Administració de programari de base propietari

Aitor Rigada Bofill

Implantació de sistemes operatius (ASX)
Sistemes informàtics (DAM)
Sistemes informàtics (DAW)

Índex

Introducció

Els sistemes informàtics no són excepcionals en les organitzacions i empreses actuals. Al contrari, en són un component cada vegada més imprescindible. Una bona administració d'aquest sistema és, doncs, clau per al bon funcionament de l'organització o empresa.

En aquesta unitat, es veurà com es gestionen correctament els usuaris d'un sistema informàtic com és el Windows 7. Una gestió correcta d'usuaris és el primer mecanisme per assegurar un sistema aïllat enfront a les amenaces d'accés no autoritzat. A més, aprendrem a configurar correctament la xarxa per permetre que el nostre sistema pugui accedir als recursos compartits d'una xarxa local o a la navegació per Internet. Finalment, veurem els aspectes més importants entorn a l'optimització del sistema per a equips portàtils i quins mecanismes ens ofereix el Windows 7 per millorar el rendiment i la durabilitat de les bateries.

En l'apartat "Administració d'usuaris i grups" es fa una introducció als diferents usuaris i grups disponibles en el sistema operatiu i com podem crear-ne, eliminar-ne o gestionar-los correctament tant utilitzant el mètode tradicional en entorn gràfic com les eines d'administració avançades que proporciona el Windows 7.

En l'apartat "Configuració del protocol de xarxa" es fa una petita introducció al model TCP/IP i s'explica de manera senzilla el funcionament de l'adreçament de la capa 2 que ens permet accedir sense problemes a Internet. A més, s'explica com es configura correctament aquest protocol en el Windows 7 utilitzant la part gràfica de gestió de la xarxa i també les ordres necessàries per fer-ho.

En l'apartat, "Optimització del sistema en ordinadors portàtils", veurem quins mecanismes proporciona el sistema operatiu per millorar el rendiment del sistema o allargar la durada de la càrrega de la bateria segons les nostres necessitats. A més, veurem quines estratègies podem aplicar pel nostre compte per intentar millorar també la durada d'una càrrega. Per finalitzar, estudiarem què són els arxius de xarxa sense connexió i quan és útil utilitzar-los.

Dins d'aquest mòdul professional, utilitzareu aquesta unitat per comprendre el funcionament del sistema operatiu Windows 7. És una unitat amb una part teòrica important per poder fonamentar la pràctica. És altament aconsellable que feu totes les activitats i els exercicis d'autoavaluació un cop llegida i compresa la part teòrica.

Resultats d'aprenentatge

En finalitzar aquest nucli formatiu d'aquesta unitat formativa l'alumne/a:

1. Configura el programari de base, atenent a les necessitats d'explotació del sistema informàtic.

- Planifica, crea i configura comptes d'usuari, grups, perfils, i polítiques de contrasenyes locals.
- Assegura l'accés al sistema mitjançant l'ús de directives de compte i directives de contrasenya.
- Instal·la, configura i verifica protocols de xarxa.
- Analitza i configura diferents mètodes de resolució de noms.
- Optimitza un sistema operatiu lliure per a sistemes portàtils.

1. Administració d'usuaris i grups

Una gestió i una configuració correctes d'usuaris pot facilitar en gran manera l'administració del sistema operatiu i evitar accessos no autoritzats al sistema. Un cop acabada aquesta unitat, heu de ser capaços de donar d'alta, modificar i eliminar usuaris i grups del sistema utilitzant l'entorn gràfic i l'entorn d'ordres.

els sistemes Windows tenen un mode bàsic de funcionament: el mode gràfic. Abans de poder treballar directament en un sistema Windows -si es troba configurat amb seguretat- en la pantalla gràfica ens caldrà indicar un nom d'usuari (*login*) i una contrasenya (*password*); és a dir, sempre ens haurem d'identificar. Tot i disposar d'aquest mode gràfic per defecte, ens podem trobar en situacions d'administració on calgui obrir des de l'entorn gràfic una consola d'administració i entrar ordres des de teclat. De fet, algunes versions de Windows disposen d'un mode d'arrencada que dóna pas a una consola de recuperació que s'utilitza quan les coses van mal dades. També hi pot haver eines de recuperació disponibles des del CDROM/DVD d'instal·lació.

1.1 Usuaris del Windows

En aquesta unitat aprendrem a gestionar usuaris locals en el sistema operatiu Windows 7 Professional. Hem de tenir clar que tots els usuaris i grups que crearem en aquest sistema operatiu seran usuaris locals, és a dir, la seva gestió (alta, baixa i modificació) únicament afectarà l'equip en el qual estem treballant.

1.1.1 Introducció als usuaris locals

S'entén per usuari local la configuració personalitzada que permet que s'iniciï una sessió de treball i s'accedeixi als recursos en l'equip local.

Quan es donen d'alta usuaris en un sistema, els comptes que es generen únicament permeten l'accés local però no l'accés a sistemes remots.

Un compte d'usuari és un conjunt d'informació que indica al Windows els arxius i directoris a què es pot accedir, els canvis que es poden dur a terme en l'equip i les preferències personals com el fons de l'escriptori o el protector de pantalla. Els comptes d'usuari permeten que diferents persones comparteixin el mateix equip, cada una amb els propis arxius i configuracions. Cada persona té accés al seu compte d'usuari mitjançant un nom i una contrasenya.

En el Windows 7, a diferència de versions anteriors com el Windows 9X o ME, és necessari que un usuari es validi en el sistema per poder-hi accedir i treballar. A

més, aquest usuari ha hagut de ser creat per un altre que pertanyi al grup d'usuaris administradors del sistema.

En tota la família Windows NT, des del Windows 2000 al Windows 7, un cop instal·lem el sistema es crea automàticament un compte d'usuari perquè una persona pugui accedir al sistema i administrar-lo com calgui. En aquest cas, durant el procés d'instal·lació es creen les credencials per a l'usuari administrador de l'equip local o usuari principal del sistema (vegeu la figura 1.1). Aquest usuari és el que ha d'iniciar la sessió per primera vegada i el que tindrà els privilegis necessaris per fer les configuracions que consideri oportunes com, per exemple, la creació d'altres comptes d'usuari.

FIGURA 1.1. Creació d'usuari inicial administrador

1.1.2 Tipus de comptes d'usuari

En el Windows 7, com en la majoria de sistemes operatius actuals (tant lliures com de propietat), tenim diferents tipus de comptes d'usuari i es poden fer servir segons les necessitats que tinguem en el nostre entorn. En aquest apartat aprendreu quins són els comptes d'usuari més destacats i quin ús tenen en el Windows 7.

Usuari administrador

L'usuari administrador és l'usuari que té control total sobre l'ordinador i pot crear, modificar i eliminar configuracions del sistema incloent-hi els usuaris i els grups.

L'usuari administrador no s'ha de donar d'alta al sistema, ja que es crea automàticament. Tampoc no el podrem eliminar però sí personalitzar-lo. Aquest usuari

serà el que ens permetrà crear altres comptes d'usuaris, modificar-los, instal·lar i desinstal·lar programari i també modificar la configuració del sistema.

> El compte d'usuari administrador es pot reanomenar, però mai eliminar ni treure del grup d'usuaris administradors.

És important reanomenar el compte d'usuari administrador com també assignar una contrasenya especial per protegir l'accés amb privilegis a l'equip local.

Convidat

Usuari que pot iniciar la sessió per utilitzar part del sistema. No pot instal·lar ni maquinari ni programari, ni crear, modificar o esborrar configuracions de cap mena. Tampoc no pot crear ni gestionar ni eliminar usuaris i grups. El compte de convidat és un compte especial que permet treballar amb l'ordinador amb un programari específic però sense poder dur a terme cap modificació.

Usuari inicial

Usuari creat durant la instal·lació del sistema operatiu i que té els mateixos privilegis que l'usuari administrador.

1.2 Gestió de contrasenyes

> Una contrasenya és un conjunt de caràcters que s'utilitza per autenticar, proveir d'identitat o guanyar accés a un recurs.

Perquè el nostre sistema sigui segur i podem evitar que qualsevol usuari malintencionat o no autoritzat hi pugui accedir, és molt aconsellable protegir tots els comptes d'usuari amb una contrasenya. Podem gestionar les contrasenyes des de la mateixa pantalla que fem servir per modificar informació dels usuaris del sistema

Els usuaris del grup d'administradors són els únics usuaris que poden veure si la resta d'usuaris del sistema tenen una contrasenya assignada, modificar-la o eliminar-la, però mai no tindran accés per veure-la.

1.2.1 Creació de contrasenyes segures

Podem seguir diverses regles per assegurar-nos que la nostra contrasenya és segura davant els intents d'accés no autoritzat al sistema. A tall de resum podem esmentar una sèrie de normes recomanables a l'hora d'escollir una contrasenya:

1. Utilitzeu, com a mínim, vuit caràcters. Exemple: **password**.
2. Utilitzeu tant lletres minúscules com majúscules. Exemple: **Password**.
3. Utilitzeu algun valor numèric. Exemple: **Passw0rd**.
4. Afegiu algun caràcter especial. Exemple: **P@ssw0rd**.

D'aquesta manera s'obté una contrasenya bastant més segura que la proposada inicialment.

1.2.2 Atacs principals contra les contrasenyes

Entre els diferents atacs que podem patir contra les contrasenyes podem destacar els següents:

1. **Força bruta**. Raó principal per la qual s'aconsellen contrasenyes llargues amb nombres i d'altres caràcters. És tracta d'intentar recuperar la contrasenya provant una a una totes les combinacions possibles de caràcters fins a trobar la que permet l'accés.
2. **Atac de diccionari**. Consisteix a intentar utilitzar les paraules d'un diccionari com a possible contrasenya com també les contrasenyes més utilitzades estadísticament.

1.2.3 Contrasenyes en el Windows 7

A l'hora d'assignar o modificar una contrasenya en el Windows 7, tenim diverses opcions:

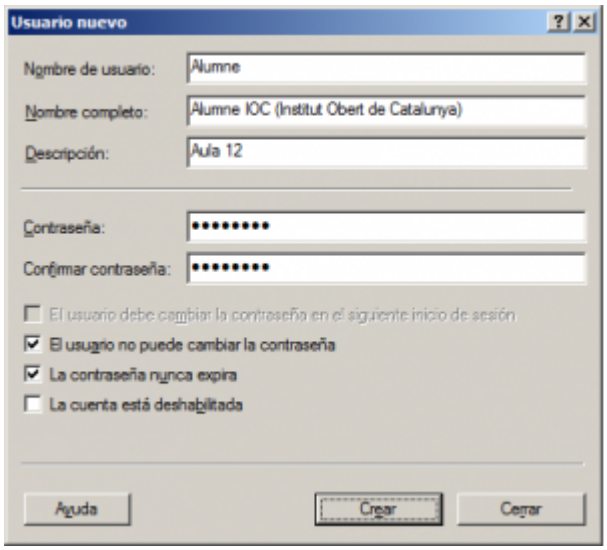
1. **L'usuari ha de modificar la contrasenya a l'inici següent de sessió.** La primera vegada que l'usuari es connecti al sistema, aquest l'obligarà a modificar la seva contrasenya tant si n'hem configurat una o com no. Quan l'usuari intenti accedir a l'equip, aquest sol·licitarà la contrasenya antiga (que hem de comunicar prèviament a l'usuari) i dues vegades la seva nova contrasenya.

2. **L'usuari no pot modificar la contrasenya.** L'usuari podrà accedir al sistema mitjançant una contrasenya (o no) però mai no la podrà modificar. En aquest cas, l'administrador sí que coneixerà la contrasenya, ja que, tant si ha estat assignada com no, ell serà el que l'haurà configurat prèviament en l'equip.

3. **La contrasenya no expira mai.** Tota contrasenya introduïda tindrà validesa fins que l'administrador ho decideixi. Si no activem aquesta opció, la contrasenya caducarà en quaranta dos dies. Aquesta configuració es podrà modificar.

4. **Compte deshabilitat.** Aquesta opció s'utilitza per denegar l'accés a un usuari concret, durant un temps determinat, sense la necessitat d'eliminar-ne les credencials de l'ordinador al qual no volem permetre l'inici de sessió. Sense aquesta opció hauríem d'eliminar el compte complet d'usuari amb tota la seva informació personal durant el temps de denegació d'accés i crear-lo novament un cop finalitzat. Vegeu la figura 1.2.

FIGURA 1.2. Creació d'usuari

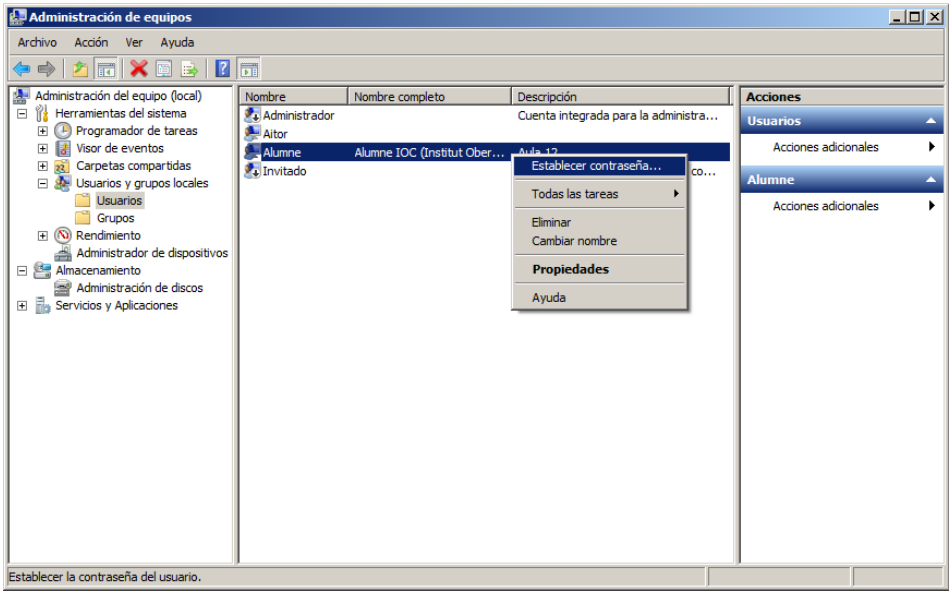


Visiteu la secció "Annexos" del web d'aquesta unitat per a descarregar-vos una pràctica relacionada amb la gestió d'usuaris i contrasenyes al Windows 7.

1.2.4 Modificació de la contrasenya

Una de les accions que pot fer l'administrador del sistema amb els usuaris creats és modificar-ne la contrasenya (vegeu la figura 1.3). És important tenir clar que com a administradors mai no podreu veure la contrasenya dels usuaris del sistema però sí modificar-la o, simplement, saber si un usuari en concret té una contrasenya o no per accedir al sistema. Per tant, sempre podreu assignar noves contrasenyes però mai recuperar les antigues en cas de pèrdua.

FIGURA 1.3. Modificació de contrasenya



És important tenir en compte que, si fem aquesta acció, serà necessari informar l'usuari sobre aquest canvi perquè pugui tornar a iniciar la sessió en el nostre sistema.

1.3 Perfils d'usuaris locals

Cada vegada que es genera un nou usuari i aquest accedeix al sistema per primera vegada, el mateix sistema genera una configuració personal i específica per a l'usuari. Entre aquestes configuracions podem destacar l'escriptori, el tauler de control i les aplicacions.

Dins del directori arrel de la instal·lació del sistema operatiu (generalment c:\) hi ha una carpeta anomenada *Usuaris* (anteriorment, *Documents and Settings*), que conté les carpetes personals dels usuaris. Cadascuna d'elles inclou nombrosos arxius i carpetes.

Cada una d'aquestes carpetes conté informació sobre l'inici de sessió personalitzada de l'usuari com, per exemple: accessos directes de l'escriptori, fons de pantalla, protector de pantalla, programes instal·lats, etc. D'aquesta manera, totes les modificacions que els usuaris facin en la seva sessió mai no afectaran la resta d'usuaris del sistema com passava en sistemes operatius anteriors.

Totes aquestes carpetes, arxius i documents no podran ser eliminats ni modificats per cap usuari que no sigui el seu propi propietari. Únicament l'administrador del sistema o un usuari amb privilegis suficients els podria modificar.

Un altre dels directoris dignes de menció és *Default*, que per defecte es trobarà ocult en el mateix directori Usuaris. Aquest directori, anomenat anteriorment *Default User*, conté la configuració per defecte de qualsevol nou usuari que creem

en el sistema, és a dir, qualsevol nou usuari que creem agafarà inicialment el contingut i les configuracions que hi ha en aquest directori. El directori *Default* i tot el seu contingut es copiaran amb el seu nom, i qualsevol modificació que aquest usuari faci només l'afectarà a ell mateix.

Si pel motiu que fos, s'esborrés accidentalment el directori d'un usuari determinat, en l'inici següent de sessió es tornaria a fer una còpia del directori *Default*.

En cada un dels perfils podem trobar diferents directoris, alguns d'ells es descriuen a continuació:

- **Dades de programa** el qual emmagatzema les dades específiques dels programes.
- **Cookies**. Emmagatzema informació sobre les preferències de l'usuari.
- **Entorn de xarxa**. Desa els accessos directes a opcions d'"Els meus llocs de xarxa".
- **Escriptori**. En el qual es desen les icones que apareixen a l'escriptori de l'usuari incloent-hi arxius, directoris i accessos directes.
- **Preferits**. En aquest directori es desen els accessos directes als programes i aplicacions preferides i les seves ubicacions.
- **Configuració local**. Emmagatzema els arxius de dades de programes, historial i arxius temporals.
- **Impressores**. Desa els accessos directes als elements de la carpeta impressores.
- **Menú inici**. Es desen els accessos directes que podeu trobar al menú inici del nostre equip.
- **Els meus documents**. Desa tots els documents de l'usuari.
- **Les meves imatges**. Desa els elements d'imatge de l'usuari.
- **Plantilles**. Conté els accessos directes a les plantilles creades per l'usuari.
- **Recent**. En aquest directori s'emmagatzemen els accessos directes utilitzats recentment.
- **SendTo**. Desa els accessos directes de les utilitats de control dels documents.

Les carpetes Configuració local, Dades de programa, Entorn de xarxa, Impressores, Plantilles, Recent i SentTo estan ocultes i no són visibles a no ser que ho indiqueu expressament, marcant "*Mostrar tots els arxius i carpetes ocultes*" en la fitxa "*Veure*" d'*Opcions de carpeta* al menú *Eines*.

Així mateix, podem trobar també fins a tres arxius anomenats NTuser.dat, que conté dades del registre de l'usuari, NTuser.dat.LOG, que és un arxiu on es desaran els canvis anteriors a la darrera modificació del registre i poder resoldre possibles problemes a l'hora de produir-se i NTuser.man el qual conté les dades del registre de l'usuari però és un arxiu de només lectura i, per tant, no es guarden els canvis.

1.4 Grups d'usuaris

S'entén per *grup local* l'entitat administrativa que és capaç d'incloure un conjunt d'usuaris o fins i tot d'altres grups de tal manera que tots els permisos o privilegis concedits a aquest grup, s'heretaran directament per tots els usuaris o grups que hi pertanyin. Tot usuari del nostre equip ha de pertànyer necessàriament a un grup per estar identificat en el sistema.

Tots els usuaris que donem d'alta en el nostre sistema han de pertànyer de manera predeterminada a un grup concret. Per tant, sempre que en el nostre sistema vulguem modificar els privilegis d'un o més usuaris, ho podem fer directament sobre els usuaris o sobre un grup que, normalment, contindrà més d'un usuari.

Els grups d'usuaris es gestionen des del mateix lloc on es gestionen els comptes d'usuaris. A continuació es mostren els grups que podem trobar per defecte en el Windows 7:

1. **Administradors.** Usuaris amb accés complet i sense cap tipus de restricció al sistema. A aquest grup pertanyen l'usuari administrador i tots els usuaris autoritzats per administrar gairebé tot l'ordinador local.
2. **Duplicadors.** Usuaris que poden replicar arxius en un domini.
3. **Convidats.** De manera predefinida, els usuaris del grup "Convidats" tenen el mateix accés que els membres del grup "Usuaris" excepte el compte de l'usuari "Convidat" que té més restriccions.
4. **Operadors de configuració de xarxa.** Els membres d'aquest grup poden tenir certs privilegis per administrar la configuració de les característiques de xarxa.
5. **Operadors de còpia de seguretat.** Els membres d'aquest grup poden invalidar restriccions de seguretat amb l'únic propòsit de fer còpies de seguretat o restaurar arxius.
6. **Usuaris.** Els usuaris que pertanyen a aquest grup no poden fer canvis accidentals o intencionats en el sistema, però poden executar la majoria d'aplicacions.
7. **Usuaris avançats.** Aquests usuaris tenen drets administratius limitats.
8. **Usuaris d'escriptori remot.** Als membres d'aquest grup es permet l'inici de sessió remot.
9. **Lectors del registre d'esdeveniments.** Els membres d'aquest grup poden llegir els registres d'esdeveniments de l'equip local.
10. **Operadors criptogràfics.** Els usuaris que pertanyen a aquest grup estan autoritzats a fer operacions criptogràfiques.

11. **Usuaris COM distribuïts.** Els membres d'aquest grup poden iniciar, activar i utilitzar objectes de COM distribuïts en l'equip.

12. **Usuaris del monitor de sistema.** Els membres d'aquest grup tenen accés a les dades del comptador de rendiments de manera local i remota.

13. **Usuaris del registre de rendiment.** Els membres d'aquest grup poden programar comptadors de registre i rendiment, habilitar proveïdors de seguiment i recopilar seguiments d'esdeveniments localment i mitjançant l'accés remot a aquest equip.

1.5 Control de comptes d'usuari (UAC)

El control de comptes d'usuari (UAC, de l'anglès *user account control*) és un nou conjunt de tecnologies introduït en el Windows Vista que té com a objectiu evitar que programes maliciosos (*malware*) puguin causar problemes al sistema operatiu. Amb l'UAC, qualsevol aplicació s'ha d'executar amb permisos d'usuari no administrador tret que el mateix usuari permeti l'execució amb permisos administratius.

En aquesta versió del Windows, i gràcies a l'UAC, els usuaris estàndard i els usuaris administradors, executen aplicacions en el context de seguretat dels usuaris estàndard.

Un *token* és un conjunt de bytes que expressa el nivell de privilegi que té un usuari concret.

Quan un usuari accedeix al sistema, el sistema operatiu crea un testimoni (*token*) d'accés per a ell. Aquest testimoni conté informació sobre el nivell d'accés que té, i inclou identificadors de seguretat específics (SID) i privilegis del Windows. Sempre que un administrador accedeix al sistema, aquest crea dos testimonis d'accés totalment independents, l'un concedeix accés d'usuari estàndard, i l'altre accés d'administrador. El testimoni d'usuari estàndard conté exactament la mateixa informació específica d'usuari que el testimoni amb accés administrador, però se n'han eliminat els privilegis del Windows administratius i els SID. El testimoni d'accés d'usuari estàndard s'utilitza per iniciar aplicacions que no fan tasques administratives o aplicacions d'usuari estàndard.

Figura 1.4. UAC Usuari administrador

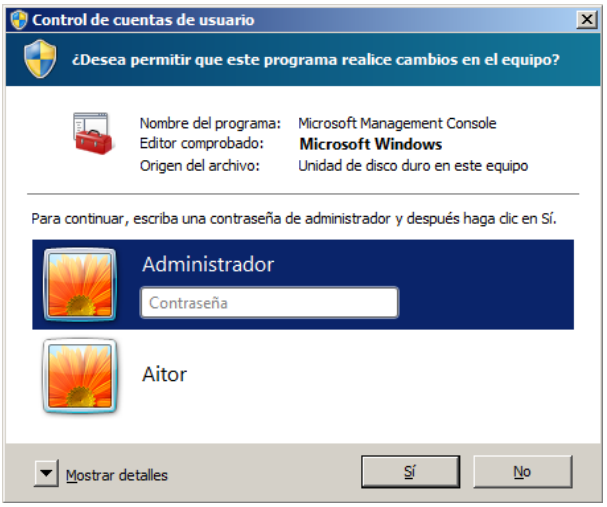
Quan un usuari que pertany al grup d'administradors locals ha d'executar alguna aplicació que du a terme tasques administratives (aplicacions d'administrador),

el Windows 7 demana a aquests usuaris que canviïn o elevin el seu context de seguretat d'usuari estàndard a usuari administrador. Aquesta experiència d'usuari d'administrador predeterminat s'anomena *mode d'aprovació d'administrador*. En aquest mode, les aplicacions requereixen un permís especific per executar-se com a aplicacions d'administrador.

Quan s'ha iniciat una aplicació d'administrador, apareix un missatge de control de comptes d'usuari de manera predeterminada (vegeu la figura 1.4). Si l'usuari és un administrador, el missatge dóna l'opció de permetre o evitar que s'inicïi l'aplicació.

Si l'usuari és un usuari estàndard i no pertany al grup d'administradors, pot especificar el nom d'usuari i la contrasenya d'un usuari que sigui membre del grup d'administradors locals. (Veure la figura 1.5).

Figura 1.5. UAC, usuari no administrador



En dissenyar una aplicació per al Windows 7, els programadors de programari han d'identificar la seva aplicació com a aplicació d'administrador o aplicació d'usuari estàndard. Si una aplicació no s'ha identificat com a aplicació d'administrador, el Windows 7 la tractarà com una aplicació d'usuari estàndard. Tot i això, els administradors també poden marcar una aplicació perquè es tracti com a aplicació d'administrador.

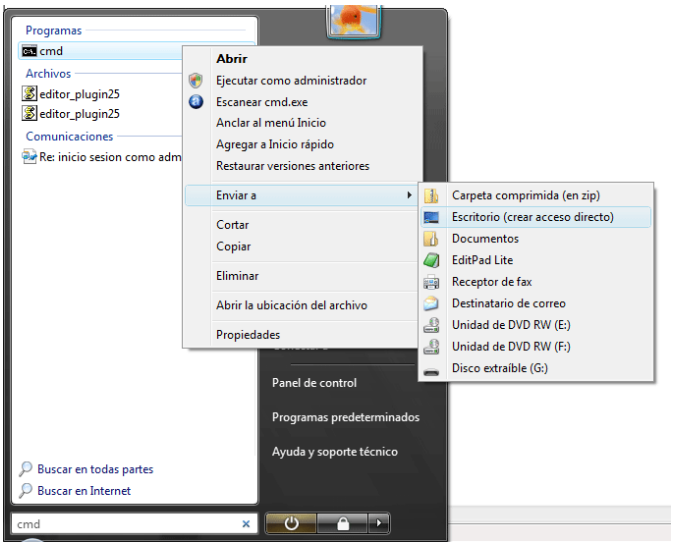
Anem a veure'n un exemple tot creant un accés directe a la consola i donant privilegis d'administrador:

Fins ara heu vist que la gestió d'usuaris en els sistemes Windows es pot fer fàcilment per mitjà d'eines gràfiques. ÉS interessant, però, disposar d'una consola que ens permeti introduir ordres. Aquesta gestió convé realitzar-la amb privilegis d'administrador.

Un cop heu accedit a l'entorn gràfic, per iniciar una consola se us recomana seguir els següents passos:

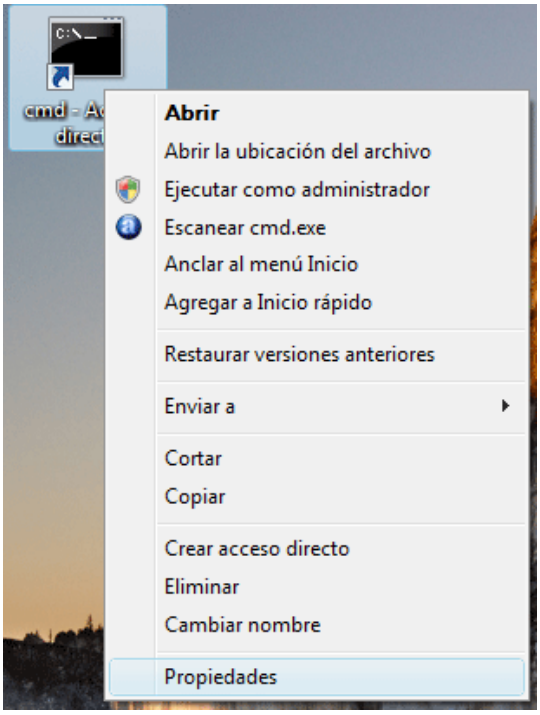
- Anar a Inici i al quadre de cerca i escrivim: cmd. Això fa que a la llista de programes aparegui la icona de la consola d'ordres (figura 1.6).

FIGURA 1.6. Llista de programes amb la icona de consola



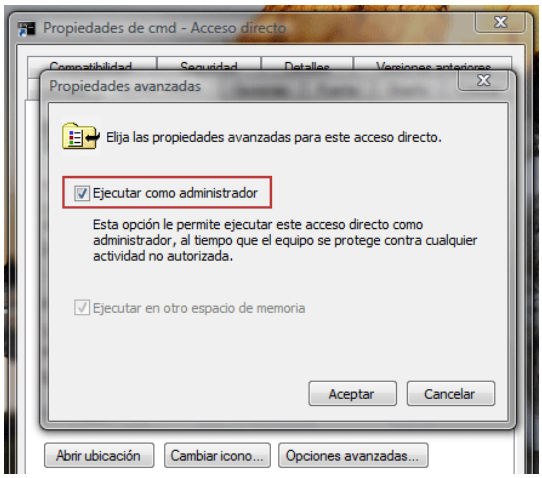
- Per fer més fàcil l'accés posterior a l'aplicació ens podeu situar amb el ratolí damunt la icona i crear un accés directe a l'escriptori tot escollint "Enviar a l'escriptori (crea accés directe)" (figura 1.7).

FIGURA 1.7. Propietats de l'accés directe a consola



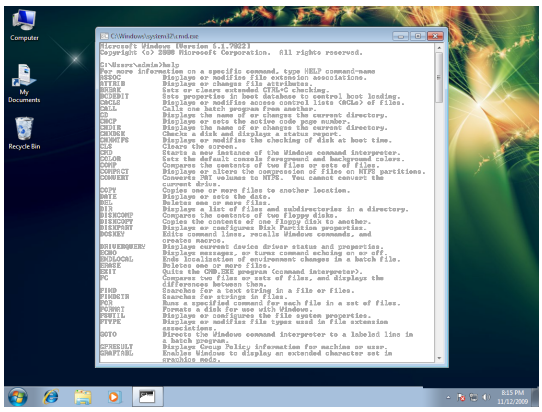
- Per donar més privilegis d'administrador a aquesta consola, ens situem damunt l'accés directe i escollim "Propietats". A les "Opcions avançades" marquem la casella "Executar com a administrador" i acceptem. Tanquem les finestres i ja tenim un accés directe a una consola d'administració (figura 1.8).

FIGURA 1.8. Propietats de l'accés directe a consola



Dins aquesta finestra (figura 1.9), ja podeu introduir les ordres. La primera ordre que podeu provar és la de l'ajuda: HELP

FIGURA 1.9. La consola



A la taula 1.1 disposeu d'una llista d'ordres bàsiques per utilitzar a la consola de Windows. A Internet disposeu de llocs web que amplien aquesta llista i d'altres que descriuen cada ordre.

TAULA 1.1. Ordres bàsiques de la consola

Ordre	Descripció
DATE	Mostra data. També permet modificar-la.
TIME	Mostra hora. També permet modificar-la.
DIR	Mostra tots els fitxers de la ruta on ens trobem.
CD	Permet canviar de carpeta.
MD carpeta	Crea una carpeta amb el nom 'carpeta'.
RMDIR carpeta	Elimina la carpeta 'carpeta'.
TREE	Mostra l'estructura de carpetes.
NOTEPAD fitxer.cmd	Programa extern que permet la creació d'un fitxer, en aquest cas un fitxer d'ordres.
.\fitxer.cmd	Crida a un fitxer d'ordres, tot executant les línies d'aquest una després de l'altra.
TYPE fitxer.txt	Mostra el contingut del fitxer especificat.

TAULA 1.1 (continuació)

Ordre	Descripció
DEL fitxer.txt	Elimina el fitxer especificat.
ATTRIB	Mostra i permet canviar atributs de fitxers.
SHUTDOWN	Permet apagar el sistema.
SYSTEMINFO	Mostra informació diversa del sistema.

Al lloc web **CommandWindows.com** (bit.ly/2OY1eJN) teniu una extensa llista d'ordres amb la seva descripció.

1.6 Dominis, grups de treball i grups domèstics

Els dominis, els grups de treball i els grups domèstics representen diferents formes d'organitzar equips en les xarxes. La diferència principal entre ells és la forma d'administrar els equips i altres recursos de les xarxes.

Tots els equips que executen Windows en una xarxa, han de ser part d'un grup de treball o d'un domini. Els equips que executen Windows en xarxes domèstiques també poden ser part d'un grup en la llar (o grup domèstic), però no és un requisit.

Generalment, els equips de xarxes domèstiques formen part d'un grup de treball i, probablement, d'un grup en la llar, i els equips de xarxes del lloc de treball formen part d'un domini.

1.6.1 En un grup de treball

- Tots els equips es troben en el mateix nivell, no hi ha cap equip que tingui el control sobre un altre.
- Cada equip disposa d'un conjunt de comptes d'usuari. Per iniciar sessió en qualsevol equip del grup de treball, heu de disposar d'un compte en l'equip.
- Normalment, no hi ha més de vint equips.
- Un grup de treball no està protegit amb contrasenya.
- Tots els equips han de trobar-se a la mateixa xarxa local o subxarxa.

1.6.2 En un grup domèstic

- Els equips d'una xarxa domèstica poden pertànyer a un grup de treball, però també poden pertànyer a un grup domèstic. Un grup domèstic permet

compartir fàcilment imatges, música, vídeos, documents i impressores amb altres persones d'una xarxa domèstica.

- El grup en la llar està protegit amb contrasenya, però solament és necessari escriure la contrasenya una vegada, en agregar l'equip al grup en la llar.

1.6.3 En un domini

- Un o més equips són servidors. Els administradors de xarxa utilitzen els servidors per controlar la seguretat i els permisos de tots els equips del domini. Així resulta més senzill efectuar canvis, ja que aquests s'apliquen automàticament a tots els equips. Els usuaris de domini han de proporcionar una contrasenya o algun altre tipus de credencial cada vegada que accedeixin al domini.
- Si es disposa d'un compte d'usuari en el domini, es pot iniciar sessió en qualsevol equip del domini sense necessitat de disposar d'un compte en aquest equip.
- Habitualment nomes es poden fer canvis limitats a la configuració d'un equip perquè els administradors de xarxa amb freqüència desitgen garantir un nivell d'homogeneïtat entre els equips.
- Un domini pot incloure milers d'equips.
- Els equips poden trobar-se en diferents xarxes locals.

1.6.4 Navegació

La navegació és el procés de buscar altres ordinadors o recursos compartits a la xarxa Windows. Heu de tenir en compte que és el mateix que utilitzar un navegador web, a part de la idea general de buscar i intentar descobrir el que podem trobar. D'altra banda, navegar per la xarxa de Windows és semblat a fer-ho per la web, ja que tots els recursos als que podem accedir poden ser modificats sense previ avís.

Abans de l'existència del navegador, els usuaris havien de conèixer el nom de l'ordinador al que es volien connectar, després havien de teclejar manualment una adreça UNC en el gestor d'arxius o l'aplicació implicada per poder accedir al recurs. Un exemple d'adreça UNC pot ser `\\servidorIOC\apunts`, o també `\\192.168.1.1\recursos`.

La navegació és molt més senzilla, ja que permet examinar els continguts de la xarxa fent ús d'una interfície de l'entorn de xarxa dels clients Windows.

1.6.5 Controlador de domini

Un controlador de domini en un domini Windows funciona de manera molt similar a un servidor NIS en una xarxa Unix, mantenint una base de dades del domini que conté la informació dels usuaris i grups, així com els seus serveis associats. Les responsabilitats d'un controlador de domini estan principalment centrades en la seguretat, incloent l'autenticació o la tasca de permetre o denegar l'accés als recursos del domini a un determinat usuari. Això es realitza normalment gràcies a l'ús d'un nom d'usuari i una clau. El servei que manté la base de dades en els controladors de domini es denomina *Security Account Manager (SAM).*

El model de seguretat de Windows gira entorn dels identificadors de seguretat (SIDs) i les llistes de control d'accés (ACLs). Els identificadors de seguretat són utilitzats per representar objectes en un domini, que inclouen (però no limiten) als usuaris, els grups, els ordinadors i els processos. Els SIDs s'escriuen normalment en un formulari *ASCII* com a camps separats per guions, tal com es mostra en el següent exemple:

```
S-1-5-21-1638239387-7675610646-9254035128-545
```

Un SID comença amb el caràcter "S", seguit d'un guió. El número immediatament posterior al primer guió es denomina identificador relatiu (RID) i és un nombre únic dins del domini que identifica a un usuari, un grup, un ordinador o qualsevol altre objecte. El número RID és anàleg al identificador d'usuari (UID) o a l'identificador de grup (GID) en un sistema Unix o dins d'un domini NIS.

Les ACLs (llistes de control d'accés), proveeixen la mateixa funcionalitat que els permisos dels arxius comuns en els sistemes Unix (rwx). No obstant això, les ACLs són més versàtils. Els permisos dels arxius Unix només poden establir permisos per al propietari del recurs, el grup al qual aquest fitxer pertany, i "uns altres", es a dir, qualsevol altre usuari. Les ACLs de Windows permeten establir permisos individuals per a qualsevol nombre arbitrari d'usuaris i/o grups. Les ACLs estan constituïdes per una o més entrades de control d'accés (ACE - Access Control Entries), cadascuna de les quals contenen un SID i drets d'accés associats a ells.

1.6.6 Autenticació

Quan un usuari tecleja el seu usuari i clau per ingressar en un domini Windows, s'invoca un "desafiament de seguretat" i un protocol de resposta entre l'ordinador client i el controlador de domini per verificar que l'usuari i la clau són vàlids. Seguidament el controlador de domini envia el SID de nou al client, qui ho utilitzarà per crear un token de seguretat (SAT - Security Access Token) que és vàlid únicament per a aquest sistema, que serà utilitzat per a autenticacions posteriors. Aquest senyal d'accés conté la informació sobre l'usuari codificada en

el seu interior, la qual inclou el nom d'usuari, el grup i els permisos que l'usuari posseeix en el domini. En aquest moment, l'usuari està autenticat en el domini.

Posteriorment, quan el client intenta accedir a un recurs compartit dins del domini, el sistema client entra en un desafiament de seguretat i un intercanvi de respostes amb el servidor del recurs. Seguidament el servidor entra en un altre desafiament de seguretat per a comprovar que el client és vàlid. El que succeeix realment és que el servidor utilitza la informació que ha obtingut del client per fer-se passar per aquest i autenticar-se ell mateix davant el controlador de domini. Si el controlador de domini, veient les seves credencials, envia un SID al servidor, aquest l'utilitzarà per crear el seu propi SAT per al client, d'aquesta forma habilita l'accés als seus recursos locals en benefici del client. En aquest punt, el client es troba autenticat per als recursos del servidor i se li permet accedir a ells. El servidor utilitza el SID emmagatzemat en el SAT per determinar que permisos de modificació i ús posseeix el client per al recurs en qüestió, això ho aconsegueix comparant-ho amb les entrades de les ACLs del recurs.

Encara que aquest mètode d'autenticació pugui semblar massa complicat, permet als clients l'autenticació sense enviar les claus en text pla a través de la xarxa, i és molt més difícil de trencar que la seguretat que proporcionen els grups de treball.

1.6.7 Dominis Active Directory

Un directori és una estructura jeràrquica que emmagatzema informació sobre els objectes existents en una xarxa i un servei de directori proporciona mètodes per a emmagatzemar les dades del directori i posar-les a disposició dels administradors i del usuaris de la xarxa.

A partir de Windows 2000, Microsoft va introduir l'Active Directory (Directori Actiu), un pas més enllà dels dominis de Windows NT. Amb Active Directory, el model d'autenticació està centrat al voltant d'LDAP, i el servei de noms ho subministra un servidor DNS en lloc d'un servidor WINS. Els dominis en Active Directory es poden organitzar en una estructura jeràrquica en arbre, en la qual, cada controlador de domini és fix, no hi ha distinció entre controlador primari i secundari, com passava en els dominis Windows NT.

Active Directory no fa canvis fonamentals en la forma en què funcionen els dominis en Windows de cara als usuaris finals però si introdueix algunes estructures de domini importants que podrien afectar a la forma d'aproximar-se al disseny del domini. Active Directory utilitza dominis com a unitats principals de l'estructura lògica. Els dominis ajuden a organitzar l'estructura de la xarxa ajustant-se a l'organització de l'empresa, ja sigui política o geogràficament.

El Directori Actiu compta amb les següents característiques:

- Incorpora un **directori** que és un magatzem de dades per a guardar informació sobre els objectes (aquests objectes inclouen normalment recursos

compartits com servidors, arxius, impressores i comptes d'usuari i d'equips en xarxa).

- Incorpora un conjunt de regles (**esquema**) bàsiques que defineixen les classes d'objectes i els atributs continguts en el directori (els atributs i les dades també són conegudes com a metadades), les restriccions i els límits en les instàncies d'aquests objectes així com el format dels seus noms.

Conceptes sobre els usuaris

Els comptes d'usuari representen a una persona i es denominen **principals de seguretat** dins del Directori Actiu, ja que són objectes del directori als que s'assignen automàticament identificadors de seguretat per a iniciar sessions en la xarxa i tindre accés als recursos.

Una compte d'usuari permet que un usuari inicii sessions en equips i dominis amb una identitat que es pot autenticar i autoritzar per a tenir accés als recursos del domini. Cada usuari que es connecta a la xarxa ha de tenir la seva pròpia compta d'usuari única i la seva contrasenya. Per tant, un compte d'usuari s'utilitza per a:

- Autentificar la identitat de l'usuari
- Autoritzar o denegar l'accés als recursos del domini
- Administrar altres principals de seguretat
- Auditar les accions realitzades per l'usuari mitjançant el seu compte

Els usuaris en Active Directory poden ser de dos tipus:

- **Usuaris globals**. Aquests comptes es creen en els servidors que siguin controladors de domini i poden utilitzar-se per a connectar-se als dominis en que s'han creat i a d'altres dominis en els que es confia (dominis de confiança).
- **Usuaris locals**, Aquests comptes d'usuari es creen en estacions de treball o servidors que no siguin controladors de domini i, per tant, no poden utilitzar-se per a connectar-se a cap domini. Un usuari local és un compte a la que es poden assignar permisos i drets per a l'equip local en el que s'ha creat.

Per defecte, durant la instal·lació d'un equip servidor, es creen dos comptes d'usuari que poden utilitzar-se per a iniciar sessió i tenir accés als recursos. Aquests comptes són:

- El compte de l'usuari **Administrador** que permet administrar l'equip en el que s'ha creat. Aquest compte pot ser reanomenat però mai podrà ser eliminat, deshabilitat ni tret del grup local d'Administradors. És recomanable reanomenar i assignar una contrasenya segura a aquest compte així com crear altres comptes d'usuari administrador per millorar la seguretat del servidor.

- El compte de l'usuari **Convidat**. Normalment aquest compte està deshabilitat (i l'hauríem de mantenir d'aquesta manera) però es podria habilitar si es desitja que algun usuari pugui connectar-se a l'equip o al domini d'aquesta forma tot i que, heu de tenir en compte, que no necessita cap contrasenya per iniciar sessió. Aquest compte pot eliminar-se i reanomenar-se.

Els perfils d'usuari

Un perfil d'usuari és una de les eines més potents per a configurar l'entorn de treball dels usuaris en xarxa.

Es poden especificar l'aspecte de l'escriptori, la barra de tasques, el contingut de menú Inici (incloent els programes o aplicacions), etc.

Cada usuari pot tenir el seu perfil que està associat al seu nom d'usuari i que es guarda en l'estació de treball (així doncs, aquells usuaris que es connecten a diferents estacions de treball poden tenir un perfil diferent en cada un d'elles). Aquest perfil s'anomena **Perfil local** perquè només és accessible des de l'estació on ha estat creat.

Els usuaris que es connecten a un servidor poden tenir, a més, perfils en aquest servidor. D'aquesta manera, es pot accedir al perfil independentment de l'estació de treball en la que s'esteu connectats. Aquest perfil s'anomena **Perfil de xarxa** ja que es pot accedir a ell des de qualsevol estació de treball que estigui connectada a la xarxa.

Hi ha dos tipus de perfils de xarxa:

- **Perfil mòbil**: Aquest tipus de perfil és assignat a cada usuari pels administradors però pot ser modificat per l'usuari i els canvis efectuats romandran un cop hagi finalitzat la sessió.

- **Perfil obligatori**: Aquest tipus de perfil té la mateixa estructura que el **perfil mòbil** però assegura que els usuaris puguin treballar en un entorn comú. Per tant, podrà ser modificat per l'usuari però tots els canvis que aquest realitzi en l configuració, es perdran un cop hagi finalitzar la sessió. Únicament podrà ser modificat (i guardats els canvis) per usuaris que pertanyin al grup d'administradors.

Els perfils mòbils

Com ja heu vist anteriorment, aquests tipus de perfils són assignats a cada usuari, poden esser modificats per ells mateixos i els canvis produïts romandran un com hagi finalitzat la connexió.

Per què això sigui possible, les dades de registre de l'usuari es desaran en un arxiu anomenat NTuser.dat (dins del subdirectori de perfils locals amb el nom de l'usuari tal i com hem vist anteriorment). Qual l'usuari es connecta, el contingut d'aquest arxiu es copia a la categoria **HKEY_CURRENT_USER** del registre. Quan l'usuari realitzi canvis al seu perfil, aquests es guardaran automàticament a

l'arxiu NTuser.dat al finalitzar la connexió, d'aquesta forma, els canvis produïts per l'usuari es mantindran la propera vegada que aquest inicïi sessió.

Els perfils obligatoris
Com ja heu vist anteriorment, aquest tipus de perfils, tenen la mateixa estructura que els perfils mòbils però asseguren que els usuaris treballin en un entorn comú. Per tant, els usuaris poden modificar-los però els canvis realitzats es perden al finalitzar la connexió i únicament es mantindran si aquests canvis són realitzats per usuaris que tinguin permisos d'administrador.

Per a aconseguir això, es desen les dades del registre d'usuari en un arxiu anomenat NTuser.man. Quan l'usuari es connecta, aquest arxiu es copia a la categoria **HKEY_CURRENT_USER** del registre. Quan l'usuari realitzi canvis en el seu perfil, aquests no es desaran en l'arxiu al finalitzar la sessió, d'aquesta manera, els canvis realitzats no es mantindran la propera vegada que l'usuari inicii sessió en l'equip.

Conceptes sobre els grups

Els comptes de grup representen a un grup i, a l'igual que els usuaris, es denominen principals de seguretat dins de l'Active Directory, ja que són objectes del directori als que s'assignen automàticament identificadors de seguretat. Podem trobar dos grups diferenciats:

- **Els grups de seguretat**: Aquests tipus de grups es mostren a dins les llistes de control d'accés discrecional (DACL) que és el lloc on estan definits els permisos sobre els recursos i els objectes. Aquests grups de seguretat es poden utilitzar també com entitats de correu electrònic, d'aquesta manera, si envieu un missatge de correu electrònic a aquest grup, el missatge serà rebut automàticament per a tots els membres del grup de seguretat.
- **Els grups de distribució**: En aquest tipus de grups no és possible habilitar la seguretat ja que no apareixen en les llistes de control d'accés discrecional (DACL). Els grups de distribució només es poden utilitzar amb aplicacions de correu electrònic (como ara Microsoft Exchange) per a enviar correu electrònic als grups dels usuaris.

Un grup de seguretat es pot convertir en un grup de distribució (i al contrari) en qualsevol moment. Cada grup de seguretat i de distribució té un àmbit que identifica l'abast d'aplicació del grup. Existeixen quatre tipus de grups diferenciats en funció del seu abast d'aplicació.

- **Grups d'àmbit universal**: Aquests tipus de grups (que únicament es poden crear en equips servidors que tinguin instal·lat el Directori Actiu) poden tenir com a membres a altres grups universals, grups globals i comptes de qualsevol domini de Windows i els hi podeu concedir permisos de qualsevol domini. També es poden denominar **grups universals**.

- **Grups d'àmbit global**: Aquests tipus de grups (que únicament es poden crear en equips servidors que tinguin instal·lat el Directori Actiu) poden tenir com a membres a grups globals i comptes únicament del domini en el que s'ha definit el grup i els hi podeu concedir permisos de qualsevol domini. Aquests grups també es poden denominar **grups globals**.

- **Grups d'àmbit global de domini**: Aquests tipus de grups (que únicament es poden crear en equips servidors que tinguin instal·lat el Directori Actiu) poden tenir com a membres a grups universals, grups globals, grups locals de domini del seu propi domini i comptes de qualsevol domini de Windows i únicament es poden utilitzar per a concedir permisos en el domini que conté el grup. També poden ser anomenats **grups de domini local**

- **Grups locals**: Aquests tipus de grups únicament els podem trobar en equips que executin una versió client de Windows o que siguin servidors membres (equips Windows Server però que no tinguin el Directori Actiu instal·lat). Poden tenir com a membre a comptes locals de l'equip en el que s'han creat i, si aquell equip forma part d'un domini, podrà tenir també comptes i grups globals del propi domini i dels dominis de confiança i es poden utilitzar per a concedir permisos en l'equip en el que s'ha creat aquest grup.

2. Configuració del protocol de xarxa

Entre tots els elements essencials per a l'existència humana, la necessitat d'interactuar està per sota de la necessitat de sustentar la vida. La comunicació és gairebé tan important per a nosaltres com l'aire, l'aigua i un lloc on viure.

Els mètodes que l'ésser humà ha utilitzat per compartir idees i informació han canviant al llarg de la història i estan en evolució constant. Mentre que la xarxa humana ha estat limitada a converses cara a cara, el progrés dels mitjans ha ampliat l'abast de les nostres comunicacions. Des de la premsa escrita fins a la televisió, cada nou avenç ha millorat la comunicació.

Com amb cada avenç en la tecnologia de la comunicació, la creació i la interconnexió de xarxes de dades sòlides té un efecte profund i han permès que l'ésser humà realitzi de forma més eficient la seva feina facilitant que les empreses exigeixin dia a dia majors reptes a qui els desenvolupen. D'aquesta forma, s'ha arribat a alternatives de gran impacte a través del temps com el correu electrònic, Internet, televisió per cable, etc.

2.1 Xarxes d'àrea local

Les infraestructures de xarxa poden variar molt en els aspectes següents:

- Mida de l'àrea coberta
- Quantitat d'usuaris connectats
- Quantitat i tipus de serveis disponibles

LAN: acrònim de l'anglès *local area network* o xarxa d'àrea local.

Una xarxa individual cobreix una única àrea geogràfica i proporciona serveis i aplicacions a persones dins d'una estructura organitzacional comuna, com una empresa, un campus o una regió. Aquest tipus de xarxa s'anomena **xarxa d'àrea local** (LAN). Com a norma general, una LAN està administrada per una única organització. El control administratiu que regeix les polítiques de seguretat i control d'accés està implementat en l'àmbit de xarxa.

2.2 Internet

Tot i que l'ús d'una LAN aporta beneficis, la majoria d'usuaris necessita comunicar-se amb recursos d'altres xarxes fora de l'organització local.

Els exemples d'aquest tipus de comunicació inclouen:

- Enviar un correu electrònic a un amic d'un altre país
- Accedir a notícies o productes d'un lloc web
- Obtenir un arxiu de l'ordinador del veí
- Enviar un missatge instantani a un familiar d'una altra ciutat
- Seguir una activitat d'un equip esportiu amb el telèfon mòbil.

2.2.1 Internetwork

Una malla global de xarxes interconnectades (*internetworks*) cobreix aquestes necessitats de comunicació humanes. Algunes d'aquestes xarxes interconnectades pertanyen a grans organitzacions públiques o privades com agències governamentals o empreses industrials, i estan reservades per al seu ús exclusiu.

La *internetwork* més coneguda, àmpliament utilitzada i a la qual accedeix el públic en general és Internet.

Internet es crea per la interconnexió de xarxes que pertanyen als proveïdors de serveis d'Internet (ISP). Aquestes xarxes ISP es connecten entre elles per proporcionar accés a milions d'usuaris a tot el món. Garantir la comunicació efectiva per mitjà d'aquesta infraestructura diversa requereix l'aplicació de tecnologies i protocols consistents i reconeguts comunament, com també la cooperació de moltes agències d'administració de xarxes.

2.3 Protocols

Tota comunicació, cara a cara o per una xarxa, està regida per regles predeterminades denominades *protocols*.

Aquests protocols són específics de les característiques de la conversa. En les nostres comunicacions personals quotidianes, les regles que apliquem per comunicar-nos utilitzant un mitjà, com el telèfon, no són necessàriament les mateixes que els protocols que s'utilitzen en un mitjà diferent, com escriure una carta.

Una *suite* de protocols és un conjunt de protocols de comunicació que implementen la pila (*stack*) de protocols de les xarxes en què s'executen.

L'èxit de la comunicació entre els *hosts* d'una xarxa requereix la interacció d'una gran quantitat de protocols diferents. Un grup de protocols interrelacionats que són necessaris per a dur a terme una funció de comunicació es denomina **suite de**

protocols. Aquests protocols s'implementen en el programari i en el maquinari que està carregat en cada *host* i dispositiu de xarxa.

Les *suites* de protocols de *networking* descriuen processos com els següents:

- El format o estructura del missatge.
- El mètode pel qual els dispositius de *networking* comparteixen informació sobre rutes amb altres xarxes.
- Com i quan es passen els missatges d'error i del sistema entre dispositius.
- L'inici i el final de les sessions de transferència de dades.

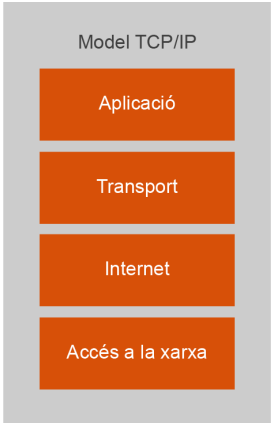
Els protocols individuals d'una *suite* de protocols poden ser específics d'un fabricant o de propietat exclusiva. En aquest context, *propietari* significa que una companyia o proveïdor controla la definició del protocol i com funciona.

Un dels protocols més comuns és el protocol d'Internet (IP, de l'anglès *Internet protocol*). IP és responsable de prendre segments de dades, encapsular-los en paquets, assignar-los les adreces correctes i seleccionar la millor ruta per enviar les dades al *host* de destinació.

2.4 Model TCP/IP

El primer model de protocol en capes per a la comunicació d'*internetworks* es va crear al principi de la dècada dels setanta i es coneix amb el nom de *model d'Internet*. Defineix quatre categories de funcions que han de tenir lloc perquè les comunicacions tinguin èxit. L'arquitectura de la *suite* de protocols TCP/IP segueix l'estructura d'aquest model. Per aquesta raó, és comú que el model d'Internet es conegui com a *model TCP/IP* (vegeu la figura 2.1).

FIGURA 2.1. Model TCP IP



Quan una companyia no controla la definició d'un protocol, s'anomena un estàndard obert.

La gran majoria dels models de protocols descriuen una pila de protocols específics del proveïdor. Tot i això, el model TCP/IP és un estàndard obert: no

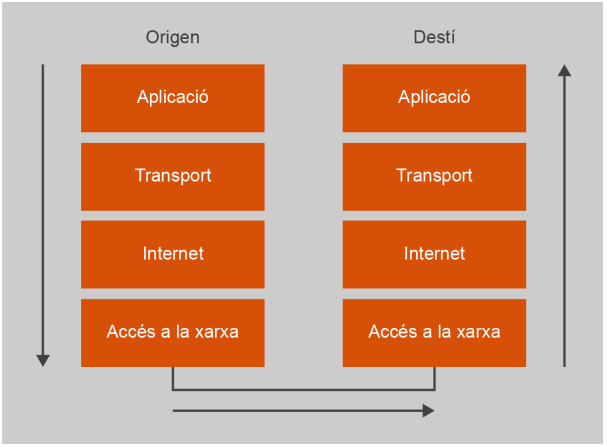
hi ha una companyia que controli la definició del model. Les definicions de l'estàndard i els protocols TCP/IP s'expliquen en un fòrum públic i es defineixen en un conjunt de documents disponibles per al públic. Aquests documents es denominen *sol·licituds de comentaris* (RFC). Contenen les especificacions formals dels protocols de comunicació de dades i els recursos que descriuen l'ús dels protocols.

Les RFC també contenen documents tècnics i organitzacionals sobre Internet, incloent-hi les especificacions tècniques i els documents de les polítiques produïts pel grup de treball d'enginyers d'Internet (IETF).

2.4.1 Procés de comunicació

El model TCP/IP descriu la funcionalitat dels protocols que formen la *suite* de protocols TCP/IP. Aquests protocols, que s'implementen tant en el *host* emissor com en el receptor, interactuen per lliurar aplicacions d'extrem a extrem utilitzant la Xarxa (vegeu la figura 2.2).

Figura 2.2. Procés de comunicació complet



Un procés complet de comunicació inclou aquests passos:

1. Creació de dades en la capa d'aplicació del dispositiu d'origen.
2. Segmentació i encapsulació de dades quan passen per la pila de protocols en el dispositiu d'origen.
3. Generació de les dades sobre el mitjà en la capa d'accés a la Xarxa.
4. Transport de les dades per la Xarxa, que està formada pels mitjans i qualsevol dispositiu intermediari.
5. Recuperació de les dades en la capa d'accés a la Xarxa del dispositiu de destinació.
6. Desencapsulació i rearmament de les dades en passar per la pila en el dispositiu final.

7. Traspàs d'aquestes dades a l'aplicació de destinació corresponent a la capa d'aplicació del dispositiu de destinació.

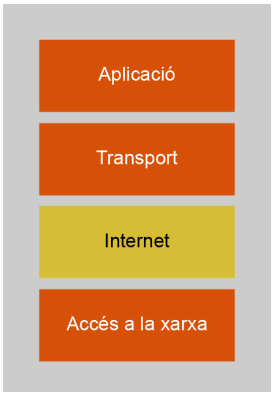
2.5 Adreçament en la Xarxa

El model TCP/IP descriu els processos de codificació, formatatge, segmentació i encapsulació de dades per transmetre per la Xarxa. Un flux de dades que s'envia des d'un origen fins a una destinació es pot dividir en parts i entrellaçar amb els missatges que viatgen des d'altres *hosts* fins a altres destinacions. Milers de milions d'aquestes parts d'informació viatgen per una xarxa en qualsevol moment. És molt important que cada part de les dades contingui informació d'identificació suficient per arribar a la destinació correcta.

Hi ha diferents tipus d'adreces que s'han d'incloure per lliurar satisfactòriament les dades des d'una aplicació d'origen que s'executa en un *host* fins a l'aplicació de destinació correcta que s'executa en l'altre. En utilitzar el model TCP/IP com a guia, es poden observar diferents adreces i identificadors necessaris en cada capa.

Els protocols de capa 2 del model TCP/IP estan dissenyats principalment per moure dades des d'una xarxa local a una altra dins d'una *internetwork* o per Internet (vegeu la figura 2.3). Les adreces de capa 2 han d'incloure identificadors que permetin a dispositius de xarxa intermediaris ubicar els *hosts* en diferents xarxes. En la *suite* de protocols TCP/IP, cada adreça IP de *host* conté informació sobre la xarxa en què està ubicat el *host*.

Figura 2.3. Capa 2



En els límits de cada xarxa local, un dispositiu de xarxa intermediari, generalment un encaminador, desencapsula la trama per llegir l'adreça *host* de destinació situada en la capçalera del paquet, la PDU (*protocol data unit*) de capa 2. Els encaminadors utilitzen la porció de l'identificador de xarxa d'aquesta adreça per determinar la ruta a utilitzar per arribar al *host* de destinació. Un cop s'ha determinat la ruta, l'encaminador torna a encapsular el paquet en una nova trama i l'envia pel seu trajecte fins al dispositiu final. Quan la trama arriba a la destinació, la trama i les capçaleres del paquet s'eliminen i les dades s'envien a les capes superiors.

2.5.1 Protocols de capa 2 de TCP/IP

La capa d'Internet ha de proveir d'un mecanisme per adreçar els dispositius finals d'origen i de destinació. Si les seccions individuals de dades s'han de dirigir a un dispositiu final, aquest ha de tenir una adreça única.

En una xarxa IPv4, quan aquesta adreça s'agrega a un dispositiu, el dispositiu s'anomena *host*.

Els protocols implementats en la capa d'Internet que porten dades d'usuari són:

- versió 4 del protocol d'Internet (IPv4)
- versió 6 del protocol d'Internet (IPv6)
- intercanvi novell de paquets d'*internetwork* (IPX)
- AppleTalk
- servei de xarxa sense connexió (CLNS/DECNet).

Els protocols d'Internet (IPv4 i IPv6) són els protocols de transport de dades de capa 2 utilitzats més àmpliament i, concretament, l'IPv4 serà el que es tractarà en aquest mòdul.

2.5.2 Adreçament IPv4

Cada dispositiu de xarxa s'ha de definir de manera exclusiva. En la capa d'Internet és necessari identificar els paquets de la transmissió amb adreces d'origen i de destinació dels sistemes finals. En l'IPv4, això significa que cada paquet té una adreça d'origen de 32 bits i una adreça de destinació de 32 bits.

Aquestes adreces s'utilitzen en les xarxes de dades com a patrons binaris. Dins dels dispositius, s'aplica la lògica digital per a la seva interpretació. Per als que formem part de la xarxa humana, una sèrie de 32 bits és difícil d'interpretar i de recordar, per tant, representem les adreces IPv4 utilitzant el format decimal puntejat.

Conversió binària/decimal

Per comprendre el funcionament d'un dispositiu en una xarxa, és necessari considerar les adreces i altres dades de la manera en què ho fa un dispositiu: en notació binària. Això significa que és necessari ser hàbil en la conversió de binari a decimal.

Les dades representades en el sistema binari poden representar moltes formes diferents de dades a la xarxa humana. En aquest tema, farem referència al sistema binari per estar relacionat amb l'adreçament IPv4.

Notació de posició

L'Aprenentatge de la notació de posició per convertir binari a decimal requereix una comprensió dels fonaments matemàtics d'un sistema de numeració anomenat notació de posició. Notació de posició significa que un dígit representa diferents valors segons la posició que ocupa. Més específicament, el valor que un dígit representa és el valor multiplicat per la potència de la base o arrel representat per la posició que el dígit ocupa. Per ajudar a entendre això, anem a veure alguns exemples:

Per al nombre decimal 245, el valor que el 2 representa és 2*10^2 (2 multiplicat per 10 elevat a la segona potència). El 2 es troba en el que comunament anomenem la posició "100".

Usant la notació de posició en el sistema de numeració en base 10, 245 representa:

```
245 = (2 * 10^2) + (4 * 10^1) + (5 * 10^0)
```

o

```
245 = (2 * 100) + (4 * 10) + (5 * 1)
```

Sistema de numeració binària

En el sistema de numeració binària l'arrel és 2. Per tant, cada posició representa potències incrementades de 2. En nombres binaris de 8 bits, les posicions representen aquestes quantitats:

```
2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
```

o, el que és el mateix:

```
128 64 32 16 8 4 2 1
```

El sistema de numeració de base 2 té solament dos dígits: 0 i 1.

Quan s'interpreta un byte com un nombre decimal, s'obté la quantitat que aquesta posició representa si el dígit és 1 i no s'obté la quantitat si el dígit és 0.

```
1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1
```

Un 1 en cada posició significa que el valor per a aquesta posició s'afegeix al total. Si tenim el número binari 11111111, obtindrem el seu valor decimal realitzant la suma de:

```
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255
```

Un 0 en cada posició indica que el valor per a aquesta posició no es suma al total. Un 0 en cada posició produeix un total de 0. És a dir, el valor binari 00000000 equival a sumar:

```
128 64 32 16 8 4 2 1
0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0
```

Exemple: Quin valor té l'octet binari 10010110?

```
128*1+64*0+32*0+16*1+8*0+4*1+2*1+1*0 = 150
```

És a dir, podem afirmar que 10010110 en binari, equival al valor 150 en format decimal.

TAULA 2.1. Taula de conversió decimal/binari

Decimal	Binari 2^3	2^2	2^1	2^0
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1

Punt decimal

Els patrons binaris que representen adreces IPv4 són expressats amb punts decimals separant cada byte del patró binari, anomenat octet, amb un punt. Se'n diu octet degut a que cada número decimal representa un byte o 8 bits.

Per exemple, l'adreça IPv4 d'un *host* de xarxa en format binari és el següent:

```
10101100000100000000010000010100
```

Si dividim l'adreça en octets mitjançant punts obtindrem:

```
10101100.00010000.00000100.00010100
```

En format decimal puntejat, només cal traduir cada octet en format decimal, de manera que s'obté un resultat com el següent:

```
10101100 = 172

```

```
00010000 = 16

00000100 = 4

00010100 = 20
```

Per tant, l'adreça IPv4 en format decimal puntejat es representaria així:

```
172.16.4.20
```

Porcions de xarxa i de host

Cada adreça IPv4 té una porció que representa la part de xarxa i una porció que representa la part de *host*. En la capa 2, es defineix una xarxa com un grup de *hosts* amb patrons de bits idèntics a la porció de xarxa. Per exemple, en l'adreça 192.168.2.6, la part de xarxa estaria definida pels tres primers octets, i la part de *host* pel darrer.

- Adreça de xarxa. Part de l'adreça IP en què es fa referència a la xarxa
- Adreces de *host*. Part de l'adreça IP assignada als dispositius finals de la xarxa. Cada dispositiu final necessita una adreça única per enviar dades a una altra xarxa.

> Dins del rang d'adreces IPv4 d'una xarxa, l'adreça més baixa es reserva per a l'adreça de xarxa. Aquesta adreça té un 0 per a cada bit en la porció de *host* de l'adreça.

Màscara de xarxa

Per poder identificar correctament quina part de l'adreça IPv4 pertany a la xarxa i quina pertany al *host* s'utilitza una tira de 32 bits que sempre acompanyen l'adreça IPv4 i que s'anomena *màscara de xarxa*. Cada un d'aquests bits ha d'estar assignat a 1 si la part equivalent de l'adreça IPv4 pertany a la xarxa, i a 0 si pertany al *host*. Per exemple:

Adreça IPv4 en binari:

```
10101100000100000000010000010100
```

Màscara IPv4 en binari:

```
11111111111111110000000000000000
```

Com es pot veure, els setze primers bits de la màscara de xarxa estan establerts a 1, amb la qual cosa els setze primers bits de l'adreça IP identifiquen la xarxa en què es troba el *host*, i els darrers setze bits representen el *host* en concret.

Si traduïm de bits a decimal obtindrem:

Adreça IPv4 en decimal:

```
172.16.4.20
```

Màscara IPv4 en decimal:

```
255.255.0.0
```

Per tant, els dos primers octets de l'adreça de la xarxa (172.16.) representen la xarxa, i els dos darrers el *host* (4.20).

La màscara de xarxa es pot representar de dues maneres diferents: el format tradicional amb quatre octets que tenen 1 binari en la part de xarxa i 0 binari en la part de *host*. Exemple:

```
255.0.0.0

255.255.0.0

255.255.255.0
```

O es pot especificar la longitud del prefix, que és la quantitat de bits de la màscara que identifica la part de xarxa (forma resumida). Exemple:

- **255.0.0.0** es representa com **/8** (8 bits).
- **255.255.0.0** es representa com **/16** (16 bits).
- **255.255.255.0** es representa com **/24** (24 bits).

Per exemple, en l'adreça 10.6.7.11 amb màscara 255.0.0.0, podem dir que el primer octet identifica la xarxa (10.0.0.0) i els darrers tres octets identifiquen el *host*. En l'adreça 192.168.11.27/24, podem dir que els primers tres octets identifiquen la xarxa (192.168.11.0) i el darrer octet identifica el *host*.

Tipus d'adreces IPv4

Dins del rang d'adreces de cada xarxa IPv4, existeixen tres tipus d'adreces:

- **Adreça de xarxa**: l'adreça en la qual es fa referència a la xarxa.
- **Adreça de broadcast**: una adreça especial utilitzada per enviar dades a tots els hosts de la xarxa.
- **Adreces host**: les adreces assignades als dispositius finals de la xarxa com ara PCs, PDAs, impressores en xarxa, etc.

Adreça de xarxa

L'adreça de xarxa és una manera estàndard de fer referència a una xarxa. Per exemple: es podria fer referència a la una xarxa com a "xarxa 10.0.0.0". Aquesta

és una forma molt més convenient i descriptiva de referir-se a la xarxa que utilitzant un terme com "la xarxa del primer pis". Tots els hosts de la xarxa 10.0.0.0 tindran els mateixos bits de xarxa.

Dins del rang d'adreces IPv4 d'una xarxa, l'adreça més baixa es reserva per a l'adreça de xarxa. Aquesta adreça té un 0 per a cada bit de host en la porció de host de l'adreça.

Adreça de broadcast

L'adreça de broadcast és una adreça especial per a permetre la comunicació a tots els host en aquesta xarxa. Per enviar dades a tots els hosts d'una xarxa, un host pot enviar un sol paquet dirigit a l'adreça de broadcast de la xarxa.

L'adreça de broadcast utilitza l'adreça més alta en el rang de la xarxa. Aquesta és l'adreça en la qual els bits de la porció de host són tots 1. Per a la xarxa 10.0.0.0, l'adreça de broadcast seria 10.255.255.255.

Adreces host

Com heu vist anteriorment, cada dispositiu final requereix una adreça única per enviar un paquet a un host concret. En les adreces IPv4, s'assignen els valors entre l'adreça de xarxa i l'adreça de broadcast als dispositius en aquesta xarxa.

Exemple

Tenim la xarxa 172.16.0.0 /16. Quina seria l'adreça de xarxa? Quina la de broadcast? Quines adreces podríem assignar als hosts?

- Adreça de xarxa: 172.16.0.0
- Adreça de broadcast: 172.16.255.255
- Rang d'adreces assignables: 172.16.0.1 a 172.16.255.254

2.5.3 Classes IPv4

Històricament, la RFC1700 agrupava rangs de d'adreces IPv4 en grandàries específiques anomenades adreces de classe A, de classe B i de classe C. També definia a les adreces de classe D (multicast) i de classe E (experimentals).

Les adreces de classes A, B i C definien xarxes de grandàries específiques, així com blocs d'adreces específics per a aquestes xarxes (taula 2.2). D'aquesta forma, s'assignaven a companyies o organitzacions tot un bloc d'adreces de classe A, classe B o classe C. Aquest ús d'espai d'adreça és denominat *adreçament amb classe*.

Taula 2.2. Descripció de les classes A, B i C

Classe d'adreça	Rang primer octet	Parts de xarxa i de host	Màscara per defecte	Número de xarxes i de hosts totals
A	1-127	X.H.H.H	255.0.0.0	128 xarxes / 16.777.214 hosts

TAULA 2.2 (continuació)

Classe d'adreça	Rang primer octet	Parts de xarxa i de host	Màscara per defecte	Número de xarxes i de hosts totals
B	128-191	X.X.H.H	255.255.0.0	16.384 xarxes / 65.534 hosts
C	192-223	X.X.X.H	255.255.255.0	2.097.150 xarxes / 254 hosts

Blocs de classe A

Es va dissenyar un bloc d'adreces de classe A per admetre xarxes extremadament grans amb més de 16 milions d'adreces host. Les adreces IPv4 de classe A usaven un prefix /8 fix, on el primer octet indicava l'adreça de xarxa. Els tres octets restants s'usaven per a les adreces host.

Per reservar espai d'adreces per a les classes d'adreces restants, totes les adreces de classe A requerien que el bit més significatiu de l'octet d'ordre superior fos un zero. Això significava que només hi havia 128 xarxes de classe A possibles, de 0.0.0.0 /8 a 127.0.0.0 /8, abans d'excloure els blocs d'adreces reservades. Tot i que les adreces de classe A reservaven la meitat de l'espai d'adreces, a causa del límit de 128 xarxes, només podien ser assignades a aproximadament 120 companyies o organitzacions.

Blocs de classe B

L'espai d'adreces de classe B va ser dissenyat per satisfer les necessitats de les xarxes de grandària moderada a gran amb més de 65.000 hosts. Una adreça IP de classe B utilitzava els dos octets d'ordre superior per indicar l'adreça de xarxa. Els dos octets restants especificaven les adreces de host. Igual que amb la classe A, s'havia de reservar espai d'adreces per a les classes d'adreces restants.

Amb les adreces de classe B, els dos bits més significatius de l'octet d'ordre superior eren 10. D'aquesta forma, es restringia el bloc d'adreces per a la classe B a 128.0.0.0 /16 fins a 191.255.0.0 /16. La classe B tenia una assignació d'adreces una miqueta més eficient que la classe A ja que dividia equitativament el 25% del total de l'espai d'adreces IPv4 entre aproximadament 16.000 xarxes.

Blocs de classe C

L'espai d'adreces de classe C era la classe d'adreces antigues més utilitzades. Aquest espai d'adreces tenia el propòsit de proporcionar adreces per a xarxes petites amb un màxim de 254 hosts.

Els blocs d'adreces de classe C utilitzaven el prefix /24. Això significava que una xarxa de classe C només utilitzava l'últim octet com a adreces host, amb els tres octets d'ordre superior per indicar l'adreça de xarxa.

Els blocs d'adreces de classe C reservaven espai d'adreces per a la classe D (multicast) i la classe E (experimental) mitjançant l'ús d'un valor fix de 110 per als tres bits més significatius de l'octet d'ordre superior. Això va restringir el bloc d'adreces per a la classe C de 192.0.0.0/24 a 223.255.255.0/24.Tot i que ocupava només el 12.5% del total de l'espai d'adreces IPv4, podia subministrar adreces a 2 milions de xarxes.

Limitacions del sistema basat en classes

No tots els requisits de les organitzacions s'ajustaven a una d'aquestes tres classes. L'assignació amb classe d'espai d'adreces sovint malgastava moltes adreces, la qual cosa esgotava la disponibilitat d'adreces IPv4. Per exemple: una companyia amb una xarxa amb 260 hosts necessitaria que se li assignés una adreça de classe B amb més de 65.000 adreces ja que una classe C (màxim 254 hosts) es feia petita.

Tot i que aquest sistema amb classe no va ser abandonat fins a finals de la dècada del 90, és possible veure restes d'aquestes xarxes en l'actualitat. Per exemple: en assignar una adreça IPv4 a un host, el sistema operatiu examina l'adreça que s'està assignant per determinar si és de classe A, classe B o classe C. Després, el sistema operatiu adopta el prefix utilitzat per aquesta classe i realitza l'assignació de la màscara de subxarxa adequada.

Adreces IPv4 públiques i privades

InterNIC...

va ser el primer organisme governamental encarregat de les adreces IP i noms de domini. Actualment, d'aquestes funcionalitats, se n'encarrega l'ICANN (de l'anglès Internet Corporation for Assigned Names and Numbers, Corporació d'Internet per a l'Assignació de Noms i Nombres).

Tot i que la majoria d'adreces IPv4 de *host* són adreces públiques designades per a l'ús en xarxes a les quals s'accedeix des d'Internet, hi ha blocs d'adreces que s'utilitzen en xarxes que requereixen accés a Internet o no. Aquestes adreces es denominen *adreces privades*.

Les adreces públiques són designades per InterNIC (de l'anglès *Internet Network Information Center*) i estan compostes per identificadors de xarxa basats en classes o blocs que són universalment únics per a Internet.

Adreces privades

Les adreces privades són adreces utilitzades per a xarxes internes. Aquestes adreces estan definides en el document RFC-1918. No són encaminables a Internet.

Els blocs d'adreces privades són:

- Des de 10.0.0.0 a 10.255.255.255 (xarxa 10.0.0.0 /8)
- Des de 172.16.0.0 a 172.31.255.255 (xarxa 172.16.0.0 /16)
- Des de 192.168.0.0 a 192.168.255.255 (xarxa 192.168.0.0 /24)

En el nostre cas, habitualment treballarem amb adreces privades, ja que són les que podem assignar als *hosts* de la xarxa. Les adreces públiques són assignades habitualment pel nostre ISP (de l'anglès *Internet service provider*, proveïdor de serveis d'Internet).

2.6 Adreçament estàtic o dinàmic per a dispositius d'usuari final

A l'hora de configurar l'adreçament de la capa 2, es pot utilitzar un adreçament estàtic (configurat manualment) o dinàmic (configurat utilitzant un servidor específic). En aquest apartat, podreu aprendre les característiques de cada un d'aquests mètodes.

2.6.1 Adreçament per a dispositius d'usuari

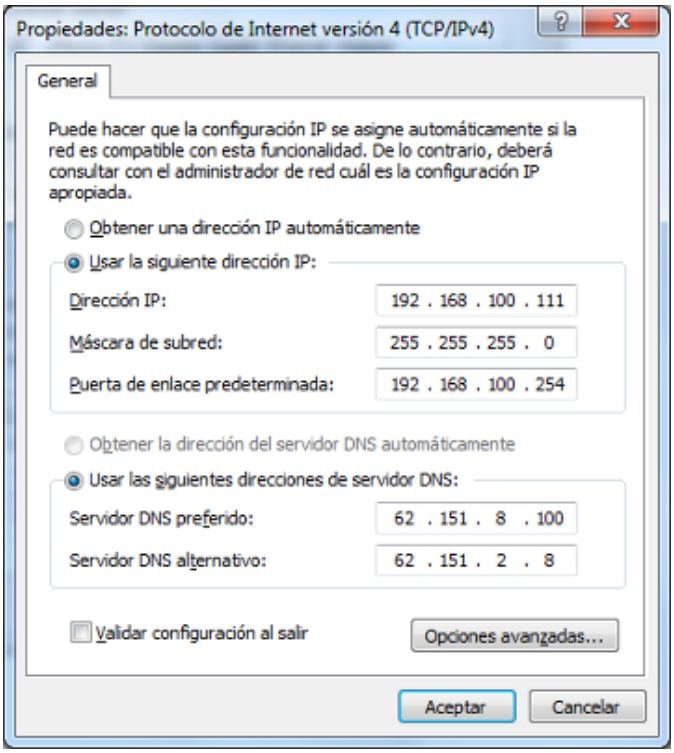
És necessari que l'assignació d'adreces IP en una xarxa estigui ben dissenyada. En la majoria de xarxes de dades, la majoria de *hosts* inclou dispositius finals com PC, telèfons IP, impressores i organitzadors personals o PDA (*personal digital assistant*). Per aquest motiu, s'han d'assignar a aquests dispositius la majoria d'adreces IPv4.

Les adreces IP es poden assignar de manera estàtica o dinàmica.

Assignació estàtica d'adreces IPv4

Amb una assignació estàtica, l'administrador de xarxa ha de configurar manualment la informació de xarxa per a un *host* concret, tal com podeu veure en la figura 2.4. Com a mínim, això implica ingressar l'adreça IP del *host* i la seva màscara de xarxa. A més, es pot configurar la passarel·la (*gateway*) per defecte i els servidors DNS.

Figura 2.4. Adreçament estàtic



La passarel·la s'utilitza per accedir a altres xarxes externes a la nostra i, típicament, conté l'adreça de la interfície interna de l'encaminador que connecta amb Internet. Els servidors DNS permeten resoldre noms de *host* (www.ioc.cat) en l'adreça IP corresponent (85.192.111.244).

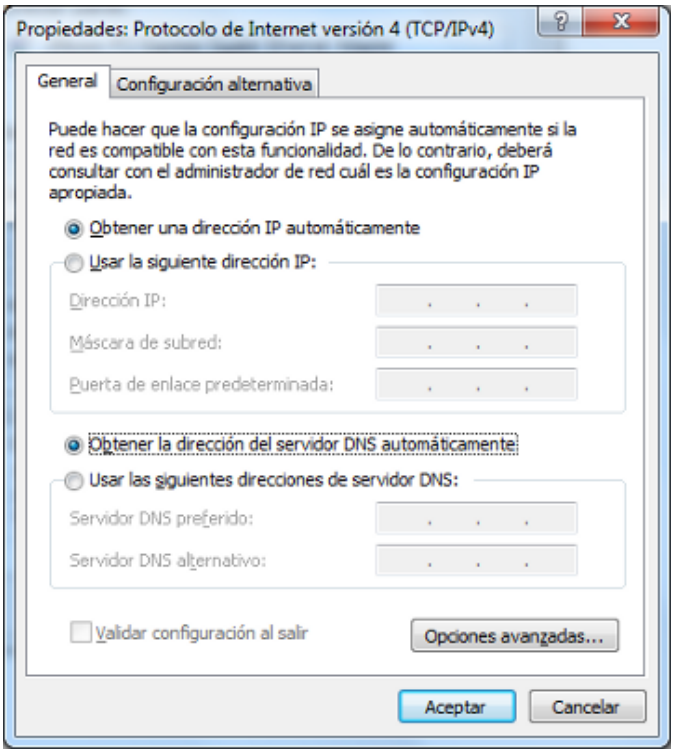
Les adreces estàtiques tenen certs avantatges en comparació amb les adreces dinàmiques. Per exemple, resulten útils per a impressores, servidors i d'altres dispositius que cal identificar de la mateixa manera a cada moment. Si normalment els *hosts* accedeixen a un servidor utilitzant una adreça IP en particular, podrien aparèixer certs problemes si se'n modificava l'adreça. D'altra banda, assignar adreces manualment pot fer que els recursos d'una xarxa es controlin més. Tot i això, és possible que per fer aquesta configuració de cada *host* calgui més temps.

En fer l'adreçament IP estàtic, s'ha de mantenir una llista precisa de les adreces IP assignades a cada dispositiu. Aquestes han de ser les adreces permanents i normalment no es poden tornar a utilitzar en cap altre *host*.

Assignació dinàmica d'adreces IPv4

A causa de la complexitat associada a l'administració d'adreces estàtiques, els dispositius d'usuaris finals acostumen a incloure adreces assignades dinàmicament. Per aconseguir això, s'utilitza un protocol anomenat **DHCP** (*dynamic host configuration protocol* o protocol de configuració dinàmica de *host*), tal com podeu veure en la configuració de la figura 2.5.

FIGURA 2.5. Adreçament dinàmic



El DHCP permet l'assignació automàtica d'informació d'adreçament com l'adreça IP, la màscara de xarxa, la passarel·la o *gateway* per defecte i d'altra informació de configuració. La configuració del servidor DHCP requereix que es defineixi un bloc d'adreces per ser assignat als clients DHCP en una xarxa. Les adreces assignades a aquest bloc s'han de planificar de manera que s'excloguin les utilitzades per a altres tipus de dispositius com ara impressores o servidors, els quals han de tenir una adreça IP estàtica.

Generalment, el DHCP és el mètode preferit per assignar adreces IP als *hosts* de grans xarxes, ja que redueix en gran part la càrrega del personal de suport a la xarxa i pràcticament elimina els errors d'entrada.

Un altre benefici del DHCP és que no s'assigna una adreça a un *host* de manera permanent, sinó que només es lloga o presta durant un temps determinat. Si un *host* s'apaga o es desconnecta en la xarxa, l'adreça assignada retorna al conjunt d'adreces disponibles del servidor DHCP i pot tornar a ser utilitzada. Aquesta configuració és molt útil per a usuaris mòbils que constantment entren i surten de la xarxa.

3. Optimització del sistema en ordinadors portàtils

En l'actualitat moltes organitzacions centren la seva atenció en l'administració d'energia com una manera de reduir costos mitjançant l'estalvi energètic. A més, un dels aspectes més crítics en l'ús dels ordinadors portàtils és la duració de la bateria. Tots els sistemes operatius utilitzen diferents estratègies per millorar el rendiment dels equips i disminuir el consum energètic, fet clau en la vida mòbil actual.

Tot i els avenços en la tecnologia, la bateria d'un portàtil dura únicament el que dura la càrrega. El secret és a aprofitar al màxim l'energia disponible.

El Windows 7 permet prolongar la duració de les bateries dels ordinadors portàtils perquè els usuaris mòbils siguin més productius i facin més feina en una sola càrrega de bateria. Per exemple, les pantalles integrades són les que consumeixen més energia en els ordinadors portàtils normals. Temes com la brillantor de la pantalla poden reduir àmpliament la duració de les bateries. Una brillantor adaptable i automàtica pot reduir, en aquest cas, el consum energètic i, per tant, augmentar la duració de les bateries.

3.1 Millores d'estalvi energètic en el Windows 7

El Windows 7 ofereix millores importants respecte a les versions anteriors del Windows pel que fa a l'estalvi energètic dels equips. Algunes de les característiques que incorpora es definiran a continuació:

- **Baix consum en mitjans desconnectats.** El baix consum en mitjans desconnectats és la capacitat de l'adaptador de xarxa per entrar en suspensió quan no funciona. Quan el Windows detecta que els mitjans s'han desconnectat (per exemple, s'ha desconnectat un cable), el Windows configura el dispositiu en estat de baixa energia i deshabilita la LAN. L'ordinador detecta automàticament quan es torna a connectar el cable i retorna l'adaptador de xarxa a l'estat d'energia completa.
- **Millora en la gestió d'energia dels processadors.** El Windows 7 incorpora una millora en l'ús dels recursos de maquinari que permeten, per exemple, escollir l'acord de rendiment òptim del processador depenent de la càrrega i la escala de rendiment que s'hagi obtingut.
- **Optimitzacions en la reproducció de DVD i navegació web.** La reproducció de DVD en el Windows 7 també ha permès obtenir un estalvi energètic respecte a les versions anteriors. Per exemple, segons dades de Microsoft, el Windows 7 redueix el consum energètic fins a un 15% en reproduccions de

DVD en comparació al Vista gràcies a la capacitat per reduir el rendiment de la CPU sense afectar la reproducció, a una millora del *Windows desktop manager* (DWM) i al processador gràfic (GPU).

- **Control d'energia en repòs.** Disposa de diferents sistemes de control per assegurar que l'ordinador no faci activitats innecessàries mentre està en repòs que obliguin a augmentar la despesa energètica.
- **Plans d'energia.** El Windows 7 facilita l'administració d'energia fent ús de diferents plans, els quals poden ajudar a reduir clarament el consum en ordinadors portàtils. Aquests plans d'energia són totalment configurables per l'usuari.

3.2 Plans d'energia

Un pla d'energia és un conjunt de valors de configuració de programari i del sistema que administren la manera en què l'equip utilitza l'energia. Els plans d'energia permeten estalviar energia, maximitzar el rendiment del sistema o aconseguir un equilibri entre les dues situacions.

En versions anteriors del Windows, els plans d'energia s'anomenaven *esquemes d'energia*.

El Windows 7 té, per defecte, tres plans d'energia diferenciats: equilibrat, economitzador i alt rendiment. A més, es pot modificar la configuració de qualsevol d'aquests plans i fins i tot crear-ne de nous. Tot i això, els plans predeterminats satisfan les necessitats informàtiques de la majoria d'usuaris amb ordinadors portàtils.

3.2.1 Tipus de plans d'energia predefinits

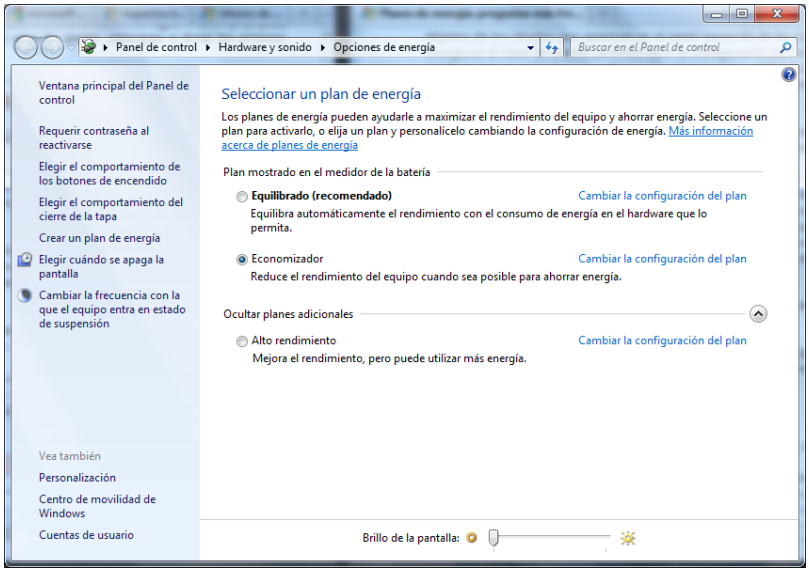
Per defecte hi ha tres plans d'energia diferenciats. Aquests plans són:

- **Equilibrat.** Ofereix el màxim rendiment quan és necessari i, estalvi energètic durant els períodes d'inactivitat.
- **Economitzador d'energia.** Estalvia energia, ja que disminueix el rendiment del sistema. Aquest pla pot ajudar els usuaris d'ordinadors portàtils a obtenir el màxim rendiment possible amb una sola càrrega de bateria.
- **Alt rendiment.** Maximitza el temps de resposta i el rendiment del sistema. Els usuaris d'ordinadors portàtils podran notar que la bateria no dura tant utilitzant aquest pla energètic, però veuran millorar el rendiment del sistema.

Alguns fabricants de portàtils afegeixen nous plans d'energia específics adaptats als seus ordinadors (vegeu la figura 3.1).

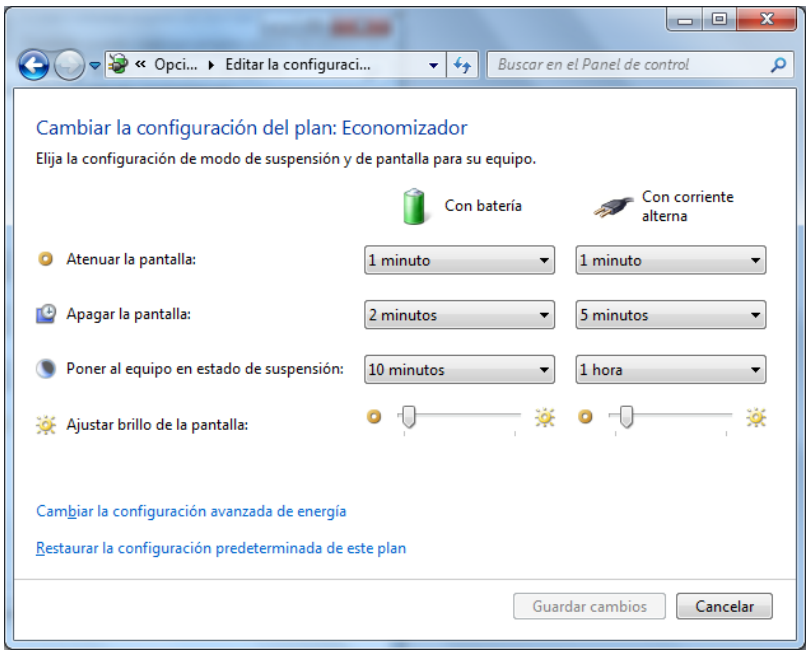
Els diferents plans d'energia es poden configurar des del tauler de control.

Figura 3.1. Gestió de plans d'energia



Sempre que l'administrador del sistema no imposi alguna restricció, es poden modificar les configuracions de tots els plans d'energia, incloent-hi els tres predefinits. A la figura 3.2 podeu veure algunes de les configuracions modificables dels plans d'energia que són les següents:

Figura 3.2. Opcions d'energia



- Atenuar la pantalla. Permet decidir quant de temps l'equip ha de restar inactiu abans d'atenuar (abaixar) la brillantor de la pantalla.

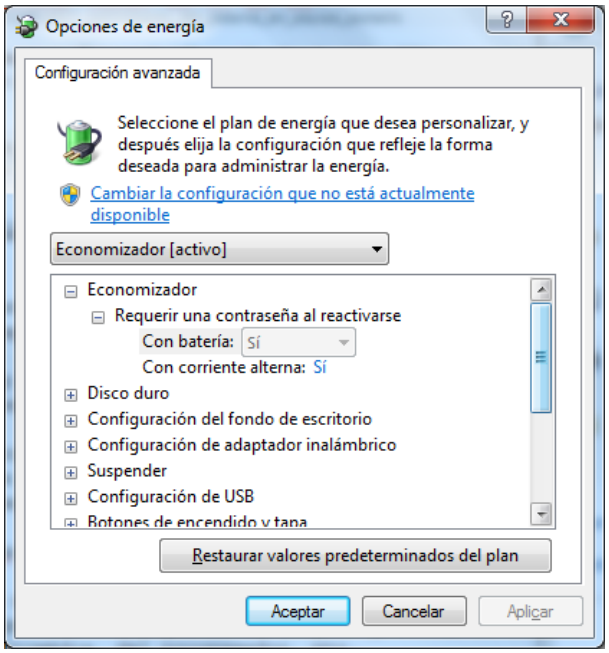
- Apagar la pantalla. Permet decidir el temps que l'equip ha de restar inactiu abans d'apagar la pantalla.

- Posar l'equip en estat de suspensió. Permet suspendre l'equip passat el temps especificat.

- Ajustar la brillantor de la pantalla. Permet triar la brillantor de la pantalla en cada pla d'energia segons si l'equip està connectat a la xarxa elèctrica o no.

A més d'aquestes configuracions, també se'n poden modificar d'altres com ara la d'energia de la targeta gràfica, en les reproduccions multimèdia, la del processador, etc.(vegeu la figura 3.3).

FIGURA 3.3. Altres opcions d'energia



3.3 Estalvi energètic

Els plans d'energia que inclou el Windows 7 permeten estalviar un alt percentatge d'energia en un equip portàtil. Tot i això, hi ha altres mètodes que poden ajudar a reduir el consum energètic. Entre aquests destaquem els següents:

- **Reduir la brillantor de pantalla.** La pantalla pot utilitzar més energia que qualsevol altre part de l'equip, fins i tot més que el disc dur i la CPU. La gran majoria dels ordinadors portàtils tenen un botó o dial dedicat a canviar la brillantor de la pantalla.

- **Desconnectar dispositius USB.** Molts dispositius USB consumeixen energia pel simple fet d'estar connectats. Si s'utilitza un ratolí USB es pot estalviar energia desconnectant-lo i utilitzant el ratolí tàctil o el llapis de *tablet PC*. Si s'utilitza un disc dur o memòria USB, és aconsellable desconnectar-la quan no s'hagi d'utilitzar per disminuir el consum.

- **Desactivar les targetes *PC card* i els dispositius sense fil integrats.** Aquests dispositius, com les targetes sense fil o el Bluetooth, també consumeixen energia addicional. Si no són necessaris es poden desactivar per augmentar la duració de les bateries.

- **Mantenir l'equip compactat.** Compactar de manera regular quan l'equip està connectat a la xarxa elèctrica pot ajudar a disminuir el consum elèctric. Un disc menys fragmentat implica que el capçal de lectura del disc s'ha de desplaçar menys i es consumeix menys energia.

- **Modificar el tema del Windows 7.** Utilitzar un tema estàndard en lloc del tema Aero, que requereix més potència de càlcul i, per tant, un consum més elevat.

- **Desactivar els efectes visuals.** Els efectes com ara les animacions i transparències són agradables a la vista però obliguen la CPU a fer càlculs addicionals.

- **Limitar les aplicacions iniciades a l'inici del sistema.** Normalment moltes de les aplicacions que instal·lem en el nostre equip inicien automàticament certs assistents o ajudants a l'inici del sistema. Totes aquestes petites aplicacions acostumen a consumir recursos addicionals que no solament fan baixar el rendiment del sistema, sinó que a més poden fer augmentar el consum energètic.

3.4 Suspensió, hibernació i suspensió híbrida

La **suspensió** és un estat d'estalvi energètic que permet a l'equip reprendre ràpidament el funcionament a ple rendiment en pocs segons quan es vol continuar treballant. Posar l'equip en estat de suspensió és semblant a posar en pausa un reproductor de DVD: l'equip interromp automàticament les seves tasques i estarà preparat per reiniciar-les quan es vulgui. En aquest cas, les dades s'emmagatzemen en memòria RAM de l'ordinador i l'equip passa a consumir molt poca energia.

La **hibernació** és un estat d'estalvi energètic dissenyat principalment per a ordinadors portàtils. Mentre que la suspensió desa el treball i la configuració en memòria RAM i consumeix una petita quantitat d'energia, la hibernació desa els documents i programes oberts en el disc dur i després apaga l'equip. De tots els estats d'estalvi d'energia del Windows, la hibernació és el que menys energia consumeix. En un equip portàtil, s'ha d'utilitzar la hibernació quan se sap que no s'utilitzarà l'equip durant un llarg període de temps i que no es podrà recarregar la bateria durant aquest temps.

La **suspensió híbrida** es va dissenyar principalment per a ordinadors de taula. La suspensió híbrida és una combinació del mode de suspensió i hibernació que desa tots els documents i programes oberts en la memòria i en el disc dur i, a continuació, l'equip passa a un estat de baix consum d'energia perquè es

pugui reprendre el treball ràpidament. D'aquesta manera, si es produeix un error d'alimentació, el Windows pot restaurar el treball des del disc dur. Quan la suspensió híbrida està activada, en col·locar l'equip en mode de suspensió, aquest passa automàticament a la suspensió híbrida. En els ordinadors de taula, la suspensió híbrida està habilitada per defecte.

3.5 Optimització del sistema per a millorar el rendiment

Normalment, al comprar un nou equip, aquest acostuma a ser prou ràpid com per a desenvolupar la seva feina amb gran agilitat, tot i això, amb l'ús del sistema i el pas del temps, aquest es va tornant cada cop més lent. És possible que aquest equip últim model que varem comprar l'any passat no sigui tant ràpid després d'instal·lar una dotzena de programes, de carregar-ho amb eines antivirus i anti-spyware, i de descarregar una quantitat incalculable de correu no desitjat d'Internet. La reducció de velocitat es pot produir tan gradualment que gairebé no la notareu; fins que, un dia, intentareu obrir un programa o un arxiu i us preguntareu: "Què ha passat amb el meu pobre equip?".

Independentment del motiu, hi ha moltes formes d'augmentar la velocitat de Windows i optimitzar el funcionament de l'equip, fins i tot sense actualitzar el maquinari. A continuació, s'inclouen alguns suggeriments que us ajudaran a optimitzar Windows 7 per obtenir un rendiment més ràpid.

3.5.1 Utilitzar el solucionador de problemes de rendiment

El primer que podeu provar és el *Solucionador de problemes de rendiment*, que pot detectar i solucionar problemes automàticament. El *Solucionador de problemes de rendiment* busca problemes que poden fer més lent el rendiment de l'equip, com la quantitat d'usuaris que actualment han iniciat sessió en l'equip i l'execució simultània de diversos programes.

Per obrir el *Solucionador de problemes de rendiment*, feu clic en el botó Inicio i, a continuació, aneu al tauler de control. En el quadre de cerca, escriviu "solucionador de problemas" i a continuació feu clic en *Solució de problemes*. En Sistema i seguretat, feu clic a Buscar problemes de rendiment. El sistema analitzarà l'equip i us mostrarà un diàleg amb els problemes de rendiment detectats i us proposarà la seva resolució.

3.5.2 Eliminar programes que no s'utilitzin mai

Molts fabricadors d'equips ens faciliten el nous equips amb programes que no vàreu demanar i que potser no necessiteu. Sovint, inclouen edicions de prova i versions d'edició limitada de programes que les empreses de programari desitgen que l'usuari provi, trobi útil i, després, pagui per actualitzar a les versions completes o les versions més noves. Si decidiu que no voleu aquests programes, heu de tenir en compte que conservar el programari en l'equip pot disminuir la velocitat en usar memòria valuosa, espai en disc i potència de processament.

Una bona idea és desinstal·lar tots els programes que no tenim intenció d'utilitzar. Això ha d'incloure tant el programari instal·lat pel fabricant com el programari que heu instal·lat vosaltres mateixos i que ja no utilitzeu; especialment, els programes d'utilitats dissenyats per administrar i ajustar el maquinari i el programari de l'equip. Els programes d'utilitats, com antivirus, netejadors de discos i eines de còpies de seguretat, s'executen, generalment, de manera automàtica en l'inici i queden actius en segon pla on no els podem veure. Molts usuaris, fins i tot, no tenen ni idea que s'estan executant.

Fins i tot si el vostre equip és més antic, pot contenir programes instal·lats pel fabricant que mai es van utilitzar o que es vareu oblidar que existien. Mai és massa tarda per desinstal·lar-los i desfer-se dels recursos del sistema desordenats i desaprofitats.

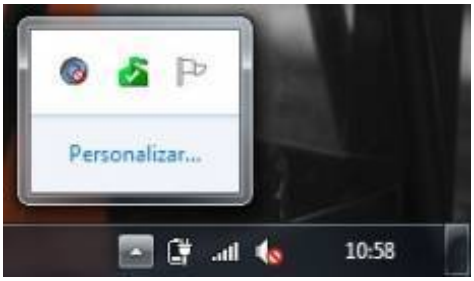
3.5.3 Limitar quants programes s'executen en l'inici

Molts programes estan dissenyats per iniciar-se automàticament quan s'inicia Windows. Els fabricants de programari, sovint, configuren els seus programes perquè s'obrin en segon pla (on no es pot veure que s'estan executant). Per tant, s'obriran directament en fer clic en les seves icones. Això resulta útil per als programes que s'usen amb més freqüència; però per als programes que mai s'usen o que s'usen amb poca freqüència, es malgasta memòria valuosa i es ralenteix el temps que utilitza Windows 7 a realitzar l'inici del sistema.

Decidir si un programa s'inicia automàticament

Però, com es pot saber quins programes s'executen automàticament en l'inici? De vegades resulta obvi perquè el programa agrega una icona a l'àrea de notificació en la barra de tasques, on pot veure que s'està executant. Podeu observar allà si hi ha algun programa en execució que no desitgeu que s'iniciï automàticament. Col·loqueu el cursor sobre cada icona per veure el nom del programa. Assegureu-vos de fer clic en el botó *Mostrar icones ocultes*, de manera que pugui veure totes les icones. Vegeu figura 3.4.

FIGURA 3.4. Veure programes iniciats automàticament



Aquesta aplicació està destinada a usuaris avançats i convé estar ben segur del que es realitza al modificar cap configuració.

Fins i tot després de comprovar l'àrea de notificació, poden quedar alguns programes que s'executen automàticament en l'inici. *Execucions automàtiques per Windows*, és una eina gratuïta de Microsoft que ens permet descobrir totes les aplicacions que s'executen a l'inici del sistema juntament amb Windows. Si voleu obtenir més informació podeu visitar l'enllaç: bit.ly/2PSmAxh

Alguns usuaris prefereixen administrar els programes que s'executen en l'inici mitjançant l'eina Configuració del sistema, una eina avançada que ajuda a identificar problemes que podrien impedir que Windows s'iniciés correctament.

Per obrir *Configuració del sistema*, feu clic successivament en el botó Inicio > Panell de control > Sistema i seguretat > Eines administratives i, a continuació, feu doble clic en *Configuració del sistema*. Són necessaris privilegis d'administrador. A la pestanya *Serveis* o *Inici de Windows* podem escollir les aplicacions i serveis que s'iniciaran automàticament.

3.5.4 Desfragmentar el disc dur

La fragmentació fa que el disc dur realitzi treball addicional que pot ralentir l'equip. El Desfragmentador de disc torna a organitzar les dades fragmentades de manera que el disc dur pugui funcionar de manera més eficaç. Aquesta eina s'executa segons una programació, però també és possible desfragmentar el disc dur de manera manual.

3.5.5 Netejar el disc dur

Els arxius innecessaris del vostre disc dur ocupen espai en disc i poden ralentir l'equip. L'Alliberador d'espai en disc elimina arxius temporals, buida la paperera de reciclatge i esborra diversos arxius del sistema i altres elements que ja no necessita.

3.5.6 Executar menys programes al mateix temps

En ocasions, canviar el comportament de l'equip pot generar un gran impacte en el rendiment del seu equip. Si sou el tipus d'usuari que desitja tenir vuit programes i

una dotzena de finestres de l'explorador oberts alhora (tot mentre envieu missatges instantanis als vostres amics), no us sorprengueu si el vostre equip es ralentitza. Mantenir molts missatges de correu electrònic oberts també pot consumir molta memòria.

Si el vostre equip funciona amb més lentitud, pregunteu-vos si realment necessiteu mantenir tots els programes i les finestres obertes al mateix temps.

Assegureu-vos d'executar únicament un programa antivirus. Executar més d'un programa antivirus també pot ralentitzar l'equip. Tot i això, si executeu més d'un programa antivirus, el *Centre d'activitats* de Windows us ho notificarà i pot ajudar-vos a resoldre el problema.

3.5.7 Desactivar efectes visuals

Si Windows s'executa lentament, es pot augmentar la seva velocitat deshabilitant alguns efectes visuals. Simplement es tracta de decidir entre aparença i rendiment. Preferiu que Windows s'executi més ràpidament o que tingui un aspecte més bonic? Si el vostre equip és prou ràpid, no cal renunciar a cap de les dues coses; però si l'equip amb prou feines pot funcionar amb Windows 7, pot resultar útil reduir les qualitats visuals extra.

Es poden triar quins efectes visuals es volen desactivar, d'un en un, o permetre que Windows els triï automàticament. Hi ha 20 efectes visuals que es poden controlar, com l'aspecte de cristall transparent, la forma en la qual s'obren o tanquen els menús i si es mostren les ombres.

Per ajustar tots els efectes visuals a fi d'obtenir un millor rendiment:

1. Accediu a *Informació i eines de rendiment*, per fer-ho, feu clic en el botó Inicio i, a continuació, feu clic en Panell de control. En el quadre de recerca, escriviu *Informació i eines del sistema* i, a continuació, en la llista de resultats, feu clic en Informació i eines de rendiment.
2. Feu clic a *Ajustar efectes visuals*. Per a fer-ho, són necessaris els permisos d'administrador.
3. Feu clic en la fitxa *Efectes visuals*, a *Ajustar per obtenir el millor rendiment* i, a continuació, feu clic a Acceptar. (Per a un opció menys dràstica, seleccioneu *Deixar que Windows triï la configuració més adequada per a l'equip*).

3.5.8 Reiniciar amb regularitat

Aquest suggeriment és simple. Reinicieu el vostre equip almenys una vegada per setmana, especialment, si l'utilitzeu molt. Reiniciar un equip és una bona forma

de netejar la memòria i assegurar-se que els processos i serveis que van començar a executar-se s'apaguin.

En reiniciar, es tanquen tots els programes de programari que s'estan executant en l'equip; no solament els programes que es veuen que s'estan executant en la barra de tasques, sinó també dotzenes de serveis que poden haver estat iniciats per diversos programes i que mai es van aturar. Reiniciar pot solucionar problemes misteriosos de rendiment quan és difícil detectar el motiu exacte.

3.5.9 Agregar més memòria

Si un equip amb Windows 7 és massa lent, en general, es deu al fet que l'equip no posseeix RAM suficient. La millor forma d'augmentar la seva velocitat és agregar més memòria.

Windows 7 es pot executar en un equip amb 1 GiB de RAM, però s'executa millor amb 2 GiB. Per a un rendiment òptim, augmenteu a 3 GiB o més.

Una altra opció és augmentar la quantitat de memòria mitjançant *Windows ReadyBoost*. Aquesta característica permet usar l'espai d'emmagatzematge en alguns dispositius de mitjans extraïbles, com ara unitats USB, per augmentar la velocitat de l'equip. És més senzill connectar una unitat flaix a un port USB que obrir el vostre portàtil i connectar els mòduls de memòria en la placa base. Per obtenir més informació sobre ReadyBoost podeu visitar el següent enllaç: bit.ly/2DEnDJT.

3.5.10 Comprovar si hi ha virus i spyware

Si l'equip s'executa lentament, és possible que estigui infectat per un virus o spyware. Això no és tan freqüent com els altres problemes, però és alguna cosa que heu de tenir-se en compte.

Un símptoma freqüent de la presència d'un virus és un funcionament molt més lent del normal. Altres signes inclouen missatges inesperats que apareixen en l'equip, programes que s'inicien automàticament o el so que indica que el disc dur treballa constantment.

> L'spyware és un tipus de programa que s'instal·la, en general, sense el vostre coneixement per observar la vostra activitat a Internet.

Podeu comprovar si hi ha spyware amb *Windows Defender* o altres programes anti-spyware.

La millor forma de combatre els virus és, en primer lloc, impedir la seva existència. Executeu sempre un programari antivirus i manteniu-lo actualitzat. Fins i tot,

encara que preneu totes les precaucions possible, és probable que el vostre equip s'infecti de totes formes.

3.6 Arxius de xarxa sense connexió

Mitjançant els arxius de xarxa sense connexió podem tenir accés als arxius emmagatzemats en carpetes de xarxa compartides tot i que aquestes no estiguin disponibles. Per fer això, es pot escollir quins fitxers de la unitat compartida en xarxa volem tenir sempre disponibles o a quins directoris complets volem tenir accés. Un cop escollits, es crea una còpia automàtica en el nostre sistema. Aquestes còpies s'anomenen *arxius sense connexió*. El Windows s'encarregarà de sincronitzar automàticament els arxius sense connexió la propera vegada que la unitat compartida estigui disponible.

Utilitzant aquest sistema, sempre que el nostre equip es pugui connectar a l'equip remot, tindrem accés als fitxers emmagatzemats en aquest. Si en algun moment es perd aquesta connexió, tindrem accés als arxius emmagatzemats en l'equip local.

3.6.1 Motius per utilitzar els arxius sense connexió

Els arxius sense connexió ofereixen diferents avantatges a tots els usuaris que treballin amb arxius emmagatzemats en carpetes compartides. Utilitzant els arxius sense connexió podreu:

- **Protegir-vos dels talls de xarxa.** Quan s'utilitzen arxius sense connexió, no importa si la xarxa ha deixat de funcionar o la carpeta de xarxa deixa d'estar disponible. Si es produeix alguna d'aquestes circumstàncies, el Windows tindrà accés automàtic a les còpies locals sense connexió en lloc dels arxius en xarxa, i podreu continuar treballant sense interrupcions.
- **Treballar amb arxius quan no esteu en la xarxa.** Normalment, en desconnectar-se de la xarxa es perd la possibilitat de tenir accés als arxius emmagatzemats en aquesta. Amb els arxius sense connexió hi podreu continuar treballant encara que no estigueu connectats a la xarxa.
- **Sincronització senzilla amb els arxius de xarxa.** La sincronització entre els arxius emmagatzemats en el sistema i els arxius de xarxa es du a terme de manera senzilla únicament fent clic en un botó.
- **Augmentar l'eficiència en treballar en connexions lentes.** Si es treballa en una xarxa amb connexió lenta, treballar amb arxius emmagatzemats en una carpeta compartida pot ser ineficaç i lent. Els arxius sense connexió eviten aquest problema permetent passar fàcilment de les còpies en xarxa a les còpies locals.

Manteniment dels arxius sincronitzats

Quan se selecciona un arxiu o una carpeta de xarxa que està disponible sense connexió, el Windows crea automàticament una còpia d'aquest arxiu o carpeta en l'equip local. Sempre que es torni a connectar la carpeta de xarxa, el Windows sincronitzarà els arxius entre l'equip i la carpeta de xarxa. També es poden sincronitzar manualment en qualsevol moment.

Si es treballa sense connexió i es fan canvis en els fitxers locals, el Windows sincronitzarà els arxius la propera vegada que es connecti la carpeta de xarxa en qüestió.

Si es treballa sense connexió mentre una altra persona modifica els arxius de la carpeta compartida, el Windows sincronitzarà els canvis amb els arxius sense connexió la propera vegada que es connecti la carpeta de xarxa. Si també s'han canviat els arxius locals, es produirà un conflicte en la sincronització i el Windows preguntarà quina de les dues versions es vol mantenir.