.0.0.0.0.0.0.0.0.0.2.2.0.6 IN PTR geomatics.cttc.es.
```

**Fig. J.3** Arxiu de configuració de l'adreçament IPv6 invers intern i extern del CTTC

## J.2 Servei Web al CTTC

El servei web utilitza el protocols HTTP per intercanviar dades entre aplicacions. La navegació web normalment es sol fer pel port 80. Al CTTC el servidor web que tenim implementat és l'Apache [], l'adaptarem perquè doni servei a les peticions IPv6 del web institucional.

A la **taula J.3** observem les característiques del servidor web.

**Taula J.3** Caraterístiques del servidor web.

| | |
|---|---|
| SO del Servidor | Ubuntu 14.04.03 LTS |
| Tipus de Màquina | Màquina virtual en clúster VMWare |
| Processador | Intel Xeon CPU E2620 @ 2GHz |
| Mem. RAM | 3GB |
| Programari | Apache/2.4.7 (Ubuntu) |

Per configurar el servei web amb IPv6 primer proveïm d'adreçament IPv6, veure **taula J.4**.

**Taula J.4** Adreçament IPv6 del servidor web del CTTC.

| | www |
|---|---|
| Adreça | 2001:40b0:7c22:6022::dddd:199 |
| Màscara | /64 |
| DNS | 2001:40b0:7c2::6020::194 |

Afegim al DNS les entrades dels diferents dominis que té el web del CTTC, tal i com em vist a l'anterior subapartat del servei DNS IPv6 J.1.2.

L'ordre que controla les IP i els ports a través dels quals escolta el servidor web és Listen. Es troba als fitxers de configuració principal /etc/apache2/apache2.conf que inclou l'arxiu ports.conf. Per escoltar, per defecte, totes les IP i el port 80 (http) tenim aquesta configuració a l'arxiu ports.conf: *Listen 80*

Per configurar amfitrions virtuals d'IPv6 cal fer servir claudàtors [] per "tancar" l'adreça d'IPv6, en el nostre cas com que el web té diferents dominis que apunten a la mateixa adreça IP afegim * a la configuració de l'arxiu /etc/apache2/sites-available/cttc.es.conf, figura **Fig J.4**:

```
<VirtualHost *:80>
...
</VirtualHost>
```

**Fig. J.4** Configuració del l'arxiu de configuració d'apache perquè mostri el web

Per comprovar que està escoltant a través de l'IPv6 el servidor al port 80 utilitzem l'eina *netstat*, figura **Fig J.5**:

```
netstat -tan
Conexiones activas de Internet (servidores y establecidos)
Proto Recib Enviad Dirección local Dirección remota Estado
...
tcp6 0 0 :::80 :
```

**Fig. J.5** Comprovació que el web esta escoltant peticions pel port 80.

# ANNEX K. ESCENARI BANC DE PROVES

Els equips que apareixen en la figura **Fig. K.1** són els que intervenen en les proves avaluar IPv6 a la xarxa del CTTC.

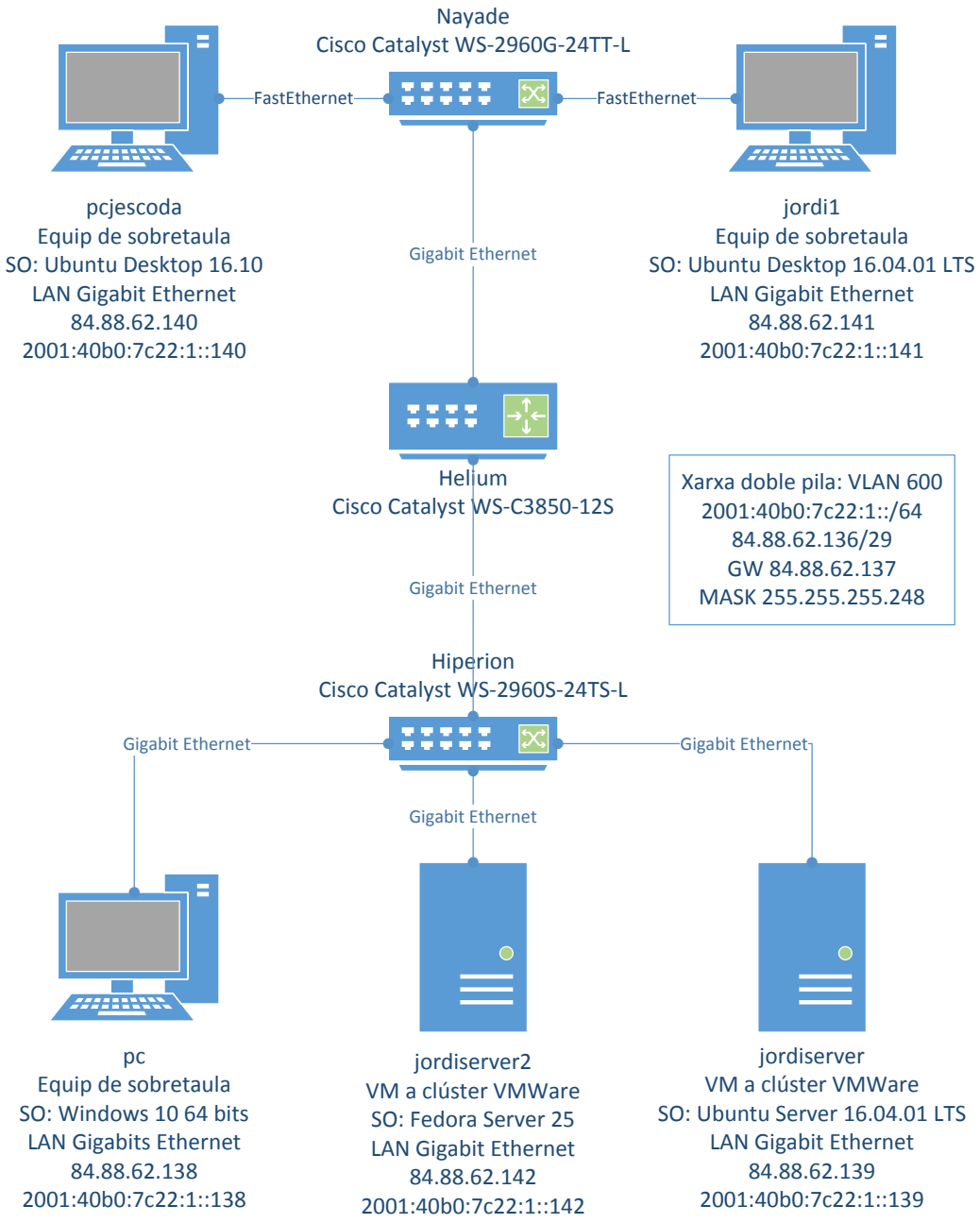



**Fig. K.1** Escenari total del banc de proves al CTTC

Les màquines que intervenen en les proves tenen les següents característiques:

**Taula K.1** Característiques dels equips del Banc de Proves.

| NOM | **jordiserver** | **jordiserver2** |
|---|---|---|
| TIPUS | Màquina virtual en clúster VMWare | |
| SO | Ubuntu Server 16.04 LTS | Fedora Server 25 |
| PROCESSADOR | Intel Xeon CPU E5-2620 @2GHz | |
| MEM. RAM | 1GB | |

| NOM | **pcjescoda** | **pc** |
|---|---|---|
| TIPUS | Equip pc de sobretaula | |
| SO | Ubuntu Desktop 16.10 | Windows 10 Pro x64 |
| PROCESSADOR | Intel Core i5 CPU 760 @ 2,8GHz | |
| MEM. RAM | 8GB | |

| NOM | **jordi1** |
|---|---|
| TIPUS | Equip pc de sobretaula |
| SO | Ubuntu Desktop 10.04.01 LTS |
| PROCESSADOR | Intel Core 2 Quad CPU Q9400 @ 2,66GHz |
| MEM. RAM | 8GB |

# ANNEX L. SCRIPTS BANC DE PROVES

## L.1 Script càlcul Round Trip Time

### pingtest.sh

```
#! /bin/bash
LOGFILE=/var/log/pingtest.log

final=$((SECONDS+3600))
echo "INICI: $(date +%x) $(date +%r)" >> $LOGFILE

printf "Hora\t\tMem\t\tCPU\t\trtt_avg\n" >> $LOGFILE

while [ $SECONDS -lt $final ]; do
      HORA=$(printf '%(%T)T\t' -1)
      MEM=$(free -m | awk 'NR==2{printf "%.2f%%\t\t", $3*100/$2 }')
      CPU=$(top -bn1 | grep load | awk '{printf "%.2f%%\t\t\n", $(NF-
2)}')

      #IPv4 test
      if [ $1 -eq 4 ]; then
                ping=$(ping -c 4 -q $2 | grep rtt | awk -F'/' '{ print
$5 }')

      #IPv6 test
      elif [ $1 -eq 6 ]; then
                ping=$(ping6 -c 4 -q $2 | grep rtt | awk -F'/' '{
print $5 }')
      fi

      echo "$HORA$MEM$CPU$ping" >> $LOGFILE
done

echo "FINAL: $(date +%x) $(date +%r)" >> $LOGFILE
```

## L.2 Script càlcul throughput i recursos equips de xarxa

### descarrega.sh

```
#!/bin/bash

CARPETA=( petit mitja gran enorme )
ARXIUS=( 1.tar 2.tar 3.tar 4.tar 5.tar )

./cisco_hiperion.sh &
pid1=$!
./cisco_helium.sh &
pid2=$!
./cisco_nayade.sh &
pid3=$!

sleep 7

for i in "${CARPETA[@]}"; do
```

```
      for j in "${ARXIUS[@]}"; do
            log=log_$i$j
            nom="$i$j.tar"
#           wget -4 -O $nom http://84.88.62.142/paquets/$i/$j -o $log
            wget               -6               -O               $nom
http://[2001:40b0:7c22:1::138]/paquets/$i/$j -o $log
            #wget -4 o wget -6
            sleep 5
      done
done

kill $pid1
kill $pid2
kill $pid3
```

**cisco_hiperion.sh**
**cisco_helium.sh** modifiquem IP='192.168.2.1' #helium
**cisco_nayade.sh** modifiquem IP='192.168.2.14' #nayade

```
#!/bin/bash

#LOGFILE="/var/log/cpu_mem_nayade.log"
LOGFILE="/var/log/cpu_mem_hiperion.log"
#LOGFILE="/var/log/cpu_mem_helium.log"


final=$((SECONDS+480))
echo "INICI: $(date +%x) $(date +%r)" > $LOGFILE
printf
"Hora\t\tCPU5s\t\tCPU1m\t\tCPU5m\t\tmem_used(MB)\t\tmem_free(MB)\t\tto
tal_mem(MB)\n" >> $LOGFILE

OIDcpu='1.3.6.1.4.1.9.9.109.1.1.1.1'
OIDcpu1m='.1.3.6.1.4.1.9.9.109.1.1.1.1.7'
OIDcpu5m='.1.3.6.1.4.1.9.9.109.1.1.1.1.8'
OIDcpu5s='.1.3.6.1.4.1.9.9.109.1.1.1.1.10'
OIDmem_used=".1.3.6.1.4.1.9.9.48.1.1.1.5.1" #Byte
OIDmem_free=".1.3.6.1.4.1.9.9.48.1.1.1.6.1" #Byte

version='2c'

community='SmartCare'

#IP='192.168.2.14' #nayade
IP='192.168.2.15' #hiperion
#IP='192.168.2.1' #helium

while [ $SECONDS -lt $final ]; do
        HORA=$(printf '%(%T)T\t' -1)

      cpu5s=`/usr/bin/snmpwalk -v 2c -c $community $IP $OIDcpu5s | awk
-F':' '{ printf "%s\t\t",$4}' | sed 's/ //g'`
      cpu1m=`/usr/bin/snmpwalk -v 2c -c $community $IP $OIDcpu1m | awk
-F':' '{ printf "%s\t\t",$4}' | sed 's/ //g'`
        cpu5m=`/usr/bin/snmpwalk -v 2c -c $community $IP $OIDcpu5m |
awk -F':' '{ printf "%s\t\t",$4}' | sed 's/ //g'`

      mem_used=`/usr/bin/snmpwalk -v 2c -c $community $IP $OIDmem_used
| awk -F':' '{ printf $4}' | sed 's/ //g'`
```

```
      mem_free=`/usr/bin/snmpwalk -v 2c -c $community $IP $OIDmem_free
| awk -F':' '{ printf $4}' | sed 's/ //g'`
      mem_total=$(($mem_free + $mem_used))

      #Byte to MB
      mem_used_MB=`echo "scale=3; $mem_used/1024/1024" | bc`
      mem_free_MB=`echo "scale=3; $mem_free/1024/1024" | bc`
      mem_total_MB=`echo "scale=3; $mem_total/1024/1024" | bc`

            echo                                                    -e
"$HORA$cpu5s$cpu1m$cpu5m$mem_used_MB\t\t\t$mem_free_MB\t\t\t$mem_total
_MB" >> $LOGFILE
      sleep 5
done

echo "FINAL: $(date +%x) $(date +%r)" >> $LOGFILE
```

## L.3 Script càlcul Time To First Byte

### ttfb.sh

```
#!/bin/bash

domini=$1
requests=20

versio=$2

log=ttfb.log
rm $log

if [ $versio -eq 4 ]; then
      for ((n=0;n<$requests;n++)); do
            curl  -4  -o  /dev/null  -w  "%{time_starttransfer}  \n"
http://$domini >> $log
      done
else
      for ((n=0;n<$requests;n++)); do
            curl  -6  -o  /dev/null  -w  "%{time_starttransfer}  \n"
http://$domini >> $log
      done
fi

sed 's/,/./g' $log > ttfb.txt

getArray() {
      array=()
      while IFS= read -r line
      do
            array+=("$line")
      done < "$1"
}
getArray "ttfb.txt"

sleep 2

n_array=`echo ${#array[@]}`
```

```
suma=`echo ${array[*]}| awk '{for(i=1;i<=NF;i++){a+=$i;}}END{print
a}'`

mitja=$(bc <<< "scale=6; $suma/$n_array")

echo -e "Protocol IPv$versio \nTime To First Byte (TTFB) promig de
$domini amb $requests peticions: $mitja"
```