

Pràctica 5. El model OSI

Objectius de la Pràctica

L'objectiu principal de la pràctica és veure com s'encapsulen i desencapsulen les diferents Unitats de Protocol d'Usuari (DPU) i que permeten transmetre informació entre dos equips de manera estàndard, independentment de les característiques dels equips en qüestió (Hardware, sistema operatiu, programa o aplicació utilitzada, etc.). Per assolir aquest objectiu utilitzarem un dels programes sniffers més utilitzats actualment: Wireshark, disponible de forma gratuïta a Internet a través de:

www.wireshark.org

Nombre de sessions

Aquesta pràctica es realitzarà en un màxim de 1 sessió. Un cop finalitzada s'enviarà un informe al professor de practiques durant la setmana posterior a través del Campus Virtual de l'assignatura.

El model de referència OSI i el protocol TCP/IP

L'Organització internacional per a la Estandardització (ISO) i la Comissió Electrotècnica internacional (IEC) van ser els encarregats de definir les normes estàndards de comunicació entre equips de forma i manera que la transmissió i recepció de dades fos independent del sistema físic i de l'aplicació lògica utilitzada pels usuaris. Fixem-nos per exemple en una simple connexió a Internet. Deixant a banda l'àmplia quantitat de sistemes hardware que es poden fer servir (ordinadors de sobretaula, portàtils, PDAs, mòbils intel·ligents, tablets...) i sistemes operatius existents (Windows x, Linux, MAC OS, Android, Unix, ...) un usuari final pot fer servir per connectar-se a internet diversos navegadors combinats amb qualsevol de les anteriors característiques, així podem connectar-nos a través de l'Internet Explorer, Mozilla Firefox, Google Chrome i Safari entre d'altres. El que està clar és que tots els equips han de fer servir el mateix estàndard. Així, tots implementaran com a capa d'aplicació el protocol HTTP, a la capa de transport utilitzaran UDP, a la capa de xarxa faran servir IP i a la capa d'accés al medi el sistema que estigui implementat (Ethernet, Wifi, ATM, ...)

La principal missió del model OSI és permetre la connexió entre usuaris independentment de la plataforma utilitzada. Per tal d'aconseguir-ho, el model s'estructura en 7 capes diferents, cadascuna amb una funció específica, necessària per relacionar-se amb els altres sistemes. Cada capa es sustenta en la capa immediatament inferior, la qual realitzarà una sèrie de funcions més primitives que quedaran encapsulades i per tant seran transparents per les capes superiors. Aquesta encapsulació de les dades associades a la pròpia capa s'anomena "Unitat de Dades de Protocol" o PDU. La característica de la PDU, és que es tracta d'un format estàndard que poden interpretar totes les capes que implementen el mateix protocol. És per això que de vegades es parla de una comunicació virtual entre

parells de capes, on el que s'intercanvien són les PDUs associades a aquestes. Per aquesta raó es veu, a la figura 1, una línia que uneix les capes de nivell N origen amb la capa de nivell N destí, intercanviant-se de forma virtual, la PDU corresponent. El mateix passa per la capa N+1. Ara bé, la informació realment passa de una capa a la immediatament inferior o superior. En el cas del node origen, la transferència es produeix des de l'Aplicació fins a la capa física, on les dades s'envien a través del medi. Per fer aquest procés, La PDU del nivell N+1 s'enviarà a través de les primitives d'intercanvi existents entre la capa N+1 i la capa N. La informació d'intercanvi es guarda en una capçalera on tindrem la Informació de Control de la Interfície (ICI), que s'afegeix a la PDU formant una IDU o Unitat de Dades de Interfície (omès a la figura 1). A la capa N, es reb la IDU, s'elimina la capçalera d'intercanvi (ICI) i es queda amb la N+1 PDU, que a la capa N es coneix com la Unitat de Dades de Servei, o SDU de la capa N. És a dir, el que és la N+1-PDU passa a ser la N-SDU, que és el que s'il·lustra a la figura 1. A la capa N, ara introduïrem la informació necessària per que la informació pugui ser extreta per la capa N del destí. Això implica introduir la capçalera de la capa N. Per tant, la N-SDU + la capçalera associada a la capa N = N-PDU, que és el que es pretén il·lustrar a la figura 1.

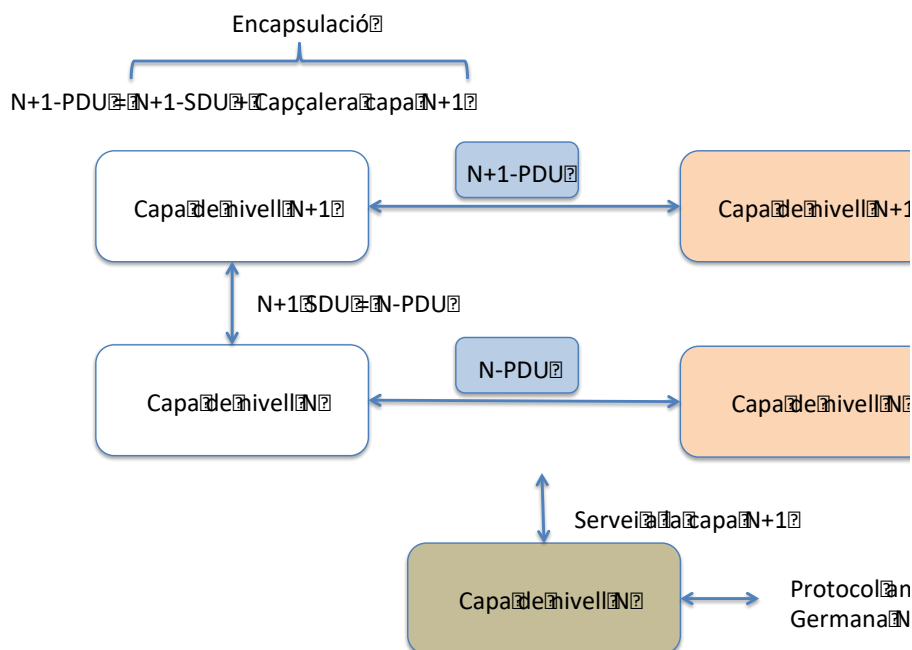


Figura 1.a Arquitectura OSI on es mostra l'estructura de capes i el mode de funcionament.

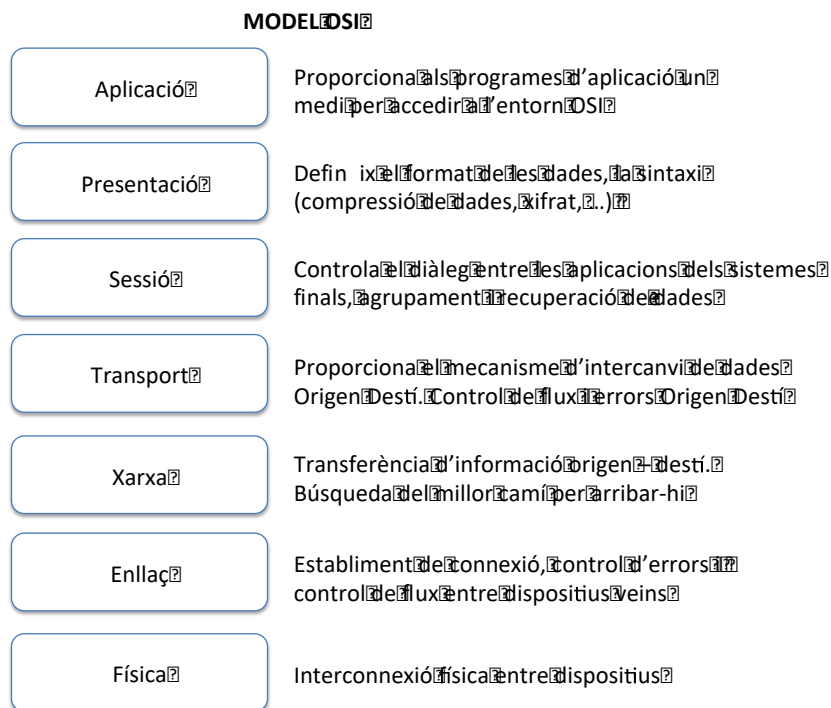


Figura 2. Estructura de capes del model OSI amb les seves característiques més importants.

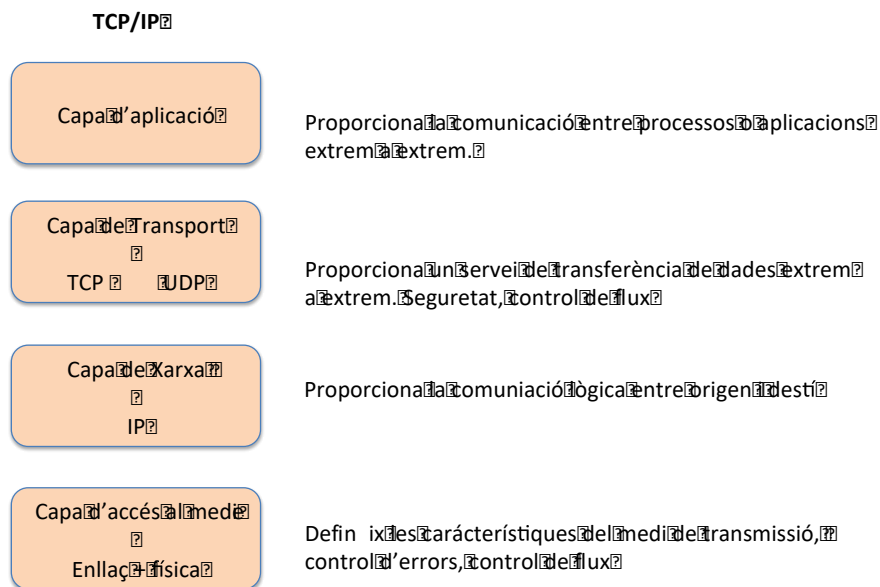


Figura 3. Protocol TCP/IP

Wireshark

Wireshark és un analitzador de protocols utilitzat per analitzar el transit de les xarxes de comunicacions, així com una eina didàctica en el funcionament de les xarxes.

Wireshark és software lliures sota llicència GPL. S'executa sobre la majoria dels sistemes operatius Unix i compatibles, Linux, MAC OSX i Microsoft Windows.

Cisco Packet Tracer

Cisco Packet Tracer és un programa desenvolupat per l'empresa Cisco per a facilitar les tasques d'aprenentatge als estudiants de xarxes. És un simulador que permet als estudiants analitzar i experimentar amb els comportaments de les xarxes i els seus diversos elements.

CiscoPacket Tracer és un software gratuït que pot executar-se en Linux i Microsoft Windows.

Realització Pràctica

Descarrega wireshark i instal·la el programari al PC (Windows). Obre wireshark. Apareixen tres grans finestres: una de captura, una de fitxers prèviament capturats i una d'accés a Internet on es troba la guia d'usuari així com la web del producte i altres opcions.

A la finestra de captura, tenim una icona on es llisten les interfícies que té el nostre sistema. Per exemple, en el cas de l'autor, apareix una interfície associada a la Ethernet i una interfície associada a la WiFi. Visualitzeu les característiques de cada interfície clicant al botó de "details". Indiqueu que teniu i expliqueu detalladament que apareix.

Seccioneu la interfície d'Ethernet. Apunteu l'adreça MAC que surt i executeu des de consola un ipconfig /all. Identifiqueu la IP associada a aquesta MAC. Descriviu curosament els detalls a l'informe.

Exercici 1

Doneu al botó d'inici (start). Veureu que apareix tot el transit que s'està monitoritzant a la xarxa local a la qual esteu treballant. Aquesta quantitat d'informació és tant elevada que resulta complicat estudiar-la en detall. Anem a filtrar les dades que ens arriben. El primer que farem serà un filtratge per IP. Per això farem servir la nostra IP, que havíem trobat prèviament en fer el ipconfig.

Poseu el següent a la zona de filtratge que trobareu just a sota de les icones:

ip.addr eq <la vostra IP>

Escolliu de la llista una de les captures on el protocol sigui TCP i seccioneu-la. A la finestra horitzontal intermitja, es desglossa tot el paquet seccionat. A la finestra inferior es desglossa el que teniu seccionat a la finestra intermitja. Així, si cliqueu a Ethernet apareix la MAC vostra i la del destinatari. Com es descriu la

vostra adreça MAC? A la adreça MAC hi han dues parts clarament diferenciades. A que corresponen? Compara el que apareix amb el que surt amb un `ipconfig/all`. Repassa els diferents camps que apareixen a la capçalera IP i amb l'ajut dels llibres `i/o Internet` identifica que fa cada un dels camps.

Exercici 2

Feu una captura de les comunicacions. Un cop està llençada la captura, des de consola feu:

```
>> telnet time-A.timefreq.bldrdoc.gov 13
```

Aneu a Capture i cliqueu stop.

Tenint en compte que no heu introduït una adreça IP, busqueu el protocol DNS que permet connectar-nos amb un servidor de DNS per tal de discernir quina IP correspon a la màquina time-A.timefreq.bldrdoc.gov.

Un cop determinada la IP, a quin port ens estem connectant? Quin protocol de transport fem servir?

Identifica l'intercanvi de comunicacions que es produeix a nivell de DNS. Quin protocol de transport fa servir DNS? Perquè? Quina és la IP del servidor de DNS? Com s'especifica la resposta? Què respon?

Feu el diagrama temporal descrivint detalladament l'intercanvi d'informació entre el vostre ordinador i el servidor de DNS.

Un cop coneguda la IP destí, proporcionada pel servidor de DNS, identifica l'intercanvi de control que es produeix a nivell de TCP per la transmissió de la informació. Expliqueu que fa cada paquet i feu un diagrama temporal on es representa aquest intercanvi. Pren molta rellevància la utilització dels flags a TCP. Indiqueu que fan i com es fan servir per gestionar la comunicació.

Exercici 3

Des de capture, cliqueu a start i feu un ping a una adreça pública coneguda d'Internet (per exemple www.google.com). Captureu el transit de la comunicació i desglosseu la comunicació en sí. Expliqueu detalladament la captura, tal i com s'ha fet en l'exercici anterior. Què és el protocol ICMP? Com funciona aquest protocol? Quins identificadors i flags fa servir?

Obriu el navegador i poseu http://ip_obtinguda a través del ping. S'obre la pàgina? Que captura el sniffer? Feu una explicació detallada.

Desglosseu la captura per connectar amb la web. Aneu al protocol TCP. Quin port de sortida heu fet servir? Identifiqueu algun protocol de control de flux? Expliqueu detalladament el que heu capturat.

Exercici 4

Obre el programa simulador Cisco Packet Tracer i crea dues xarxes connectades a través del núvol. Cada una de les xarxes ha de tenir un router genèric i dos switchos de 24 canals.

Connecta uns quants ordinadors (entre cinc i vuit) als switchos. En una de les xarxes munta un subnetting variable i assigna les IP's de manera estàtica. A l'altra xarxa munta en el router un servidor DHCP per tal d'assignar IPs de forma dinàmica. En totes dues xarxes configura NAT.

- i) Fes PING des de un dels ordinadors de la xarxa dinàmica a un dels ordinadors de l'altra xarxa. Mostra els diferents empaquetats que es realitzen.
- ii) Configura una pàgina web en un dels equips i connectat des de l'altra xarxa a aquesta pàgina. Mostra els diferents empaquetats que es realitzen.
- iii) Mostra una imatge on es visualitzi la xarxa. Captura el tràfic generat.

Informe de la pràctica

L'informe d'aquesta pràctica ha de constar de:

- 1.- Objectius de la pràctica
- 2.- Resposta a les diferents qüestions que en ella es plantegen als alumnes
- 3.- Explicació de la feina realitzada al laboratori
- 4.- Conclusions