

LOCALITZADOR GRÀFIC D'ADRECES IP

Juan Castro Mayorgas

Memòria tècnica corresponent al
projecte de fi de carrera de:

Enginyeria Tècnica d'Informàtica de Sistemes

Universitat Oberta de Catalunya

Primer semestre 2009-2010

Consultor: Maria Isabel March Hermo

Per a la Mayte

AGRAÏMENTS

Des de què vaig començar a treballar en aquest projecte he rebut el suport incondicional de la meva estimada Mayte que, tot i haver vist com molts caps de setmana compartia més temps amb l'ordinador que amb ella, sempre ha estat al meu costat en els moments de dificultat trobats en el projecte.

Vull expressar també el meu agraïment als meus pares, germans i fillola que sempre els he tingut amb mi, i molt especialment al Pol, que amb els seus dos anys m'ha regalat moments d'una alegria sense preu.

RESUM

Internet s'ha convertit en una font extraordinària de recursos per una audiència en constant creixement arreu el món. A l'igual que en altres activitats de la nostra societat, el coneixement de la localització geogràfica d'aquests recursos i de la gent que hi accedeix és útil tant pels usuaris com pels proveïdors d'informació. La geolocalització IP, però, pot donar informació errònia o amb un nivell de precisió que no vagi més enllà de la referència a un país.

Aquest treball recull els diferents actors que formen part de la geolocalització IP i s'ha analitzat el paper que juguen en aquest procés així com la seva influència en el nivell de fiabilitat i exactitud final. Amb aquests sòlids fonaments s'ha desenvolupat una aplicació per representar gràficament en un mapa la geolocalització IP d'un dispositiu i la dels nodes que formen el camí realitzat fins arribar-hi, així com tota la informació addicional que de cada IP s'ha pogut obtenir.

El resultat ha estat una memòria tècnica de tot el treball de recerca juntament amb una aplicació que s'executa en l'entorn de Microsoft Windows i plataforma .NET, caracteritzada per la seva facilitat d'ús gràcies a un disseny simple molt intuïtiu i efectiu, la rapidesa d'execució per què aprofita la programació de fils, i un positiu impacte visual ja que fa servir l'API de *Google Maps* per a la representació visual de la traça.

Paraules clau: IP, traceroute, geolocalització IP, Whois, DNS, Google API, .NET

Nom d'àrea de TFC: Xarxes de computadors

ÍNDIX DE CONTINGUTS

AGRAÏMENTS	ii
RESUM	iii
ÍNDIX DE CONTINGUTS	iv
ÍNDIX DE FIGURES	vi
CAPITOL 1: INTRODUCCIÓ	1
1.1. JUSTIFICACIÓ I CONTEXT EN EL QUAL ES DESENVOLUPA: PUNT DE PARTIDA I APORTACIÓ DEL TFC.....	1
1.2. OBJECTIUS DEL TFC.....	2
1.3. ENFOCAMENT I METODOLOGIA	3
1.4. PLANIFICACIÓ.....	4
1.4.1. Activitat 1: Recerca.....	5
1.4.2. Activitat 2: Traçador de ruta	5
1.4.3. Activitat 3: Obtenció de dades addicionals.....	6
1.4.4. Activitat 4: Visualització	7
1.4.5. Activitat 5: Memòria.....	7
1.4.6. Activitat 6: Presentació virtual.....	8
1.4.8. Diagrama de GANNT.....	8
1.4.9. Desviacions produïdes respecte al pla de treball inicial	8
1.5. PRODUCTES OBTINGUTS.....	9
1.6. BREU DESCRIPCIÓ DELS ALTRES CAPÍTOLS DE LA MEMÒRIA	9
CAPITOL 2: FONAMENTS DE LA GEOLOCALITZACIÓ IP	11
2.1. INTRODUCCIÓ	11
2.2. ADRECES IP	12
2.3. PROTOCOL ICMP.....	14
2.4. DNS INVERTIT.....	16
2.5. DNS-LOC	16
2.6. SERVEI WHOIS	17
2.7. GEOCODIFICACIÓ	20
2.7.1. Yahoo API.....	21
2.7.2. Google Maps API.....	21
2.7.3. Hostip.info.....	22
2.7.4. MaxMind.....	23
2.8. VISUALITZACIÓ EN UN MAPA.....	23

2.9. EXEMPLES D'APLICACIONS EXISTENTS	24
2.9.1. VisualRoute	24
2.9.2. Path Analyzer Pro.....	25
2.9.3. IP Geocaltor.....	27
2.10. CONCLUSIONS	27
CAPITOL 3: EL TRAÇADOR DE RUTA	29
3.1. OBJECTIUS.....	29
3.2. DISSENY I IMPLEMENTACIÓ.....	29
3.2.1. La classe <i>Hop</i>	29
3.2.2. La classe <i>Route</i>	30
3.2.3. Implementació	31
3.2.4. Integració amb la interfície d'usuari.....	33
CAPITOL 4: OBTENCIÓ DE DADES ADDICIONALS.....	34
4.1. OBJECTIUS.....	34
4.2. DISSENY I IMPLEMENTACIÓ.....	34
4.2.1. La classe <i>DomainPool</i>	35
4.2.2. La classe <i>Hop</i> actualitzada.....	36
4.2.3. La classe <i>Route</i> actualitzada.....	37
4.2.4. Implementació	39
4.2.5. Integració amb la interfície d'usuari.....	44
CAPITOL 5: VISUALITZACIÓ	45
5.1. OBJECTIUS.....	45
5.2. DISSENY I IMPLEMENTACIÓ.....	45
Exemples	46
CAPITOL 6: CONCLUSIONS.....	48
BIBLIOGRAFIA	49
ANNEX A: MANUAL D'USUARI.....	51
A.1. REQUISITS	51
A.2. INSTAL·LACIÓ.....	51
A.3. MENÚ.....	51
A.4. UTILITZACIÓ	52

ÍNDIX DE FIGURES

Figura 1. Diagrama GANNT del pla de treball en el seu plantejament inicial	8
Figura 2. Jerarquia de delegació	13
Figura 3. Els cinc RIRs arreu el món	13
Figura 4. Datagrama IP amb missatge ICMP	14
Figura 5. Format del missatge ICMP	14
Figura 6. Exemple de polilínia amb Google API	24
Figura 7. Pantalla de visualització de VisualRoute	25
Figura 8. Dades d'una traça amb Path Analyzer Pro	26
Figura 9. Representació de la traça en un mapa amb Path Analyzer Pro	26
Figura 10. IP Geolocator	27
Figura 11. Procés de traça.....	32
Figura 12. Procés de resolució de nom.....	33
Figura 13. Visualització de part d'una traça	33
Figura 14. Dependència de dades	35
Figura 15. Concurrència de processos	35
Figura 16. Versió resumida del procés de recerca de nodes	40
Figura 17. Procés d'obtenció de la resolució inversa de l'adreça IP.....	40
Figura 18. Procés de consulta WhoisTLD	41
Figura 19. Procés de consulta WhoisNET.....	42
Figura 20. Procés d'obtenció de localització	43
Figura 21. Interfície amb la traça i les dades addicionals.....	44
Figura 22. Area de visualització del mapa	45
Figura 23. Traça a durinn.rhnet.is.....	46
Figura 24. Traça a www.cctld.ru	47
Figura 25. Traça a www.bttb.net.....	47

CAPÍTOL 1

INTRODUCCIÓ

El terme geolocalització està d'actualitat gràcies, sobretot, a la incorporació de la tecnologia GPS en cada vegada més dispositius, com els nous models telèfons mòbils i navegadors per a automòbil i a Google Maps, que ha democratitzat la representació visual d'unes coordenades en mapes de gran qualitat i amb moltes funcionalitats afegides.

La geolocalització és el procés de determinació de la posició geogràfica d'una persona o objecte. El prefix 'geo' serveix per a posar de manifest que aquesta posició s'expressa mitjançant unes coordenades de latitud i longitud que, per inferència, poden derivar en unes dades de carrer, codi postal, ciutat i país. En el context d'Internet, la geolocalització IP és el procés d'identificació, a través de la seva adreça IP, de l'emplaçament geogràfic d'un dispositiu connectat a Internet.

Seguretat, màrqueting, personalització de continguts, preservació de drets, són algunes de les utilitats derivades de la geolocalització IP. Per exemple, Yahoo, presenta a l'usuari la versió localitzada del seu portal en relació al país associat a l'adreça IP origen.

No obstant, la geolocalització IP no sempre és un procés amb resultats precisos. Gairebé la totalitat de recursos que es fan servir per a determinar la localització, són fonts d'informació creades amb altres objectius i el seu ús per a posicionar geogràficament una adreça IP pot donar resultats erronis. Així doncs, a vegades el resultat del procés de determinació de la localització presentarà un grau de precisió molt baix o mostrarà contradiccions depenent de la font d'informació o simplement no serà viable.

1.1. JUSTIFICACIÓ I CONTEXT EN EL QUAL ES DESENVOLUPA: PUNT DE PARTIDA I APORTACIÓ DEL TFC

Considero realment apassionant tot el que envolta Internet i, sobre tot, el seu funcionament. Si més no, han estat les assignatures relacionades amb xarxes (Xarxes de

Computadors, Estructura de Xarxes de Computadors i Seguretat en Xarxes de Computadors), les que he trobat més enriquidores encara que, al mateix temps, complexes.

L'opció de desenvolupar un treball de fi de carrera en l'àrea de xarxes era una oportunitat que no podia desaprofitar. Tota l'oferta de projectes dintre de l'àrea era igualment atractiva però l'elecció del **Localitzador Gràfic d'Adreces IP** ha vingut condicionada per la convicció de què no només seria el producte final d'un projecte, sinó una aplicació amb garanties d'ús dintre del meu entorn personal i empresarial.

Aquest TFC té com a punt de partida l'estat de l'art de la geolocalització IP, amb l'anàlisi dels diferents conceptes implicats i les diverses eines i serveis que giren al seu voltant. Aquesta fase de recerca garanteix que el producte de programari objectiu d'aquest TFC sigui un programari actual, desenvolupat amb criteri i que integra, amb intel·ligència, aquelles eines o serveis externs que aporten un valor afegit al producte.

Així doncs, amb el Localitzador Gràfic d'Adreces IP, he tingut l'ocasió d'aprofundir coneixements en el món del protocol TCP/IP i conèixer quins són els recursos i mecanismes que disposem per a conèixer informació geogràfica d'una adreça IP i poder-la representar en un mapa.

1.2. OBJECTIUS DEL TFC

Tal com recull el pla docent de l'assignatura, l'objectiu final del projecte és el de *“realitzar una aplicació gràfica que permeti mostrar a partir d'una adreça IP tota la informació relacionada amb ella i el recorregut realitzat per arribar a la seva localització geogràfica”*.

Aquest enunciat, estableix implícitament que l'aplicació resultant haurà de ser capaç de:

- Descobrir la ruta de salts fins al node destí.
- Obtenir informació geogràfica de cada un dels nodes.
- Visualització gràfica de la ruta en un mapa.

Aquest objectiu inicial defineix només les funcionalitats a grans trets de l'aplicació a desenvolupar i, per tant, deixa la porta oberta a infinites possibilitats sobre les seves característiques funcionals i d'implementació. Per tant, el primer objectiu d'aquest projecte

ha estat concretar les funcionalitats de l'aplicació d'acord amb el resultat d'una primera etapa de recerca i en consonància amb la càrrega de treball assignada en el pla d'estudis a l'assignatura de Treball Fi de Carrera.

Com ha resultat d'aquest procés, les característiques principals de l'aplicació són les següents:

- Molt fàcil d'utilitzar.
- No necessita procés d'instal·lació.
- Executable en sistemes operatius de la família Windows (XP, 2000, Vista).
- Interfície gràfica molt intuïtiva, on l'usuari té l'opció de sol·licitar la ruta a una adreça IP o nom de dispositiu i va veient progressivament la informació textual que s'obté mitjançant una taula.
- Representació gràfica de la ruta i dels seus nodes realitzada en un mapa construït amb Google API que l'usuari pot ampliar, reduir i desplaçar.
- Ràpid d'execució, ja que l'aplicació realitza la majoria de comunicacions IP de forma asíncrona i per tant permet que, per exemple, el procés de traça segueixi el seu curs mentre que s'està obtenint informació del Whois d'un node en particular.
- Multi-frontal, per què el programari comunica amb el frontal a través d'esdeveniments i per tant el mateix codi es pot fer servir per a crear l'aplicació amb un frontal en mode text.

Addicionalment, han estat objectius personals, l'adquisició de nous coneixements teòrics així com els pràctics derivats del desenvolupament de programari en entorn de Windows, .NET i C# que han constituït tot un repte.

1.3. ENFOCAMENT I METODOLOGIA

Les característiques d'aquest projecte fan que l'aplicació s'hagi desenvolupat per capes. Cada capa ha inclòs un conjunt de funcionalitats (subconjunt de les funcionalitats globals de l'aplicació final) que han estat la base sobre la que s'ha implementat la capa següent. Al mateix temps, cada capa ha donat lloc a una versió parcial del producte on s'ha executat un conjunt de proves per a confirmar el seu correcte funcionament i assoliment dels objectius

parcials fixats. Aquest mètode de treball ha beneficiat l'elaboració del projecte ja que cada etapa ha estat basada sobre un programari ja provat.

Les tres capes de les que ha constatat el desenvolupament del projecte són:

1. **Ruta de salts:** Donada una adreça IP, obtenir una llista de les diferents adreces IP dels nodes pels quals es passa fins arribar a l'adreça IP destí i els temps de resposta obtinguts en cada un d'ells.
2. **Obtenció d'informació addicional:** Donada una adreça IP, obtenir la seva informació addicional incloent-hi la seva localització geogràfica així com les coordenades de latitud i longitud.
3. **Visualització de traça:** Representació gràfica en un mapamundi de la traça identificant els diferents nodes que la formen.

Abans de tot, però, i com a primer pas en la metodologia a seguir, ha estat la fase de recerca, per adquirir els coneixements i fonaments necessaris per a la correcta definició de les funcionalitats, disseny i implementació de cada una de les capes.

Per altra banda, entre les diferents plataformes i entorns de desenvolupament, he optat per implementar l'aplicació per a sistema operatiu Windows i programar-lo en llenguatge C# (llenguatge creat específicament pel desenvolupament d'aplicacions en la plataforma de treball .NET de Microsoft). La plataforma .NET és un excel·lent entorn de programació per a la programació en xarxa. C#, per la seva banda, és un llenguatge molt similar a Java i juntament amb la seva plataforma de treball .NET facilita la programació en entorns de finestres i proveeix de potents eines per a la comunicació amb APIs i/o serveis externs que han estat d'utilitat pel projecte i l'han dotat d'un caràcter integrador.

1.4. PLANIFICACIÓ

Sota les consideracions assenyalades en el punt anterior, el projecte ha constatat de tres etapes de desenvolupament de programari més les etapes inicial de recerca, la paral·lela a tot el projecte de documentació i la final de presentació. Seguidament es detalla el detall de cada activitat.

1.4.1. Activitat 1: Recerca

Objectiu:

Adquirir i/o aprofundir coneixements sobre els conceptes relacionats amb el projecte, conèixer programari existent i eines i tecnologies aplicables.

Descripció:

Mitjançant la recerca d'informació, hem d'obtenir els coneixements teòrics necessaris així com les tecnologies que podríem aplicar. Aquesta recerca inclou els següents temes:

- Mecanisme d'obtenció de nodes d'una traça mitjançant paquets ICMP.
- Sistemes per a l'obtenció d'informació geogràfica a través de l'adreça IP: Whois, DNS-LOC, altres possibles alternatives.
- La visualització del mapa i la ruta mitjançant un mapa estàtic o fent servir un API extern com, per exemple, GoogleMaps API.
- Confirmació de C# com a llenguatge de programació vàlid pel desenvolupament d'aquesta aplicació com aplicació independent.

Resultat:

- Adquisició dels coneixements teòrics pel desenvolupament de l'aplicació.
- Definició de la plataforma de desenvolupament, llenguatges de programació i components i eines de lliure distribució.
- Ajustament de la temporització en base a la definició prèvia.

Temporització:

2 setmanes (del 28.09.2009 al 18.10.2009)

1.4.2. Activitat 2: Traçador de ruta

Objectiu:

Anàlisi, disseny i implementació d'un traçador de ruta.

Descripció:

A partir dels resultats de l'activitat 1, descobrir els diferents nodes IP que formen part de la ruta fins a una adreça IP destí. Aquest traçador haurà de ser capaç d'admetre com a dada d'entrada tant una adreça IP com un nom dispositiu en la seva forma canònica. Donarà informació de la latència.

Resultat:

Programari traçador de la ruta en format consola i/o Windows.

Temporització:

2,5 setmanes (del 19.10.2009 al 04.11.2009)

1.4.3. Activitat 3: Obtenció de dades addicionals

Objectiu:

Anàlisi, disseny i implementació del programari necessari per a obtenir informació addicional de les adreces IP que formen part de la ruta.

Descripció:

A partir dels resultats de l'activitat 1 (on haurem decidit quins mecanismes farem servir per a obtenir la informació de localització d'una IP) i del programari de l'activitat 2, implementar el programari que obtingui les dades addicionals, incloses les de localització geogràfica, de les adreces IP de la ruta.

Resultat:

Programari actualitzat amb la inclusió de les dades addicionals.

Temporització:

3,5 setmanes (del 05.11.2009 al 29.11.2009)

1.4.4. Activitat 4: Visualització

Objectiu:

Anàlisi, disseny i implementació del programari que representi gràficament en un mapa la ruta.

Descripció:

A partir dels resultats de l'activitat 1 (on haurem decidit quins mecanismes farem servir per a la visualització de la traça en un mapa) i dels programaris anteriors, afegir la funcionalitat de representació visual de la traça.

Resultat:

Programari amb la seva versió final.

Temporització:

4 setmanes (del 30.11.2009 al 27.12.2009)

1.4.5. Activitat 5: Memòria

Objectiu:

Elaboració de la memòria.

Descripció:

Elaboració de la memòria tècnica d'acord a les especificacions del pla docent. La memòria es desenvolupa en paral·lel a la resta d'activitats.

Resultat:

Memòria tècnica.

Temporització:

del 28.09.2009 al 05.01.2010

1.4.6. Activitat 6: Presentació virtual

Objectiu:

Creació de la presentació virtual.

Descripció:

Elaboració de la presentació virtual d'acord a les especificacions del pla docent.

Resultat:

Presentació virtual.

Temporització:

1 setmana (del 06.01.2010 al 12.01.2010)

1.4.8. Diagrama de GANNT

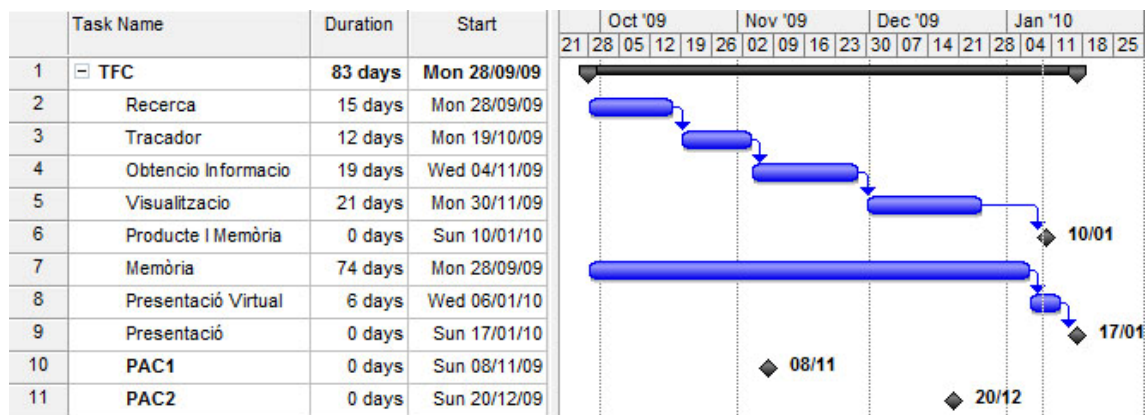


Figura 1. Diagrama GANNT del pla de treball en el seu plantejament inicial

1.4.9. Desviacions produïdes respecte al pla de treball inicial

Encara que el pla de treball s'ha seguit segons el plantejament inicial, s'han produït diferències en la durada de, principalment, les activitats 4 (obtenció de dades addicionals) i 5 (visualització). Per una banda, les tasques associades a l'obtenció de dades addicionals han estat més nombroses de les inicialment previstes. Per altra banda, l'encertada decisió de fer

servir Google Maps com interfície per a la presentació gràfica de la ruta ha reduït considerablement la durada d'aquesta activitat i l'excedent d'hores s'ha traslladat a l'activitat anterior per a optimitzar el temps de resposta, mitjançant programació asíncrona, del procés d'obtenció de dades addicionals.

1.5. PRODUCTES OBTINGUTS

L'elaboració d'aquest projecte lliura dos productes ben diferenciats: una memòria tècnica i una aplicació.

La memòria tècnica inclou tot el treball de recerca i descripció de les diferents fases d'anàlisi, disseny i implementació del programari final.

L'aplicació lliurada, denominada YAVIT, sigles angleses de Yet Another Visual Ip Tracer, és un programari que s'executa en el sistema operatiu Windows i està caracteritzat principalment per la seva facilitat d'ús gràcies a una interfície d'usuari molt intuïtiva, on l'usuari, després d'haver introduït l'adreça IP o nom de dispositiu destí, veu representat en una taula les dades dels diferents nodes que formen part de la ruta i la seva visualització gràfica en un mapa construït amb GoogleMaps.

1.6. BREU DESCRIPCIÓ DELS ALTRES CAPÍTOLS DE LA MEMÒRIA

Els següents capítols de la memòria estan estructurats seguint el guió de la metodologia de treball establerta.

El capítol 2, "Fonaments de la Geolocalització IP", constitueix tota la fase de recerca del projecte, on a través de diferents fonts d'informació, majoritàriament Internet, s'analitzen els diferents conceptes relacionats amb la geolocalització IP juntament amb serveis i aplicacions existents.

El capítol 3, "El traçador de ruta", està dedicat al disseny i implementació de la primera capa de l'aplicació: la ruta de salts.

El capítol 4, “Obtenció de dades addicionals”, correspon al disseny i implementació de la segona capa de l’aplicació: l’obtenció de les dades addicionals associades als nodes de la ruta.

El capítol 5, “Visualització”, pertany a l’etapa final del desenvolupament del projecte, on es dissenya e implementa la capa de representació de la traça en un mapa.

El capítol 6 i últim, correspon a l’exposició del conjunt de conclusions derivades d’aquest projecte.

Finalment, s’inclou un annex que equival al manual d’usuari de l’aplicació.

CAPÍTOL 2

FONAMENTS DE LA GEOLOCALITZACIÓ IP

2.1. INTRODUCCIÓ

En el context d'Internet, la Geolocalització IP, és la identificació de la localització geogràfica del dispositiu que de cara a la xarxa Internet té assignada aquesta adreça. No obstant, tal com es veurà més endavant, això no sempre serà possible.

Són moltes les aplicacions que fan ús d'aquesta funcionalitat. Entre elles es troben:

- **Màrqueting geogràfic.** La publicitat que es visualitza en una pàgina web està determinada per la localització de l'adreça IP del visitant.
- **Estudis de mercat.** Els administradors de llocs web, obtenen informació valuosa sobre l'origen geogràfic dels seus visitants.
- **Lluita contra el correu brossa.** Amb les localitzacions geogràfiques de les adreces IP incloses en les capçaleres dels missatges, s'obté informació de la seva procedència.
- **Variabilitat del contingut.** Es basa en acomodar el contingut d'una pàgina web al visitant d'acord a la seva localització. Per exemple, un lloc web pot automàticament visualitzar una pàgina en l'idioma associat a la localització IP del visitant.
- **Seguretat / censura.** Aplicació de filtres segons la procedència geogràfica de l'adreça origen o destí.
- **Frau / Investigació.**
- **Preservació dels drets.** Gràcies a la geolocalització IP, és possible la distribució de continguts del qual només està llicenciat la distribució en unes zones geogràfiques concretes.
- **Avaluació de riscos.** el nombre de salts que hi ha en una traça és directament proporcional al nombre de dispositius involucrats. Quants més dispositius, més probabilitats de possibles incidències.

- **Visualització dels acords entre operadors.** La informació dels salts i la seva localització donen informació afegida sobre els operadors de trànsit que interconnecta les diferents xarxes. A vegades, la manca d'interconnexió entre dos operadors locals fa que, a vegades, la ruta IP entre dos ordinadors d'una mateixa ciutat amb diferents operadors locals sigui a través de tercers països.

En els següents apartats es descriuen els diferents conceptes associats a la geolocalització IP i eines i aplicacions existents en l'actualitat.

2.2. ADRECES IP

Són l'objecte a geolocalitzar en l'aplicació. És un número de 32 bits amb el que un dispositiu connectat a Internet s'identifica per comunicar-se. Les adreces IP s'agrupen en 5 classes, segons la següent taula:

Primers bits	Direcció de xarxa	Direcció d'estació	Tipus	Rang
0	7 bits	24 bits	Classe A	0.x.x.x - 127.x.x.x
10	14 bits	16 bits	Classe B	128.x.x.x - 191.x.x.x
110	21 bits	8 bits	Classe C	192.x.x.x - 223.x.x.x
1110	0 bits	28 bits	Classe D	224.x.x.x - 247.x.x.x
1111	0 bits	28 bits	Classe E	248.x.x.x - 255.x.x.x

D'aquests rangs, les següents adreces tenen un significat especial i no es poden fer servir per a identificar remotament a un dispositiu i, per tant, no seran adreces de les quals es pugui consulta informació geogràfica:

Rang	Motiu
224.x.x.x – 247.x.x.x (tota la classe D)	Destinades a trànsit <i>multicast</i> . No s'assignen a dispositius concrets.
248.x.x.x. – 255.x.x.x (tota la classe E)	Xarxes experimentals. No tenen cap ús.
Adreça de xarxa	Identifica la xarxa a la que pertany un dispositiu.

0.0.0.0	No es pot assignar a cap dispositiu
127.x.x.x	<i>Loopback</i>
255.255.255.255	<i>Broadcast</i>
10.0.0.0 – 10.255.255.255	Ús privat.
172.16.0.0 – 172.31.255.255	Ús privat.
192.168.0.0 – 192.168.255.255	Ús privat

Les adreces IP no estan repartides de forma aleatòria, han d'estar controlades per tal d'evitar duplicitat. IANA (*the Internet Assigned Numbers Authority*), organització depenent de la ICANN (*Internet Corporation for Assigned Names and Numbers*) és l'encarregada, entre altres responsabilitats, de gestionar la provisió d'adreces IP arreu el món. IANA no ho fa directament si no que segueix una estructura jerarquitzada on IANA delega recursos als diferents RIR (*Regional Internet Registry*) que gestionen una regió particular del món. Aquests, a la seva vegada, deleguen els seus recursos als LIR (Local Internet Registry) que són els que finalment assignen les adreces al clients.

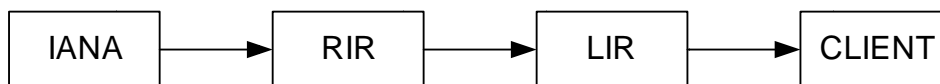


Figura 2. Jerarquia de delegació

Actualment operen un total de cinc RIRs:

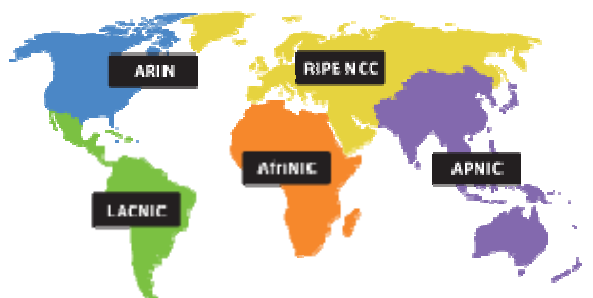


Figura 3. Els cinc RIRs arreu el món

Nom RIR	Regió
AfriNIC (<i>African Network Information Center</i>)	Africa
APNIC (<i>Asia-Pacific Network Information Center</i>)	Asia i regió del Pacífic
ARIN (<i>American Registry for Internet Numbers</i>)	Nord amèrica i parts del Caribe
LACNIC (<i>Latin American and Caribbean Internet Address Registry</i>)	Amèrica Latina i part del Caribe
RIPENCC (<i>RIPE Network Coordination Center</i>)	Europa, Orient mitjà i Asia central

IANA també és l'encarregada de l'operativa i manteniment de la zona arrel de DNS i del domini .ARPA, que és el TLD (*top level domain*) del domini IN-ADDR.ARPA, per a la resolució inversa d'una adreça IP.

2.3. PROTOCOL ICMP

El protocol ICMP es va definir en la RFC 792 i permet la notificació de missatges administratius i d'error entre els dispositius de xarxa. Posteriors especificacions (RFC 950, RFC 1256, RFC 1122) incorporen més tipus de missatges i detalls del protocol.

L'ICMP no està encapsulat sota TCP o UDP i fa servir el seu propi codi de protocol (1).

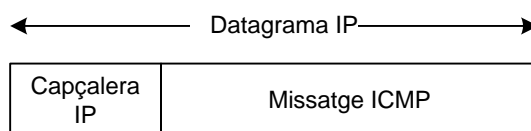


Figura 4. Datagrama IP amb missatge ICMP

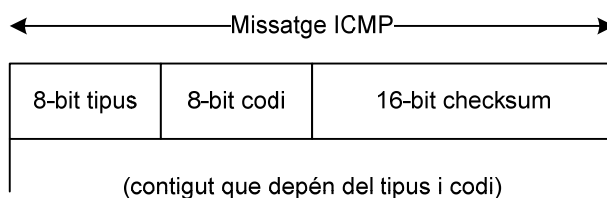


Figura 5. Format del missatge ICMP

El missatge ICMP està format pels següents camps:

- **Tipus:** Defineix el tipus de missatge ICMP present en el paquet. Actualment hi han definits tretze tipus.
- **Codi:** Dóna informació addicional del tipus de missatge.
- **Checksum:** Serveix per a comprovar la integritat del paquet.
- **Contingut:** És de longitud variable i el seu contingut depèn del tipus de missatge.

De tot el conjunt de tipus-codi de missatges hi ha tres que són els que participen en el descobriment dels salts fins arribar a destí:

- **Tipus 8, codi 0:** Correspon al missatge de petició d'eco (*echo request*). Aquest paquet permet a un dispositiu el requerir un altre paquet ICMP de resposta des d'el dispositiu remot (resposta d'eco o *echo reply*).
- **Tipus 0:** Correspon al missatge de resposta d'eco (*echo reply*). Aquest paquet és la resposta a un paquet de petició d'eco.
- **Tipus 11:** Aquest missatge informa que un paquet ha superat el temps de vida (*time to live o TTL*) definit en la capçalera IP. Cada vegada que un paquet travessa un encaminador, el valor del TTL decreix en una unitat. Si el valor del TTL arriba a zero abans de què el paquet arribi a destí, l'últim encaminador que ha rebut el paquet ha d'enviar un missatge ICMP tipus 11 a l'emissor del missatge.

Així doncs, en un procediment on s'envia consecutivament a una adreça destí un missatge ICMP de tipus *echo request* amb valors de TTL incrementats des de 1 fins a, per exemple, 30, s'obtindran missatges ICMP de tipus 11 per cada un dels encaminadors que formen part de la ruta i, per tant, aquesta queda revelada.

Malgrat tot, és possible que un o més dispositius participants en la ruta tinguin filtrat la resposta a una petició d'eco. En aquest cas, l'adreça IP d'aquests nodes seria desconeguda. Alternatives segures per a evitar aquestes situacions no hi han. Una opció seria fer servir la mateixa tècnica però utilitzant un port TCP o UDP en comptes d'un paquet ICMP. En tot cas, el problema de filtratge seguiria present.

2.4. DNS INVERTIT

Igual que mitjançant el servei de noms de domini (DNS) es tradueix, el nom d'un dispositiu a la seva adreça IP, també es pot saber pel procés invers, el nom de dispositiu associat a una IP determinada.

Per exemple, donada l'adreça 62.149.162.64, la comanda 'nslookup 62.149.162.64' tradueix l'adreça a 'host64-162-149-62.serverdedicati.aruba.it'.

D'aquesta informació es podria interpretar que la localització d'aquesta IP està en Itàlia (el TLD és .it) i associada a una companyia denominada Aruba.

No obstant, per una banda, la resolució inversa d'una adreça IP depèn de la correcta configuració dels servidors de DNS que gestionen la xarxa a la qual pertany la IP. Per altra banda, quan el camp TLD és genèric (.com, .net, .org, etc.), aquest no aporta informació. Finalment, és probable que les lletres indicatives del país no corresponguin a la localització real de la IP. Tot i això és informació que pot ser rellevant.

2.5. DNS-LOC

La RFC 1876 especifica un mecanisme per a incloure localització geogràfica en el sistema de noms de domini (DNS).

La sintaxi d'aquest registre és la següent:

```
<owner> <TTL> <class> LOC (d1 [m1 [s1]] {"N"|"S"} d2 [m2 [s2]] {"E"|"W"}  
alt["m"] [siz["m"]] [hp["m"]] [bp["m"]]) )
```

La descripció de cada un dels camps és la següent:

Paràmetre	Descripció	Unitat	Valors
d1	Graus de latitud	°	0 .. 90
m1	Minuts de latitud	'	0 .. 59
s1	Segons de latitud	''	0 .. 59.999

N/S	Hemisferi nord o sud		N ó S
d2	Graus de longitud	°	0 .. 90
m2	Minuts de longitud	'	0 .. 59
s2	Segons de longitud	"	0 .. 59.999
E/W	Longitud Est o Oest		E ó W
alt	Altitud amb precisió de 0.01 m	m	-100000.00 .. 42849672.95
siz	Diàmetre de l'esfera que conté el punt indicat. El valor per defecte és 1m	m	0 .. 90000000.00
hp	Precisió horitzontal en metres. El valor per defecte és 10000m	m	0 .. 90000000.00
vp	Precisió vertical en metres. El valor per defecte és 10m	m	0 .. 90000000.00

Exemples d'aquest registre són:

```
hertz.com          loc 35 32 54.006 N 97 36 47.000 W 371.85m 200m 10000m 1m
```

```
11.81.21.12.in-addr.arpa loc 35 32 54.006 N 97 36 47.000 W 371.85m 200m
10000m 1m
```

No obstant, aquest tipus de recurs està actualment en desús i són pocs els servidors que mantenen registres de tipus de registre en els seus DNS, per la qual cosa descartarem el seu ús.

2.6. SERVEI WHOIS

Whois és un protocol que es fa servir per a obtenir informació sobre les organitzacions i contactes associats a recursos d'Internet com dominis o adreces IP. L'especificació actual del protocol WHOIS es troba al RFC 3912. El servei se subministra a través de connexió TCP al port 43 dels servidors Whois.

Tal com s'ha vist anteriorment en aquest capítol, les adreces IP estan gestionades per cinc RIRs. Aquest cinc RIRs posen a disposició de qualsevol, a través dels seus servidors whois la informació sobre els registradors de les adreces IP i les seves dades de contacte.

RIR	Servidor Whois
AfriNIC	whois.afrinic.net
APNIC	whois.apnic.net
ARIN	whois.arin.net
LACNIC	whois.lacnic.net
RIPENCC	whois.ripe.net

Un exemple de resposta a una consulta al servidor Whois de RIPE per a l'adreça IP 87.223.129.56 és la següent:

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag.
% Information related to '87.223.128.0 - 87.223.255.255'
inetnum:        87.223.128.0 - 87.223.255.255
netname:        JAZZTEL-ADSL
descr:          Jazz Telecom S.A.
country:        ES
admin-c:        JAZZ3-RIPE
tech-c:         JAZZ3-RIPE
remarks:        SPAM, Net Abuse and Security-Issues: abuse@jazztel.com
status:         ASSIGNED PA
mnt-lower:      JAZZSEC
mnt-by:         JAZZSEC
source:         RIPE # Filtered
role:           JAZZTEL RIPE
address:        Jazz Telecom S.A.
address:        Anabel Segura 11
address:        28108, Alcobendas (Madrid)
address:        Albatros - Edificio C
address:        Spain
phone:          +34 91 183 9000
fax-no:         +34 91 291 7570
abuse-mailbox:  abuse@jazztel.com
admin-c:        AHA14-RIPE
admin-c:        MVM79-RIPE
admin-c:        CGG10-RIPE
tech-c:         AHA14-RIPE
tech-c:         MVM79-RIPE
tech-c:         CGG10-RIPE
nic-hdl:        JAZZ3-RIPE
remarks:        trouble: *****
remarks:        trouble: For SPAM, Net Abuse, Intrusion and Security Issues
remarks:        trouble:
remarks:        trouble: Please Contact: abuse@jazztel.com
remarks:        trouble:
remarks:        trouble: All messages to any other our e-mails, related to
remarks:        trouble: these issues will be ignored
remarks:        trouble: *****
```

```
mnt-by:          JAZZSEC
source:          RIPE # Filtered
% Information related to '87.223.224.0/19AS12715'
route:          87.223.224.0/19
descr:          Jazz Telecom S.A.
descr:          Global Spanish ISP
origin:         AS12715
remarks:        SPAM, Net Abuse and Security-Issues: abuse@jazztel.com
mnt-by:          JAZZSEC
source:          RIPE # Filtered
```

Es pot observar que aquesta informació no és massa acurada si s'avalua a nivell de precisió geogràfica. En aquest exemple, és cert que l'adreça IP pertany a la xarxa de Jazztel i que està situada a Espanya (codi de país ES). No obstant, situa la IP a la ciutat de Madrid, quan aquesta adreça IP està vinculada a una xarxa de la ciutat de Barcelona.

La raó és que en molts casos, les adreces estan assignades a grans proveïdors d'internet i les dades de localització que figuren corresponen a les del proveïdor i no a les del desplegament que hagi fet de la xarxa.

Un altre problema aparent presentat és l'elecció del servidor whois al que s'ha de fer la consulta en funció de l'adreça IP. Encara que IANA manté un llistat que va actualitzant constantment amb tot l'espai d'adreces IP amb la relació de rangs i RIRs no és necessari treballar amb aquesta informació ja que el servidor whois de ARIN o bé dona la informació directament o bé dona la referència del servidor whois al qual s'ha de realitzar la consulta.

També, a través d'altres servidors Whois es pot obtenir informació dels titulars dels noms de dominis. Quan en l'exemple anterior, s'obtenia la IP 62.149.162.64 associada a una entitat denominada Aruba a Itàlia, una consulta al servidor Whois corresponent al TLD .IT (whois.nic.it) pel domini aruba.it dona el següent resultat:

```
Domain: aruba.it
Status: ACTIVE
Created: 1999-12-07 00:00:00
Expire Date: 2010-03-26
Last Update: 2009-09-03 11:13:40
```

```
Registrant
Name: aruba Spa
Organization: aruba Spa
ContactID: ARUB44-ITNIC
Address: P.zza Garibaldi, 8
52010 - BIBBIENA (AR)
IT
Nationality: IT
Phone: +39.057551571
Email: susanna@aruba.it
```

Created: 2008-03-26 15:37:42
Last Update: 2008-03-26 15:37:42

Admin

Name: Susanna Santini
Organization: aruba Spa
ContactID: SS106895-ITNIC
Address: P.zza Garibaldi, 8
52010 - BIBBIENA (AR)
IT
Phone: +39.057551571
Email: susanna@aruba.it
Created: 2008-03-26 15:37:43
Last Update: 2008-03-26 15:37:43

Tech

Name: Susanna Santini
Organization: aruba Spa
ContactID: SS106895-ITNIC
Address: P.zza Garibaldi, 8
52010 - BIBBIENA (AR)
IT
Phone: +39.057551571
Email: susanna@aruba.it
Created: 2008-03-26 15:37:43
Last Update: 2008-03-26 15:37:43

Registrar

Organization: Aruba s.p.a.
Name: ARUBA-MNT

Nameservers

dns.technorail.com
dns2.technorail.com

A l'igual que abans, també hi és el problema inicial de decidir el servidor whois associat a cada TLD. Però també té una solució molt simple: una primera consulta whois al servidor <TLD>.WHOIS-SERVERS.NET (per exemple it.whois-servers.net) retorna el servidor whois que conté la informació relativa al titular del domini.

Així doncs, el servei de Whois dona informació, per una banda de la xarxa a la qual pertany una adreça IP i d'on es pot obtenir amb certa fiabilitat el país on està localitzada i per altra banda, informació del titular del domini que fa ús d'aquesta adreça.

2.7. GEOCODIFICACIÓ

Amb les consultes whois de l'apartat anterior, s'obté informació de localització de l'adreça IP. Però per a poder representar aquesta posició en un mapa, és necessari disposar de les coordenades de longitud i latitud geogràfiques. Per a obtenir aquestes dades hi ha dues

opcions: o bé es manté una base de dades amb la relació dels noms geogràfics i les seves coordenades geogràfiques (informació que es pot descarregar des de la *National Geospatial-Intelligence Agency* a <http://earth-info.nga.mil/gns/html/namefiles.htm>) o bé es fa ús d'un servei que faciliti aquesta informació. A continuació s'exposen interfícies externes que proveeixen d'aquesta geocodificació.

2.7.1. Yahoo API

Yahoo posa a disposició pública una sèrie d'APIs i serveis. Concebut com 'serveis web', Yahoo ofereix el servei de geocodificació, transformant una adreça física en les coordenades de latitud/longitud corresponents.

Per exemple, les coordenades geogràfiques de la seu central de la UOC, a partir de la seva adreça física, s'obté a través de la següent crida:

```
http://local.yahooapis.com/MapsService/V1/geocode?appid=YD-
G7bey8_JXxQP6rx1.fBFGgCdNjoDMACQA--&street=Av. Tibidabo, 39-
41&city=Barcelona&Country=ES
```

El resultat d'aquesta consulta és:

```
<?xml version="1.0" ?>
<ResultSet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="urn:yahoo:maps" xsi:schemaLocation="urn:yahoo:maps
http://api.local.yahoo.com/MapsService/V1/GeocodeResponse.xsd">
<Result precision="address">
<Latitude>41.414891</Latitude>
<Longitude>2.133477</Longitude>
<Address>avinguda del Tibidabo, 39</Address>
<City>08035 Barcelona</City>
<State>Spain</State>
<Zip />
<Country>ES</Country>
</Result>
</ResultSet>
```

Així doncs, la crida a aquesta interfície ha posicionat l'adreça "Av. Tibidabo, 39-41 Barcelona ES" en les coordenades geogràfiques de latitud 41.414891 i longitud 2.133477.

2.7.2. Google Maps API

A l'igual que Yahoo, Google ofereix també uns serveis de geocodificació amb característiques similars. Per a la geocodificació de la mateixa adreça d'abans, la crida és:

http://maps.google.com/maps/geo?output=xml&key=key&q=Av. Tibidabo 39-41
Barcelona ES

I el resultat de la crida és:

```
<?xml version="1.0" encoding="UTF-8" ?>
<kml xmlns="http://earth.google.com/kml/2.0">
<Response>
<name>Av. Tibidabo 39-41 Barcelona ES</name>
<Status>
<code>200</code>
<request>geocode</request>
</Status>
<Placemark id="p1">
<address>Avinguda del Tibidabo, 39, 08035 Barcelona, España</address>
<AddressDetails Accuracy="8" xmlns="urn:oasis:names:tc:ciq:xsd:schema:xAL:2.0">
<Country>
<CountryNameCode>ES</CountryNameCode>
<CountryName>España</CountryName>
<AdministrativeArea>
<AdministrativeAreaName>CT</AdministrativeAreaName>
<SubAdministrativeArea>
<SubAdministrativeAreaName>Barcelona</SubAdministrativeAreaName>
<Locality>
<LocalityName>Barcelona</LocalityName>
<Thoroughfare>
<ThoroughfareName>Avinguda del Tibidabo, 39</ThoroughfareName>
</Thoroughfare>
<PostalCode>
<PostalCodeNumber>08035</PostalCodeNumber>
</PostalCode>
</Locality>
</SubAdministrativeArea>
</AdministrativeArea>
</Country>
</AddressDetails>
<ExtendedData>
<LatLonBox north="41.4180969" south="41.4118016" east="2.1367075"
west="2.1304122" />
</ExtendedData>
<Point>
<coordinates>2.1335522,41.4149448,0</coordinates>
</Point>
</Placemark>
</Response>
</kml>
```

Els valors de les coordenades geogràfiques coincideixen amb les obtingudes amb la interfície de Yahoo i afegeix informació addicional com, per exemple, el codi postal.

2.7.3. Hostip.info

És un servei gratuït que ofereix una interfície per a l'obtenció de les coordenades geogràfiques però, en aquest cas, a partir de la mateixa adreça IP. Aquesta interfície retorna, donada una adreça IP, la localització física (país i, opcionalment, ciutat). En els casos que la

interfície retorna la ciutat, també dona la seva latitud i longitud geogràfiques. Per exemple, una consulta a aquesta interfície per l'adreça IP 87.223.243.165 es realitza amb la següent crida:

```
http://api.hostip.info/?ip=87.223.243.165
```

De manera semblant a les interfícies de Yahoo i Google, la resposta es rep en format xml:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<HostipLookupResultSet version="1.0.0" xmlns:gml="http://www.opengis.net/gml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.hostip.info/api/hostip-1.0.0.xsd">
<gml:description>This is the Hostip Lookup Service</gml:description>
<gml:name>hostip</gml:name>
<gml:boundedBy>
<gml:Null>inapplicable</gml:Null>
</gml:boundedBy>
<gml:featureMember>
<Hostip>
<gml:name>Barcelona</gml:name>
<countryName>SPAIN</countryName>
<countryAbbrev>ES</countryAbbrev>
<!-- Co-ordinates arè available as lng,lat -->
<ipLocation>
<gml:pointProperty>
<gml:Point srsName="http://www.opengis.net/gml/srs/epsg.xml#4326">
<gml:coordinates>2.15,41.3833</gml:coordinates>
</gml:Point>
</gml:pointProperty>
</ipLocation>
</Hostip>
</gml:featureMember>
</HostipLookupResultSet>
```

2.7.4. MaxMind

És una versió comercial dels serveis que proporciona HostIp.info amb l'opció alternativa de descarregar-se les bases de dades amb la informació dels rangs d'adreces IP i la seva localització física (ciutat i País) i geogràfica (latitud i Longitud) amb actualitzacions mensuals.

2.8. VISUALITZACIÓ EN UN MAPA

Per a la representació visual de la traça es pot fer servir qualsevol mapamundi estàtic o aprofitar serveis externs que es puguin integrar. Com l'objectiu inicial era utilitzar Google Maps, s'ha hagut d'avaluar la possibilitat de què l'API de Google proveeixi de les eines

adequades per a poder visualitzar la ruta sobre aquests mapes. Tal com reflexa la seva documentació en línia, la interfície de GoogleMaps permet la superposició de capes personalitzades i dibuixar sobre elles, línies, polígons, icones i qualsevol altre objecte.

Un exemple de representació d'un traç sobre un mapa amb GoogleMaps és el següent:

```
bar polyline = new GPolyline([
    new GLatLng(37.4419, -122.1419),
    new GLatLng(37.4519, -122.1519)
], "#ff0000", 10);
map.addOverlay(polyline);
```

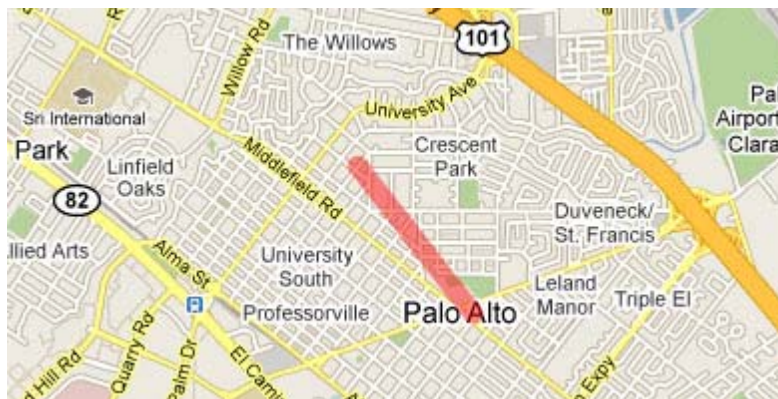


Figura 6. Exemple de polilínia amb Google API

2.9. EXEMPLES D'APLICACIONS EXISTENTS

A continuació es mostra les dues aplicacions més representatives per a la visualització de traces IP així com un exemple en línia de geolocalització IP que fa servir GoogleMaps API.

2.9.1. VisualRoute

És potser, el més conegut entre tots els programes visualitzadors de la traça. Està molt orientat a l'anàlisi de connexió entre els diferents punts que formen la ruta. Les seves principals característiques són:

- Sistema operatiu Windows.
- Processament en paral·lel.
- Subministra molta informació sobre els temps de resposta dels diferents salts.

- Té en compte les múltiples rutes que es poden donar fins a un destí (tal com es veu en la figura en el quart salt).
- Afegeix test de temps de resposta en la resolució inversa de les IP.
- Permet la traça prenent com origen altres seus de la companyia.
- Basat en Java
- Preu de la versió personal de 49.95\$.

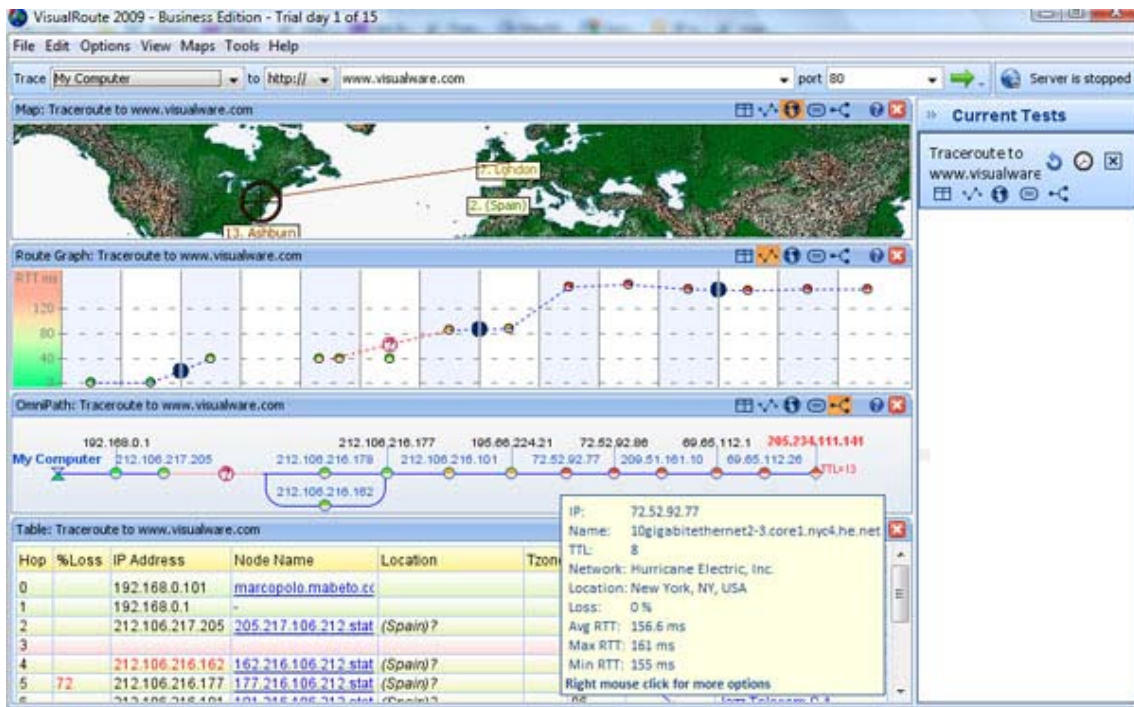


Figura 7. Pantalla de visualització de VisualRoute

Aquest programa deixa, no obstant, amb incertesa la localització d'alguns nodes que amb les consultes a la interfície de HostIp han donat amb precisió.

2.9.2. Path Analyzer Pro

A l'igual que Visualroute, Path Analyser Pro aporta molta informació per a l'anàlisi de la xarxa. Les seves principals característiques són:

- Plataforma Windows i MacOS.
- Desenvolupat en C/C++. No precisa Java

- Genera informes
- Concurrent, per permetre concurrència de traces
- Preu de la versió personal de 29.95\$.
- Permet test repetitius per a l'anàlisi de la xarxa i la cerca de nodes conflictius
- Incorpora la funcionalitat de fer la traça d'un missatge de correu electrònic

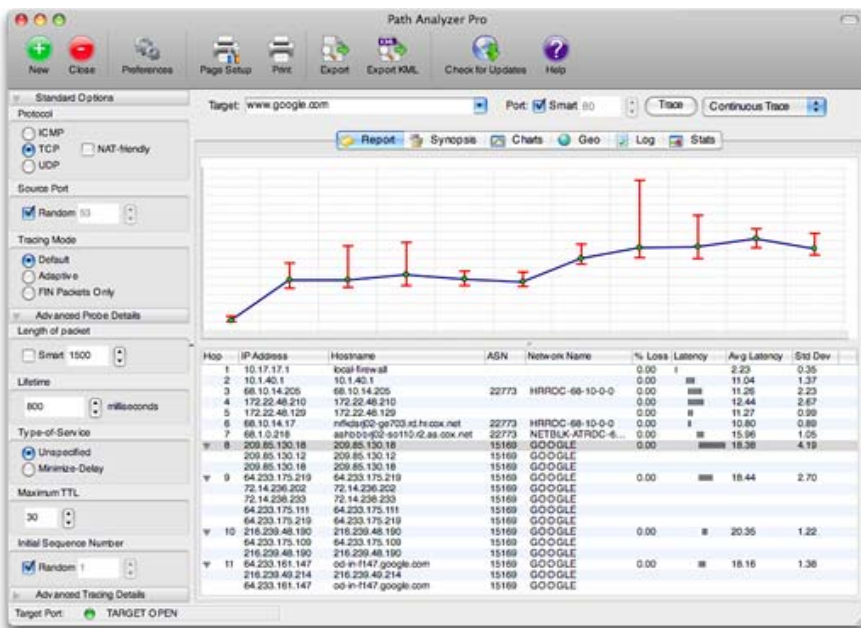


Figura 8. Dades d'una traça amb Path Analyzer Pro



Figura 9. Representació de la traça en un mapa amb Path Analyzer Pro

2.9.3. IP Geolocator

És una utilitat accessible en línia que fa servir GoogleMaps per a posicionar en un mapa la localització d'una adreça IP.



Figura 10. IP Geolocator

2.10. CONCLUSIONS

Encara que existeixen diversos mecanismes per a la geolocalització IP cap d'ells és una solució fiable al 100%. Les solucions més fiables estan associades a serveis proporcionats per companyies que mantenen les seves pròpies bases de dades alimentades per diferents fonts d'informació (Whois, DNS, mètodes heurístics) incloent la participació dels internautes i per tant, sembla lògic que per aconseguir una bona precisió, s'hauria de comptar amb algú d'aquests serveis. No obstant, això no voldria dir que no s'hagi de tindre en compte la informació del Whois o dels DNS ja que aporten molta informació sobre el propietari del rang d'adreces IP i del domini associat a la seva resolució inversa.

En síntesi, els punts claus que han fet de punt de partida per a la implementació de l'aplicació són els següents:

- Només certs rangs d'adreces IP són assignables a dispositius que puguin ser localitzables remotament.
- Els missatges ICMP tipus 8, 0 i 11 juntament amb l'ús del camp TTL són els que permeten descobrir la ruta IP fins arribar a destí.
- Els diferents RIR tenen informació sobre les adreces que gestionen. No obstant, ARIN.WHOIS.NET es pot fer servir com únic punt d'entrada ja que en cas de no ser el gestor de l'adreça a consultar, retorna la referència del servidor Whois que la gestiona.
- La resolució inversa de l'adreça IP dóna informació addicional sobre aquesta IP. Per obtenir informació del TLD del domini s'ha d'accedir primerament a <TLD>.whois-servers.net per rebre el nom del servidor whois del qual es pot consultar la informació.
- Pocs DNS mantenen registres LOC de les seves adreces IP i per tant és descartat.
- La informació procedent del whois potser poc acurada.
- HostIp.info proveeix d'una interfície gratuïta que retorna la localització física i les coordenades geogràfiques amb més precisió que les consultes a servidors Whois. En el cas de què HostIp.info no retorni les coordenades geogràfiques, s'han d'obtenir a partir de la interfície de geocodificació de GoogleMaps. També, si HostIp.info no retorna cap informació de la localització física, aquesta informació s'haurà de treure de la informació del Whois.
- La representació de la ruta a través de GoogleMaps és perfectament viable ja que la interfície de programació habilita eines per a la superposició de línies i altres objectes amb flexibilitat.

CAPÍTOL 3

EL TRAÇADOR DE RUTA

3.1. OBJECTIUS

Aquest primer nivell de desenvolupament és el que s'encarrega de determinar quin són els nodes que constitueixen la ruta fins arribar al destí. El procés per a l'obtenció de la ruta és l'explicat en el capítol 2.3 (Protocol ICMP) i els requisits marcats per a aquesta etapa són els següents:

- La dada d'entrada (l'adreça destí de la ruta) pot ser introduïda de qualsevol forma, ja sigui com a adreça IP directament o com nom canònic de dispositiu.
- Durant el procés de descobriment de la ruta, es pot treure el temps de resposta a l'eco.
- El procés iteratiu d'enviaments de paquets no ha de bloquejar l'ús de la interfície d'usuari.
- El codi ha de ser independent de la interfície. D'aquesta manera, el mateix codi serveix per a una interfície en mode text.

3.2. DISSENY I IMPLEMENTACIÓ

3.2.1. La classe *Hop*

Aquesta classe és la que conté la informació d'un node de la ruta. Les següents taules llisten el contingut de la classe *HOP*:

Membres		
Nom	Tipus	Descripció
m_HopNumber	Int	Número de salt
m_Address	IPAddress	Adreça IP

m_Status	IPStatus	Estat retornat de la resposta a sol.licitud d'eco
m_Type	TypeOfIP	Tipus d'adreça IP
m_RoundTripTime	Long	Temps de resposta

Mètodes		
Nom	Tipus	Descripció
Hop(int number, IPAddress address, IPStatus status, long roundTripTime)	Public	Constructor. Crea un node.
TypeOfIP GetTypeOfIP(IPAddress address)	Public	Mètode estàtic per a tipificar el tipus d'adreça IP.

El mètode estàtic *GetTypeOfIP* tipifica el tipus d'adreça IP d'acord a la classificació definida en l'apartat 2.2 (adreces IP) i que es codifica de la següent forma:

Valor	Descripció
PublicIP	Adreça IP pública
PrivateIP	Adreça IP privada (p.e. 192.168.0.1)
UnknownIP	Adreça IP desconeguda degut a error en la resposta ICMP
BadIP	Adreça IP amb format vàlid però a la que no es pot fer una traça. Exemples serien una adreça de les classes D o E, l'adreça de <i>broadcast</i> , etc.

D'aquesta classificació, només les adreces etiquetades com a PublicIP són sobre les que té sentit llençar una traça o sobre les que es podrà fer consultes.

3.2.2. La classe *Route*

La classe *Route* és l'encarregada de proveir les dades i mètodes per a l'execució de la traça.

Membres		
Nom	Tipus	Descripció
m_Target	IPAddress	Adreça IP destí

m_Hops	List	Llista de nodes que formen la ruta
m_IsCompleted	bool	Estat de si la ruta està finalitzada o no
m_State	Enum	Estat del proces de traça.
m_RoundTripTime	Long	Temps de resposta

Mètodes		
Nom	Tipus	Descripció
Route ()	Public	Constructor. Instancia un objecte de tipus Route
Clear ()	Private	Esborra la ruta i llibera recursos
Hop (int hopNumber)	Public	Retorna el Hop indicat per parametre
Go (IPAddress target)	Public	Fa el proces de traça
OnPingCompleted ()	Private	Procesa el callback d'una crida asincrona al enviament d'un paquet ICMP
ProcessHop(int hopNumber, IPAddress ip, IPStatus status)	Private	Procesa el retorn del paquet ICMP i crea el node.

Delegats / Esdeveniments		
Nom	Tipus	Descripció
HopFoundHandler () / OnHopFound	Public	Notificacio de node trobat.
RouteCompletedHandler() / OnRouteCompleted	Public	Notificació de que ja s'ha acabat la traça

El nivell superior, subscriu els esdeveniments *OnHopFound* i *OnRouteCompleted*. D'aquesta forma serà notificat cada vegada que s'afegeix un nou salt a ruta per visualitzar-lo en la seva interfície i també assabentar-se de quan el procés de descobriment de ruta ha acabat.

3.2.3. Implementació

El proces de traça *Router.GO(Ipaddress)* queda reflexat en el següent diagrama:

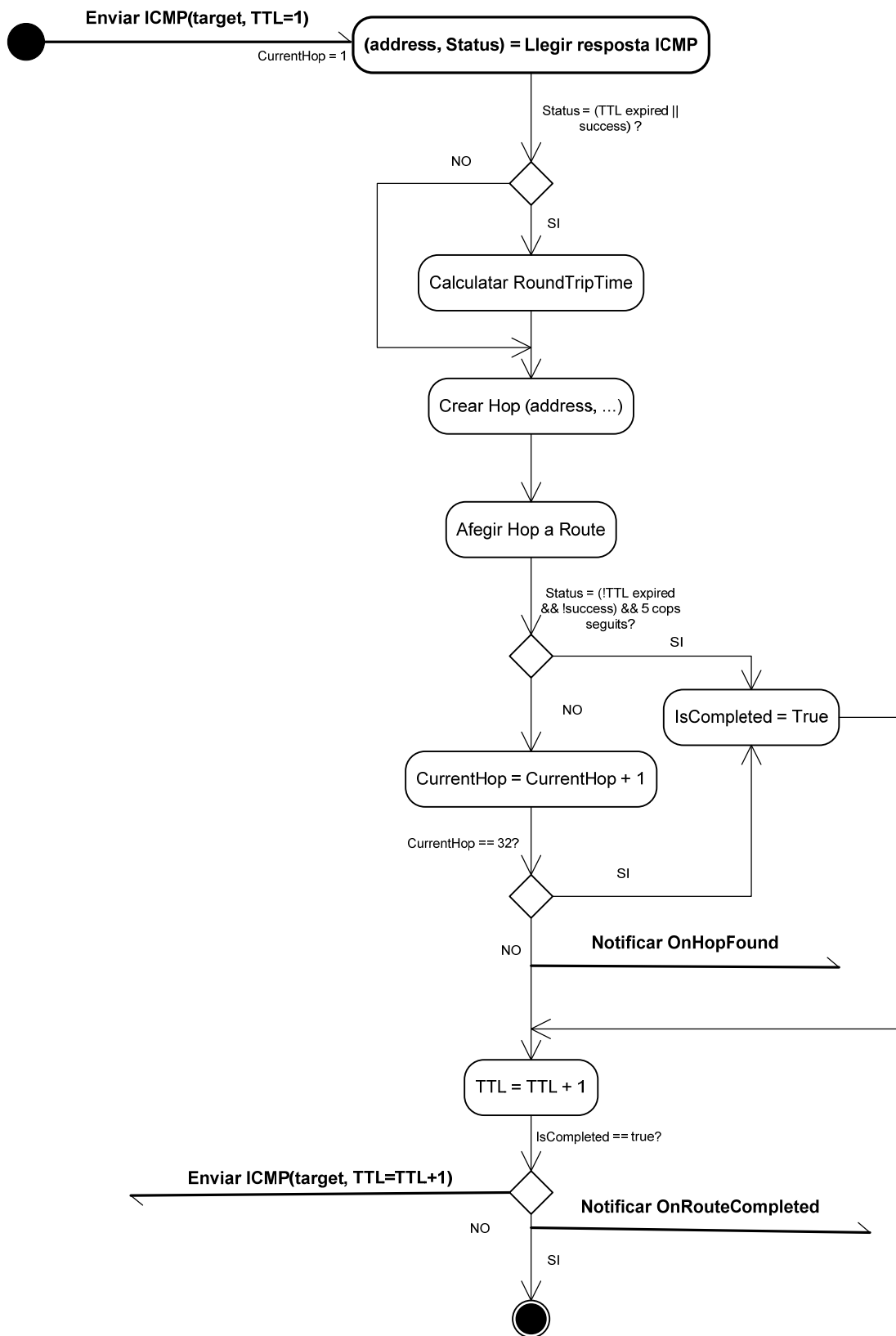


Figura 11. Procés de traça

Com que el procés de traça requereix l'adreça IP destí com a paràmetre, la interfície ha d'obtenir aquesta adreça en cas de que l'usuari hagi escrit un nom d'host. Aquesta traducció es fa també en modus asíncron per a no bloquejar l'intefície:

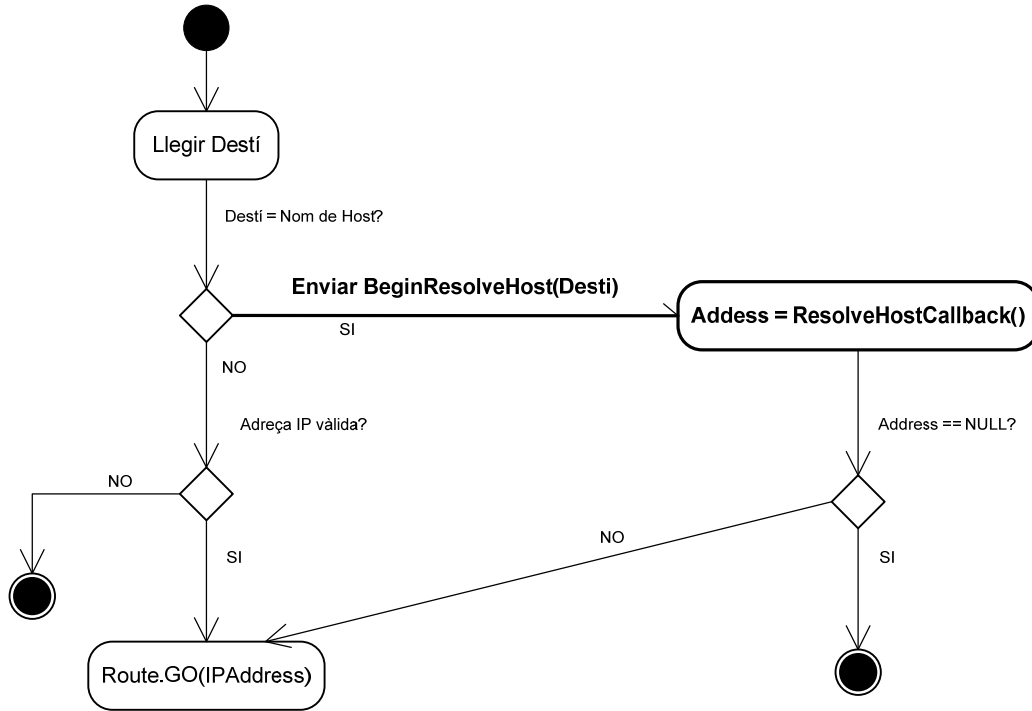


Figura 12. Procés de resolució de nom

3.2.4. Integració amb la interfície d'usuari

En l'exemple que es mostra a continuació, la interfície ha subscrit els esdeveniments de *OnHopFound* i *OnRouteCompleted* per a visualitzar en el mateix temps que es van descobrir els nodes, l'adreça IP i el temps de resposta:

salt	temps	adreça IP
1	1 ms	192.168.0.1
2	40 ms	87.219.168.1
3	-	-
4	38 ms	212.106.216.163
5	-	-
6	87 ms	212.106.216.101
7	87 ms	195.66.224.21
8	154 ms	72.52.92.77
9	215 ms	72.52.92.226
10	341 ms	216.218.134.218

Figura 13. Visualització de part d'una traça

CAPÍTOL 4

OBTENCIÓ DE DADES ADDICIONALS

4.1. OBJECTIUS

Tal com s'ha explicat en el capítol 2 (*Fonaments de la Geolocalització IP*), existeixen una sèrie de procediments pels quals s'obté informació addicional d'una adreça IP. En aquest nivell, es treu la següent informació addicional de les adreces IP dels nodes de la ruta:

- Nom canònic corresponent al DNS invertit.
- Informació Whois del propietari del domini corresponent al nom canònic de l'adreça IP.
- Informació de Whois de la xarxa a la qual pertany l'adreça IP.
- Localització física (ciutat – país).
- Coordenades geogràfiques (latitud – longitud).

Així mateix, seguint la mateixa filosofia de disseny aplicada al primer nivell, els requisits marcats per a aquesta etapa són els següents:

- Els procediments per a obtenir informació addicional de les adreces IP als nodes s'han d'executar durant el transcurs de descobriment de la ruta.
- Per tal d'evitar bloquejos de la interfície d'usuari i optimitzar els temps de resposta, les connexions als diferents servidors de dades es fan de forma asíncrona.
- Obtenir de forma concurrent aquella informació que no tingui dependència mútua.
- El codi ha de ser independent de la interfície.

4.2. DISSENY I IMPLEMENTACIÓ

Una primera fase del disseny consisteix en analitzar les dependències entre les diferents tasques d'obtenció d'informació addicional, per avaluar la possibilitat d'execució concurrent i optimitzar els temps d'execució. El següent diagrama mostra aquestes dependències:

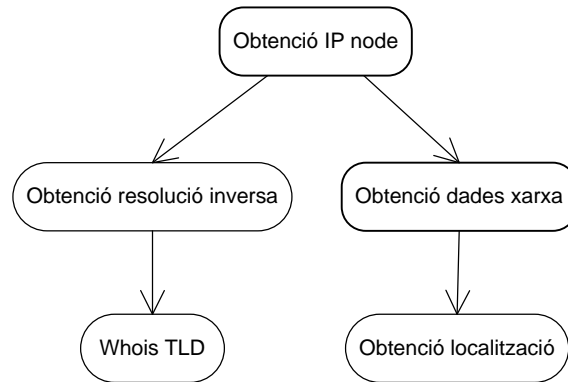


Figura 14. Dependència de dades

Els processos de resolució inversa i d'obtenció de dades de xarxa no depenen entre ells i, per tant, es poden executar concurrentment tal com indica el diagrama següent:

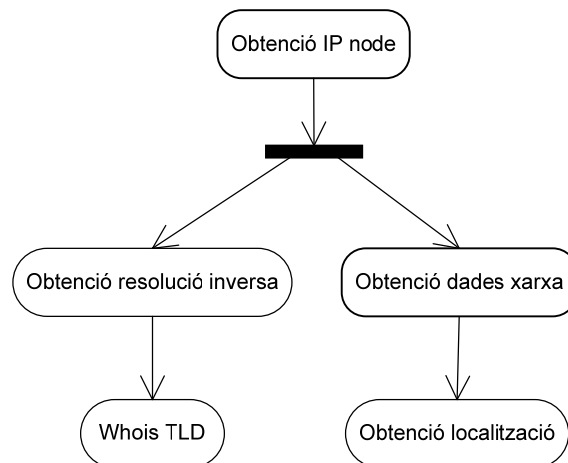


Figura 15. Concurrencia de processos

Seguidament s'exposa com queden actualitzades les classes *Hop* i *Route*, la nova classe *DomainPool* i els diagrames d'implementació de cada activitat.

4.2.1. La classe *DomainPool*

Durant el transcurs d'una traça, és molt fàcil, que diferents nodes de la ruta pertanyin al mateix domini. No té sentit, quan existeix aquesta duplicitat de nom de domini, de realitzar la consulta whois repetidament pel mateix domini. Per a evitar aquesta situació, es defineix la classe *DomainPool*.

Membres		
Nom	Tipus	Descripció
m_DomainPool	Llista de InternetDomain	Manté la llista d'elements InternetDomain (nom de domini i informació whois)

Mètodes		
Nom	Tipus	Descripció
DomainPool ()	Private	Constructor. Crea la instància de la llista.
Clear ()	Public	Esborra la llista
Add (domainName, Registrant)	Public	Afegeix un domini a la llista
IndexOf (domainName)	Public	Retorna posició de la llista pel domini indicat
GetRegistrant(domainName)	Public	Retorna la informació del domini indicat
GetRegistrant (posicio)	Public	Retorna la informació del domini de la posició indicada a la llista

4.2.2. La classe *Hop* actualitzada

Aquesta classe afegeix nous camps i mètodes per a donar cabuda a la nova informació:

Membres		
Nom	Tipus	Descripció
m_HopNumber	Int	Número de salt
m_Address	IPAddress	Adreça IP
m_Status	IPStatus	Estat retornat de la resposta a sol.licitud eco
m_Type	TypeOfIP	Tipus d'adreça IP
m_RoundTripTime	Long	Temps de resposta
m_ReverseHostName	String	Nom canònic
m_DomainOwnerIndex	Int	Posició de la llista de DomainPool on és la informació del domini
m_NetworkName	String	Nom de la Xarxa (informació tret del whois)

m_NetworkOwner	String	Informació del Whois de la xarxa
m_CityRegion	String	Ciutat o Regió
m_Country	String	País
m_CountryCode	String	Codi ISO de país
m_IsReliable	Bool	Indica si la localització física inclou el nom de ciutat/Regió
m_Latitude	String	Latitud geogràfica de la IP
m_Longitude	String	Longitud geogràfica de la IP
m_Completed	Flags	Indica quin tipus d'informació addicional hi ha obtinguda

Mètodes		
Nom	Tipus	Descripció
Hop(int number, IPAddress address, IPStatus status, long roundTripTime)	Public	Constructor. Crea un node.
TypeOfIP GetTypeOfIP(IPAddress address)	Public	Mètode estàtic per a tipificar el tipus d'adreça IP.

4.2.3. La classe *Route* actualitzada

La classe Route incorpora principalment nous mètodes, delegats i esdeveniments per als processos d'obtenció de dades addicionals i notificacions.

Membres		
Nom	Tipus	Descripció
m_Target	IPAddress	Adreça IP destí
m_Hops	List	Llista de nodes que formen la ruta
m_IsCompleted	bool	Estat de si la ruta està finalitzada o no
m_State	Enum	Estat del procés de traça.
m_RoundTripTime	Long	Temps de resposta

Mètodes		
Nom	Tipus	Descripció
Route ()	Public	Constructor. Instancia un objecte de tipus Route
Clear ()	Private	Esborra la ruta i llibera recursos
Hop (int hopNumber)	Public	Retorna el Hop indicat per parametre
Go (IPAddress target)	Public	Fa el proces de traça
OnPingCompleted ()	Private	Processa el callback d'una crida asincrona al enviament d'un paquet ICMP
ProcessHop(int hopNumber, IPAddress ip, IPStatus status)	Private	Processa el retorn del paquet ICMP i crea el node.
GetHostEntryCallback(..)	Private	Processa el callback d'executar una crida asíncrona a <i>GetReverseHost</i>
GetTLD (name)	Public	Retorna el TLD d'un nom de host
GetDomain (name)	Public	Retorna el nom de domini extret d'un nom d'host
WhoisTLD (hopNumber)	Private	Obté la informació de Whois del domini del número de node indicat
WhoisBeginConnectCallback (...)	Private	Processa el <i>callback</i> de connexió als whois dels TLD
WhoisNet (hopNumber)	Private	Obté la informació de whois de la IP
WhoisNetBeginConnectCallback(...)	Private	Processa el <i>callback</i> de la connexió als servidors de whois dels RIR
GetNetworkName (...)	Private	Retorna el nom de la xarxa a partir de la informació del whois.
Geocode (hopNumber)	Private	Inicia proces d'obtenció de dades geogràfiques
HostIpInfoCode (hopNumber)	Private	Consulta a <i>hostip.info</i> les dades geogràfiques de la IP del node.
hostipinfoCallback(..)	Private	Processa el <i>callback</i> de la connexió a <i>hostip.info</i>
GoogleCode (hopNumber)	Private	Consulta en <i>maps.google.com</i> les coordenades geogràfiques d'una localització física
GoogleCodeCallback(...)	Private	Processa el <i>callback</i> de la connexió a <i>maps.google.com</i>
CheckIfCompleted()	Private	Comprova si s'ha acabat el procés de ruta i en cas afirmatiu llença l'esdeveniment <i>OnRouteCompleted</i>

Delegats / Esdeveniments		
Nom	Tipus	Descripció
HopFoundHandler () / OnHopFound	Public	Notificació de node trobat.
RouteCompletedHandler() / OnRouteCompleted	Public	Notificació de que ja s'ha acabat la traça
ReverseFoundHandler() / OnReverseFound	Public	Notificació de que s'ha trobat nom canònic
WhoisTLDFoundHandler() / OnWhoisTLDFound	Public	Notificació de que es té whois del domini.
WhoisNetFoundHandler() / OnWhoisNetFound	Public	Notificació de que es té whois de la xarxa
LocationFoundHandler() / OnLocationFound	Public	Notificació de que es té localització
CoordinatesFoundHandler() / OnCoordinatesFound	Public	Notificació de que es té les coordenades geogràfiques

El nivell superior, subscriu tots els esdeveniments i així pot actualitzar la informació en la seva interfície d'usuari al mateix temps que les dades van apareixent. Si la interfície només subscriu l'esdeveniment de *OnRouteCompleted* serà notificat quan el procés de descobriment de ruta i informació addicional hagi acabat.

4.2.4. Implementació

A continuació es detalla cada una de les tasques que engloben el nivell d'obtenció de dades addicionals.

Obtenció de nodes

L'esquema l'indicat en el capítol anterior i se simplifica aquí com un sol procés al que se li ha afegit les crides concurrents a obtenció de dades de resolució inversa i de xarxa:

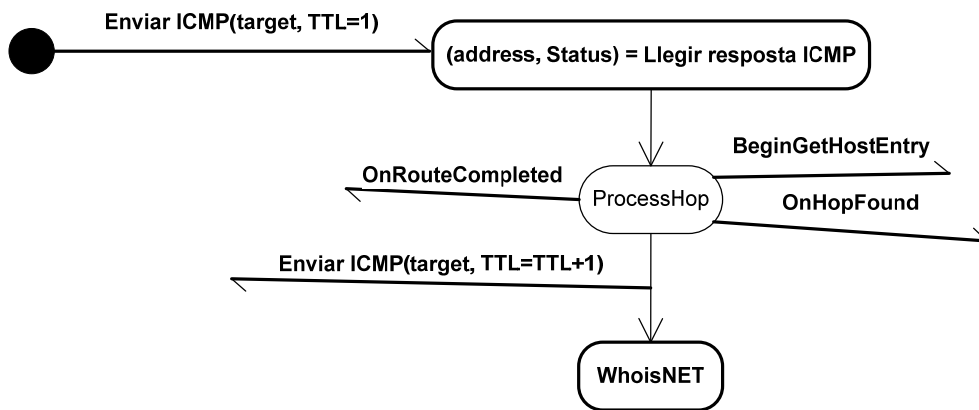


Figura 16. Versió resumida del procés de recerca de nodes

Obtenció de resolució inversa DNS

Aquest procediment realitzat amb crides asíncrones, continua, una vegada obté el nom associat a l'adreça IP, amb la fase de consulta d'informació addicional del domini associat al nom (WhoisTLD).

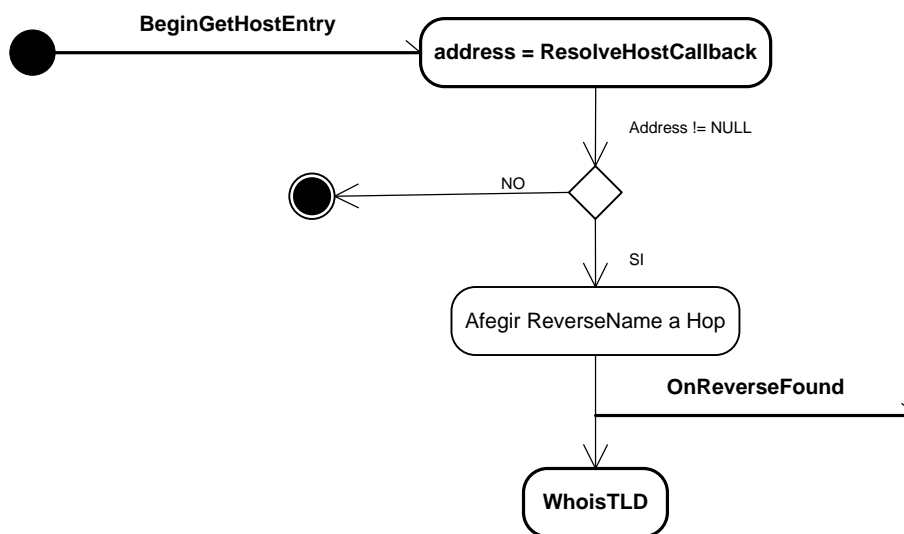


Figura 17. Procés d'obtenció de la resolució inversa de l'adreça IP

Propietari del domini (WhoisTLD)

En el cas de què l'adreça IP tingui un nom canònic associat, podem obtenir la informació corresponent al propietari del domini. Això comporta fer una consulta al whois del TLD del domini. Així mateix, molt dominis tenen una jerarquia de segon nivell aplicada i per

tant, hem de tenir en compte exemples com el següent a l'hora de treure el nom de domini sobre el que fer la consulta whois:

Nom canònic	Domini a consultar
163.216.106.212.static.jazztel.es	jazztel.es
f6.top.vip.oqk.yahoo.co.jp	yahoo.co.jp

La consulta whois es fa en un màxim de dos passos. En el primer d'ells, es consulta <TLD>.whois-servers.net. Aquesta primera consulta pot retorna les dades del whois del domini o bé, retorna el nombre del servidor whois sobre el que s'ha de fer la consulta. En aquest cas, es llança una nova consulta sobre aquest segon servidor.

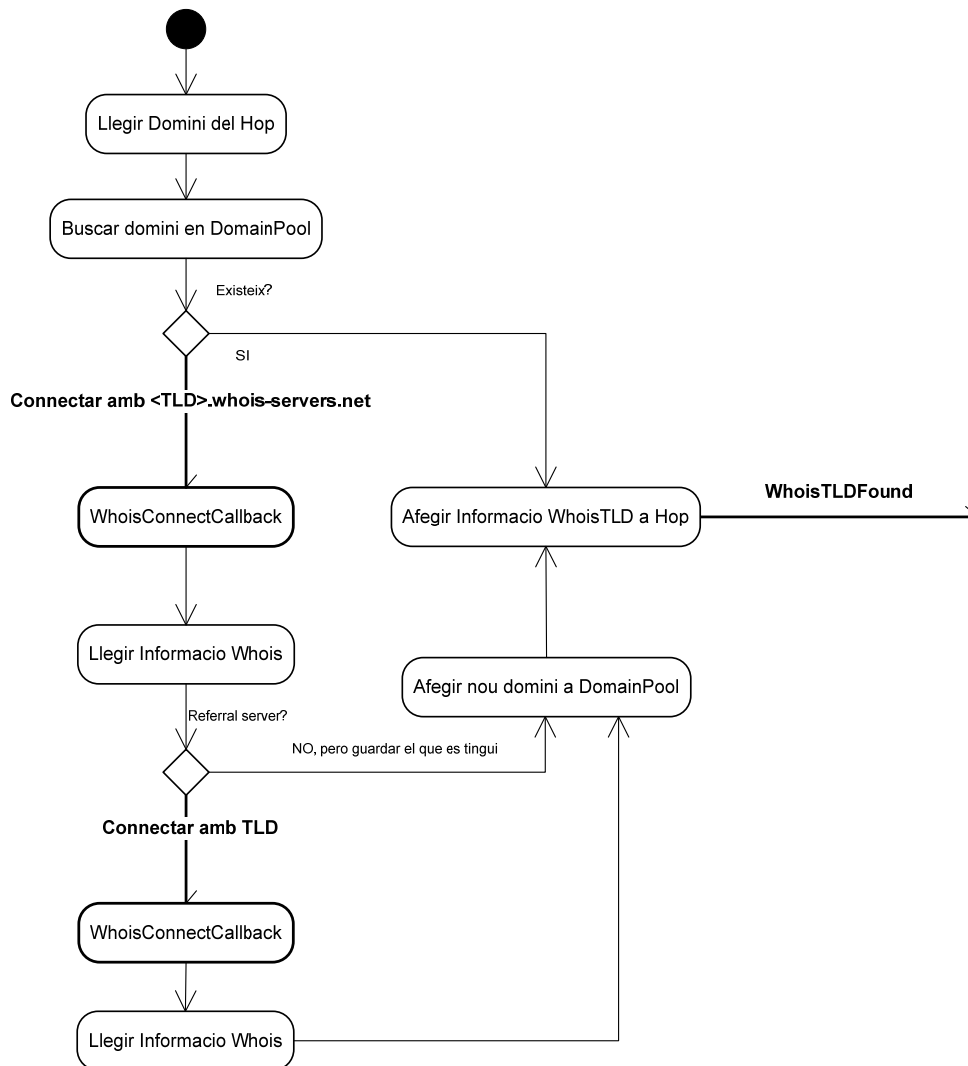


Figura 18. Procés de consulta WhoisTLD

Propietari de la Xarxa (WhoisNET)

A l'igual que per a la consulta del propietari del domini, la consulta del propietari de la xarxa també tindrà un màxim de dos passos: en el primer d'ells, es consulta whois.arin.net. Si aquesta primera consulta dóna informació sobre el servidor whois al que s'ha de dirigir la consulta llavors es realitza la pregunta a aquest nou servidor. En cas contrari es llegeix la informació que es tingui. En el segon servidor només s'ha de llegir la informació.

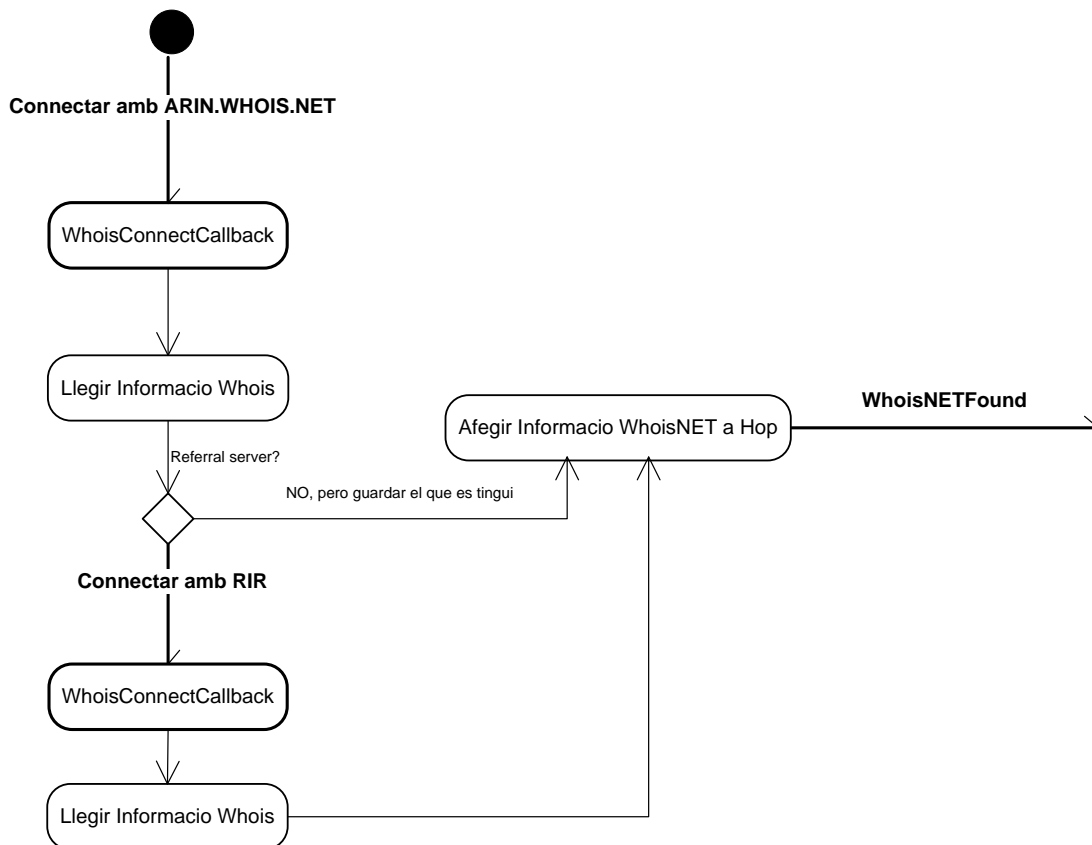


Figura 19. Procés de consulta WhoisNET

Localització geogràfica

Per la implementació de l'obtenció de dades de localització (ciutat-país i latitud-longitud) se segueix el procediment definit en les conclusions del capítol anterior:

- Realitzar una primera consulta al servei Hostip.info on es pot arribar a obtenir la ciutat, país, codi de país i coordenades geogràfiques. No obstant, les coordenades

geogràfiques només s'obtenen si hi ha informació de la ciutat. Per altra banda, pot ser que aquesta consulta no retorni cap tipus d'informació.

- Llegir el codi de país de la informació de la xarxa per a quan hostip.info no ha donat resultat.
- Fer servir la interfície de geocodificació de *maps.google.com/maps/geo* per a quan es necessiten les coordenades geogràfiques quan la consulta a hostip.info no les ha donat.

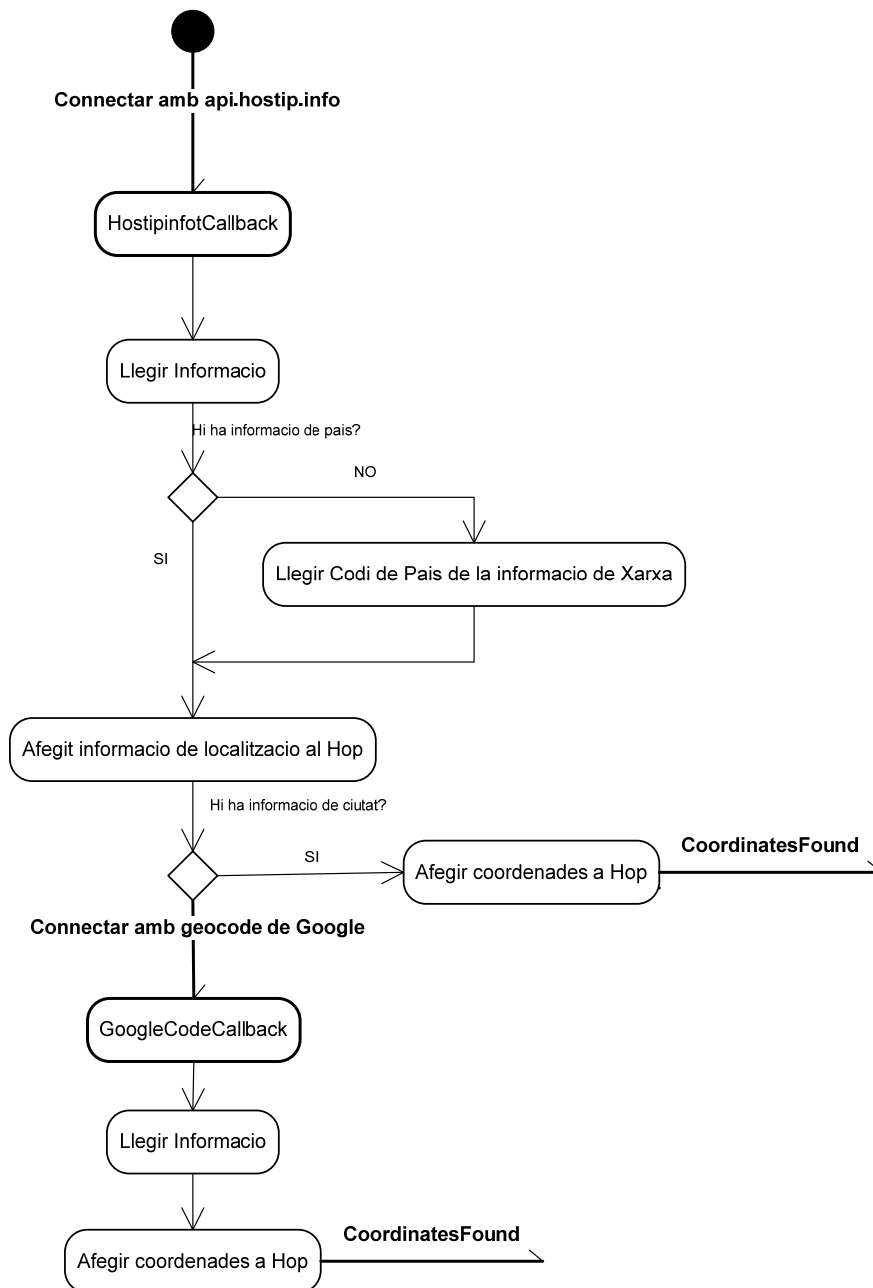


Figura 20. Procés d'obtenció de localització

4.2.5. Integració amb la interfície d'usuari

La interfície, que ha subscrit tots els esdeveniments definits en la classe *Route*, pot visualitzar la traça a mesura que es va descobrint, juntament amb la informació addicional. Par d'aquesta informació addicional, es visualitza en finestres separades degut a la seva extensió:

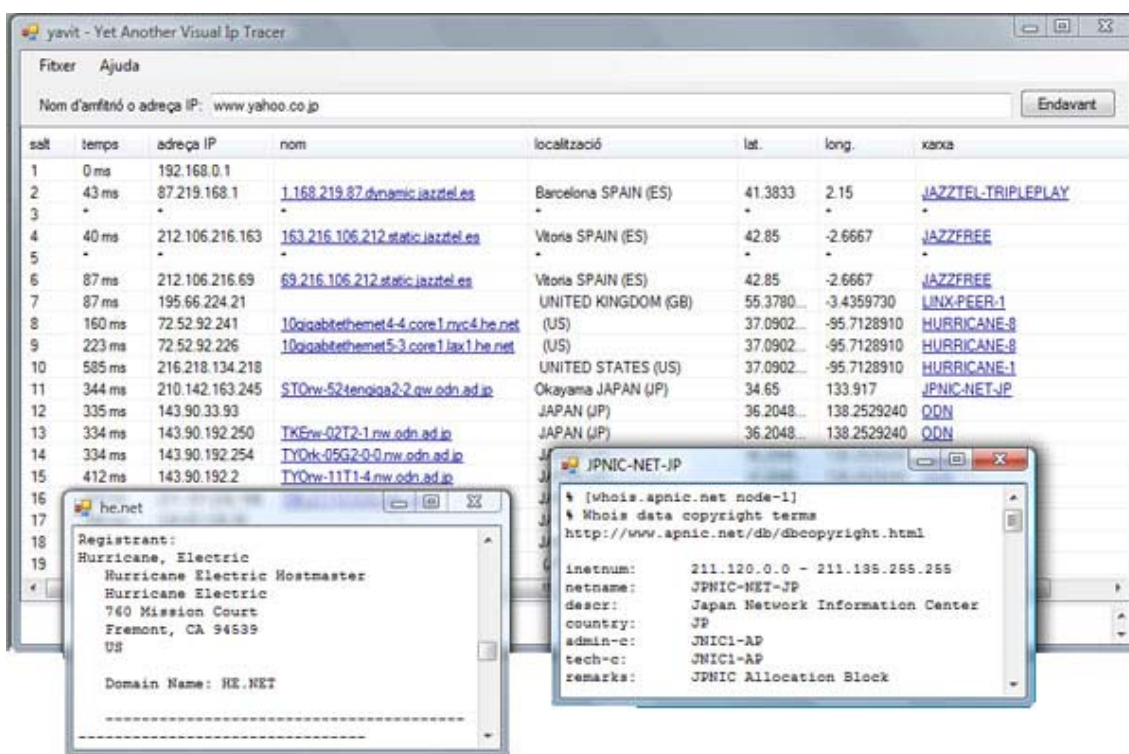


Figura 21. Interfície amb la traça i les dades addicionals

CAPÍTOL 5

VISUALITZACIÓ

5.1. OBJECTIUS

Aquest és l'últim nivell en el desenvolupament de l'aplicació. L'aplicació ja té implementat tots els processos necessaris per a descobrir la traça i al mateix temps ha recollit informació addicional de cada un dels nodes, entre les que es troben les coordenades geogràfiques.

D'acord amb les conclusions tretes del capítol 2, l'objectiu d'aquest nivell és representar la ruta en mapa fent servir l'API de GoogleMaps. Així com els nivells inferiors eren independents de la interfície de l'usuari, aquest últim nivell, de presentació, forma part de la interfície.

5.2. DISSENY I IMPLEMENTACIÓ

Per a la visualització del mapa en l'aplicació, disposarem d'una àrea de mida flexible dintre de la finestra de l'aplicació:

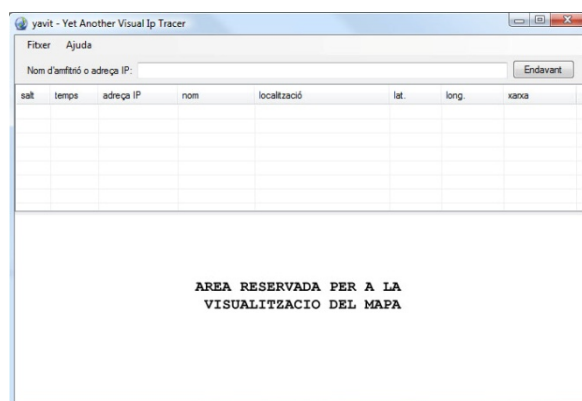


Figura 22. Àrea de visualització del mapa

Per altra banda, donats les possibilitats que ofereix l'API de GoogleMaps, es fa servir els següents criteris de representació:

- La traça es dibuixa amb una línia de color vermella amb una opacitat del 50%.
- Els nodes estan marcat amb icones numerats d'acord amb el número de salt.
- Els nodes dels que es disposa d'informació de ciutat, es representen de color verd.
- Els nodes dels que només es disposa de la informació del país es visualitza en color taronja. En aquest cas, les coordenades corresponen al centre geogràfic del país.
- Els nodes incorporen una bombolla d'informació amb les dades de nom de dispositiu, xarxa a la qual pertany i nom de domini.

Per a la incorporació del mapa dintre de l'aplicació, es crea un objecte de la classe *HttpRequest* al que se li afegeix el codi HTML i javascript necessari d'acord amb la informació que s'ha obtingut de la ruta.

Exemples

Seguidament es mostren uns quants exemples de traçes a diferents destinacions:

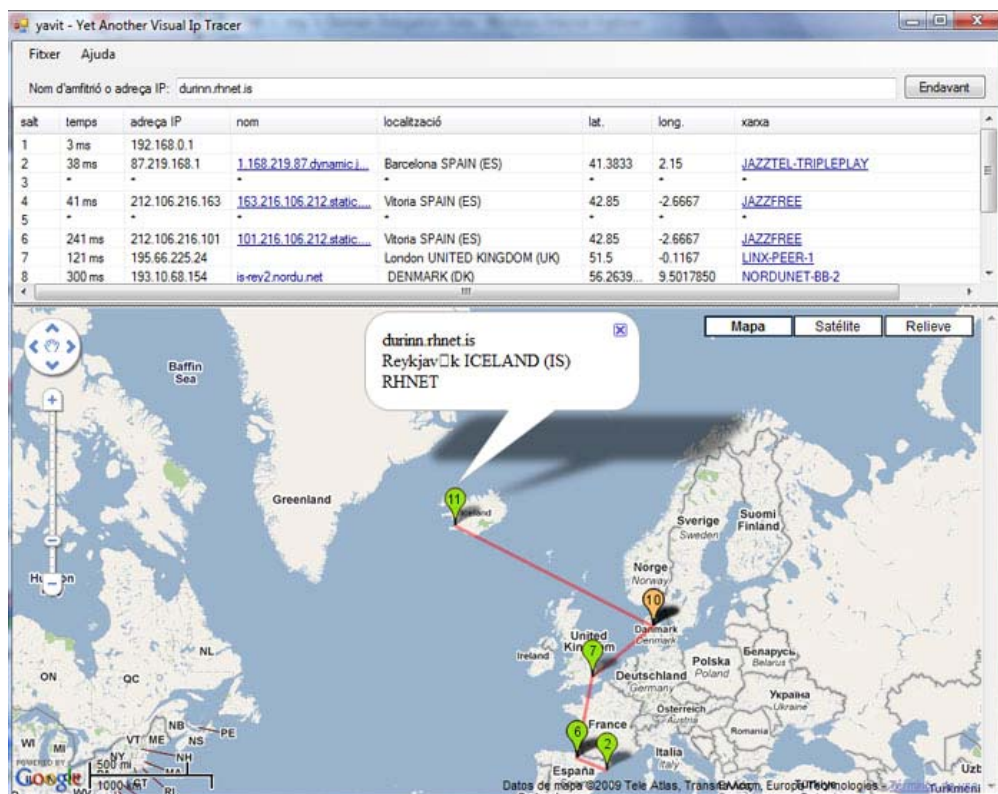


Figura 23. Traça a durinn.rhnet.is

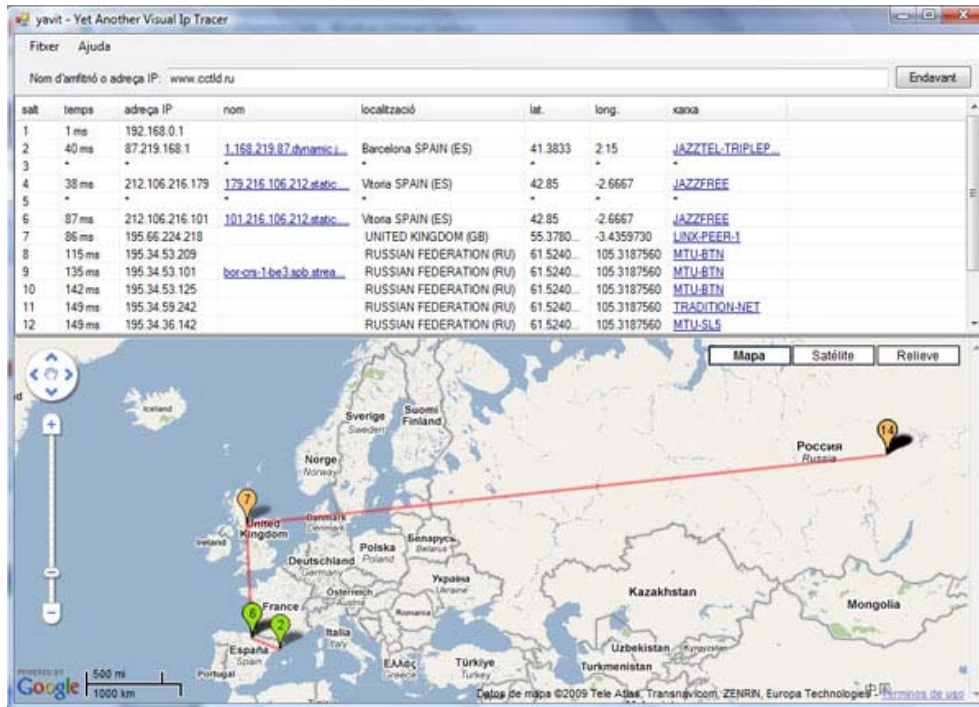


Figura 24. Traça a www.cctld.ru

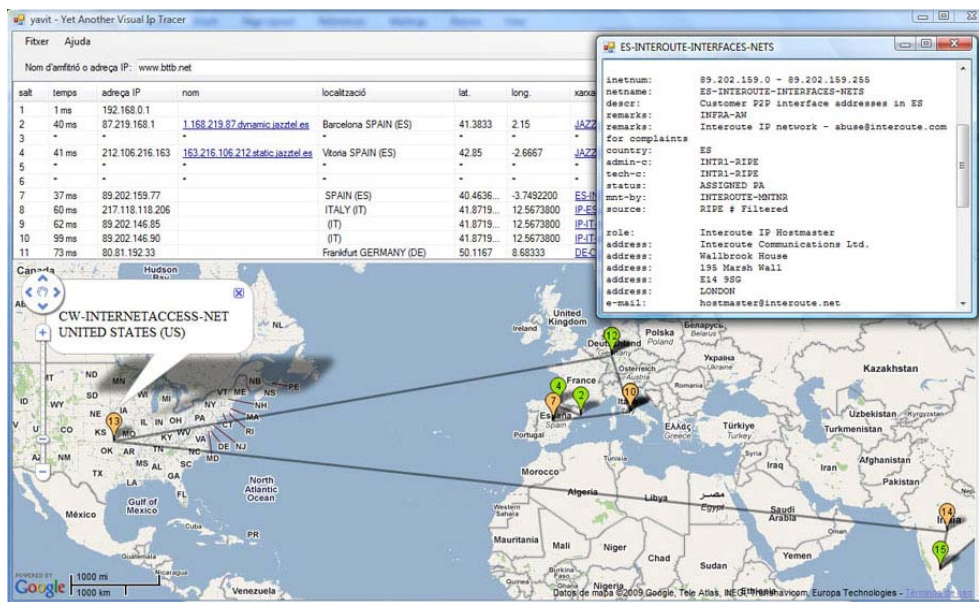


Figura 25. Traça a www.bttb.net

CAPÍTOL 6

CONCLUSIONS

La geolocalització IP és un procés de precisió variable. L'únic servei pensat expressament per a posicionar geogràficament una adreça IP o xarxa (DNS-LOC) gairebé no es fa servir per la manca de dades. L'alternativa és, doncs, utilitzar serveis no pensats per aquest objectiu però que poden donar uns resultats acceptables.

La informació té cada vegada més valor en la nostra societat i això inclou la localització d'adreces IP. Per això, davant la problemàtica de la manca de precisió, empreses privades han començat a mantenir les seves pròpies bases de dades i comercialitzen un servei de geolocalització IP que fa servir importants empreses de tot el món.

Aquest projecte ha assolit els objectius fixats i ha aportat una solució basada en la combinació dels mecanismes tradicionals de cerca (servidors whois, DNS invertit, etc.) juntament amb un servei alternatiu gratuït (amb menys precisió que els comercials) i que ha demostrat que pot donar informació més precisa que pels camins tradicionals.

També, l'aplicació desenvolupada és una alternativa molt intuïtiva i de fàcil ús a les ja existents per a la visualització de traces IP i que incorpora GoogleMaps com a eina de representació del Mapa.

BIBLIOGRAFIA

Blum, Richard. 2003. *C# Network Programming*. s.l. : SYBEX, 2003.

GeoBytes, Inc. IP Address Locator. [En línia] <http://www.geobytes.com/IpLocator.htm>.

Google, Inc. Geocoding - Google Maps API Services - Google Code. *Google.com*. [En línia] <http://code.google.com/apis/maps/documentation/geocoding/>.

—. Superposiciones en mapas - API de Google Maps - Google Code. *Google*. [En línia] <http://code.google.com/intl/es/apis/maps/documentation/overlays.html>.

IPelligence Geolocation Solutions. Find IP Address geolocation. *IP Geolocator*. [En línia] <http://www.ipelligence.com/geolocation>.

ISO. ISO - Maintenance Agency for ISO 3166 country codes. *www.iso.org*. [En línia] http://www.iso.org/iso/country_codes.

Makofske, David B., Donahoo, Michael J. and Calvert, Kenneth L. 2004. *TCP/IP Sockets in C#: Practical Guide for Programmers*. s.l. : Morgan Kaufmann, 2004.

MaxMind, Inc. MaxMind . City/ISP/Org Web Service. [En línia] http://www.maxmind.com/app/web_services_cityisporg_usage.

My IP Address Lookup and GeoTargetting. [En línia] <http://www.hostip.info/>.

Visualware. VisualRoute IPv4 and IPv6 traceroute, connectivity test. *Visualware's VisualRoute 2009*. [En línia] <http://www.visualroute.com/>.

VOSTROM Holdings, Inc. Path Analyzer Pro - Graphical Traceroute, WhoIs, Charts, Maps, Performance Testing, ip location, tracert, trace route. *Path Analyzer Pro*. [En línia] <http://www.pathanalyzer.com/>.

Williams, Mike. Google Maps API Tutorial. [En línia] <http://econym.org.uk/gmap/>.

Wright, Gary R. and Stevens, W. Richard. 1994. *TCP/IP Illustrated, Volume 1*. s.l. : Addison-Wesley, 1994.

—. 1994. *TCP/IP Illustrated, Volume 2*. s.l. : Addison-Wesley, 1994.

Yahoo, Inc. Yahoo! Maps Web Services - Geocoding API. *Yahoo.com*. [En línea] Yahoo, Inc. <http://developer.yahoo.com/maps/rest/V1/geocode.html>.

ANNEX A

MANUAL D'USUARI

A.1. REQUISITS

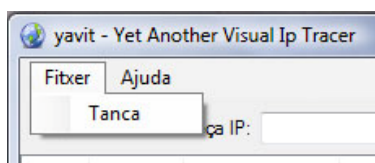
Per a l'execució de l'aplicació YAVIT es necessari:

- Sistema operatiu de la família Windows: WindowsXP, Windows Vista.
- Microsoft .NET Framework 2.1 o superior.
- Connexió a Internet correctament configurada.

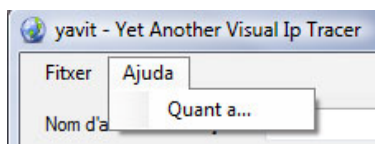
A.2. INSTAL·LACIÓ

No requereix de cap procés d'instal·lació. Copiar el Programa en qualsevol carpeta o directori i executar.

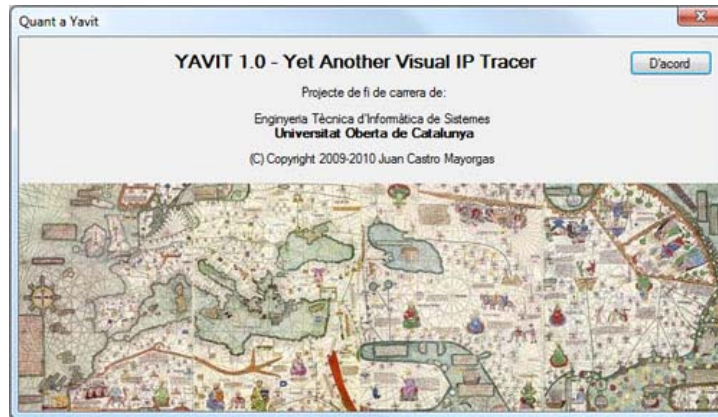
A.3. MENÚ



L'opció *Fitxer/Tanca* dona per terminada la execució de l'aplicació i tanca la finestra.

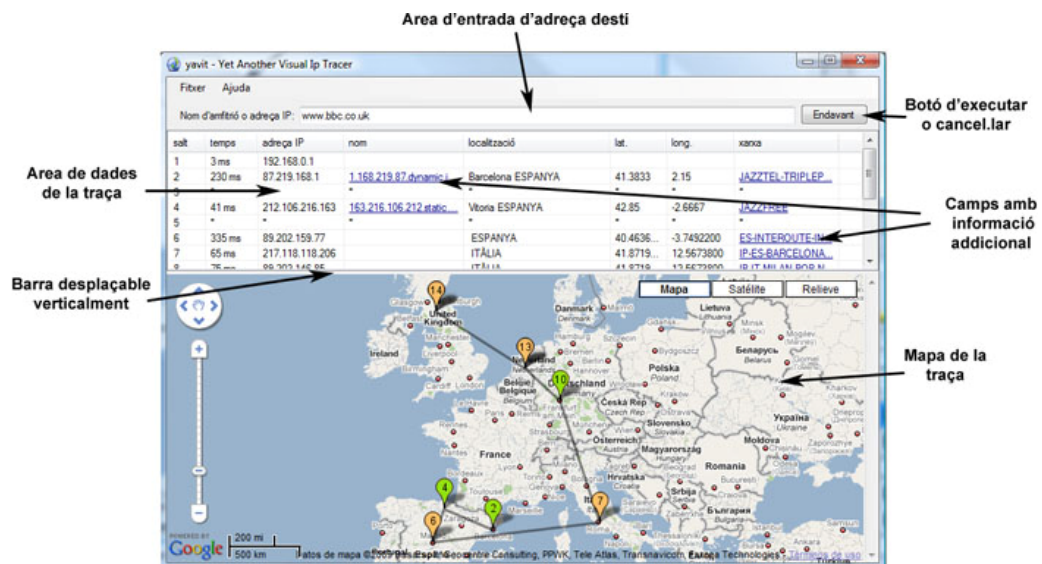


L'opció *Ajuda/Quant a...* obre una caixa de diàleg amb informació del projecte i autor del programa:



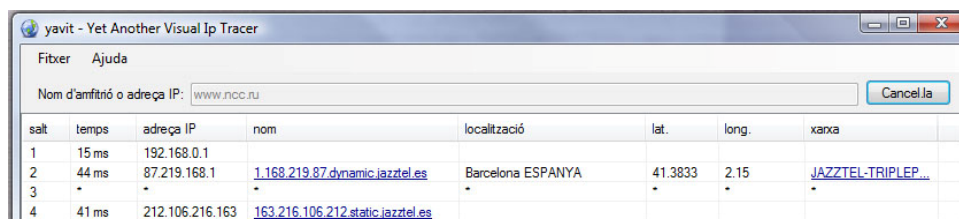
A.4. UTILITZACIÓ

Els elements principals de la interfície són els següents:

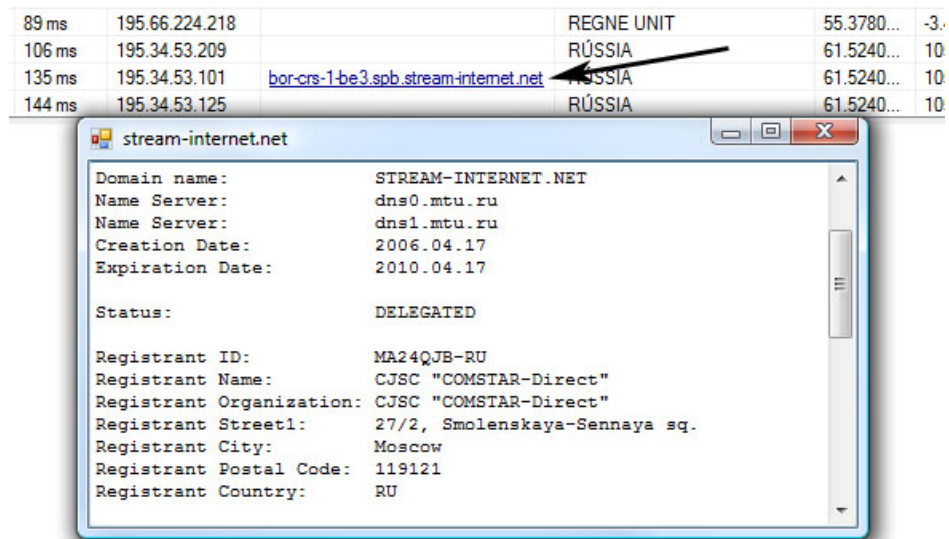


El procediment per a realitzar la traça a una adreça destí és el següent:

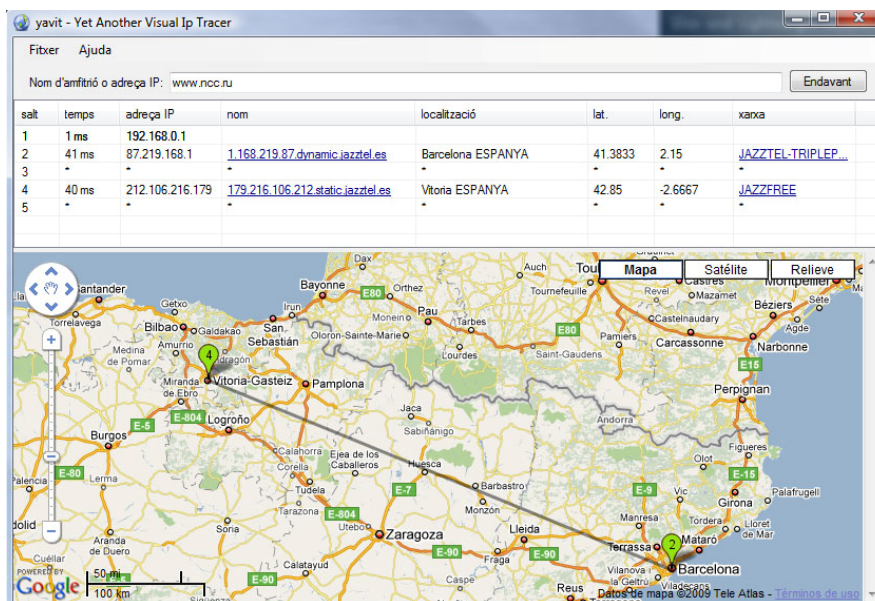
1. Introduir en l'àrea d'entrada, l'adreça destí i prémer el botó *Endavant*. En aquest moment la traça comença a realitzar-se i el botó passa a denominar-se *Cancel·la*.



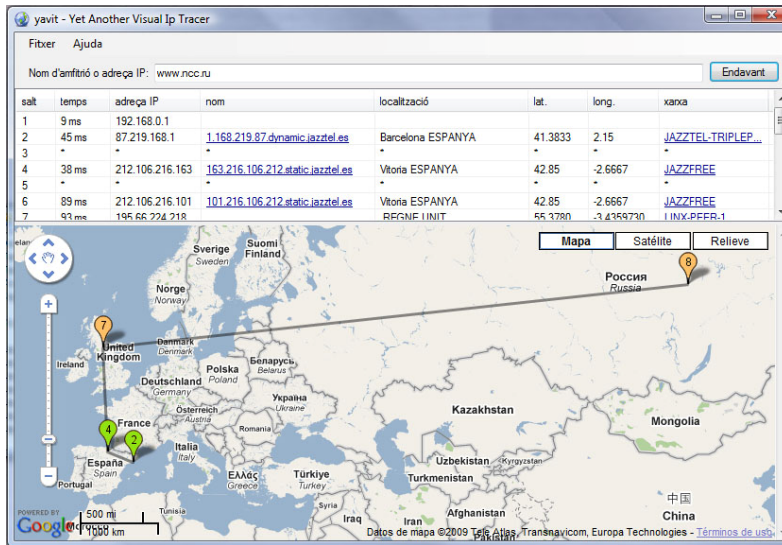
2. En qualsevol moment es pot fer clic sobre els valors dels camps nom i xarxa, on es visualitza en una finestra externa, les dades associades.



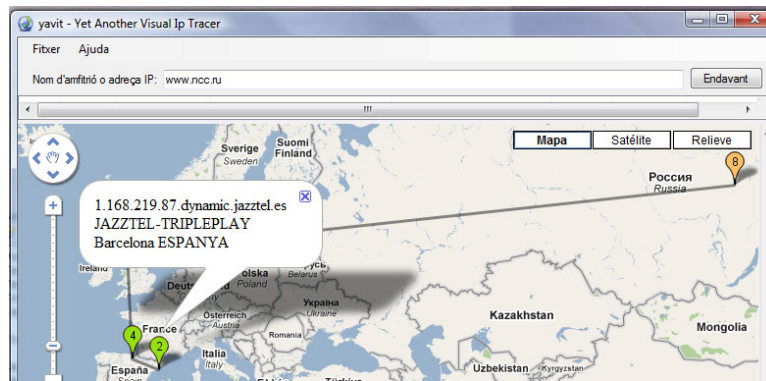
3. Si es prem el botó *Cancel·la* la traça para i visualitza la traça del trajecte que tenia fet fins el moment:



4. Si la traça no es cancel·la, visualitzarà la ruta sencera en el mapa:



5. En el mapa es pot fer clic sobre els nodes i es visualitza la informació rellevant d'aquest node:



6. Finalment, la interfície de botons i ratolí que ofereix GoogleMaps està activada en l'àrea del mapa i per tant, aquest pot ser ampliat, reduït, desplaçat, etc.:

