Administració de la xarxa

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190189

UOC
Universitat Oberta de Catalunya

Índex

Introducció

A l'hora de dissenyar i implementar una xarxa hem de tenir en compte els sis passos bàsics següents:

1) Selecció del disseny del cablatge i del maquinari.

2) Instal·lació del maquinari i del sistema operatiu de xarxa.

3) Configuració del sistema operatiu i càrrega de les aplicacions.

4) Creació de l'entorn d'usuari.

5) Inicialització de l'administració de la xarxa.

6) Manteniment i monitorització de l'activitat de la xarxa.

Vegeu també

Vegeu el mòdul "Administració d'usuaris".

En aquest mòdul pretenem abastar breument diversos aspectes del disseny i el desenvolupament posterior d'una xarxa d'ordinadors. Així, doncs, comencem el mòdul amb la descripció dels elements que la integren, i l'acabarem definint les responsabilitats de l'administrador i del departament d'informàtica envers el funcionament correcte de la xarxa. No pretenem fer un recull exhaustiu d'una matèria tan densa i heterogènia, sinó tan sols dotar l'administrador d'alguns criteris generals que el puguin ajudar a l'hora de començar (i mantenir) una tasca tan complexa com la que hem descrit.

Objectius

Els materials didàctics d'aquest mòdul contenen les eines necessàries perquè l'estudiant assoleixi els objectius següents:

1. Conèixer bàsicament els elements físics d'una xarxa d'ordinadors i la manera com podem interconnectar aquests elements entre si.

2. Conèixer els protocols de comunicació que han d'utilitzar els ordinadors de la xarxa, i també la manera com es configuren les estacions i alguns serveis.

3. Conèixer les tasques que ha de dur a terme l'administrador una vegada la xarxa ja es trobi en funcionament (tasques de manteniment, supervisió i seguretat).

1. Importància de les xarxes

Els ordinadors personals permeten als usuaris individuals de gestionar les seves pròpies dades per a cobrir les necessitats particulars. Malgrat tot, els ordinadors aïllats no poden oferir un accés directe a les diferents dades d'una organització, ni poden compartir d'una manera fàcil la informació o els programes de què disposen. En aquest sentit, les xarxes proporcionen una bona solució de compromís entre els dos extrems: el processament individual i el processament centralitzat.

Entre els molts beneficis que comporta la implementació d'una xarxa podem trobar els següents:

- Compartició de dispositius perifèrics: discos durs de gran capacitat, dispositius de sortida de cost elevat (com, per exemple, impressores làser o traçadors –*plotters*–, etc.).
- Comunicació dels usuaris de l'organització entre ells (correu electrònic).
- Facilitat de manteniment del programari (sovint bona part del programari es comparteix des de la xarxa, en lloc d'instal·lar-se individualment en cada estació de treball).
- Gestió centralitzada dels recursos compartits, independentment del grau de dispersió geogràfica que pugui tenir l'organització.

Tenint en compte aquesta dispersió, les xarxes es poden classificar de la manera següent:

- Xarxes d'àrea local (LAN[1]): de 10 a 1.000 m (per exemple, una sala de l'organització, un campus, etc.).
- Xarxes d'àrea metropolitana (MAN[2]): d'1 a 10 km (per exemple, una ciutat).
- Xarxa d'àrea estesa (WAN[3]): més de 10 km (per exemple, un país).

(1)LAN és la sigla de *local area network*.

(2)MAN és la sigla de *metropolitan area network*.

(3)WAN és la sigla de *wide area network*.

Tenint en compte la importància que té una xarxa en l'activitat diària de qualsevol organització, es fa evident la necessitat d'una figura que s'encarregui de dissenyar-la, implementar-la, mantenir-la i actualitzar-la sempre que es requereixi. Aquesta figura, l'administrador de la xarxa, ha de conèixer els elements

físics que la componen, els protocols de comunicació entre els diferents ordinadors (i els seus sistemes operatius), i també els requeriments mínims de seguretat que ha de satisfer la xarxa.

2. Elements i disseny físic d'una xarxa

A l'hora de dissenyar la nostra pròpia xarxa cal que, abans de començar, tinguem en compte una sèrie d'aspectes bàsics que podem veure reflectits tot seguit en les preguntes següents:

- Quants ordinadors (estacions de treball) hem de connectar a la xarxa?
- Quants ordinadors caldrà afegir en futures ampliacions?
- On i com es disposen els ordinadors? (cal fer un croquis de la disposició de les màquines).
- Necessitem un servidor?
- Quina velocitat de transmissió es requereix?
- Quins recursos cal compartir?
- Quin programari voldríem instal·lar? En tenim les versions per a funcionar sobre xarxa?

Abans de començar a contestar aquestes preguntes, ens caldrà fer un breu repàs de diversos conceptes que han aparegut en altres assignatures de xarxes d'ordinadors.

2.1. Elements d'una xarxa

Els elements bàsics d'una xarxa són el cablejat, els elements de connexió i els elements d'interconnexió de xarxes.

2.1.1. Cablejat d'una xarxa

Podem distingir els següents tipus de cables:

1) Parell trenat

Aquest tipus de cablejat està format per diversos fils conductors que es trenen entre si amb la finalitat de protegir-los del soroll ambiental. És el cablejat més econòmic i fàcil d'instal·lar. Poden arribar a distàncies de fins a 100 m (sense patir esmorteïments del senyal) i a velocitats que poden variar entre els 10 i els 100 Mbps. Hi ha diverses categories de cable parell trenat:

- Cable apantallat[4]. Format per dos parells de fils conductors recoberts per una malla.

- Cable sense apantallar[5]. Format per quatre parells de fils conductors. Al mateix temps, els cables UTP es poden subdividir en diverses categories:
  – Categoria 3: poden arribar a velocitats de transmissió de 30 Mbps.

(4)En anglès, *shielded twisted pair* (STP).

(5)En anglès, *unshielded twisted pair* (UTP).

– Categoria 5: és el tipus de cable que s'utilitza més sovint. Pot arribar a velocitats de 100 Mbps (xarxes fast ethernet). La categoria 5a (també anomenada 5+ o 5e) representa una millora de la categoria 5 i pot arribar fins a 1.000 Mbps (xarxes gigabit ethernet).
– Categoria 6: pot arribar a velocitats de 1.000 Mbps/16 bps.

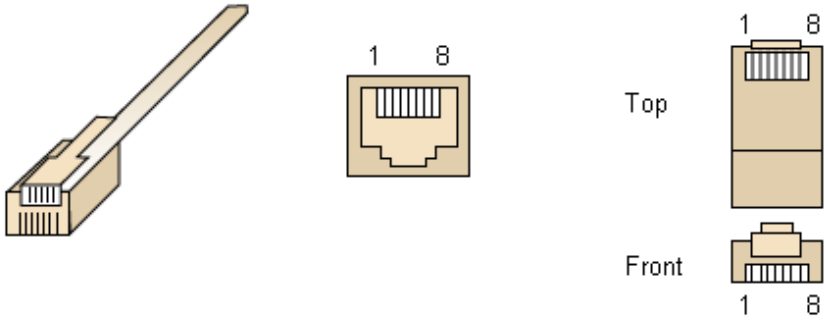
Altres categories de cables UTP

A banda de les categories 3, 5 i 6 hi ha altres categories de cables UTP: les categories 6 i 7, que s'usaran en el futur per a xarxes 10 gigabit ethernet (10.000 Mbps).

Podem veure en la figura següent l'aspecte d'un parell trenat UTP[6], el connector femella i el connector mascle, respectivament:

(6)UTP és la sigla d'*unshielded twisted pair*.

Aspecte d'un cable UTP



Per exemple, connectant tots els ordinadors a un concentrador mitjançant un parell trenat i sense necessitat d'utilitzar un servidor dedicat, podem dissenyar una xarxa molt senzilla, perfectament vàlida per a compartir recursos i que es pot ampliar fàcilment fins a ocupar tots els ports del concentrador.

Xarxes punt a punt

S'anomenen *punt a punt* (en anglès, *peer-to-peer*) les xarxes en les quals no hi ha un servidor dedicat. Totes les estacions de treball tenen el mateix estatus i comparteixen els recursos.

Crossover

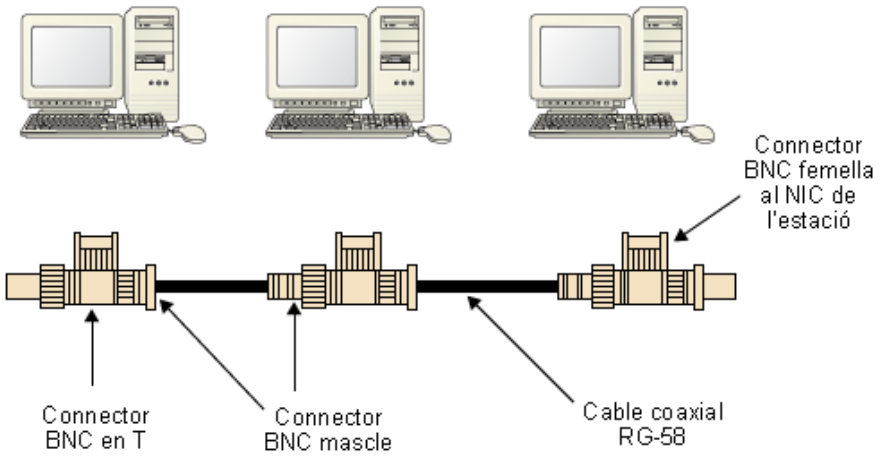
Quan s'utilitza un concentrador, els dos extrems del cable (el que es connecta al concentrador i el que es connecta a la targeta de xarxa de l'ordinador) s'insereixen en el connector RJ45 de la mateixa manera, però quan els dos extrems es connecten directament entre dos ordinadors, cal fer el que s'anomena un cable creuat (*crossover*) i intercanviar l'ordre dels cables que transmeten les dades.

2) Cable coaxial

El cable coaxial disposa d'un únic conductor intern i diverses capes de protecció. N'hi ha de gruixut i de prim (RG-58A/U), i en distàncies no superiors als 2 km pot permetre velocitats de transmissió de 20 Mbps, mentre que en distàncies curtes (no superiors als 100 m) pot arribar als 100 Mbps. El cable coaxial, si es compara amb el parell trenat, redueix els problemes d'esmorteïment del senyal a llargues distàncies i el percentatge de potència que es perd en forma de radiació. És molt sensible a les accions de possibles espies i susceptible al soroll produït pels aparells elèctrics (per exemple, un motor).

Per a connectar diferents segments de cable coaxial s'utilitzen connectors BNC. Per a connectar un ordinador a la xarxa s'utilitzen connectors BNC en forma de T.

Connexió d'un ordinador a la xarxa amb cable coaxial



3) Fibra òptica

La transmissió de la informació es duu a terme per un feix de llum que circula per un nucli fotoconductor. Permet una gran amplada de banda i pot arribar a velocitats de transmissió de l'ordre de centenars de Mbps i Gbps i tot. La fibra òptica pateix un esmorteïment mínim del senyal, és immune a les interferències electromagnètiques i resulta difícil d'interceptar i espiar, ja que no emet cap senyal que pugui ser monitoritzat. Normalment s'utilitza conjuntament amb altres tipus de cablejat.

Hi ha dos tipus diferents de fibra òptica, les **fibres monomode** i les **fibres multimode**. Les primeres es caracteritzen perquè només admeten un únic mode de transport (només poden transmetre els feixos de llum que segueixen l'eix de la fibra). Tenen una amplada de banda que pot arribar als 100 GHz/km. Pel que fa a les fibres multimode, amb un diàmetre de nucli més gran que les monomode, transporten múltiples modes de forma simultània. Són més fàcils d'implantar i tenen una amplada de banda que pot arribar fins als 500 MHz/km (menor que les monomode). Poden ser, per exemple, especialment adequades per sistemes de videovigilància o LAN[7].

[7]LAN és l'abreviatura de *xarxa d'àrea local*.

Vegeu també

Vegeu els sistemes de videovigilància o LAN en el mòdul "Administració de la seguretat".

2.1.2. Elements de connexió de xarxes

Entre els elements de connexió de xarxes podem distingir les següents:

- **Targetes d'interfície de xarxa (NIC[8])**. La connexió dels ordinadors a la xarxa es fa mitjançant les targetes d'interfície de xarxa.

[8]NIC és la sigla de *network interface card*.

Targeta d'interfície de xarxa

- **Tallafoc**[9]. És qualsevol dispositiu (maquinari o programari) que permeti d'evitar que els usuaris no autoritzats accedeixin a una màquina determinada.

(9)En anglès, *firewall*.

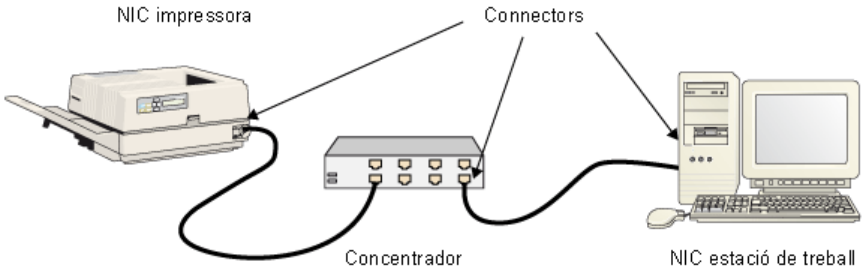
Vegeu també

Vegeu els tallafocs en l'apartat 5 d'aquest mateix mòdul.

- **Concentrador**[10]. Els concentradors són dispositius que permeten de compartir una línia de comunicació entre diversos ordinadors. Repeteixen tota la informació que reben de manera que la puguin rebre tots els dispositius connectats als seus ports.

(10)En anglès, *hub*.

Exemple de configuració d'un concentrador



- **Commutador**[11]. Gestiona el flux del trànsit de xarxa segons l'adreça de destinació de cada paquet. En altres paraules, els commutadors poden esbrinar quins dispositius es troben connectats als seus ports i redirigeixen la informació únicament al port destinació, en lloc de fer-ho indiscriminadament com els concentradors.

(11)En anglès, *switch*.

Observació

Totes les estacions connectades al mateix concentrador o *stack* de concentradors competeixen per l'amplada de banda del canal.

- **Xarxa troncal**[12]. S'anomenen d'aquesta manera els cables principals que connecten entre si els segments d'una xarxa local. Habitualment són enllaços d'alta velocitat (per exemple, fibra òptica).

(12)En anglès, *backbone*.

- **Armaris de connexió**. Generalment la xarxa es divideix en diferents armaris de connexió que abasten tot el servei de xarxa en un entorn deter-

minat com, per exemple, tota la planta d'un edifici. Tots aquests armaris tenen una connexió a un armari central en el qual, normalment, es troben agrupades totes les comunicacions i resideixen els diferents servidors. Acostuma a ser una sala amb condicionament atmosfèric adequat, tant pel que fa a la temperatura com a la humitat, i normalment disposa d'alimentació elèctrica ininterrompuda.

- **Servidor**. És l'ordinador que permet de compartir els seus perifèrics amb altres estacions de la xarxa. N'hi ha de molts tipus i es poden agrupar en tres categories generals: servidors d'impressió, de comunicacions i de fitxers. Dins d'una xarxa, poden estar dedicats exclusivament a donar aquests serveis, o bé també poden no ser exclusius i utilitzar-se com a estacions de treball.

- **Estació de treball**. Cada estació de treball executa el seu sistema operatiu propi (Unix, Linux, Windows 2000, etc.) i sobre aquest sistema operatiu s'executa un programari de xarxa, que li permet de comunicar-se amb els servidors i els altres dispositius de la xarxa, de manera que sigui tan senzill gestionar els recursos locals com els del servidor.

2.1.3. Elements d'interconnexió de xarxes

Entre els elements d'interconnexió de xarxes podem distingir les següents:

- **Repetidors**. Són dispositius "no intel·ligents" que amplifiquen el senyal i eviten els problemes d'esmorteïment que es produeixen quan el cable arriba a una certa distància (recordeu que, segons el cablatge que es faci servir, aquestes distàncies varien).

- **Pont**[13]. Connecten entre si dos segments de xarxa (que poden ser diferents, com es mostra a l'exemple de la figura següent). A diferència del repetidor, el pont és prou "intel·ligent" per a filtrar el trànsit d'informació entre els segments. Amb la incorporació d'un pont, cada segment té una adreça diferent, de manera que la informació sempre es direcciona envers la seva destinació i s'eviten els colls d'ampolla que es produeixen quan totes les estacions de treball es connecten en el mateix segment.

Observació

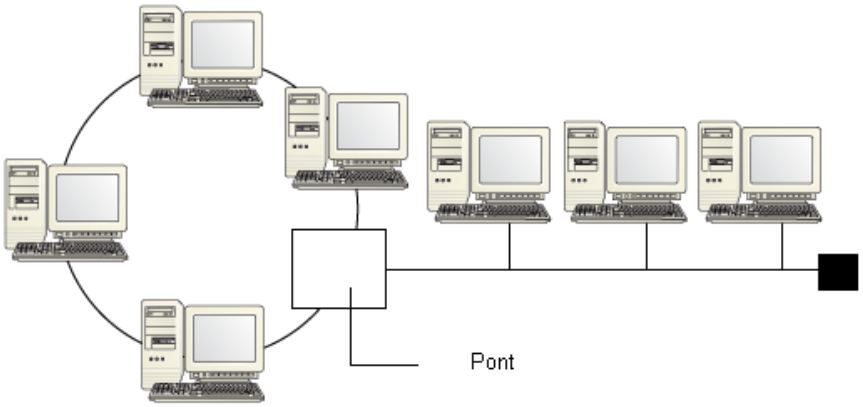
Els repetidors actuen en la capa física i els ponts actuen en la capa d'enllaç de dades. L'encaminador actua en la capa de xarxa.

(13)En anglès, *bridge*.

Funcions dels ponts

Les funcions bàsiques dels ponts són l'autoaprenentatge, la filtració i el reenviament.

Interconnexió de xarxes mitjançant un pont



- **Encaminador**[14]. Són dispositius que gestionen el trànsit de paquets que prové de l'exterior de la xarxa cap a l'interior (i a l'inrevés). Poden ser dispositius molt sofisticats i tenir capacitat d'actuar com a tallafoc. Són similars als ponts, però en canvi ofereixen serveis d'encaminament de les dades que es transmeten; és a dir, no solament poden filtrar la informació, sinó que, a més, també poden trobar la ruta de destinació més eficient per als paquets d'informació que es transmeten.

(14)En anglès, *router*.

- **Passarel·la**[15]. Actuen en els nivells superiors de la jerarquia de protocols OSI. Permeten la interconnexió de xarxes que fan servir protocols incompatibles.

(15)En anglès, *gateway*.

2.2. Topologia i tipus de xarxes

La topologia de la xarxa es refereix al camí físic que segueixen les dades per la xarxa, la manera lògica com es connecten els diferents dispositius que la formen. Sovint, cal diferenciar entre la **topologia lògica** i la **topografia** o **disseny físic** (la manera com es "tiren" els cables).

Reflexió

La topologia lògica pot ser, doncs, diferent de la topografia, com veurem en els exemples que s'estudiaran més endavant.

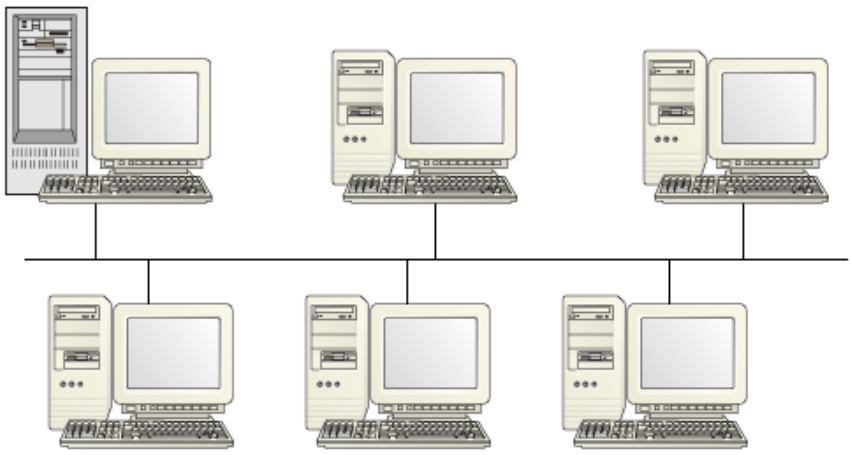
Bàsicament hi ha tres topologies que cal tenir en compte en una LAN:

- **Topologia de bus**: en una xarxa en bus, tots els nodes (els servidors i les estacions de treball) es connecten a un cable comú (bus). Els trets més característics d'aquesta topologia són els següents:
  - Els nodes no retransmeten ni amplifiquen la informació.
  - El temps de retenció de la informació en els nodes és nul.
  - Tots els missatges arriben a tots els nodes.
  - No és necessari cap encaminament de la informació.
  - La fiabilitat de la comunicació depèn únicament del bus (punt crític).
  - La configuració és flexible i modular.
  - És una tecnologia de baix cost que encara es fa servir freqüentment.

– Ofereix facilitat per a interceptar la informació circulant.

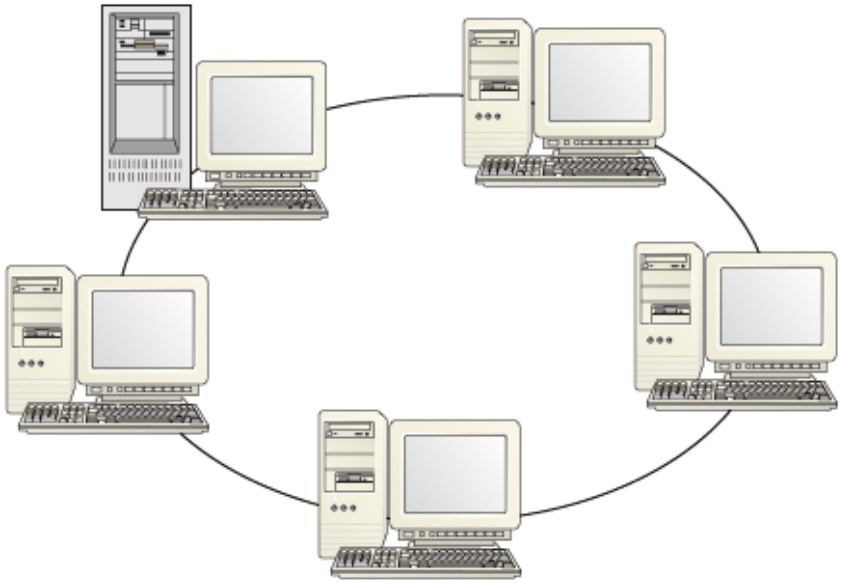
L'existència d'un únic bus fa que l'excés de trànsit pugui provocar una disminució important del rendiment de la xarxa. Per a controlar el trànsit de la xarxa es poden fer servir commutadors que siguin capaços de discriminar el trànsit circulant.

Xarxa amb topologia de bus



- **Topologia en anell**: en una xarxa en anell el cable va d'estació a estació (i al servidor) sense cap punt final. Cada node té connexions amb dues estacions més. Els trets més característics d'aquesta topologia són els següents:
  – Cada node amplifica i repeteix la informació que rep.
  – Els missatges viatgen per l'anell node a node, de manera que totes les informacions passen per tots els mòduls de comunicació de les estacions (facilitat per a interceptar la informació).
  – No cal dirigir l'encaminament de la informació.
  – La fiabilitat de l'anell depèn de cadascun dels nodes i de la via de comunicació que forma l'anell. La caiguda d'una sola estació podria provocar que la xarxa sencera deixés de funcionar.

Xarxa amb topologia d'anell

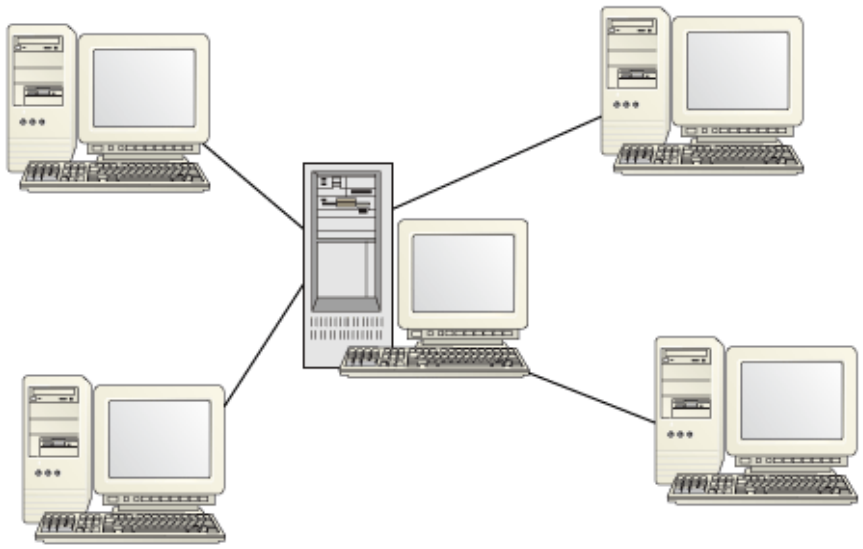


- **Topologia en estrella**: en aquest cas, totes les estacions de treball i el servidor es connecten a un sol concentrador o commutador. Observem que l'element diferenciador més important respecte a les altres topologies és la centralització de les connexions. Aquest fet la converteix en una topologia especialment resistent a la caiguda de les estacions de treball, tot i que com a principal defecte ens ofereix un punt crític, l'element central, el qual si és atacat, o cau per qualsevol motiu, pot provocar la caiguda de la xarxa sencera. Els trets més característics d'aquesta topologia són els següents:
  - Totes les estacions es comuniquen entre si mitjançant un node central.
  - El dispositiu central pot ser actiu o passiu.
  - Les fallades tenen una repercussió molt diferent segons on es produeixen.

Canvis en el disseny

Quan s'han d'afegir concentradors per a donar servei a més usuaris, s'ha de plantejar un possible canvi en el disseny, ja que encadenar commutadors entre si és molt còmode, però pot crear problemes de trànsit i, en certs casos, confusió.

Xarxa amb topologia d'estrella



A l'hora de triar una topologia de xarxa s'han de tenir en compte els aspectes següents:

- Distància màxima que es pot obtenir.
- Nombre màxim d'estacions.
- Flexibilitat a l'hora d'afegir o eliminar estacions de treball.
- Tolerància a caigudes de les estacions.
- Retard dels missatges.
- Cost.
- Flux d'informació que pot circular per la xarxa.

Documentar ajuda

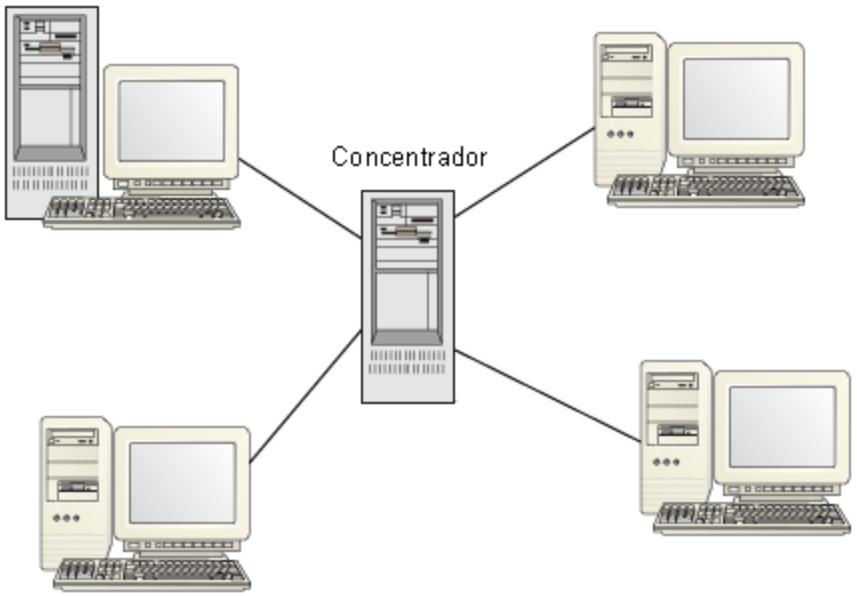
"Documentar" el disseny i els components que formen part de la xarxa ajuda en les futures tasques de manteniment.

Les topologies de bus i d'anell són les més utilitzades en xarxes locals, tot i que per motius de flexibilitat, fiabilitat i seguretat, el disseny físic en estrella també ha esdevingut molt popular amb xarxes que, lògicament, poden funcionar en bus o anell, però que tenen una topologia física d'estrella.

Observació

Encara que físicament no es deixin connectats, és aconsellable tenir els cables tirats pels canals amb un 10% més del que es preveu fer servir.

Disseny físic basat en concentradors



Observem que en el concentrador es barregen tots els senyals de totes les estacions i es transmeten a totes com si es tractés d'una configuració en bus.

2.3. Tipus de xarxes locals

L'Institute of Electrical and Electronic Engineers (IEEE) és un organisme que data de l'any 1980 i que va elaborar les normes IEEE 802.X.

Les normes IEEE 802.x defineixen els estàndards pel que fa al funcionament de les xarxes d'àrea local:

- **IEEE 802.3**. Estàndard basat en la versió 2.0 de la xarxa ***Ethernet***. Defineix una xarxa amb topologia de bus i mètode d'accés CSMA/CD (totes les estacions poden accedir simultàniament al medi i competeixen per la utilització del canal de comunicació). El seu camp d'aplicació es troba en entorns tècnics i oficines, universitats i hospitals.

- **IEEE 802.4**. Defineix una xarxa amb topologia de bus i pas de testimoni (tan sols pot accedir a la utilització del canal l'estació en possessió del testimoni). S'utilitza en entorns industrials i es coneix amb el nom de ***Token-bus***.

- **IEEE 802.5**. Estàndard basat en la xarxa ***Token-ring*** d'IBM. Defineix una xarxa amb topologia d'anell i pas de testimoni. Ha esdevingut popular en entorns d'oficines, amb un nivell d'implantació similar a les **xarxes *Ethernet***.

De tots els estàndards que acabem d'esmentar, possiblement les xarxes *Ethernet* són les que han tingut més popularitat.

La major part de les implementacions de xarxes Ethernet tenen velocitats de transmissió de 10 Mbps i es detallen a continuació segons el cablejat que s'utilitzi:

- **1Base-5**: cable de parell trenat amb una velocitat de transmissió d'1 Mbps i una longitud màxima de segment de cinc-cents metres.
- **10Base-T**: cable de parell trenat UTP amb una longitud màxima de segment de cent metres sobre una topologia física d'estrella.
- **100Base-T**: semblant a l'anterior, però amb velocitats de transmissió de 100 Mbps (anomenada també *fast Ethernet*).
- **10Base-5 (*thick wire*)**: cable coaxial gruixut amb una velocitat de transmissió de 10 Mbps. Accepta fins a cent llocs de treball en segments de longitud de com a molt cinc-cents metres.
- **10Base-2 (*thin wire*)**: cable coaxial prim amb una velocitat de transmissió de 10 Mbps. Accepta fins a trenta llocs de treball en segments de longitud de com a molt cent vuitanta-cinc metres.
- **10Base-F**: fibra òptica amb velocitats de transmissió de 10 Mbps.

Canvis tecnològics

Si s'ha de fer un canvi tecnològic important (per exemple, passar d'Ethernet de 10 Mb a 100 Mb o 1 Gb), s'hauria d'analitzar si és millor fer-ho d'una manera gradual o bé canviar de cop i interrompre tots els serveis durant el temps que faci falta.

Observació

A cada implementació de xarxa Ethernet (1Base-5, etc.), el primer nombre fa referència a la velocitat en Mbps i el segon als metres que pot tenir el segment –multiplicat per cent, sense que el senyal pateixi esmorteïments.

2.3.1. Xarxes locals sense fil

A l'hora de triar un tipus de xarxa també val la pena considerar altres opcions diferents dels tipus que hem estudiat fins ara. Per exemple, en tots els tipus examinats hem pogut copsar els problemes següents:

- Dificultat, o impossibilitat i tot, per a fer arribar el cablejat quan el lloc és físicament de difícil accés.
- Necessitat de fer una estimació de creixement de la xarxa i desenvolupar més infraestructura de la que es necessita en un principi per a poder preveure aquest creixement en el futur.
- En tots els casos cal foradar les parets o el terra per a tirar el cablejat necessari.

Per a poder resoldre aquest tipus de problemes han aparegut les anomenades xarxes locals sense fil[16], és a dir, xarxes basades en ones de ràdio o infraroges. L'objectiu primordial en aquestes xarxes és la comoditat de l'usuari final (o sigui, la possibilitat de connectar-se a la xarxa des de qualsevol lloc de l'organització i en qualsevol moment) i la facilitat d'implementació i creixement de la xarxa (sense oblidar que aspectes com la fiabilitat i l'amplada de banda també són importants).

(16)En anglès, *wireless local area network* (WLAN).

L'IEEE[17] ha definit la norma 802.11 (i posteriors) per a regular el funcionament de les xarxes sense fil. La més estesa és la norma 802.11g, amb velocitats de fins a 50 Mbps. Emet dins la banda de 2.4 GHz ISM (*industrial, scientific and medical*).

(17)IEEE són les sigles de l'Institute of Electrical and Electronic Engineers.

Normes 802.11

Hi ha diverses normes 802.11. Són les següents: 802.11a, 802.11b, 802.11g, 802.11 Super G, 802.11i i 802.16.

Les xarxes locals sense fil poden operar en mode *ad-hoc* o en mode infraestructura:

- **Mode *ad-hoc*** (client *vs*. client): totes les màquines que es troben dins la mateixa zona d'abast es poden comunicar entre si directament. No és habitual, encara que és pràctic, per exemple, per intercanviar la informació entre dos ordinadors (seria similar a la connexió de dos ordinador mitjançant un cable trenat).

- **Mode infraestructura** (client *vs*. punt d'accés): les estacions es comuniquen amb els anomenats *punts d'accés*, que actuen de repetidors i difonen la informació a la resta de la xarxa.

Com que la informació no necessita cap mitjà determinat per a circular, aquestes xarxes presenten problemes de seguretat importants. Per exemple, en una configuració normal de xarxa, el tallafoc sol ser un element crític de la seguretat i reuneix bona part de les mesures de protecció que eviten els atacs exteriors. En una xarxa sense fil, els atacants ja no necessiten "passar" pel tallafoc i poden atacar directament altres dispositius de la xarxa. La norma 802.11 preveu la utilització del protocol *wired equivalent protocol* (WEP) per a resoldre aquests problemes, però no és un mecanisme de protecció segur perquè actualment pot ser desencriptat sense gaires problemes.

WEP

Wired equivalent protocol (WEP) es basa en una encriptació RC4. Una clau WEP predeterminada s'ha de situar en cada punt d'accés i en cada client. Només aquells clients amb la mateixa clau se'ls permetrà l'accés.

Arran dels problemes de seguretat provocats pel protocol WEP, s'ha desenvolupat l'anomenat *Wi-Fi protected access* (WPA), el qual forma part de l'especificació 802.11i. Així doncs, en l'actualitat, ens trobarem amb mecanismes de seguretat com l'ús d'encriptació AES, un millor protocol d'autenticació (ús del WPA) i control de la integritat del missatge (ús de la funció *hash* MIC, en lloc del CRC-32 emprat en el protocol WEP).

Elements portables

És important que per a aprofitar tots els avantatges de les xarxes sense fil, les estacions de treball també puguin ser elements portables, com un ordinador portàtil o un PDA.

Malgrat tot, cal tenir present que les xarxes locals sense fil requereixen, a causa de la seva natura intrínseca, unes mesures de seguretat més grans que les que s'adoptarien en una xarxa "cablejada" normal.

Finalment, també cal tenir present la tecnologia *worldwide interoperability for microwave access* (WiMAX), estàndard (IEEE 802.16) de transmissió sense fil de dades, dissenyat per a ser utilitzat en l'àrea metropolitana, que proporciona accessos concurrents en àrees de com a molt 48 quilòmetres de radi, i amb velocitats de transmissió fins a 70 Mbps. Com és evident, aquesta tecnologia permet connectar el nostre dispositiu mòbil (ordinador portàtil, PDA, etc.) en qualsevol indret i, entre altres avantatges, podria fer arribar Internet a zones de difícil accés on no sigui possible instal·lar cap infraestructura. Emet dins la banda de 2 a 11 Ghz i de 10 a 60 Ghz per a comunicació entre antenes proveïdores de servei. L'algorisme d'encriptació emprat és un triple DES, però es preveu l'adopció de l'algorisme AES.

3. Protocols de comunicació

Una vegada instal·lat el maquinari, el cablejat i els diversos dispositius que formen la xarxa, cal instal·lar el programari de xarxa, que en gestionarà tots els serveis. Aquests serveis s'articulen sobre un conjunt de protocols que permetran la comunicació entre els diferents ordinadors de la xarxa. Els protocols més comuns són els de la família TCP/IP (entre d'altres, com per exemple Apple Talk per a sistemes Apple Macintosh, IPX/SPX,etc.).

Conjunt de protocols TCP/IP

TCP i IP només són dos dels protocols englobats dins el conjunt genèric TCP/IP, però són els més coneguts i, finalment, són els que donen el nom al conjunt sencer. Altres protocols TCP/IP són *address resolution protocol* (ARP), *Internet control message protocol* (ICMP).

3.1. Protocol TCP/IP

TCP/IP està format per un conjunt de protocols que permeten de compartir recursos als ordinadors d'una xarxa. El va desenvolupar l'any 1972 el Departament de Defensa dels Estats Units amb la finalitat d'interconnectar els recursos de la coneguda xarxa ARPANET (una xarxa del Departament de Defensa), i amb el pas del temps s'ha convertit en l'estàndard utilitzat a Internet. També es troba estretament vinculat al sistema operatiu Unix, tot i que actualment la gran majoria de sistemes operatius suporten TCP/IP. De fet, els protocols TCP/IP són extremadament flexibles, de manera que gairebé totes les tecnologies subjacents (*Ethernet*, *Token-ring*, etc.) es poden fer servir per a transmetre trànsit TCP/IP.

Prototol UDP

El protocol *user datagram protocol* (UDP) és un protocol no fiable i no orientat a connexió, situat a la capa de transport del model OSI (la mateixa que el protocol TCP).

Quan s'utilitza el protocol TCP/IP, la informació es transmet com una seqüència de *datagrames* que contenen les dades que cal transmetre i informació de control. Cadascun d'aquests datagrames s'envia individualment a la xarxa, de manera que la informació original pugui ser reconstruïda en arribar a la màquina destinació a partir del reagrupament dels datagrames enviats (val a dir que els datagrames no han d'arribar necessàriament amb el mateix ordre en què van ser lliurats).

El protocol *transmission control protocol* (TCP) garanteix la recepció de les dades i que els datagrames siguin refets en l'ordre correcte (servei fiable de transmissió extrem a extrem). Al mateix temps, aquest servei descansa en el proporcionat pel protocol *Internet protocol* (IP), que no és fiable, i que fa funcions d'encaminament dels datagrames.

3.2. Protocol IPv6

El protocol IPv6, o *next generation Internet protocol* (IPng), és la nova versió del protocol IP[18], destinada a substituir la que encara s'està utilitzant (coneguda com a **IPv4**). Fou dissenyat per Steve Deering i Craig Mudge, i adoptat per

(18)IP és la sigla de l'expressió anglesa *Internet protocol*.

l'Institute Engineering Task Force (IETF) l'any 1994. A la nova versió es varen eliminar aquelles funcions del protocol IP que no s'empraven i se n'afegiren de noves. Vegem tot seguit quines són les prestacions més importants d'IPv6:

- **Major capacitat d'adreçament**. Una de les principals deficiències del protocol IPv4 consistia en la seva poca capacitat d'adreçament (2^{32}). Les noves adreces, formades per 16 octets, permeten una capacitat d'adreçament molt més elevada i suficient per evitar el col·lapse de l'assignació d'adreces: 2^{128}, aproximadament, $3{,}4 \times 10^{38}$. A més, pel mateix motiu, amb IPv4 no es poden assignar adreces públiques a tots els usuaris o dispositius, sense les quals els serveis d'extrem a extrem no poden funcionar (per exemple, veu i vídeo sobre IP).

- **Seguretat integrada mitjançant *Internet protocol security* (IPSec)**.

- **Mobilitat**: Possibilitat que un node mantingui la seva adreça IP, malgrat la seva mobilitat.

- **Autoconfiguració**: El nou protocol també inclou de base la possibilitat que el mateix *host* sigui capaç d'autoconfigurar les seves interfícies i connectar-se a la xarxa.

Vegeu també

Sobre la seguretat mitjançant IPSec vegeu el subapartat 5.4 d'aquest mòdul, referit a les VPN.

Altres propietats interessants inclouen un nou sistema de representació de noms de domini (DNS), fàcilment ampliable a noves prestacions, túnels IPv6 en IPv4 (permeten que màquines amb IPv6 instal·lat es puguin comunicar entre si a través d'una xarxa IPv4), i nous tipus d'adreces:

- **unicast**: un paquet lliurat a una adreça d'aquest tipus tan sols arribarà a la interfície identificada amb aquesta adreça (és l'equivalent de les adreces IPv4 actuals).

- **anycast**: en aquest cas, l'adreça arribarà a "alguna" (l'adreça més propera segons el protocol d'encaminament) de les interfícies identificades amb l'adreça del conjunt.

- **multicast**: en aquest cas, l'adreça arribarà a "totes" les adreces de les interfícies del grup (equivalent a les adreces *broadcast* d'IPv4).

4. Configuració de la xarxa en els ordinadors (client/servidor)

Tot i que el concepte client/servidor abasta altres aspectes que aquí no exposarem, en el cas que ens ocupa entendrem que l'ordinador que actua com a servidor és aquell al qual arriben les sol·licituds d'altres ordinadors (els clients), normalment connectats a la mateixa xarxa.

Per a poder treballar en un entorn client/servidor cal que els clients executin el programari de xarxa sobre el sistema operatiu "normal" de l'estació de treball. D'altra banda, el servidor també executarà el seu programari a l'espera de rebre les sol·licituds de les estacions de treball que volen accedir als seus serveis. Aquest flux d'informació requereix que servidors i clients comparteixin el mateix protocol de comunicació.

4.1. Configuració de les estacions de treball

A continuació parlarem molt breument dels passos que cal seguir per a connectar una estació de treball a la xarxa. Aquesta operació depèn molt del sistema i protocol que es triï, de manera que totes les indicacions que es donaran són de caràcter molt general.

1) Instal·lació i configuració dels controladors de la targeta de xarxa. El primer pas consisteix a instal·lar i configurar els controladors del NIC[19] de la nostra estació de treball. En aquests casos, especialment quan les targetes són de fabricants diferents, la instal·lació i configuració dels controladors pot ser una tasca complicada en la qual s'hagin de resoldre conflictes d'entrada/sortida (E/S) i d'interrupcions amb altres NIC o altres recursos del sistema.

[19]NIC és la sigla de targetes d'interfície de xarxa, en anglès, *network interface card*.

Observació

Tingueu present que una estació de treball pot necessitar més d'una targeta de xarxa.

2) Selecció i configuració del protocol de comunicació. En cas que necessitem connexió amb Novell, caldrà instal·lar el protocol SPX/IPX. Per a fer-ho amb Macintosh, cal el protocol Apple Talk. Com ja s'ha indicat, però, el protocol més comú és TCP/IP, imprescindible si volem tenir accés a Internet.

Targeta *Plug and Play*

Si la targeta de xarxa és *Plug and Play*, es configurarà automàticament.

3) Instal·lació i configuració de clients.

4) Altres aspectes configurables. A partir d'aquest moment, es poden configurar altres aspectes, com els següents:

- Control d'accessos:
  - Per recursos: permet de proporcionar una contrasenya per cada recurs compartit.

  - Per usuaris: permet d'especificar els usuaris i grups que tenen accés a cadascun dels recursos compartits.

- Compartició de fitxers:
  - Permís de lectura.
  - Complet.
  - Permís de lectura o complet segons contrasenya.

- Compartició d'impressores.

- Identificació de la màquina (serà el nom amb què apareixerà a la xarxa).

- Grup de treball al qual pertany la màquina.

Instal·lació d'impressores

La impressora ha d'estar instal·lada amb els controladors necessaris en l'ordinador on estigui connectada. Les estacions que l'hagin de fer servir també necessitaran tenir instal·lats els controladors.

4.2. Monitorització de la xarxa

Una vegada configurada la xarxa, cal supervisar-ne el funcionament per a garantir la prestació dels serveis que ofereix i detectar els problemes que es puguin produir. Per a poder determinar on es localitzen els possibles problemes, hi ha diverses eines que ajuden l'administrador a acotar les zones en què es produeixen. Així, doncs, és possible tenir un ordinador en el qual es vegi reflectida la xarxa i en un moment determinat es pugui veure què és el que no funciona correctament.

Pel que fa a les estacions de treball, és evident que quan es produeix algun problema, els mateixos usuaris es queixen i notifiquen que la seva màquina no funciona correctament, o que el servidor dóna problemes. S'ha de tenir en compte, però, que els usuaris no han de ser necessàriament experts en xarxes d'ordinadors, i es pot donar el cas que un usuari digui que la xarxa no va bé (o que funciona lentament), quan el que succeeix en realitat és que l'usuari té el disc dur al 99% d'ocupació, i és el sistema operatiu el que funciona lentament. Tot i això, hi ha eines d'administració remota que poden facilitar diagnòstics sense necessitat de desplaçar-se a l'estació on es produeix el problema.

Control de l'estat dels ports

Alguns dispositius de connexió fins i tot disposen d'un petit servidor web per a mostrar l'estat dels ports i, simplement escrivint http://adreça_ip_del_dispositiu, ja es pot veure quin n'és l'estat.

També és important mantenir un control del funcionament dels commutadors i concentradors de la xarxa. En aquest sentit, hi ha programari específic que permet l'enregistrament dels errors de temperatura o mal funcionament que poden patir aquests equips. Normalment aquests dispositius tenen dues vies d'accés, una pel port sèrie i una altra per la xarxa (cadascun dels dispositius hauria de tenir assignada una adreça IP). Una possible avaria podria consistir, doncs, en el fet que un dels ports d'un commutador s'hagués espatllat, de manera que utilitzant la xarxa ens podríem connectar al commutador i verificar l'estat dels ports.

5. Seguretat de la xarxa

Com s'ha vist en els apartats anteriors, una xarxa és un conglomerat de molts elements heterogenis. Per tant, no podem confiar la seguretat d'un sistema tan complex a l'acumulació de mesures de control en el punt més evident: el servidor. Així, doncs, pel que fa a la seguretat de la xarxa (entesa de la manera més genèrica possible), s'hauria de tenir en compte els punts següents:

Vegeu també

Per aprofundir sobre la seguretat d'una xarxa vegeu el mòdul "Administració de la seguretat".

- **Sistema de fitxers**. S'ha de garantir que només puguin accedir als fitxers o modificar-los els usuaris autoritzats a fer-ho.

Vegeu també

Vegeu el mòdul "Administració d'usuaris".

- **Codi maliciós**. S'ha d'evitar el codi maliciós. S'anomena *codi maliciós* el codi que s'insereix dins d'un programa "autoritzat" i que fa una sèrie d'accions desconegudes per a l'usuari, les quals actuen normalment en detriment seu. Els exemples més coneguts de codi maliciós són els virus i els troians.

- **Autenticació d'usuaris**. S'ha d'habilitar un procés de verificació de la identitat d'una persona a l'hora d'accedir a un recurs. Habitualment els usuaris s'autentiquen mitjançant un nom d'usuari i una contrasenya (hi ha diferents tipus d'autenticació i diferents polítiques d'assignació de contrasenyes, els quals pot determinar un administrador).

Vegeu també

Vegeu el mòdul "Administració de la seguretat" per a més detalls sobre l'autenticació d'usuaris.

- **Criptografia**. S'han d'utilitzar eines criptogràfiques. Aquestes permeten de garantir la confidencialitat de les dades que circulen per la xarxa o es troben emmagatzemades en un sistema informàtic.

- **Eines de seguretat**. L'administrador pot fer ús de diverses eines amb la finalitat de comprovar i mantenir la seguretat de la xarxa. En general, podem diferenciar les següents:
  - Eines per a comprovar la vulnerabilitat de les mateixes màquines (per exemple, un escàner de ports).
  - Eines que ofereixen serveis segurs (per exemple, l'ús de *Secure Shell* en lloc de l'habitual *Telnet*).
  - Eines que garanteixen la integritat del sistema (com ara *Tripwire*).

- **Monitorització del sistema**. S'ha de fer un seguiment de l'activitat del sistema. S'anomena *logging* el procediment mitjançant el qual s'enregistren en un fitxer les activitats que tenen lloc en un sistema operatiu o en una aplicació. La importància dels fitxers *log* és evident i ens permetrà d'esbrinar "què" ha passat en un sistema informàtic i, si cal, prendre les mesures adients. És molt important plantejar "quines" aplicacions han d'enregistrar *log* i "quan" ho han de fer, i també quan s'han d'eliminar o

migrar a un dispositiu d'emmagatzemament per a poder tenir espai en el sistema.

- **Seguretat de les topologies i els tipus de xarxa**.

- **Seguretat del maquinari de xarxa**. Pel que fa a la seguretat dels commutadors, concentradors i encaminadors, cal tenir en compte els aspectes següents:
  - S'ha d'activar l'encriptació (en cas que els dispositius ho admetin).
  - En cas que no sigui necessari, cal desactivar el control remot d'administració.
  - S'han de canviar les contrasenyes d'administració predeterminades dels dispositius.

Vegeu també

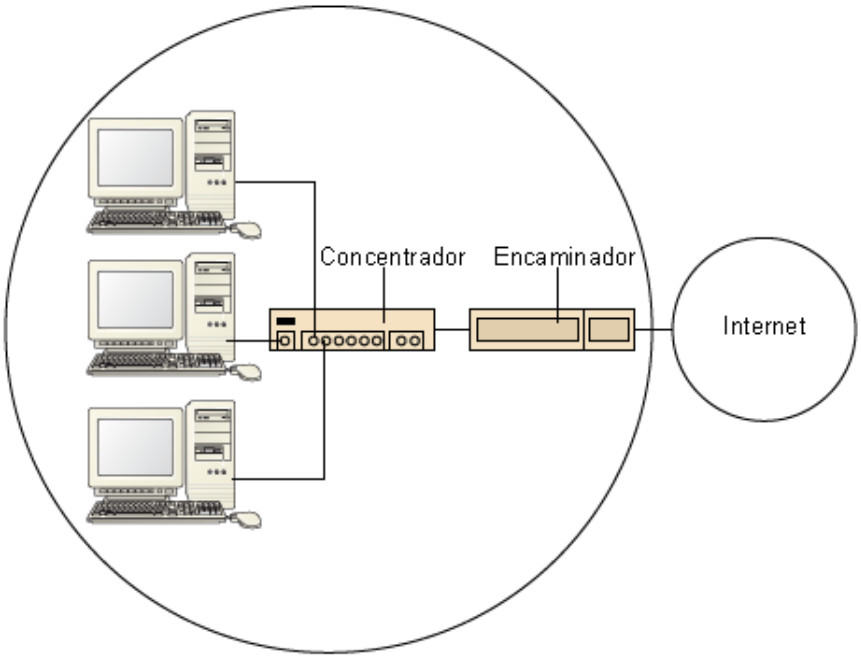
Recordeu que la seguretat de les topologies i els tipus de xarxa són aspectes que ja s'han desenvolupat en l'apartat 2 d'aquest mateix mòdul.

Contrasenyes predeterminades

Molts intrusos (*hackers*) coneixen les contrasenyes predeterminades dels dispositius, la qual cosa els permet d'accedir als sistemes d'una manera molt senzilla i evitant tots els mecanismes de seguretat explícits.

Cal destacar que l'encaminador pot esdevenir el punt més crític d'una xarxa des del punt de vista de possibles atacs externs:

L'encaminador com a element crític en la seguretat



- **Sistema de control d'accés a LAN basat en autenticació**. Mitjançant aquest sistema, els dispositius (en lloc dels usuaris) que volen connectar-se al medi comú s'hauran d'autenticar (basant-se en l'adreça MAC del dispositiu). Aquest mètode requereix tres components:
  - Client. És el dispositiu (per exemple, un portàtil) que desitja connectar-se a la LAN. Consisteix en un programari instal·lat o integrat en el dispositiu que es vol autenticar.

  - Autenticador. És l'element que controla l'accés físic al medi, basant-se en l'estat d'autenticació del client. L'estat inicial dels ports de l'autenticador és "no controlat". Si el procés d'autenticació finalitza

afirmativament, aleshores el port canvia el seu estat a "controlat" i el dispositiu és autoritzat per a accedir al medi.

– Servidor d'autenticació. És el dispositiu de "confiança" que s'encarregarà d'efectuar la validació de la identitat del client. Notificarà el resultat a l'autenticador.

Tots aquests apartats s'han de tenir en compte a l'hora de dissenyar la xarxa de comunicacions, ja que comporten despeses importants si es volen fer bé les coses. El cap del departament d'informàtica haurà de fer una bona planificació dels recursos que són necessaris.

5.1. Tallafocs

Els tallafocs són dispositius que eviten l'accés d'usuaris no autoritzats a un *host* determinat. L'administrador ha d'instal·lar aquests dispositius tenint en compte l'estructura de la xarxa i determinar els serveis que han de quedar disponibles per als usuaris.

A la pràctica, les funcions del tallafoc les poden dur a terme dispositius diversos:

- Programaris.
- Encaminadors.
- Ordinadors dedicats exclusivament a les tasques de filtració de paquets (servidors intermediaris, *proxy*).

El tallafoc és, probablement, un dels elements més importants per a la seguretat de la nostra xarxa. Amb la utilització dels tallafocs és possible evitar, per exemple, els atacs SYN. Cal considerar, a l'hora d'instal·lar un tallafocs, els aspectes següents:

Vegeu també

Sobre els atacs SYN vegeu el mòdul "Administració de la seguretat".

- No s'han d'emprar en lloc d'altres eines, sinó conjuntament amb aquestes. Hem de tenir en compte que el tallafoc serà el punt que rebrà tots els atacs sobre el nostre sistema.

- Centralitza una bona part de les mesures de seguretat de la xarxa en un únic sistema (no cal que sigui un únic dispositiu), i si es veu compromès, la xarxa quedarà exposada als atacs dels intrusos.

- Pot proporcionar una falsa sensació de seguretat als administradors. No per instal·lar un tallafoc podem assumir que la xarxa és segura i prescindir de vigilar la seguretat dels equips interns de la xarxa.

En general, les decisions bàsiques de configuració d'un tallafoc són:

- La configuració i el nivell de seguretat potencial del tallafoc estarà en relació amb l'ús del dispositiu. Així, la política serà diferent si connecta dues subxarxes diferents, que si ha de filtrar els paquets de l'organització amb l'exterior.

- S'ha de definir i implementar a través de la política de seguretat el nivell de monitorització i de control desitjat en l'organització. S'ha d'indicar bàsicament què s'ha de permetre i què s'ha de denegar. Hi ha dues possibilitats:
  – Política restrictiva: es denega tot allò que explícitament no es permet.
  – Política permissiva: es permet tot, excepte el que s'ha negat explícitament.

- La inversió ha de ser proporcional al valor estimat del que desitgem protegir. Un sistema de tallafoc pot ser molt barat o costar milers d'euros.

Hi ha diverses arquitectures de tallafocs diferents, però ens centrarem en les arquitectures DMZ[20]. Aquesta arquitectura col·loca una subxarxa entre les xarxes externa i interna. A la majoria d'arquitectures de tallafocs, la seguretat se centra en l'anomenat *host bastion*, de tal manera que si la seva seguretat queda compromesa, la resta de la xarxa queda automàticament exposada. Com el dispositiu *host bastion* és un objectiu interessant per a molts atacants, l'arquitectura DMZ és un intent d'aïllar-la en una xarxa perimetral, de tal forma que l'intrús que accedeixi a aquesta màquina no aconsegueixi un accés total a la subxarxa protegida.

[20]DMZ és la sigla de *DeMilitarized Zone*, en català, zones desmilitaritzades.

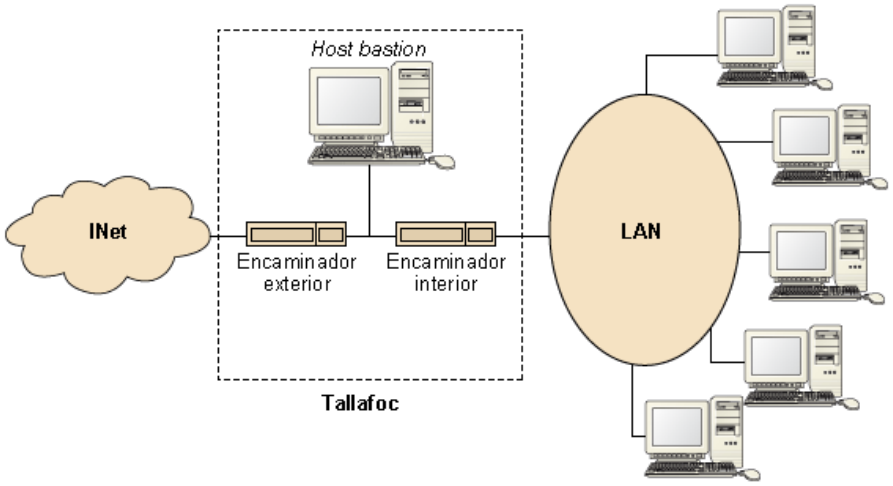
Host bastion

Host bastion és el dispositiu o sistema que es troba especialment assegurat i que filtra el trànsit d'entrada i sortida i amaga la configuració de la xarxa cap a fora.

En l'actualitat, aquesta és l'arquitectura més complexa i segura. S'usen dos encaminadors, anomenats interior i exterior, connectats ambdós a la xarxa perimetral.

En aquesta xarxa perimetral, que és el sistema tallafoc, s'inclou el *host bastion* i també es podrien incloure altres sistemes que requereixin un accés controlat, com per exemple el servidor de correu, els quals, *host* i servidor, serien els únics elements visibles des de l'exterior de la nostra xarxa. L'encaminador exterior té assignada la tasca de blocar el flux no desitjat en ambdós sentits (entre la xarxa perimetral i la xarxa externa), mentre que l'interior té la mateixa tasca, però amb el flux d'informació entre la xarxa interna i la perimetral. Un atacant hauria de trencar la seguretat d'ambdós encaminadors per a poder accedir a la xarxa protegida.

Arquitectura DMZ



5.2. Sistemes de detecció d'intrusos

Els sistemes de detecció d'intrusos (IDS) monitoritzen els continguts del flux d'informació a través de la xarxa a la recerca i rebuig de possibles atacs. Poden combinar maquinari i programari, i normalment s'instal·len en els dispositius més externs de la xarxa, com tallafocs o servidors cau[21]. Admeten dos tipus de classificacions:

[21] En anglès, *proxy*.

1) Segons l'activitat que realitzen:

a) Basats en xarxa. Monitoritzen una xarxa. Solen ser elements passius que no sobrecarreguen la xarxa en excés.

b) Basats en *host*. Monitoritzen un *host* (o un conjunt d'aquests) i permeten un control més detallat, registrant els processos i usuaris implicats en les activitats registrades per l'IDS[22]. Consumeixen recursos del *host* i incrementen el flux d'informació a través de la xarxa.

[22] Recordeu que IDS és la sigla de sistema de detecció d'intrusos.

c) Basats en aplicacions. Monitoritzen els fitxers de registre o *log* d'una aplicació específica per a detectar activitats sospitoses. Consumeixen molts recursos del *host*.

2) Segons el tipus d'anàlisi que realitzen:

a) Basats en signatures. De forma similar als programaris antivirus, aquests tipus d'IDS monitoritzen la xarxa a la recerca de patrons (signatures d'atac) que permetin identificar un atac ja conegut. Aquests tipus d'IDS requereixen que les bases de dades de signatures d'atac es trobin constantment actualitzades.

b) Basats en anomalies. En aquest cas, l'IDS cercarà comportaments anòmals a la xarxa (un escaneig de ports, paquets malformats, etc.).

Pot produir falsos positius a causa de l'ambigüitat del que es podria considerar un "comportament anòmal d'usuari", però permeten adaptar-se a nous atacs sense necessitat d'afegir noves signatures.

SNORT

Un IDS molt conegut, gairebé una eina de referència, *open source*, és l'anomenat SNORT.

5.3. Esquers i xarxes d'esquers

Un esquer[23] és un sistema informàtic (o programaris) que s'ofereix de forma deliberada a l'accés públic amb la finalitat d'estudiar les pautes dels possibles atacants que pugui tenir.

[23]En anglès, *honeypot*.

Per tant, aquests tipus de sistemes no podran contenir cap informació important i necessitaran d'eines passives d'auditoria que puguin permetre conèixer, amb posterioritat a l'atac, què és el que ha passat en el sistema. Freqüentment, aquests tipus de sistemes també contenen directoris o noms de fitxers amb identificacions llamineres que despertin la curiositat dels atacants. A més de la seva finalitat d'anàlisi, també poden utilitzar-se per a distreure l'atenció dels possibles atacants del veritable sistema, el qual no hauria de ser accessible a través del sistema utilitzat com a esquer. Els esquers no es troben, generalment, completament securitzats i les aplicacions i dispositius es configuren amb les opcions per defecte, les quals solen presentar múltiples forats de seguretat.

La generalització del concepte d'esquer a una xarxa s'anomena *honeynet*. En aquest cas, els atacants, a més de servidors no completament securitzats, també poden trobar dispositius perifèrics a la xarxa, com encaminadors o tallafocs.

5.4. Xarxa privada virtual

Una xarxa privada virtual (VPN[24]) és una xarxa privada que s'estén a diferents punts remots mitjançant l'ús d'infraestructures públiques de transport (com per exemple, Internet).

[24]VPN és la sigla de *virtual private network*.

La transmissió de paquets de dades es realitza mitjançant un procés d'encapsulació, i per seguretat, d'encriptació, ja que no cal oblidar que les dades circularan, durant un temps, per trams de xarxa pública. Aquests paquets de dades de la xarxa privada viatgen a través d'un "túnel" definit a la xarxa pública. És a dir, s'aprofita el baix cost de l'accés a Internet, s'afegeixen tècniques d'encriptació forta per a aconseguir seguretat i es simulen les clàssiques connexions punt a punt.

D'aquesta forma, un usuari (una sucursal de l'organització, un teletreballador, un representant comercial, etc.) connectat a través d'Internet a la xarxa corporativa de l'organització, establint un túnel VPN, pot funcionar com si estigués dins de la pròpia organització a tots els efectes de connectivitat.

En el cas d'accés remot en un equip, la VPN permet a l'usuari accedir a la seva xarxa corporativa, assignant-li al seu ordinador remot les adreces i privilegis d'aquesta, encara que la connexió s'hagi efectuat mitjançant una xarxa pública com és Internet.

La característica que converteix la connexió "pública" en "privada" (en una VPN) és el que s'anomena un túnel, terme referit al fet que únicament ambdós extrems són capaços de veure el que es transmet pel túnel, convenientment encriptat i protegit de la resta d'Internet. La tecnologia de túnel xifra i encapsula els protocols de xarxa que s'utilitzen en els extrems sobre el protocol IP. D'aquesta forma podem operar com si es tractés d'un enllaç dedicat convencional, de forma transparent a l'usuari.

El protocol més estès per a la creació de les VPN és *Internet protocol security* (IPSec). Consisteix en un conjunt d'estàndards industrials que comproven, autentiquen i encripten les dades en els paquets IP, i protegeixen les dades en les transmissions de xarxa. En definitiva, IPSec aporta la propietat de confidencialitat mitjançant l'encriptació de trànsit IP, integritat en el trànsit IP mitjançant el rebuig del trànsit modificat, així com autenticació i prevenció contra els atacs de reproducció. IPSec utilitza certificats (signats digitalment per una entitat emissora de certificats) per a comprovar la identitat d'un usuari, equip o servei, i enllacen de forma segura una clau pública a l'entitat que disposa de la clau privada corresponent.

Altres protocols VPN

Altres protocols VPN són, per exemple, Point-to-Point Tunneling Protocol (PPTP) i Layer 2 Tunneling Protocol (L2TP).

Vegeu també

Vegeu el mòdul "Administració de la seguretat".

El protocol té dues formes operacionals:

- **Mode transport**. Emprat per a protegir connexions individuals d'usuaris remots. Les comunicacions s'encripten entre un ordinador remot (el client VPN) i el servidor de VPN. Aquesta configuració pot ser d'interès, per exemple, quan l'organització disposa de dades molt confidencials que haurien de romandre ocultes per a molts usuaris. D'aquesta manera, se separen les dades confidencials gràcies al servidor VPN, de forma que només hi puguin accedir els usuaris autoritzats.

- **Mode túnel**. Les comunicacions s'encripten entre dos dispositius de tipus enrutador (o un enrutador i el servidor de VPN), amb el qual es protegeixen totes les comunicacions de tots els ordinadors situats rere cada enrutador.

A més de les VPN basades en xarxa pública, també cal esmentar les VPN de confiança[25], en les quals l'extensió es realitza sobre una xarxa privada, de confiança, i per tant, permet estalviar d'encriptar el flux d'informació que circula a través del túnel. Els protocols emprats en aquests tipus de xarxes són diferents i poden ser: *Asynchronous Transfer Mode* (ATM), *Multi-Protocol Label Switching* (MPLS) i *Layer 2 Forwarding* (L2F).

(25)VPN de confiança s'expressa en anglès com a *trusted VPN*.

6. Responsabilitats de l'administrador

Com podem intuir, l'administració d'una xarxa és una tasca molt complexa que abasta moltíssims aspectes, com ara els següents:

- Vetllar pel funcionament correcte de la xarxa.
- Garantir que el temps de resposta estigui dins els marges establerts.
- Controlar la seguretat del sistema informàtic a la part que utilitza la xarxa com a mitjà de transmissió.
- Gestionar i controlar les impressores que formen part de la xarxa d'ordinadors.
- Gestionar els serveis propis de la xarxa, com ara l'FTP, el Telnet, etc.

Tot i que es pot tenir la sensació que una vegada la xarxa ja es troba en funcionament no necessita cap manteniment, la configuració de la xarxa que interconnecta tots els recursos s'ha de repassar constantment, ja que el més habitual és que sempre hi hagi alguna modificació en les connexions a causa de llocs de treball que canvien, creació de nous punts de treball, sales de reunions que necessiten un punt de connexió per a fer una presentació, connexions temporals per a fer tests, etc. Per tant, s'ha de tenir present que cal tenir actualitzada la configuració de la xarxa per a poder respondre amb rapidesa a qualsevol petició de canvi per part d'algun usuari o departament.

El **temps de resposta** que s'exigeixi a la xarxa també és un aspecte que l'administrador ha de poder garantir. Molt sovint ens podem trobar amb usuaris que es queixen de la lentitud del sistema, però un administrador ha de saber demostrar que la xarxa funciona en les condicions que es van establir en el seu dia per tal de garantir el funcionament correcte de tots els serveis, i en cas que aquest temps no sigui l'esperat, ha de delimitar el problema fins a trobar-ne la solució o, si no es detecta cap element que funcioni malament a la xarxa, proposar la solució adient per a disminuir la càrrega i poder garantir la qualitat dels serveis que proporciona la xarxa.

La importància de la documentació

És recomanable tenir una documentació actualitzada i ben detallada de la xarxa que s'administra.

D'altra banda, també és molt important mantenir un control del que passa a la xarxa i verificar si hi ha algun tipus d'atac al sistema informàtic. Hi ha força eines per a ajudar l'administrador a enregistrar-los i monitoritzar-los, i segons les característiques que tingui el sistema val més la pena fer-ne servir unes o unes altres.

En tant que la xarxa és el medi pel qual els usuaris tenen accés a serveis proporcionats per servidors, és important tenir un control de les possibles **actualitzacions dels seus sistemes operatius** i del programari que hi tenen instal·lat. Paral·lelament a aquests serveis, hi ha un aspecte al qual s'ha de dedicar atenció: les impressores que hi ha a la xarxa han de tenir una gestió especial, ja que els controladors han d'estar disponibles per a ser instal·lats en qualsevol de les màquines que hagin de tenir accés a les impressores, i s'ha de pensar en una estructura que permeti als usuaris de tenir les màquines deslligades de les impressores, per a poder apagar-les i no tenir cap efecte sobre altres usuaris que vulguin imprimir.

Vegeu també

Al mòdul "Administració de la seguretat" trobareu un apartat sencer dedicat al "ciberdelicte".

També és especialment important disposar de les **llicències de programari** de xarxa (per exemple, les llicències de campus de la universitat, o multivolums, etc.). Com és evident, instal·lar programari amb llicències monousuari en xarxes és una pràctica que pot tenir conseqüències en forma de sanció. L'administrador de la xarxa també ha de conèixer quins mecanismes té a la seva disposició per a denunciar qualsevol infracció de què hagi estat objecte (o que observi en la xarxa que administra: atacs dels intrusos [*hackers*], presència de fotografies de pornografia infantil, etc.).

Vegeu també

Les consideracions sobre si les xarxes proporcionen (o no) un espai d'ús privat als usuaris es veuran en el mòdul "Administració de la seguretat".

Resum

Les xarxes d'ordinadors permeten d'aprofitar millor els recursos del sistema. En aquest mòdul s'han vist els elements que formen part de la xarxa i alguns criteris que poden ajudar els administradors a l'hora de triar aquests elements i connectar-los entre si. Una vegada es disposa de la xarxa, físicament parlant, cal fer que els ordinadors parlin el mateix "idioma", és a dir, tinguin definit el mateix protocol de comunicacions (el més utilitzat és el TCP/IP), la instal·lació del qual es troba íntimament lligada a la configuració de les estacions de treball. Tot i l'heterogeneïtat de les xarxes, els protocols i els sistemes operatius de xarxa, aquestes accions sempre s'han de fer d'una manera o altra, tot i que la manera com es fan pot variar molt.

Finalment, una vegada la xarxa ja estigui en funcionament, l'administrador no pot oblidar que les xarxes no es mantenen per si soles i que requereixen un gran esforç de manteniment: creació i administració de l'entorn de l'usuari, monitorització de la xarxa, actualització de programari, detecció d'atacs, etc.

Activitats

1. En cas que tingueu accés a una xarxa d'ordinadors, responngueu les qüestions següents:

a) Localitzeu i identifiqueu físicament tots els elements que formen part de la xarxa.
b) Quina topologia s'ha utilitzat en el seu disseny?
c) Quins protocols de comunicació es fan servir?
d) Com es configuren les estacions de treball?
e) Quins programaris de monitorització s'utilitzen?
f) Localitzeu i identifiqueu els elements de seguretat (programari i maquinari).

2. Si no disposeu d'accés a una xarxa d'ordinadors, enumereu i descriviu tots els elements que participen en una connexió a Internet per la xarxa telefònica:

Casa <-> Proveïdor de serveis d'Internet <-> Internet

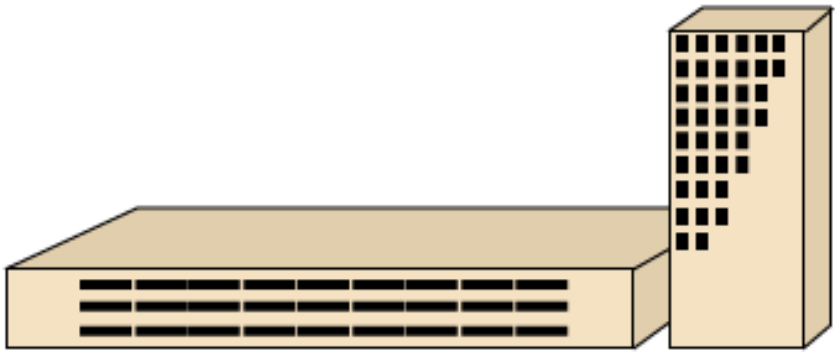
Un element que caldrà que tingueu en compte és que per tal de respondre a possibles problemes legals (i a efectes de tarificació), un proveïdor d'Internet hauria d'enregistrar les adreces IP que va proporcionant dinàmicament als usuaris, juntament amb el número de telèfon que s'ha fet servir per a connectar-s'hi, i també l'interval de temps en què s'han utilitzat.

Exercicis d'autoavaluació

1. Ompliu cadascuna de les caselles de la taula següent amb alguna d'aquestes opcions: baix/moderat/alt.

	Parell trenat	Coaxial	Fibra òptica
Cost			
Amplada de banda			
Longitud			
Interferències			
Fiabilitat			

2. Heu de dissenyar i implementar una xarxa per a un edifici com el següent, format per un bloc de quatre plantes i una nau industrial que treballa amb molts motors. Dissenyeu un traçat per al cablejat elèctric per tal d'alimentar els motors i després poseu els dispositius de comunicació que s'haurien d'instal·lar, tant en la nau industrial com en l'edifici, per a tenir una xarxa local que comuniqués les oficines amb els punts de treball de la nau industrial.



3. Determineu quina de les característiques següents no es pot atribuir a qualsevol topologia en estrella:

a) Totes les estacions es connecten a un element central.
b) Quan una estació emet un missatge sempre arriba a totes les estacions de la xarxa.
c) És una topologia resistent a la caiguda de les estacions de treball.
d) El dispositiu central pot ser actiu o passiu.

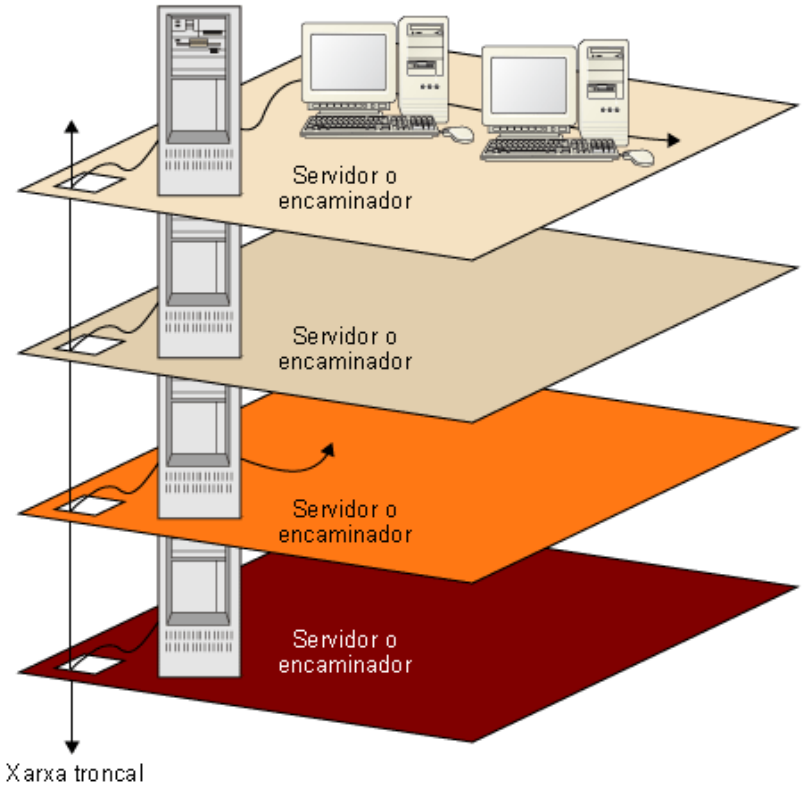
Solucionari

Exercicis d'autoavaluació

1.

	Parell trenat	Coaxial	Fibra òptica
Cost	Baix	Moderat	Alt
Amplada de banda	Moderat	Alt	Molt alt
Longitud	100 m	1 km	Alguns km
Interferències	Baix	Molt baix	Cap
Fiabilitat	Alt	Alt	Molt alt

2.

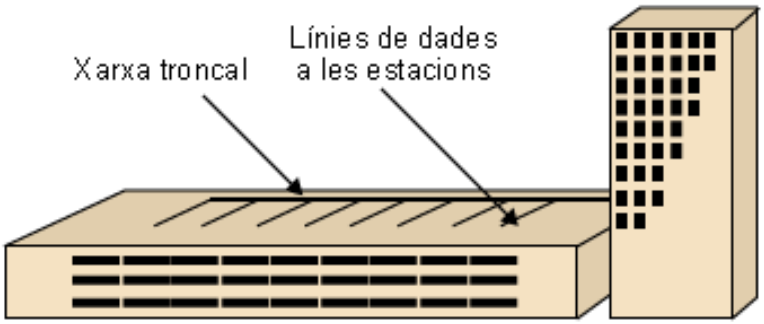


A la planta, el cablejat també hauria de seguir un esquema de tipus xarxa troncal (*backbone*), amb branques en els punts necessaris. Les qüestions bàsiques que cal tenir en compte en el disseny són les següents:

Les distàncies del cablejat no han de ser superiors a les permeses. En cas contrari, cal posar regeneradors del senyal.

S'ha de tenir molt en compte el problema de les interferències elèctriques i, per tant, electricitat i dades no poden anar pels mateixos llocs.

Si hi ha armaris de connexió, cal tenir en compte les qüestions de protecció de les vibracions i de l'alimentació elèctrica.



3. b.

Glossari

10Base-T *m* Cable de parell trenat UTP amb una longitud màxima de segment de cent metres sobre una topologia física d'estrella.

100Base-T *m* Cable de parell trenat UTP amb velocitats de transmissió de 100 Mbps.
sin. ***fast Ethernet***.

10Base-2 *m* Cable coaxial prim amb una velocitat de transmissió de 10 Mbps. Accepta fins a trenta llocs de treball en segments de longitud de com a molt cent vuitanta-cinc metres.
sin. ***thin wire***.

10Base-5 *m* Cable coaxial gruixut amb una velocitat de transmissió de 10 Mbps. Accepta fins a cent llocs de treball en segments de longitud de com a molt cinc-cents metres.
sin. ***thick wire***.

backbone *m* Vegeu **xarxa troncal**.

commutador *m* Dispositiu que gestiona el flux del trànsit de xarxa tenint en compte l'adreça de destinació de cada paquet. En altres paraules, els commutadors poden esbrinar quins dispositius es troben connectats als seus ports i redirigeixen la informació únicament al port destinació, en lloc de fer-ho indiscriminadament, com els concentradors.
en switch.

concentrador *m* Dispositiu que permet de compartir una línia de comunicació entre diversos ordinadors. Repeteix tota la informació que rep perquè pugui arribar a tots els dispositius connectats.
en hub.

DHCP *m* Vegeu **protocol dinàmic de configuració de l'hoste**.

dynamic host configuration protocol *m* Vegeu **protocol dinàmic de configuració de l'hoste**.

encaminador *m* Dispositiu que gestiona el trànsit de paquets provinent de l'exterior de la xarxa cap a l'interior (i a l'inrevés). Pot tenir capacitat d'actuar com a tallafoc. Pot filtrar i trobar l'encaminament òptim dels paquets.
en router.

fast Ethernet *f* Vegeu **100Base-T**.

firewall *m* Vegeu **tallafoc**.

hub *m* Vegeu **concentrador**.

IEEE *m* Vegeu **Institute of Electrical and Electronic Engineers**.

Institute of Electrical and Electronic Engineers *m* Organisme que data de l'any 1980 i que va elaborar les normes IEEE 802.X, les quals defineixen els estàndards pel que fa al funcionament de les xarxes d'àrea local.
sigla: **IEEE**.

network interface card *f* Vegeu **targeta d'interfície de la xarxa**.

NIC *f* Vegeu **targeta d'interfície de la xarxa**.

protocol dinàmic de configuració de l'hoste *m* Protocol TCP/IP que permet l'assignació dinàmica d'adreces IP.
en dynamic host configuration protocol.
sigla: **DHCP**.

router *m* Vegeu **encaminador**.

switch *m* Vegeu **commutador**.

tallafoc *m* Qualsevol dispositiu (maquinari o programari) que permet d'evitar que els usuaris no autoritzats accedeixin a una màquina determinada.
en firewall.

targeta d'interfície de la xarxa *f* Targeta d'interfície que permet la connexió de l'estació de treball a la xarxa.
en network interface card.

sigla: **NIC**.

thick wire *m* Vegeu **10Base-5**.

thin wire *m* Vegeu **10Base-2**.

wireless local area network *f* Vegeu **xarxa d'àrea local sense fil**.

WLAN *f* Vegeu **xarxa d'àrea local sense fil**.

xarxa d'àrea local sense fil *f* Xarxa de telecomunicacions local sense fil basada en ones de ràdio o infraroges.
en wireless local area network.
sigla: **WLAN**.

xarxa troncal *f* Conjunt de cables principals que connecten entre si els segments d'una xarxa local. Habitualment són enllaços d'alta velocitat (per exemple, fibra òptica).
en backbone.

Bibliografia

Anònim (2000). *Linux Máxima Seguridad*. Prentice Hall.

Arnedo Moreno, J. (2002). *Xarxes locals sense fils*. (Article UOC)

Colobran Huguet, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Halsall F. (1996). *Data communications, computer networks and open systems*. McGraw-Hill.

Jimeno García, M. T.; Míguez Pérez, C.; Matas García, A. M.; Pérez Agudín, J. (2008). *Guía práctica hacker*. Madrid: Anaya Multimedia.

Palet Martínez, Jordi. *Tutorial d'IPv6*.

Tanembaum, A. S. (1991). *Redes de ordenadores*. Prentice-Hall Hispanoamericana.