Configuració i administració de commutadors

Víctor Carceler Hontoria, Eduard García Sacristán, Ramón Murillo Casals, Juan Carlos Pérez Vázquez, Jordi Prats Català, Oriol Torres Carrió

Adaptació de continguts: Eduard García Sacristán

Índex

Introducció

De vegades, la quantitat de *hosts* de les xarxes locals i el trànsit que aquests generen fan que el funcionament de les xarxes no sigui òptim a causa de la quantitat de col·lisions que es produeixen.

Els ponts i els commutadors serveixen per dividir les xarxes locals en segments de col·lisió més petits, i fan que els segments per separat siguin més eficients que la xarxa original. Els ponts i els commutadors són dispositius de capa d'enllaç (capa 2 del model OSI), per tant, fan servir la informació a nivell d'enllaç per filtrar el trànsit dins de la xarxa local (adreces MAC).

Per entendre el funcionament de les xarxes s'han de comprendre els diferents aspectes dels models i de les capes i els conceptes bàsics de les xarxes. També és important conèixer les diferents tecnologies a nivell físic i d'enllaç per connectar els diferents *hosts* dins d'una xarxa d'àrea local. Però fins ara no heu començat a treballar en la configuració i administració dels dispositius de connexió de xarxes. En aquesta unitat començareu per primera vegada a treballar amb dispositius de xarxes, a configurar-los i a administrar-los.

En l'apartat "Configuració de commutadors" veureu el concepte de domini de col·lisió i domini de col·lisió *broadcast*, i quins dispositius es fan servir per dividir-los. Posteriorment veureu com es configura el commutador: connexió al commutador, modes de funcionament del commutador i configuració de contrasenyes.

En l'apartat "Administració de commutadors", veureu com es fan les tasques comunes a qualsevol administrador de xarxa relacionades amb els commutadors. Aprendreu a treballar amb els fitxers de configuració, la configuració remota del commutador per mitjà de Telnet i SSH, l'administració de les taules MAC, l'administració de seguretat dels ports i la configuració del protocol de *spanning tree*.

La majoria dels continguts d'aquesta unitat tenen a veure amb la configuració de commutadors. És més que probable que no disposeu de cap commutador per estudiar la unitat a casa. Però es poden fer servir simuladors de xarxa per simular la connexió de diversos dispositius a una xarxa local (*hosts*, commutadors i encaminadors) i configurar-los. És recomanable que instal·leu un simulador de xarxa i aneu provant les diferents ordres que us anem presentant en els materials. Feu proves amb xarxes dins del simulador i proveu a canviar la configuració dels commutadors per comprovar com canvia el funcionament de la xarxa.

Per seguir els continguts d'aquest mòdul, és convenient anar fent les activitats i els exercicis d'autoavaluació i llegir els annexos. Tot i que les unitats formatives tenen un contingut important des del punt de vista conceptual, sempre s'ha procurat donar-los un enfocament pràctic en les activitats proposades.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Administra commutadors establint opcions de configuració per a la seva integració a la xarxa:
    - Connecta commutadors entre si i amb les estacions de treball.
    - Interpreta la informació que proporcionen els *leds* del commutador.
    - Utilitza diferents mètodes per accedir al mode de configuració del commutador.
    - Identifica els fitxers que guarden la configuració del commutador.
    - Administra la taula d'adreces MAC del commutador.
    - Configura la seguretat del port.
    - Actualitza el sistema operatiu del commutador.
    - Utilitza les ordres proporcionades pel sistema operatiu del commutador que permeten fer el seguiment de possibles incidències.
    - Comprova l'*Spanning Tree Protocol* a un commutador.
    - Modifica els paràmetres que determinen el procés de selecció del pont arrel.

1. Configuració de commutadors

Els ponts i commutadors són dispositius de comunicació de dades que funcionen a la capa 2 del model de referència OSI. Per aquest motiu, se'ls coneix sovint com a *dispositius d'enllaç de dades*.

Els ponts van estar disponibles comercialment al començament de la dècada dels anys vuitanta. Quan van aparèixer per primera vegada permetien la retransmissió de trames entre xarxes homogènies. Més endavant el funcionament dels ponts entre xarxes diferents va estar estandarditzat. Els ponts fan servir les adreces MAC per reenviar selectivament les trames entre diferents xarxes, dividint els dominis de col·lisió en dues parts.

Avui en dia, la tecnologia de commutació ha substituït els ponts. Els commutadors són una millora dels ponts augmentant-ne la capacitat amb la inclusió de més ports, fins al punt en què era possible tenir un únic *host* per cada port del commutador.

Els commutadors treballen amb un sistema operatiu propi que permet que els administradors hi treballin de manera còmoda.

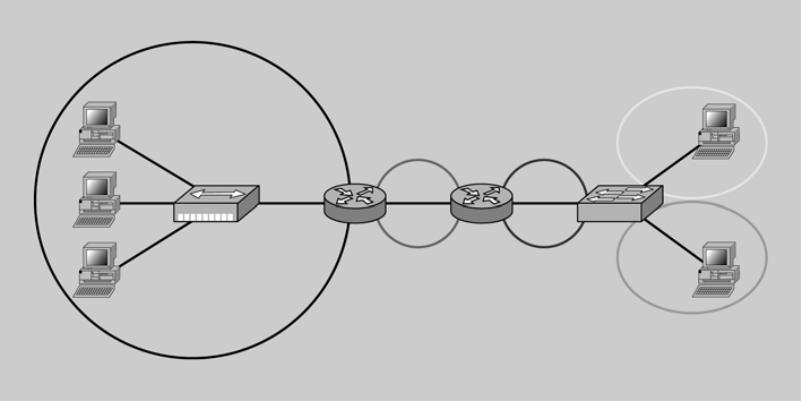
1.1 Segmentació de la xarxa

Tal com mostra la figura 1.1, un domini de col·lisió és un segment físic d'una xarxa d'ordinadors on hi ha possibilitats que els paquets xoquin, això és, en el cas en què dos ordinadors transmetin per un mitjà compartit.

Segment de xarxa

Un segment de xarxa és qualsevol mitjà de xarxa compartit com, per exemple, un cable i un dispositiu, és a dir, un commutador o un concentrador.

FIGURA 1.1. Cinc dominis de col·lisió



Ethernet funciona bé quan hi ha pocs *hosts* en la xarxa. En aquest cas el trànsit que hi ha en la xarxa és reduït, es produeixen poques col·lisions i la velocitat de funcionament de la xarxa és acceptable.

Però, quan augmenta la quantitat de *hosts* que volen enviar trames a la xarxa, també augmenta la quantitat de col·lisions i el rendiment de la xarxa comença a baixar, fins al punt de fer-la inoperativa si tenim massa *hosts* intentant fer enviaments al mateix temps.

Per aquest motiu va sorgir la necessitat de segmentar les xarxes.

Segmentar significa dividir un domini de col·lisió en dues o més parts, de manera que trames enviades en diferents segments no col·lisionin entre elles.

Els dispositius que es van dissenyar per segmentar xarxes s'anomenaven *ponts*. Els **ponts** s'encarreguen d'escoltar dels diferents segments i reenvien les trames que calgui als altres segments. Per fer això analitzen les adreces MAC d'origen i destinació de la trama.

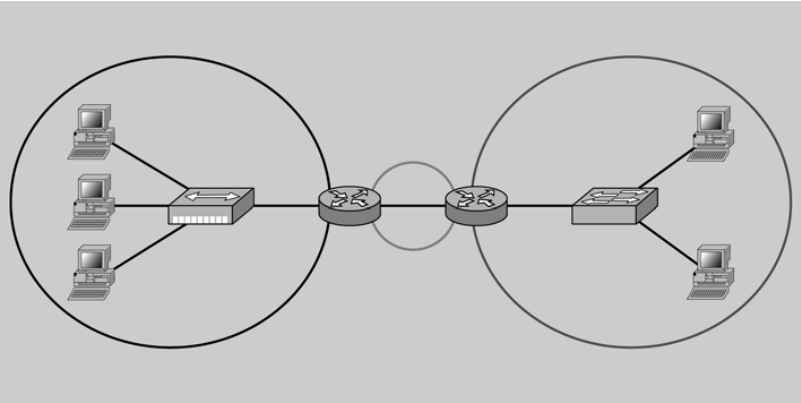
Els motius per segmentar una xarxa amb un pont són els següents:

- **Trànsit**. Es pot reduir el trànsit d'una xarxa segmentant-la amb un pont. En cas que molt del trànsit sigui local, aquest no cal que es propagui a tota la xarxa (per exemple: diferents departaments es comunicaran més amb les màquines del mateix departament, aquests paquets no cal que es propaguin per tots els segments).
- **Fiabilitat**. Un ordinador avariat que estigui transmetent dades contínuament a la xarxa pot col·lapsar tot el trànsit. Dividint en segments a soles es veuria afectada una part de la xarxa.
- **Connectivitat**. Amb un pont es poden connectar xarxes d'estàndards diferents (per exemple: un segment Ethernet amb un altre anell de testimoni o *token ring*).
- **Nombre d'ordinadors**. Algunes xarxes locals tenen un nombre màxim de *hosts* que poden estar connectats. Segmentant la xarxa, aquesta quantitat màxima de *hosts* seria per cada segment, i no per tota la xarxa.
- **Mida de la xarxa**. Es necessita que la xarxa cobreixi una distància més gran que la mida màxima que permet.
- **Seguretat**. En una xarxa de difusió o *broadcast*, qualsevol ordinador pot accedir a totes les trames que passen per la xarxa. Si es divideix en segments, només aquest ordinador podrà accedir a les trames que s'enviïn pel seu segment.

Des del punt de vista dels dispositius que hi ha en una xarxa, cal destacar que els ponts, els commutadors i els encaminadors segmenten dominis de col·lisió.
Els concentradors presenten un únic domini de col·lisió, és a dir, en cas que dos equips provoquin una col·lisió en un segment associat a un port del concentrador, tots els altres dispositius es veuen afectats (encara que estiguin connectats a diferents ports).

Tal com es veu en la figura 1.2, un domini de col·lisió *broadcast* (també anomenat *domini de difusió*) està constituït per tots els dispositius que estan connectats en una xarxa d'àrea local i que reben difusions de trames de dades enviades d'una màquina a totes les altres (trames *broadcast*). A grans trets, podem dir que un domini de col·lisió *broadcast* és un grup de dispositius de la xarxa que envien i reben missatges *broadcast* entre ells.

FIGURA 1.2. Tres dominis de col·lisió broadcast



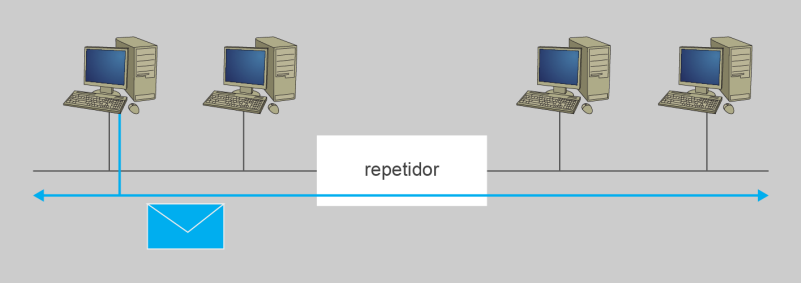
1.2 Ponts

Els dominis de col·lisió en una xarxa queden definits pels diferents dispositius que es fan servir per interconnectar els diferents segments de xarxa.

Els dispositius de capa 1 del model OSI (amplificadors i repetidors) no divideixen els dominis de col·lisió. Tot i que els dispositius no estan connectats físicament al mateix segment de cable, sí que estan connectats lògicament. Penseu que un amplificador i un repetidor retransmeten les trames per tots els segments on són connectats, per tant, les trames dels *hosts* col·lisionaran si aquests estan connectats a segments diferents per aquests dispositius de capa 1, com es pot veure en la figura 1.3.

Els dispositius de capa 1 estenen els segments de cable Ethernet, però no divideixen els segments de col·lisió.

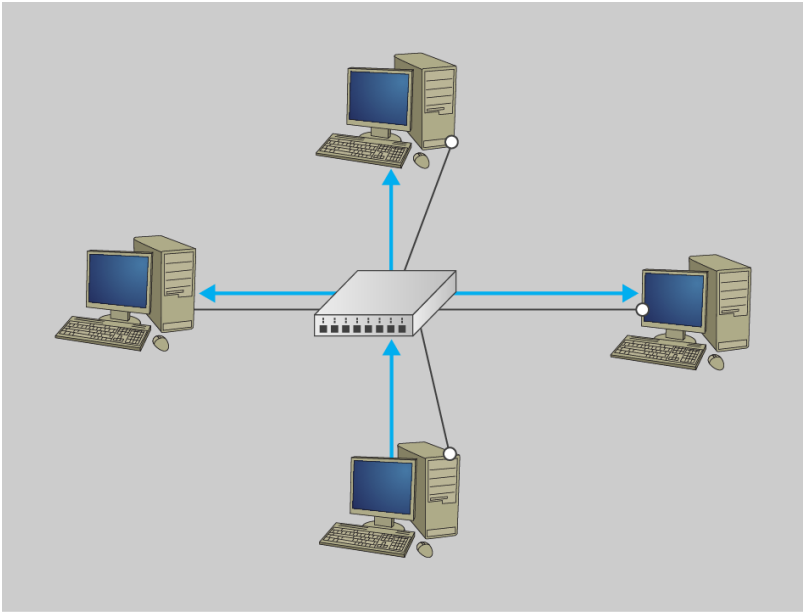
FIGURA 1.3. Xarxa amb repetidor



Els repetidors no divideixen segments de col·lisió.

Els concentradors es comporten de la mateixa manera. Centralitzen en un dispositiu la connexió de diferents segments de xarxa, però aquests estan tots connectats entre ells. Una trama enviada a un dels ports del concentrador es retransmet a la resta, com es pot veure en la figura 1.4.

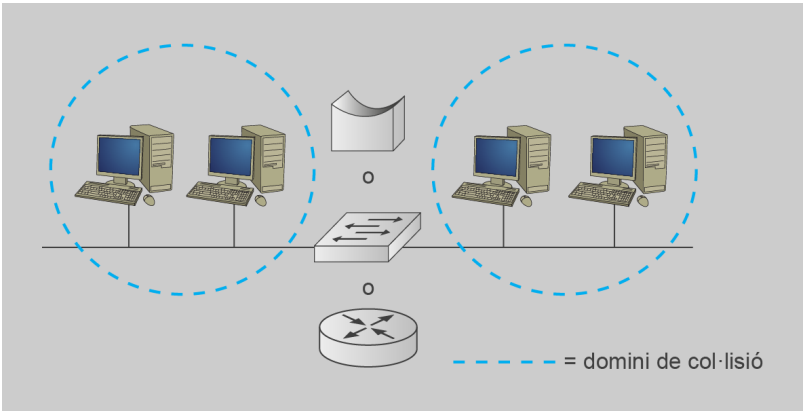
FIGURA 1.4. Funcionament d'un concentrador



El concentradors no divideixen segments de col·lisió.

Els dispositius de capa 2 (ponts i commutadors) i **capa 3** (encaminadors) sí que divideixen els dominis de col·lisió. Aquesta divisió es coneix com a *segmentació*, ja que si instal·leu un d'aquest dispositius enmig d'una xarxa, n'esteu dividint el domini de col·lisió en dos de més petits, com es pot veure en la figura 1.5.

FIGURA 1.5. Els ponts, els commutadors i els encaminadors divideixen els dominis de col·lisió.



Aquests dominis de col·lisió més petits tenen menys *hosts* i menys trànsit que el domini de col·lisió original. Com menys *hosts*, menys probabilitats que dos *hosts* facin un enviament alhora i, per tant, també menys probabilitats que es produeixin les col·lisions.

1.2.1 Funcionament dels ponts transparents

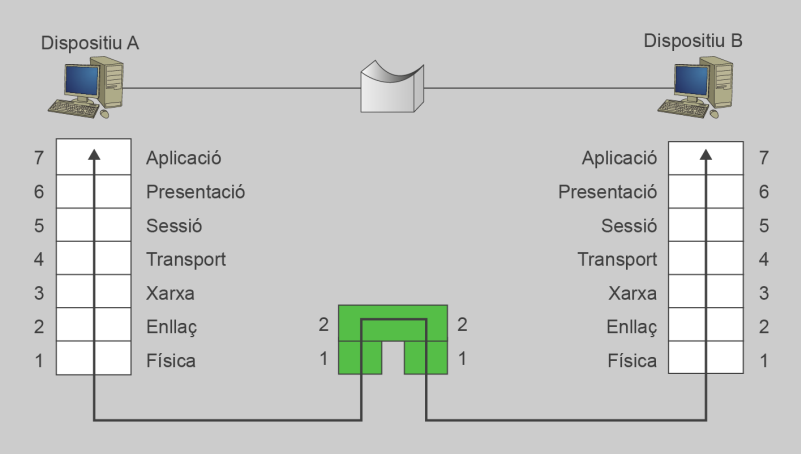
Ethernet és un mitjà compartit, això vol dir que únicament pot enviar un *host* alhora. A mesura que s'afegeixen més nodes a un domini de col·lisió, la probabilitat de col·lisió en el mitjà físic augmenta. Quan es produeix una col·lisió, tots els *hosts* que hi han participat han de retransmetre les trames, ja que aquestes han quedat irreconeixibles, i la xarxa ha perdut amplada de banda útil en retransmissions.

Una solució és segmentar un segment de xarxa gran en dominis de col·lisió més petits. Aquests dominis amb menys *hosts* tindran menys probabilitats de col·lisió i, per tant, s'aprofitarà millor l'amplada de banda de la xarxa. Els ponts són els dispositius que es van dissenyar per a aquest propòsit, per dividir dominis de col·lisió.

Els primers ponts s'anomenaven **ponts transparents** (en anglès, *transparent bridges*), ja que el seu funcionament era totalment transparent per als *hosts* de la xarxa on estaven connectats. Els ponts es podien fer servir sense haver de fer cap tipus de modificació o configuració en els *hosts* o en el protocol de xarxa utilitzat. Aquest nom (*ponts transparents*) encara es fa servir amb freqüència per referir-se als ponts.

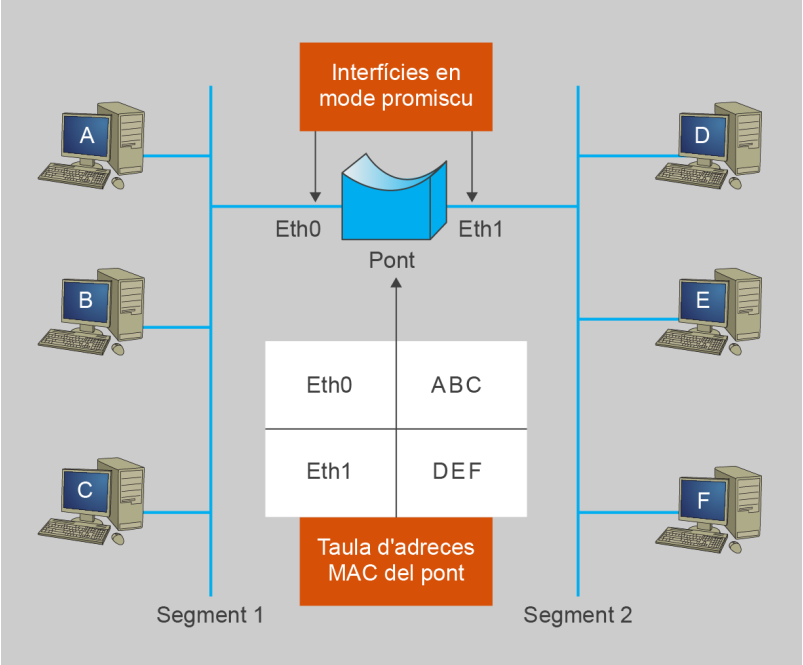
Els ponts treballen a nivell 2 del model OSI, com es pot veure en la figura 1.6.

FIGURA 1.6. Els ponts en el model OSI



Quan un pont s'engega, aprèn la localització dels *hosts* analitzant l'adreça MAC d'origen de les trames a les quals està connectat directament per mitjà dels seus ports. En tot moment el pont funciona en mode promiscu, escoltant totes les trames que s'envien per tots els segments de xarxa als quals està connectat (independentment de l'adreça de destinació de la trama).

FIGURA 1.7. Funcionament d'un pont transparent



Mireu per exemple la figura 1.7. Si el pont rep per la interfície Eth0 una trama amb adreça MAC d'origen A, el pont arriba a la conclusió que el *host* A es pot trobar a partir del segment que està connectat a aquesta interfície, en aquest cas la LAN A accessible per Eth0. En realitat, el *host* A pot ser en el segment al qual està connectat la interfície Eth0 (LAN A), o podria ser en un altre segment al qual s'accedeix des d'aquest segment. Per exemple, en la LAN A hi podria haver un altre pont que connectés amb una altra LAN on podria ser el *host*.

A partir d'aquest procés en què el pont veu on es troben els *hosts* a partir de les adreces MAC d'origen de les trames, el pont construeix una taula (el que es coneix com a *procés d'aprenentatge*) com la que es pot veure aen la taula 1.1.

TAULA 1.1. MAC del pont

Adreça del host	Interfície del pont
A	Eth0
B	Eth0
C	Eth0
D	Eth1
E	Eth1
F	Eth1

La taula MAC conté la relació d'interfície i adreça MAC dels hosts

Propagació per inundació

En la propagació per inundació, un dispositiu de xarxa propaga una trama o paquet de dades per totes les interfícies que té, excepte la que ha rebut la trama o paquet. D'aquesta manera propaga la trama per tota la xarxa. En la qual, si hi ha bucles, hi pot haver un problema de trames que donen voltes indefinidament per la xarxa.

Aquesta taula es coneix com a **taula MAC del pont**.

El pont fa servir aquesta taula per saber si les trames que escolta per les seves interfícies han de passar a l'altre segment de xarxa. Quan el pont rep una trama per qualsevol de les seves interfícies, consulta l'adreça MAC de destinació en la taula MAC.

Poden passar dues coses:

- Que l'adreça MAC de destinació no es trobi en la taula MAC: en aquest cas el pont no sap on és el *host* de destinació. Per assegurar-se que la trama arriba al seu destinatari el pont reenvia la trama per totes les interfícies a les quals està connectat excepte per on ha arribat. Això es coneix com a **propagació per inundació**.
- Que l'adreça MAC es trobi en la taula MAC. Aquí el funcionament del pont depèn d'on sigui l'adreça de destinació en la taula MAC. De nou ens podem trobar amb dos casos diferents:
  - L'adreça MAC de destinació es troba en la mateixa interfície per la qual ha arribat la trama al pont. En aquest cas, tant el *host* destinatari com l'emissor es troben en el mateix segment de xarxa. No cal retransmetre aquesta trama, per tant, el pont no fa res.
  - L'adreça MAC de destinació es troba en la taula MAC en una interfície diferent de la interfície per la qual ha arribat aquesta trama al pont. En aquest cas, el pont retransmet la trama per la interfície on es troba el *host* de destinació.

Les trames *broadcast* i *multicast* es propaguen sempre per totes les interfícies del port, excepte per on ha arribat la trama (per inundació). Les trames *broadcast* han d'arribar a tota la xarxa, per tant, és normal que es retransmetin així. La gestió dels grups *multicast* es fa en capes superiors del model OSI (capa de xarxa), per tant, a nivell d'enllaç (que és on treballen els ponts) no es tracten.

El **ponts** segmenten dominis de col·lisió i filtren el trànsit analitzant les adreces MAC de les trames.
Els ponts no segmenten els dominis de col·lisió *broadcast*.

Exemple de funcionament del pont

Imaginem els equips del cas de la xarxa que es mostra en la figura 1.7. Tant els *hosts* com el pont s'acaben d'engegar, per tant, la taula d'adreces MAC està buida. El *host* A envia una trama al *host* B. Aquesta trama es propagarà per tot el segment de col·lisió 1 arribant a B, C i la interfície Eth0 del pont. Cadascun dels dispositius farà el següent:

- ***Host* B**. la targeta de xarxa de B comprova l'adreça MAC de destinació de la trama que està escoltant i com coincideix amb la pròpia, copia la trama en memòria i l'envia a la capa de xarxa.
- ***Host* C**. La targeta de xarxa de C comprova l'adreça MAC de destinació de la trama que està escoltant i, com que no coincideix amb la l'adreça MAC de la seva targeta, la descarta.

- **Pont**. Hem dit que els ports del pont funcionen en mode promiscu, per tant, tracten totes les trames que escolten del mitjà, independentment de si l'adreça MAC de destinació és la seva o no. El pont fa dues coses:
  - Comprova si l'adreça MAC de destinació (B) es troba en la taula MAC. Com que no és així (al començament la taula MAC és buida), propaga la trama per inundació (transmet la trama per totes les interfícies excepte per on ha arribat, en aquesta la propaga a Eth1, on tots els ordinadors la descartaran).
  - Inclou el *host* A en la taula MAC. Com que la trama procedent de A hi ha arribat per la interfície Eth0, pot deduir que per arribar a A haurà de transmetre les trames per aquesta interfície.

El contingut de la taula MAC després d'aquest enviament el podeu veure en la taula 1.2.

Taula 1.2. Taula MAC del pont

Adreça del host	Interfície del pont
A	Eth0

Taula MAC després de l'enviament d'A cap a B

A continuació el *host* F envia una trama dirigida cap a A. Aquesta trama es propaga pel segment de col·lisió 2 i arriba als *hosts* D i E i a la interfície Eth1 del pont. Els *hosts* D i E descarten la trama, ja que no es dirigeix a ells (comproven que l'adreça MAC de destinació no correspon a la pròpia). La interfície Eth1 del pont accepta la trama, ja que funciona en mode promiscu i fa dues coses:

- Comprovar si l'adreça MAC de destinació es troba en la taula d'adreces MAC del pont. En aquest cas sí és així, i envia la trama per la interfície que li indica la taula (Eth0).
- Fitxar l'emissor. Introdueix F en la taula MAC.

La taula 1.3 mostra el contingut de la taula MAC després d'aquest enviament.

Taula 1.3. Taula MAC del pont

Adreça del host	Interfície del pont
A	Eth0
F	Eth1

Taula MAC després de l'enviament de F cap a A

Vegem a continuació un tercer enviament, en aquest cas de D cap a F. De nou, la trama es propaga per tot el domini de col·lisió B i arriba a E, F i el pont. Cadascun dels dispositius farà el següent:

- ***Host* F**. La targeta de xarxa de F comprova l'adreça MAC de destinació de la trama que està escoltant i com coincideix amb la pròpia, copia la trama en memòria i l'envia a la capa de xarxa.

- ***Host* E**. La targeta de xarxa de E comprova l'adreça MAC de destinació de la trama que està escoltant i, com que no coincideix amb la l'adreça MAC de la seva targeta, la descarta.
- **Pont**. El pont fa dues coses:
  - Comprova si l'adreça MAC de destinació (F) es troba en la taula MAC. En aquest cas sí que s'hi troba. A més a més, l'adreça MAC de destinació (F) la té enregistrada en la taula que es troba en la mateixa interfície (Eth1) per la qual li ha arribat la trama. El pont entén (encertadament) que si F es troba per Eth1 i la trama li ha arribat des d'Eth1, aquesta trama ja li haurà arribat a F i, per tant, **no la propaga** a l'altre port.
  - Inclou el *host* D en la taula MAC.

La taula 1.4 mostra el contingut de la taula MAC després d'aquest enviament.

TAULA 1.4. Taula MAC del pont

Adreça del host	Interfície del pont
A	Eth0
F	Eth1
D	Eth1

Taula MAC després de l'enviament de D cap a F

En resum, quan rep una trama, el pont:

- Comprova l'adreça MAC d'origen i fitxa l'emissor en la taula MAC amb la interfície per la qual ha arribat la trama.
- Comprova l'adreça MAC de destinació i:
  - Si no es troba en la taula MAC, propaga la trama per inundació.
  - Si la troba per la mateixa interfície per la qual ha arribat la trama, no propaga la trama, ja que aquesta ja haurà arribat a la destinació.
  - Si la troba per una interfície diferent, propaga la trama per la interfície on es troba la destinació.

És en els casos en què el pont troba l'adreça MAC de destinació en la mateixa interfície per on li arriba la trama (i, per tant, no la propaga) on el pont fa la seva funció de filtratge de trànsit entre els diferents segments de col·lisió.

Per adaptar-se als canvis de la xarxa (per exemple, un ordinador es desconnecta i es torna a connectar en un altre segment de la xarxa), les entrades en la taula MAC tenen un temps de caducitat. Passat un temps sense que l'adreça no hagi enviat cap trama a la xarxa, s'esborra de la taula.

El ponts transparents aïllen el trànsit entre els diferents segments, per tant, redueixen el trànsit total de la xarxa. Aquest filtratge es produeix quan els dos *host* que es comuniquen es troben en el mateix segment. En aquest cas, el trànsit

no es propaga pels ponts a la resta de segments, la qual cosa redueix les col·lisions i fa que s'aprofiti millor l'amplada de banda. Quant es millorarà el rendiment de la xarxa depèn de la quantitat de trànsit hi hagi entre els diferents segments de xarxa i la quantitat de trànsit *broadcast* i *multicast*.

1.3 Commutadors

Avui en dia, la tecnologia de commutació (i els dispositius que la fan servir: els commutadors) s'ha establert com a substitut dels ponts. Els commutadors dominen l'espai que abans ocupaven els ponts en el disseny de xarxes anteriors.

Els commutadors tenen un rendiment superior al dels ponts, una quantitat més alta de ports, un cost per port inferior i una gran flexibilitat a l'hora de configurar-los. Tot això ha contribuït al fet que els commutadors hagin substituït pràcticament per complet els ponts de les xarxes.

1.3.1 Característiques dels commutadors

En general, els ponts únicament tenen dos ports i divideixen un domini de col·lisió en dues parts. Un **commutador** de xarxa d'àrea local (*LAN switch* en anglès) és un dispositiu que funciona de manera semblant a un pont, però té més ports. Això permet segmentar una xarxa, no ja en dues parts, sinó en múltiples (fins al punt de poder tenir un únic *host* per cada port). La quantitat superior de ports també incrementa l'amplada de banda disponible per als *hosts*.

Interfície o port?

A efectes pràctics es fa servir indistintament la paraula *port* o *interfície* per referir-se a les diferents interfícies físiques dels dispositius de xarxa.

La tendència cap a un nombre inferior d'usuaris per segment es coneix com a *microsegmentació*. La microsegmentació permet la creació de segments privats o dedicats, és a dir, un usuari per segment.

Les xarxes locals basades en commutadors es coneixen com a **xarxes locals commutades** (en anglès, *switches LAN*).

Així doncs, un commutador és bàsicament un pont multiport, i pot tenir dotzenes de ports. En lloc de crear únicament dos dominis de col·lisió, com feien els ponts, cada port del commutador constitueix un domini de col·lisió. En un commutador amb deu ports amb un *host* connectat a cada port, hi ha deu dominis de col·lisió, un per cada port i *host*. Cada un d'aquest dominis de col·lisió és un mitjà compartit (el cable) amb únicament dos dispositius, que volen enviar (el *host* i el propi commutador).

Full-duplex

Una comunicació *full-duplex* és aquella en què la informació es pot enviar en els dos sentits simultàniament. Un exemple de comunicació *full-duplex* seria la comunicació per mitjà de telèfons.

En aquest cas, les targetes de xarxa del *host* i el port del commutador es poden configurar per funcionar en mode *full-duplex*. Quan es fa servir cablejat de parell trenat, un parell serveix per enviar el senyal del commutador al *host*, i l'altre per a la comunicació entre el *host* i el commutador. Aquests senyals es poden transmetre de manera simultània i es poden produir comunicacions en totes dues direccions

al mateix temps (*full-duplex*). Treballant en mode *full-duplex* no hi ha col·lisions en el mitjà, ja que les comunicacions van per parells diferents. Desapareixent les col·lisions es diu que desapareix el domini de col·lisió, i l'amplada de banda (teòrica) de la connexió es duplica.

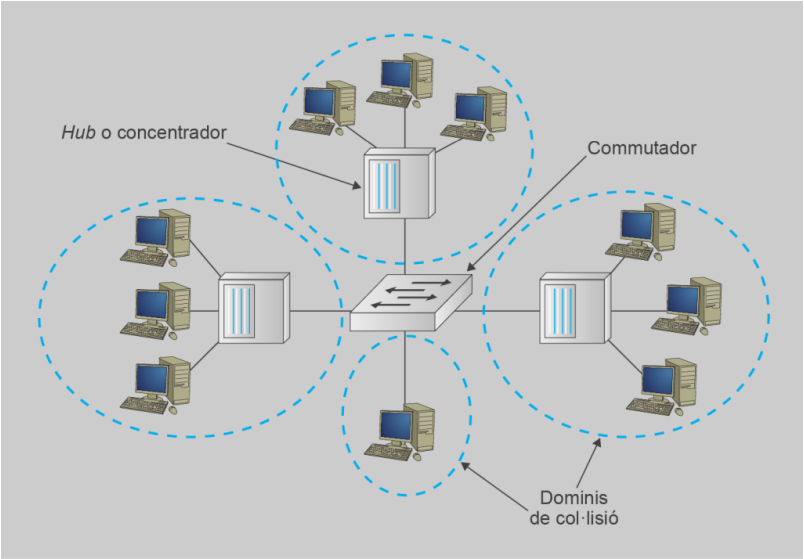
Cada *host* rep accés instantani a l'amplada de banda completa i no ha de competir per l'amplada de banda disponible amb altres *hosts*.

En la secció "Annexos" del web teniu un recurs que exemplifica de manera interactiva el funcionament d'un commutador.

Cada port defineix un domini de col·lisió i es pot connectar a aquest o bé a un *host*, o bé a un altre dispositiu de connexió de xarxes (com un altre commutador, un concentrador, etc.), com es pot veure en la figura 1.8.

El commutador continua tenint una taula d'adreces MAC amb la relació MAC-port per saber per on ha d'enviar les trames. A continuació podeu veure un exemple de la taula MAC d'un commutador.

Figura 1.8. Un commutador amb quatre ports fx6




```
Commutador_aula#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.424e.d7ae    DYNAMIC     Fa0/4
   1    000a.4178.63ce    DYNAMIC     Fa0/6
   1    0030.f27d.4bb5    DYNAMIC     Fa0/3
   1    00d0.ba4b.1b8c    DYNAMIC     Fa0/5
   3    0030.f298.31c4    DYNAMIC     Fa0/2
```

Entre les especificacions d'un commutador hi ha la memòria que té i la quantitat d'adreces MAC que pot emmagatzemar. Si la quantitat de *hosts* de la xarxa és superior a la quantitat d'adreces MAC que pot emmagatzemar el commutador, aquest esborrarà algunes adreces de la taula per desar-ne d'altres. Això provocarà un trànsit afegit a la xarxa, ja que les trames dels *hosts* que s'han esborrat de la taula es retransmetran per inundació, la qual cosa afectarà el rendiment de la xarxa.

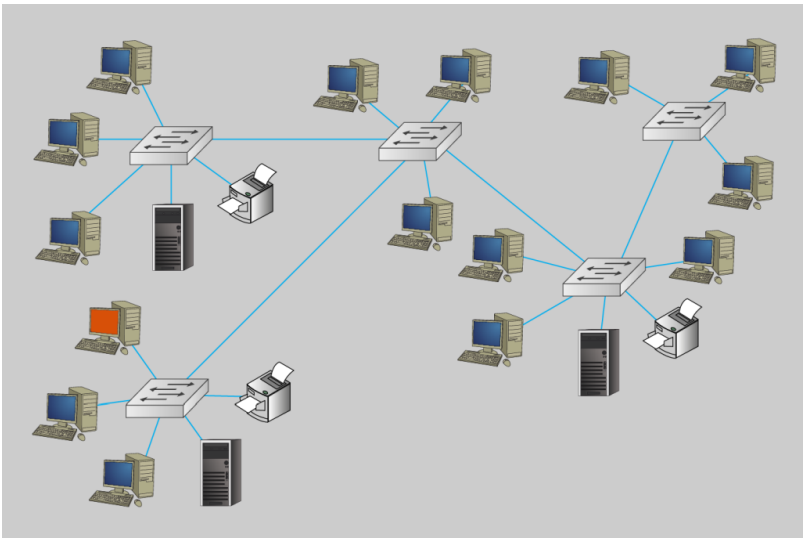
En el cas de xarxes Ethernet, l'ús de commutadors aporta una millora addicional al rendiment de la xarxa. Ethernet fa servir CSMA/CD com a protocol d'accés al mitjà. Amb CSMA/CD l'eficiència de la xarxa disminueix a mesura que augmentem el nombre de *hosts* en el domini de col·lisió. Per això, dividint una xarxa en diferents segments amb un commutador també en millorem el rendiment en tenir una quantitat de *hosts* inferior.

CSMA/CD

CSMA/CD (accés múltiple amb escolta de portadora i detecció de col·lisió, de l'anglès *carrier sense multiple access with collision detection*) és un mode d'accés al mitjà que es fa servir a Ethernet. Està basat en consultar l'estat del mitjà físic abans de transmetre. Mentre està transmetent, es fa una comprovació del mitjà per verificar que no es produeixen col·lisions.

Els commutadors, com els ponts, divideixen dominis de col·lisió. Les decisions que prenen estan basades en les adreces MAC de les trames que s'envien per la xarxa. Aquestes adreces corresponen a la capa 2 del model OSI o no afecten l'adreçament lògic de xarxa (capa 3). Així, els ponts i els commutadors divideixen els dominis de col·lisió, però no tenen efectes sobre els dominis de col·lisió *broadcast*. Les trames *broadcast* són retransmeses per tots els ports, pels ponts i pels commutadors, com es pot veure en la figura 1.9.

FIGURA 1.9. Xarxa commutada



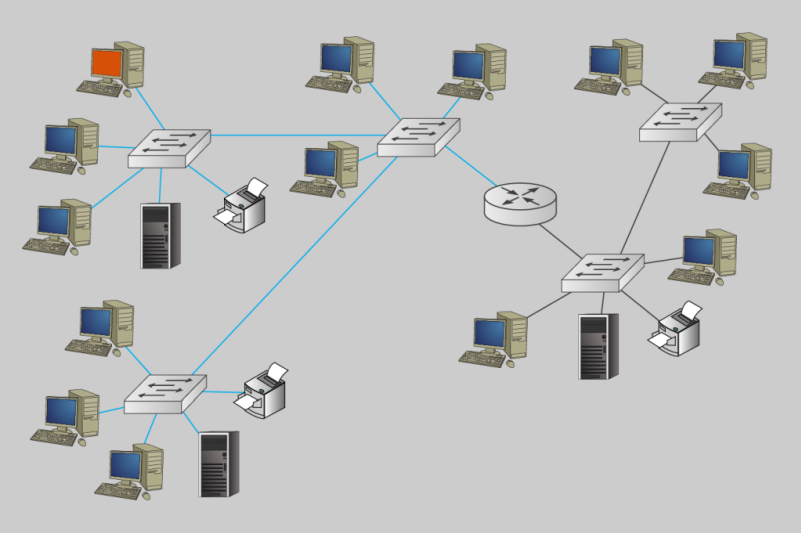
Els commutadors no divideixen dominis de col·lisió broadcast

Encara que els ponts i els commutadors redueixen els dominis de col·lisió, tots els *hosts* connectats als commutadors pertanyen al mateix domini de col·lisió *broadcast*. El encaminadors es poden fer servir per dividir dominis de col·lisió *broadcast*, ja que per defecte no retransmeten el trànsit *broadcast*. Creant diferents dominis de col·lisió *broadcast* amb un encaminador, es redueix el trànsit *broadcast* en la xarxa, i augmenta la disponibilitat d'amplada de banda per a les comunicacions *unicast*.

Per tant, no importa quants ponts i commutadors tenim en la xarxa, tota formarà part del mateix domini de col·lisió *broadcast*. Per dividir dominis de col·lisió *broadcast* s'han d'afegir a la xarxa dispositius de xarxa (capa 3 del model OSI) com els encaminadors (*routers*, en anglès). En el mateix cas, afegint un encaminador s'hauria dividit el domini de col·lisió *broadcast* de la xarxa, com es pot veure en la figura 1.10.

Els **ponts** i els **commutadors** divideixen dominis de col·lisió, però no dominis de col·lisió *broadcast*.
Els **encaminadors** divideixen dominis de col·lisió i dominis de col·lisió *broadcast*.

FIGURA 1.10. Xarxa amb encaminador



Els encaminadors divideixen dominis de col·lisió

1.3.2 Formes de commutació

Els commutadors poden commutar les trames entre els diferents ports seguint dues filosofies diferents:

- emmagatzematge i reenviament (en anglès, *store & forward*)
- travessant el commutador (en anglés, *cut-through*).

Els commutadors bàsicament funcionen com ponts multiport. Abans de retransmetre una trama fan una comprovació d'errors, recalculant el CRC (*Cyclic redundancy check*, codi de redundància cíclica) i comparant-lo amb el CRC emmagatzemat en la trama. Si en la comprovació d'errors és troben errades la trama es descarta; si els CRC coincideixen, la trama s'analitza per veure l'adreça MAC de destinació i poder-la reenviar pel port corresponent.

Per poder fer aquest procés de comprovació d'errors, el commutador s'ha d'esperar a rebre la trama sencera. Aquesta forma de funcionament dels commutadors es coneix com a **emmagatzematge i reenviament**.

El fet d'haver d'esperar a tenir la trama sencera introdueix un retard important en seva la propagació (moltes vegades superior al mateix procés de commutació). A més a més, si la trama ha de passar per més d'un commutador, aquest retard es multiplica pel nombre de commutadors, ja que la comprovació s'ha de fer en cada un. Si no s'hagués de fer la comprovació d'errors, el temps de commutació es

reduiria molt, ja que el commutador podria començar a retransmetre els primers bits de la trama a partir del moment d'haver rebut l'adreça MAC de destinació de la trama (no cal que el commutador esperi a rebre tota la trama sencera abans de començar la seva retransmissió). En aquest cas el commutador copia en el *buffer* únicament la informació suficient de la trama per poder llegir l'adreça MAC de destinació i així determinar a quin port s'han de reenviar les dades. L'adreça MAC de destinació es troba en els primers 6 bytes de la trama després del preàmbul.

Aquest mode de funcionament del commutador es coneix com a *funcionament* ***travessant el commutador***. El problema del mètode de funcionament de travessar el commutador, és que en no fer la comprovació d'errors, les trames incorrectes són reenviades pels commutadors fins que arriben a la destinació. Els *hosts* de destinació d'aquestes trames sí que fan la comprovació d'errors i descarten les trames (per tant, no hi ha perill que errades siguin rebudes pels *hosts*). En qualsevol cas, encara hi ha un problema, ja que es retransmet trànsit inútil amb dades errònies per la xarxa, omplint amplada de banda innecessàriament.

Per solucionar aquest problema, els commutadors que funcionen en mode travessant el commutador segueixen fent la comprovació de CRC, però després que la trama s'hagi commutat. Si el commutador detecta un errada no pot descartar la trama, ja que aquesta ja ha estat enviada pel port de destinació. Si se supera un llindar d'errades definit per l'administrador, el commutador posa aquest port "sota sospita" perquè està produint moltes errades i canvia el mode de funcionament a emmagatzematge i reenviament. Això té sentit, ja que un port amb molts errors té més possibilitats de seguir produint errades (per tenir un cable en condicions dolentes o una targeta de xarxa errònia en una estació).

Si passada una estona el port torna a tenir un índex d'errades per sota del llindar definit, es torna a funcionar amb el mètode de travessar el commutador.

També hi ha dues alternatives de la commutació pel mètode de travessar el commutador:

- **Commutació per enviament ràpid**. Ofereix les retransmissions més ràpides. Fa la retransmissió immediatament després d'haver llegit l'adreça de destinació. Si la trama té errades, aquesta es retransmet igual, ja que no fa comprovació d'errors.

- **Commutació lliure de fragments**. En aquesta forma de commutació, el commutador emmagatzema els primers 64 bytes de la trama i fa una comprovació abans de reenviar-la. El motiu d'emmagatzemar únicament els primers 64 bytes és que la majoria de les errades i col·lisions de la xarxa es produeixen en aquests primers 64 bytes. Es podria dir que aquesta forma de funcionament està a mig camí entre emmagatzematge i reenviament i commutació per travessar el commutador.

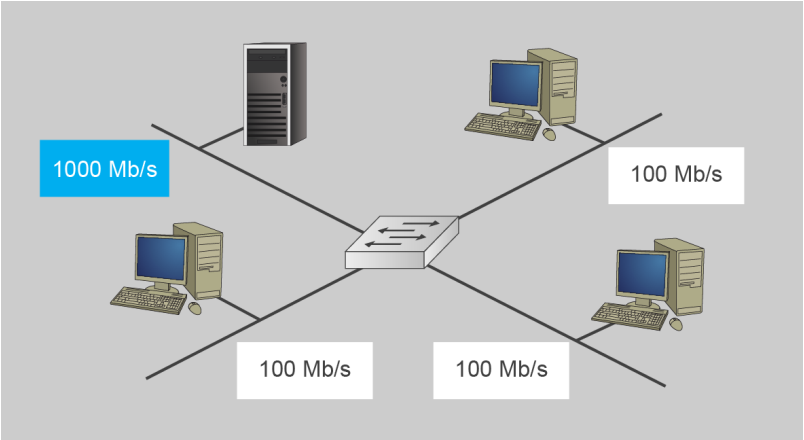
1.3.3 Commutació simètrica i asimètrica

La commutació es pot classificar en simètrica o asimètrica depenent de la manera d'assignar l'amplada de banda als ports dels commutadors.

La commutació **simètrica** dóna la mateixa amplada de banda a tots els ports d'un commutador. Per exemple, tots els ports del commutador poden treballar a 100 Mbps.

La commutació **asimètrica** proporciona diferents amplades de banda als diferents ports del commutador. Per exemple, uns ports poden funcionar a 100 Mbps i altres a 1.000 Mbps, com es pot veure en la figura 1.11. Això permet donar més amplada de banda als ports on sabem que tindrem més trànsit. Per exemple, es podria donar aquesta amplada de banda superior per la connexió amb un servidor o per la connexió de tots els *hosts* a un altre segment de xarxa, i evitar així colls d'ampolla en el funcionament de la xarxa. El fet que els ports puguin funcionar a diferents velocitats implica que el commutador ha de tenir *buffers* de memòria (memòria intermèdia) per emmagatzemar les trames que s'han de retransmetre. Per exemple, si s'envien trames d'un port que funciona a 100 Mpbs a un altre que funciona a 10 Mbps, el commutador ha de emmagatzemar les trames, ja que la velocitat amb què es reben les trames és deu vegades superior a la velocitat amb què es transmeten les trames de sortida.

FIGURA 1.11. Commutador amb assignació d'amplada de banda asimètrica



S'assigna més amplada de banda al port que connecta el servidor.

En l'actualitat la majoria dels commutadors són asimètrics, ja que ofereixen una funcionalitat més flexible.

1.4 Configuració del commutador

Els elements de connexió de xarxes (com commutadors i encaminadors) són peces de maquinari molt semblants a ordinadors personals. Tenen uns components

interns encarregats de fer els càlculs, encaminar o commutar i una sèrie de ports (també denominats *interfícies*) per comunicar-se amb l'exterior. Per facilitar el funcionament del maquinari (de la mateixa manera que passa amb els ordinadors personals) sobre aquest dispositiu s'executa un sistema operatiu.

En el cas dels dispositius Cisco, el sistema operatiu que corre sobre l'equipament és el Cisco IOS (*internetwork operating system*). Aquest sistema operatiu funciona en la majoria de dispositius Cisco (independentment del tipus d'equipament, commutadors, encaminadors, punts d'accés sense fil, etc.).

Cisco Systems

Cisco Systems és una de les empreses d'*Internetworking* més importants en l'actualitat. El seu nom és el sobrenom de la ciutat de San Francisco als Estats Units, a prop de la qual hi ha l'empresa, a l'anomenat Silicon Valley.

Per norma general, s'accedeix al sistema operatiu per mitjà d'una interfície de línia d'ordres o CLI (en anglès, *command line interface*). Depenent del tipus de dispositiu on estigui funcionant el Cisco IOS i la seva versió donarà accés a un tipus d'opcions i funcions o a d'altres.

Internament, un commutador consta dels elements següents:

- **Memòria RAM** (*random access memory*, memòria d'accés aleatori). És on emmagatzemen les dades temporals del commutador. A més, com en la memòria RAM de qualsevol ordinador, si hi ha un tall de corrent tot el que hi ha emmagatzemat s'esborra. També s'hi poden trobar els arxius de configuració mentre s'hi treballa.
- **Memòria NVRAM** (*non volatile RAM*, RAM no volàtil). Aquesta memòria emmagatzema la còpia dels arxius de configuració i inici del commutador. El contingut d'aquesta memòria no s'esborra si hi ha un tall del subministrament elèctric.
- **Memòria flaix**. És la ROM esborrable i reconfigurable que conté la imatge i el microcodi del sistema operatiu. No cal oblidar que un commutador és un ordinador i com a tal necessita un sistema operatiu per funcionar.
- **ROM** (*read only memory*, memòria només de lectura). Conté el diagnòstic d'engegada del sistema i programari del sistema operatiu. Per actualitzar el contingut de la ROM, cal extreure el circuit integrat de l'encaminador i substituir-lo per un de nou.
- **Interfícies**. Són les connexions de xarxa per on entren i per on s'envien les trames cap a les diferents xarxes.

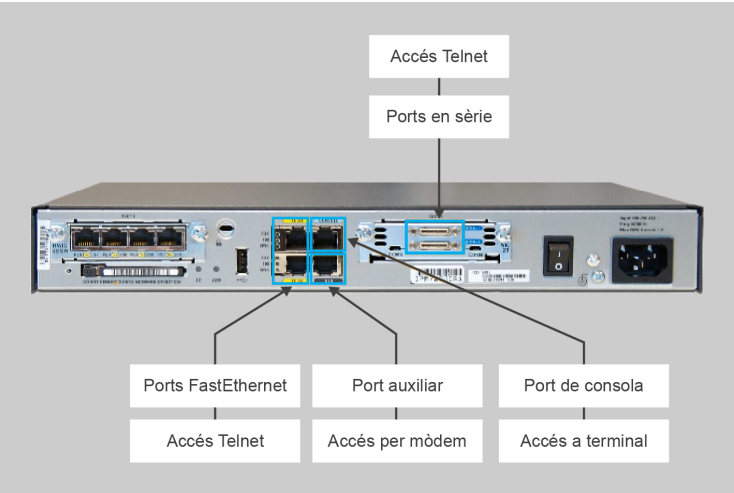
El IOS està emmagatzemat dins del dispositiu com un fitxer dins de la memòria flaix. Aquesta memòria és no volàtil (el seu contingut no s'esborra cada vegada que s'apaga el dispositiu). Es poden descarregar versions més noves del sistema operatiu simplement descarregant el fitxer amb la nova versió del sistema i carregant aquest fitxer en el dispositiu.

Els dispositius de connexió de xarxes (commutadors i encaminadors) no tenen cap pantalla per interactuar i tampoc no tenen una sortida per connectar un monitor, per tant, com hi podem treballar?

La manera d'administrar un commutador o encaminador és establint una connexió

des d'un ordinador. Hi ha tres maneres de connectar un dispositiu de xarxa, cada una associada a un port diferent, com es pot veure en la figura 1.12.

FIGURA 1.12. Ports d'un encaminador



- consola
- Telnet o SSH
- port aux

1.4.1 Connexió per consola

Aquest mètode fa servir el port de consola que es troba a la part posterior del dispositiu de xarxa. Aquest port es comunica a través d'una connexió sèrie de baixa velocitat per connectar el port de consola del dispositiu de xarxa al port sèrie (port COM) de l'ordinador. Per connectar-se a través de la consola caldrà un programa de comunicació pel port sèrie de l'ordinador com **minicom** en sistemes GNU/Linux o **hyperterminal** en sistemes MS Windows.

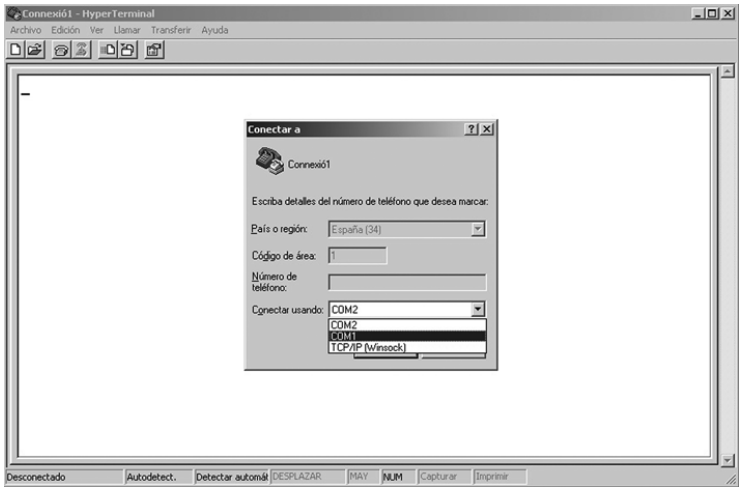
Per connectar-se amb el dispositiu amb cable de consola cal tenir accés físic a ell, ja que haurem de connectar un cable directament des del port sèrie de l'ordinador al port de consola del dispositiu.

Si el sistema operatiu que utilitzeu és un Windows, l'aplicació per realitzar aquesta connexió serà l'hyperterminal (figura 1.13). A partir de la versió XP el mateix sistema operatiu ja incorpora aquesta aplicació, per la qual cosa si treballeu amb una versió anterior us haureu de baixar una aplicació similar des d'Internet.

Un cop l'aplicació està en marxa, només cal introduir-hi un nom adequat per guardar el tipus de connexió i configurar el port (figura 1.14) amb el qual s'ha fet la connexió entre el commutador i la vostra màquina.

FIGURA 1.13. Hyperterminal

FIGURA 1.14. Elecció del port



Un cop seleccionat correctament el port al qual teniu el commutador connectat, cal configurar el programa per tenir una comunicació correcta entre el commutador i la vostra màquina. Penseu que una configuració incorrecta provocaria que les dues màquines no es pugessin entendre i, per tant, no veuríeu la pantalla de configuració del commutador, sinó només una pantalla en blanc en la qual no podríeu fer res. Si això passés, hauríeu d'aturar la connexió, tornar a configurar el programa adequadament i tornar a provar de fer la connexió.

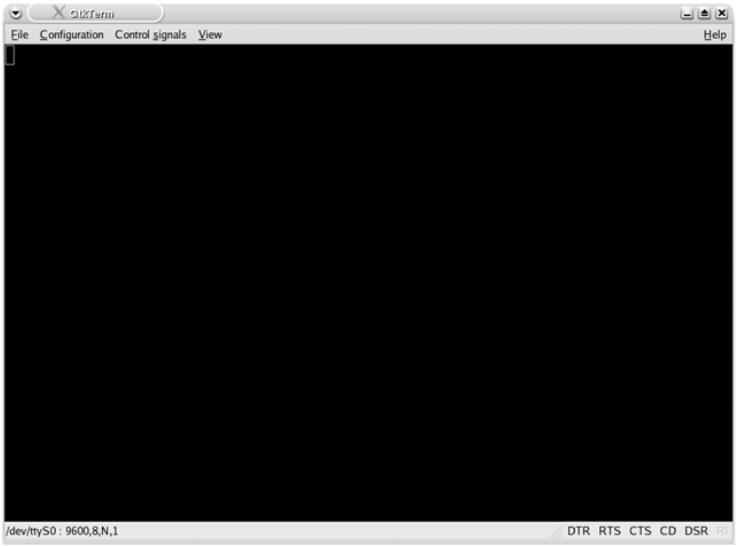
La pantalla que veieu en la figura 1.15 mostra les dades adequades per a la transmissió entre el vostre ordinador i el commutador: una velocitat de transferència de 9.600 bps, 8 bits de dades a cada trama transmesa, cap bit de paritat o control d'errors, un bit d'aturada i cap mena de control de flux.

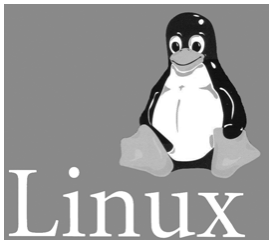
Després d'haver fet la configuració correctament, ja es pot començar la configuració del commutador.

FIGURA 1.15. Configuració de l'Hyperterminal

En cas que feu servir un sistema operatiu de codi obert -és a dir, un Linux-, es pot configurar el commutador amb l'aplicació gtkterm (figura 1.16), una aplicació molt similar a l'Hyperterminal que utilitza Windows. Si no disposeu d'aquesta aplicació, caldrà que us baixeu d'Internet el paquet rpm adient i us l'instal·leu.

FIGURA 1.16. Gtkterm

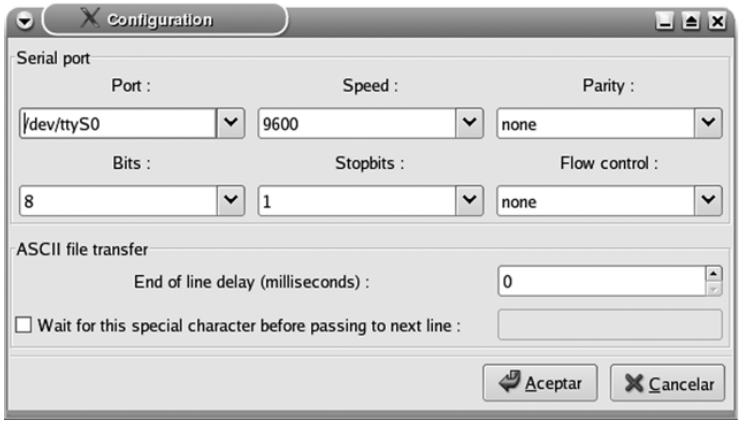




Logo Linux

L'aplicació de Linux també necessita una configuració per adaptar les dades a la velocitat del commutador. Per configurar-la, cal anar a Configuració i en el menú que es desplega seleccionar Port. Un cop seleccionat, s'obrirà la finestra de configuració de la figura 1.17.

FIGURA 1.17. Configuració de l'aplicació gtkerm



Configuració...

... de l'aplicació gtkterm per a la connexió entre l'ordinador i el commutador per transmetre la configuració. Si algun d'aquests paràmetres no coincideixen, la connexió no serà possible.

Cal seleccionar el port adient. Recordeu que utilitzeu Linux i el port COM 1 en Linux és el dispositiu /dev/ttyS0. La configuració ha de ser la mateixa que si utilitzéssiu Windows, ja que el commutador no té en compte el sistema operatiu de l'ordinador amb el qual es fa la connexió perquè disposa d'un sistema operatiu propi.

Un cop realitzades les configuracions oportunes, ja esteu en disposició de configurar un commutador. Com que segurament no disposareu de cap commutador o si en teniu algun no el voldreu utilitzar per no malmetre la configuració existent, farem servir un simulador per aprendre a configurar un commutador.

Abans d'arrencar el commutador per la seva configuració s'ha de confirmar el següent:

- Tots els cables de xarxa estan correctament endollats.
- El PC està connectat al port de consola del commutador. Per això heu de fer servir un cable de consola RJ-45 a DB-9 (port serial de l'ordinador).
- L'aplicació d'emulació de terminal, com hyperterminal, està funcionant i està configurada correctament.

A continuació s'ha d'endollar a la corrent elèctrica el commutador. Molts dels commutadors no tenen botó per apagar, per tant s'engegaran en aquest moment.

Quan s'engega el commutador s'inicia la prova POST. Durant aquesta prova, els leds del commutador poden parpellejar mentre es fan les proves. Finalment, el led LED SYST del commutador indicarà si ha passat la prova:

- **Verd**: parpelleja ràpidament en color verd si el POST ha sigut correcte.
- **Taronja**: vol dir que el commutador no ha passat el POST. En aquest cas es veurà un informe per la consola.

1.4.2 Connexió per Telnet i SSH

A diferència de la connexió de consola, la connexió per mitjà de Telnet i SSH (*secure shell*, intèrpret d'ordres segura) permet obrir una sessió de la CLI de manera remota als encaminadors. Per poder-se connectar amb el dispositiu de xarxa aquest ha de tenir actius els serveis de xarxa (com a mínim tenir configurada l'adreça IP d'una de les seves interfícies).

El Cisco IOS té un client i un servidor Telnet que serveixen per fer connexions remotes i permetre que altres dispositius es connectin a ell. Amb una d'aquestes connexions, es podria fer la configuració del dispositiu de xarxa. Per motius de seguretat s'ha de configurar una contrasenya per a la connexió remota per mitjà de Telnet.

També es pot fer servir SSH per fer connexions amb el dispositiu de xarxa. SSH és un protocol d'accés remot a dispositius per xarxa (com Telnet), però fa servir tècniques de xifratge en les comunicacions de manera que les dades, quan estan en trànsit d'un dispositiu i l'altre, per la xarxa, no són llegibles per tercers.

> De manera general, és millor fer servir SSH en lloc de Telnet quan estigui disponible per a més seguretat.

1.4.3 Connexió per port auxiliar

Es pot fer una connexió remota al dispositiu per mitjà d'una connexió telefònica mitjançant un mòdem connectat al port auxiliar del dispositiu. A diferència de la connexió per mitjà de Telnet i SSH, aquesta forma de connexió no requereix que estigui activada cap connexió de xarxa del dispositiu per funcionar.

També es pot fer servir el port aux de manera local en lloc del port de consola, amb una connexió directa amb l'ordinador (que executi un programa d'emulació de terminal). Per exemple, si tenim problemes amb el port de consola, o si no coneixem alguns dels paràmetres del port de consola, podem fer servir aquesta connexió.

1.5 Treball amb el Cisco IOS

Una vegada heu accedit al sistema operatiu hi podeu treballar. El que veureu serà un pantalla semblant a la que es veu a continuació, amb el sistema esperant l'entrada d'ordres.

```
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE
    (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Cisco WS-C2950T-24 (RC32300) processor (revision C0) with 21039K bytes of
    memory.
Processor board ID FHK0610Z0WC
Running Standard Image
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 0090.210C.4366
Motherboard assembly number: 73-5781-09
Power supply part number: 34-0965-01
Motherboard serial number: FOC061004SZ
Power supply serial number: DAB0609127D
Model revision number: C0
Motherboard revision number: A0
Model number: WS-C2950T-24
System serial number: FHK0610Z0WC

Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE
    (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!
```

En la secció "Annexos" del web teniu un manual d'ús del simulador de xarxes Packet Tracer. Aquest simulador és el que heu d'utilitzar per fer les activitats proposades.

El sistema Cisco IOS està dissenyat com un sistema operatiu que té diferents modes de treball, des de cada mode es pot accedir a certes opcions i funcions del sistema operatiu.

Els diferents modes del IOS són:

- mode usuari
- mode d'execució privilegiat
- mode de configuració global
- altres modes de configuració específics (configuració d'interfícies, etc.)

1.5.1 Mode usuari

El mode d'usuari és el primer al qual s'accedeix quan s'entra en la CLI del dispositiu Cisco. Aquest mode permet executar una sèrie limitada d'ordres bàsiques. La majoria d'aquestes ordres serveixen per visualitzar configuracions o estats del dispositiu, però no per modificar-les. No es permet canviar la configuració del dispositiu des del mode d'usuari.

prompt

Es diu *prompt* el caràcter o sèrie de caràcters que es mostren en una línia d'ordres per indicar que està a l'espera d'ordres.

Per defecte no cal cap contrasenya per accedir al dispositiu en mode usuari, encara que es pot configurar. Per saber que estem treballant en mode usuari, la CLI ens mostra el **prompt** amb el símbol >, per exemple:

```
Switch>
```

1.5.2 Mode d'execució privilegiat

El mode d'execució privilegiat permet la configuració i administració del dispositiu. Per entrar en el mode privilegiat s'ha de fer servir l'ordre **enable**. Per saber que estem treballant en mode d'execució privilegiat, la CLI ens mostra el prompt amb el símbol #, per exemple:

```
Switch#
```

Per sortir del mode privilegiat i tornar al mode d'execució d'usuari es fa servir l'ordre ***disable***. Podeu veure aquí el procés d'entrada i sortida del mode d'execució privilegiat des del mode d'execució d'usuari.

```
Switch>enable
Switch#exit


Switch con0 is now available

Press RETURN to get started.



Switch>
```

Es pot configurar una contrasenya per accedir al mode d'execució privilegiat. Per entrar en la resta de modes d'execució, s'ha de fer des del mode d'execució privilegiat.

1.5.3 Mode de configuració global

Des del mode de configuració global es pot accedir a les opcions de l'IOS per configurar gran part del commutador. I també es pot accedir a altres modes de configuració com, per exemple, el mode de configuració d'interfície.

En aquesta secció de codi es pot veure com s'accedeix al mode de configuració global des del mode d'usuari i com se'n surt.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
```

1.5.4 Mode de configuració d'interfície

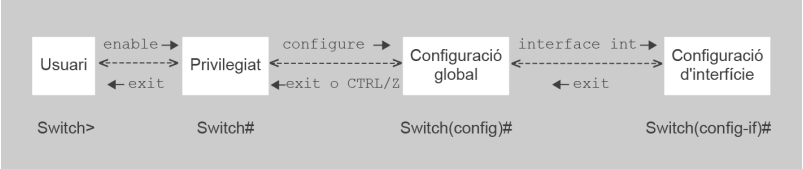
A banda del mode de configuració global, hi ha altres modes de configuració per configurar seccions concretes del commutador. El mode de configuració d'interfície és un d'aquests modes. Aquest mode permet configurar totes les característiques i opcions de cadascuna de les interfícies (ports) del commutador. S'accedeix al mode de configuració d'interfície des del mode de configuració global, especificant quina és la interfície que es vol configurar. Per exemple, per accedir a la configuració del port FastEthernet 0/1:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#
```

Fixeu-vos en tots els exemples com el **prompt** va canviant de manera que ens indica en quin mode de configuració del sistema operatiu ens trobem.

En la figura 1.18 podeu veure un esquema de com es passa entre els diferents modes d'execució del Cisco IOS.

FIGURA 1.18. Modes d'execució IOS



1.6 Ajuda del Cisco IOS

El sistema operatiu del Cisco ofereix una sèrie d'ajudes a l'hora de treballar-hi que faciliten la feina de l'administrador.

En primer lloc, hi ha ajuda contextual depenent de l'estat en què us trobeu. En qualsevol moment del treball podeu inserir el caràcter ?, que us mostrarà les diferents ordres o opcions de l'ordre actual. Aquí en podeu veure un exemple.

```
Switch(config-if)#?
  cdp               Global CDP configuration subcommands
  channel-group     Etherchannel/port bundling configuration
  channel-protocol  Select the channel protocol (LACP, PAgP)
  description       Interface specific description
  duplex            Configure duplex operation.
  exit              Exit from interface configuration mode
  mac-address       Manually set interface MAC address
  mls               mls interface commands
  no                Negate a command or set its defaults
  shutdown          Shutdown the selected interface
  spanning-tree     Spanning Tree Subsystem
  speed             Configure speed operation.
  storm-control     storm configuration
  switchport        Set switching mode characteristics
  tx-ring-limit     Configure PA level transmit ring limit
```

En un moment donat, cridant l'ajuda contextual amb ? us diu les possibles ordres que teniu disponibles. Una vegada comenceu a escriure una ordre, si torneu a introduir ? us dirà les diferents opcions de l'ordre. Per exemple:

```
Switch(config-if)#switchport ?
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  native         Set trunking native characteristics when interface is in
                 trunking mode
  nonegotiate    Device will not engage in negotiation protocol on this
                 interface
  port-security  Security related command
  priority       Set appliance 802.1p priority
  trunk          Set trunking characteristics of the interface
  voice          Voice appliance attributes
Switch(config-if)#switchport
```

També es pot fer servir el signe d'interrogació una vegada heu començat a escriure una ordre; per exemple, si escriviu `c?` us mostrarà les ordres que comencen per la lletra *c*.

```
Switch#c?
clear  clock  configure  connect  copy
Switch#c
```

1.6.1 Accés ràpid i ordres abreviades

Com els sistemes operatius dels ordinadors personals, el Cisco IOS també disposa d'ordres d'accés ràpid a ordres anteriors. A més a més proporciona formes abreviades de les ordres (cosa no disponible en la majoria dels sistemes operatius):

- **Tabulador**. La tecla de tabulació completarà les ordres incompletes. Així si escriviu en el mode d'usuari "ena" i premeu la tecla de tabulació us acabarà d'escriure l'ordre **enable**. Us completarà l'ordre únicament quant hi hagi una única ordre a la qual podeu fer referència. Per exemple, si en lloc de "en", escriviu únicament "e" i premeu el tabulador, veureu que no us completa l'ordre, perquè hi ha dues possibles ordres que comencen per *e* (**enable** i **exit**).

- **Tecles de fletxes de dalt i baix**. En l'IOS es guarda un historial de les últimes ordres introduïdes. Amb les tecles de dalt i baix podeu accedir a les ordres de l'historial.

- **Control + C**. Permet interrompre l'entrada d'una ordre i sortir del mode de configuració.

- **Ordres abreviades**. Les ordres es poden abreviar en la quantitat mínima de caràcters que les identifiquen en una selecció única. Per exemple, des del mode d'execució privilegiat hi ha l'ordre **configure terminal**. Introduint únicament "conf t" s'executarà la mateixa ordre, ja que no hi ha cap ordre que comenci per *conf* excepte **configure** i no hi ha cap opció de **configure**

que comenci per la lletra *t* excepte **terminal**. L'ordre **con t** no funcionaria, ja que sí que existeixen dues ordres que comencen per *con* (**configure** i **connect**).

1.6.2 Verificació de la sintaxi

En cas d'introduir una ordre de manera incorrecta (o amb una opció incorrecta), l'IOS mostrarà un comentari que descriu l'errada. Per exemple:

```
Switch(config-if)#switchport mode access ip
                                         ^
% Invalid input detected at '^' marker.
```

Hi ha tres tipus diferents de missatges d'error:

- **Ambiguous command**: ordre ambigua, quan amb els caràcters que hem introduït d'una ordre no es pot saber sense ambigüitat a quina correspon.
- **Incorrect command**: ordre incorrecta, quan l'ordre introduïda no correspon a cap ordre de l'IOS.
- **Incomplete comand**: ordre incompleta, quan no heu especificat totes les opcions necessàries per a l'ordre.

1.7 Configuració del commutador

El commutador té diferents opcions de configuració i administració. Per obtenir totes les opcions possibles heu de treballar des dels diferents modes d'execució del commutador, és a dir:

- **Mode d'usuari**: per veure l'estat del commutador.
- **Mode d'execució privilegiat**: per configurar i administrar el commutador.
- **Mode de configuració global**: per configurar i administrar altres opcions del commutador.
- **Mode de configuració d'interfície**: per configurar els ports del commutador.

1.7.1 Mostrar l'estat del commutador

Des del mode d'execució d'usuari podeu veure l'estat actual del commutador. L'ordre per veure l'estat del commutador és **show**, i les diferents opcions que té

les podeu trobar en l'ajuda contextual de l'IOS introduint el caràcter **?** després de l'ordre **show**:

```
Switch>show ?
  arp                Arp table
  cdp                CDP information
  clock              Display the system clock
  dtp                DTP information
  etherchannel       EtherChannel information
  flash:             display information about flash: file system
  history            Display the session command history
  interfaces         Interface status and configuration
  ip                 IP information
  mac-address-table  MAC forwarding table
  mls                Show MultiLayer Switching information
  privilege          Show current privilege level
  sessions           Information about Telnet connections
  tcp                Status of TCP connections
  terminal           Display terminal configuration parameters
  users              Display information about terminal lines
  version            System hardware and software status
  vlan               VTP VLAN status
  vtp                VTP information
```

ARP

El protocol ARP (de l'anglès ***address resolution protocol***, protocol de resolució d'adreces) és un protocol que permet obtenir l'adreça MAC d'un *host* a partir de la seva adreça IP.

Aquesta és l'explicació de les ordres més importants:

- **arp**: mostra la taula ARP.
- **clock**: mostra el rellotge del sistema.
- **flash**: mostra el contingut de la memòria flaix.
- **history**: mostra l'historial d'ordres del sistema.
- **interfaces**: mostra l'estat i la configuració de les interfícies. El resultat serà semblant al que es veu en la porció de codi següent.

```
Switch>show interfaces
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0010.115d.ab01 (bia 0010.115d.ab01)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
```

L'ordre ens mostra molta informació de la interfície, entre d'altres:

- si la interfície està activa o no
- l'adreça MAC de la interfície
- l'amplada de banda
- les estadístiques d'ús de la interfície
- si la interfície està configurada com a *full-duplex* o *half-duplex*.

Es pot comprovar la configuració i l'estat d'una interfície en concret afegint el nom de la interfície com a paràmetre opcional. Per exemple, per veure l'estat de la interfície FastEthernet 0/1:

```
Switch> show interface FastEthernet 0/1
```

- **ip interface**: es pot veure la configuració IP i l'estat de les interfícies.
- **version**: dóna informació sobre el maquinari del commutador i la versió del sistema operatiu.
- **vlan**: mostra la configuració de les xarxes locals virtuals (*virtual LAN*).
- **mac-address-table**: mostra la taula d'adreces MAC del commutador. Per exemple:

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2f98.0b6a    DYNAMIC     Fa0/1
   1    012a.eff7.ac5d    STATIC      Fa0/2
Switch>
```

Tenim quatre columnes en la taula MAC:

- **Vlan**: vlan a què pertany el port.
- **Mac address**: adreça MAC del *host*.
- **Type**: pot tenir dos valors,
  - **Dynamic.** Aquesta és una adreça MAC que el commutador ha après analitzant les adreces MAC d'origen de les trames.
  - **Static.** És una adreça MAC que ha introduït manualment l'administrador amb l'ordre **mac-address-table static** del mode de configuració global.
- **Ports**: port del commutador al qual està associada aquesta MAC.

1.7.2 Ordres del mode d'execució privilegiat

Des del mode d'execució privilegiat podeu accedir a les ordres següents:

- **configure terminal**. Entra en el mode de configuració global.
- **copy origen destinació**. Serveix per copiar un fitxer en un altre. Si mireu les opcions de l'ordre amb el caràcter ?:
  - **flash**. Per copiar a/des la memòria flaix
  - **ftp**. Per copiar al/del servei d'FTP del sistema
  - **running-config**. Per copiar al/del fitxer de configuració en execució
  - **startup-config**. Per copiar al/del fitxer de configuració d'arrencada
  - **tftp**. Per copiar al/del servei de trivial FTP del sistema

Un exemple d'ordre seria:

```
copy running-config startup-config
```

Per copiar la configuració en execució al fitxer de configuració d'arrencada.

Si voleu podeu tenir diferents fitxers de configuració emmagatzemats en el sistema, només els heu de copiar amb diferents noms en la memòria flaix. Podeu veure un exemple de com es fa en la porció de codi següent:

```
Switch#copy running-config flash:
Destination filename [running-config]? conf-commutador_central-sense_vlan.dat
Building configuration...
[OK]
Switch#
```

- **delete flash**. Serveix per esborrar un fitxer de la memòria. Us demanarà el nom del fitxer a esborrar i la confirmació que el voleu esborrar.
- **dir**. Mostra una llista dels fitxers en el sistema de fitxers que es troba en la memòria flaix. Per exemple:

```
Switch#dir
Directory of flash:/

    1  -rw-     3058048          <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
    2  -rw-        1178          <no date>  conf-commutador_central-sense_vlan.
        dat

64016384 bytes total (60957158 bytes free)
Switch#
```

- **disable**. Permet sortir al mode d'execució d'usuari.
- **exit**. Surt de la CLI.

- **reload**. Reinicia el commutador. Es torna a arrencar el commutador, es carrega de nou el Cisco IOS i es torna a aplicar el fitxer de configuració *startup-config*.
- **show**. Permet veure l'estat i la configuració del commutador. En aquest cas, com que estem en el mode d'execució privilegiat podem visualitzar més coses que des del mode d'execució d'usuari.
  - **access-lists**. Mostra les llistes de control d'accés del commutador.
  - **arp**. Mostra la taula ARP del commutador.
  - **mac-address-table**. Mostra informació sobre el contingut de la taula d'adreces MAC del commutador.
  - **port-security**. Mostra informació sobre la seguretat dels ports del commutador.
  - **running-config**. Mostra el contingut del fitxer de configuració en execució del commutador (el fitxer *running-config*). Aquest és un exemple de fitxer de configuració:

```
commutador_central#show running-config
Building configuration...

Current configuration : 1273 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname commutador_central
!
enable secret 5 $1$mERr$/Q/mbs3O9oHsKR7rNG4e81
enable password contrasenya1234
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 duplex full
 speed 100
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
 duplex half
 speed 100
!
interface FastEthernet0/3
 switchport mode trunk
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
```

```
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

- **spanning-tree**. Mostra informació sobre el protocol STP (*spanning tree protocol*).
- **startup-config**. Mostra el contingut del fitxer de configuració d'arrencada del commutador (el fitxer *startup-config*). L'estructura del fitxer de configuració d'arrencada és semblant a la del fitxer de configuració en execució.
- **vlan**. Mostra informació sobre les VLAN (*virtual local area network,* o xarxa d'àrea local virtual) configurades en el commutador.
- **vtp**. Mostra la informació sobre el protocol VTP (*VLAN trunking protocol*, o protocol d'enllaços troncals VLAN).
- **vlan**. Serveix per configurar les xarxes d'àrea local virtuals en el commutador.

1.7.3 Ordres del mode de configuració global

Per entrar en el mode de configuració global heu d'introduir l'ordre:

```
Switch#configure terminal
```

des del mode d'execució privilegiat. Fixeu-vos que el **prompt** del CLI canvia a:

```
Switch(config)#
```

Des del mode de configuració global es poden fer canvis sobre el funcionament del commutador. Des del mode de configuració global es pot entrar en altres modes de configuració específics (mode de configuració d'interfície, de línia, etc.).

Aquestes són algunes de les ordres més importants del mode de configuració global:

- **access-list**. Gestiona les llistes de control d'accés del commutador.
- **banner motd** ***caràcter_sortida***. Defineix un missatge *motd* (*message of the day*, missatge del dia) de benvinguda del commutador. Aquest missatge es mostra quan entrem per primera vegada en el commutador. Per exemple, en la porció de codi següent podeu veure com es defineix un missatge estàndard d'entrada al dispositiu. Juntament amb l'ordre especifiquem quin caràcter farem servir per indicar que s'acaba el missatge del dia, en aquest cas es fa servir el caràcter $.

```
commutador_central(config)#banner motd ?
  LINE  c banner-text c, where 'c' is a delimiting character
commutador_central(config)#banner motd $
Enter TEXT message.  End with the character '$'.
Commutador central. No feu modificacions si no esteu autoritzats.
Demaneu la contrassenya al vostre administrador.
$

commutador_central(config)#
```

- **hostname** ***nom_dispositiu***. Aquesta ordre serveix per canviar el nom del dispositiu. Aquest és el nom que es mostra en el prompt del CLI. Canviar el nom als dispositius és important, ja que penseu que els dispositius es poden configurar de manera remota amb sessions de Telnet. Un administrador podria ser en un ordinador amb sessions obertes amb diferents commutadors i encaminadors, els quals (si no se'n canvien els noms) tindran tots prompts idèntics. Aquí podeu veure un exemple de canvi de nom i com es modifica la línia del prompt.

```
commutador_central(config)#hostname Switch
Switch(config)#hostname commutador_aula
commutador_aula(config)#
```

Escolliu els noms dels dispositius de xarxa adequadament de manera que siguin prou descriptius de la seva funció o localització. Noms com *commutador1*, *commutador2*, etc. no donen cap pista de quin dispositiu és. En canvi, noms com *commutador_aules* o *encaminador_adsl* poden indicar a l'administrador de quin dispositiu es tracta. Hi ha certes regles que s'han de complir quan escollim un nom per a un dispositiu:

- Ha de començar amb una lletra.
- En el nom únicament es poden fer servir lletres, dígits i guions.
- Ha d'acabar amb una lletra o un dígit.
- No pot tenir espais en blanc.
- La longitud màxima del nom és de seixanta-tres caràcters.
- Cal respectar l'ús de majúscules i minúscules.

Per anular els efectes de l'ordre **hostname**, es pot escriure l'ordre:

```
commutador_central(config)#no hostname
Switch(config)#
```

per tornar al nom per defecte.

> En la CLI hi ha moltes ordres que es poden desfer negant-les amb **no** ***ordre***.

- **interface** ***nom_interficie***. Serveix per entrar en el mode de configuració de la interfície. Per exemple, per configurar el primer port FastEthernet del commutador escriuríem en la CLI:

```
Switch(config)#interface FastEthernet 0/1
```

Podeu consultar el nom de les diferent interfícies del dispositiu amb:

```
Switch(config)#show interfaces
```

1.7.4 Configuració de contrasenyes

La configuració de contrasenyes és la millor manera d'evitar accessos no desitjats als dispositius de la xarxa. Els dispositius han de tenir configurades contrasenyes a nivell local per evitar l'accés no autoritzat. També és important mantenir una bona política de seguretat i limitació física en l'accés als dispositius de xarxa, col·locant-los en sales o armaris tancats amb clau.

L'IOS permet tenir diferents contrasenyes per a diferents nivells jeràrquics de seguretat al dispositiu. Les contrasenyes més importants són:

- **Contrasenya de consola**. Limita l'accés al dispositiu des de la connexió de consola.
- ***Enable password***. Limita l'accés al mode d'execució privilegiat.

- **Contrasenya secreta d'*enable***. També limita l'accés al mode d'execució privilegiat, però en aquest cas la contrasenya està encriptada.
- **Contrasenya VTY**. Limita l'accés mitjançant connexions Telnet.

És important escollir correctament les contrasenyes que es posaran en els dispositius de xarxa. No s'han d'escollir contrasenyes massa senzilles o fàcils d'esbrinar. També és un bon costum tenir claus d'autenticació diferents per als diferents nivells d'accés dels dispositius.

> Com a norma general una contrasenya hauria de tenir almenys vuit caràcters i contenir caràcters en majúscula, minúscula i caràcters numèrics.

Contrasenya de consola

Per canviar la contrasenya de consola s'han d'introduir les ordres següents des del mode de configuració global:

```
1 Switch(config)#line console 0
2 Switch(config–line)#password Contrasenya
3 Switch(config–line)# login
```

La primera ordre s'utilitza per començar la configuració de la primera línia de consola (en molts casos aquesta és l'única línia de consola del dispositiu). La segona ordre permet posar una contrasenya en la línia de consola. I la tercera ordre serveix per configurar el dispositiu perquè demani l'autenticació quan inicia la sessió.

Si sortiu de la CLI amb l'ordre **exit** (potser l'heu d'introduir més d'una vegada) o reinicieu el commutador amb l'ordre **reload**, veureu que us demanarà la contrasenya quan intenteu accedir a la CLI.

Quan escriviu la contrasenya a l'inici de sessió no es mostren els caràcters per seguretat.

Contrasenyes del mode d'execució privilegiat

Aquestes contrasenyes serveixen per limitar l'accés no autoritzat al mode d'execució privilegiat, per això també se les coneix com a *contrasenyes enable* (**enable** és l'ordre que es fa servir per accedir al mode d'execució privilegiat des del mode d'execució d'usuari).

Hi ha dues contrasenyes per restringir l'accés al mode d'execució privilegiat: **enable password** i **enable secret**.

La diferència entre elles és que **enable secret** encripta la contrasenya, mentre que **enable password** no. Per aquest motiu és preferible fer servir **enable password** quan sigui possible (en alguns dispositius antics no està disponible **enable password**).

Les ordres per configurar la contrasenya d'entrada al mode d'execució privilegiat són:

```
Switch(config)#enable password contrasenya
Switch(config)#enable secret contrasenya
```

És interessant veure el contingut de la memòria d'execució (running-config) per adonar-se que una de les contrasenyes és visible, mentre que l'altra està encriptada.

```
Current configuration : 1111 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$mERr$DSTbrxCVds2AqV1lvsySz0
enable password contrasenya
!
[...]
```

Una vegada establerta la contrasenya d'accés al mode d'execució privilegiat, podeu comprovar que us demana la contrasenya després de fer servir l'ordre **enable**.

Perquè la configuració de contrasenyes es mantingui després de reiniciar el dispositiu, s'ha de fer una còpia de la configuració en el fitxer d'arrencada.

Encriptació de contrasenyes

Podem configurar que les contrasenyes estiguin encriptades en els fitxers de configuració, tant si són contrasenyes *secret* com *password*. Per fer-ho hi ha l'ordre **service password-encryption** del mode de configuració global, que dóna un servei d'encriptació de les contrasenyes no encriptades. Una vegada executades, les contrasenyes es mostren encriptades en els fitxers de configuració.

Restablir la contrasenya enable

Què passa si l'administrador no recorda la contrasenya d'entrada al dispositiu? Els commutadors disposen d'un mètode per restablir les contrasenyes. Per fer-lo servir hem de tenir accés físic al commutador (no es pot fer de manera remota).

A continuació veurem el procés de recuperació per a un commutador de la sèrie 2950. S'han de seguir els passos següents:

- Connectar un PC al port de consola del commutador i executar una emulació de terminal (amb hyperterminal o minicom) amb les dades següents:
  - bauds: 9.600
  - bits de dades: 8
  - paritat: cap
  - bits d'aturada: 1
  - control de flux: XON/XOFF
- Desconnectar el commutador del corrent elèctric.

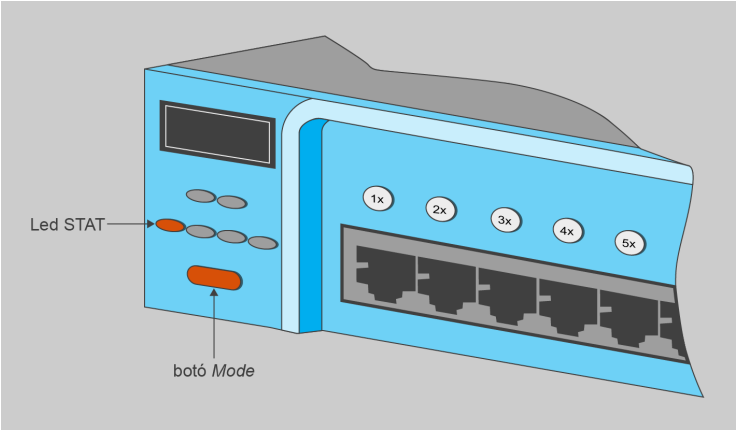
Recuperació de contrasenyes

El procés de restablir contrasenyes no és exactament el mateix per a tots els dispositius. Per veure una descripció dels diferents modes de recuperació de contrasenyes podeu visitar aquesta pàgina web:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

- Connectar el commutador al corrent elèctric de nou. S'ha de prémer el botó ***Mode***, que és en la part esquerra del frontal del commutador (el podeu veure en la figura 1.19), mentre es torna a endollar el commutador al corrent.

FIGURA 1.19. Botó Mode del commutador



- S'ha de deixar anar el botó ***Mode*** cinc segons després que el LED d'estat (STAT) s'apagui. Quan deixem anar el botó ***Mode*** el LED SYST parpelleja en taronja.
- Això mostrarà el prompt

```
switch:
```

- Inicialitzem el sistema d'arxius flaix amb **flash_init**:

```
switch: flash_init
Initializing Flash...
flashfs[0]: 143 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 3612672
flashfs[0]: Bytes used: 2729472
flashfs[0]: Bytes available: 883200
flashfs[0]: flashfs fsck took 86 seconds
....done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
switch:
```

Assegureu-vos que introduïu el caràcter de dos punts (:) després de la paraula *flaix*.

- Carreguem els fitxers d'ajuda amb **load_helper**.
- Mirem el contingut de la flaix amb **dir flash:**.

```
Switch#dir flash:
Directory of flash:/

    1  -rwx     3058048          <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
    2  -rwx         616          <no date>  vlan.dat
    3  -rwx        5825          <no date>  config.text

64016384 bytes total (60956603 bytes free)
```

- Canviem el fitxer de configuració per config.text.old **rename flash:config.text flash:config.text.old**.

- Reiniciem el commutador amb l'ordre **boot**:

```
switch: boot
Loading "flash:c2950-i6q4l2-mz.121-22.EA4.bin
    "...##############################
################################################################################

##################################################################
File "flash:c2950-i6q4l2-mz.121-22.EA4.bin" uncompressed and installed, entry
    po
int: 0x3000
executing...
```

- Ens demanarà si volem fer servir el diàleg de configuració, escollim l'opció No.

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]: n

!--- Type "n" for no.

Press RETURN to get started.

!--- Press Return or Enter.

Switch>
```

- Entrem en el mode d'execució privilegiat i tornem a anomenar el fitxer de configuració amb el seu nom original:

```
Switch>enable
Switch#rename flash:config.text.old flash:config.text
Destination filename [config.text]
```

- Posem el fitxer de configuració com a configuració en execució amb **copy flash:config.text running-config**.

```
Switch#copy flash: running-config
Source filename []? config.text
Destination filename [running-config]?

1117 bytes copied in 0.416 secs (2685 bytes/sec)
Switch#
```

- Ara ja podem restablir les contrasenyes que vulguem i, després, desar la configuració:

```
Switch# configure terminal
Switch(config)#enable secret contrasenya_secret
Switch(config)#enable password contrasenya_password
Switch(config)#line vty 0 4
Switch(config-line)#password contrasenya_vty
Switch(config-line)#login
Switch#copy running-config startup-config
```

- Finalment reiniciem el commutador amb **reload**.

1.7.5 Configuració d'interfícies

Per accedir al mode de configuració d'interfícies s'ha d'introduir des del mode de configuració global l'ordre **interface nom_de_la_interfície**:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#
```

Fixeu-vos com canvia la línia del prompt.

Des del mode de configuració d'interfície podeu executar (entre d'altres) les ordres següents:

- **description o descripció**: serveix per donar un text identificatiu a la interfície. És semblant a l'ordre **hostname**, però en aquest cas el nom l'assignem a un port i no al dispositiu sencer. La descripció de la interfície es pot veure en la que es mostra amb **show interfaces**, per exemple:

```
commutador_aula(config-if)#description Connexio amb encaminador
commutador_aula(config-if)#exit
commutador_aula(config)#exit
commutador_aula#
%SYS-5-CONFIG_I: Configured from console by console

commutador_aula#show interfaces FastEthernet 0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is Lance, address is 0010.115d.ab01 (bia 0010.115d.ab01)
  Description: Connexio amb encaminador
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
```

Fixeu-vos que la descripció de la interfície es troba en la tercera línia que es mostra amb l'ordre **show interfaces**.

- **duplex {*full* | *half* | *auto*}**: permet configurar la interfície perquè funcioni en mode *full-duplex*, *half-duplex* o en mode automàtic.
- **mac-address o adreça MAC**: permet indicar manualment l'adreça MAC de la interfície.
- **shutdown**: deshabilita la interfície. Es pot tornar a habilitar amb **no shutdown**.
- **speed**: permet configurar la velocitat del port. Algunes interfícies poden treballar a diferents velocitats. Per exemple, la majoria de ports FastEthernet permeten treballar tant a 10 Mbps com a 100 Mbps. També teniu l'opció de configurar la interfície per configurar la velocitat de treball de manera automàtica. En aquest cas, el port del commutador i el del dispositiu que hi està connectat escullen la velocitat de funcionament del port mitjançant un procés que es coneix com a **autonegociació**. A continuació podeu veure un exemple de les diferents velocitats que es poden especificar per la interfície Gigabit Ethernet.

```
commutador_aula(config)#interface GigabitEthernet 1/1
commutador_aula(config-if)#speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  1000  Force 1000 Mbps operation
  auto  Enable AUTO speed configuration

commutador_aula(config-if)#speed
```

2. Administració de commutadors

Plug-n-Play

Es diu que un dispositiu és Plug-and-Play quan es pot connectar a un ordinador sense haver de configurar res.

Els commutadors són dispositius que poden funcionar de manera Plug-and-Play, es connecten en una xarxa i comencen a funcionar sense cap tipus de configuració. L'administrador de la xarxa, però, pot fer diverses tasques de configuració i administració per millorar el funcionament del commutador. Administrar les taules MAC, els fitxers de configuració i actualitzar la versió del sistema operatiu són tasques comunes dels administradors.

Actualment, la seguretat a les xarxes també s'ha convertit en un objectiu prioritari. Un administrador ha de configurar els commutadors per intentar protegir-los contra atacs d'usuaris malintencionats.

2.1 Seqüència d'arrencada del commutador

Quan s'engega un commutador el primer que es fa és carregar el programari del carregador d'arrencada. Aquest carregador és un petit programa que es troba emmagatzemat en la ROM del commutador i s'executa quan aquest s'engega.

El carregador d'arrencada fa les funcions següents:

- S'encarrega de la inicialització a baix nivell de la CPU. Inicialitza els registres de la CPU que controlen on està assignada la memòria física, la quantitat de memòria i la seva velocitat.
- Du a terme el procés POST d'autodiagnòstic pel subsistema de la CPU. Fa una comprovació de la memòria de la CPU.
- Inicialitza el sistema d'arxius flaix en la targeta del sistema.
- Carrega una imatge predeterminada del programari del sistema operatiu en la memòria i engega el commutador. En primer lloc, el carregador d'arrencada intentarà trobar la imatge de l'IOS de Cisco en el commutador cercant primer en un directori que té el mateix nom que l'arxiu imatge. Si no l'hi troba, cercarà en cada subdirectori abans de continuar la cerca en el directori original.

A continuació el sistema operatiu s'encarrega d'inicialitzar les interfícies (els ports) consultant els fitxers de configuració del sistema operatiu. Aquest fitxers de configuració es troben en la memòria flaix.

2.1.1 Inicialització d'emergència

El carregador d'arrencada també proporciona un mètode d'arrencada del commutador en cas que el sistema operatiu no es pugui utilitzar. El carregador d'arrencada permet arrencar el dispositiu amb línia d'ordres per poder fer canvis en els fitxers emmagatzemats en la memòria flaix abans de carregar el sistema operatiu. Des d'aquesta línia d'ordres es pot restablir una contrasenya, tornar a instal·lar una imatge del sistema operatiu o formatar el sistema d'arxius flaix.

2.2 Configuració de la interfície d'administració

Tot i que els commutadors són dispositius de xarxa que corresponen a la capa 2 del model OSI (capa d'enllaç), alguns dels commutadors permeten dur a terme una configuració TCP/IP d'aquests. El motiu principal és que configurant el commutador a nivell de xarxa (capa 3 del model OSI) podem fer connexions remotes amb aquest per mitjà de **Telnet** i **SSH**.

Configuració IP?

La configuració de capa 3 del model OSI no sempre és necessària. És imprescindible si voleu configurar el commutador remotament per mitjà d'una connexió Telnet o SSH, o si voleu fer servir un servidor TFTP. En un altre cas, no necessitareu configurar l'adreça IP d'un commutador.

Per configurar el commutador s'ha de proveir de l'adreça IP, la màscara de xarxa i un encaminador per defecte. L'adreça IP s'assigna a una interfície virtual anomenada *LAN virtual* (VLAN). Posteriorment s'assignarà aquesta LAN virtual a un o més ports del commutador.

Per defecte, l'administració del commutador es fa mitjançant la primera LAN virtual (VLAN1), encara que se'n pot fer servir qualsevol altra per configurar-lo.

2.2.1 Configurar la interfície d'administració

Per configurar l'adreça IP i la màscara de xarxa de la LAN virtual heu d'entrar en el mode de configuració d'interfície, en aquest cas de la VLAN que voleu configurar. L'ordre per configurar l'adreça IP i la màscara és **ip address** ***adreça IP màscara de xarxa***.

Una vegada heu configurat l'adreça IP i la màscara, s'ha d'activar la interfície amb l'ordre **no shutdown**.

Aquí teniu un exemple de tots els passos per fer-ho:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.0.155 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

A continuació s'ha d'assignar un port perquè treballi des d'aquesta VLAN. Heu d'entrar al mode de configuració de la interfície que voleu configurar i fer servir l'ordre **switchport** ,que serveix per configurar les característiques de commutació d'un port. Aquestes són les opcions més importants de l'ordre **switchport**:

- **access**: canvia les característiques del mode d'accés de la interfície.
- **mode**: estableix el mode de funcionament troncal de la interfície.

Les diferents opcions del mode troncal són:

- **access**: estableix el mode a accés.
- **trunk**: estableix el mode a troncal.
- **dynamic**: estableix el mode troncal dinàmicament a model troncal o d'accés.
- **native**: estableix les característiques natives quan la interfície treballa en mode troncal.
- **nonegotiate**: serveix per dir que la interfície no farà servir el protocol d'autonegociació del port.
- **port-security**: ordres relatives a la seguretat del port.
- **trunk**: estableix el funcionament troncal del port.

Hem de configurar el port per funcionar amb mode d'accés i donar-hi accés a la LAN virtual que hem configurat. En aquest cas configurarem la interfície FastEthernet 0/20 del commutador:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet 0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

%LINK-5-CHANGED: Interface Vlan10, changed state to up
% Access VLAN does not exist. Creating vlan 10
Switch(config-if)#exit
Switch(config)#
```

Podeu comprovar l'estat de la interfície fent servir l'ordre **show ip interface**, que mostrarà la configuració de les VLAN.

```
Switch#show ip  interface
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled
Vlan10 is up, line protocol is up
  Internet address is 172.17.99.11/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
```

```
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Null turbo vector
  IP multicast fast switching is disabled
```

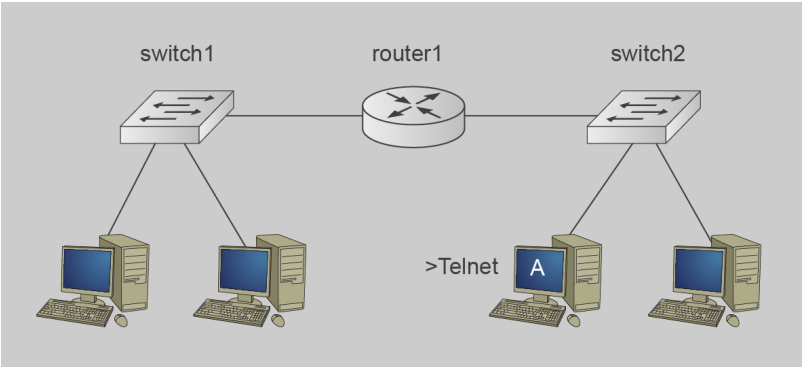
Quan activeu una VLAN manualment, la VLAN per defecte (la 1) es desactiva automàticament. També podeu veure la informació de manera resumida amb l'ordre **show ip interface brief**.

Configuració de l'encaminador per defecte

El pas següent és la configuració del commutador perquè pugui enviar paquets IP a altres xarxes per mitjà d'un encaminador. Per això heu de configurar un encaminador per defecte. De nou, aquesta configuració és innecessària en un commutador que no farà connexions per Telnet o SSH.

Fixeu-vos en la figura 2.1. L'ordinador A fa una connexió Telnet amb el commutador **switch1**. El commutador **switch1** necessita configurar l'adreça de l'encaminador **router1** per poder enviar paquets de tornada a l'ordinador A, ja que aquest es troba en una LAN diferent de la LAN del commutador **switch1**.

FIGURA 2.1. Configuració de l'encaminador per defecte en un commutador



S'ha de configurar un encaminador per defecte per poder-se comunicar amb //hosts// d'altres LAN

Gateway

Gateway és un terme en desús per referir-se als encaminadors. En alguns sistemes i programes s'ha fet la traducció literal 'porta d'enllaç', però també està en desús. En aquests materials farem servir la paraula **encaminador** o la seva versió anglesa *router*.

L'ordre que serveix per configurar l'encaminador per defecte és **ip default-gateway *IP_de_l'encaminador*** des del mode de configuració global. Una vegada heu configurat l'encaminador per defecte podeu fer una prova de connectivitat amb l'ordre **ping *IP_de_l'encaminador***.

Per exemple:

```
Switch(config)#ip default-gateway 192.168.15.1
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#ping 192.168.15.1
```

```
6
7  Type escape sequence to abort.
8  Sending 5, 100-byte ICMP Echos to 192.168.15.1, timeout is 2 seconds:
9  .!!!!
10 Success rate is 80 percent (4/5), round-trip min/avg/max = 19/28/32 ms
```

ping

L'ordre **ping** envia una sèrie de missatges **ICMP echo request** a una destinació determinada. Aquesta destinació tornarà un missatge de res**ICMP echo reply**. Generalment es fa servir per provar la connectivitat de dos *hosts*.

L'ordre **ping** envia cinc missatges **ICMP echo request**, i ens dóna estadístiques dels paquets enviats i rebuts.

2.3 Configuració de Telnet i SSH

Hi ha casos en què la configuració del commutador per mitjà del port de consola no resulta adequada. Per exemple, penseu que treballeu en una empresa gran que té diferents xarxes locals en cada planta d'un edifici. Si voleu canviar la configuració (per exemple, la contrasenya) a tots els commutadors, heu d'anar un a un i fer una connexió física amb un cable al port de consola per poder-los configurar. Seria més ràpid si l'administrador de la xarxa pogués configurar tots els commutadors des d'un ordinador connectat a la xarxa.

Telnet i SSH ens permeten fer una connexió remota del commutador per poder-lo configurar.

2.3.1 Configuració de Telnet

Els primers models de commutadors únicament feien servir aquest mètode per connectar remotament, per això encara està molt estès.

Amb Telnet es pot entrar en una VTY (terminal virtual) del commutador. En principi les línies VTY són insegures, ja que admeten l'accés de qualsevol usuari que comenci sessió amb aquestes. Per aquest motiu s'han de configurar contrasenyes per restringir l'accés per Telnet.

Vegem a continuació la seqüència d'ordres per establir la contrasenya:

```
1 Switch(config)#line vty 0 4
2 Switch(config-line)#password clau12345
3 Switch(config-line)#login
```

Per configurar la contrasenya del commutador heu d'entrar en el mode de configuració de VTY des del mode de configuració global. Molts dispositius de xarxa Cisco tenen cinc línies VTY i s'ha de configurar la contrasenya d'entrada per a totes. L'ordre **line VTY 0 4** estableix que s'estan configurant totes les línies de VTY (de la 0 a la 4).

L'ordre per establir la contrasenya és **password *contrasenya***. L'ordre **login** serveix per habilitar la petició de la contrasenya quan l'usuari inicia sessió. Per admetre

connexions sense autenticació de contrasenya s'ha de fer servir l'ordre **no login**, però això és un mètode de configuració insegur, ja que qualsevol usuari pot entrar i configurar el commutador.

Una vegada establerta la contrasenya es pot fer una connexió per Telnet al commutador. Es demanarà la contrasenya en fer **login**. Per exemple això és el que veuríem des del *host* on fem la connexió:

```
$>telnet 192.168.0.1
Trying 192.168.0.1 ...Open


User Access Verification

Password:

Switch>
```

Telnet és el mètode per defecte de connexió a VTY, per això no cal configurar-lo per fer-lo servir. Però si hem configurat l'accés per VTY amb SSH i volem tornar a fer servir Telnet, l'haurem de configurar manualment.

2.3.2 Configuració d'SSH

La funció de configuració d'SSH no està implantada al simulador Packet Tracer i, per tant, no es pot provar.

El problema principal de Telnet, és que envia totes les comunicacions de manera oberta per la xarxa sense encriptar. Qualsevol usuari que faci servir un programa de rastreig pot analitzar aquestes trames i veure'n el contingut. Per aquest motiu és millor fer servir **ssh**, ja que encripta les dades abans d'enviar-les a la xarxa.

Per fer funcionar **ssh** s'han de generar claus RSA (pel nom dels seus tres autors: Rivest, Shamir i Adleman). Per generar les claus RSA encriptades es fa servir l'ordre **crypto key generate rsa**.

Aquests són els passos a seguir per configurar el commutador com a servidor SSH:

1. Entrar en el mode de configuració global amb **configure terminal**.
2. Configurar un nom de *host* per al commutador amb **hostname *nom_commutador***.
3. Configurar el domini del commutador amb **ip domain-name *nom_commutador***.
4. Habilitar el servidor SSH i generar les claus RSA amb **crypto key generate rsa**.
5. Escollir quina versió d'SSH volem que executi el commutador amb **ip ssh version 2**. Si és possible, es recomana fer servir la versió 2 d'SSH, ja que utilitza uns algorismes d'encriptació de seguretat millors que els de la versió 1.

6. Escollir el temps d'espera en segons amb l'ordre **ip ssh time-out** ***temps_en_segons***. L'opció per defecte és cent vint segons, però es pot modificar. Aquest és el temps que permet el commutador perquè es facin totes les fases de connexió als clients.

7. Especificar la quantitat de vegades que un client es pot autenticar en el servidor amb l'ordre **ip ssh authentication-retries** ***número_de_intents***. Es pot escollir qualsevol valor entre 0 i 5 (3 és el valor per defecte).

8. Configurar les línies TTY per limitar-ne l'accés únicament a SSH amb **transport input ssh** en la configuració de les línies VTY. Així s'eviten connexions al commutador que no siguin SSH.

Aquest seria el procés sencer per la configuració:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname miswitch
miswitch(config)#
miswitch(config)#ip domain-name rtp.cisco.com

miswitch(config)#crypto key generate rsa

miswitch(config)#ip ssh version 2
miswitch(config)#ip ssh time-out 60
miswitch(config)#ip ssh authentication-retries 2


miswitch(config)#line vty 0 4
miswitch(config-line)#transport input SSH
```

2.4 Administració de les taules MAC

Els commutadors determinen si han d'enviar les trames per altres ports analitzant l'adreça de destinació de la trama. Aquesta adreça la cerquen en una taula interna anomenada *taula d'adreces MAC*, que conté les adreces MAC que es poden trobar per cada port.

Per visualitzar el contingut de la taula MAC del commutador feu servir l'ordre **show mac-address-table**, des del mode d'usuari o el mode d'execució privilegiat.

Per exemple, aquesta seria una taula MAC d'un commutador:

```
Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0060.2f98.0b6a    DYNAMIC     Fa0/1
   1    012a.eff7.ac5d    STATIC      Fa0/2
   1    0345.ae23.fe4a    DYNAMIC     Fa0/5
   1    0056.735e.67a2    DYNAMIC     Fa0/8
   1    12ea.35a7.003e    DYNAMIC     Fa0/9
   1    ff45.0020.24a3    DYNAMIC     Fa0/11
```

```
13    1    0060.42a2.7352    DYNAMIC     Fa0/14
14    1    1003.24a5.ee0f    DYNAMIC     Fa0/16
```

Aquestes adreces poden ser:

- **Dinàmiques**. Apreses automàticament pel commutador analitzant les adreces dins de les trames. Aquestes adreces expiren passat un temps si no es fan servir. El temps d'expiració per defecte és de tres cents segons. Si el temps d'expiració és molt curt, les adreces es podrien esborrar de la taula de manera prematura, la qual cosa produiria una propagació del trànsit per inundació innecessàriament. Si el temps d'expiració és molt llarg la taula es podria omplir d'adreces innecessàries que no es fan servir.
- **Estàtiques**. Configurades manualment per l'administrador de la xarxa. Aquestes adreces no expiren mai i el commutador sempre sap a quina interfície ha d'enviar les trames dirigides a aquesta adreça.

L'ordre per assignar una adreça MAC a la taula d'adreces MAC de manera estàtica és la següent:

mac-address-table static ***adreça MAC*** **vlan** ***{1-4096, ALL}*** **interface** ***id_de_la_interfície***

Per exemple, des del mode de configuració global:

```
1 Switch(config)mac-address-table static 0060.a014.e06e vlan 1 interface
      FastEthernet 0/3
```

Fixeu-vos que aquesta adreça, en la taula d'adreces MAC que us mostra l'ordre **show**, està marcada com a estàtica.

Per esborrar una adreça MAC estàtica de la taula d'adreces MAC del commutador heu d'escriure la mateixa ordre precedida de **no**. Per exemple, per esborrar l'adreça MAC que hem afegit amb l'ordre anterior, hauríeu de executar:

```
1 Switch(config)no mac-address-table static 0060.a014.e06e vlan 1 interface
      FastEthernet 0/3
```

2.4.1 Administració dels fitxers de configuració

Els dispositius (tant els commutadors com els encaminadors) de xarxa Cisco tenen diferents tipus de memòries:

- **Memòria RAM** (*random access memory*, memòria d'accés aleatori). És la memòria sobre la qual treballa el dispositiu. Aquesta memòria és volàtil, per tant, quan s'apaga el dispositiu tot el seu contingut s'esborra.

- **Memòria NVRAM** (*non volatile RAM*, RAM no volàtil). És una memòria no volàtil, per tant, manté el contingut encara que s'apagui el dispositiu. En aquesta memòria es troben els fitxers de configuració del dispositiu.
- **Memòria flaix**. És una memòria no volàtil. Serveix com a memòria secundària per emmagatzemar altres fitxers com, per exemple, altres versions del sistema operatiu del dispositiu.

Els dispositius de xarxa necessiten dos tipus de fitxers per funcionar: el sistema operatiu i la configuració. El sistema operatiu serveix per fer funcionar el maquinari del dispositiu. Els fitxers de configuració serveixen per personalitzar i configurar les diferents opcions del dispositiu.

Hi ha dos fitxers de configuració en els dispositius Cisco:

- ***running-config*** (fitxer de configuració en execució). Aquest fitxer conté la configuració actual amb la qual s'està executant el sistema. Qualsevol canvi que es faci sobre la configuració del sistema per mitjà d'ordres de l'IOS es farà sobre aquest fitxer. El fitxer de configuració en execució es troba situat sobre la memòria RAM; per tant, quan s'apaga el dispositiu s'esborra.
- ***startup-config*** (fitxer de configuració d'arrencada). Aquest fitxer conté la configuració inicial del dispositiu. Situat en la memòria NVRAM, és un fitxer persistent, es manté el contingut quan es reinicia el dispositiu.

Podeu veure el contingut d'aquests fitxers amb l'ordre **show**. Per exemple, per veure el contingut del fitxer en execució podeu escriure:

```
Switch#show running-config
```

El resultat per a un commutador:

```
Building configuration...

Current configuration : 1149 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname commutador_aula
!
enable secret 5 $1$mERr$5jbOD5lHVUWxAAsNOD6eO/
enable password clau1234
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 duplex full
 speed 100
!
interface FastEthernet0/2
 switchport access vlan 3
 tx-ring-limit 100
!
```

```
interface FastEthernet0/3
!
interface FastEthernet0/4

[...]

!
interface FastEthernet0/24
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

Les línies que comencen pel caràcter **!** es tracten com a comentaris. No s'ha de tenir en compte el contingut sencer d'una línia que comenci amb el caràcter **!**.

En les diferents parts del fitxer es pot veure l'espai per a les diferents configuracions del commutador. Fixeu-vos en la diferència de com estan emmagatzemades les contrasenyes *password* i *secret*; únicament *secret* està encriptada. Per aquest motiu es recomana fer servir *secret* sempre que estigui disponible.

En el procés d'arrencada del dispositiu es fa una còpia del fitxer de configuració d'arrencada (*startup-config*) des de l'NVRAM sobre el fitxer d'execució (*running-config*) en la RAM. És a dir, la configuració d'arrencada es converteix en la configuració d'execució.

Tots els canvis fets en la configuració del dispositiu únicament modificaran la configuració en execució. Si es vol que aquesta configuració sigui permanent, el que s'ha de fer és copiar el fitxer de configuració en execució sobre el fitxer de configuració d'arrencada,des del mode d'execució privilegiat, amb l'ordre:

```
Switch#copy running_config startup_config
```

És important estar segur que la configuració actual del dispositiu és correcta, ja que copiant-la al fitxer de configuració d'arrencada l'estem fent permanent (serà la configuració que es farà servir la propera vegada que s'arranqui el dispositiu). Si heu comés un error en la configuració del fitxer, el commutador tindrà una configuració incorrecta la propera vegada que arranqui.

En qualsevol moment es pot fer l'acció contrària. Imagineu, per exemple, que heu comés un error en fer els canvis en la configuració del dispositiu. Aquests canvis, en realitat, únicament han modificat el fitxer *running-config*. Podríeu esmenar l'error tornant a configurar el dispositiu o, més fàcil, copiar la configuració d'arrencada en el fitxer d'execució des del mode d'execució privilegiat amb:

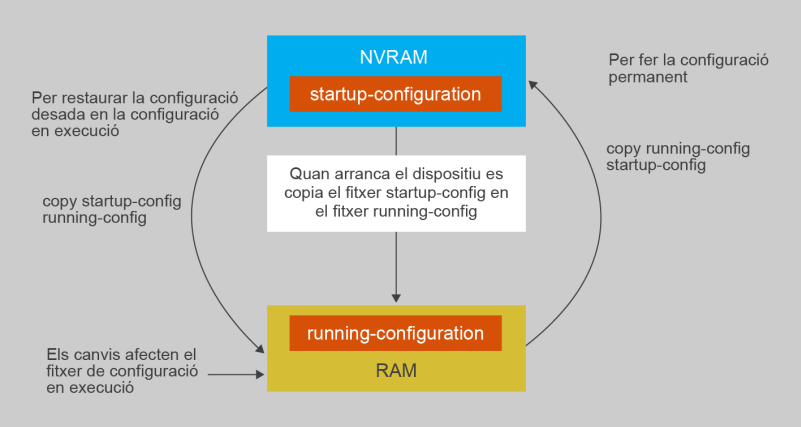
```
Switch#copy startup_config running_config
```

Però aquesta ordre no sobreescriu completament la configuració en execució, sinó que únicament afegeix les ordres existents de la configuració d'arrencada a la configuració en execució. Per això, en alguns casos els resultats poden no ser els esperats.

Per assegurar-se que la configuració de l'execució és la que volem després d'haver copiat un fitxer de configuració en la configuració d'arrencada, el més adequat és reiniciar el commutador. Per a això feu servir l'ordre **reload** des del mode d'execució privilegiat.

En la figura 2.2 podeu veure un resum del funcionament dels fitxers de configuració i els diferents tipus de memòria.

FIGURA 2.2. Memòria i fitxers



Desar diferents fitxers de configuració en disc

En alguns casos a l'administrador li pot interessar desar en memòria diferents configuracions del commutador en memòria no volàtil. Per exemple, es podria desar una configuració del commutador que faci servir VLAN amb enllaços troncals i una altra que no les faci servir.

En aquests casos la millor solució és desar els fitxers de configuració en la memòria flaix. Es pot fer la còpia en la memòria flaix indistintament des del fitxer *running-config* (fitxer de configuració en execució) o des de l'*startup-config* (fitxer de configuració d'arrencada).

L'ordre que heu de fer servir és **copy startup-config flash**. Us demanarà el nom del fitxer que es desarà en la memòria flaix:

```
Switch#copy startup-config flash:
Destination filename [startup-config]? configuracio_vlan.bak

921 bytes copied in 0.416 secs (2213 bytes/sec)
Switch#
```

Recordeu que quan modifiqueu el fitxer de configuració *startup-config*, perquè faci efecte, heu de **reiniciar** el commutador.

Per restaurar la configuració desada en flaix en alguns dels fitxers d'execució del commutador heu de fer servir l'ordre contrària. De nou us demanarà pel nom del fitxer que es troba en la flaix:

```
Switch#copy flash: startup-config
Source filename []? configuracio_vlan.bak
Destination filename [startup-config]?
[OK]

921 bytes copied in 0.416 secs (2213 bytes/sec)
Switch#
```

Esborrar fitxers de configuració

L'administrador té l'opció d'esborrar els fitxers de configuració del commutador. D'aquesta manera s'assegura que el commutador es configurarà la propera vegada que s'engegui.

Per esborrar el contingut de la configuració d'arrencada es pot fer servir l'ordre següent des del mode d'execució privilegiat **erase startup-config**.

Per esborrar un fitxer de configuració emmagatzemat en la memòria flaix feu servir **delete flash:**. Us demanarà el nom del fitxer a esborrar, per exemple:

```
Switch#delete flash:
Delete filename []?configuracio_vlan.bak
Delete flash:/configuracio_vlan.bak? [confirm]y
Switch#
```

Gestió dels fitxers de configuració per TFTP

Una manera ràpida, flexible i segura d'administrar els fitxers de configuració dels commutadors és mitjançant el TFTP (*trivial file transfer protocol*, protocol de transferència de fitxers trivial). Amb el TFTP podem fer còpies de seguretat dels fitxers de configuració del commutador de manera remota i tenir-los disponibles des d'un altre ordinador.

Per poder fer servir el client de TFTP del commutador heu d'haver configurat una adreça IP per a una interfície del commutador.

El sistema Cisco IOS té incorporat un client FTP que permet fer connexions a un servidor que es trobi en la seva xarxa.

Fer una còpia de seguretat amb el TFTP

Fem servir l'ordre **copy** per fer una còpia d'un fitxer del commutador al servidor del TFTP, però en aquest cas especifiquem que la destinació no és un fitxer intern a la memòria flaix del commutador, sinó l'adreça del servidor TFTP. La sintaxi de l'ordre és **copy *fitxer_origen* tftp:**. El fitxer d'origen pot ser un dels fitxers de configuració del commutador (*startup-config* o *running-config*) o un fitxer de la memòria flaix. En aquest exemple, comprovem que la connectivitat amb el servidor és correcta i després copiem un fitxer de la memòria flaix al servidor TFTP:

```
Switch#ping 192.168.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.10, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 15/27/32 ms

Switch#show flash:
Directory of flash:/

    1  -rw-     3057198          <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
    3  -rw-         856          <no date>  no_vlan
    2  -rw-         616          <no date>  vlan.dat

64016384 bytes total (60957720 bytes free)
Switch#copy flash: tftp:
Source filename []? no_vlan
Address or name of remote host []? 192.168.0.10
Destination filename [conf_commutador]? commutador_central_no_vlan

Writing conf_commutador...!!
[OK - 856 bytes]

856 bytes copied in 0.416 secs (2723 bytes/sec)
Switch#
```

Restaurar una còpia de seguretat amb el TFTP

Per restaurar una còpia de seguretat d'un fitxer amb el TFTP el procés és similar. S'ha d'establir comunicació amb el servidor TFTP per copiar un fitxer del servidor TFTP al commutador (a la memòria flaix o a qualsevol dels fitxers de configuració). Per exemple:

```
Switch#copy tftp: flash:
Address or name of remote host []? 192.168.0.10
Source filename []? commutador_central_no_vlan
Destination filename [fitxer]? no_vlan

Accessing tftp://192.168.0.10/fitxer...
Loading fitxer from 192.168.0.10: !
[OK - 1117 bytes]

1117 bytes copied in 0.032 secs (34906 bytes/sec)
```

2.5 Actualitzar el sistema operatiu del commutador

Una tasca habitual de l'administrador de la xarxa és canviar o actualitzar el sistema operatiu dels dispositius de la xarxa. Potser el fitxer que conté el sistema operatiu s'ha fet malbé en la memòria i s'ha de tornar a carregar. També és possible que hagi sortit una altra versió del sistema operatiu i l'administrador de la xarxa la vulgui provar en els seus dispositius.

Per comprovar quina és la versió del sistema operatiu que executeu podeu fer servir l'ordre **show version**:

```
host#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE
    (fc1)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba
Image text-base: 0x80010000, data-base: 0x80562000

[...]
```

En aquest cas, la versió **12.1(22)EA4**.

El procés d'actualització del sistema operatiu del commutador consta de tres passos:

1. Carregar la nova imatge del sistema operatiu a la memòria del commutador.
2. Configurar el commutador perquè carregui la nova versió del sistema operatiu quan s'engegui.
3. Reiniciar el commutador.

La manera habitual de carregar la imatge del sistema operatiu és posar-la disponible mitjançant un servidor del TFTP. Un servidor del TFTP és un programari molt lleuger que es pot instal·lar fàcilment en qualsevol ordinador. Una vegada disponible, accedim des del commutador pel TFTP per copiar la imatge en la memòria flaix interna del commutador. Abans de copiar la imatge és important comprovar que disposem de suficient espai en la memòria flaix per albergar la nova imatge. Podeu fer això amb l'ordre **show flash:**:

```
Switch#show flash:
Directory of flash:/

    1  -rw-     3058048          <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
    3  -rw-        1005          <no date>  conf_commutador
    4  -rw-        1117          <no date>  no_vlan
    2  -rw-         616          <no date>  vlan.dat

60898994 bytes total (60956603 bytes free)
```

Al final podeu veure la quantitat d'espai utilitzada i la que queda lliure.

En aquest exemple suposarem que volem descarregar la nova imatge del sistema operatiu anomenada **c2950-i6q4l2-mz.121-22.EA8.bin** i que aquesta es troba en un ordinador on hem instal·lat un servidor TFTP. Aquest ordinador té l'adreça IP **192.168.0.10**.

El pas següent seria fer una còpia del fitxer del servidor TFTP en la memòria flaix interna amb l'ordre **copy tftp: flash:**. Us demanarà les dades de l'adreça IP, el nom del fitxer en el servidor i el nom que voleu donar al fitxer en la memòria flaix del commutador.

```
Switch#copy tftp: flash:
Address or name of remote host []? 192.168.0.10
Source filename []? c2950-i6q4l2-mz.121-22.EA8.bin
Destination filename [c2950-i6q4l2-mz.121-22.EA8.bin]?
```

```
5
6  Accessing tftp://192.168.0.10/c2950-i6q4l2-mz.121-22.EA8.bin....
7  Loading c2950-i6q4l2-mz.121-22.EA8.bin from 192.168.0.10:
8  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
9  [OK - 3117390 bytes]
10
11 3117390 bytes copied in 4.859 secs (641570 bytes/sec)
12 Switch#
```

Podeu comprovar que teniu els dos fitxers:

```
1  Switch#dir flash:
2  Directory of flash:/
3
4      1  -rw-     3058048          <no date>  c2950-i6q4l2-mz.121-22.EA4.bin
5      5  -rw-     3117390          <no date>  c2950-i6q4l2-mz.121-22.EA8.bin
6      3  -rw-           0          <no date>  conf_commutador
7      4  -rw-        1117          <no date>  no_vlan
8      2  -rw-         616          <no date>  vlan.dat
9
10 64016384 bytes total (57839213 bytes free)
```

El pas següent és indicar al commutador que volem que la propera vegada que s'engegui ho faci amb la nova versió del sistema operatiu. Per això fem servir l'ordre **boot system** ***fitxer amb la imatge del sistema operatiu***.

```
1  Switch(config)#boot system flash:/c2950-i6q412-mz.121-22.EA8.bin
2  Switch(config)#end
3  Switch#
4  %SYS-5-CONFIG_I: Configured from console by console
5
6  Switch#copy running-config startup-config
7  Destination filename [startup-config]?
8  Building configuration...
9  [OK]
```

Una vegada canviada i desada la configuració, podem reiniciar el commutador amb l'ordre **reload**. En el procés d'inici podeu veure com es carrega la nova imatge del sistema operatiu:

```
1  Loading "flash:/c2950-i6q4l2-mz.121-22.EA8.bin"...
2  ############################################################################ [OK]
```

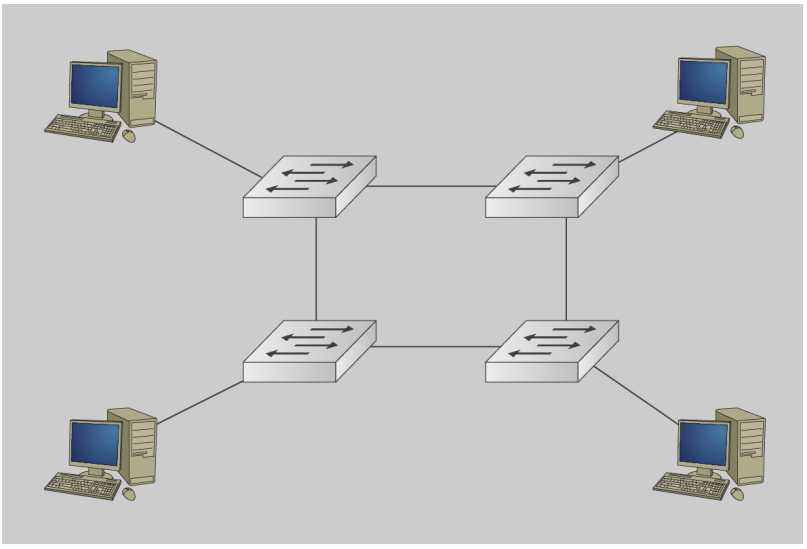
Finalment, amb l'ordre **show version** podeu veure quina és la versió del sistema operatiu que s'ha carregat:

```
1  Switch#show version
2  Cisco Internetwork Operating System Software
3  IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA8, RELEASE SOFTWARE
       (fc1)
4  Copyright (c) 1986-2006 by cisco Systems, Inc.
5  Compiled Fri 12-May-06 17:19 by pt_team
6  Image text-base: 0x80010000, data-base: 0x80562000
7
8  [...]
```

2.6 Configuració de l'spanning tree protocol

En alguns casos resulta interessant unir les LAN amb més d'un commutador. Fixeu-vos per exemple en la topologia de la figura 2.3.

FIGURA 2.3. Redundància a nivell d'enllaç



Si falla un commutador, la xarxa pot continuar funcionant

Aquesta redundància a l'hora de connectar les xarxes dóna més fiabilitat, ja que en cas de fallar un dels commutadors, encara hi ha connectivitat entre les diferents xarxes (almenys amb la majoria).

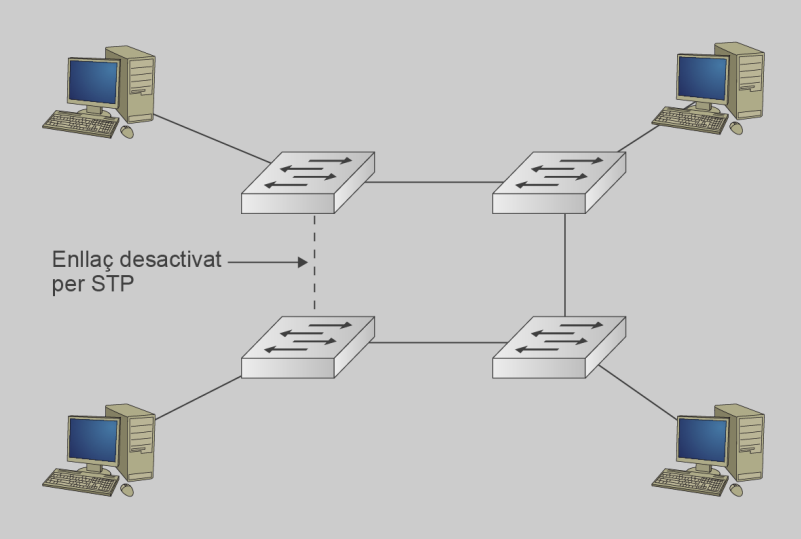
Però si analitzem el funcionament dels commutadors i dels ponts veiem que es poden produir situacions no desitjades. Els ponts i els commutadors propagaven per inundació les trames *broadcast* i les trames que no es troben en la seva taula d'adreces MAC. En el cas de la figura 2.3, una trama *broadcast* o una de dirigida a un ordinador que encara no ha enviat cap trama (i, per tant, no està emmagatzemada en cap taula MAC de cap commutador) s'anirà propagant per inundació d'un commutador als altres fins que faci tota la volta i torni al commutador original que la va propagar. Aquest commutador no pot reconèixer si ja ha enviat aquesta trama o no, i la torna a propagar, de manera que aquesta trama es queda fent voltes permanentment a la xarxa. Es diu que s'ha creat un **bucle a nivell d'enllaç**.

Pont o commutador?

Alguns dels algorismes que s'executen en els commutadors fan referència a tècniques de *bridging* o algorismes sobre ponts. Recordeu que un commutador funciona de manera semblant a un pont amb múltiples interfícies.

Per solucionar aquest problema es va crear l'***spanning tree protocol*** (protocol d'arbre d'expansió). El protocol de *spanning tree* (STP) permet que els commutadors s'enviïn paquets d'informació entre ells sobre la topologia de les connexions. Aquests paquets d'informació es coneixen com a *trames BPDU* (*bridge protocol data unit* o unitat de dades de protocol de ponts). Una vegada els commutadors saben quina és la topologia de la xarxa, desactiven connexions redundants per garantir que hi hagi un únic camí (directe o indirecte) per unir totes les xarxes (figura 2.4). D'aquesta manera s'evita la creació de bucles en la xarxa.

FIGURA 2.4. Spanning tree protocol



L'STP desactiva les connexions necessàries per trencar els bucles

L'execució de l'STP es repeteix cada cert temps. Així, si un dels enllaços no funciona (per exemple, perquè un commutador s'ha avariat), la propera vegada que s'executi el protocol s'habilitarà un camí alternatiu per substituir-lo.

2.6.1 Funcionament del protocol

L'STP fa servir l'algorisme de *spanning tree* (STA o *spanning tree algorithm*) per determinar quines interfícies dels commutadors s'han de desactivar per trencar el bucle.

L'STA escull un commutador com a **port arrel** i el fa servir com punt de referència per al càlcul de rutes. Els commutadors que executen l'STP intercanvien trames BPDU on envien un identificador de port, també anomenat BID (*bridge identifier*). El BID té els camps següents:

- Camp de prioritat del pont
- Camp identificador de sistema estès
- Adreça MAC

Es determina el BID més baix mitjançant la combinació d'aquests camps. El commutador amb BID més baix de la xarxa és escollit com a arrel de l'arbre d'expansió que calcula l'STA.

Després de determinar quin és el commutador arrel, l'STA calcula la ruta més curta per arribar-hi des de la resta de commutadors. En el càlcul del cost de la ruta es té en compte la velocitat dels ports que s'han de travessar per arribar al commutador arrel. Si hi ha més d'una ruta per arribar a l'arrel, l'STA escull la ruta de cost més baix.

Quan l'STA determina quines rutes han d'estar disponibles, bloqueja els ports dels commutadors necessaris per trencar els bucles a la xarxa.

2.6.2 Funcions dels ports

L'STP configura els ports dels commutadors amb diferents funcions per evitar els bucles en la xarxa. Hi ha quatre funcions diferents:

- **Port arrel**. N'hi ha en els commutadors que no són arrel. És el port del commutador amb una ruta millor fins al commutador arrel. Únicament hi ha un port arrel per commutador.
- **Port designat**. En el commutador arrel, tots els ports són designats. En un commutador que no és arrel, el port designat és aquell que envia trames cap al port arrel segons sigui necessari.
- **Port no designat**. És el port del commutador que està bloquejat, de manera que no envia ni rep trames.
- **Port desactivat**. És un port del commutador que està desconnectat per l'administrador.

2.6.3 Administració d'STP en els commutadors

En general, l'STP és prou transparent per als administradors, ja que simplement connectant els commutadors, aquests ja tenen la configuració d'STP per defecte i desactiven els ports necessaris per trencar els bucles. Però hi ha certs valors de configuració que es poden modificar per rectificar els resultats de l'STA.

Cost de travessar els ports

L'STA calcula les rutes cap al commutador arrel per trobar la ruta de cost més baix. Per al càlcul del cost de les rutes, té en compte la velocitat de transmissió del ports per on ha de travessar per arribar al commutador arrel. L'IEEE estableix els costos que es poden veure en la taula 5 per travessar els ports:

TAULA 2.1. Cost de travessar els ports

Velocitat del port	Cost
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

A velocitats més baixes, el cost de travessar el port augmenta

L'administrador del commutador pot configurar el cost de travessar un port. Per fer-ho hi ha l'ordre **spannin-tree cost *valor*** des del mode de configuració d'interfície.

Les ordres de canvi de prioritat de port no funcionen en el simulador de xarxa.

Per tornar a deixar el valor del cost de travessar el port predeterminat, podeu cancel·lar l'ordre anterior amb **no spanning-tree cost**.

Podeu veure les funcions i prioritats dels ports amb l'ordre **show spanning-tree** i **show spanning-tree detail** des del mode d'execució privilegiat.

```
switch#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0F06.457A.DA0C
             Cost        19
             Port        3(FastEthernet0/3)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     AB36.425A.D45A
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
```

Amb aquesta ordre podeu veure:

- la prioritat de l'arrel
- l'adreça MAC de l'arrel
- la prioritat del commutador
- l'adreça MAC del commutador
- el cost dels ports
- les funcions dels ports
- l'estat dels ports

ID de pont

El BID es fa servir per determinar quin dels commutadors de la xarxa es converteix en el commutador arrel del protocol STP. Dels camps del BID, la prioritat del pont és un valor que es pot personalitzar per modificar el resultat de l'STA i modificar el commutador que es converteix en commutador arrel.

L'administrador pot voler modificar el resultat de l'STA i fer que un commutador sigui escollit com a commutador arrel. En primer lloc, pot fer servir l'ordre **spanning-tree vlan *id_de_la_VLAN* root primary** des del mode de configuració global. Per exemple:

```
Switch(config)#spanning-tree vlan 1 root primary
```

Aquesta ordre fa que el commutador tingui el valor més baix de prioritat de la xarxa (estableix la prioritat del commutador per sota de la prioritat més baixa de commutador detectada en la xarxa).

L'ordre **spanning-tree vlan *id_de_la_VLAN* root secondary** permet configurar el commutador com a arrel alternativa. Si el commutador arrel falla, aquest commutador s'escollirà com a nou pont arrel.

L'administrador de la xarxa pot fer una configuració més específica dels commutadors especificant manualment el valor de prioritat que tindran assignats els commutadors. L'ordre per assignar la prioritat exacta del commutador és **spanning-tree vlan *id_de_la_VLAN* priority *valor***. Els valors de prioritat que es poden assignar al commutador han de ser múltiples de 4.096, si intenteu posar un altre valor, el Cisco IOS us donarà un missatge d'error i mostrarà els possibles valors que pot tenir el camp de prioritat:

```
Switch(config)#spanning-tree vlan 1 priority 50000
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch(config)#
```

2.7 Configuració de seguretat

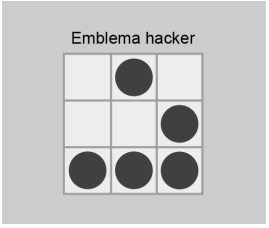
L'administrador pot configurar una sèrie de paràmetres del commutador per aconseguir una millor seguretat de la xarxa. La seguretat d'una xarxa s'ha de planificar per a tots els àmbits (físic, enllaç, xarxa, aplicació).

S'ha d'assegurar una restricció en l'accés físic als dispositius de xarxa. Tot i que és impossible assegurar que cap usuari malintencionat pugui accedir als cables de xarxa dels ordinadors, sí que podem assegurar que no puguin accedir físicament als dispositius de xarxa (commutadors i encaminadors). Aquests dispositius s'han de situar bé en sales on l'accés està restringit (com tancar amb clau les sales de servidors) o bé dins d'armaris tancats en cas que s'hagin d'instal·lar en espais d'accés compartit (com passadissos).

Respecte al commutador, s'han de afegir contrasenyes d'accés al commutador i als diferents modes de configuració d'aquest. Per fer-ho hi ha les ordres **enable password** i **enable secret** del commutador.

2.7.1 Seguretat en els ports del commutador

Per la manera de funcionar dels commutadors, un usuari malintencionat (amb els coneixements suficients sobre el funcionament dels commutadors) podria aconseguir que la xarxa funcionés d'una manera diferent de l'esperada.



Emblema hacker

Hackers

Els usuaris que volen trencar la seguretat de la xarxa fan servir programes que envien milers de trames per segon amb diferents MAC per emplenar les taules MAC dels commutadors.

Un dels atacs més comuns és l'**atac per inundació**. En aquest atac un usuari envia multitud de trames a un commutador amb adreces MAC d'origen aleatori. El commutador anirà desant aquestes adreces en la taula MAC interna fins que aquesta s'ompli i, per tant, esborri les adreces MAC desades (passant a funcionar així com un concentrador, propagant les trames per inundació).

Els ports del commutador es poden assegurar. Una mesura de seguretat per als ports és limitar la quantitat d'adreces MAC permeses en el port. Definint una sèrie d'adreces MAC permeses per un port, el commutador no commutarà trames amb una adreça MAC amb un origen fora del rang definit, evitant així els atacs per inundació.

Es poden configurar diferents formes de seguretat al port del commutador respecte de les adreces MAC vàlides al port:

- **Adreces MAC segures estàtiques**. Es poden configurar adreces MAC en la taula d'adreces MAC del commutador. També quedaran desades en la configuració d'execució del commutador. Per fer-ho es fa servir l'ordre **switchport port-security mac-address *adreça MAC*** des del mode de configuració d'interfície. Abans de configurar una adreça MAC estàtica s'ha de configurar el mode d'accés amb **switchport mode acces**, i la seguretat del port amb **switchport port-security**, o donarà un missatge d'error. Aquí teniu un exemple de com es configura una adreça MAC estàtica en un port del commutador. Fixeu-vos com aquesta queda reflectida en el fitxer de configuració del commutador.

```
Switch(config)#interface FastEthernet 0/10
Switch(config-if)#switchport port-security mac-address AB30.346D.F006
Port-security not enabled on interface FastEthernet0/10.

Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address AB30.346D.F006
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show running-config
Building configuration...

Current configuration : 1304 bytes
!
[...]

!
interface FastEthernet0/10
 switchport mode access
```

```
23 switchport port-security
24 switchport port-security mac-address AB30.346D.F006
```

Adreces enganxades

Fins a cert punt, la manera de funcionar dels ports quan estan configurats de manera *sticky* en justifica el nom. Quan les adreces MAC s'aprenen de manera dinàmica, queden en la taula d'adreces MAC del commutador de manera temporal. Quan el port està configurat com a *sticky* les adreces queden enganxades de manera permanent al port, a la seva configuració.

- **Adreces MAC segures dinàmiques**. El commutador aprèn les adreces MAC de manera dinàmica apuntant les adreces MAC d'origen de les trames que rep. Aquestes adreces no queden configurades en el commutador quan s'apaga, per tant, s'esborren i la propera vegada que s'engega no estan disponibles.

- **Adreces MAC segures enganxades**. El port registra de manera automàtica l'adreça MAC a partir de l'adreça MAC d'origen de les trames. A més a més, el commutador desa automàticament aquestes adreces MAC en la configuració en execució. Això és coneix com a *configuració sticky* en anglés, que vol dir 'enganxada'. L'ordre per configurar el funcionament del port com a *sticky* és **switchport port-security mac-address sticky**. En el moment d'executar l'ordre, les adreces MAC segures dinàmiques es converteixen en adreces MAC segures enganxades, i aquestes s'afegeixen a la configuració en execució (al fitxer *running-config*). Hi ha l'ordre per desactivar l'aprenentatge d'adreces enganxades. Com en moltes ordres al Cisco IOS precedim l'ordre amb un **no**: **no switchport port-security mac-address sticky**. Una vegada executada l'ordre, les adreces enganxades s'eliminen del fitxer de configuració en execució, però es mantenen en la taula d'adreces MAC del commutador. Per configurar la quantitat màxima d'adreces MAC que hi pot haver registrades en un port del commutador hi ha l'ordre **switchport port-security maximum *nombre_adreces***.

Si es desen les adreces MAC enganxades en un fitxer de configuració d'arrencada (*startup-config*), quan es torni a engegar el commutador aquestes adreces ja estaran configurades.

Amb aquestes configuracions de port, l'administrador es pot assegurar que:

- En cap port del commutador no s'afegiran més adreces MAC de les establertes.
- Les adreces MAC que estan configurades com a segures accediran a cada port del commutador.

Es produeix una violació de la seguretat quan alguna d'aquestes característiques no es compleix. Per exemple, es produirà una violació de la seguretat:

- Quan en un port del commutador s'hi intentin afegir més adreces MAC de la quantitat màxima definida.
- Quan s'accedeixi amb una adreça MAC segura des d'un altre port diferent al que està configurada.

SNMP

Simple network management protocol és un protocol de capa d'aplicació que serveix per intercanviar informació d'administració entre els dispositius de xarxa.

En aquest casos el commutador es pot comportar de diferents maneres:

- **Protecció**. En cas que s'hagi superat el límit màxim d'adreces MAC segures que està establert en el port, es descarten les trames que tenen una adreça MAC d'origen que no està configurada com a segura en el commutador. Aquesta situació es mantindrà fins que s'augmenti la quantitat màxima d'adreces MAC segures del port.
- **Restricció**. De la mateixa manera que en el mode de protecció, en cas que s'hagi superat el límit màxim d'adreces MAC segures que està establert en el port, es descarten les trames que tenen una adreça MAC d'origen que no està configurada com a segura en el commutador. Aquesta situació es mantindrà fins que s'augmenti la quantitat màxima d'adreces MAC segures del port. La diferència és que en aquest cas s'adverteix de la violació de la seguretat. Es registra la incidència en el registre del sistema (*syslog*), s'augmenta el comptador d'incidències i s'envia una trama SNMP (*simple network management protocol*, protocol senzill d'administració de xarxa).
- **Desactivació**. En aquest mode el port es desactiva a causa de la violació de seguretat. Per fer constar la incidència es registra un missatge en el registre del sistema (*syslog*) i s'augmenta el comptador d'incidències. També s'envia una trama SNMP. Per tornar a activar el port s'ha de fer explícitament des del mode de configuració d'interfície amb les ordres **shutdown** seguides de **no shutdown**.

Per canviar el mode de funcionament del port quan es produeix una violació de la seguretat, s'ha d'escriure des del mode de configuració d'interfície l'ordre **switchport port-security violation *mode***, en què mode és un dels tres modes de funcionament del port (**protect**, **restrict**, **shutdown**):

```
Switch(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

Per comprovar l'estat actual de la seguretat del port feu servir l'ordre **show port-security interface *nom_interfície***. Per exemple:

```
switch#show port-security interface FastEthernet 0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Podeu veure:

- Si la seguretat del port està activada.
- L'estat del port.

- El mode de funcionament del port si es produeix una violació de la seguretat.
- La quantitat màxima d'adreces segures per a la interfície.
- La quantitat d'adreces MAC de la interfície.
- El comptador de violacions de seguretat.

Si el que voleu és comprovar les adreces MAC segures configurades en totes les interfícies del commutador, feu servir l'ordre **show port-security address**.

```
Switch#show port-security address
      Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address     Type       Ports   Remaining Age(mins)
10   23A7.E073.0050  SecureConfigured Fa0/1   -
10   00F3.FF8E.A265  SecureConfigured Fa0/7   -

------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```