

# Xarxes: Treball de simulació d'una xarxa

GUILLEM CASASSAS BERTRAN, PAU SANCHEZ VALDIVIESO I ALBERT ESPÍN ROMÁN

TERCERA AVALUACIÓ PARCIAL | 17.01.2017

## Taula de continguts

1. Introducció i objectius.....	3
2. Explicació de la realització pràctica: construcció i anàlisi de la xarxa simulada.....	4
2.1. Visió general de la xarxa construïda.....	4
2.2. Routing o encaminament a la xarxa.....	8
2.3. Anàlisi dels camins, el trànsit i l'encapsulament de les dades.....	12
2.3.1. Exemple 1: Ping d'un ordinador de l'habitació taronja a un portàtil de l'habitació blava.....	12
2.3.2. Exemple 2: Enviament d'un correu electrònic amb SMTP mitjançant el servidor de l'habitació groga.....	28
3. Conclusions.....	47

## 1. Introducció i objectius

Aquest treball, que consisteix en la simulació d'una xarxa, va ser proposat pel professorat de Xarxes com a tercera avaluació parcial de l'assignatura; alternativament es podia realitzar aquest mateix exercici amb una xarxa real, però vam escollir l'opció de simular-la.

Els alumnes han de demostrar que comprenen el funcionament d'una xarxa i que són capaços de simular-ne una. Per a fer-ho, cal aplicar els coneixements superiors a les capes de baix nivell vistes fins ara (si prenem com a referència el model teòric OSI, ens referim a la capa física i a la d'enllaç): ara és l'hora d'estudiar el procés d'encaminament dels paquets a la següent capa, la de xarxa, així com el seu transport segur extrem a extrem a la capa de transport, l'establiment i control de sessions a la capa de sessió, l'encryptació, compressió i representació interna de la capa de presentació i finalment, al nivell més alt, l'accés dels usuaris i les aplicacions les comunicacions a la capa d'aplicació. Si prenem com a referència el model TCP/IP, l'utilitzat a la pràctica, podem dir que treballarem per sobre de les capes MAC i LLC, és a dir, als nivells d'IP, de TCP o UDP i al nivell d'aplicació.

A grans trets, el que ens proposa el guió del treball, com veurem al següent apartat amb molt més detall, no és altra cosa que simular una xarxa i crear subxarxes de diferent tipus dins d'aquesta, com una cablejada o unasesne fils. Simularem la connexió de diferents ordinadors a la xarxa i l'enviament d'informació a través de la mateixa; analitzarem les dades que s'envien, inspeccionant el format de la informació a cada capa i el pas o evolució d'aquesta entre un nivell i un altre per adaptar-se al context d'aquest i complir el propòsit final d'enviar o rebre dades amb èxit, seguint un camí o ruta des de l'origen fins al destí de la informació.

Com podem veure, aquest treball no només ens insta a posar en pràctica els coneixements de les capes encara no avaluades a l'assignatura, sinó que ens convida a tornar a aplicar tot allò que ja hem après a fer, amb especial èmfasi a l'anàlisi del format i organització de les unitats de dades (des de seqüències de bits no estructurades fins a dades pròpies d'un software o aplicació, passant pel nivell de trama, datagrama i segment) mitjançant l'ús d'un software sniffer.

Per a la realització del treball, hem escollit utilitzar el simulador Cisco Packet Tracer, ja que ens hem informat que permet tant simular xarxes com analitzar el tràfic d'aquestes (el que anteriorment havíem fet amb Wireshark per a xarxes reals); addicionalment, ens ha semblat que es tracta, aparentment, d'una eina amb molta documentació disponible i molt utilitzada en context d'aprenentatge sobre el funcionament de les xarxes; els seus desenvolupadors, en particular, la cataloguen com l'eina adequada per sortir de dubtes en quant a preguntes de l'estil «què passaria si...» fem una certa acció a la nostra xarxa, tot plegat sense la possibilitat d'espantllar res, ja que tot és simulat.

## 2. Explicació de la realització pràctica: construcció i anàlisi de la xarxa simulada

### 2.1. Visió general de la xarxa construïda

L'objectiu que ens plantegem és el de construir una xarxa amb diferents routers, commutadors i ordinadors o equips d'altres tipus. Dividirem aquesta xarxa en diferents subxarxes per posar en pràctica els principis de subnetting, que ens permeten estructurar una xarxa en grups d'equips més pròxims entre si que es poden comunicar amb els de les altres subxarxes seguint un camí, a través dels routers, per exemple. La nostra xarxa tindrà la topologia pròpia d'una xarxa de commutació, ja que els paquets es transferiran de node en node a través de camins entre dispositius (seran commutats); no es tractarà en cap cas d'una xarxa de difusió ja que no tindrem cada dispositiu connectat amb tota la resta; ni d'una de difusió, en què tots es comuniquen per un únic canal comú.

Hem pensat que una forma de fer més interessant la xarxa a construir podria ser el fet de donar-li un propòsit o caràcter més definit, més concret, que no el d'una simple xarxa abstracta. És per això que hem plantejat la nostra xarxa com la xarxa d'una casa, on cada espai de la mateixa correspon a una subxarxa.

Tenim, concretament, quatre espais: tres habitacions i un jardí, a més d'un compartiment amb dos routers, cadascun d'ells connectats amb dos espais diferents, i connectats aquests dos routers també entre si, per fer possible que un missatge de qualsevol equip d'una zona pugui arribar a l'altra punta de la casa, a un altre espai. Si bé la xarxa s'hauria pogut implementar amb un únic router, el fet de tenir dos ens permet practicar amb les diferents tècniques d'enrutament més a fons.

Hem volgut que la nostra xarxa, a més, no estigués limitada al concepte tradicional de xarxa únicament d'ordinadors, sinó que pogués ser vista des d'una perspectiva més actual o moderna, com a xarxa d'Internet de les coses (IoT, Internet of Things; o bé IoE, Internet of Everything), en què qualsevol aparell de la casa amb la capacitat d'estar connectat amb altres equips pugui estar-ho, ja sigui a través d'enllaços cablejats o per l'aire, segons permeti el maquinari de cada objecte.

Així doncs, la xarxa de la casa que hem implementat permet connectar, per exemple, un smartphone amb una porta intel·ligent (es podria implementar que li enviés un missatge per a obrir-la a distància), tenint en compte que la connexió entre aquests dos aparells no és directa, sinó que l'smartphone enllaça amb connexió inalàmbrica amb un punt d'accés, que està connectat a un router, que troba la ruta més ràpida fins la porta, connectada amb cable Ethernet a la xarxa. És per aquesta connectivitat de la casa obtinguda gràcies a la seva xarxa, que considerarem que és una casa intel·ligent o «smart house», un habitatge on molts dels seus elements es poden comunicar i poden ser controlats a distància mitjançant missatges transmesos per la xarxa.

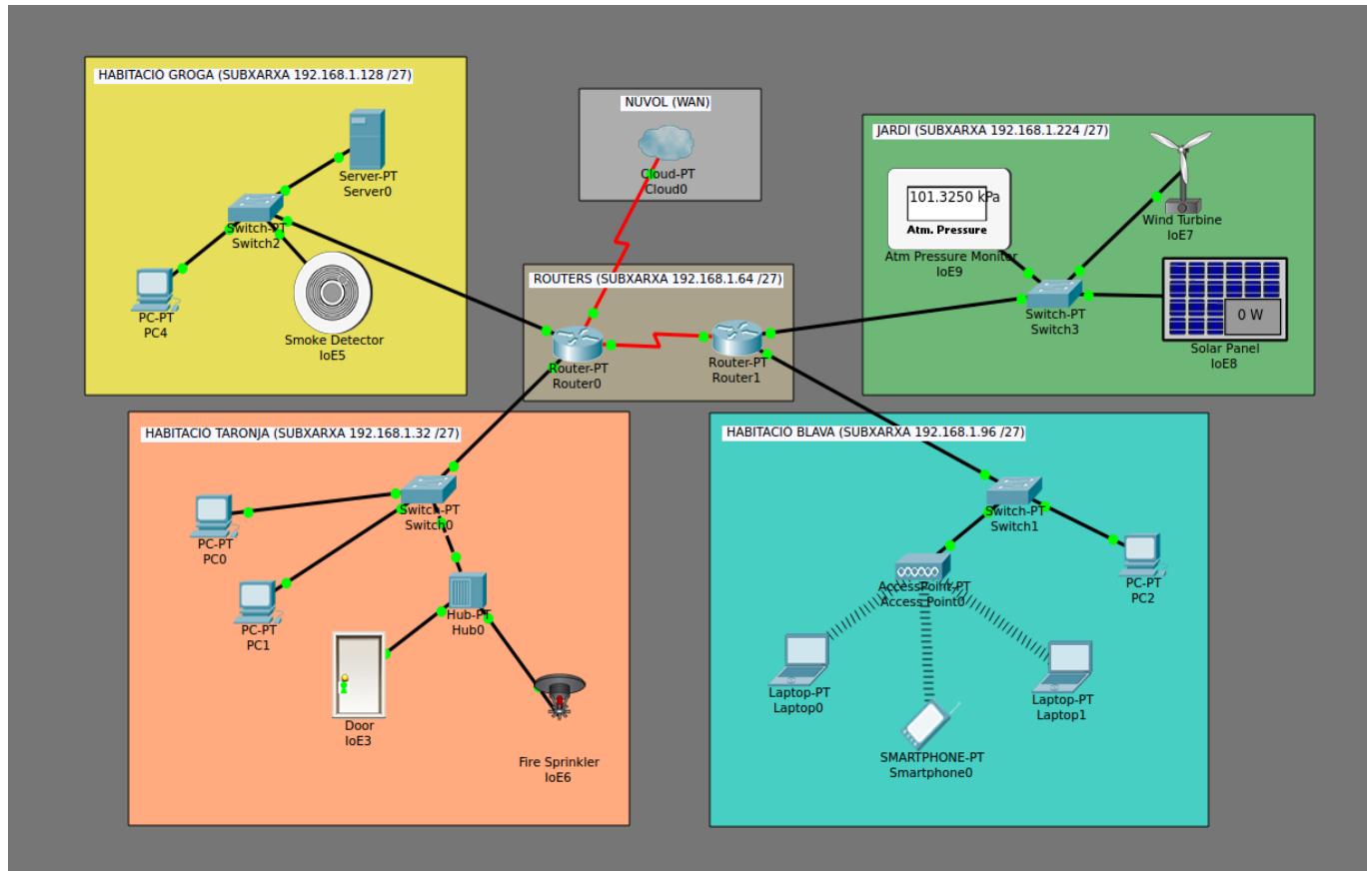


Figura 1: La xarxa que hem muntat, com a conjunt de subxarxes d'una «smart house»

Hem dit que la nostra xarxa consta per tant de 4 espais, a cadascun dels quals hem volgut donar una subxarxa independent, juntament amb una cinquena subxarxa per connectar els routers (podríem haver utilitzat una de les altres 4 per encabir els routers, però hem decidit donar-los una subxarxa pròpia); cadascun dels routers pertany en certa manera a cada subxarxa a la qual està directament connectat, ja que li proporciona l'adreça de porta d'enllaç o «Gateway», com veurem més endavant.

Hem definit que l'adreça IP privada de xarxa de la nostra xarxa és 192.168.1.0, de tipus C, que té per màscara 255.255.255.0, i que per tant pot ser representada com a 192.168.1.0 / 24. A priori, podem tenir 256 - 2 adreces independents per a dispositius de la nostra xarxa (descartem les IPs de xarxa i Broadcast), ja que tenim 8 bits pel hostid (els 24 bits de netid són 192.168.1), i per tant  $2^8$  possibilitats, menys les 2 reservades.

Com hem dit, però, volem dividir la xarxa en 5 subxarxes, i sabem que prenent bits addicionals del hostid podem delimitar aquestes subxarxes. Som conscients que agafant  $n$  bits obtindrem accés a tantes xarxes com el resultat d'elevat aquest nombre a 2: per a 5 subxares calen un mínim de 3 bits, ja que  $2^2 = 4 < 5$  però  $2^3 = 8 > 5$ . La nostra màscara passa per tant a ser de 27 bits, 255.255.255.248.

A la següent imatge mostrem les adreces de xarxa (o, millor dit, de subxarxa) de les nostres subxarxes, així com una breu etiqueta que identifica els tipus d'enllaç i la filosofia de cada subxarxa.

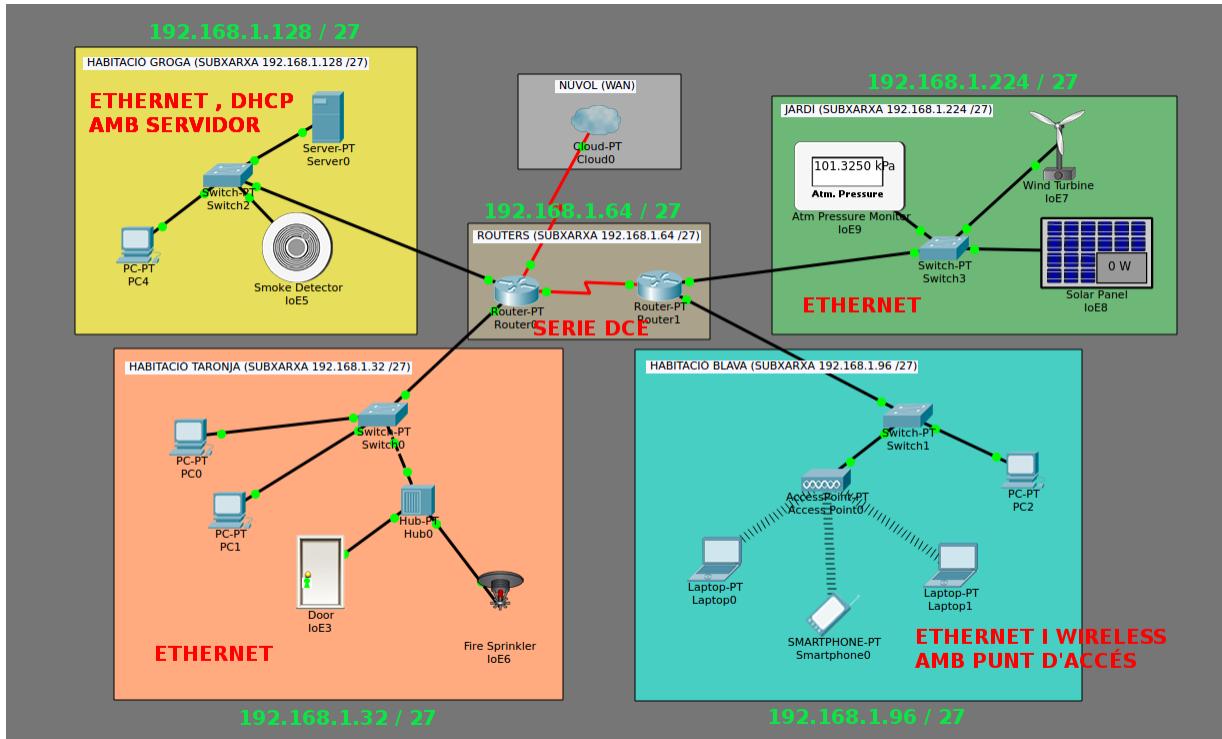


Figura 2: Indicació de l'adreça IP base de les subxarxes, així com el tipus de subxarxa que són (com pot ser Ethernet, wireless, etcètera).

A continuació analitzem el que mostra la imatge. Primerament, veiem que l'habitació groga, la de més a l'esquerra, té la IP base o de subxarxa 192.168.1.128 / 27, per tant els seus dispositius podran tenir adrecess des de 192.168.1.129 fins la darrera abans de Broadcast, 192.168.1.158; un total de 32 - 2 adreces úniques. Aquesta limitació a 30 IPs diferents és comú a la resta de subxarxes, per tant ja no repetirem aquesta dada quan parlem de les altres subxarxes; es deu al fet que una adreça de tipus C té una màscara de 24 bits 1s de partida, que com ja hem dit hem ampliat amb 3 1s més del hostid, de manera que només queden 5 bits dels 32 d'una adreça IP pels hostids de cada subxarxa, aspirant a  $2^5 - 2$  (subxarxa i Broadcast) adreces disponibles pels diferents dispositius; 30, com havíem dit.

L'habitació groga té una subxarxa cablejada amb Ethernet, que utilitza adreces dinàmiques proveïdes per DHCP (Dynamic Host Configuration Protocol). Aquest protocol permet que un servidor tingui la capacitat d'assignar adreces dinàmicament als dispositius de la xarxa (subxarxa al nostre cas), de manera que una mateixa adreça IP pot pertànyer a equips diferents al llarg del temps, però sempre en moments diferents (fins que no està lliure, una IP no pot ser assignada pel servidor). L'adreça que identifica la subxarxa és 192.168.1.128, i per tant hem fet que el router tingui 192.168.1.129 com a adreça estàtica de la seva interfície d'Ethernet, connectada a la subxarxa de l'habitació groga; al servidor li hem donat

l'adreça 192.168.1.140, i hem activat el servei DHCP en ell perquè pugui donar un màxim de 6 adreces dinàmiques a partir de la 192.168.1.150; d'aquesta manera, el servidor ha assignat a l'ordinador de la seva subxarxa precisament l'adreça 192.168.1.150 de forma dinàmica, i 192.168.1.151 al detector de fum, un dispositiu IoE connectat amb Ethernet; tots tres elements estan connectats per un switch o commutador, que treballa a nivell d'enllaç i que en rebre una trama d'una de les seves connexions Ethernet commuta el missatge cap a la connexió de sortida que determini adient, no a totes com faria un hub, que, treballant a nivell de capa física, envia a tots els dispositius a què està connectat allò que un li ha enviat, tret de l'emissor.

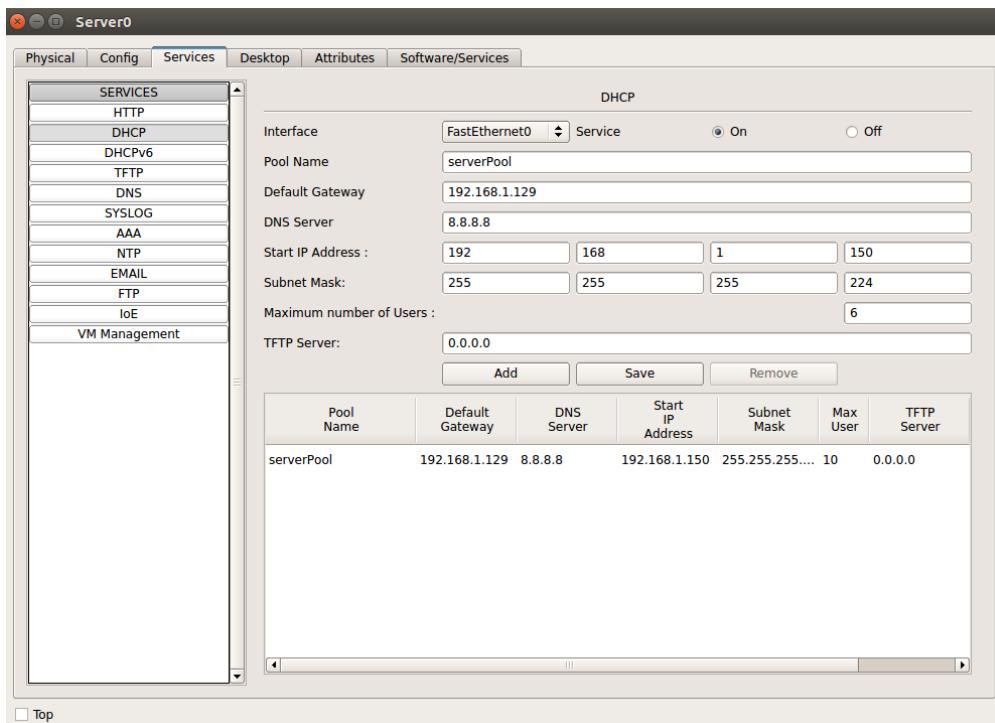


Figura 3: Configuració del servei DHCP del servidor de l'habitació groga perquè pugui assignar IPs dinàmicament

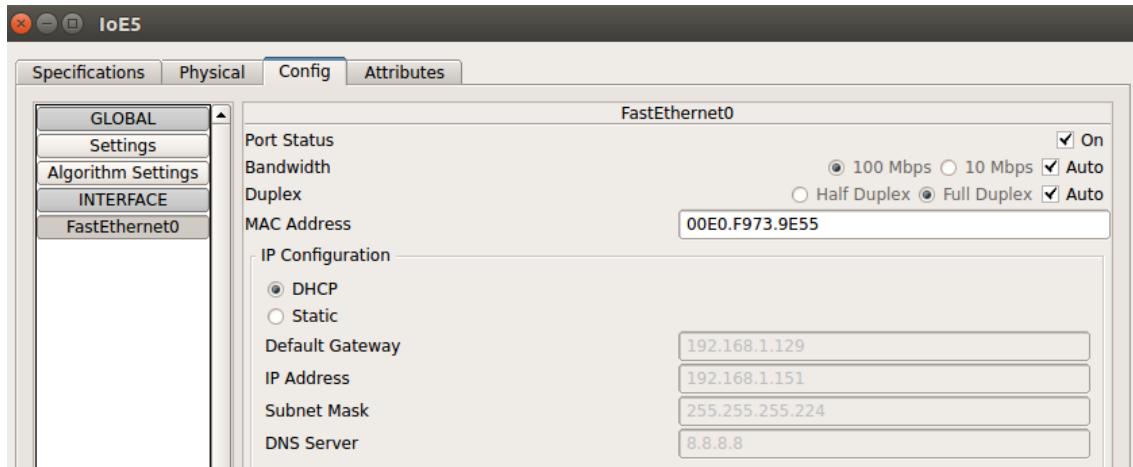


Figura 4: El servidor de l'habitació groga assigna automàticament una adreça IP de forma dinàmica al detector de fum, per mitjà de DHCP

El jardí i l'habitació taronja també són subxarxes basades amb Ethernet i connectades a un router que els subministra una adreça de porta d'enllaç i que els permet connectar-se amb la resta de la subxarxa. La diferència més destacable amb l'habitació groga és que, de forma diferent a ella, aquests espais treballen tots amb IPs estàtiques, que hem assignat manualment a cada dispositiu terminal.

L'habitació blava té una particularitat major, ja que conté dispositius connectats de forma cablejada amb Ethernet però també equips que s'incorporen a la xarxa inalàmbricament, gràcies a que hem instal·lat en ells mòduls «Linksys WPC300N» que els doten de connectivitat wireless (fent servir protocols IEEE 802.11, com podria ser Wifi) amb un punt d'accés que s'uneix a la xarxa de forma cablejada, amb Ethernet.

Finalment, indiquem que els dos routers de la nostra xarxa, els quals subministren cadascun adreces de Gateway a dues subxarxes diferents, estan connectats entre si mitjançant un cable sèrie. És una connexió força particular, ja que un dels routers assumeix el rol de DCE, element de commutació, i l'altre, a l'altra banda del cable, fa el paper de DTE, dispositiu terminal, tot i que en realitat no ho sigui. L'equip DCE estableix el Clock Rate (56Kb/s, per exemple), i l'altre router l'assumeix.

## 2.2. Routing o encaminament a la xarxa

El procés d'enrutament o routing consisteix en cercar la millor ruta (o, a efectes pràctics, la ruta que sembla millor d'acord un conjunt limitat de mesures) per enviar un datagrama a un destí, i elaborar i mantenir taules d'enrutament on guardar informació que possibilite o simplement agilitzi aquest procés. Les decisions d'enrutament recauen sobre els routers, i s'ubiquen en la capa de xarxa del model OSI. Distingim entre els protocols d'enrutament, aquells que cerquen les rutes o camins, i els enruteables, com

IP, que permeten posar en circulació paquets gràcies a la inclusió de dades clau dels dispositius de la xarxa a la seva capçalera (concretament un sistema d'adreçament, com les adreces IP del protocol IP) que permeten als protocols d'enrutament encaminar els paquets a través de la xarxa.

En aquest treball hem experimentat amb dos sistemes de routing, el protocol RIP, per una banda, i, per l'altra, una taula estàtica seguint el criteri «Next hop»: un sistema en què, donada una adreça IP destí a la qual el router no està connectat directament, la vinculem a una adreça IP a la qual sí que està connectat, per tal que envii el paquet cap allà; el dispositiu amb aquesta adreça de «next hop» és doncs el següent salt o pas cap a on volem que s'enviïn les dades que arriben al router i que tenen un cert destí.

A continuació mostrem un sistema molt simple amb 2 routers, cadascun d'ells connectat amb dos ordinadors a través de switchos. Aquests routers estan connectats. Hem format un total de 3 xarxes diferents (en allunyem per un moment del sistema de subxarxes de l'«smart house» presentat abans); una xarxa correspon a cada conjunt ordinador-router (cada ordinador té configurada com a IP de gateway la IP del router al qual està connectat amb un switch, i té una IP de dispositiu que pertany a la seva xarxa, obviament), més una d'addicional per connectar els routers.

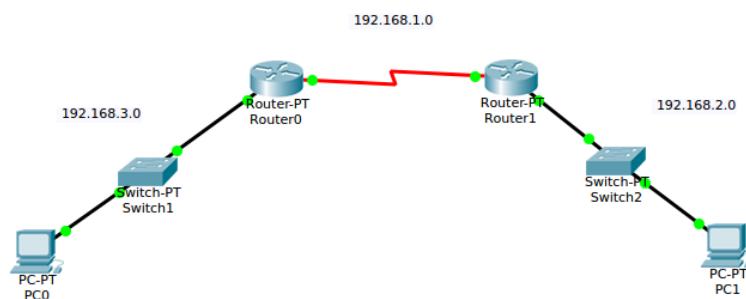


Figura 5: Dos ordinadors connectats a dos routers connectats entre si

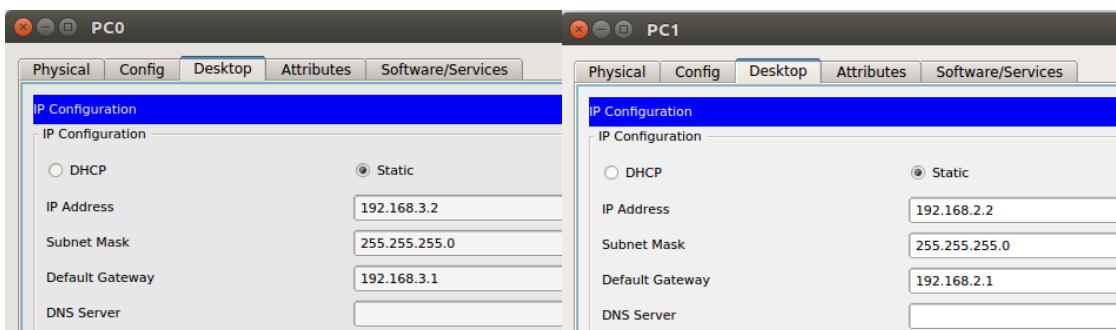


Figura 6: Configuració IP (estàtica) dels dos ordinadors, amb la seva IP de dispositiu, la màscara corresponent (és una IP de tipus C) i la IP del router com a Gateway

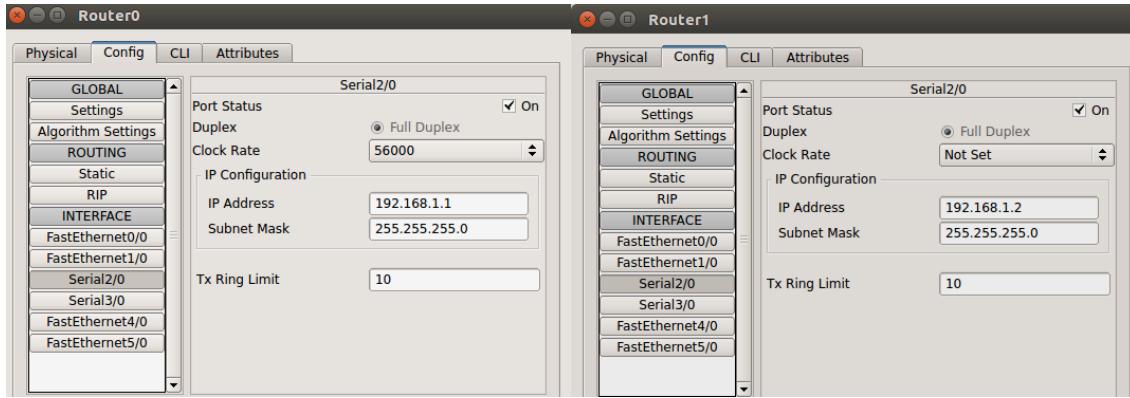


Figura 7: configuració de la interfície sèrie dels dos routers que els connecta; un actua com a DCE, fixant el clock rate, que l'altre assumeix, emulant un DTE; les seves IP pertanyen a una petita xarxa emprada per a connectar els routers

En aquest punt, el sistema muntat permet l'enviament d'informació de cada ordinador al seu router, però no anar més enllà. El procés que es produeix perquè un paquet arribi de l'ordinador al router és senzill: l'equip crea el paquet (per exemple un paquet ICMP, per esbrinar quin és l'estat de la xarxa, veure si funciona correctament) i el transmet al mitjà físic encapsulat dins d'una trama del protocol de capa d'enllaç Ethernet, fent-lo arribar al commutador, que simplement el fa arribar al router, l'única connexió que té a part de l'ordinador, la MAC del qual és coincident amb l'adreça MAC de la trama. En arribar al router, aquest, un cop ha extret del payload de la trama Ethernet el paquet, a nivell de capa de xarxa, veu a la capçalera IP que l'adreça de destí és la seva i es queda les dades, enviant una senyal de recepció a l'ordinador.

Si intentem fer arribar les dades no al router adjacent sinó al següent, aquell que està connectat amb l'adjacent, el missatge ja no arriba, ja que la taula de rutes del primer router és buida. És necessari configurar algun mecanisme, ja sigui més automàtic o més manual, perquè aquesta taula quedi estableguda i el router sàpiga com enrutar un cert paquet, quan miri la seva IP destí.

Per a aquest exemple senzill, hem escollit fer-ho amb el protocol d'enrutament RIPv1. Com es pot veure a la imatge inferior, hem indicat a la taula RIP quines són les adreces IP de xarxa a les quals el nostre router està connectat. Fent això per a cada router del nostre sistema de dos routers, els missatges ja podran arribar d'un ordinador a l'altre, situat cadascun en un extrem oposat del recorregut. Això és així perquè quan arriba el paquet al primer router analitzarà la seva taula RIP d'adreses, per a les quals, internament, ha calculat dades de distància per calcular camins eficients, el que es coneix com un mètode de «distance vector» o vector de distància (ho fa en base a nombre de salts a fer, quedant-se amb el recorregut que arriba al destí amb menys). Veu que té a la taula una adreça de xarxa coincident amb la de la IP destí, així que fa arribar el paquet a l'altre router, que veu que la IP destí pertany a la seva xarxa i correspon a un equip al seu abast, un ordinador, al qual fa arribar el paquet fent-lo passar pel commutador que els connecta.

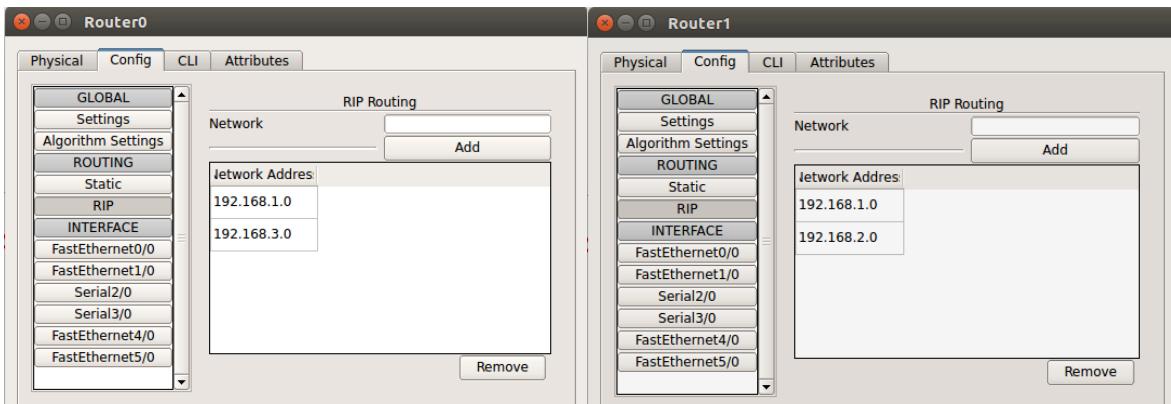


Figura 7: Configuració de les taules RIP de cada router, que contenen les adreces IP a què està connectat cada router, fent possible el trànsit de dades entre tots dos

El protocol RIP pot ser aplicar a subxarxes amb la versió RIPv2, però no és l'única metodologia possible per a definir les taules d'enrutament i els processos per escollir les millors rutes. Una altra possibilitat, que mostrem a continuació aplicada a les subxarxes de la nostra xarxa d'«smart house» consisteix en establir estàticament quin camí seguir si arriba al router una adreça que té per destí una certa xarxa o subxarxa: indiquem el següent salt a realitzar, també anomenat «next hop». Aquest esquema pot tenir sentit si per algun criteri concret volem imposar certes rutes fixes per al trànsit entre punts diferents de la xarxa; en general, en xarxes tan massives com pot ser Internet, però, aquesta configuració manual no es dóna, sinó que el routing recau en gran mesura en protocols com el RIP, i altres tècniques dinàmiques i impersonals per trobar rutes.

A la següent imatge es pot veure la configuració de taula d'enrutament estàtica que acabem d'explicar, que, de forma resumida, diu el següent: si al router connectat a les habitacions groga i taronja arriba informació que ha d'arribar al jardí o a l'habitació blava, el següent pas és el router de la dreta; si el router de la dreta rep dades que han d'arribar a l'habitació groga o taronja, farà servir el router esquerre com a següent node per on fer passar els paquets.

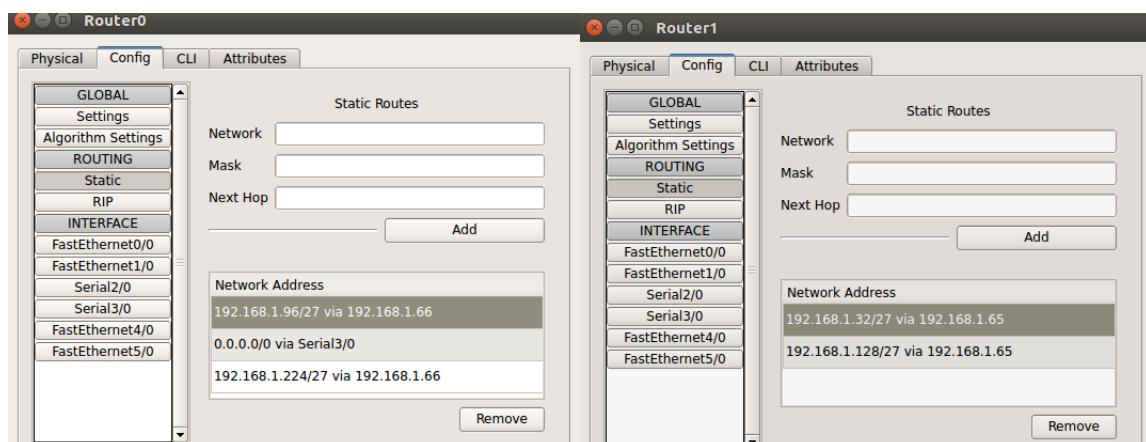


Figura 8: taula de rutes estàtiques dels dos routers de la xarxa de l'«smart house»; les fem servir per indicar el següent node per un paquet amb una certa adreça de xarxa destí

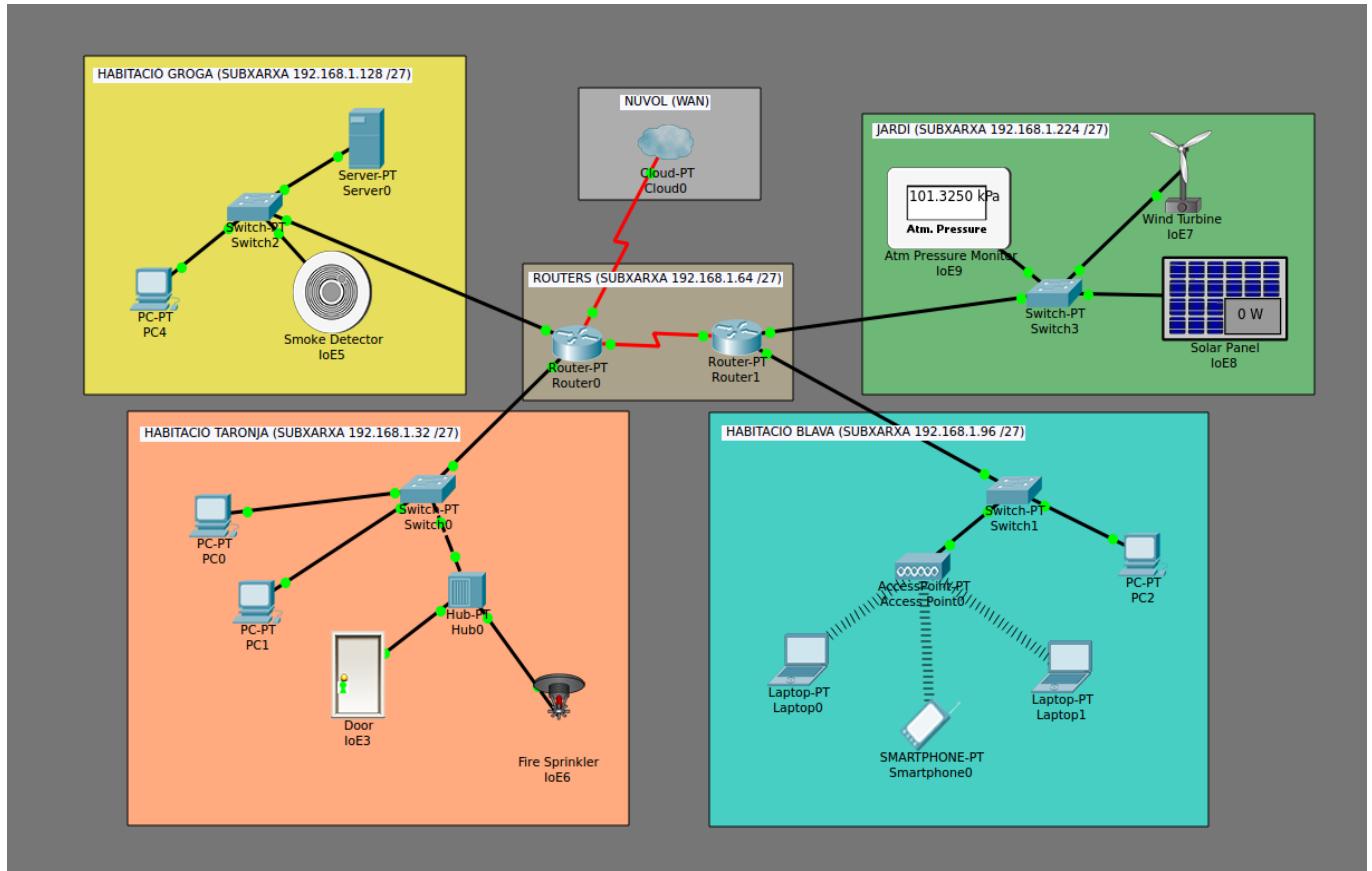


Figura 9: xarxa de l'«smart house», mostrada de nou per facilitar la comprensió de l'explicació de les taules estàtiques i les rutes que defineixen, feta al paràgraf anterior

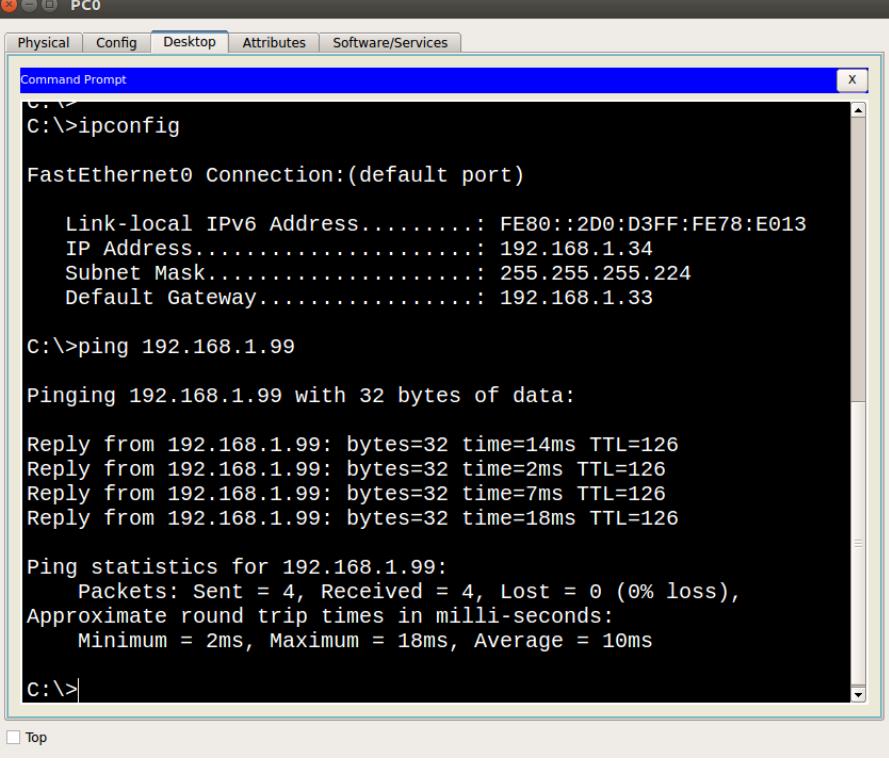
## 2.3. Anàlisi dels camins, el trànsit i l'encapsulament de les dades

A continuació veurem un seguit d'exemples pràctics on s'empren diferents protocols d'aplicació per fer arribar dades d'una zona a una altra de la xarxa, concretament a una subxarxa diferent de l'original; observarem i analitzarem el paper que juga cada element de la xarxa a través del camí que segueixen les dades, encapsulant i desencapsulant els missatges per adaptar-los al medi i a la forma de funcionar de cada sistema o protocol.

### 2.3.1. Exemple 1: Ping d'un ordinador de l'habitació taronja a un portàtil de l'habitació blava

Al següent exemple mostrarem el recorregut d'una PDU de Ping que viatja des d'un dels ordinadors de sobretaula de l'habitació taronja fins arribar a un portàtil de l'habitació blava, que la sobrescriu i retorna, perquè l'equip emissor sàpiga que és possible la comunicació amb el portàtil; al cap i a la fi aquest és l'objectiu d'un missatge Ping, determinar si és possible comunicar-se.

Primer de tot, mostrem com realitzar l'operació de Ping des de la consola de l'ordinador emissor, com vam fer a la primera pràctica de Xarxes.



```
C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address.....: FE80::2D0:D3FF:FE78:E013
    IP Address...................: 192.168.1.34
    Subnet Mask..................: 255.255.255.224
    Default Gateway............: 192.168.1.33

C:\>ping 192.168.1.99

Pinging 192.168.1.99 with 32 bytes of data:

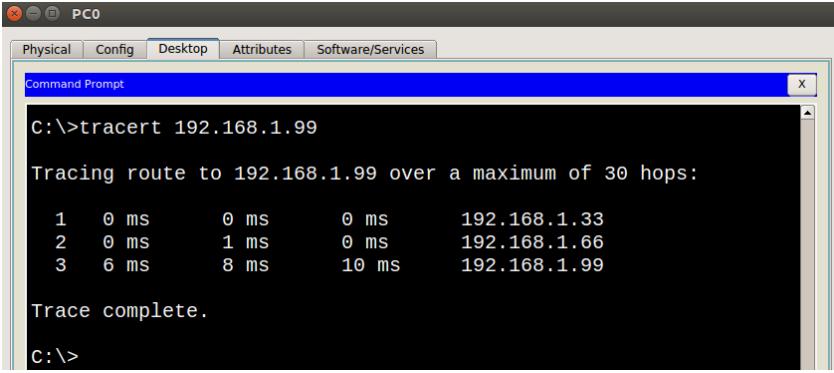
Reply from 192.168.1.99: bytes=32 time=14ms TTL=126
Reply from 192.168.1.99: bytes=32 time=2ms TTL=126
Reply from 192.168.1.99: bytes=32 time=7ms TTL=126
Reply from 192.168.1.99: bytes=32 time=18ms TTL=126

Ping statistics for 192.168.1.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 18ms, Average = 10ms

C:\>
```

Figura 10: Ping des de terminal

Seguidament, mostrem, com també vam aprendre a la primera pràctica, mitjançant la comanda «tracert», el recorregut que segueix la informació, el camí de les dades; no hi ha sorpreses: es visiten les tres subxarxes que cal travessar, la d'origen, corresponent a l'habitació taronja, la del compartiment dels routers, que és intermitja, i, darrerament, la de l'habitació blava, on s'ubica el portàtil destinatari de la informació.



```
C:\>
C:\>tracert 192.168.1.99

Tracing route to 192.168.1.99 over a maximum of 30 hops:
  1  0 ms       0 ms       0 ms      192.168.1.33
  2  0 ms       1 ms       0 ms      192.168.1.66
  3  6 ms       8 ms      10 ms      192.168.1.99

Trace complete.

C:\>
```

Figura 11: Tracert des de terminal per veure el recorregut de la informació

Ara analitzarem més a poc a poc tot el procés de comunicació, veient quin aspecte presenten les dades al seu pas per cada dispositiu.

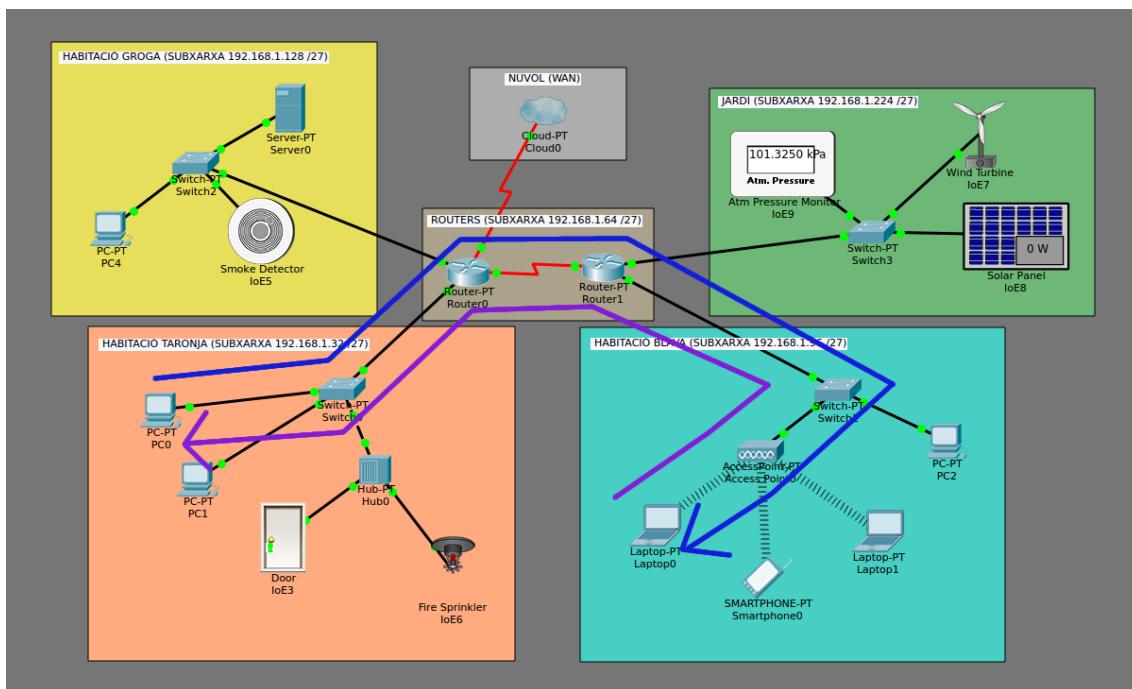


Figura 12: Recorregut del missatge Ping (en blau es representa l'anada, en porpra la tornada)

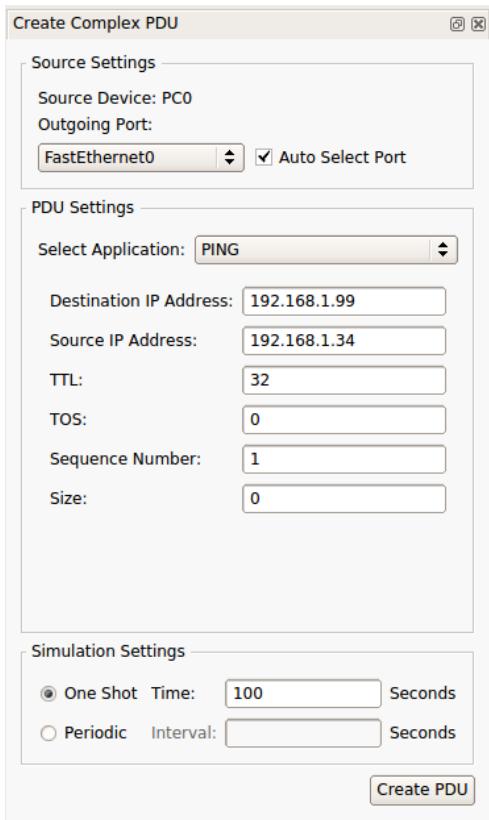


Figura 13: Configuració de la PDU de Ping a enviar

Com veurem tot seguit, Ping utilitza el protocol de xarxa ICMP (Internet Control Message Protocol). Aquest protocol s'ubica a la capa de xarxa, per sobre d'IP, però no substituint-lo: quan s'utilitza ICMP, se segueix utilitzant IP. Les funcions d'ICMP són les de diagnosi, notificació i control d'errors d'una xarxa. Té diferents codis que identifiquen situacions que es poden donar a una xarxa, com que el destí indicat a la capçalera IP sigui inaccessible, o que l'origen hagi deixat d'emetre inesperadament en mig d'una transmissió, per exemple. Al cas de Ping, s'utilitzen dos codis ICMP, com veurem, un per la petició de Ping (codi 8, subtipus 0: «Echo request»), que és el que envia l'emissor, i un per la resposta, contestada pel receptor i que ha d'arribar a l'emissor original (codi 0, subtipus 0: «Echo reply»).

El primer pas de la transmissió consisteix en l'elaboració, per part del procés de Ping executat a l'ordinador «PC0» de l'habitació taronja, del paquet ICMP d'«Echo request», que ve definit pel codi 8 i el subtipus 0 com veiem a la imatge inferior; també veiem que el paquet s'identifica amb un número de seqüència i s'utilitza el mètode Checksum per detectar possibles errors. Això té lloc a la capa de xarxa, en què també s'elabora, per sota d'ICMP, el datagrama IP a enviar, sent l'adreça origen la de l'ordinador emissor i la de destí la del portàtil receptor. En crear la PDU original hem fixat un TTL (Time To Live) de 32 unitats, xifra que indica el nombre de salts que el datagrama pot fer a través dels dispositius de la xarxa abans de considerar-se eliminable (cada node per on passi reduirà en 1 unitat aquest comptador, sempre i quan treballi en capa de xarxa; un hub o un switch no podran, un router sí). Veiem també que el datagrama conté unes dades de mida variable (en el cas que ens ocupa, un Ping no genera pràcticament res d'informació, així que aquesta secció de dades tindrà una mida petita: pràcticament tot el que cal informar queda dit amb el codi ICMP).

En analitzar l'adreça IP de destí, l'ordinador veu que no pertany a la seva subxarxa, així que l'enviarà en direcció a la porta de sortida o Gateway de la subxarxa, el router esquerre de la xarxa de l'«smart house», cosa que requerirà passar pel switch que hi ha al mig.

En quant a capa MAC, veiem que es fa servir el protocol Ethernet (IEEE 802.3) per transmetre: els camps més rellevants que podem veure són el preàmbul, que permet identificar la trama com d'Ethernet, així com les adreces MAC d'origen i destí (en aquest cas l'origen ja coneix la MAC del destí d'alguna transmissió anterior, altrament s'utilitzaria el protocol ARP per resoldre-la). És important destacar que la MAC destí de la trama Ethernet no és en cap cas la del portàtil destí del paquet ICMP, sinó el del següent dispositiu enrutador del sistema: el router Gateway de la subxarxa, com ja hem dit. Observem també el codi de redundància cíclica o FCS (Frame Check Sequence), utilitzat per detectar errors a nivell de capa MAC.

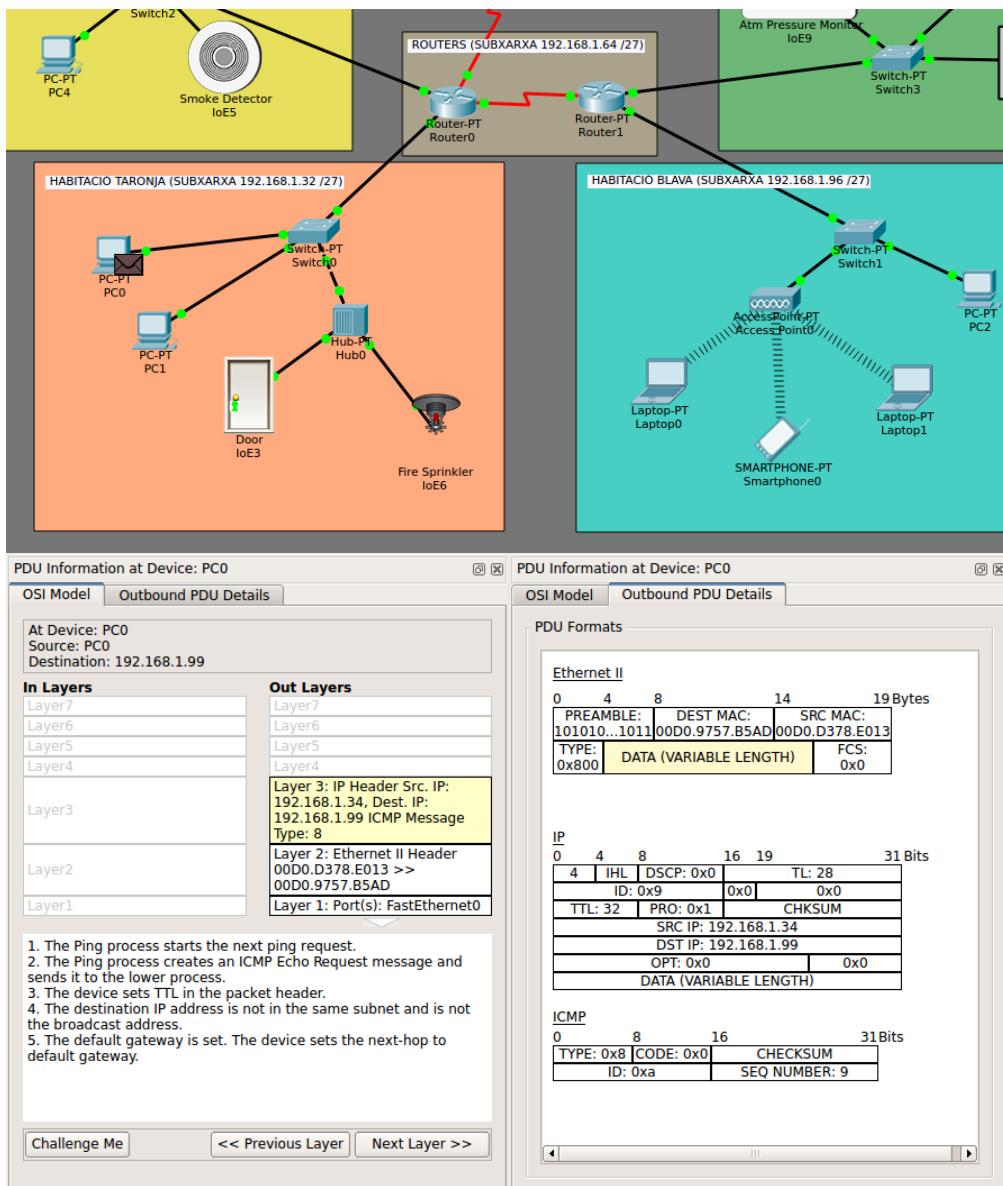


Figura 14: Primer pas del recorregut Ping

A continuació, l'ordinador envia la trama Ethernet, sent el cable d'Ethernet el mitjà físic que l'uneix amb el switch. El switch detecta que li ha arribat una trama MAC amb adreça MAC origen coneuguda a la seva taula d'adreses MAC: és la de l'ordinador emissor. Analitzant la trama detecta que la MAC destí correspon a l'interfície Ethernet del router amb què està directament connectat, així que commuta la trama cap al router.

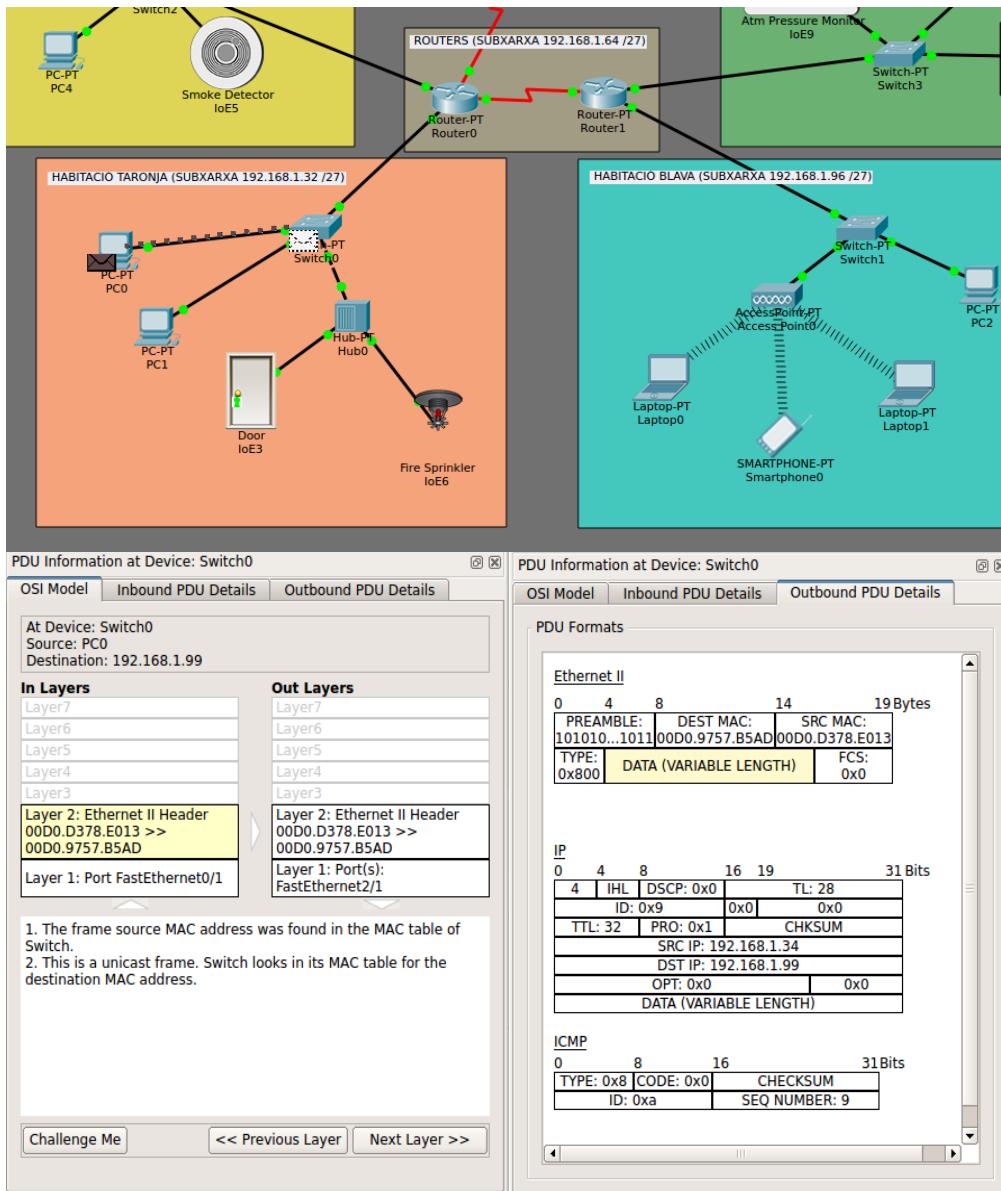


Figura 15: Segon pas del recorregut Ping

El router esquerre rep la trama Ethernet procedent del switch, i, a nivell d'enllaç, comprova que la MAC destí de la trama és la seva, de manera que accepta la trama. La PDU és desencapsulada al nivell de xarxa, descobrint-se la IP destí de les dades, que el router no troba directament a la seva taula CEF (Cisco Express Forwarding, una tecnologia propietat de Cisco que agilitza les comunicacions a nivell de capa 3), però sí que troba la IP de la subxarxa de l'IP destí a la taula d'enrutament, que indica que la següent parada de les dades ha ser el router de la dreta. Així, el router de l'esquerra disminueix en 1 unitat el temps de vida (TTL) del datagrama IP i encapsula les dades en una trama HDLC per a la seva transmissió cap al router dret; mirant la trama HDLC veiem les seves característiques banderes d'inici i final, l'adreça HDLC destinatària, el camp de control (que sent totalment nul, 0x0, indica que és una trama d'informació, altrament almenys un bit seria 1), així com el camp de dades i el FCS.

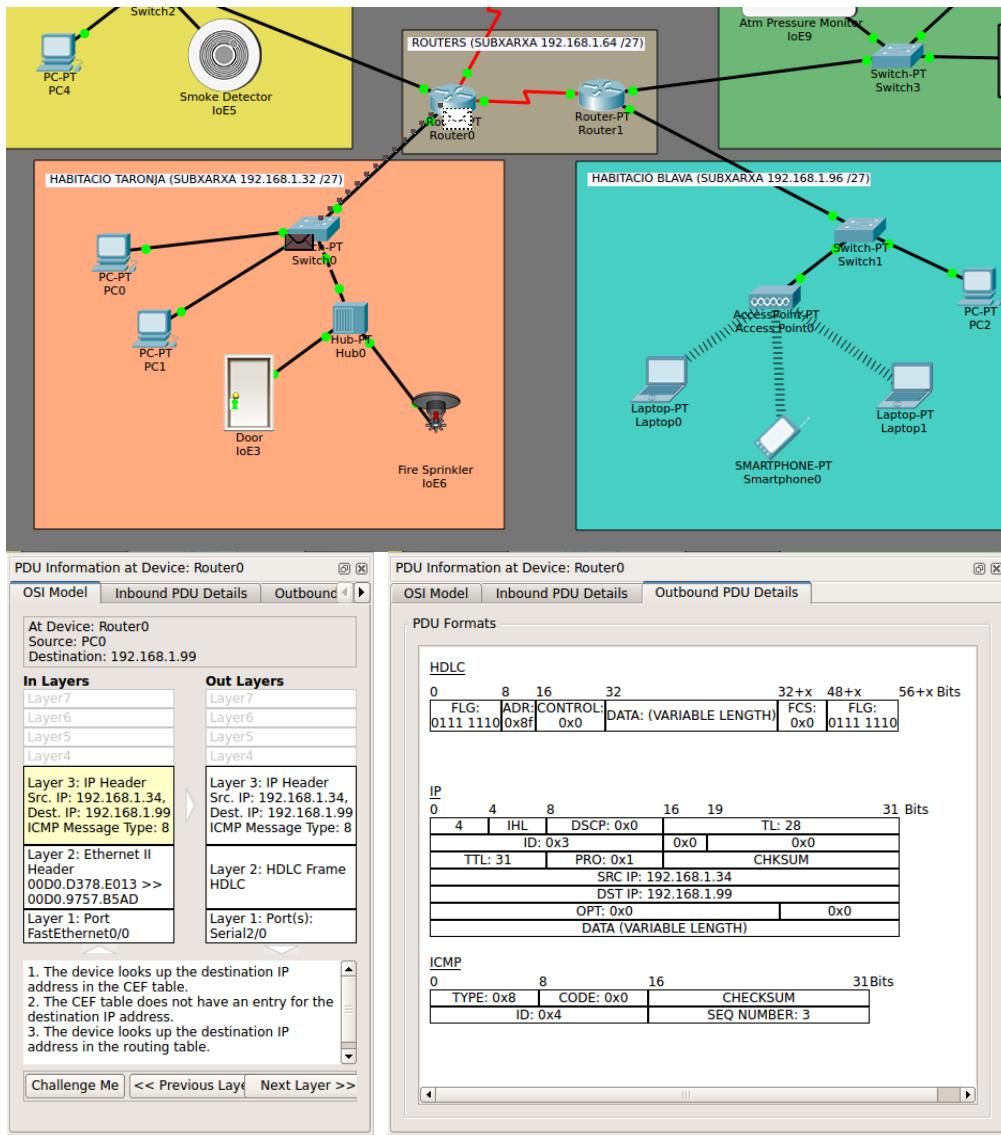


Figura 16: Tercer pas del recorregut Ping

El router de la dreta rep la trama HDLC i desencapsula el payload, passant-lo a la capa de xarxa. El router troba una referència a la IP destí del datagrama IP a la seva taula CEF: es tracta d'un dispositiu de la seva subxarxa. En conseqüència, decrementa el TTL i ho encapsula com una trama Ethernet amb la seva adreça MAC com a origen i sent la MAC destí la MAC del portàtil destí de les dades, que la sap gràcies a la taula d'adjacència a nivell d'enllaç. La trama Ethernet s'envia al switch que connecta amb el dispositiu destí.

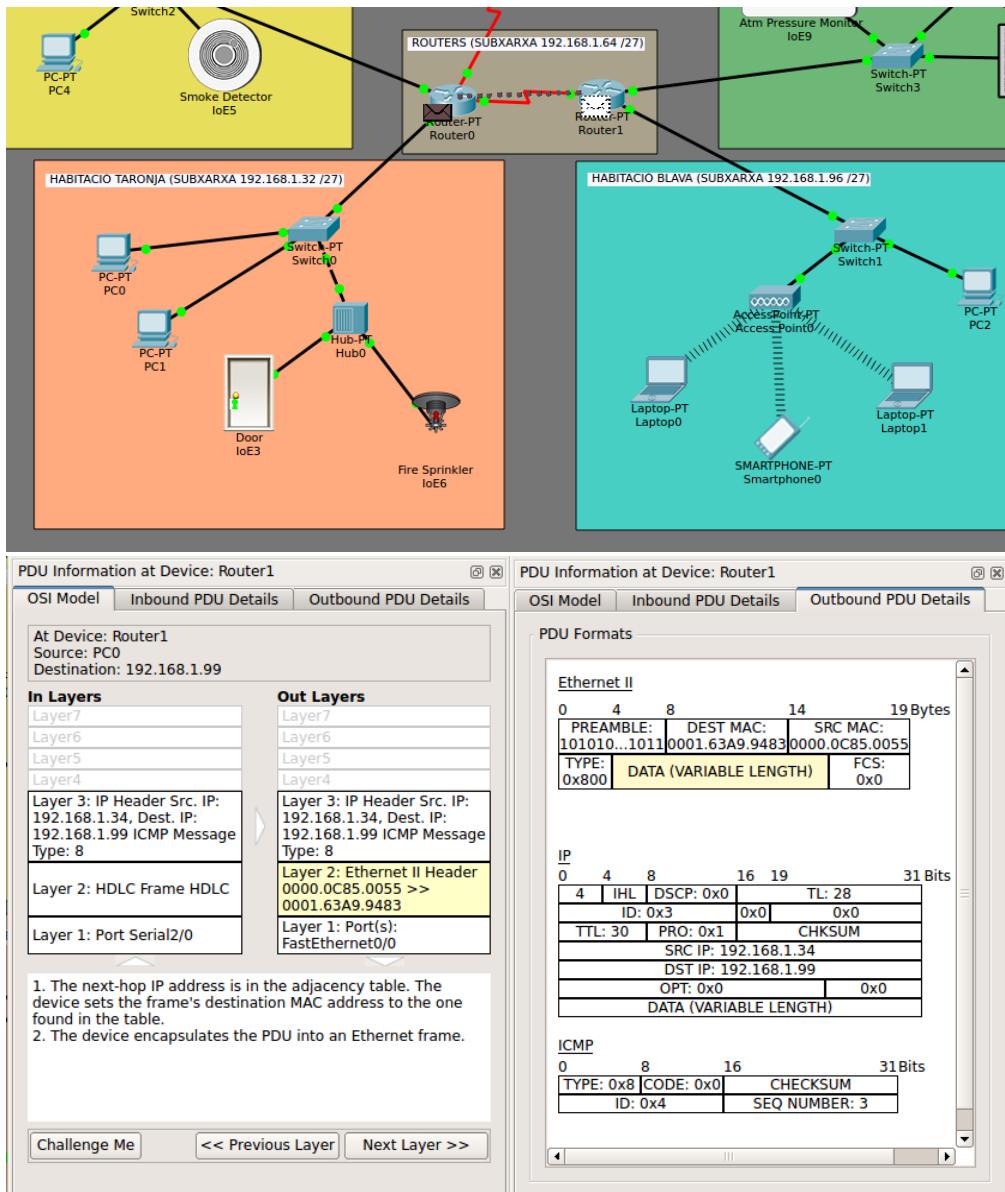


Figura 17: Quart pas del recorregut Ping

El switch veu a nivell MAC que la MAC d'origen de la trama correspon amb un dels dispositius amb què està connectat (el router de la dreta), i que el dispositiu de la MAC destí pot ser accedit a través del punt d'accés inalàmbric, així que envia la seqüència de bits de capa física al punt d'accés.

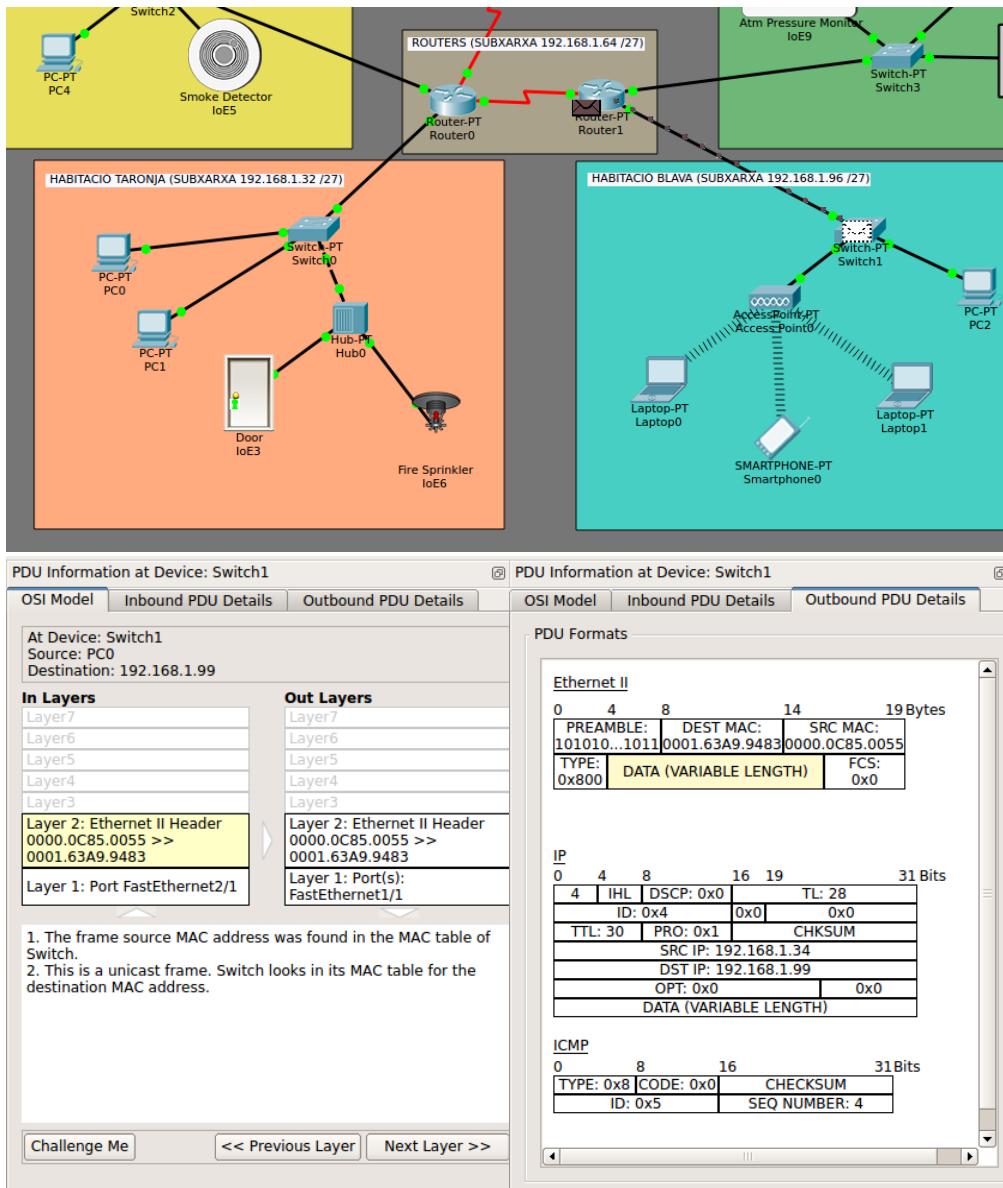


Figura 18: Cinquè pas del recorregut Ping

A continuació el punt d'accés rep la seqüència de bits a través del mitjà físic: el punt d'accés és, precisament, un dispositiu que treballa bàsicament sobre la capa física, si bé genera una trama destinada a enllaços wireless, i el podem entendre com un hub inalàmbric, ja que envia per l'aire les dades, de forma que tots els dispositius connectats per wireless al punt d'accés les rebran; ho constarem mirant la trama wireless, que incorpora les adreces dels dos portàtils i l'smartphone, tots els dispositius connectats al punt d'accés. Dins de les dades d'aquest encapsulat per wireless trobem el paquet ICMP.

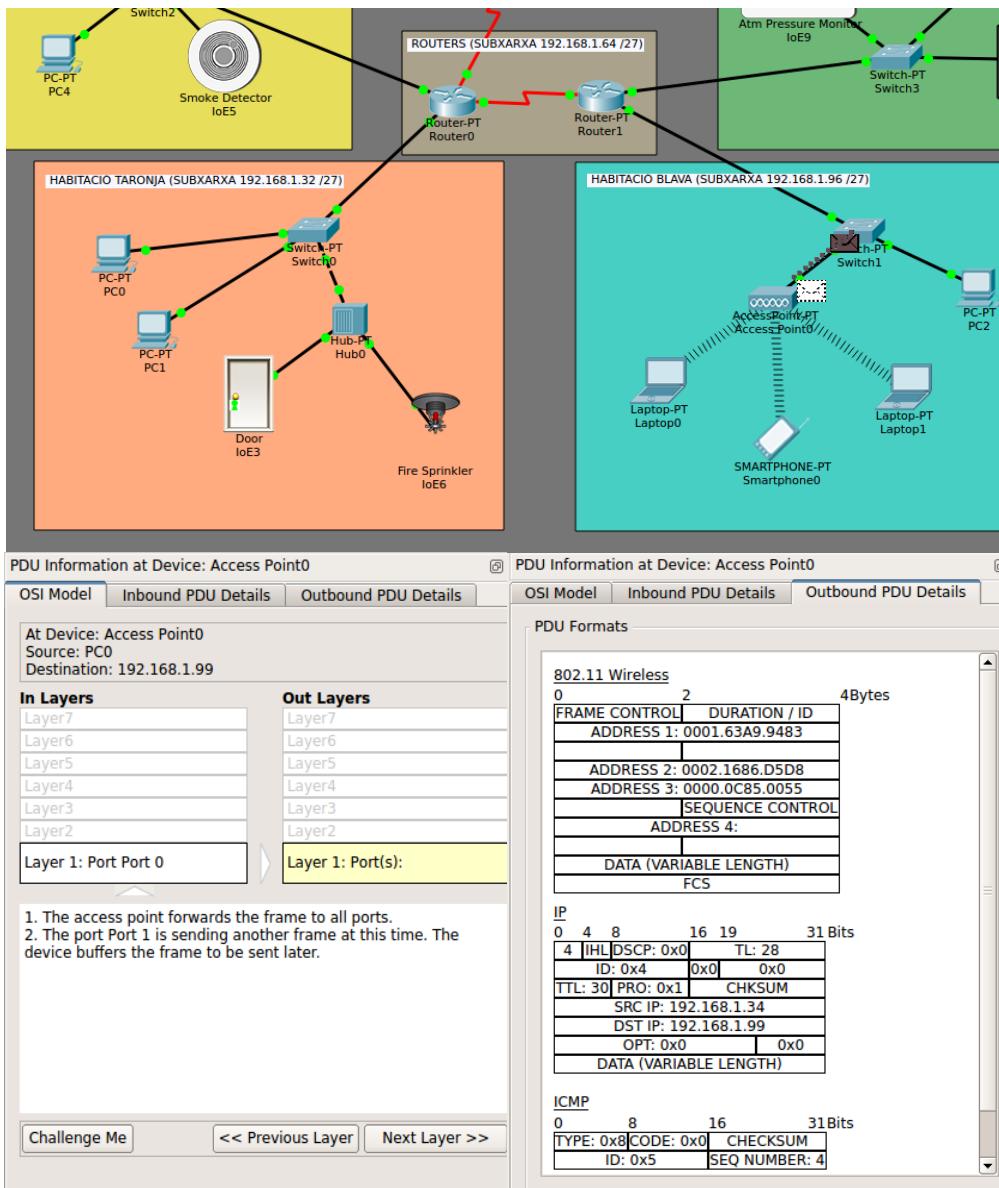


Figura 19: Sisè pas del recorregut Ping

Tots els dispositius connectats per wireless al punt d'accés reben la trama; l'smarhpone i un dels portàtils la descarten en comprovar que la MAC destí no és la seva, mentre que el portàtil restant sí que detecta que és la seva, i desencapsula la trama passant les dades al nivell IP, on es constata que la IP destí del paquet és la del dispositiu. Es veu que el paquet és un ICMP de codi «Echo request», per tant, implica que s'ha de respondre, de manera que es canvia el camps de codi i subtípus d'ICMP a 0 i 0, respectivament, convertint el paquet en una resposta de ping, és a dir, en un «Echo reply». Al datagrama IP es reseteja el TTL (al valor per defecte 128) i s'inverteixen les IP d'origen i destí, ja que ara s'ha de realitzar el camí invers.

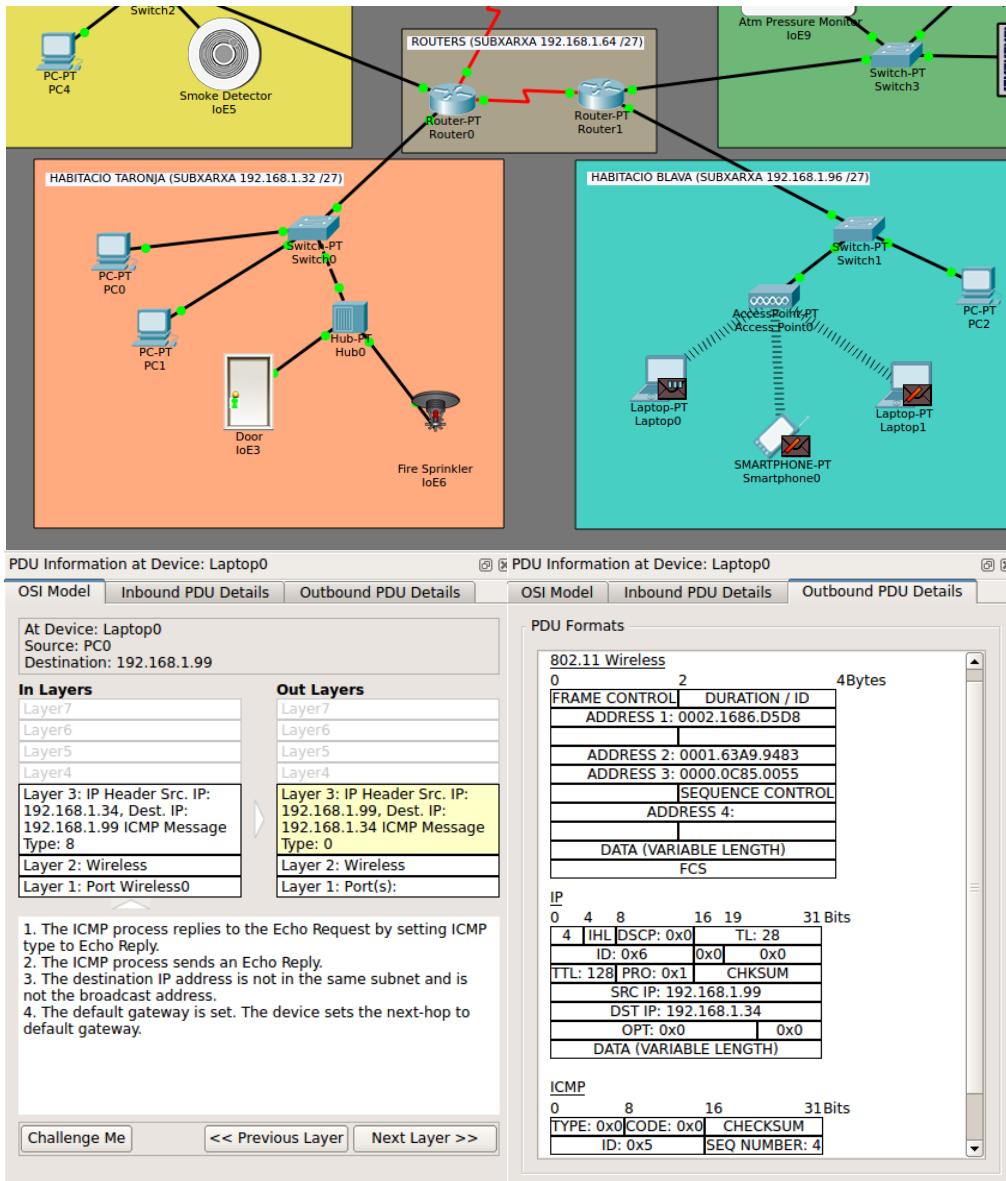


Figura 20: Setè pas del recorregut Ping

Es detecta que la nova IP destí, que no és altre que la de l'ordinador que va iniciar el ping, el de l'habitació taronja, no pertany a la subxarxa del portàtil, de forma que cal fer sortir el paquet pel gateway de la subxarxa, és a dir, cal enviar-la al router, de manera que s'encapsula la trama com una trama wireless, partint de l'estructura de la rebuda del punt d'accés, perquè pugui tornar al punt d'accés, que eventualment l'enviarà de tornada al router dret, que veurà a la taula d'enrutament que la IP destí del datagrama apareix a la seva taula d'enrutament i que cal adreçar-la cap al router de l'esquerra, que té el dispositiu destí sota la seva subxarxa i farà arribar el paquet a l'ordinador de l'habitació taronja a través del switch. Com tot aquest procés de tornada del paquet és molt similar al que ja hem vist al recorregut d'anada, ens limitem a mostrar les imatges del recorregut, però no ha explicar-lo, ja que és el mateix que abans només que en sentit invers.

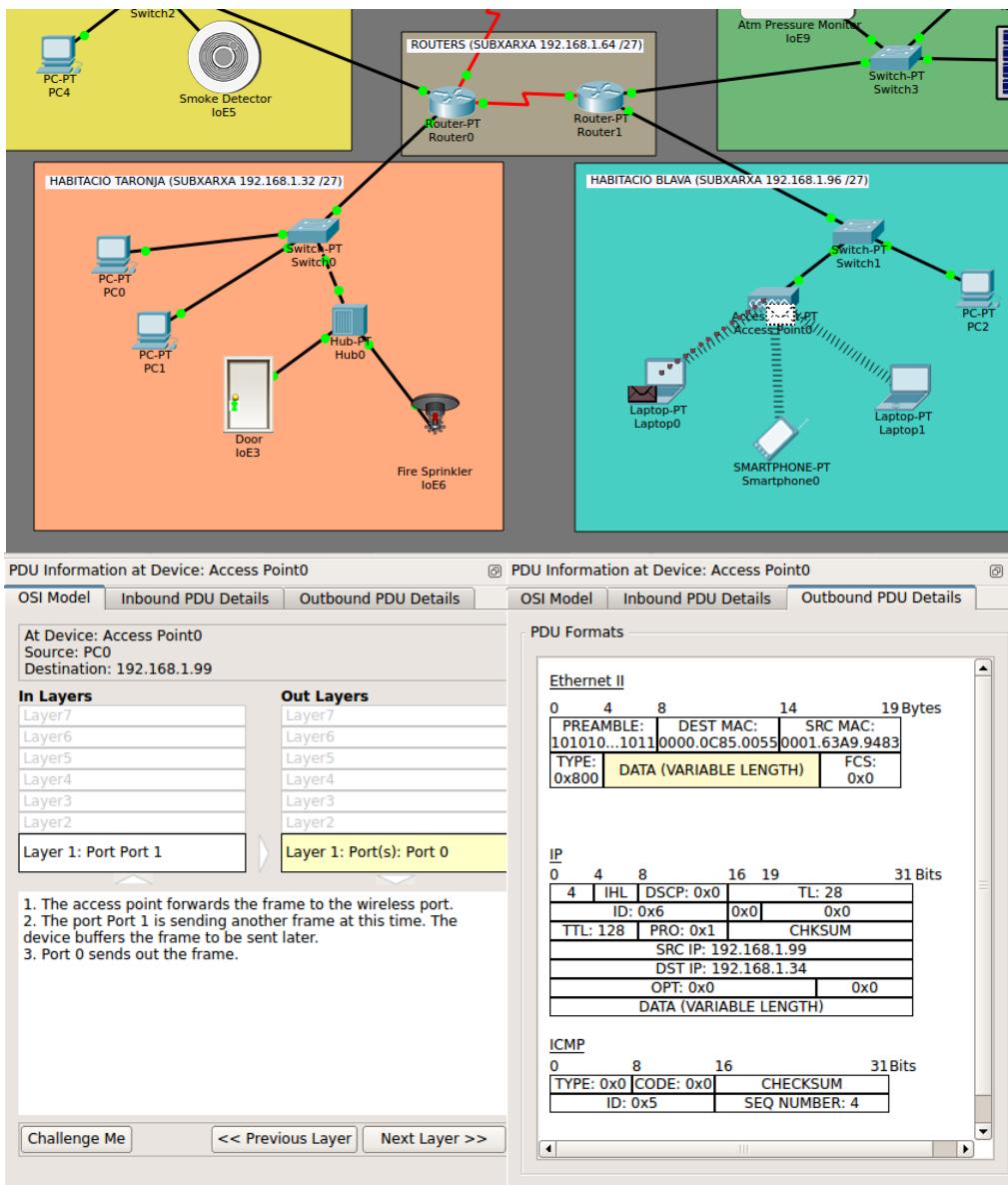


Figura 21: Vuitè pas del recorregut Ping

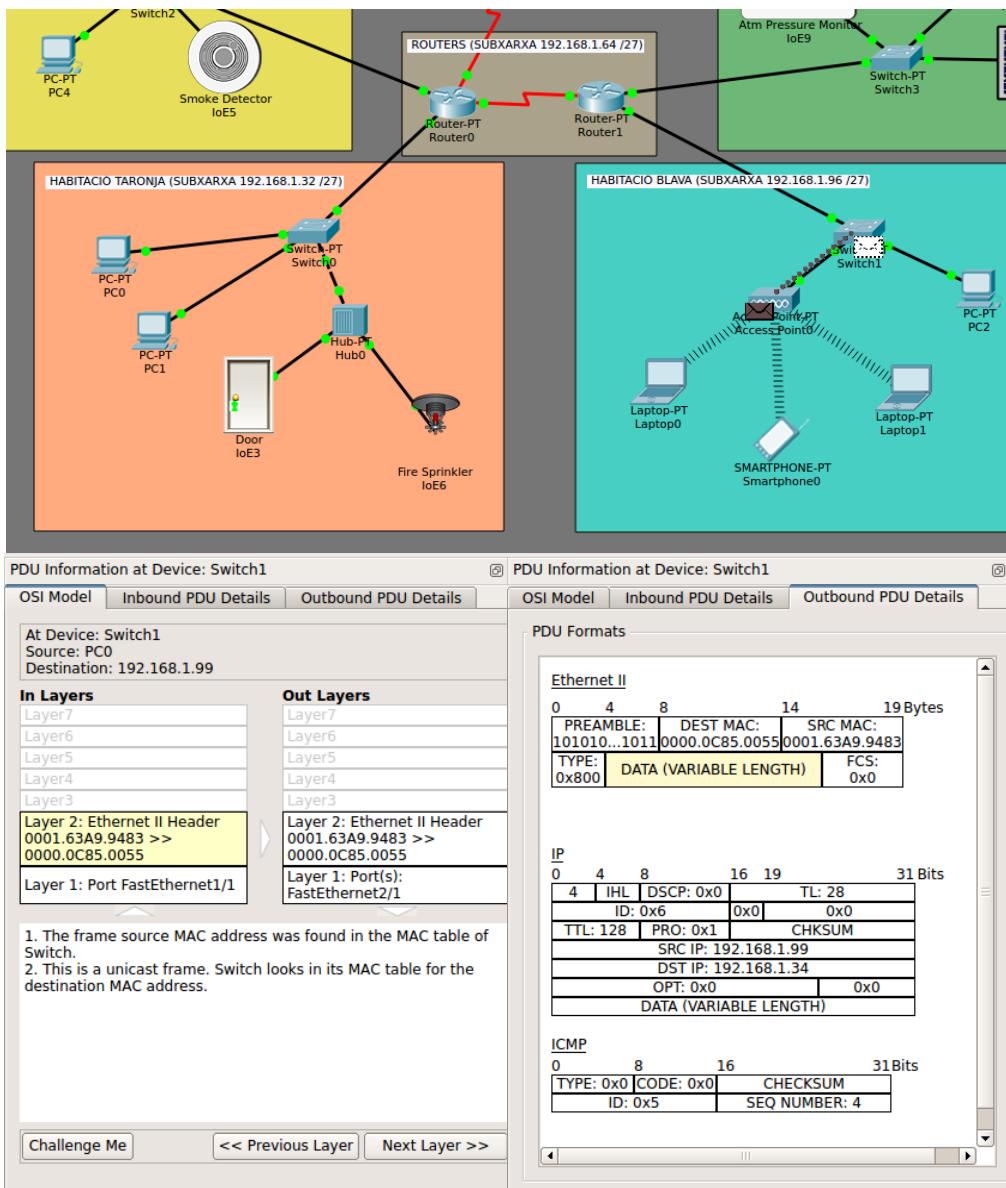
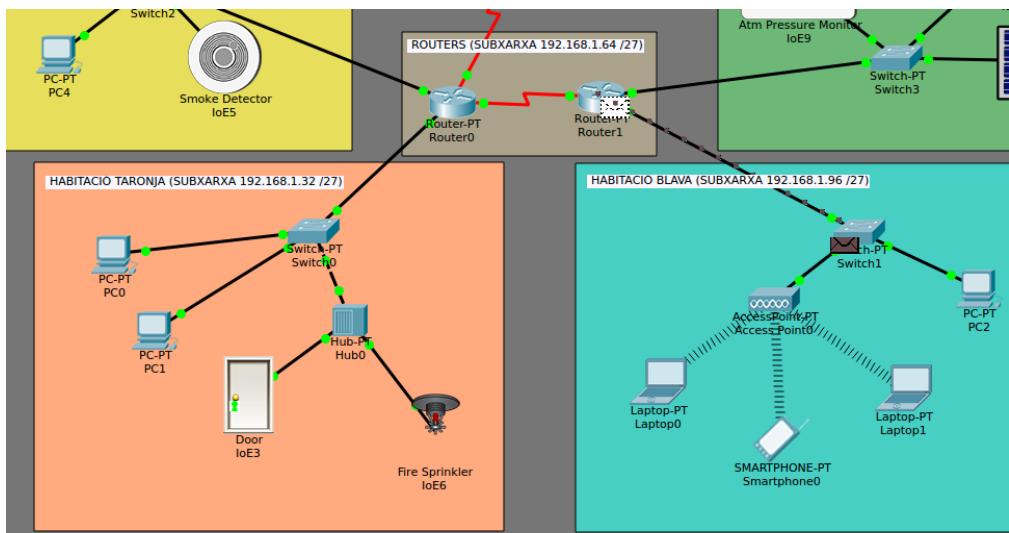


Figura 22: Novè pas del recorregut Ping



**PDU Information at Device: Router1**

OSI Model	Inbound PDU Details	Outbound PDU Details
At Device: Router1 Source: PC0 Destination: 192.168.1.99		
<b>In Layers</b>	<b>Out Layers</b>	
Layer7	Layer7	
Layer6	Layer6	
Layer5	Layer5	
Layer4	Layer4	
Layer 3: IP Header Src. IP: 192.168.1.99, Dest. IP: 192.168.1.34 ICMP Message Type: 0	Layer 3: IP Header Src. IP: 192.168.1.99, Dest. IP: 192.168.1.34 ICMP Message Type: 0	
Layer 2: Ethernet II Header 0001.63A9.9483 >> 0000.0C85.0055	Layer 2: HDLC Frame HDLC	
Layer 1: Port FastEthernet0/0	Layer 1: Port(s): Serial2/0	

1. The device looks up the destination IP address in the CEF table.  
 2. The CEF table does not have an entry for the destination IP address.  
 3. The device looks up the destination IP address in the routing table.

**PDU Formats**

**HDLC**

0	8	16	32	32+x	48+x	5
FLG: 0111 1110	ADR: 0x8f	CONTROL: 0x0	DATA: (VARIABLE LENGTH)	FCS: 0111 1110	FLG:	

**IP**

0	4	8	16	19	31
4	IHL	DSCP: 0x0	TL: 28		
	ID: 0x6	0x0	0x0		
TTL: 127	PRO: 0x1		CHKSUM		
	SRC IP: 192.168.1.99				
	DST IP: 192.168.1.34				
	OPT: 0x0		0x0		
	DATA (VARIABLE LENGTH)				

**ICMP**

0	8	16	31 Bits
TYPE: 0x0	CODE: 0x0	CHECKSUM	
ID: 0x5		SEQ NUMBER: 4	

Figura 23: Desè pas del recorregut Ping

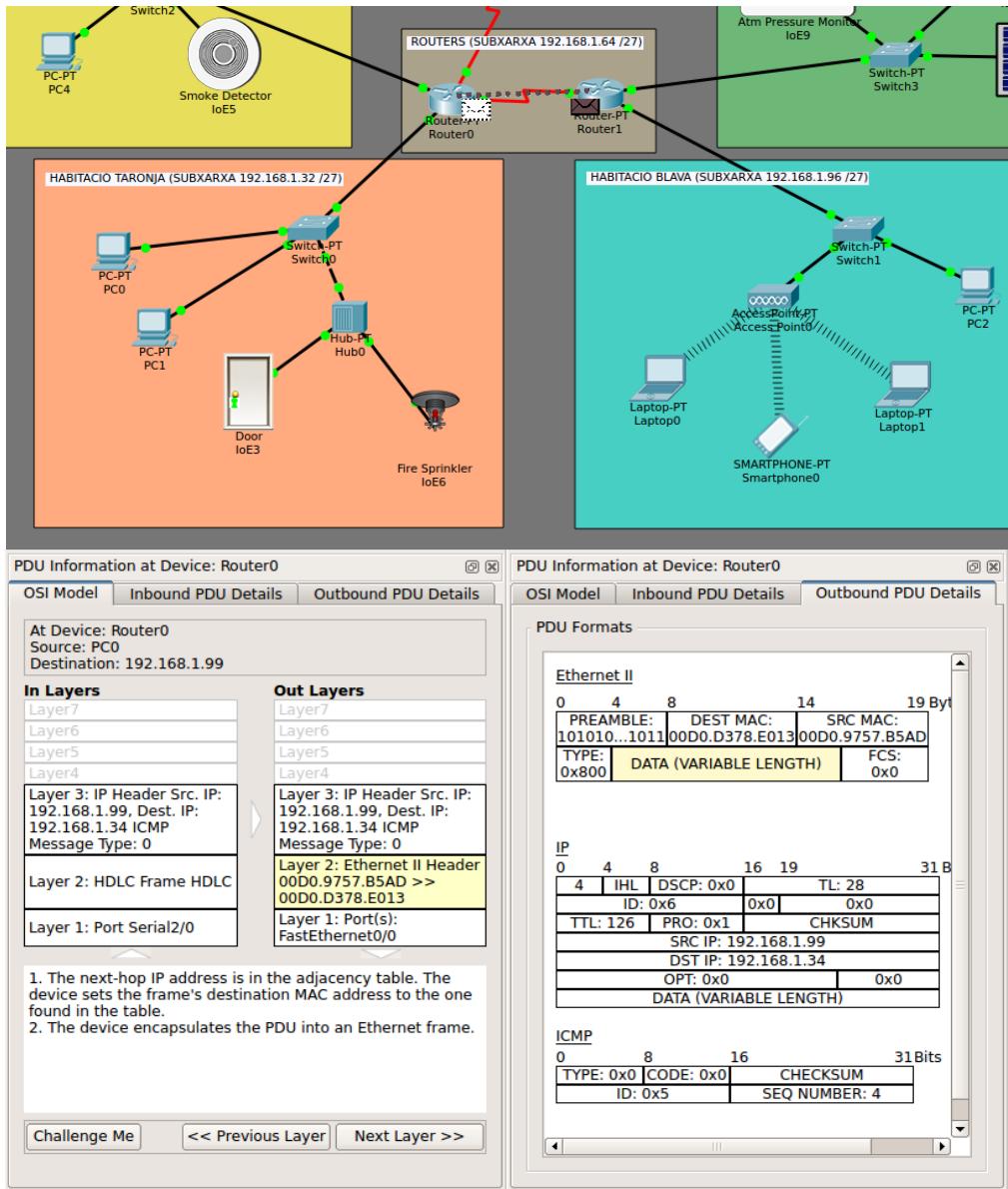


Figura 24: Onzè pas del recorregut Ping

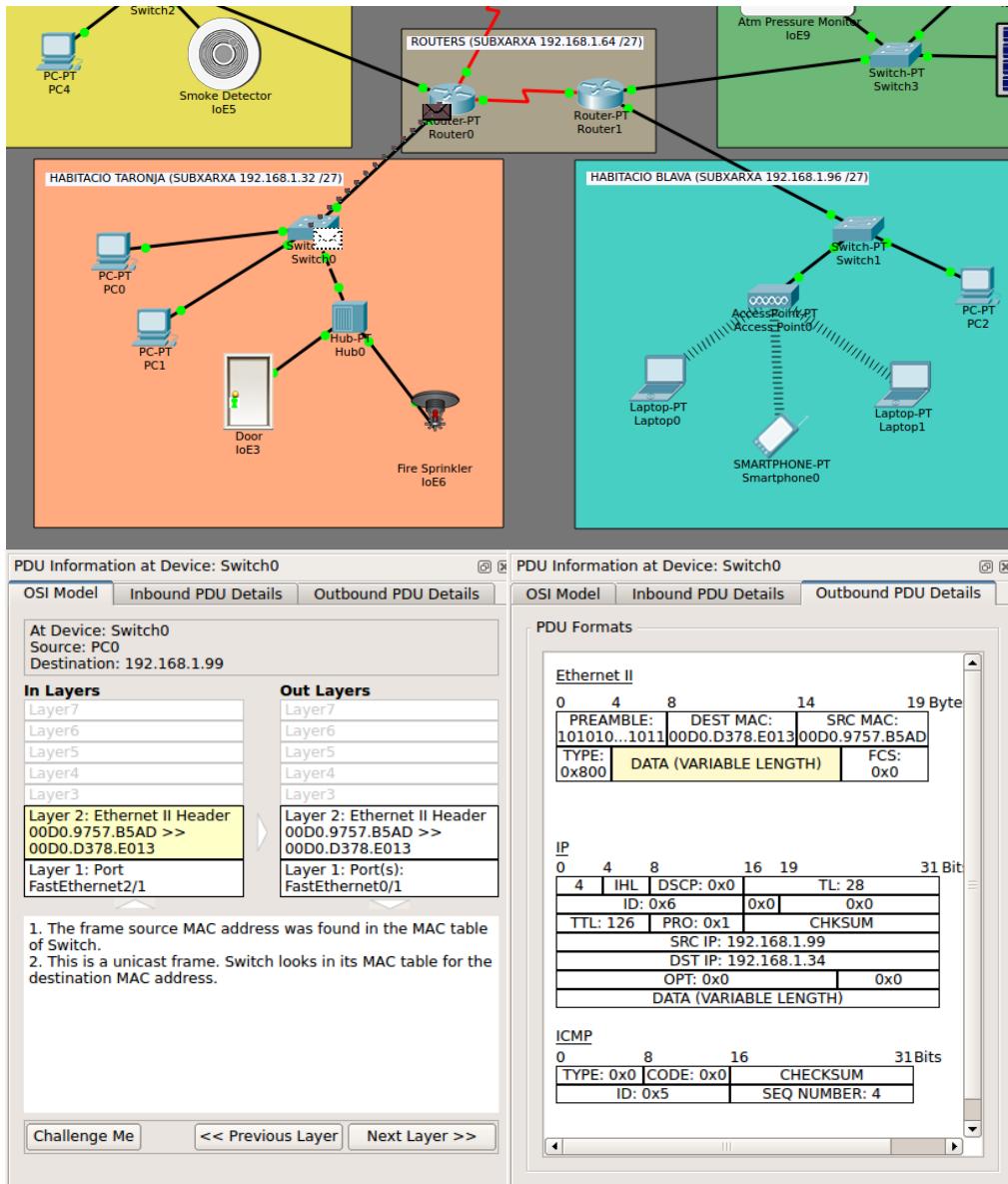


Figura 25: Dotzè pas del recorregut Ping

Finalment, arriba una trama Ethernet a l'ordinador de l'habitació taronja, que té per MAC destí la MAC d'aquest ordinador, que per tant desencapsula la trama i obté un paquet ICMP, que s'entrega al procés ICMP creat per l'ordinador, que retorna al procés de capa d'aplicació, el procés ping creat a terminal, les dades de la resposta rebuda del portàtil al que s'havia enviat el ping. Aquestes dades són les que es mostren per pantalla si fem servir l'aplicació ping des del terminal.

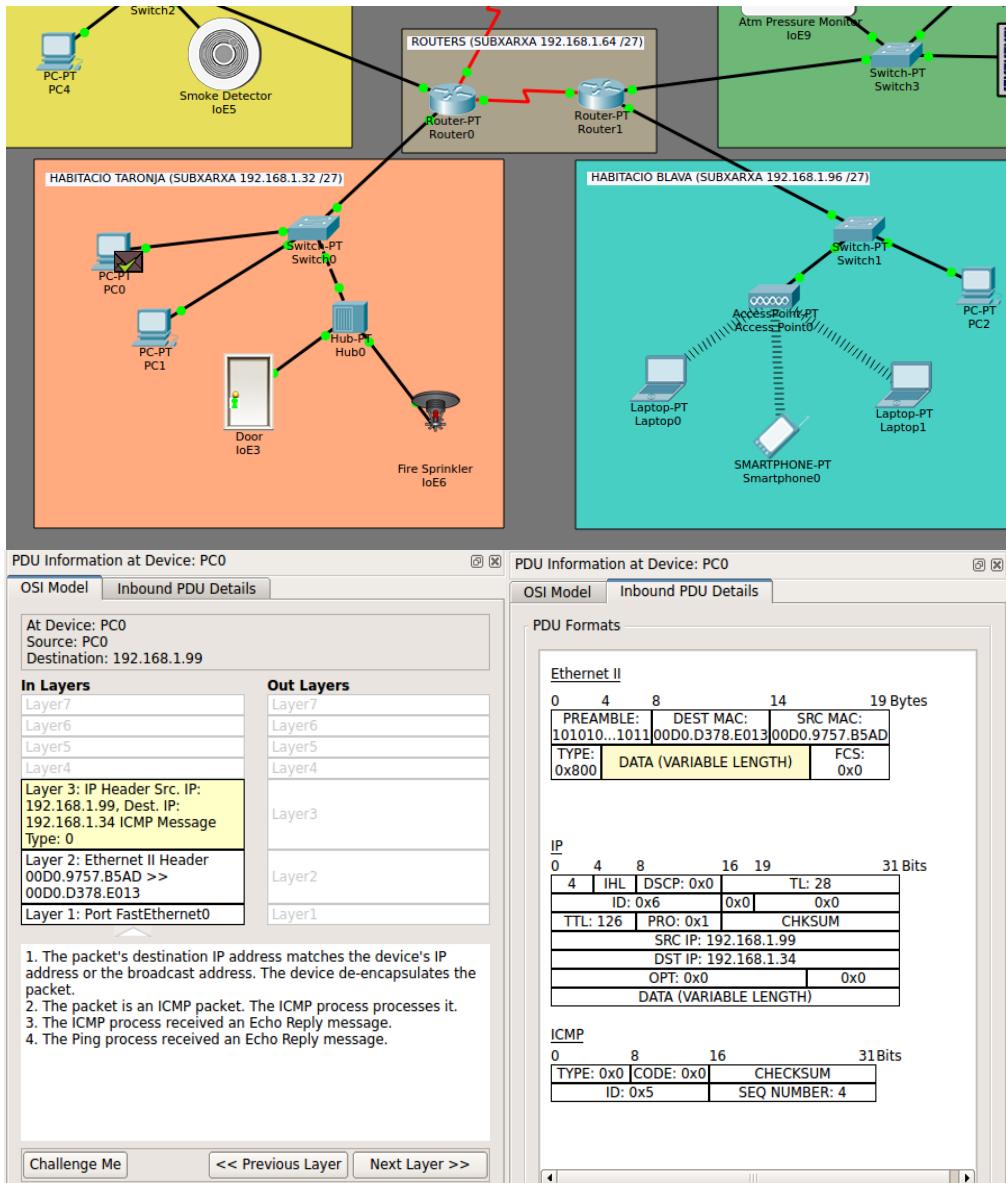


Figura 26: Tretzè i darrer pas del recorregut Ping

### 2.3.2. Exemple 2: Enviament d'un correu electrònic amb SMTP mitjançant el servidor de l'habitació groga

A continuació configurem els dos ordinadors de l'habitació groga perquè es comuniquin. Aquesta comunicació consisteix en un correu electrònic enviat des del primer equip al segon, amb la intermediació del servidor de l'habitació, que ofereix un domini; s'opera amb el protocol d'aplicació SMTP (Simple Mail Transfer Protocol), que utilitza TCP a la capa de transport per garantir la seguretat i la fiabilitat de la transmissió, així com IP a nivell de xarxa.

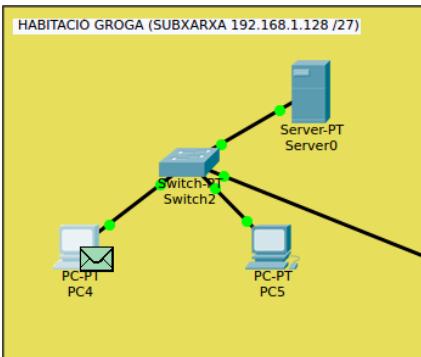


Figura 27: L'habitació groga

Per fer possible la comunicació per correu electrònic, activem el servei SMTP al servidor, i hi introduïm un domini, «xarxes.com», i afegim dos usuaris, «pc4» i «pc5», els dos ordinadors de l'habitació groga, amb «1» com a contrasenya per a tots dos. A cada ordinador, configurem l'usuari de correu com «pc4» i «pc5» respectivament, amb la contrasenya indicada, indicant l'adreça IP del servidor i l'aspecte de la direcció de correu: tindrem [«pc4@xarxes.com»](mailto:pc4@xarxes.com) i [«pc5@xarxes.com»](mailto:pc5@xarxes.com). Indiquem que aquest domini, «xarxes.com» podria ser un domini existent a Internet, però això no obstaculitzarà en cap cas el simulador.

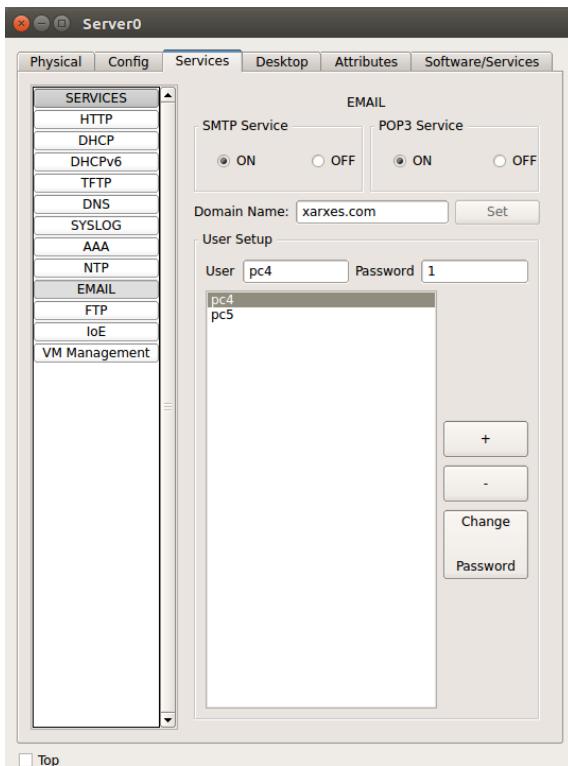


Figura 28: configuració del servidor per poder operar amb emails

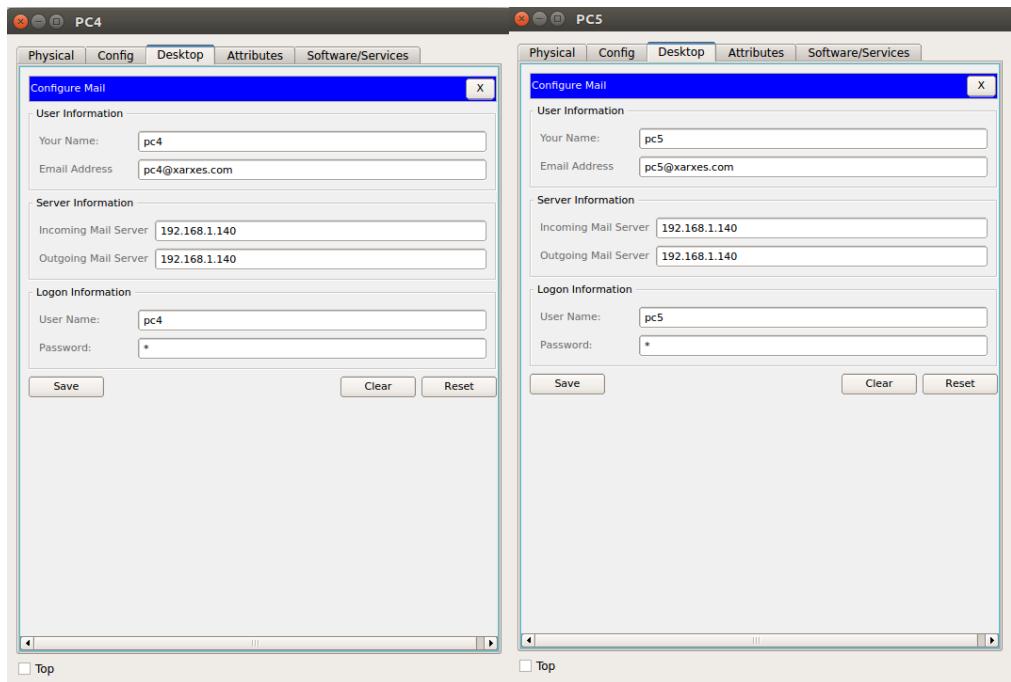


Figura 29: configuració dels ordinadors per poder operar amb emails

Ara que ja està tot configurat, podem enviar un correu. Des de l'aplicació de correu electrònic d'un dels ordinadors enviem un correu a l'altre, que és capaç de rebre'l amb èxit com mostren les imatges següents.

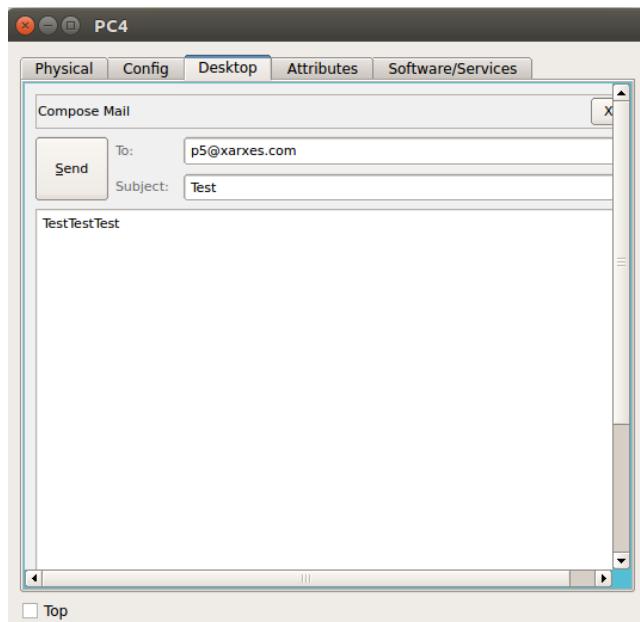


Figura 30: Un dels ordinadors, «pc4», envia un correu dirigit a l'altre, «pc5»

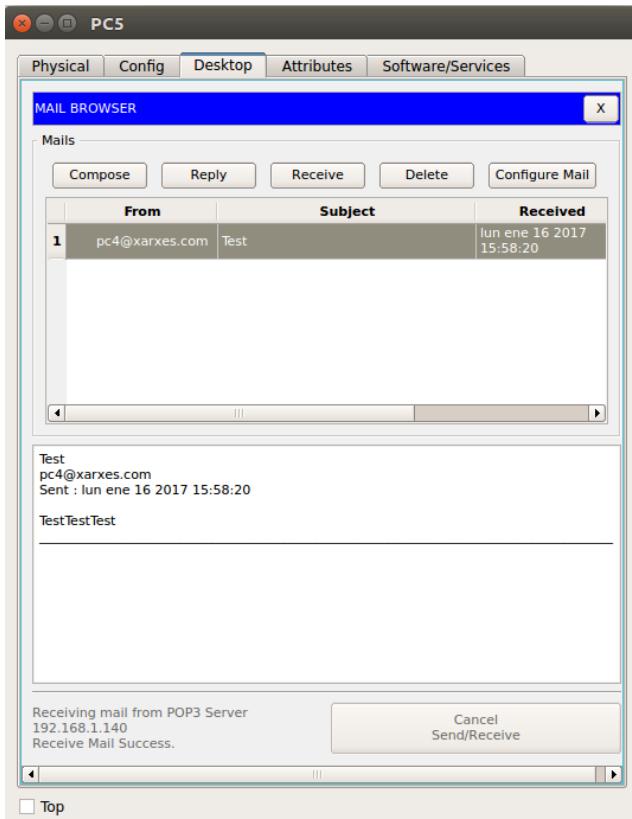


Figura 31: l'ordinador receptor, «pc5», rep l'email de «pc4» gràcies al servei POP3 del servidor (similar a SMTP, també dedicat a gestionar la transferència de correus electrònics)

A continuació analitzem el tràfic que es genera a la xarxa quan un ordinador envia un correu: veurem el recorregut de les dades i l'encapsulació en PDUs de diferents nivells. Comencem per indicar que el correu s'envia al servidor, no directament a l'altre ordinador; l'altre ordinador, podria, més endavant, consultar la seva safata d'entrada, que no és altra cosa que preguntar al servidor si hi ha algun correu per a ell, i, en cas afirmatiu, poder-lo rebre. Veurem doncs com l'ordinador «PC4» envia un correu per a «PC5» que es guardarà al servidor, que té el domini.

El primer pas consisteix en l'obertura de la connexió a l'ordinador origen. Com es vol fer servir SMTP, el segment de TCP queda configurat amb port destí 25, ja que per conveni aquest número de port està reservat per a connexions SMTP. El port d'entrada obert a la màquina origen és el 1025, un dels destriables per a transmissions sortints. L'adreça IP destí és la del servidor de correu electrònic de l'habitació groga, per tant 192.168.1.140. Per iniciar la comunicació, i pel fet que TCP treballa extrem a extrem, caldrà que l'extrem destí accepti la transmissió amb l'origen: per indicar que es vol iniciar aquesta comunicació, el flag de control SYN es posa a 1 al segment TCP a enviar; es fixa una mida de finestra, una mida màxima de segment i s'inicialitzen a 0 els nombres de seqüència i ACK que permetran controlar la correcta i ordenada transmissió de les dades. La PDU de transport s'encapsula dins del camp de dades d'un datagrama IP a la capa de xarxa; podem veure que la IP destí pertany a la subxarxa actual, ja que l'ordinador

i el servidor estan, tots dos, a la subxarxa de l'habitació groga. Per tant, el següent salt de la informació serà el propi destí, passant, això sí, a través del switch. S'encapsula la PDU de xarxa com a payload de la trama Ethernet a la capa MAC, on es posa com a MAC origen la de l'ordinador emissor i com a destí la del servidor, que ja es coneix (sinó, caldria resoldre-la amb el protocol ARP, Adress Resolution Protocol).

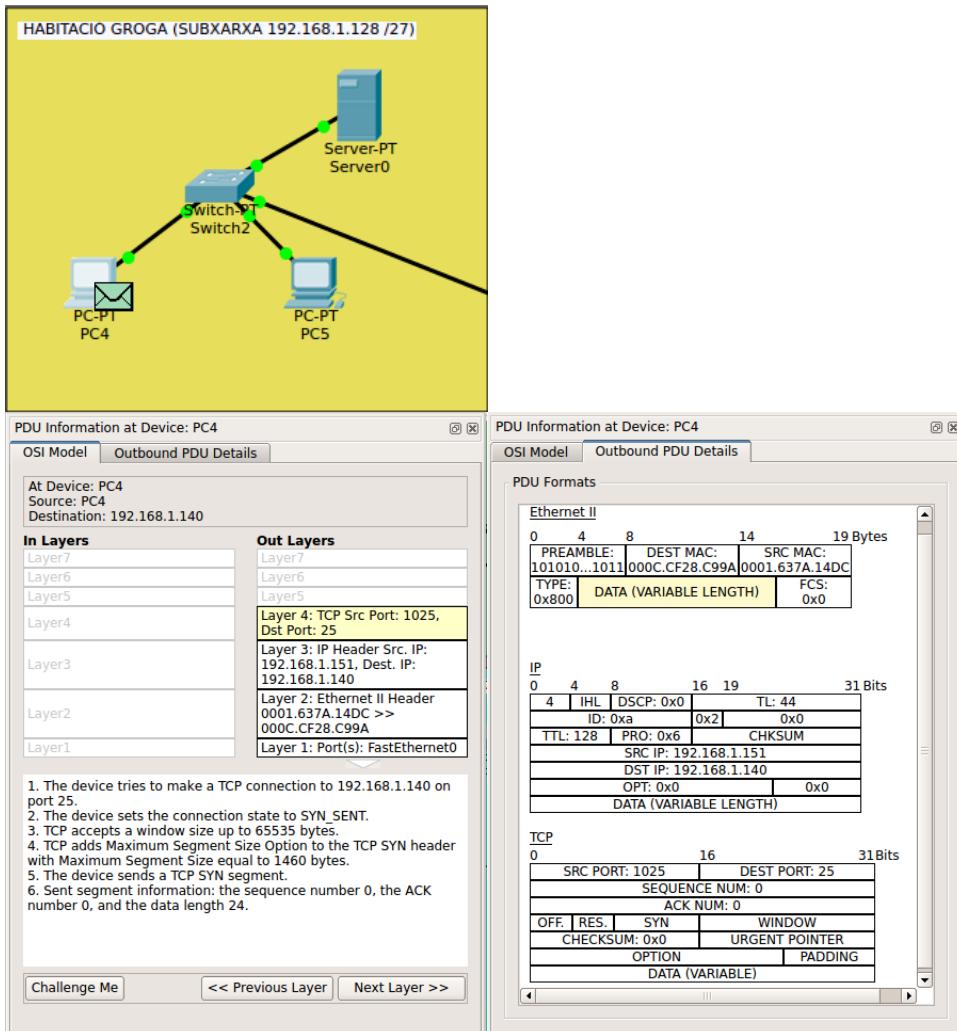


Figura 32: Primer pas del recorregut SMTP

El switch rep la trama Ethernet de l'ordinador, i veu a la seva taula MAC que l'adreça MAC destí es correspon amb la del servidor, així que commuta la trama cap al servidor.

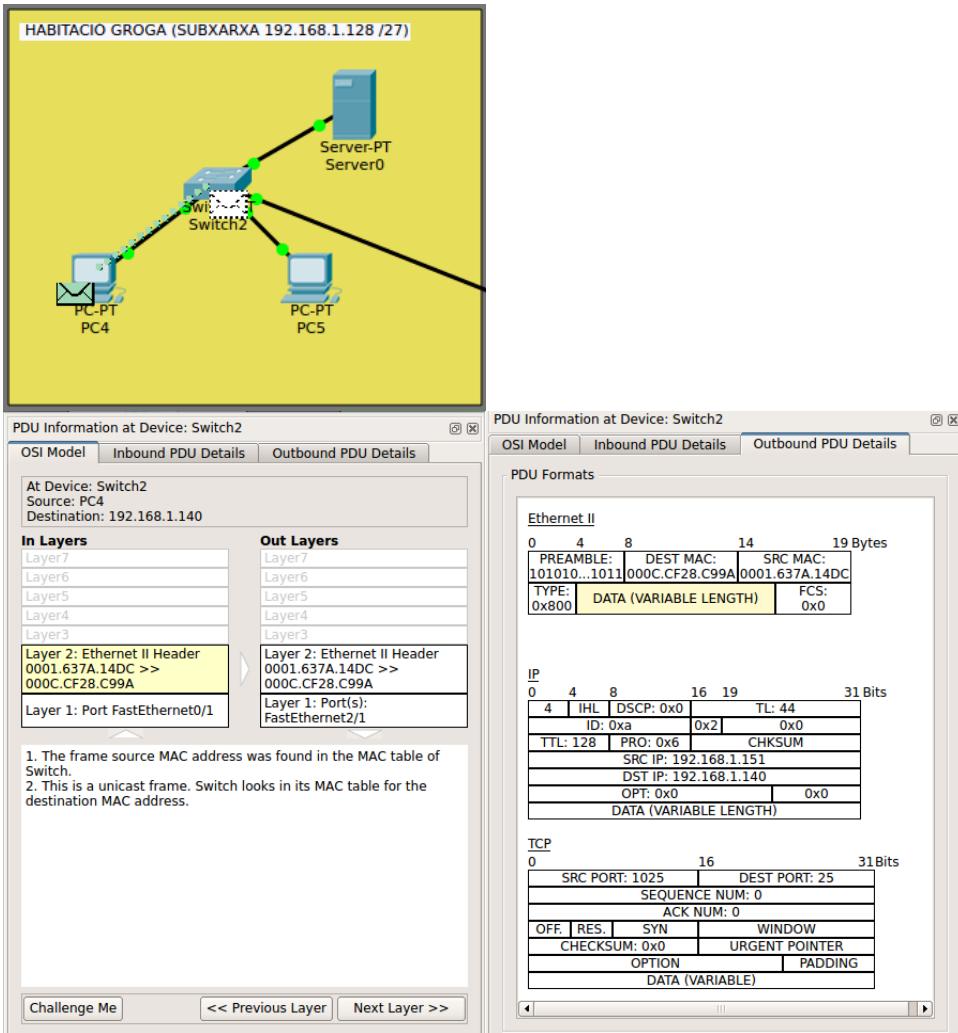


Figura 33: Segon pas del recorregut SMTP

El servidor, a nivell de capa MAC, veu que la trama d'Ethernet el té a ell com a receptor, ja que la MAC destí és la seva adreça MAC; desencapsula les dades per obtenir la PDU del nivell IP, on veu que la IP destí del datagrama és la seva; finalment obté la PDU de transport, que no és altra que una sol·licitud TCP per obrir una connexió al port 25. Aquest port no està ocupat, i els requisits de mida de finestra i segment són acceptables, així que l'extrem del servidor accepta obrir la connexió TCP: enviarà a l'ordinador una confirmació d'inici de transmissió, i per fer-ho manté el flag de SYN a 1 i posa també a 1 el flag d'ACK (per tant enviarà el que es coneix com un segment SYN+ACK a l'ordinador); el número d'ACK del segment, per tant, passa de 0 a 1, s'incrementa, i els ports d'origen i destí s'inverteixen, ja que la informació viatjarà ara en sentit contrari.

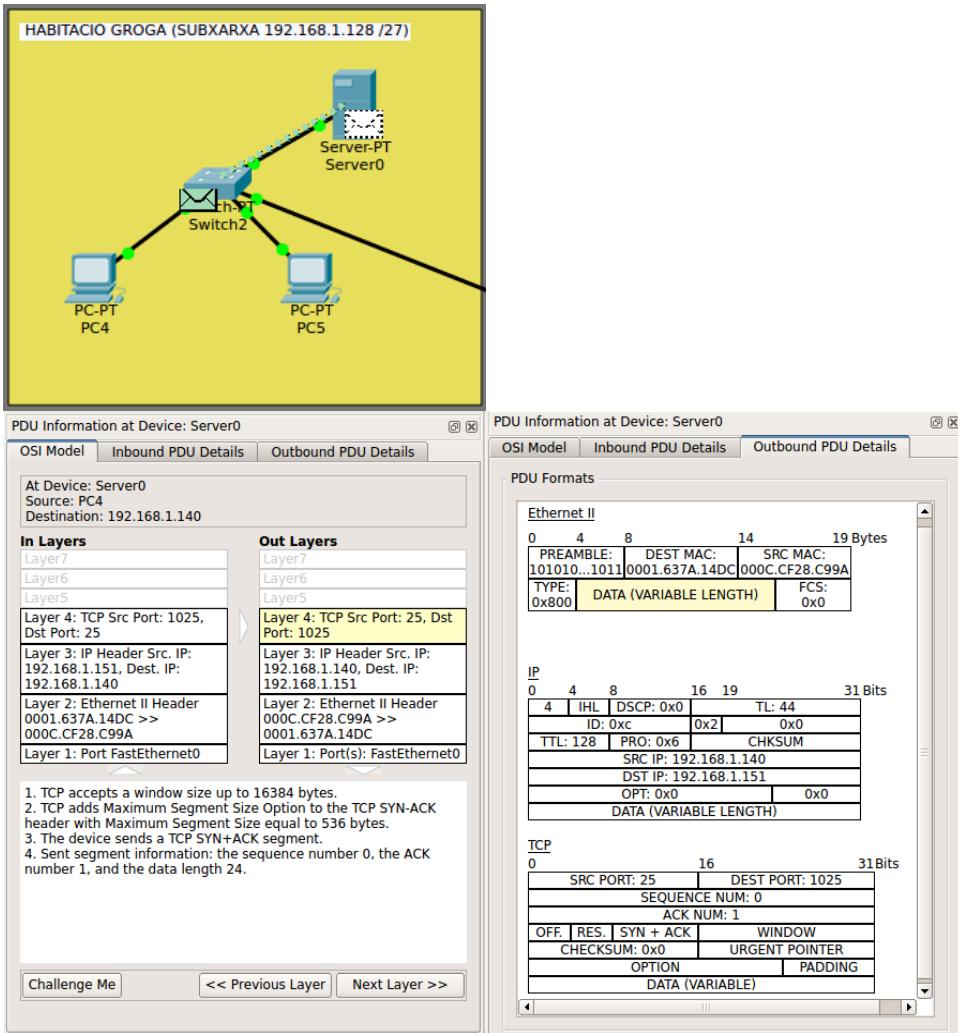


Figura 34: Tercer pas del recorregut SMTP

El switch rep la trama Ethernet amb què el servidor ha encapsulat les dades, i procedeix a fer-les arribar a l'ordinador que va iniciar la comunicació, ja que la MAC destí és la seva.

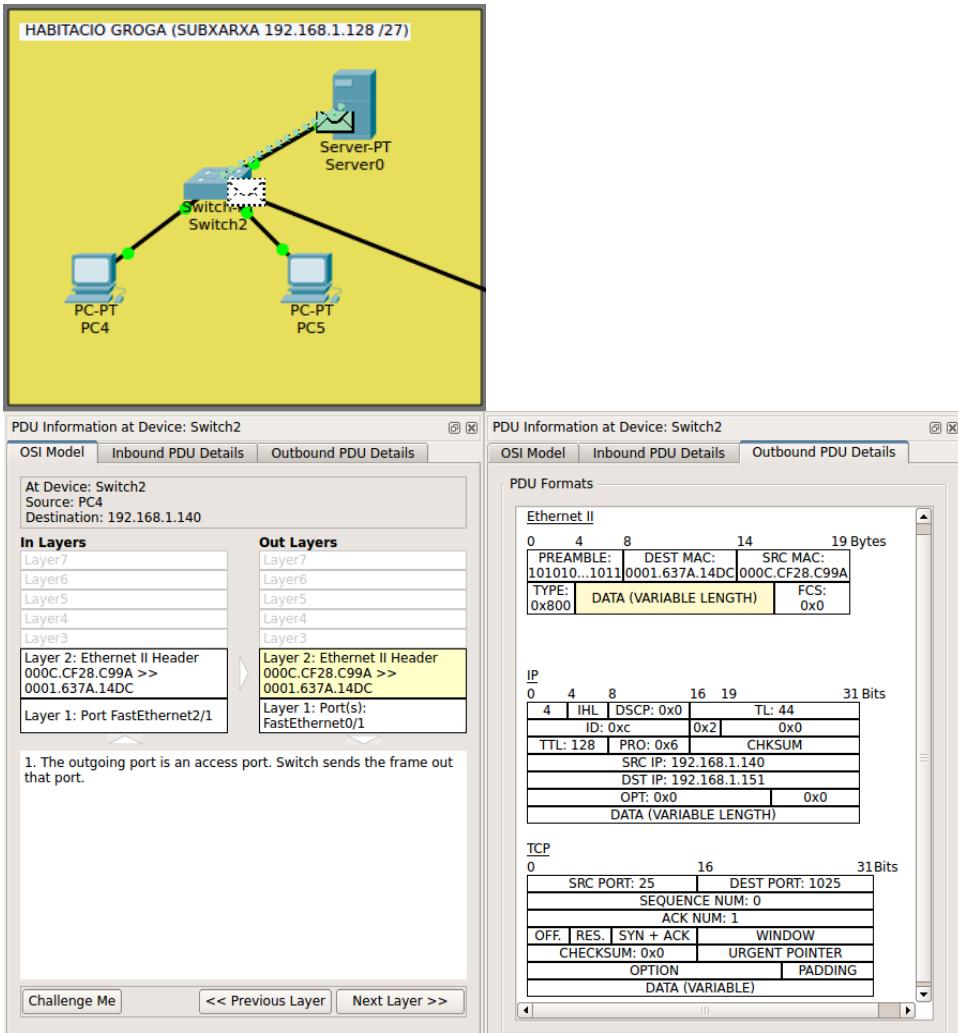


Figura 35: Quart pas del recorregut SMTP

En aquest punt de la transmissió, l'ordinador rep la trama Ethernet, veu que la MAC destí és la seva, així que desencapsula el payload per obtenir el datagrama IP; veu que la IP destí és la seva, així que obté la PDU del nivell TCP. Veu que és un segment SYN+ACK, i els números de seqüència i ACK són els esperats, així que considera establerta la connexió amb èxit amb l'extrem del servidor, de manera que ara podrà començar la fase de transferència de dades de TCP. Primer de tot, però, envia un segment TCP amb el flag ACK com a únic flag actiu per confirmar a l'altre extrem que ha rebut la seva confirmació (aquesta sistema de confirmació als dos extrems de TCP el coneixem com a «three-way handshaking», ja que un demana sincronització, l'altre accepta i finalment l'extrem d'inici indica que ha rebut l'acceptació).

Mentre vagi transportant-se aquest segment d'ACK, però, l'ordinador ja pot anar preparant, a nivell d'aplicació, les dades SMTP a enviar, és a dir, el correu, que té per destinatari l'aplicació de client de correu del servidor. Aquestes dades s'encapsulen al camp de dades del segment de TCP (que incrementa el nombre de seqüència de 0 a 1 té els flags PSH i ACK activats, ja que ja transmet informació i serveix també per contestar la darrera transmissió), i aquest al camp de dades del datagrama IP, que s'encapsula

per la seva banda dins del payload d'una trama Ethernet; ja hem enumerat en ocasions anteriors els camps de les capçaleres de cada tipus d'encapsulació. Aquest missatge s'adreçarà al servidor passant pel switch.

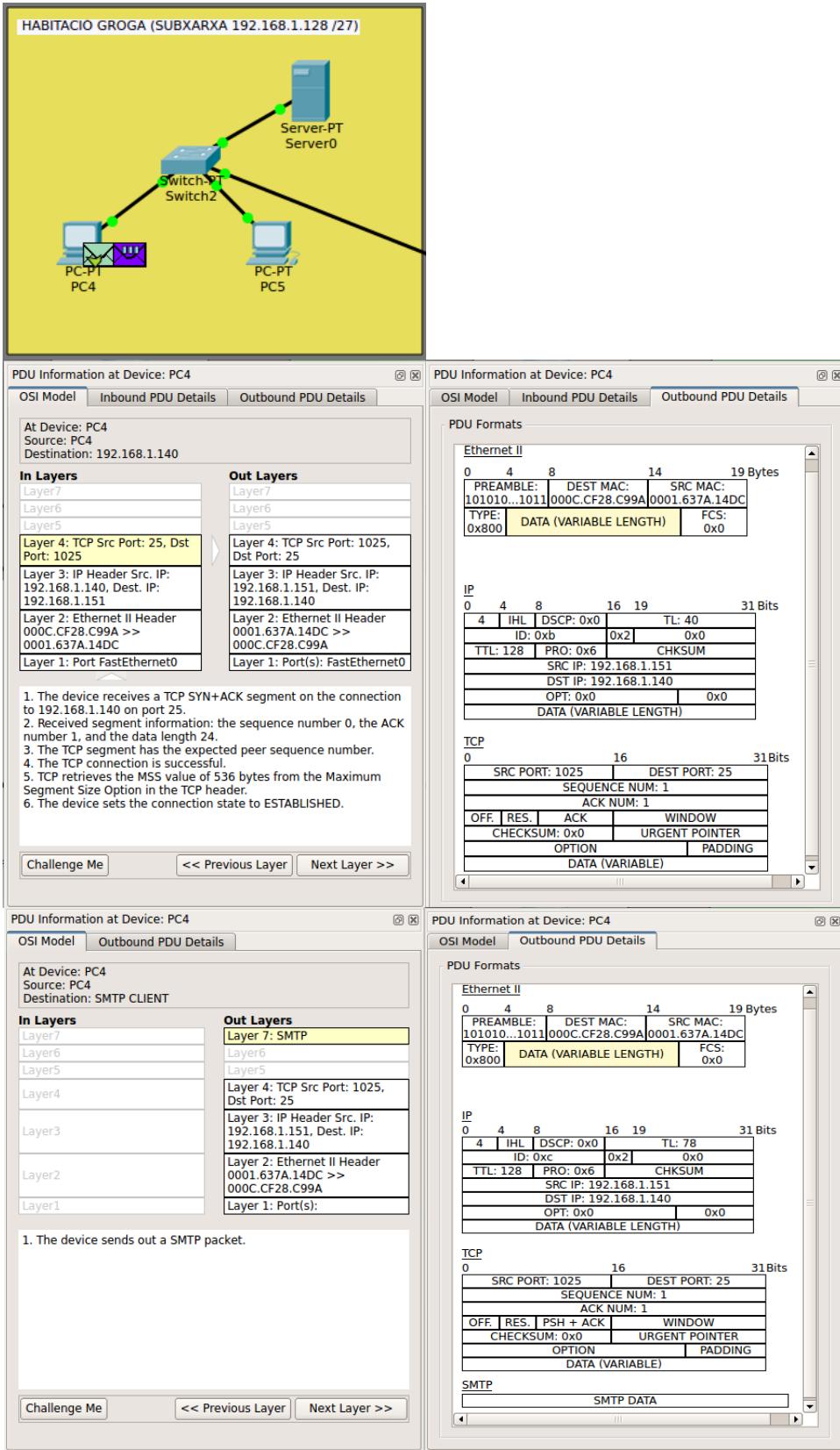


Figura 36: Cinquè pas del recorregut SMTP

El switch rep la trama Ethernet que encapsula l'ACK al SYN+ACK, i el dirigeix cap al servidor. La trama que encapsularà les dades SMTP del correu encara no ha sortit de l'ordinador.

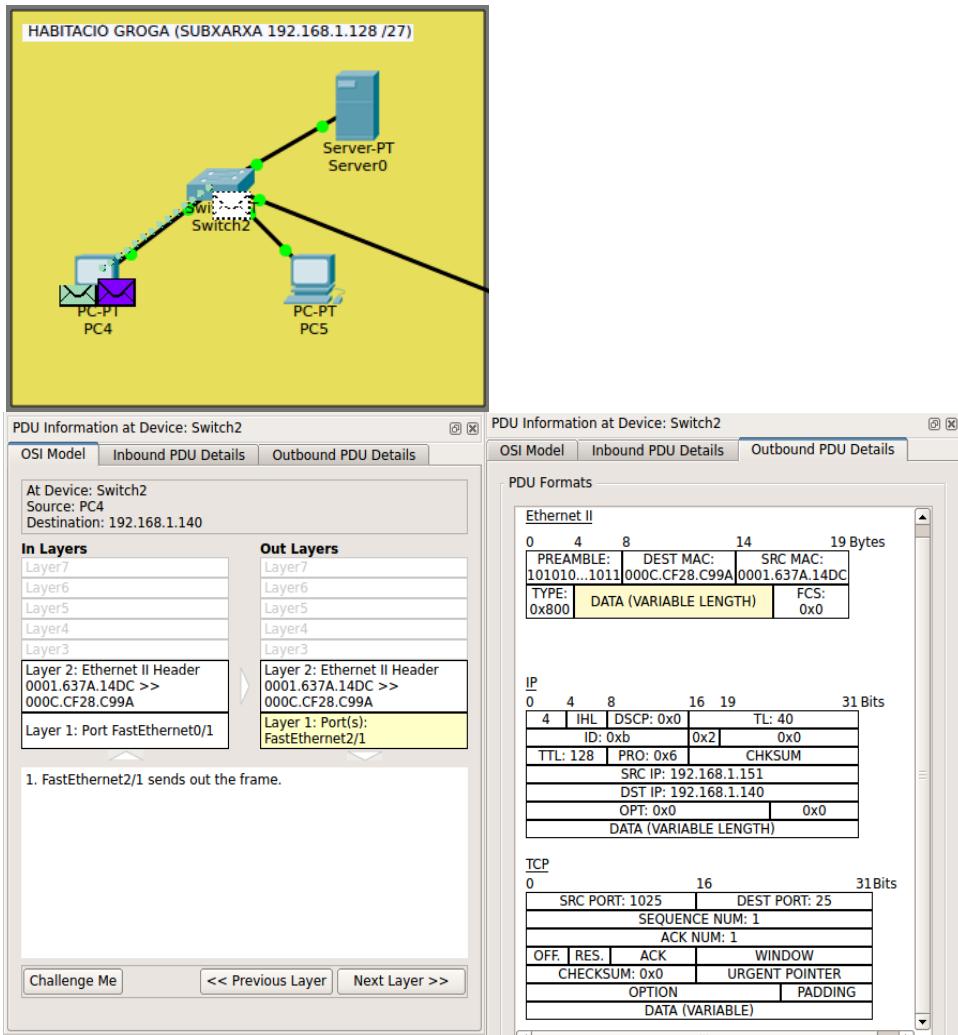


Figura 37: Sisè pas del recorregut SMTP

El servidor rep el segment TCP d'ACK (encapsulat dins d'un datagrama IP dins d'una trama Ethernet, és clar), considerant per tant que les properes transmissions de l'altre extrem TCP ja seran dades en si, dóna per acabada en aquest extrem la confirmació d'inicialització. En paral·lel, el switch rep la trama Ethernet que encapsula les dades SMTP, que farà arribar al servidor properament.

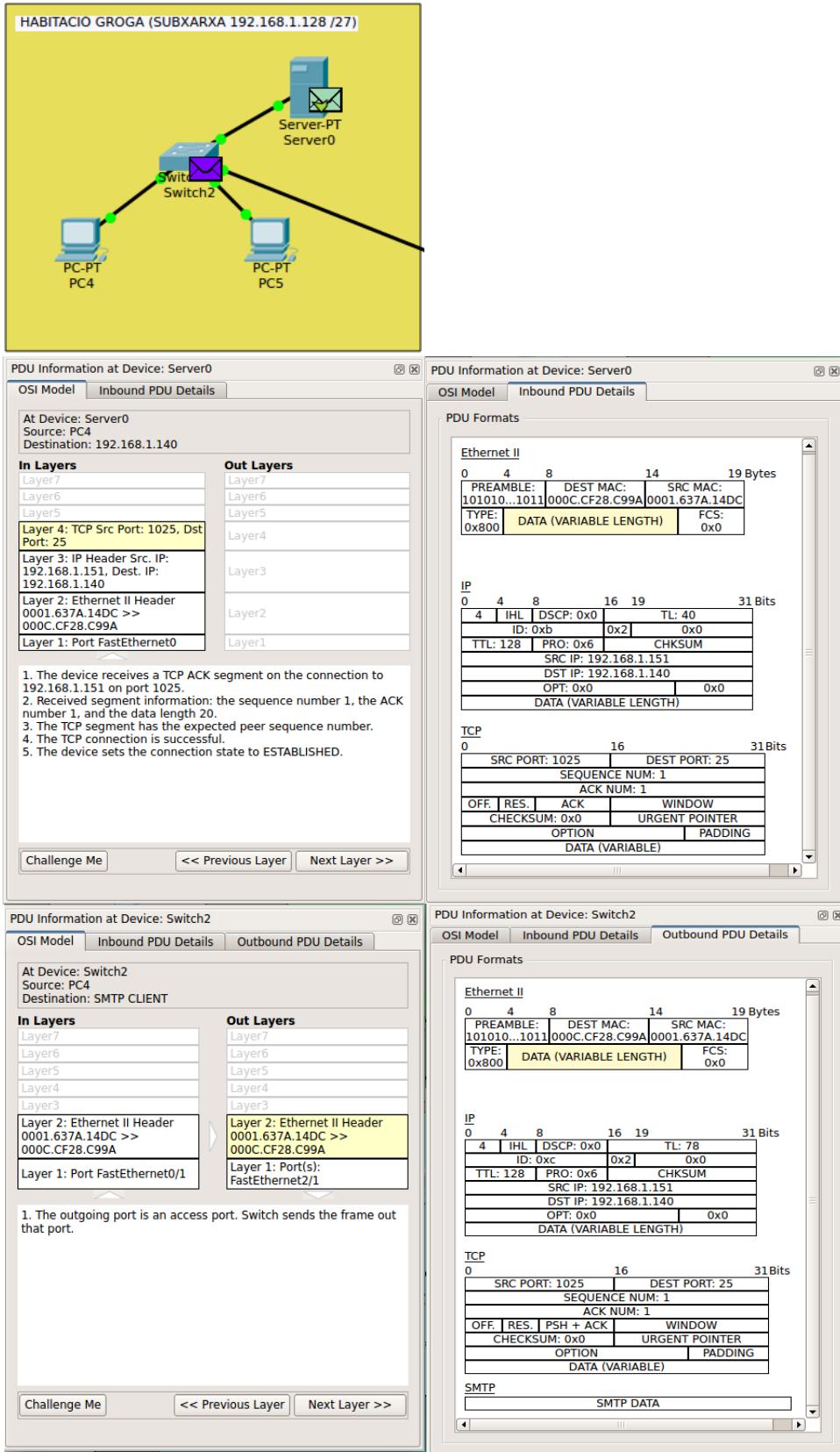


Figura 38: Setè pas del recorregut SMTP

Tot seguit, el servidor rep procedent del switch una trama Ethernet, que desencapsula fins arribar al nivell TCP, on veu que el nombre de seqüència i ACK són els esperats, i, com és un segment de PSH, cal passar les dades al nivell superior; es desencapsulen les dades com a informació de SMTP a nivell d'aplicació, i l'aplicació de correu electrònic genera unes dades de resposta del tipus «Response success»; confirmen la recepció del correu enviat al servidor. Tot plegat es torna a encapsular fins arribar a la capa física, que transmet les dades encapsulades cap a l'ordinador, passant primer pel switch.

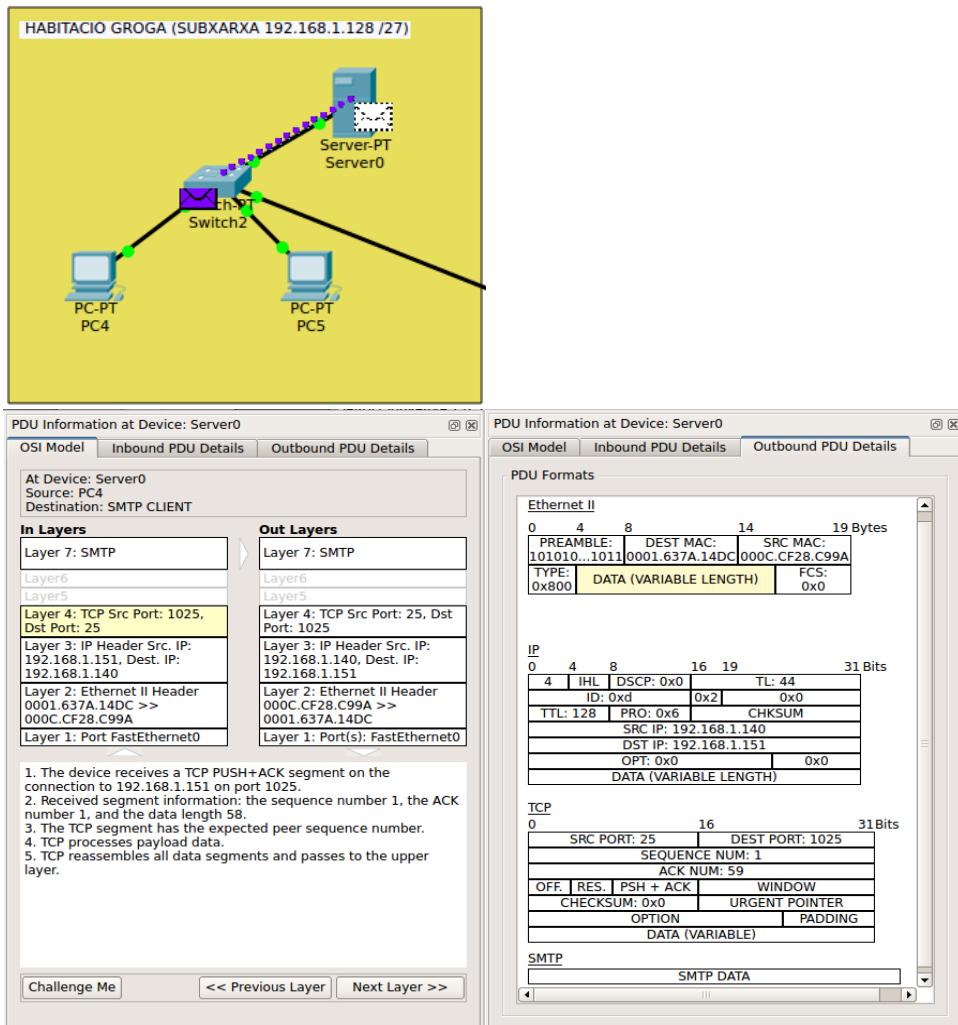


Figura 39: Vuitè pas del recorregut SMTP

El switch fa arribar la trama Ethernet amb les dades a l'ordinador, de forma anàloga a com ja hem indicat anteriorment.

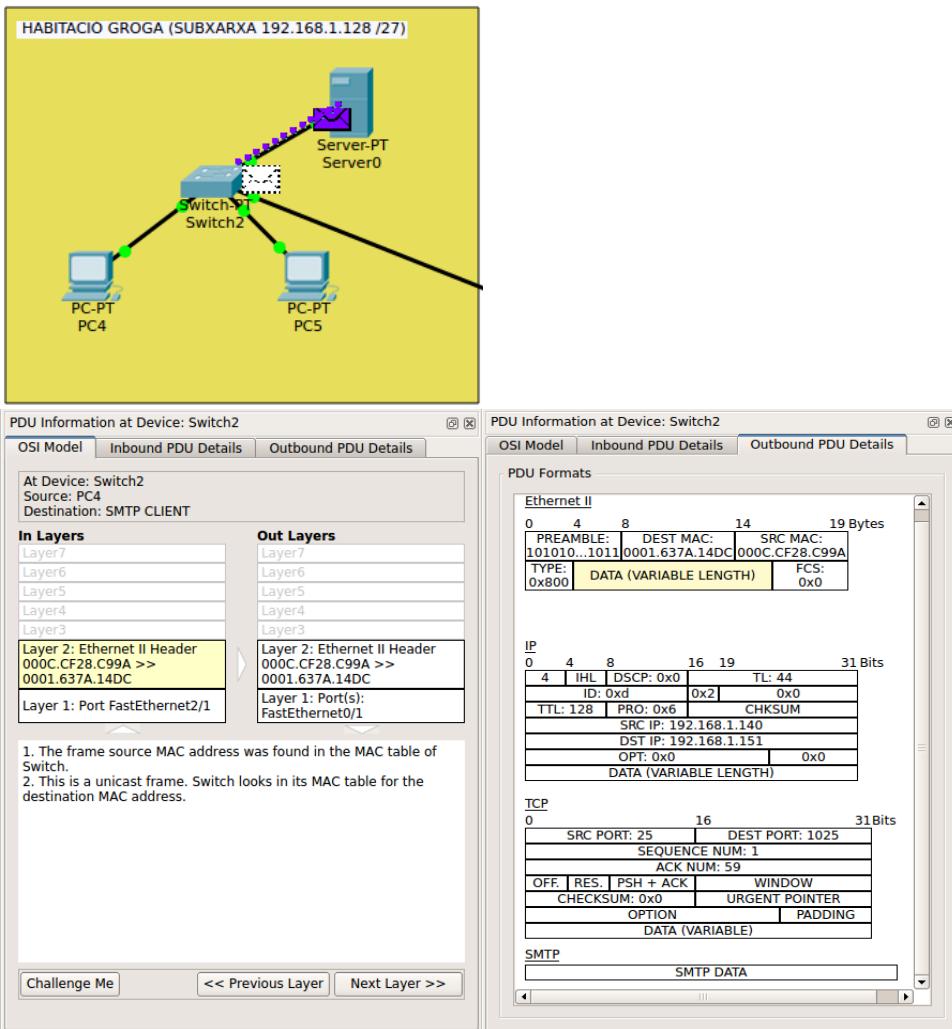


Figura 40: Novè pas del recorregut SMTP

L'ordinador rep les dades i va comprovant a cada nivell de la pila TCP/IP que li corresponen i que són correctes, fins arribar a desencapsular-les totalment com a SMTP: l'aplicació de correu sap ara que el servidor ha rebut el correu, per tant la seva feina ha acabat. Cal però, fer un darrer pas: tancar la connexió entre els ports de TCP. Per a fer-ho, es prepara un nou segment TCP de finalització, és a dir, amb el flag de FIN a 1. També es posa a 1 el flag ACK, per confirmar la recepció del segment anteriorment enviat des del servidor. Tot plegat es va encapsulant en baixar per la pila TCP/IP fins arribar a la capa MAC, on esdevé una trama Ethernet que s'envia al switch.

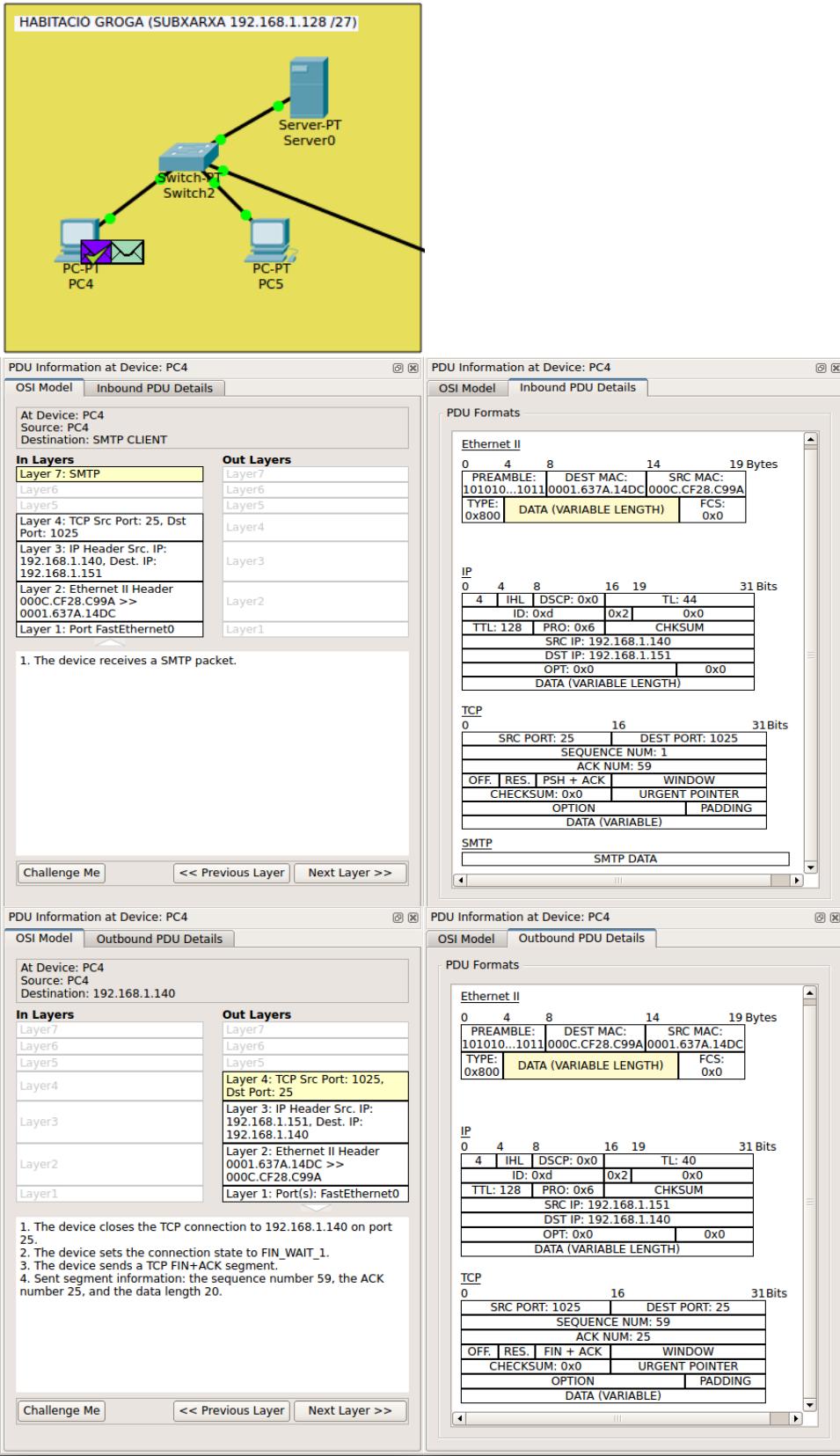


Figura 41: Desè pas del recorregut SMTP

El switch rep la trama Ethernet i la commuta cap al servidor ja que la MAC destí és la d'aquest.

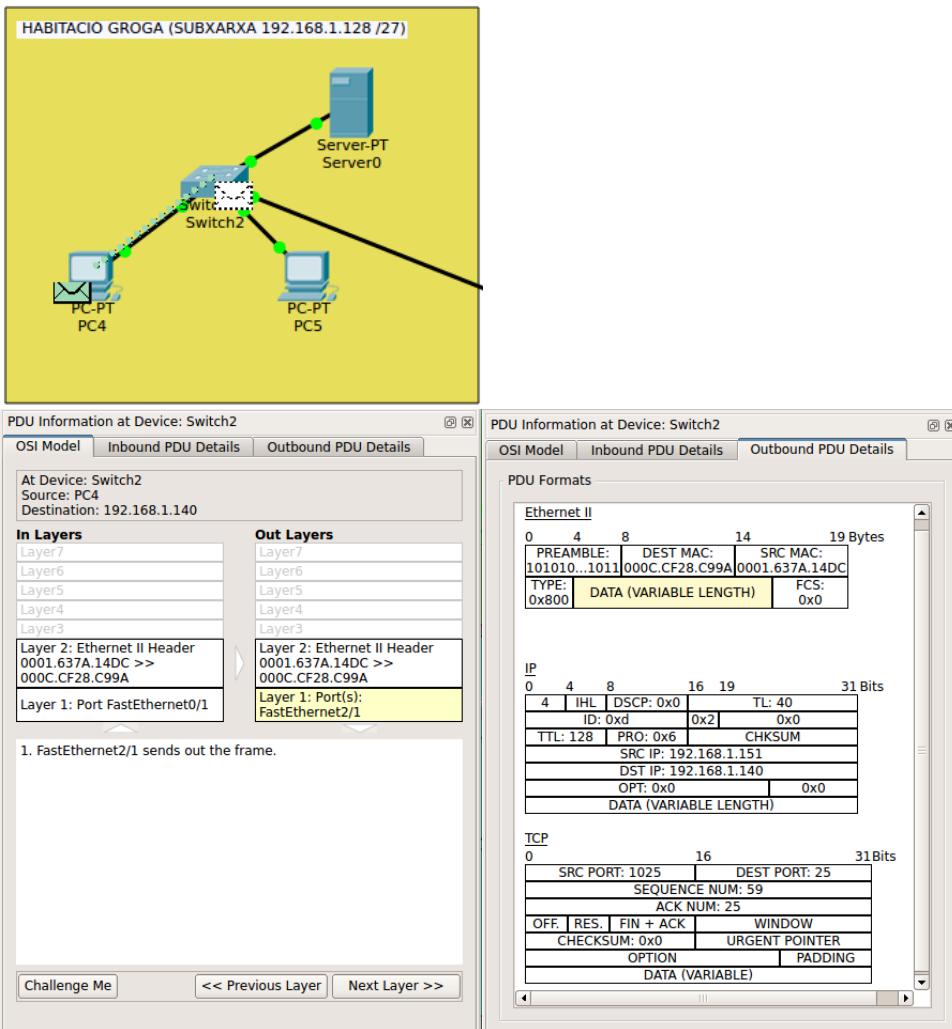


Figura 42: Onzè pas del recorregut SMTP

El servidor desencapsula les dades rebudes fins arribar al nivell TCP. Veu que es tracta d'un segment de finalització perquè està activat el flag FIN. Determina doncs, que cal tancar el port de connexió amb l'altre extrem, el 25, i disconnectar l'activitat TCP de la connexió. Envia un darrer segment en direcció a l'ordinador per confirmar-li la finalització al seu extrem; manté, així, els flags FIN i ACK a 1.

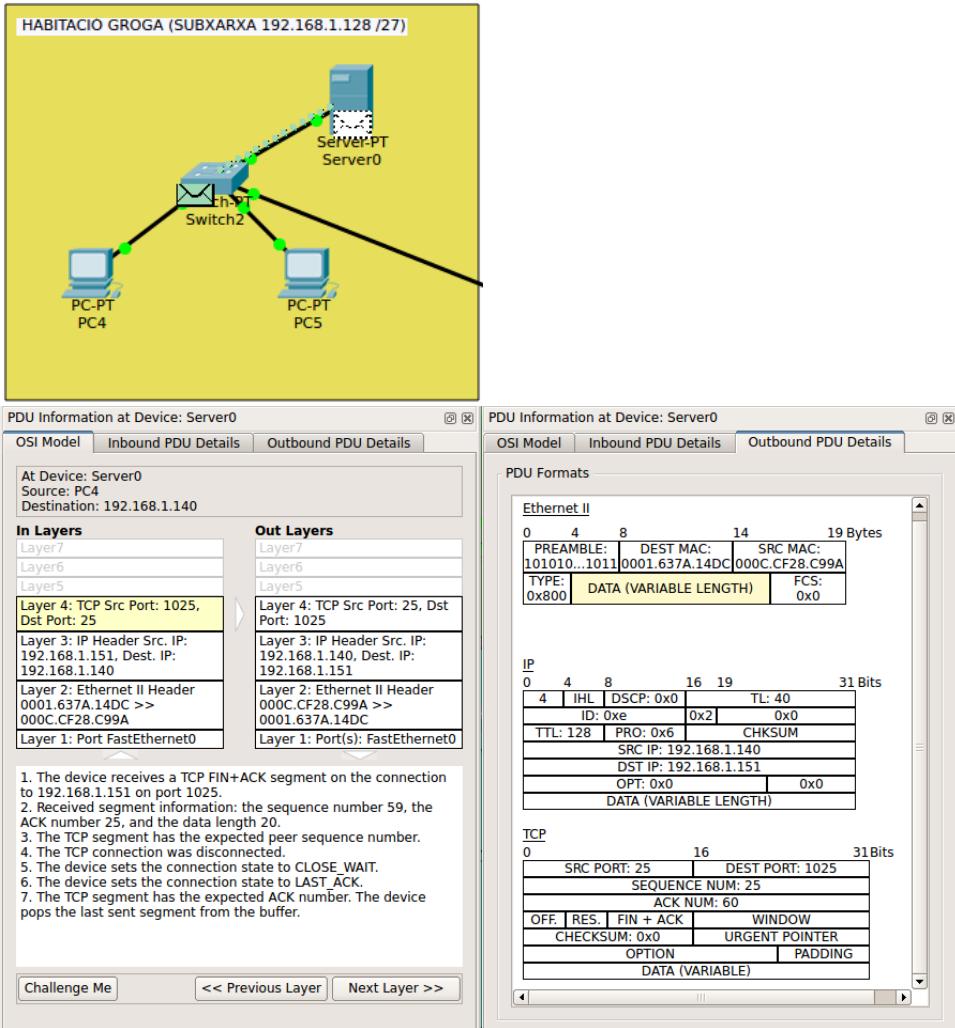


Figura 43: Dotzè pas del recorregut SMTP

El switch obté el missatge del servidor encapsulat com a trama Ethernet; com la MAC destí de la trama és l'ordinador al qual està connectat, transmet la trama a aquest ordinador per l'interfície Ethernet corresponent.

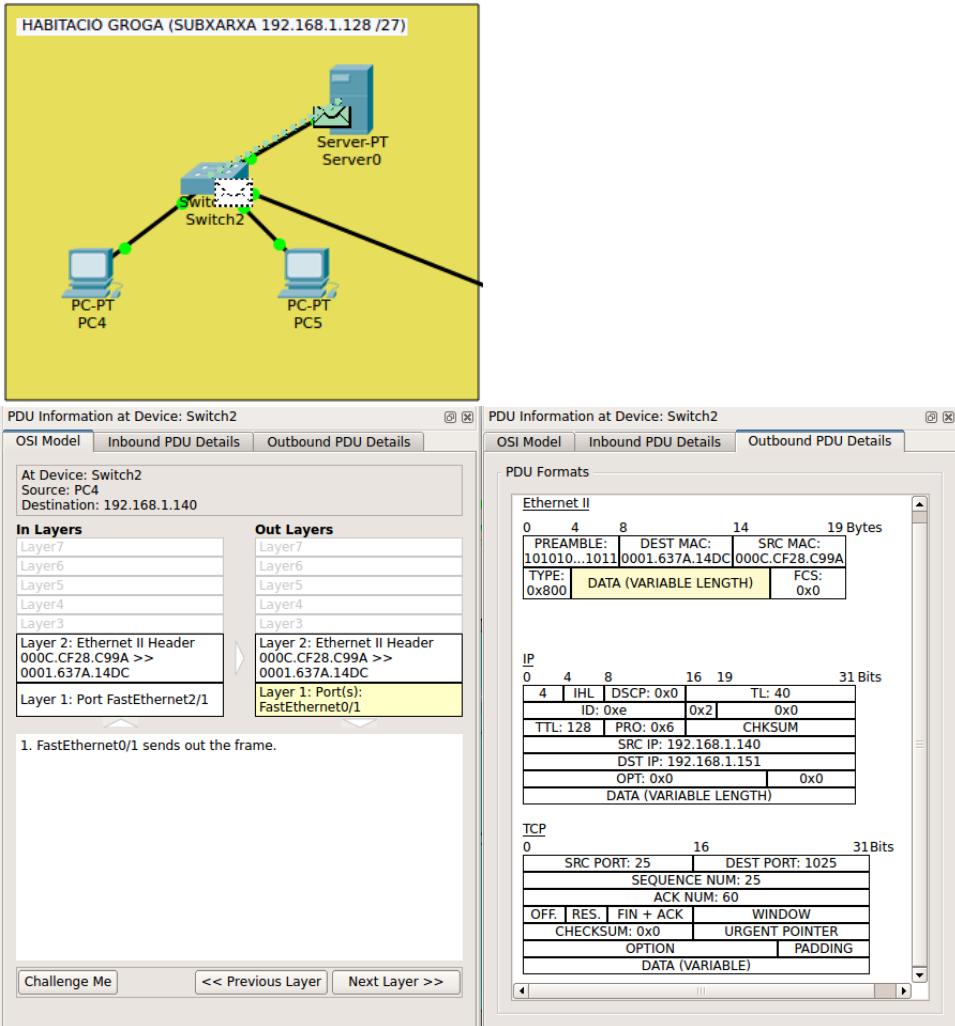


Figura 44: Tretzè pas del recorregut SMTP

L'ordinador rep la trama Ethernet i desencapsula les dades que conté fins al nivell d'enllaç. Allà descobreix que ha rebut un segment de FIN+ACK, que confirma que l'altre extrem ha rebut la sol·licitud de finalització, de manera que aquest extrem també tancarà el seu port, el 1025, per disconnectar-se. S'envia un darrer segment d'ACK en direcció a l'altre extrem per confirmar la recepció de la finalització (recordem que a TCP tot es confirma als dos extrems independentment, com hem vist en l'establiment de la connexió).

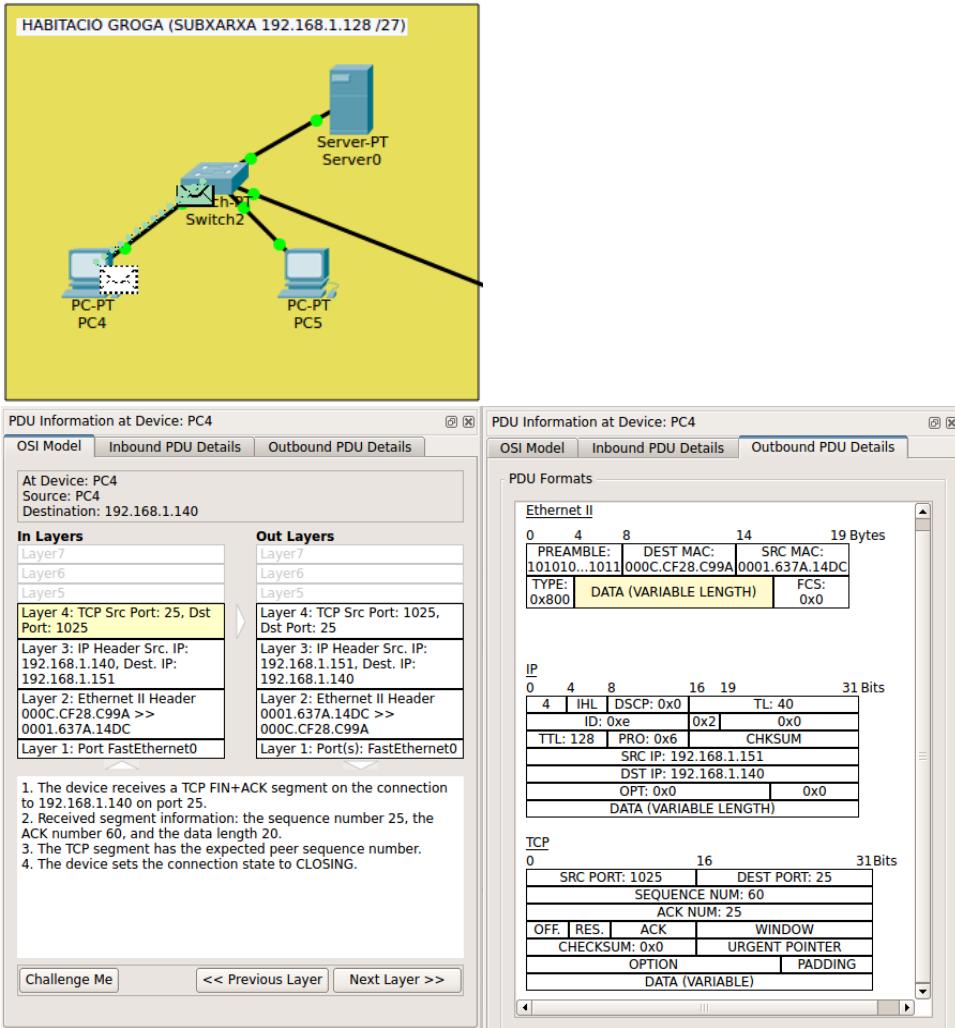


Figura 45: Catorzè pas del recorregut SMTP

El switch rep la trama Ethernet i la commuta cap al servidor ja que la MAC destí és la d'aquest.

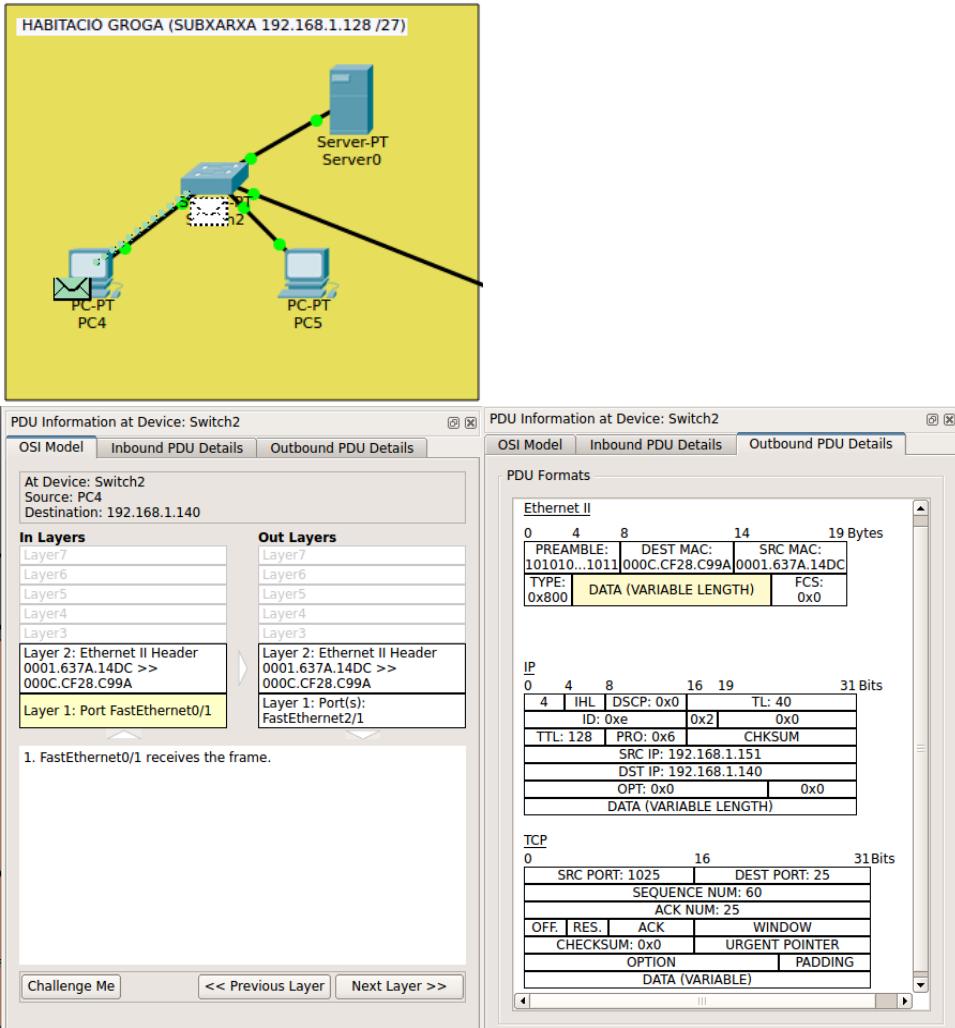


Figura 46: Quinzè pas del recorregut SMTP

Finalment, el servidor desencapsula la trama Ethernet fins arribar al nivell TCP, on descobreix que es tracta d'un segment d'ACK: indica per tant, que s'ha rebut la indicació de tancar la connexió de l'altre extrem, i, per tant, es pot tancar definitivament el port d'aquest extrem i amb ell tota la connexió, que ja estava pendent de ser finalitzada. S'acaba, doncs, tota la transmissió de dades.

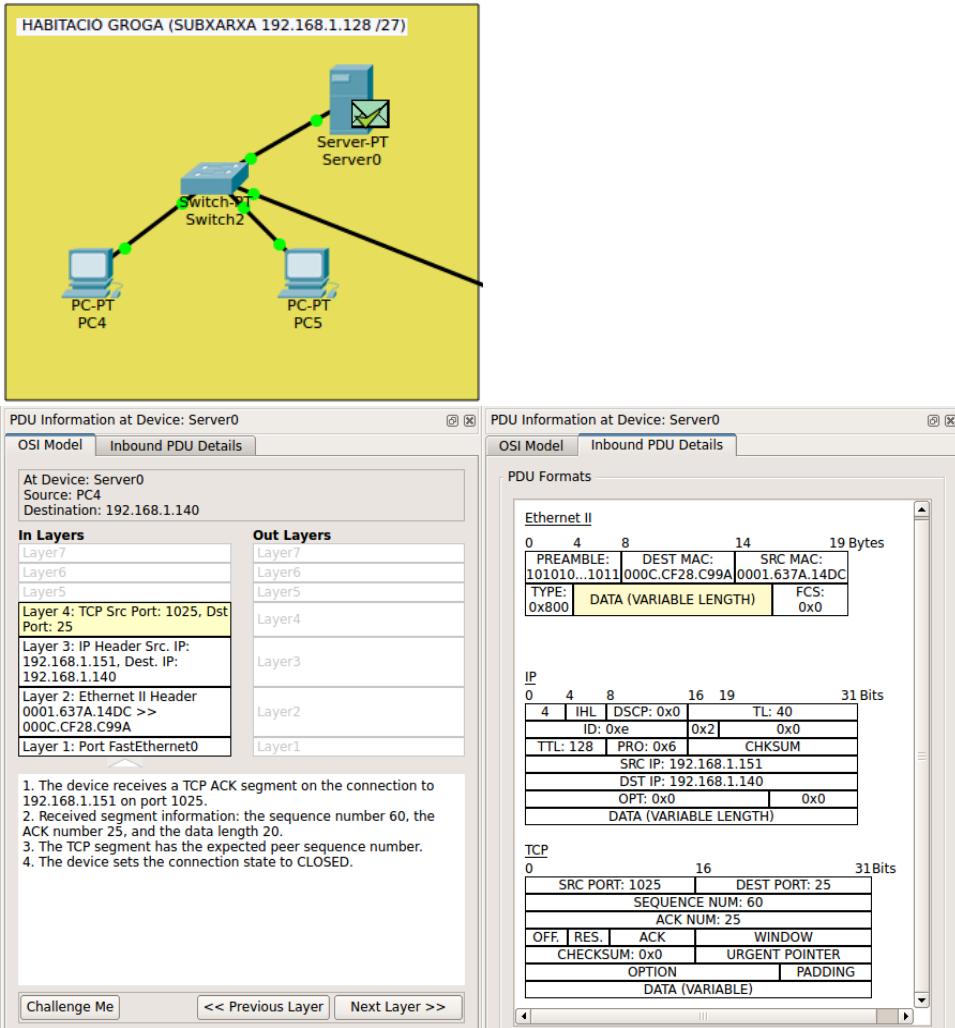


Figura 47: Setzè i darrer pas del recorregut SMTP

### 3. Conclusions

Aquest treball ens ha permès consolidar els coneixements apresos al llarg de tota l'assignatura, en gran part gràcies al detallat anàlisi de com els missatges (trames, paquets, datagrames, segments o dades d'aplicació, segons el nivell TCP/IP o OSI de cada moment) es transmeten, es reben, s'encapsulen i es desencapsulen, fent servir els protocols adients de cada nivell de què disposa cada dispositiu.

Hem revisat per tant els conceptes de la primera part del curs, analitzant la transmissió física i a nivell d'enllaç, sobretot a través d'Ethernet, però també hem vist un protocol wireless. També hem aprofundit en els conceptes d'enrutament o encaminament apresos més endavant a l'assignatura, i hem vist com crear subxarxes i quins procediments i tècniques fan servir els routers per dirigir la informació, com per exemple RIP o el mètode estàtic del «Next hop», i també recursos que encara no coneixíem com les taules CEF dels routers de Cisco.

Hem après, de forma general, a formular el problema de muntar una xarxa (especialment una xarxa com a conjunt de subxarxes) amb un simulador, Cisco Packet Tracer, capaç d'emular amb un grau de precisió elevada les situacions i casos que podem trobar si muntem una xarxa real, però amb una major llibertat per experimentar ja que, com tot és simulat, no hi ha perill de fer malbé cap dispositiu.

Finalment, indiquem també que hem après dades interessants sobre el funcionament i configuració de processos o aplicacions d'usuari que havíem fet servir abans, com Ping o SMTP, i que ara sabem com treballen a la xarxa i com fan servir la pila TCP/IP per transmetre informació.

Com a conclusió final, indiquem que, després de tots els experiments realitzats, entenem que el sistema per capes de TCP/IP, amb la versatilitat que aporta el fet de poder intercanviar protocols d'un nivell per uns altres segons els medis, les tecnologies i els dispositius permetin, és un dels pilars de les comunicacions en xarxa, i que gràcies al seu sistema d'encapsulament i desencapsulat de dades i als sistemes de control dels protocols, basats en bona mesura en flags de control, és capaç d'adaptar-se a les diferents situacions i escenaris de transferència d'informació per tal que aquesta sigui possible.