Monitoratge i detecció d'incidències

Xavier Marchador Márquez

Índex

Introducció **5**

Resultats d'aprenentatge **7**

1 Procediments sistemàtics de verificació i prova d'elements de connectivitat de xarxes locals **9**
1.1 Procediments de verificació de la connectivitat . . . 11
1.1.1 Procés de verificació del nivell físic . . . 13
1.1.2 Procés de verificació del nivell d'enllaç . . . 14
1.1.3 Procés de verificació del nivell de xarxa . . . 14
1.1.4 Procés de verificació del nivell de transport . . . 14
1.1.5 Procés de verificació del nivell d'aplicació . . . 15
1.2 Eines de verificació de la connectivitat . . . 16
1.3 Casos pràctics: verificació de les connexions i documentació dels processos de prova i verificacions fets . . . 18
1.3.1 Pèrdua de connexió en el servidor web . . . 18
1.3.2 Configuració i diagnòstic dels equips de xarxa . . . 21

2 Actualització dels dispositius de xarxa **29**
2.1 Components actualitzables . . . 29
2.1.1 Actualització de maquinari . . . 30
2.1.2 Dispositius no modulars . . . 30
2.1.3 Dispositius modulars . . . 31
2.1.4 Actualització de programari . . . 32
2.2 Substitució de components dels dispositius de comunicacions . . . 32
2.3 Descripció dels passos que cal seguir en l'actualització de programari de dispositius de comunicació . . . 34
2.4 Cas pràctic: exemple d'actualització de programari . . . 36

Introducció

Les xarxes de dades, a causa de les seves àmplies possibilitats com a mecanisme de compartició d'informació i de recursos, s'han convertit en una eina de treball imprescindible. Cada vegada costa més recordar aquells anys en què els ordinadors eren simples substituts de les calculadores tradicionals i un element decoratiu en els despatxos dels directors.

En els últims anys les xarxes han passat a formar part de les nostres vides, sobretot gràcies a l'expansió de la xarxa més famosa i gran que hi ha: Internet.

La ciència avança amb passos de gegant, i dia rere dia apareixen en el mercat tot tipus de productes de l'electrònica de consum amb un denominador comú: la possibilitat de connectar-los en xarxa.

La proliferació de les xarxes i la dependència que en tenim ha fet necessari que les empreses disposin de personal tècnic qualificat que es pugui fer càrrec de l'administració, manteniment i supervisió. Les tasques que aquests tècnics han de fer requereixen uns determinats coneixements i, en certs casos, disposar d'eines específiques.

Quan a un administrador de xarxa se li notifica o detecta una incidència, principalment un tall o degradació del servei, aquest es posa en alerta per tal de trobar indicis o pistes que li puguin suggerir per on pot començar a cercar l'origen del problema.

Resoldre problemes de xarxa és una tasca complexa tot i disposar d'eines. Es necessita formació, metodologia i experiència per poder actuar de manera acurada en aquestes situacions.

En aquest mòdul adquirireu part d'aquesta formació i podreu veure algunes metodologies i procediments per tal de poder fer front a aquests problemes de manera professional, amb confiança i seguretat.

Tot i que els procediments descrits en aquest mòdul i els exemples dels casos pràctics descriuen situacions habituals, no cobreixen totes les possibles situacions amb què us podeu trobar, ja que això resultaria impossible; per tant, és molt important adquirir una base de coneixements i anar acumulant experiència.

Al llarg de la vostra carrera professional anireu adquirint aquesta experiència, que us servirà per anar modelant els vostres propis procediments i mecanismes de supervisió i resolució d'incidències.

En l'apartat "Procediments sistemàtics de verificació i prova d'elements de connectivitat de xarxes local" veurem quins són els procediments que hem de seguir per tal d'obtenir la informació necessària per a documentar la xarxa, la qual cosa ens ajudarà a identificar els problemes que al llarg del temps haurem de

fer front. Veurem quines eines tenim al nostre abast per tal d'identificar l'origen del problema i com podem solucionar-ho.

En l'apartat "Actualització dels dispositius de xarxa" veurem que hi ha dispositius de xarxa modulars i d'altres no modulars, els quals poden ser actualitzats a nivell de programari o maquinari per aconseguir millores en el rendiment de la xarxa, disposar de noves funcionalitats o simplement substituir els components defectuosos. Veurem quins passos cal seguir per realitzar aquestes actualitzacions de manera segura i evitar que aquestes provoquin problemes en la xarxa.

Resultats d'aprenentatge

En finalitzar aquesta unitat l'alumne/a:

1. Aplica els procediments de prova i verificació dels elements de connectivitat de la xarxa i les eines per a aquests processos.
    - Explica les etapes d'un procés de verificació de connectivitat en una xarxa local.
    - Enumera les eines utilitzades per verificar la connectivitat en una xarxa local, segons les tecnologies implementades a les xarxes locals.
    - Explica el funcionament operatiu de les eines de gestió de xarxa per comprovar l'estat dels dispositius de comunicacions, tenint en compte les especificacions tècniques de les eines.
    - En un cas pràctic d'una xarxa local ja instal·lada, verifica les opcions de connexió permeses i prohibides, així com l'accés als recursos compartits, seguint uns procediments donats.
    - En un cas pràctic d'una xarxa local ja instal·lada, documenta els processos de prova i verificació duts a terme, d'acord amb unes especificacions tècniques.
2. Enumera els components actualitzables dels dispositius de comunicacions i en descriu les característiques.
    - Identifica els paràmetres de compatibilitat dels components que s'han d'actualitzar per assegurar l'efectivitat en els processos segons les especificacions tècniques dels esmentats components.
    - Descriu els passos que s'han de seguir per actualitzar el programari de dispositius de comunicacions, i detalla les accions fetes en cada pas i les eines del programari utilitzades en els components de dispositius de comunicacions.
    - Substitueix components de dispositius de comunicacions per aconseguir una configuració donada, seguint uns procediments definits.
    - Actualitza el programari de dispositius de comunicacions per aconseguir una configuració donada, seguint uns procediments definits.

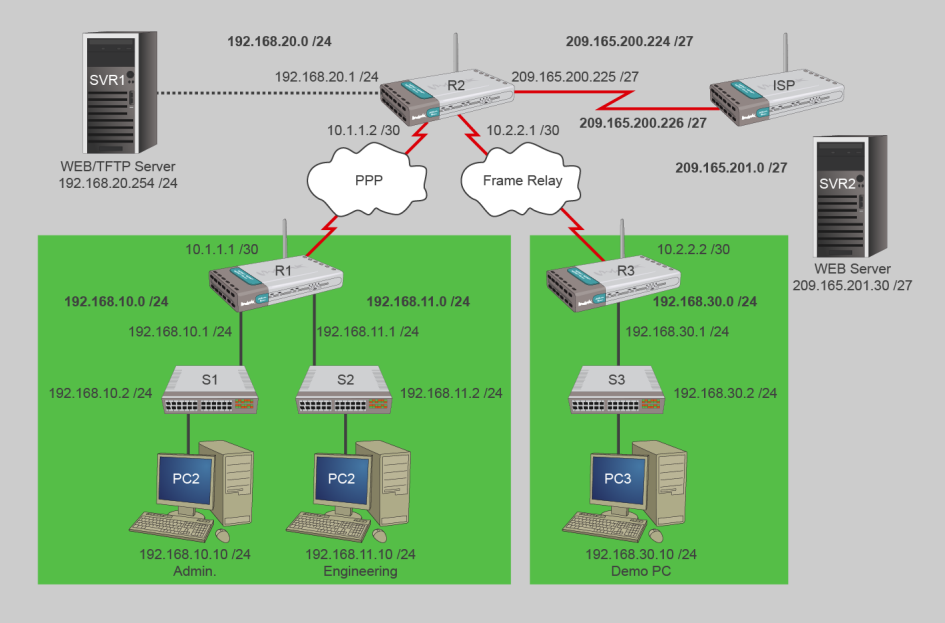
1. Procediments sistemàtics de verificació i prova d'elements de connectivitat de xarxes locals

Per tal de ser capaços de supervisar una xarxa i poder diagnosticar i resoldre correctament els problemes que poden sorgir heu de saber com ha estat dissenyada la xarxa, quins dispositius en formen part i quin és el seu funcionament en condicions normals. Aquesta informació és coneix com a *línia base* (*baseline*).

Com més informació de la xarxa tingueu més robust serà el vostre coneixement i més acurada serà la vostra actuació davant els problemes. És recomanable que com a mínim la documentació de la xarxa inclogui la informació següent:

- Diagrama de la topologia.
- Configuració dels dispositius de xarxa (encaminadors, concentradors, commutadors, etc).
- Documentació d'equips finals (servidors, ordinadors d'escriptori, dispositius mòbils, etc).

Figura 1.1. Exemple de diagrama de topologia



1. Diagrama de la topologia. El diagrama que podeu observar en la figura 1.1 conté un gràfic de les connexions dels diferents equips de xarxa i els equips finals, incloent-hi el medi, tecnologia i adreçament IP. Aquesta informació us serà molt útil per tal de saber amb un cop d'ull quins són els principals recursos de xarxes afectats pel mal funcionament d'un determinat dispositiu.

2. Configuració dels dispositius de xarxa. Aquest document ha de contenir informació sobre el tipus de maquinari de xarxa, i ha d'identificar cadascun dels dispositius de manera única facilitant una relació dels dispositius veïns connectats. Com a mínim hauríeu de disposar de les dades següents:

- Fabricant i model del dispositiu.
- Versió del sistema operatiu.
- Nom o identificador únic.
- Adreçament físic i lògic (si en té).
- Tipus de port de connexió.
- Dispositius veïns amb qui està connectat.
- Ubicació del dispositiu.

Problemes en les xarxes

Una de les principals causes de problemes en les xarxes és la connexió de dispositius no controlats o supervisats directament pels administradors de la xarxa com ara ordinadors portàtils d'usuaris convidats, els quals són susceptibles d'estar mal configurats.

3. Documentació d'equips finals. Els servidors, ordinadors d'usuari, telèfons mòbils multimèdia (*smartphones*) i la resta de dispositius que permeten als usuaris accedir o proporcionar contingut són susceptibles de causar problemes en una xarxa a causa d'un mal ús o la vulnerabilitat del programari. Per tant, és important saber quins programes o serveis executa. És recomanable conèixer:

- Nom o identificador únic.
- Sistema operatiu (nom, versió i pedaços de seguretat instal·lats).
- Adreçament IP.
- Aplicacions o serveis que fan un ús intensiu de la xarxa (DNS, HTTP, VoIP, etc.).
- Ubicació del dispositiu.

TAULA 1.1. Inventari de dispositius

ID dispositiu	Sistema operatiu	Adreçament	Aplicacions de xarxa	Ubicació
SWEB01	Linux Debian Etch	192.168.1.100/24	Apache 2.0 (HTTP)	Sala màquines Prestatge 1
SFTP01	Windows Server 2003 R2 + SP2	192.168.1.200/24	IIS 6.0 (FTP)	Sala màquines Prestatge 3
PCA02	Windows XP + SP3	192.168.5.1/25	-	Despatx administració
PCD01	Windows Vista + SP1	192.168.2.5/5	-	Despatx gerència

Disposar de la documentació de la xarxa és el primer pas, però no serà suficient per poder detectar incidències. Una xarxa de comunicacions presenta un comportament diferent al llarg del dia, ja que els usuaris que la fan servir i el trànsit de dades que transporta no són sempre els mateixos.

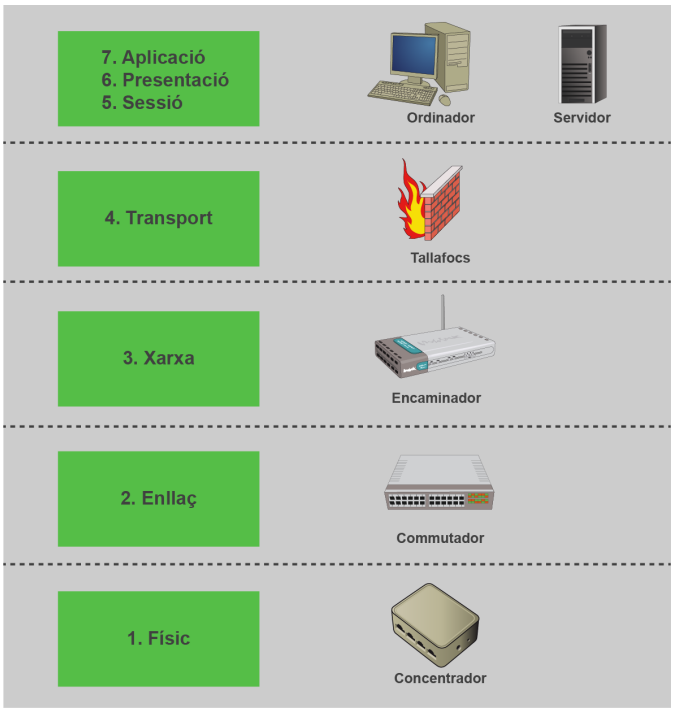
Una vegada la xarxa està totalment configurada i operativa n'hem d'observar el comportament, recollint estadístiques sobre l'amplada de banda ocupada, el tipus de trànsit que hi circula, els serveis més utilitzats i els usuaris que consumeixen més recursos. Tots aquests factors repercuteixen de manera directa en l'estat de salut dels dispositius de xarxa, i un mal disseny o supervisió poden provocar que aquests pateixin càrregues de processador massa elevades o que hi hagi més volum de trànsit del que els circuits poden suportar, cosa que provoca, en molts casos, deficiències en el servei i fins i tot talls en la connexió.

Gràcies a les dades recollides sobre l'ús de la xarxa en diferents hores i dies podrem establir un patró d'ús que ens permetrà utilitzar-lo com a punt de referència. Qualsevol pauta de comportament fora dels valors registrats pot ser un indici d'un problema en la xarxa. Arribats a aquest punt, haureu de comprovar l'estat dels diferents dispositius de la xarxa per tal d'esbrinar si realment hi ha un problema.

1.1 Procediments de verificació de la connectivitat

Quan es rep un avís per part d'un usuari que Internet o un altre servei determinat de xarxa no funciona és quan s'ha de decidir quin enfocament se seguirà per tal d'intentar entendre què és el que no funciona.

Figura 1.2. Model de referència OSI



Els **models de xarxa lògics** com l'OSI (interconnexió de sistemes oberts, de l'anglès: *Open System Interconnection*, figura 1.2) i el TCP/IP separen les funcionalitats de la xarxa en diferents nivells o capes que faciliten l'aïllament del problema en la capa afectada.

Models de referència

El model de referència OSI va ser desenvolupat l'any 1977 per part de la *International Organization for Standardization* (ISO), mentre que el model TCP/IP va ser creat l'any 1970 per la *Internet Engineering Task Force* (IETF).

És important que tingueu clar en quina capa treballa cada dispositiu de xarxa i l'efecte que pot tenir que no funcioni correctament per poder estimar com pot afectar això el rendiment global de la xarxa. Si, per exemple, la connectivitat pateix talls intermitents, podem pressuposar un problema físic amb el cablatge o els connectors; en canvi, si tots els indicadors d'estat dels dispositius de cada extrem indiquen que hi ha connexió però no ens aconseguim connectar, ens podem centrar en la capa de xarxa i revisar l'adreçament IP.

Dels set nivells OSI, la majoria de dispositius de xarxa treballen en els quatre inferiors (físic, enllaç, xarxa i transport), mentre que les aplicacions dels usuaris treballen principalment en els nivells superiors. Això us servirà per escollir la millor aproximació a l'hora de verificar els problemes de connexió d'una xarxa.

Col·lisions

Les col·lisions es produeixen quan dos equips intenten transmetre simultàniament pel mateix segment de xarxa.

Els símptomes més comuns de problemes segons la capa on es troben són els següents:

- **Físic**: en aquest nivell els problemes més comuns són connexions intermitents, congestió de trànsit, col·lisions, ús elevat de CPU dels dispositius de xarxa i rendiment inferior als valors normals.
- **Enllaç**: falla la connectivitat en capes superiors, el trànsit arriba a la destinació però amb un rendiment inferior, el trànsit no arriba a la destinació, hi ha un excés de trànsit de gestió de protocols d'estat de l'enllaç o de senyalització.
- **Xarxa**: si falla el nivell de xarxa probablement no hi haurà connectivitat o si n'hi ha la xarxa funcionarà amb un rendiment inferior a l'esperat; el trànsit segueix un recorregut poc òptim fins a la destinació.
- **Transport**: els problemes més habituals d'aquest nivell són que falla un tipus específic de trànsit, intermitències en la connexió o problemes de seguretat.

Les capes superiors (sessió, presentació i aplicació) moltes vegades per simplificar, i atès que treballen de manera molt propera una amb l'altra, es tracten com si fos una sola capa i s'hi fa referència com a *capa d'aplicació*.

TAULA 1.2. Simplificació de les capes superiors

Número de capa	Nom de capa	Capa resultant
7	Aplicació	Aplicació
6	Presentació	Aplicació
5	Sessió	Aplicació

Els símptomes més habituals de problemes en aquesta capa són que les aplicacions dels usuaris funcionen més lentament de l'esperat, que apareixen errors per pantalla o que certes funcionalitats de l'aplicació no funcionen correctament.

1.1.1 Procés de verificació del nivell físic

Per tal de verificar que al nivell més baix de tots la configuració és correcta, haureu de revisar els cables i els connectors. És important que reviseu que aquests no tinguin talls, que no estiguin deteriorats o que facin bon contacte. Si això sembla correcte reviseu que el tipus de cable i connector sigui el que toqui, ja que molts cables i connectors són d'aparença similar però des del punt de vista elèctric no són compatibles i provoquen tot tipus de problemes si es connecten per error.

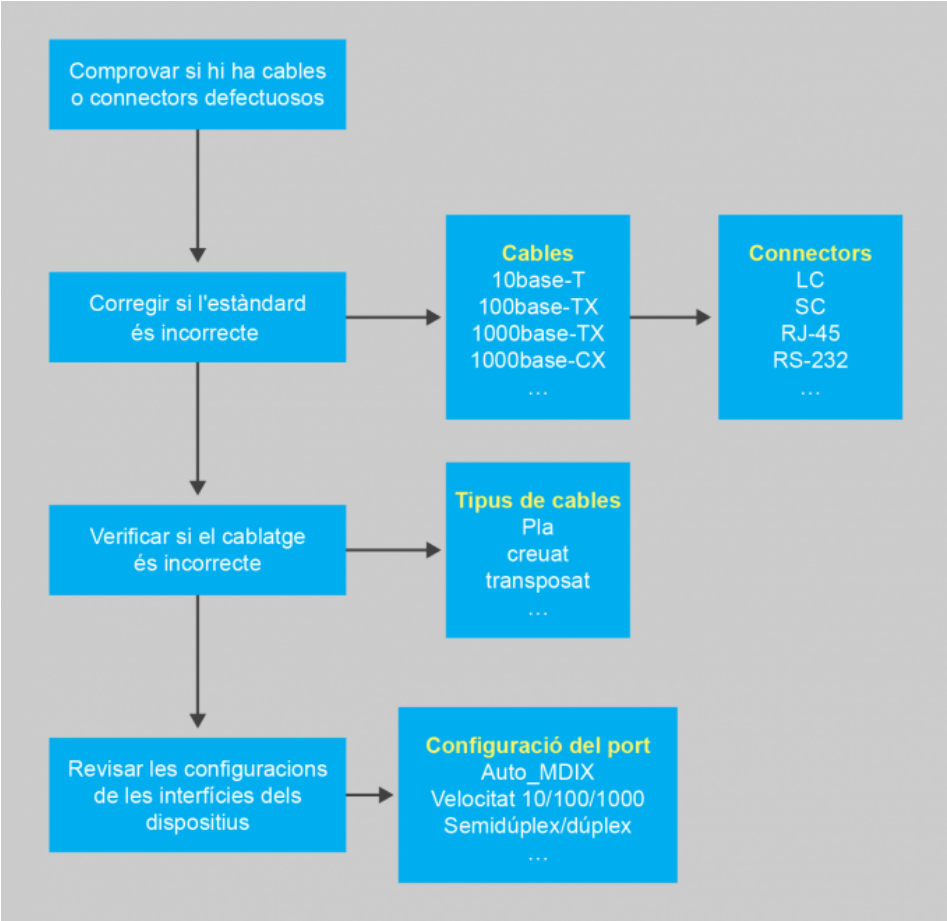
No forceu mai un connector, ja que és probable que si no entra amb facilitat sigui perquè el connector no és del tipus adequat.

Si els cables i els connectors semblen en bon estat comproveu que els fils tinguin la configuració pertinent (cable pla, creuat o transposat) i que la configuració del port de connexió de l'equip sigui correcta, revisant que la velocitat (10, 100, 1000 Mbps, etc.) i el mode de funcionament (dúplex o semidúplex) siguin els mateixos als dos extrems. Podeu agafar com a referència l'esquema de la figura 1.3 per tal de diagnosticar problemes relacionats amb els components físics.

Modes dúplex

Dúplex és un mode de transmissió que permet enviar i rebre dades simultàniament, mentre que el semidúplex sols permet enviar o rebre dades però no en tots dos sentits al mateix temps (emissió i recepció).

FIGURA 1.3. Procediment de diagnòstic d'incidències



1.1.2 Procés de verificació del nivell d'enllaç

Diem que es produeix un bucle quan la informació es propaga per la xarxa indefinidament a causa de l´existència de múltiples camins que formen un circuit tancat.

Els problemes que es produeixen al nivell d'enllaç són més comuns a les xarxes d'àrea ampla (WAN) que a les xarxes d'àrea local (LAN); no obstant això, encara que treballeu només en entorns de LAN és recomanable verificar que no es produeixen bucles.

Una *virtual local area network* (VLAN) és un mecanisme que permet segmentar una xarxa d'àrea local física en diverses xarxes lògiques.

Avui dia és molt habitual tenir una gran quantitat d'equips finals connectats en un mateix commutador gran i no pas en diversos commutadors petits. Per poder segmentar aquest commutador en diverses xarxes es fan servir les xarxes d'àrea local virtuals (VLAN). Quan dos equips que pertanyen a la mateixa xarxa no es puguin comunicar reviseu que la VLAN que té configurat el port del commutador de cadascun dels equips sigui la mateixa, ja que en cas de no ser-ho els equips no es podran veure. Això seria l'equivalent que cadascun estigués connectat a un commutador físic diferent. Pareu compte també que la configuració dels ports de *trunk* (si n'hi ha) sigui correcta i que cap sistema final estigui connectat a un punt de *trunk*.

1.1.3 Procés de verificació del nivell de xarxa

Els problemes de nivell de xarxa acostumen a estar provocats per un problema en l'adreçament IP, les taules d'encaminament o un canvi de topologia.

Reviseu si hi ha hagut algun canvi en la topologia de la xarxa, és a dir, que no s'hagi connectat un nou dispositiu o que algun altre s'hagi desconnectat. Les xarxes disposen de mecanismes per tornar a convergir quan es produeix algun d'aquest canvis, però els resultats no són sempre els esperats.

Comproveu també que algun equip de xarxa no s'hagi reiniciat, ja que a efectes pràctics això tindria el mateix comportament que si l'haguéssiu desconnectat, i els mecanismes de convergència entrarien en funcionament igualment.

Convergència d'una xarxa

Quan es produeix algun canvi de configuració o topologia en una xarxa, els equips que en formen part s'han d'habituar a la nova situació, fet que pot provocar que certs serveis o protocols no funcionin de manera habitual. Quan tots els equips de xarxa s'han assabentat i adaptat a la nova situació es diu que la xarxa ha convergit.

Llista de control d'accés

Una llista de control d'accés o ACL, com indiquen les seves sigles en anglès, és un conjunt de regles que serveix per permetre o denegar l'accés a determinats serveis, protocols i equips de la xarxa.

1.1.4 Procés de verificació del nivell de transport

Els problemes de nivell de transport acostumen a provocar que certes aplicacions o serveis no funcionin correctament, de manera que es produeixen talls intermitents o permanents en el servei.

La font d'origen del problema pot estar en un tallafocs que filtra el trànsit, una llista de control d'accés d'un encaminador o un problema en la configuració del programari.

Recordeu que en el nivell de transport és igual d'important revisar la configuració dels equips de xarxa i la dels ordinadors i servidors mateixos que participen en el procés de comunicació.

Serveis típics que poden provocar problemes en aquest nivell són els servidors de DNS, el DHCP i les configuracions de NAT. En aquest últim cas hi ha certes aplicacions que poden requerir configuracions específiques per tal de poder funcionar correctament darrere d'un NAT.

El "network address translation" (NAT)

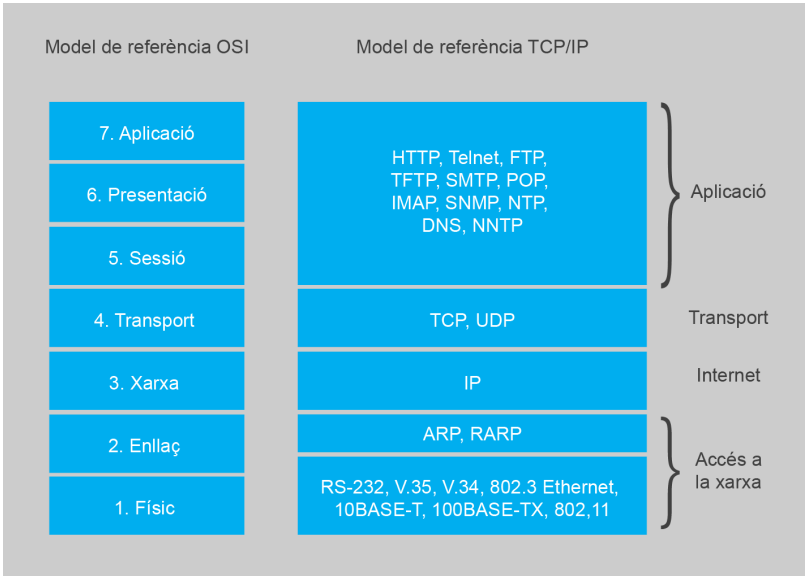
És un mecanisme que permet a diversos equips interns de la xarxa connectar-se a altres xarxes públiques, com per exemple Internet, amb una sola adreça IP, que comparteixen entre tots. Aquest mecanisme també permet amagar l'adreça IP real d'un equip intern. Fer servir NAT en una xarxa té avantatges i desavantatges. Com a avantatge podem esmentar que aprofitem millor l'encaminament IP públic i augmentem la seguretat en la xarxa interna, ja que que el seu encaminament queda ocult des de l'exterior de la xarxa. Com a desavantatge, podem destacar que certes aplicacions no funcionen correctament i que cal tenir cura de la manera en què es configura el NAT en dispositius tallafoc si es vol accedir a determinats serveis com servidors de vídeo en temps real, xarxes privades virtuals (VPN), etc.

1.1.5 Procés de verificació del nivell d'aplicació

En el nivell d'aplicació resideixen la majoria de protocols que ofereixen serveis entre màquines, com per exemple el correu electrònic, el servidor de pàgines web, la transferència de fitxers o l'establiment de sessions de terminal.

La figura 1.4 mostra els protocols més comuns segons el nivell al qual pertanyen.

Figura 1.4. Comparació del model OSI amb el model TCP_IP



1.2 Eines de verificació de la connectivitat

Hi ha diverses eines que us poden ajudar a diagnosticar i corregir errors en la xarxa. Aquestes eines poden ser de programari o maquinari. En el primer cas (vegeu la taula 1.3) en podem trobar de gratuïtes que venen amb el mateix sistema operatiu que estem fent servir o d'altres comercials que podeu adquirir en funció de les vostres necessitats.

Taula 1.3. Taula d'ordres i programes de diagnòstic de xarxa

Programari	Sistema operatiu	Tipus	Serveix per
ping	Tots	Proves de connexió.	Provar la connectivitat d'extrem a extrem, que el trànsit arriba a la destinació i pot tornar. Comprovar que la pila de protocols TCP/IP està correctament instal·lada i operativa.
telnet	Multiplataforma	Gestió remota i proves de ports.	Permet establir sessions de terminal amb dispositius de xarxa o servidors. Permet administrar remotament aquests dispositius. Comprovar que un determinat port de connexions no està filtrat i que el servei que hi ha al darrere està operatiu.
arp	Multiplataforma	Comprova l'estat de la targeta de xarxa.	Comprovar la correspondència d'una adreça IP amb l'adreça física (MAC).
nslookup*, *dig*, *host	Multiplataforma	Comprovacions DNS.	Fer consultes al DNS per saber si un domini és resoluble, si el servidor de DNS està operatiu i per saber si hi ha una entrada directa i inversa per a un nom i adreça IP.
netstat*, *lsof	Segons el programari	Comprova l'estat de les connexions.	Comprovar l'estat de les connexions d'un ordinador, mostrant les sessions establertes i les que estan en mode d'espera.
tcpdump*, *wireshark	Multiplataforma	Sniffers	Analitzar i conèixer el tipus de trànsit d'entrada i sortida des d'un determinat equip cap a un altre.
nmap	Multiplataforma	Escaneig de ports.	Analitzar quins ports i serveis té operatius un determinat equip.
HP Openview*, *Solar Winds*, *CiscoView*, *What's up Gold*, *SpiceWorks*, *Nagios	Segons el programari	Eines de monitoratge de xarxa (NMS).	Monitorar la xarxa, recollir informació de l'estat dels dispositius, generar gràfiques i estadístiques d'ús, configurar els equips a distància, etc.

Les eines de maquinari ens permeten analitzar l'estat dels components de la xarxa a més baix nivell i de manera independent del sistema operatiu dels dispositius que formen part de la xarxa.

Les eines més habituals són:

- **Mòduls d'anàlisi de xarxa**: els mòduls d'anàlisi de xarxa (NAM) són targetes que es poden instal·lar en determinats equips de xarxa i que permeten analitzar el trànsit que hi passa i generar gràfiques, estadístiques i informes sobre aquest. No tots els dispositius de xarxa ho admeten; de fet, és una de les opcions més cares, ja que els equips que ho poden fer servir són de gamma alta. Tot i això, és una bona opció perquè són una font d'informació fiable, ja a que obtenen la informació directament de l'equip en què estan connectats.

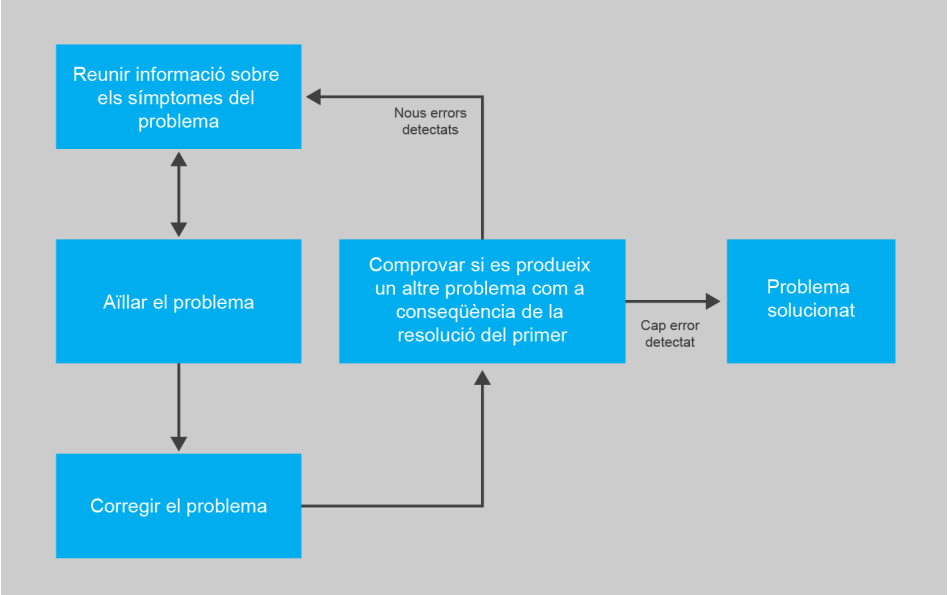
- **Multímetres digitals**: els multímetres digitals són eines de mà que ens permeten analitzar valors físics dels components de la xarxa com ara valors de voltatge, corrent, resistència i altres factors que poden afectar l'estat de les fonts d'alimentació dels dispositius de xarxa.

- **Comprovadors de cable**: els comprovadors de cable permeten analitzar l'estat dels cables i els seus connectors. Hi ha diversos tipus de comprovadors en funció del cable que hem d'analitzar (fibra òptica, coure, etc.). Aquests dispositius ens permeten detectar si el cable està creuat, tallat, si té els parells de cable mal connectats, etc. En el cas de la fibra també ens poden proporcionar informació sobre si la fibra és multimode o monomode i la potencia de transmissió.

- **Analitzadors de xarxa**: els analitzadors de xarxa van més enllà del simple comprovador de cable; a part de la informació que proporcionen, poden comprovar l'estat de les connexions amb dispositius de xarxa com ara commutadors i encaminadors i poden proporcionar informació sobre el port on està connectat, la VLAN per la qual circulen els paquets, l'amplada de banda utilitzada i moltes altres dades. Aquesta informació normalment es pot transferir a un ordinador amb un programari de monitoratge de xarxa per tal de ser analitzada amb detall.

Una vegada tenim clar quines eines tenim al nostre abast per detectar incidències a la xarxa podeu fer servir l'esquema de la figura 1.5 per tal de diagnosticar els problemes.

FIGURA 1.5. Diagnòstic i resolució de problemes de xarxa



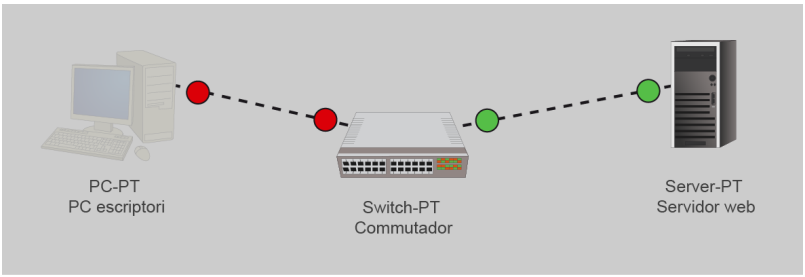
1.3 Casos pràctics: verificació de les connexions i documentació dels processos de prova i verificacions fets

En aquest apartat veurem dos casos pràctics que simulen errors a l'hora de connectar-se a un servidor web. Es pretén que veieu quins són els passos que heu de seguir per diagnosticar l'origen del problema i com el podeu solucionar.

1.3.1 Pèrdua de connexió en el servidor web

Carregueu el laboratori *lab1* en el *packet tracer* i reviseu la topologia de xarxa configurada. Hauríeu de veure el mateix que a la figura 1.6.

FIGURA 1.6. Laboratori del cas pràctic 1



Us informen que el PC-Escriptori no és capaç d'accedir al Servidor-Web i que, per tant, la pàgina web que allotja no es pot mostrar. Com a tècnics informàtics, us demanen que verifiqueu el motiu pel qual passa això i que ho deixeu en funcionament el més aviat possible.

Revisant la topologia podeu veure que aquesta és molt bàsica: només hi ha un PC d'escriptori, un commutador i un servidor, fet que us facilitarà molt el procés de verificació del cablatge i altres components físics de la connexió.

Primer de tot, comproveu que efectivament el servidor web no és accessible (figura 1.7), ja que a vegades es poden produir problemes puntuals de càrrega que només afecten a intervals de temps. Per fer-ho, obriu el navegador web des del PC i connecteu-vos a l'adreça 192.168.0.100.

Figura 1.7. Servidor web no accessible

Com podeu veure, obteniu un missatge d'error i no es mostra la plana web.

Reviseu la configuració del PC per verificar que la targeta de xarxa està configurada correctament.

```
PC>ipconfig /all

Physical Address.................: 0007.ECCC.3294
IP Address.......................: 192.168.0.5
Subnet Mask......................: 255.255.255.0
Default Gateway..................: 192.168.0.1
DNS Servers......................: 192.168.0.1
```

Adreça de loopback

L'adreça IP 127.0.0.1 està reservada per fer proves de connectivitat local i mai no pot ser assignada a un ordinador com a adreça de xarxa principal, ja que és comuna a tots els ordinadors.

Ara mireu si sou capaços de fer un *ping* al mateix equip PC per comprovar la connectivitat local de l'equip. Tots els ordinadors es poden fer *ping* a si mateixos mitjançant l'adreça de *loopback*.

```
PC>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time=10ms TTL=128
Reply from 127.0.0.1: bytes=32 time=10ms TTL=128
Reply from 127.0.0.1: bytes=32 time=20ms TTL=128
Reply from 127.0.0.1: bytes=32 time=10ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 20ms, Average = 12ms
```

Com podeu veure, hi ha resposta, fet que indica que la pila de protocols TCP/IP està instal·lada correctament.

Adreça de xarxa

L'adreça de xarxa 192.168.0.0/24 resumeix les adreces compreses entre 192.168.0.0 i 192.168.0.255, totes dues incloses.

Ara comproveu l'adreça IP del servidor i mireu si està configurada amb el mateix criteri que el PC.

```
SERVER>ipconfig /all

Physical Address.................: 0001.423A.39C2
```

```
IP Address.....................: 192.168.0.100
Subnet Mask....................: 255.255.255.0
Default Gateway................: 192.168.0.1
DNS Servers....................: 0.0.0.0
```

Podeu veure com l'adreça pertany a la mateixa xarxa 192.168.0.0/24 i que, per tant, pel que fa a la configuració sembla correcta. La taula 1.4 reflecteix la configuració dels dos equips.

TAULA 1.4. Adreçaments de xarxa

Equip	Adreça IP	Màscara de xarxa	Porta d'enllaç
PC-Escriptori	192.168.0.5	255.255.255.0	192.168.0.1
Servidor-Web	192.168.0.100	255.255.255.0	192.168.0.1

Proveu, doncs, a fer el *ping* des del PC al servidor.

```
PC>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Podeu observar que no hi ha resposta. Atès que la configuració sembla correcta, reviseu el cablatge dels diferents equips implicats en el procés de comunicació.

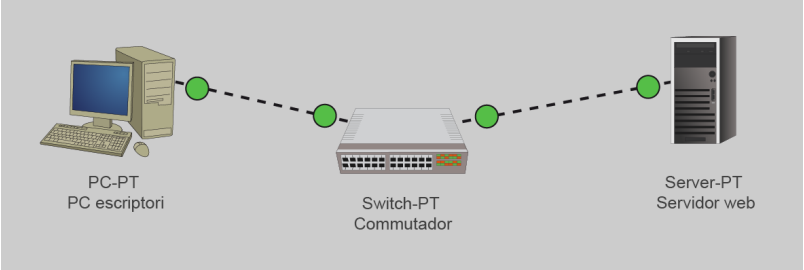
Com podeu veure, la connexió entre el PC i el commutador està en vermell, mentre que la connexió entre el commutador i el servidor està en verd. Això, si es tractés d'uns equips reals, seria l'equivalent a comprovar els LED de senyalització dels connectors de xarxa i dir que no hi ha connectivitat entre el PC i el commutador.

Amb una revisió més acurada podeu apreciar com el cable de xarxa que uneix el PC amb el commutador, que és el que no funciona, és de tipus discontinu, mentre que el que uneix el servidor amb el commutador és continu. Segons les especificacions dels *packet tracer*, el primer és de tipus creuat i el segon pla.

Recordeu que quan un PC es connecta a un concentrador o commutador heu de fer servir cables plans, ja que si no és així el més probable és que no hi hagi connexió.

Canvieu el tipus de cable entre el PC i el commutador per un de pla i comproveu de nou si hi ha connectivitat. El nou diagrama hauria de ser similar al de la figura 1.8.

FIGURA 1.8. Laboratori operatiu



| |Cisco packet tracer

Ara feu el *ping* i verifiqueu que els *pings* arriben a la destinació.

```
PC>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=101ms TTL=128
Reply from 192.168.0.100: bytes=32 time=50ms TTL=128
Reply from 192.168.0.100: bytes=32 time=40ms TTL=128
Reply from 192.168.0.100: bytes=32 time=40ms TTL=128

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 101ms, Average = 57ms
```

Tal com es mostra en el resultat, tots els *pings* han arribat a la destinació i, per tant, la connexió ha quedat restablerta. Sols resta comprovar que el servidor web torna a ser accessible. Si ho és, vol dir que el servidor proporciona aquest servei i que el port 80 (que correspon a HTTP) és accessible; si no poguéssim accedir al servidor caldria verificar aquestes dues coses.

Obriu de nou el navegador web des del PC i comproveu que la plana web es carrega correctament com es pot observar en la figura 1.9.

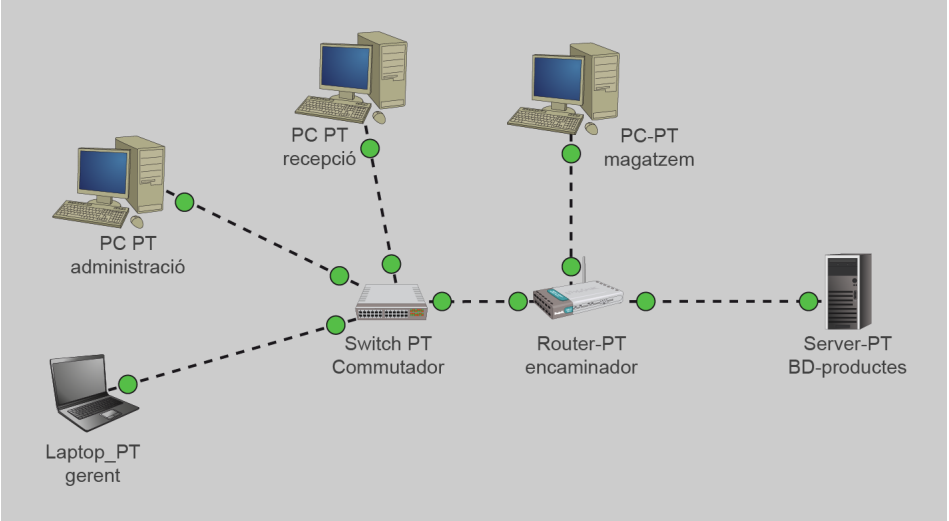
FIGURA 1.9. Servidor web operatiu

Un cop fetes aquestes comprovacions ja podeu informar a l'usuari que pot tornar a fer servir la plana web.

1.3.2 Configuració i diagnòstic dels equips de xarxa

Carregueu el segon laboratori, el *lab2*, en el *packet tracer* i verifiqueu que la topologia és similar a la de la figura 1.10.

FIGURA 1.10. Laboratori cas pràctic 2

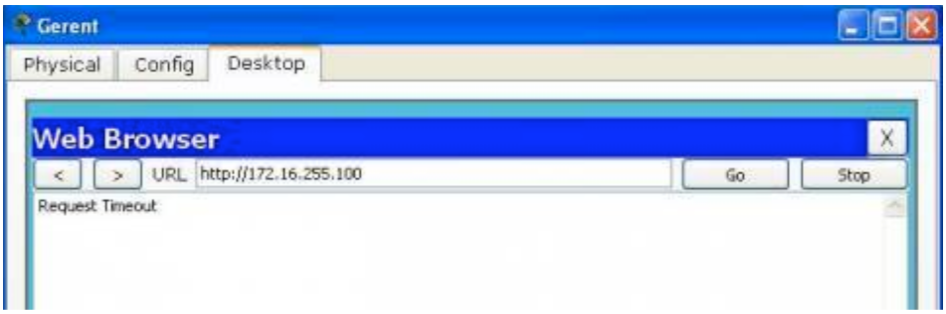


A última hora de la tarda, quan ja sortíeu per la porta de la feina, rebeu una trucada al vostre telèfon mòbil informant-vos que el vostre gerent acaba d'arribar d'una important reunió de negocis i com a conseqüència dels temes tractats vol actualitzar la base de dades de l'empresa però la seva connexió no funciona correctament. És necessari que torneu a l'oficina per solucionar el problema.

El primer que heu de fer és demanar l'ordinador portàtil del gerent per tal de fer les proves pertinents.

Proveu de connectar-vos al servidor web des del portàtil i comproveu si la pàgina web que permet introduir dades en la base de dades es carrega correctament. Hauríeu de veure una cosa similar a la figura 1.11.

FIGURA 1.11. Servidor web no accessible



Efectivament, sembla que no es connecta correctament, ja que rebeu una resposta del navegador web de tipus *request timeout*, sol·licitud de temps d'espera.

Atès que esteu tractant un ordinador una mica crític i no teniu molt clar l'estat actual de la xarxa després dels diversos canvis que s'han fet pel que fa a la topologia i la incorporació de nou personal tècnic, estimeu convenient anar a cercar la documentació sobre l'adreçament IP i els equips implicats.

La taula 1.5 mostra el que teniu documentat.

Taula 1.5. Inventari i connexions dels dispositius

Nom equip	Adreça IP	Màscara de xarxa	Porta d'enllaç	Equip on està connectat	Tipus d'equip
Recepció	192.168.20.10	255.255.255.0	192.168.20.1	Commutador (Fa1/1)	PC escriptori
Administració	192.168.20.11	255.255.255.0	192.168.20.1	Commutador (Fa2/1)	PC escriptori
Gerent	192.168.20.12	255.255.255.0	192.168.20.1	Commutador (Fa3/1)	PC portàtil
Magatzem	192.168.1.5	255.255.255.0	192.168.1.1	Encaminador (Fa1/0)	PC escriptori
BD_Productes	172.16.255.100	255.255.0.0	172.16.255.1	Encaminador (Fa2/0)	Servidor BD
Commutador	-	-	-	Fa0/1 - Encaminador (Fa0/0)	Commutador nivell 2
Encaminador	192.168.20.1 192.168.1.1 172.16.255.1		-	Fa0/0 – Commutador (Fa0/1) Fa1/0 – PC magatzem Fa2/0 – Servidor productes	Encaminador nivell 3-4

Amb la documentació a les nostres mans, apreciem com l'ordinador de recepció, administració i el del gerent comparteixen el mateix adreçament IP, el pertanyent a la xarxa 192.168.20.0/24.

Una bona pràctica és consultar a la gent del mateix departament o àrea que nosaltres sabem que comparteixen el mateix equipament de xarxa, en aquest cas el commutador, si ells també tenen problemes.

La resposta és unànime: a tots ells els funciona correctament la xarxa, i no tenen problemes per connectar-se entre si, però del servidor de productes no saben res, ja que no el fan servir.

Quines altres preguntes considereu adient fer al gerent o a la resta de personal?

Ara, agafeu el portàtil del gerent i proveu de fer *ping* a la porta d'enllaç, la qual, segons la documentació, és la 192.168.20.1.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Tal com podeu veure, els *pings* no han arribat a la seva destinació. Comproveu la configuració de xarxa de l'equip per veure que els valors definits són els que corresponen. Per això, fem servir l'ordre *ipconfig*.

```
PC>ipconfig /all

Physical Address.....: 000C.85D8.7374
IP Address.....: 10.10.5.8
Subnet Mask.....: 255.0.0.0
Default Gateway.....: 10.10.5.1
DNS Servers.....: 0.0.0.0

PC>
```

Són correctes les dades que veieu? Modifiqueu l'adreça IP, la màscara de xarxa i la porta d'enllaç amb les dades que corresponen segons la documentació de la taula 1.5.

Podeu fer servir la mateixa ordre *ipconfig* per canviar aquests valors. Si no sabeu la sintaxi, feu servir el paràmetre **/?**.

```
PC>ipconfig /?
Packet Tracer PC IP Configuration

Usage:
ipconfig { /? | /renew | /release | <IP> <subnet mask>
[<default gateway>] }
```

Ara, definiu els nous valors i comproveu que s'han introduït correctament.

```
PC>ipconfig 192.168.20.12 255.255.255.0 192.168.20.1
PC>ipconfig /all

Physical Address.....: 000C.85D8.7374
IP Address.....: 192.168.20.12
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.20.1
DNS Servers.....: 0.0.0.0
```

A continuació, feu *ping* de nou a la porta d'enllaç per comprovar que la connexió ha estat restablerta.

```
PC>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time=70ms TTL=255
Reply from 192.168.20.1: bytes=32 time=50ms TTL=255
Reply from 192.168.20.1: bytes=32 time=40ms TTL=255
Reply from 192.168.20.1: bytes=32 time=80ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 80ms, Average = 60ms
```

Ara, verifiqueu que també podeu fer *ping* a la resta d'ordinadors de la mateixa xarxa i, finalment, comproveu que el servidor també respon.

```
PC>ping 172.16.255.100

```

```
Pinging 172.16.255.100 with 32 bytes of data:

Reply from 172.16.255.100: bytes=32 time=80ms TTL=127
Reply from 172.16.255.100: bytes=32 time=70ms TTL=127
Reply from 172.16.255.100: bytes=32 time=70ms TTL=127
Reply from 172.16.255.100: bytes=32 time=61ms TTL=127

Ping statistics for 172.16.255.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 80ms, Average = 70ms
```

El servidor ja respon amb l'adreçament IP que correspon a l'ordinador. Proveu una altra vegada que el servidor web mostra la pàgina.

Us heu pogut connectar al servidor web? Torneu a veure el mateix resultat que a la figura 1.11? Quin pot ser el motiu?

Comproveu que el servidor web és accessible des d'un altre ordinador del mateix rang, com per exemple el d'administració, i des de d'un altre d'extern com el del magatzem.

Heu pogut accedir des de l'ordinador d'administració? I des del de magatzem?

Recordeu que tot i que el cablatge i la configuració IP sigui correcta és possible que certs serveis no estiguin disponibles. A quin nivell pertany el servei al qual esteu intentant accedir? En quin nivell es poden establir els filtres que ens permeten o deneguen els accessos a determinats serveis o aplicacions?

Un company vostre us informa que durant els dies que vosaltres heu estat fora de l'oficina per les vacances d'estiu el mateix gerent va ordenar que des dels ordinadors d'administració i recepció no es pogués accedir al servidor però, és clar, no va tenir en compte que això també l'afectaria a ell el dia que volgués accedir al servidor. Així doncs, li comenteu el problema i demana que traieu aquest impediment ràpidament.

Reviseu la documentació i no veieu cap registre del dia que es van habilitar els filtres d'accés. Així doncs, com que no teniu informació pel que fa a això heu d'investigar on estan aquests filtres.

> En un escenari molt gran, això podria portar hores si no està documentat, ja que cada ordinador client o el servidor mateix podria tenir un tallafocs de tipus programari que estigués filtrant el trànsit.

CLI

El CLI és el *command line interface*, el qual és un intèrpret d'ordres que ens permet donar instruccions al dispositiu. És el mecanisme habitual de gestió dels dispositius de xarxa que no disposen de servidor web de gestió.

El mateix company que us ha informat sobre l'activació dels filtres durant les vacances d'estiu us diu que com que la xarxa no disposa de tallafocs dedicat i no hi havia pressupost per a comprar-ne un es va decidir habilitar una llista de control d'accés (ACL) en l'encaminador mateix.

Connecteu-vos a l'encaminador i feu clic damunt de la pestanya on diu *CLI*. Veureu la informació següent:

```
Encaminador con0 is now available

```

```
3
4 Press RETURN to get started.
```

Pressioneu la tecla d'entrar i accedireu a l'intèrpret d'ordres.

A continuació, escriviu l'ordre *enable* i a continuació *show running-config*.

```
1 Encaminador>
2 Encaminador>enable
3 Encaminador#show running-config
```

A continuació, veureu tota la configuració del dispositiu de xarxa; pareu especial atenció a les línies on es defineixen les llistes de control d'accés (ACL).

```
1  Building configuration...
2
3  Current configuration : 852 bytes
4  !
5  version 12.2
6  no service timestamps log datetime msec
7  no service timestamps debug datetime msec
8  no service password-encryption
9  !
10 hostname Encaminador
11 !
12 !
13 !
14 !
15 !
16 !
17 !
18 !
19 !
20 !
21 ip name-server 0.0.0.0
22 !
23 !
24 !
25 !
26 !
27 !
28 interface FastEthernet0/0
29  ip address 192.168.20.1 255.255.255.0
30  ip access-group SERVIDOR-MAGATZEM in
31  duplex auto
32  speed auto
33 !
34 interface FastEthernet1/0
35  ip address 192.168.1.1 255.255.255.0
36  duplex auto
37  speed auto
38 !
39 interface FastEthernet2/0
40  ip address 172.16.255.1 255.255.0.0
41  duplex auto
42  speed auto
43 !
44 interface FastEthernet3/0
45  no ip address
46  duplex auto
47  speed auto
48 !
49 router rip
50 !
51 ip classless
52 !
53 !
```

```
ip access-list extended SERVIDOR-MAGATZEM
 deny tcp 192.168.20.0 0.0.0.255 host 172.16.255.100 eq www
 deny tcp 192.168.20.0 0.0.0.255 host 172.16.255.100 eq 443
 permit ip any any
!
!
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
!
end


Encaminador#
```

La primera ordre carrega en la interfície de xarxa Fa0/0, que és la que dóna connexió als ordinadors connectats al commutador, una llista d'accés que es diu **SERVIDOR-MAGATZEM**, la qual, segons podeu veure en les ordres posteriors, filtra tot el trànsit de tipus web que s'origina a la xarxa 192.168.20.0/24 cap al servidor 172.16.255.100. Tota la resta de trànsit està permès.

Per tant, el que farem per eliminar la llista de control d'accés i poder accedir al servidor web és el següent:

```
Encaminador#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Encaminador(config)#interface fa0/0
Encaminador(config-if)#no ip access-group SERVIDOR-MAGATZEM in
Encaminador(config-if)#exit
Encaminador(config)#no ip access-list extended SERVIDOR-MAGATZEM
Encaminador(config)#exit
Encaminador#
%SYS-5-CONFIG_I: Configured from console by console
Encaminador#write mem
Building configuration...
[OK]
Encaminador#
```

Ara ja hem eliminat la llista de control d'accés; proveu si podeu connectar correctament al servidor web mitjançant el navegador. Hauríeu de veure una cosa similar a la figura 1.12.

FIGURA 1.12. Servidor web operatiu

Ja podeu notificar al gerent que pot accedir correctament al servidor web. Si ell us diu que tot està correcte podreu marxar a casa.

És important que tots els canvis que heu fet, pel que fa a la modificació de configuració de l'encaminador, canvi d'adreçament IP, etc., quedin reflectits en la documentació, ja que potser més endavant torna a passar alguna cosa similar a la d'avui i el tècnic que s'hagi de fer càrrec de la incidència pot fer servir la vostra experiència per mirar de resoldre la incidència amb menys temps i amb més professionalitat.

En aquest cas, la llista de control d'accés estava en l'encaminador, l'únic de la xarxa, però en empreses grans normalment hi ha diversos commutadors, encaminadors, servidors i diversos tallafocs a escala de maquinari i de programari. Si la documentació no preveu de manera acurada la configuració real dels equips, trobar la font del problema pot esdevenir una tasca molt feixuga.

2. Actualització dels dispositius de xarxa

Les xarxes estan formades per multitud de dispositius que ens proporcionen accés a una determinada funcionalitat o servei, i sense la seva existència la xarxa no seria possible. Tots els aparells implicats, des de la targeta de comunicacions (NIC) fins a l'encaminador, passant pels concentradors, commutadors i els cables i connectors mateixos, són necessaris per igual perquè tot el conjunt funcioni i puguem gaudir dels serveis i beneficis que ens ofereix una xarxa de comunicacions.

Quan es parla d'**actualitzar un dispositiu** el que realment es pretén és millorar el servei que ofereix aquell dispositiu en concret. Aquesta millora pot ser que afecti al rendiment del servei, fent que aquest funcioni de manera més estable i més ràpida o que afegeixi noves funcionalitats, les quals no són possibles d'obtenir sense l'actualització.

No tots els dispositius es poden actualitzar; tenim per exemple els cables de xarxa i els connectors: si volem obtenir més velocitat això implicarà probablement canviar-los per uns de nous amb especificacions millors. En el cas que la velocitat sigui suficient però hi hagi deteriorament ocasionat pel pas del temps, el cable o el tros de cable i els connectors afectats per la degradació s'hauran de canviar per uns de nous.

Altres dispositius més complexos, com els encaminadors o tallafocs, estan formats per diversos components de tipus maquinari, ja sigui tot una única peça o un conjunt, que anomenem *modular*. Aquests tipus de dispositiu disposen d'un programari que els gestiona, a mode de sistema operatiu, l'estat del qual és primordial per al seu funcionament correcte. Si les ordres que aquest sistema dóna al maquinari no són del tot correctes o es vol obtenir una nova funcionalitat, serà necessari actualitzar-lo també.

FTTH

La *fiber to the home* (FTTH) és una nova tecnologia de comunicacions de banda ampla que permet donar connectivitat als usuaris directament amb fibra òptica, a diferència de l'ADSL, que ho fa amb els parells de coure del cable telefònic.

L'evolució de les noves tecnologies és constant, la banda ampla ja arriba gairebé a totes les llars i quan ja disposem d'una nova tecnologia n'apareix una altra. El mòdem de 56 kb, XDSI, ADSL i FTTH són alguns exemples de com l'actualització de programari i maquinari és necessària per tal de gaudir d'aquestes noves prestacions.

2.1 Components actualitzables

Hi ha multitud de components que poden ser actualitzats; de fet, la majoria de dispositius són actualitzables, i els que no ho són, simplement es canvien per nous.

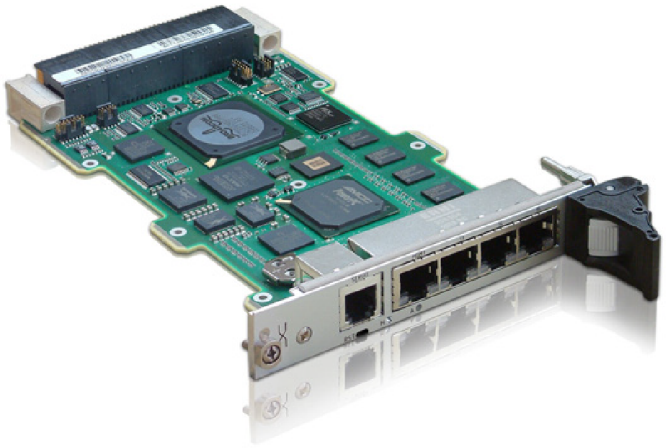
Es pot actualitzar o canviar tant el maquinari que compon un determinat dispositiu com el sistema operatiu que el gestiona. Segons la complexitat del dispositiu i si

aquest requereix poder interpretar ordres rebudes per un tècnic, aquest sistema operatiu pot ser molt complex o més senzill. En molts casos podeu veure com es fa referència a aquest sistema operatiu com a microprogramari.

2.1.1 Actualització de maquinari

Hi ha diversos tipus de dispositius: els no modulars, els quals funcionen com un component únic i que no poden funcionar sense la suma de totes les seves parts, i els equips modulars (figura 2.1), els quals poden fer les mateixes tasques que els no modulars però reparteixen aquestes tasques entre diversos components que poden funcionar de manera independent, cosa que en facilita la manipulació.

FIGURA 2.1. Targeta d'expansió per a equip modular



Els equips modulars permeten actualitzar només aquella part del component que no funciona correctament o que ha quedat obsoleta i requereix una millora, mentre que els no modulars han de ser substituïts totalment.

Els components més habituals que es poden actualitzar en els dispositius de xarxa són les memòries RAM, les memòries ROM, els ports de connexió per afegir nous tipus de cables i connectors com els de fibra òptica o coure, les fonts d'alimentació o els ventiladors.

2.1.2 Dispositius no modulars

Els equips de xarxa han estat tradicionalment components cars, no modulars i que, donada la criticitat del servei que oferien, s'ha preferit no actualitzar-los per no haver d'interrompre el servei o per no haver d'adquirir un nou equip pel cost econòmic i de temps que representava posar-los en funcionament. Els dispositius de xarxa actuals de gamma baixa acostumen a ser d'aquest tipus, ja que la seva fabricació és més senzilla i econòmica i el baix preu del producte no justifica la complexitat de la fabricació en mòduls.

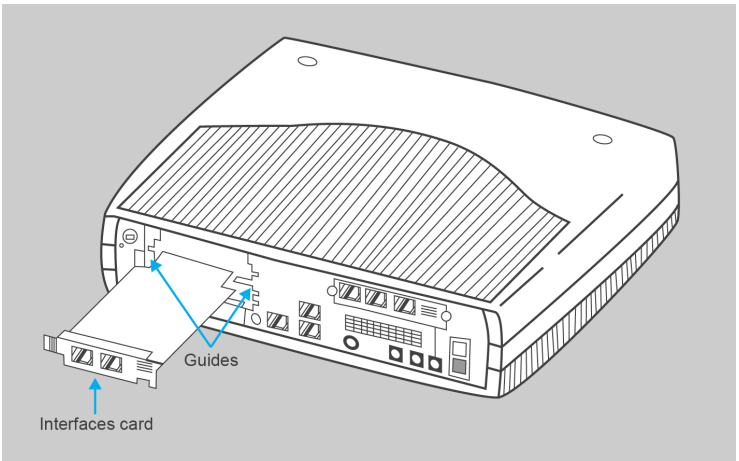
Els encaminadors domèstics d'ADSL són un exemple de dispositius de xarxa no modulars (figura 2.2), ja que tenen un baix cost i una funcionalitat molt concreta.

Figura 2.2. Encaminador de gamma baixa no modular

2.1.3 Dispositius modulars

Un dels avantatges dels equips modulars (figura 2.3) és la disminució del cost d'adquisició del component que s'ha d'actualitzar en lloc d'haver de comprar tot un equip nou sencer.

Figura 2.3. Esquema d'equip modular



Un altre punt a favor d'aquest tipus de dispositius és que normalment, quan s'actualitza un dispositiu que no és modular, aquest s'ha d'aturar o deixar inoperatiu mentre es fa l'actualització, de manera que el servei que ofereix queda interromput fins que l'actualització ha finalitzat. En canvi, en els modulars, atès que sols es canvia un component del dispositiu, només queda interrompuda la part de servei gestionada pel component que s'està actualitzant, i la resta de l'aparell continua funcionant amb normalitat.

Els equips modulars són cars i costen més de fabricar, però en entorns crítics en què no es pot canviar un equip sencer de cop perquè no es poden aturar tots els serveis que depenen de l'equip, comprar-los és fàcilment justificable.

2.1.4 Actualització de programari

Els aparells i dispositius que comprem, com tot aparell tecnològic, passa per un complex procés de disseny, fabricació i testos de comprovacions per tal de garantir que el producte funciona correctament i que és apte per ser venut.

Atesa la complexitat que comporta dissenyar un sistema operatiu que gestiona totes les funcionalitats que els diferents mòduls de maquinari poden oferir, tot sovint els aparells es posen a la venda amb problemes de fabricació que no es van detectar a temps o que es van detectar però que per estratègies comercials es van ignorar amb la intenció de solucionar-los en un futur.

L'actualització de programari permet al fabricant oferir als seus clients solucions i millores en el sistema operatiu dels productes per tal de corregir els problemes detectats o afegir noves funcionalitats.

Tot i que no és tan habitual com en el maquinari, hi ha fabricants que han dissenyat el sistema operatiu del maquinari de manera modular, fet que facilitarà l'actualització del mòdul o funcionalitat afectada per la millora. Aquests tipus de sistemes operatius són més complexos de gestionar, atès que l'actualització es pot fer a cop calent, és a dir, sense aturar la resta de serveis del dispositiu.

Avui dia la majoria de sistemes són encara no modulars, però la tendència és que de mica en mica els nous desenvolupaments es comencin a centrar en l'altre tipus.

2.2 Substitució de components dels dispositius de comunicacions

L'actualització d'un component de programari o maquinari és sempre un procés delicat que requereix una sèrie de comprovacions prèvies. No heu de fer mai una actualització de manera impulsiva, ja que podeu deixar inutilitzat de manera permanent el dispositiu que esteu actualitzant.

Abans d'adquirir un nou component de maquinari per substituir un equip obsolet o que requereix una nova funcionalitat, és imprescindible que avalueu els avantatges i inconvenients del procés d'actualització.

Els avantatges acostumen a estar clars i són precisament aquests els que us motivaran a fer el canvi: millores en les prestacions del producte que afegeixen noves possibilitats de connexió, augmentar la capacitat del maquinari per donar servei a més personal per expansió de l'empresa, solucionar problemes de mal

funcionament que es produeixen per error de maquinari, adquisició i implantació de noves tecnologies, etc.

Finestra de tall

És el temps que s'estima per fer una actuació en un dispositiu que el pot afectar de manera significativa degradant el servei o tallant-lo totalment. És important notificar-ho als usuaris afectats amb la màxima antelació possible.

D'altra banda, els factors en contra també estan presents, entre els quals podem tenir que una actualització defectuosa, un error en la selecció del component per actualitzar o una mala manipulació del dispositiu el poden deixar totalment inoperatiu. A part d'això, quan es fa una actualització el servei que ofereix aquest dispositiu deixa d'estar disponible i s'ha de calcular molt bé la finestra de tall necessària per a l'actuació i notificar-ho amb dies d'antelació als usuaris afectats. No obstant això, a vegades els càlculs no són correctes o apareixen contratemps que fan que les previsions no es puguin complir.

És molt important comprovar amb detall el model exacte del dispositiu que s'ha d'actualitzar; per a això, ens podem ajudar amb el número de sèrie o *part number* del producte, el qual el podem fer servir per cercar en la web del fabricant totes les parts i components actualitzables i les peces compatibles. La figura 2.4 mostra l'etiqueta proporcionada pel fabricant on estan anotats el model exacte i número de sèrie de l'equip.

Figura 2.4. Números de sèrie i de components

Hi ha molts dispositius que tenen la mateixa aparença i *a priori* sembla que més d'un component actualitzable sigui compatible, però això no sempre serà cert, ja que tot i que l'aspecte visual pot coincidir, hi ha d'altres característiques com el voltatge elèctric emprat pel component, l'any de fabricació, el joc de xips que el controla, etc., que els poden fer totalment incompatibles entre si, i una mala elecció de component pot espatllar l'aparell o invalidar la garantia del fabricant.

Una vegada tenim tota la informació necessària, podem procedir a adquirir la nova targeta d'expansió per a l'equip. Segons el tipus de dispositiu i el fabricant, l'adquisició estarà acompanyada d'un servei d'instal·lació oficial, cosa que implicarà que un tècnic certificat es desplaçarà a les vostres instal·lacions per fer ell mateix la instal·lació del nou mòdul o dispositiu.

Altres vegades, aquest servei no estarà inclòs, i haureu de ser vosaltres els que valoreu la contractació d'aquest servei addicional o fer vosaltres mateixos la instal·lació. Heu de tenir sempre clar que, en la majoria dels casos, la garantia

del fabricant quedarà invalidada si es produeix un problema per una manipulació incorrecta. La figura 2.5 mostra un equip modular Cisco de gamma alta.

FIGURA 2.5. Equip modular de gamma alta

2.3 Descripció dels passos que cal seguir en l'actualització de programari de dispositius de comunicació

L'actualització del programari requereix encara més atenció que l'actualització de maquinari. Una mala actualització del programari pot ser nefasta per al funcionament del dispositiu i pot solucionar problemes i provocar-ne d'altres.

De la mateixa manera que amb l'actualització de maquinari, heu de comprovar els números de sèrie, models i característiques completes dels dispositius abans de fer una actualització figura 2.6) i llegir la documentació subministrada amb la nova versió de programari que voleu instal·lar.

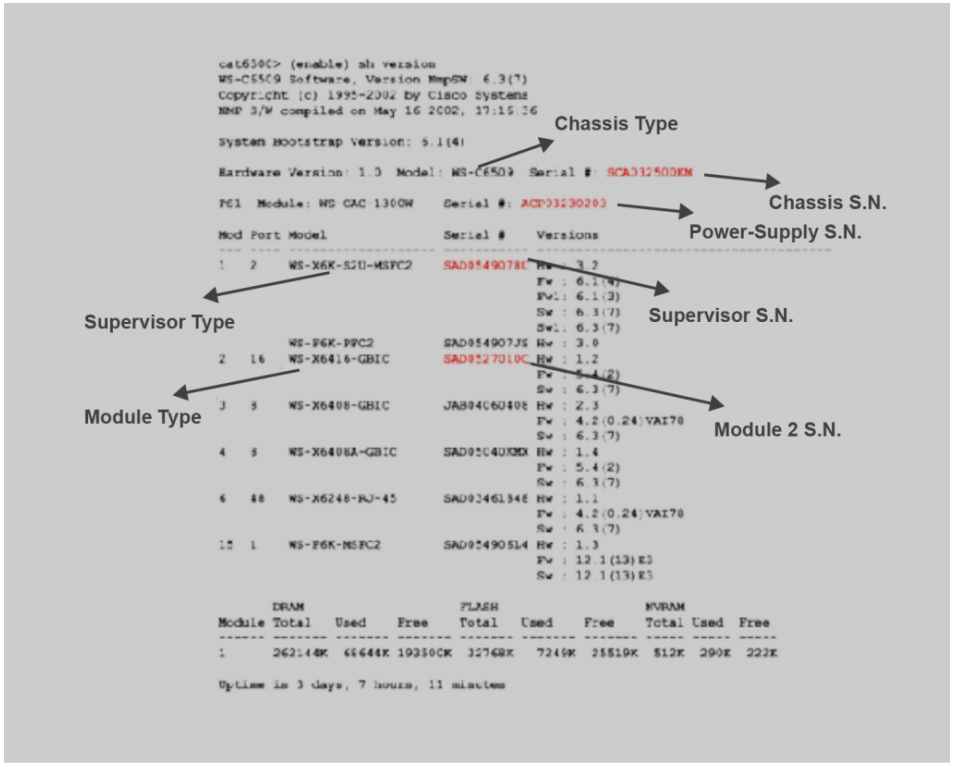
Numeració de les actualitzacions

Els fabricants acostumen a anomenar els fitxers de les actualitzacions amb una simbologia que resumeix les funcionalitats més importants, i també el tipus de maquinari al qual va destinada. És important estar familiaritzat amb la manera de fer del fabricant en qüestió.

Heu de tenir en compte que el programari és el sistema operatiu que controla totes les funcionalitats del maquinari, com si es tractés del cervell. Per tant, si aquest no funciona correctament el maquinari no ho farà.

L'actualització del programari es fa normalment baixant de la pàgina web del fabricant del producte un fitxer, la majoria de vegades comprimit, que conté diversos fitxers amb la documentació de les característiques de la nova versió que us esteu baixant. És a dir, expliquen les millores introduïdes i els defectes i problemes secundaris detectats. També s'inclou en alguns casos un programari que permet fer l'actualització i comprovar si la versió de programari és compatible amb el maquinari en qüestió. No obstant això, aquesta última funcionalitat no sempre estarà disponible i serà responsabilitat vostra comprovar la compatibilitat de les versions.

FIGURA 2.6. Informació del model i versió dels components del dispositiu



Altres fabricants no proporcionen un programa específic per a les actualitzacions, sinó que sols faciliten la nova versió del sistema operatiu, i l'usuari mitjançant un protocol anomenat *TFTP* fa ell mateix l'actualització fent una copia de l'SO actual en el servidor TFTP i baixant posteriorment la nova versió.

Actuació

Es coneix com a actuació qualsevol manipulació programada sobre un dispositiu o servei que pot provocar talls o degradació del servei.

No és senzill establir unes pautes úniques universals per actualitzar el programari dels dispositius, atès que cada fabricant pot fer servir un mètode diferent. No obstant això, podeu fer servir els passos i consells següents per tal d'intentar minimitzar al màxim els problemes que poden aparèixer durant l'actualització i fer que el procés sigui el més fiable possible.

1. Cercar i documentar la marca, model i data de compra del dispositiu.
2. Anotar tots els números de sèrie, *part-numbers*, identificadors i qualsevol altre tipus d'informació que puguin oferir les etiquetes del maquinari.
3. Comprovar nom i versió del sistema operatiu actual del dispositiu.
4. Cercar en el Web o en qualsevol altre canal oficial de comunicació amb el fabricant les noves versions de programari disponibles per al dispositiu. Per fer-ho el fabricant us demanarà la informació recollida en els tres primers punts.
5. Llegir la documentació de les noves versions del programari i cercar aquella que inclou les característiques o millores que necessiteu. Reviseu el significat de la numeració de les actualitzacions.
6. Escolliu la versió que considereu més adient per al vostre cas i baixeu-la.

7. Si podeu, proveu-la primer en un entorn de proves abans de fer-ho en l'equip de producció per tal de provar com respon la nova versió.

8. Feu còpia de seguretat del sistema operatiu actual i de la seva configuració, ja sigui mitjançant el programari subministrat pel fabricant, un servidor de TFTP, *xmodem* o qualsevol altre mètode suportat.

9. Programeu una finestra de tall i aviseu amb antelació als usuaris del dia, l'hora i l'estona en què el servei quedarà degradat o inoperatiu.

10. Un dia abans feu un recordatori als usuaris sobre l'actuació, ja que si el primer avís el vau fer amb molta antelació és possible que ja no ho recordin.

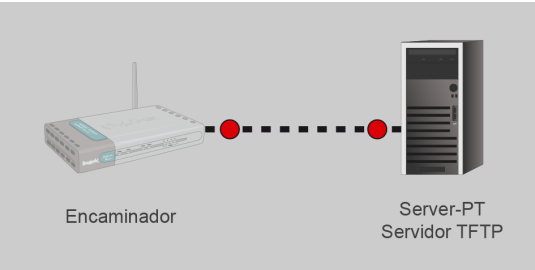
11. Feu l'actualització i verifiqueu que el sistema funciona adequadament. No podreu verificar el cent per cent de les funcionalitats noves però com a mínim les més critiques per garantir que el servei ha quedat restablert.

12. Quan creieu que l'actualització es pot donar per finalitzada notifiqueu als usuaris que ha acabat i comenteu si el procés ha resultat satisfactori i dins de la finestra de tall prevista o si, al contrari, hi ha hagut problemes i heu hagut de fer marxa enrere (per això és important fer còpia de seguretat del sistema operatiu actual).

2.4 Cas pràctic: exemple d'actualització de programari

Carregueu el laboratori *lab3* del *packet tracer* i verifiqueu que veieu un escenari similar al de la figura 2.7.

FIGURA 2.7. Diagrama de xarxa del cas pràctic del laboratori 3



Cisco IOS

IOS és el nom del sistema operatiu que fan servir la majoria de dispositius del fabricant Cisco. L'altre sistema operatiu, més antic que l'IOS, que s'utilitza, és el CatOS. Altres fabricants com Juniper fan servir el JunOS.

Esteu configurant un equip de xarxa, un encaminador de la sèrie 1841 de Cisco que, segons us diuen, té una IOS molt bàsica i que, per tal d'aprofitar l'equip de xarxa en un entorn més complex, requereix una versió de sistema operatiu més avançada. Us demanen que procediu a fer l'actualització a la IOS corresponent i que comproveu que arrenca correctament.

Per fer aquesta actualització, us han facilitat un servidor de TFTP el qual ja conté un repositori de versions. Aquest servidor té l'adreça IP 192.168.1.100 i la màscara de xarxa 255.255.255.0.

El primer que heu de fer és connectar el servidor de TFTP amb l'encaminador fent servir qualsevol dels ports de coure de tipus Fast Ethernet disponibles. Agafeu per exemple el Fa0/0.

Quin tipus de cable heu de fer servir per connectar el servidor amb l'encaminador?

Una vegada connectat amb el cable corresponent, configureu la interfície Fa0/0 amb una adreça IP del mateix rang IP que el servidor de TFTP, per exemple la 192.168.1.1. Per fer-ho en mode d'ordres, entreu dins l'encaminador a la pestanya CLI i premeu la tecla d'entrar per tal de començar a introduir les ordres.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
Router(config)#exit
Router#
```

Proveu a fer *ping* des de l'encaminador al servidor de TFTP i verifiqueu que hi ha resposta.

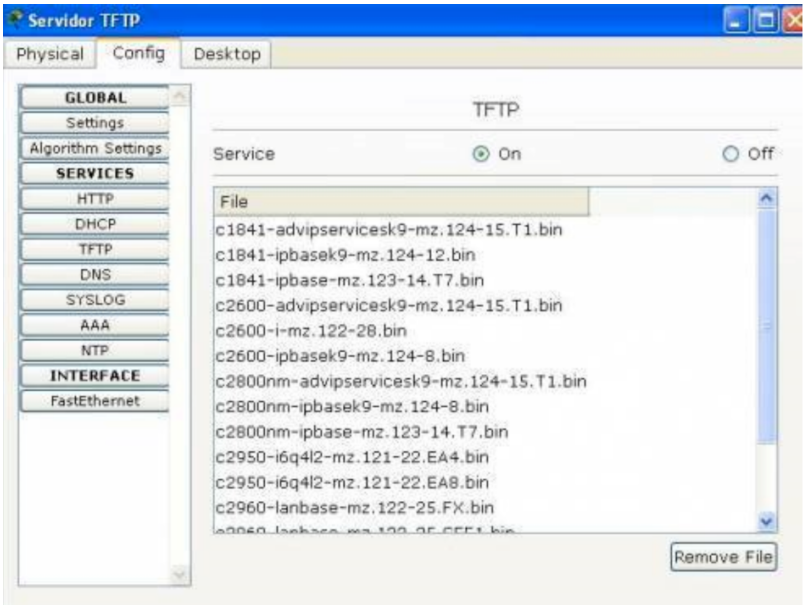
```
Router#ping 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/40 ms

Router#
```

Ara, el servidor de TFTP és accessible; comproveu que el servei de TFTP està activat. Per fer-ho accediu a: *Config*> *Services*> *TFTP* i verifiqueu que l'opció *Service* està en *On*, tal com es veu a la figura 2.8.

Figura 2.8. Versions del sistema operatiu disponibles al servidor TFTP



Veureu que el servidor de TFTP té tot un seguit de fitxers; cadascun es correspon a una versió d'IOS específica per a un model concret d'equip i unes característiques determinades.

El model d'encaminador vostre és un 1841, tal com us han dit, però és important que ho verifiqueu vosaltres mateixos. Aprofiteu que verifiqueu el model exacte i determineu la versió actual d'IOS que està fent servir. Per fer-ho, feu servir l'ordre *show versions* i fixeu-vos en el resultat.

```
1  Router#show version
2  Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7, RELEASE
       SOFTWARE (fc2)
3  Technical Support: http://www.cisco.com/techsupport
4  Copyright (c) 1986-2006 by Cisco Systems, Inc.
5  Compiled Mon 15-May-06 14:54 by pt_team
6
7  ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
8
9  System returned to ROM by power-on
10 System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
```

La primera línia us indica que es tracta del programari de gestió per a un equip de la sèrie 1841.

La línia 10 us indica que la versió actual del sistema operatiu que s'està fent servir és la *c1841-ipbase-mz.123-14.T7.bin*.

Ara, comproveu quines versions del nou sistema operatiu que estan disponibles al servidor de TFTP són compatibles. Quines són? Què passaria si no escolliu una imatge compatible?

De totes les imatges, escollireu la *c1841-advipservicesk9-mz.124-15.T1.bin*, i serà aquesta la que carregareu en l'encaminador. Per a fer-ho, utilitzeu les ordres següents:

```
1  Router#copy tftp: flash:
2  Address or name of remote host []? 192.168.1.100
3  Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
4  Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?
5  Accessing tftp://192.168.1.100/c1841-advipservicesk9-mz.124-15.T1.bin...
6  Loading c1841-advipservicesk9-mz.124-15.T1.bin from 192.168.1.100:
7  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
8  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
9  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
10 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
11 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
12 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
13 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
14 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
15 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
16 !!!!!!!!!!!!!!!!!!
17 [OK - 33591768 bytes]
18
19 33591768 bytes copied in 15.553 secs (226772 bytes/sec)
20 Router#
```

A la pregunta de *Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?* heu de prémer entrar per tal d'acceptar el nom de la imatge.

A continuació, verifiqueu que la imatge s'ha copiat correctament i que està disponible.

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

    6  -rw-    33591768          <no date>  c1841-advipservicesk9-mz.124-15.T1.
       bin
    5  -rw-    13832032          <no date>  c1841-ipbase-mz.123-14.T7.bin
```

Veureu que apareixen les dues imatges, l'actual i la nova. Ara indiqueu a l'encaminador que voleu fer servir la nova. Feu servir l'ordre *boot*, reinicieu l'equip amb *reload* i premeu entrar quan us demani la confirmació.

```
Router(config)#boot system flash c1841-advipservicesk9-mz.124-15.T1.bin
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#reload
Proceed with reload? [confirm]
```

Una vegada hagi arrencat veureu el següent:

```
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
63488K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1
    ,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!
```

A continuació, torneu a executar l'ordre *show version* i comproveu que la nova imatge s'ha carregat correctament.

```
Router>en
Router#sh ver
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1
    ,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is //flash:c1841-advipservicesk9-mz.124-15.T1.bin//
```

Si és així, ja podeu començar a fer servir la nova versió del sistema operatiu.