Mòdul 0225 – Xarxes d'àrea local

Índex

Cicle formatiu: Sistemes Microinformàtics i Xarxes (SMX)

Durada: 198 h (132 h centre + 66 h empresa)

RA4 -- Instal·lació i configuració d'equips de xarxa

Criteri general (4): Instal·la equips en xarxa, descrivint les seves prestacions i aplicant tècniques de muntatge.

4.1. Protocols TCP/IP

Criteri 4.7/4.8 -- Identifica els protocols i configura els paràmetres bàsics.

Model TCP/IP i OSI

El model TCP/IP organitza la comunicació en quatre capes:

Capa TCP/IP	Equivalent OSI	Protocols
Aplicació	Aplicació/Presentació/Sessió	HTTP, FTP, DNS, DHCP, SMTP
Transport	Transport	TCP, UDP
Internet	Xarxa	IP, ICMP, ARP
Accés a la xarxa	Enllaç + Física	Ethernet (802.3), Wi-Fi (802.11)

Ports TCP/IP més importants

Els **ports** identifiquen el servei o aplicació de destí dins d'un host. El rang va de 0 a 65.535:

- **Ports ben coneguts** (0--1.023): assignats per la IANA a serveis estàndard. Requereixen privilegis de root per obrir-los.
- **Ports registrats** (1.024--49.151): usats per aplicacions de tercers.
- **Ports dinàmics / efímers** (49.152--65.535): assignats temporalment als clients en cada connexió.

Port	Protocol	Transport	Descripció
20	FTP-DATA	TCP	Transferència de dades FTP (mode actiu)
21	FTP	TCP	Control de connexió FTP
22	SSH	TCP	Accés remot segur (Secure Shell)
23	Telnet	TCP	Accés remot sense xifrar (obsolet, insegur)
25	SMTP	TCP	Enviament de correu electrònic
53	DNS	TCP/UDP	Resolució de noms de domini
67	DHCP	UDP	Servidor DHCP (assignació d'adreces IP)
68	DHCP	UDP	Client DHCP
69	TFTP	UDP	Transferència de fitxers trivial (sense autenticació)
80	HTTP	TCP	Web sense xifrar
110	POP3	TCP	Recepció de correu (descarrega i esborra del servidor)
123	NTP	UDP	Sincronització de l'hora de xarxa
143	IMAP	TCP	Recepció de correu (gestió al servidor)

161	SNMP	UDP	Monitoratge i gestió de dispositius de xarxa
162	SNMP Trap	UDP	Notificacions SNMP dels dispositius
443	HTTPS	TCP	Web amb xifrat TLS/SSL
465	SMTPS	TCP	SMTP xifrat (TLS)
587	SMTP	TCP	Enviament de correu amb autenticació (submission)
993	IMAPS	TCP	IMAP xifrat (TLS)
995	POP3S	TCP	POP3 xifrat (TLS)

> **Recordatori:** TCP estableix una connexió orientada (amb confirmació), adequat per a transferències fiables. UDP és sense connexió i més ràpid, adequat per a DNS, streaming i VoIP.

Consultar i filtrar ports en ús a Ubuntu 24.04:

```
ss -tulnp                          # tots els ports en escolta
ss -tulnp | grep :80               # filtrar el port 80
sudo ss -tlnp | grep LISTEN        # només TCP en escolta
```

Adreçament IPv4

Una **adreça IPv4** té 32 bits, representada en notació decimal separada per punts (p. ex. `192.168.1.10`). Es compon de:

- **Part de xarxa**: identifica la xarxa.
- **Part de host**: identifica el dispositiu dins la xarxa.

La **màscara de subxarxa** determina quina part és xarxa i quina és host. En notació CIDR: `192.168.1.0/24` (24 bits per a la xarxa).

Classes d'adreces IPv4:

Classe	Rang 1r octet	Màscara per defecte	Ús habitual
A	1 -- 126	/8 (255.0.0.0)	Grans xarxes
B	128 -- 191	/16 (255.255.0.0)	Xarxes mitjanes
C	192 -- 223	/24 (255.255.255.0)	Xarxes petites
D	224 -- 239	---	Multicast
E	240 -- 255	---	Reservat

Adreces privades (RFC 1918):

Rang	Classe	Màscara
10.0.0.0 -- 10.255.255.255	A	/8
172.16.0.0 -- 172.31.255.255	B	/12
192.168.0.0 -- 192.168.255.255	C	/16

Les adreces privades no s'encaminen a Internet; cal NAT (*Network Address Translation*) per accedir-hi.

Adreces especials:

- `127.0.0.1` → loopback (proves locals)

- `169.254.x.x` → APIPA (assignació automàtica quan no hi ha DHCP)
- Adreça de xarxa: tots els bits de host a 0 → `192.168.1.0`
- Adreça de difusió (*broadcast*): tots els bits de host a 1 → `192.168.1.255`

Taula completa de màscares de subxarxa

Aquesta taula cobreix tots els prefixos CIDR possibles per a IPv4, amb la màscara en notació decimal, els bits disponibles per a hosts, el nombre d'hosts útils (sense adreça de xarxa ni broadcast) i la màscara curta (*wildcard*) necessària per a OSPF i ACL de Cisco.

CIDR	Màscara decimal	Wildcard	Bits host	Hosts útils	Ús típic
/0	0.0.0.0	255.255.255.255	32	4.294.967.294	Ruta per defecte
/8	255.0.0.0	0.255.255.255	24	16.777.214	Xarxes classe A
/9	255.128.0.0	0.127.255.255	23	8.388.606	
/10	255.192.0.0	0.63.255.255	22	4.194.302	
/11	255.224.0.0	0.31.255.255	21	2.097.150	
/12	255.240.0.0	0.15.255.255	20	1.048.574	172.16.0.0/12 (xarxa privada B)
/13	255.248.0.0	0.7.255.255	19	524.286	
/14	255.252.0.0	0.3.255.255	18	262.142	
/15	255.254.0.0	0.1.255.255	17	131.070	
/16	255.255.0.0	0.0.255.255	16	65.534	Xarxes classe B
/17	255.255.128.0	0.0.127.255	15	32.766	
/18	255.255.192.0	0.0.63.255	14	16.382	
/19	255.255.224.0	0.0.31.255	13	8.190	
/20	255.255.240.0	0.0.15.255	12	4.094	
/21	255.255.248.0	0.0.7.255	11	2.046	
/22	255.255.252.0	0.0.3.255	10	1.022	
/23	255.255.254.0	0.0.1.255	9	510	
/24	255.255.255.0	0.0.0.255	8	254	Xarxes classe C (**molt comú**)
/25	255.255.255.128	0.0.0.127	7	126	Divisió de /24 en 2
/26	255.255.255.192	0.0.0.63	6	62	Divisió de /24 en 4
/27	255.255.255.224	0.0.0.31	5	30	Divisió de /24 en 8
/28	255.255.255.240	0.0.0.15	4	14	Divisió de /24 en 16
/29	255.255.255.248	0.0.0.7	3	6	Xarxes petites (oficines)
/30	255.255.255.252	0.0.0.3	2	2	Enllaços punt a punt
/31	255.255.255.254	0.0.0.1	1	0	Enllaços P2P (RFC 3021)
/32	255.255.255.255	0.0.0.0	0	1 (host únic)	Ruta a host individual

Com calcular la màscara decimal a partir del prefix CIDR:

El valor de cada octet de la màscara s'obté sumant els pesos dels bits actius (a 1). Els primers n bits són 1 i la resta 0.

Exemple per a `/26` (26 bits a 1):

```
Octet 1:  11111111 = 255
Octet 2:  11111111 = 255
Octet 3:  11111111 = 255
Octet 4:  11000000 = 128 + 64 = 192
Màscara:  255.255.255.192
```

Com calcular la wildcard:

La *wildcard mask* és simplement `255.255.255.255 − màscara`:

```
255.255.255.255
-255.255.255.192  (màscara /26)
= 0.0.0.63        (wildcard de /26)
```

Valors possibles del quart octet de la màscara (per a subxarxes /24 a /32):

Bits a 1 (en l'octet)	Valor decimal	CIDR (sobre /24)
00000000	0	/24
10000000	128	/25
11000000	192	/26
11100000	224	/27
11110000	240	/28
11111000	248	/29
11111100	252	/30
11111110	254	/31
11111111	255	/32

IPv6

IPv6 utilitza **128 bits** (en lloc dels 32 d'IPv4), representada en hexadecimal separat per dos punts:

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Es pot abreujar eliminant zeros inicials i substituint grups de zeros consecutius per `::` (una sola vegada):

```
2001:db8:85a3::8a2e:370:7334
```

Tipus d'adreces IPv6:

Tipus	Prefix	Descripció
Unicast global	2000::/3	Equivalen a les adreces públiques IPv4
Unicast local d'enllaç	fe80::/10	Autoconfigurada, no enrutable
Multicast	ff00::/8	Substitueix el broadcast d'IPv4
Loopback	::1/128	Equivalent a 127.0.0.1 en IPv4

Avantatges principals d'IPv6: espai d'adreçament pràcticament il·limitat, autoconfiguració (SLAAC), millor seguretat integrada (IPsec), eliminació de NAT.

Configuració d'adaptadors de xarxa

En Ubuntu 24.04

Ubuntu 24.04 utilitza **Netplan** com a sistema de configuració de xarxa. Els fitxers de configuració són en format YAML i es troben a `/etc/netplan/`. El backend per defecte és **NetworkManager** (en sistemes d'escriptori) o **systemd-networkd** (en servidors).

Noms d'interfícies predicibles: Ubuntu 24.04 no usa els noms tradicionals `eth0` o `wlan0`. Els noms depenen del maquinari: - Ethernet: `enp3s0`, `ens33`, `eno1`... (format `en` + tipus + slot) - Wi-Fi: `wlp2s0`, `wlan0` (en alguns casos), `wlx...` (USB)

Per veure els noms reals de les interfícies del sistema:

```
ip link show
# o bé:
nmcli device status
```

Configuració estàtica amb Netplan (`/etc/netplan/01-network-manager-all.yaml` o similar):

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp3s0:
      dhcp4: false
      addresses:
        - 192.168.1.10/24
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

Aplicar els canvis:

```
sudo netplan apply
```

Configuració per DHCP amb Netplan:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp3s0:
      dhcp4: true
```

Gestió amb `nmcli` (interfície de línia d'ordres per a NetworkManager):

```
# Llistar connexions i dispositius
nmcli connection show
```

```
nmcli device status

# Crear una connexió estàtica
nmcli connection add type ethernet ifname enp3s0 con-name
 ↪  "xarxa-estatica" \
  ipv4.addresses 192.168.1.10/24 \
  ipv4.gateway 192.168.1.1 \
  ipv4.dns "8.8.8.8 1.1.1.1" \
  ipv4.method manual

# Activar / desactivar una connexió
nmcli connection up "xarxa-estatica"
nmcli connection down "xarxa-estatica"

# Connectar a una xarxa Wi-Fi
nmcli device wifi connect "NomXarxa" password "contrasenya"

# Llistar xarxes Wi-Fi disponibles
nmcli device wifi list
```

Gestió gràfica: en l'entorn d'escriptori GNOME d'Ubuntu 24.04, la configuració de xarxa es pot fer des de **Configuració del sistema** → **Xarxa** o fent clic a la icona de xarxa de la barra superior.

Verificació de la configuració DNS:

```
resolvectl status          # estat complet del resolver
resolvectl query ioc.cat   # resolució d'un nom
cat /etc/resolv.conf       # fitxer de resolució (gestionat per
 ↪  systemd-resolved)
```

> A Ubuntu 24.04, `/etc/resolv.conf` és un enllaç simbòlic gestionat per **systemd-resolved**. No s'ha d'editar directament; cal usar `nmcli` o Netplan.

En Windows: Panel de control → Centre de xarxes → Canviar la configuració de l'adaptador → Propietats → Protocol Internet versió 4 (TCP/IPv4).

DHCP (*Dynamic Host Configuration Protocol*): permet que un servidor assigni automàticament adreça IP, màscara, passarel·la i DNS als clients. El procés DORA:

1. **Discover** -- el client emet un broadcast buscant un servidor DHCP.
2. **Offer** -- el servidor ofereix una adreça IP.
3. **Request** -- el client sol·licita l'adreça oferta.
4. **Acknowledge** -- el servidor confirma l'assignació.

Sistema binari i potències de 2

Les adreces IPv4 són nombres binaris de 32 bits. Entendre el sistema binari i les potències de 2 és imprescindible per treballar amb màscares de subxarxa i per fer càlculs d'adreçament.

Taula de potències de 2 (2^0 a 2^{32}):

Exponent	Valor	Ús en xarxes
2^0	1	
2^1	2	Subxarxa amb 0 hosts útils (cas límit)
2^2	4	Subxarxa /30 → 2 hosts útils
2^3	8	Subxarxa /29 → 6 hosts útils
2^4	16	Subxarxa /28 → 14 hosts útils
2^5	32	Subxarxa /27 → 30 hosts útils
2^6	64	Subxarxa /26 → 62 hosts útils
2^7	128	Subxarxa /25 → 126 hosts útils
2^8	256	Subxarxa /24 → 254 hosts útils (xarxa /24)
2^9	512	Subxarxa /23 → 510 hosts útils
2^{10}	1.024	Subxarxa /22 → 1.022 hosts útils
2^{11}	2.048	Subxarxa /21 → 2.046 hosts útils
2^{12}	4.096	Subxarxa /20 → 4.094 hosts útils
2^{13}	8.192	
2^{14}	16.384	
2^{15}	32.768	
2^{16}	65.536	Subxarxa /16 → 65.534 hosts útils
2^{24}	16.777.216	Subxarxa /8 → 16.777.214 hosts útils
2^{32}	4.294.967.296	Total d'adreces IPv4 possibles

Pesos dels bits en un octet (8 bits):

Bit	7	6	5	4	3	2	1	0
Pes	128	64	32	16	8	4	2	1
Suma màx.								**255**

> La suma de tots els pesos (128+64+32+16+8+4+2+1) = **255**, que és el valor màxim d'un octet. En binari: `11111111`.

Conversió decimal ↔ binari

De decimal a binari

Mètode de divisions successives per 2:

Es divideix el nombre per 2 repetidament i s'anoten els residus. El resultat binari es llegeix de baix a dalt (de l'últim residu al primer).

Exemple: convertir 192 a binari

```
192 ÷ 2 = 96  residu 0
 96 ÷ 2 = 48  residu 0
 48 ÷ 2 = 24  residu 0
 24 ÷ 2 = 12  residu 0
```

```
12 ÷ 2 =  6  residu 0
 6 ÷ 2 =  3  residu 0
 3 ÷ 2 =  1  residu 1
 1 ÷ 2 =  0  residu 1   ← llegir cap amunt
```

Resultat (llegit de baix a dalt): **11000000** → `192` en decimal = `11000000` en binari.

Mètode de les potències (taula de pesos) --- recomanat per a octets:

Es comprova si el nombre és ≥ al pes de cada bit, de major a menor. Si sí → 1 i es resta; si no → 0.

Exemple: convertir 172 a binari

Pes	128	64	32	16	8	4	2	1
¿≥?								
Bit	1	0	1	1	0	1	0	0
Resta	172-128=44	---	44-32=12	12-16<0 → 12-8=4	---	4-4=0	---	---

Resultat: **10101100** → `172` = `10101100`

Taula de conversió ràpida dels octets més comuns en xarxes:

Decimal	Binari	Decimal	Binari
0	00000000	128	10000000
1	00000001	192	11000000
10	00001010	224	11100000
16	00010000	240	11110000
32	00100000	248	11111000
64	01000000	252	11111100
127	01111111	254	11111110
128	10000000	255	11111111
168	10101000	172	10101100

De binari a decimal

Mètode: multiplicar cada bit pel seu pes i sumar.

Exemple: convertir `11000000` a decimal

Bit	1	1	0	0	0	0	0	0
Pes	128	64	32	16	8	4	2	1
Prod.	128	64	0	0	0	0	0	0

Suma: 128 + 64 = **192**

Exemple: convertir `10101000` a decimal (adreça típica: 168)

Bit	1	0	1	0	1	0	0	0
Pes	128	64	32	16	8	4	2	1
Prod.	128	0	32	0	8	0	0	0

Suma: 128 + 32 + 8 = **168**

Exemple complet: adreça IP en binari

L'adreça `192.168.1.10` en binari octet per octet:

```
192  →  11000000
168  →  10101000
  1  →  00000001
 10  →  00001010
```

Representació completa (32 bits):

```
11000000.10101000.00000001.00001010
```

Càlcul de subxarxes

El **subnetejat** (*subnetting*) consisteix a dividir una xarxa IP en subxarxes més petites, assignant una part dels bits de host a la identificació de subxarxa.

Conceptes bàsics

Donada una adreça en notació CIDR `X.X.X.X/n`:

- **n** = nombre de bits de xarxa (prefix)
- **32 − n** = nombre de bits de host
- **Nombre d'hosts útils** = 2^(32−n) − 2 (es resten l'adreça de xarxa i la de broadcast)
- **Adreça de xarxa**: tots els bits de host a 0
- **Adreça de broadcast**: tots els bits de host a 1
- **Rang d'hosts útils**: des de (adreça de xarxa + 1) fins a (broadcast − 1)

Taula de màscares CIDR

CIDR	Màscara decimal	Bits host	Núm. hosts útils	Increment
/24	255.255.255.0	8	254	256
/25	255.255.255.128	7	126	128
/26	255.255.255.192	6	62	64
/27	255.255.255.224	5	30	32
/28	255.255.255.240	4	14	16
/29	255.255.255.248	3	6	8
/30	255.255.255.252	2	2	4
/23	255.255.254.0	9	510	512
/22	255.255.252.0	10	1.022	1.024
/21	255.255.248.0	11	2.046	2.048

/20	255.255.240.0	12	4.094	4.096
/16	255.255.0.0	16	65.534	65.536

L'increment (o *block size*) és el salt entre subxarxes consecutives: 2^(bits de host).

Mètode de càlcul pas a pas

Donada l'adreça `192.168.1.0/26`, calcular: màscara, adreça de xarxa, broadcast, rang d'hosts i nombre de subxarxes respecte a /24.

Pas 1 -- Identificar els bits - Prefix /26 → 26 bits de xarxa, **6 bits de host** - Bits de subxarxa respecte a /24 = 26 − 24 = **2 bits** → 2^2 = **4 subxarxes**

Pas 2 -- Màscara en binari i decimal

```
11111111.11111111.11111111.11000000
   255  .   255  .   255  .  192
```

Màscara: **255.255.255.192**

Pas 3 -- Increment 6 bits de host → 2^6 = **64** (l'increment entre subxarxes)

Pas 4 -- Llistar les 4 subxarxes

Subxarxa	Adreça de xarxa	Primer host	Últim host	Broadcast
1a	192.168.1.**0**	192.168.1.1	192.168.1.62	192.168.1.**63**
2a	192.168.1.**64**	192.168.1.65	192.168.1.126	192.168.1.**127**
3a	192.168.1.**128**	192.168.1.129	192.168.1.190	192.168.1.**191**
4a	192.168.1.**192**	192.168.1.193	192.168.1.254	192.168.1.**255**

Cada subxarxa té **62 hosts útils** (2^6 − 2 = 62).

Exemple 2: subnetejat des de /16

Donada `172.16.0.0/20`, quantes subxarxes hi ha respecte a /16 i quants hosts per subxarxa?

- Bits de subxarxa: 20 − 16 = **4 bits** → 2^4 = **16 subxarxes**
- Bits de host: 32 − 20 = **12 bits** → 2^{12} − 2 = **4.094 hosts útils** per subxarxa
- Increment: 2^{12} = 4.096 → el salt és en el 3r octet: de 256/16 = 16 en 16

Subxarxa	Adreça de xarxa	Broadcast
1a	172.16.**0**.0	172.16.**15**.255
2a	172.16.**16**.0	172.16.**31**.255
3a	172.16.**32**.0	172.16.**47**.255
…	…	…
16a	172.16.**240**.0	172.16.**255**.255

Verificació d'una adreça: a quina subxarxa pertany?

Per saber a quina subxarxa pertany `192.168.1.100/26`:

Increment = 64. Les subxarxes comencen a: 0, 64, 128, 192…

100 és entre 64 i 127 → pertany a la subxarxa **192.168.1.64/26** - Broadcast: 192.168.1.127 - Rang d'hosts: 192.168.1.65 -- 192.168.1.126

Eina pràctica a Ubuntu 24.04

```
# ipcalc: calcula subxarxes de forma automàtica
sudo apt install ipcalc
ipcalc 192.168.1.0/26
ipcalc 172.16.0.0/20

# sipcalc: càlcul avançat incloent IPv6
sudo apt install sipcalc
sipcalc 192.168.1.64/26
```

4.2. VLAN

Criteri 4.10 -- Crea i configura VLAN.

Una **VLAN** (*Virtual LAN*) és una segmentació lògica d'una xarxa física en múltiples xarxes broadcast independents, implementada a escala de commutador (*switch*).

Avantatges de les VLAN

- **Seguretat**: separa grups d'usuaris (p. ex. administració i producció) sense necessitat de xarxes físiques separades.
- **Rendiment**: redueix el domini de broadcast; menys trànsit innecessari.
- **Flexibilitat**: permet reorganitzar la xarxa lògica sense moure cables.

Estàndard IEEE 802.1Q (VLAN tagging)

Les trames Ethernet s'etiqueten amb un **identificador de VLAN (VID)** de 12 bits, que permet fins a 4.094 VLAN (1 i 4095 reservades).

Tipus de ports en un commutador gestionat

- **Port d'accés (*access port*)**: connecta dispositius finals (PC, impressores). El dispositiu no sap que forma part d'una VLAN; el switch afegeix i elimina l'etiqueta de forma transparent.
- **Port troncal (*trunk port*)**: interconnecta switches o connecta un switch amb un encaminador. Transporta trànsit de múltiples VLAN simultàniament, amb l'etiqueta 802.1Q.

Configuració bàsica de VLAN en Cisco IOS (Packet Tracer)

Crear una VLAN i assignar-li un nom:

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name Administracio
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name Produccio
Switch(config-vlan)# exit
```

Assignar un port a una VLAN (port d'accés):

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

Configurar un port troncal:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
```

Verificació:

```
Switch# show vlan brief
Switch# show interfaces trunk
```

Encaminament entre VLAN (*inter-VLAN routing*)

Com que les VLAN formen dominis de broadcast separats, per comunicar dispositius de VLAN diferents cal un **encaminador** (o un switch de capa 3). La tècnica habitual és el **router-on-a-stick**: el port del router connectat al switch és un trunk, i es creen subinterfícies per a cada VLAN.

4.3. Encaminaments

Encaminament estàtic

L'**encaminament** (*routing*) és el procés pel qual un dispositiu de capa 3 (encaminador o *router*) decideix per quin camí reenviar cada paquet IP.

En l'**encaminament estàtic**, les rutes es configuren manualment per l'administrador. No s'adapten automàticament als canvis de topologia, però són simples, previsibles i consumeixen molt pocs recursos.

Conceptes de la taula d'encaminament

Cada entrada d'una taula d'encaminament conté:

Camp	Descripció
Xarxa destí	Adreça de la xarxa a la qual es vol arribar (amb màscara CIDR)
Passarel·la (*gateway*)	Adreça IP del següent salt (*next hop*) cap a la destinació
Interfície	Interfície de xarxa local per on s'envia el paquet
Mètrica	Cost de la ruta (menor = preferit quan hi ha múltiples camins)

Ruta per defecte (*default route*): `0.0.0.0/0` → captura tots els paquets sense ruta més específica. Equival a “enviar-ho tot al router de sortida a Internet”.

Gestió d'encaminament estàtic a Ubuntu 24.04

Visualitzar la taula d'encaminament:

```
ip route show
# Exemple de sortida:
# default via 192.168.1.1 dev enp3s0 proto dhcp
# 192.168.1.0/24 dev enp3s0 proto kernel scope link src 192.168.1.10
# 10.0.2.0/24 dev enp3s0 proto kernel scope link
```

Afegir una ruta estàtica temporal (es perd en reiniciar):

```
# Ruta cap a una xarxa remota a través d'una passarel·la
sudo ip route add 10.20.0.0/24 via 192.168.1.254

# Ruta per defecte
sudo ip route add default via 192.168.1.1
```

```
# Ruta cap a una xarxa directament accessible per una interfície
sudo ip route add 10.30.0.0/24 dev enp3s0
```

Eliminar una ruta:

```
sudo ip route del 10.20.0.0/24 via 192.168.1.254
sudo ip route del default
```

Ruta estàtica persistent amb Netplan (Ubuntu 24.04):

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp3s0:
      dhcp4: false
      addresses:
        - 192.168.1.10/24
      routes:
        - to: default
          via: 192.168.1.1
        - to: 10.20.0.0/24
          via: 192.168.1.254
        - to: 172.16.0.0/16
          via: 192.168.1.253
      nameservers:
        addresses: [8.8.8.8]
```

```
sudo netplan apply
```

Ruta estàtica persistent amb nmcli:

```
# Afegir ruta a una connexió existent
nmcli connection modify "nom-connexio" \
  +ipv4.routes "10.20.0.0/24 192.168.1.254"

nmcli connection up "nom-connexio"
```

Encaminament estàtic en Cisco IOS (Packet Tracer)

```
Router> enable
Router# configure terminal

! Ruta estàtica: ip route <xarxa> <màscara> <next-hop o interfície>
Router(config)# ip route 10.20.0.0 255.255.255.0 192.168.1.254

! Ruta per defecte
Router(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.1
```

```
! Verificació
Router# show ip route
Router# show ip route static
```

Quan usar encaminament estàtic

Situació	Recomanació
Xarxes petites amb topologia fixa	Adequat
Ruta de sortida a Internet (default)	Molt habitual
Xarxes grans o amb molts encaminadors	Millor usar dinàmic
Topologia que canvia sovint	Millor usar dinàmic
Connexions de resguard (*backup*)	Adequat (amb mètriques)

Encaminament dinàmic

En l'**encaminament dinàmic**, els encaminadors intercanvien informació de rutes entre ells mitjançant **protocols d'encaminament**. La taula d'encaminament s'actualitza automàticament quan canvia la topologia de la xarxa (un enllaç cau, s'afegeix una nova xarxa, etc.).

Classificació dels protocols d'encaminament

Per àmbit:

- **IGP** (*Interior Gateway Protocol*): s'usa dins d'un sistema autònom (una organització). Exemples: RIP, OSPF, EIGRP.
- **EGP** (*Exterior Gateway Protocol*): s'usa entre sistemes autònoms (entre ISPs). Exemple: BGP.

Per algorisme:

Tipus	Funcionament	Protocols
Vector de distàncies	Cada router envia la seva taula de rutes als veïns. Tria la ruta per mètrica acumulada (salts).	RIP, EIGRP
Estat d'enllaç	Cada router coneix tota la topologia. Calcula el camí més curt (Dijkstra).	OSPF, IS-IS
Path vector	Intercanvia camins complets per evitar bucles. Usat entre sistemes autònoms.	BGP

RIP (Routing Information Protocol)

Protocol de vector de distàncies, senzill i adequat per a xarxes petites.

- **Mètrica**: nombre de salts (*hops*). Màxim: **15 salts** (16 = xarxa inaccessible).
- **Actualitzacions**: cada **30 segons**, per broadcast/multicast a tots els veïns.
- **Versions**: RIPv1 (classful, sense suport CIDR), **RIPv2** (classless, suporta CIDR i VLSM).
- **Convergència**: lenta; pot trigar minuts a adaptar-se a canvis.

Configuració de RIPv2 en Cisco IOS:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.20.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit

! Verificació
Router# show ip route rip
Router# show ip protocols
Router# debug ip rip
```

4.4. Xarxes sense fil (WLAN)

Criteri 4.1 -- Identifica les característiques funcionals de les xarxes sense fils.

WLAN (*Wireless Local Area Network*) permet la connexió en xarxa entre dispositius sense necessitat de cables físics, mitjançant l'espectre radioelèctric.

Estàndard IEEE 802.11 (Wi-Fi)

La tecnologia WLAN és regulada per l'estàndard **IEEE 802.11**, que defineix les capes física i d'enllaç de dades. Des del punt de vista del sistema operatiu i dels protocols superiors (TCP/IP), una interfície Wi-Fi es comporta igual que una interfície Ethernet.

Evolució dels estàndards principals:

Estàndard	Any	Velocitat màx.	Freqüència	Notes
802.11	1997	2 Mbps	2,4 GHz	Original, obsolet
802.11b	1999	11 Mbps	2,4 GHz	Primera difusió massiva
802.11a	1999	54 Mbps	5 GHz	Incompatible amb b
802.11g	2003	54 Mbps	2,4 GHz	Compatible amb b
802.11n	2009	600 Mbps	2,4 i 5 GHz	Compatible amb b, a, g
802.11ac	2014	≥1 Gbps	5 GHz	Wi-Fi 5; MIMO millorat
802.11ax	2019	≥9,6 Gbps	2,4, 5 i 6 GHz	Wi-Fi 6/6E; OFDMA

> La **Wi-Fi Alliance** és l'organisme que certifica la interoperabilitat entre productes de fabricants diferents sota la marca Wi-Fi.

Medi de transmissió i CSMA/CA

Les WLAN utilitzen radiofreqüència (RF), un medi **compartit**. A diferència d'Ethernet, un node no pot detectar col·lisions mentre transmet, per tant, s'usa **CSMA/CA** (*Carrier Sense Multiple Access with Collision Avoidance*):

- El node escolta el medi abans de transmetre (*carrier sense*).
- Si el medi està lliure, espera un temps aleatori addicional i llavors transmet.
- El receptor envia una confirmació ACK per cada trama rebuda correctament.

Això redueix l'amplada de banda efectiu: en 802.11b (11 Mbps), el rendiment real és d'uns 5--5,5 Mbps.

Canals i freqüències

La banda de **2,4 GHz** es divideix en fins a 14 canals (a Europa, 13), cadascun amb 22 MHz d'amplada. Per evitar interferències entre punts d'accés propers, cal una separació mínima de **5 canals**. Els canals no encavalcats habituals a Europa són l'**1, 6 i 11**.

La banda de **5 GHz** ofereix molts més canals no encavalcats i menys interferències, però amb menor penetració a través de parets.

4.5. Modes de funcionament WLAN

Criteri 4.2 -- Identifica els modes de funcionament de les xarxes sense fils.

Mode infraestructura

És el mode habitual. Hi ha un o més **punts d'accés (AP)** que actuen com a concentradors centrals. Els clients es connecten a l'AP, que els proporciona accés a la xarxa cablejada i a Internet.

- L'AP actua com a dispositiu de capa 2 (equivalent a un commutador).
- Cada AP cobreix una **cel·la** (àrea de cobertura) d'uns 30--100 metres en interiors.
- Amb múltiples AP encavalcats (20--30% de superposició), s'aconsegueix **itinerància** (*roaming*) sense interrupció.

Mode ad hoc (peer-to-peer)

Comunicació directa entre dispositius sense cap AP central. Indicat per a connexions temporals entre pocs dispositius. Les limitacions principals són la compatibilitat entre targetes de fabricants diferents i l'absència d'infraestructura de xarxa.

SSID i associació

El **SSID** (*Service Set Identifier*) és el nom de la xarxa sense fil, de fins a 32 caràcters sensibles a majúscules. Tots els dispositius d'una mateixa xarxa han de tenir el mateix SSID.

Escaneig actiu: el client envia una trama *probe request* amb l'SSID buscat; l'AP respon si coincideix.

Escaneig passiu: el client escolta les trames *beacon* que l'AP emet periòdicament anunciant la seva presència i SSID.

4.6. Dispositius sense fil

Criteri 4.3 -- Instal·la adaptadors i punts d'accés sense fil.

Adaptadors de xarxa sense fil (NIC Wi-Fi)

Permeten als equips connectar-se a una WLAN. Formats habituals:

- **Integrada**: la majoria de portàtils i dispositius mòbils moderns.
- **PCIe interna**: per a equips de sobretaula.
- **USB externa**: opció fàcil d'instal·lar en qualsevol equip.
- **PCMCIA/ExpressCard**: en portàtils antics.

Instal·lació: generalment és *plug and play*; els sistemes operatius moderns inclouen controladors genèrics. En alguns casos cal instal·lar el controlador del fabricant.

Punt d'accés (AP)

Dispositiu de capa 2 que interconnecta clients Wi-Fi amb la xarxa cablejada. Converteix les trames 802.11 a format Ethernet 802.3. Els clients s'han d'**associar** a l'AP per obtenir accés a la xarxa.

Encaminador sense fil (*wireless router*)

Integra tres funcions en un sol dispositiu: **AP + commutador Ethernet + encaminador**. És el dispositiu habitual en xarxes domèstiques i petites oficines. Generalment, incorpora un servidor DHCP i permet compartir una connexió a Internet.

Antenes

Tots els dispositius Wi-Fi porten antenes integrades. En cas de necessitar major cobertura o cobertura direccional, es poden substituir o afegir antenes externes.

Tipus principals:

Tipus	Directivitat	Guany típic	Ús recomanat
Vertical/dipol	Omnidireccional	2--12 dBi	Cobertura circular (oficines, llars)
Yagi	Direccional	12--18 dBi	Enllaços de mitjana distància
Panell (*patch*)	Direccional	12--20 dBi	Interiors i exteriors
Parabòlica	Molt direccional	Fins a 27 dBi	Enllaços de llarga distància

Propietats a tenir en compte: impedància (normalment 50 Ω), amplada de banda, patró de radiació, guany (en dB) i polarització.

4.7. Instal·lació i configuració bàsica

Criteris 4.4, 4.5, 4.6 -- Configura modes de funcionament, comprova connectivitat, instal·la programari.

Procediment d'instal·lació d'un punt d'accés

Es recomana un procés **incremental**:

1. Instal·lar físicament el punt d'accés i connectar-lo a la xarxa cablejada.
2. Accedir a la interfície web de configuració (normalment a `192.168.1.1`).
3. Configurar l'SSID i el canal (sense seguretat inicialment).
4. Connectar un client sense fil i verificar que obté adreça IP per DHCP.
5. Verificar connectivitat (`ping` a la passarel·la i a Internet).
6. Activar la seguretat (WPA2).
7. Verificar que el client es reconnecta correctament amb les credencials de seguretat.

Paràmetres bàsics de configuració de l'AP

Accedint a la interfície web de l'AP (ex. `http://192.168.1.1`, usuari/contrasenya per defecte del fabricant):

Configuració de la xarxa (LAN/DHCP): - Adreça IP de l'AP dins la xarxa local. - Activació/desactivació del servidor DHCP integrat. - Rang d'adreces IP que oferirà el DHCP.

Configuració sense fil: - **SSID**: nom de la xarxa. Canviar el valor per defecte. - **Canal**: triar un canal lliure (en 2,4 GHz, preferiblement 1, 6 o 11). - **Mode de xarxa**: seleccionar el mode compatible amb els dispositius (Mixed, B/G/N, etc.). - **Banda de ràdio**: 20 MHz per a 802.11b/g, 40 MHz per a 802.11n. - **SSID broadcast**: si s'oculta l'SSID o es difon públicament.

Contrasenya d'administrador: canviar sempre la contrasenya per defecte de l'AP.

Verificació de connectivitat

Un cop instal·lat i configurat, s'ha de verificar:

```
# Mostrar configuració de xarxa (Ubuntu 24.04)
ip addr show
ip route show

# Verificar connectivitat capa 3
ping -c 4 192.168.1.1   # passarel·la
ping -c 4 8.8.8.8       # Internet (IP)
ping -c 4 www.google.com # Internet (DNS)

# Informació de la connexió Wi-Fi (Ubuntu 24.04)
nmcli device wifi list           # xarxes disponibles
nmcli connection show --active   # connexions actives
iw dev wlp2s0 link               # detalls de l'associació actual
iw dev wlp2s0 station dump       # estadístiques de la connexió
```

> **Nota:** `iwconfig` forma part del paquet `wireless-tools`, que a Ubuntu 24.04 **no està instal·lat per defecte**. L'eina moderna equivalent és `iw`. Si cal, es pot instal·lar amb: `sudo apt install wireless-tools`

En Windows: `ipconfig /all`, `ping`, `tracert`.

4.8. Seguretat en xarxes sense fil

Criteri 4.9 -- Aplica mecanismes bàsics de seguretat.

Amenaces específiques de les WLAN

Una xarxa sense fil és accessible per a qualsevol persona dins el radi de cobertura de l'AP. Amb una targeta Wi-Fi i programari adequat (*sniffer*, com Wireshark), un atacant pot capturar el trànsit sense necessitat d'accés físic a la xarxa.

Evolució dels protocols de seguretat Wi-Fi

Protocol	Any	Xifratge	Autenticació	Estat
WEP	1997	RC4 (40/128 bits)	Clau compartida	**Insegur**, no usar
WPA	2003	TKIP	PSK o RADIUS/EAP	Deprecat
WPA2	2004	AES (CCMP)	PSK o RADIUS/EAP	**Recomanat**
WPA3	2018	AES (256 bits)	SAE o RADIUS/EAP	Recomanat en maquinari modern

> Des del **març de 2006**, tots els dispositius Wi-Fi certificats han de suportar WPA2.

Modes d'autenticació WPA2

- **WPA2-Personal (PSK):** utilitza una contrasenya (*pre-shared key*) d'entre 8 i 63 caràcters, compartida per tots els clients. Adequat per a llars i petites empreses.
- **WPA2-Enterprise:** utilitza un servidor **RADIUS** per a l'autenticació individual de cada usuari (protocol EAP). Cada usuari té les seves pròpies credencials. Recomanat en entorns corporatius.

Paràmetres de configuració WPA2-Personal a l'AP: - Mode de seguretat: `WPA2-Personal` (o `PSK2`) - Tipus de xifratge: **AES** (més robust que TKIP) - Clau compartida (*Pre-shared Key*): mínim 12 caràcters, combinant majúscules, minúscules, números i símbols. - Renovació de clau (*Key Renewal*): interval de renovació de la clau de sessió.

Mesures addicionals de seguretat

Ocultació de l'SSID: l'AP no difon el nom de la xarxa. Els clients han de conèixer l'SSID per connectar-se. *Limita la comoditat, però no és una protecció real*, ja que l'SSID és fàcilment descobert amb eines de captura de paquets.

Filtratge per adreça MAC: l'AP manté una llista blanca (o negra) d'adreces MAC autoritzades. *No és una protecció robusta*, ja que les adreces MAC es poden falsificar (*MAC spoofing*) fàcilment.

Recomanació: usar sempre **WPA2** (o WPA3) com a mesura principal, i complementar-la amb l'ocultació de l'SSID i el filtratge MAC com a capes addicionals.

Altres bones pràctiques:

- Canviar la contrasenya d'administrador de l'AP (mai deixar la de fàbrica).
- Actualitzar el firmware de l'AP.
- Reduir la potència de transmissió per minimitzar la cobertura fora de l'edifici.
- Situar l'AP allunyat del perímetre de l'edifici.

RA5 -- Resolució d'incidències d'una xarxa d'àrea local

Criteri general (5): Manté una xarxa local interpretant recomanacions dels fabricants de maquinari o programari i establint la relació entre disfuncions i les seves causes.

5.1. Estratègies de diagnòstic

Criteri 5.1/5.2 -- Identifica incidències i comportaments anòmals; determina si la disfunció és de maquinari o programari.

Metodologia de resolució de problemes

La resolució d'incidències ha de seguir un **procediment sistemàtic**, treballant per capes del model OSI de baix a dalt (o a l'inrevés, depenent dels símptomes):

De baix a dalt (bottom-up): es comença verificant la capa física i es puja progressivament. Indicat quan es desconeix l'origen del problema.

De dalt a baix (top-down): es comença des de l'aplicació. Indicat quan els símptomes apunten a una capa concreta.

Divideix i venceràs (*divide and conquer*): es comença per una capa intermèdia (normalment la capa 3, xarxa) i es puja o baixa en funció del resultat.

Fases del procés de resolució

1. **Identificar el problema**: recollir informació dels usuaris i del sistema.
2. **Establir una teoria de causa probable**: basant-se en els símptomes.
3. **Provar la teoria**: dur a terme proves per confirmar o descartar.
4. **Establir un pla d'acció**: decidir la solució.
5. **Implementar la solució**: aplicar els canvis.
6. **Verificar el funcionament**: comprovar que el problema s'ha resolt.
7. **Documentar**: elaborar l'informe d'incidència.

Paràmetres de rendiment a monitorar

- **Amplada de banda (*bandwidth*)**: capacitat nominal de la connexió.
- **Rendiment (*throughput*)**: velocitat de transferència real.
- **Latència**: temps de resposta (mesurable amb `ping`).
- **Pèrdua de paquets**: percentatge de paquets que no arriben.
- **Jitter**: variació en la latència (crític en VoIP i streaming).

5.2. Tipus d'incidències

Criteri 5.2 -- Identifica si la disfunció és deguda al maquinari o al programari.

Incidències físiques (maquinari / capa 1)

Símptoma	Causa probable
Cap connectivitat, LED apagat	Cable desconnectat, port del switch apagat
Connectivitat intermitent	Cable deteriorat, connector mal crimpat
Velocitat molt inferior a l'esperada	Cable de categoria inadequada, NIC danyada
Senyal Wi-Fi dèbil	Distància excessiva, obstacles, interferències
Dispositiu no reconegut	Controlador no instal·lat, maquinari defectuós

Verificació física:

- Revisar que tots els cables estan ben connectats.

- Observar els LEDs dels dispositius de xarxa.
- Provar amb un cable diferent (comprovador de cables).
- Verificar que els dispositius estan alimentats.

Incidències lògiques (programari / configuració)

Símptoma	Causa probable
Adreça IP 169.254.x.x	El client no obté adreça DHCP
No es pot fer ping a la passarel·la	Adreça IP incorrecta o sense passarel·la
Ping a IP funciona, però no a nom	Error de resolució DNS
Connectivitat parcial	Firewall, filtratge, VLAN mal configurada
No es pot connectar a Wi-Fi	Credencials incorrectes, mode de seguretat incompatible
Velocitat Wi-Fi baixa	Canal congestionat, interferències

5.3. Monitoratge de xarxes

Criteri 5.3/5.4 -- Monitora senyals visuals dels dispositius; verifica protocols de comunicació.

Senyals visuals dels dispositius

Els dispositius de xarxa disposen de LEDs indicadors que donen informació de l'estat:

LED	Estat	Significat
Power (PWR)	Verd continu	Dispositiu encès i operatiu
Power (PWR)	Apagat	Sense alimentació
Link/Speed	Verd continu	Connexió establerta
Link/Speed	Apagat	No hi ha connexió física
Activity (ACT)	Parpelleig verd	Trànsit de dades actiu
Wi-Fi	Verd continu	Xarxa sense fil activa
Wi-Fi	Apagat	Xarxa sense fil desactivada

Verificació de protocols de comunicació

Per verificar l'estat dels protocols a cada capa:

Capa física i d'enllaç (capa 1-2):

```
ip link show                    # estat de totes les interfícies
ip -s link show enp3s0          # estadístiques detallades (errors,
 ↪  paquets)
ethtool enp3s0                  # velocitat, duplex, estat de l'enllaç
 ↪  (Ethernet)
iw dev wlp2s0 link             # informació de l'associació Wi-Fi actual
```

```
iw dev wlp2s0 station dump     # estadístiques Wi-Fi (senyal,
 ↪  velocitat, paquets)
```

Capa de xarxa (capa 3):

```
ip addr show                   # adreces IP assignades a totes les
 ↪  interfícies
ip route show                  # taula d'encaminament
ip neigh show                  # taula ARP/NDP (substitueix arp -n)
ping -c 4 192.168.1.1          # test de connectivitat capa 3
ping -6 -c 4 fe80::1%enp3s0   # test de connectivitat IPv6 local
 ↪  d'enllaç
```

Capa de transport i aplicació (capes 4-7):

```
ss -tulnp                      # ports TCP/UDP en escolta amb nom del
 ↪  procés
ss -tp                         # connexions TCP establertes amb PID
```

> **Nota:** `netstat` forma part del paquet `net-tools`, que a Ubuntu 24.04 **no està instal·lat per defecte**. L'eina moderna i recomanada és `ss` (del paquet `iproute2`, sempre present).

5.4. Eines de diagnòstic

Criteri 5.4/5.5 -- Eines de diagnòstic; localitza la causa de la disfunció.

Comandes de diagnòstic

`ping` -- Comprova connectivitat entre dos nodes enviant paquets ICMP Echo Request:

```
ping -c 4 192.168.1.1          # test de connectivitat bàsic (4
 ↪  paquets)
ping -c 4 8.8.8.8              # connectivitat cap a Internet
ping -6 -c 4 ::1              # ping IPv6 loopback (Ubuntu 24.04: -6,
 ↪  no ping6)
```

Informació que proporciona: temps de resposta (ms), pèrdua de paquets (%).

`traceroute` / `tracert` -- Mostra el camí dels paquets fins a la destinació, passarel·la a passarel·la:

```
traceroute 8.8.8.8             # Linux (cal instal·lar: sudo apt
 ↪  install traceroute)
traceroute -6 2001:4860:4860::8888  # traçat IPv6
tracert 8.8.8.8                # Windows
```

Útil per identificar on es talla la comunicació.

`nslookup` / `dig` / `resolvectl` -- Resolució de noms DNS:

```
resolvectl query ioc.cat       # consulta DNS amb systemd-resolved
 ↪  (Ubuntu 24.04)
resolvectl status             # estat del resolver DNS per interfície
dig ioc.cat                    # consulta DNS detallada
dig @8.8.8.8 ioc.cat           # forçar un servidor DNS concret
nslookup ioc.cat               # consulta simple (compatible
 ↪  Windows/Linux)
```

`ip` -- Mostra i gestiona la configuració de xarxa (substitueix `ifconfig`):

```
ip addr show                   # adreces IP de totes les interfícies
ip addr show enp3s0            # adreça IP d'una interfície concreta
ip route show                  # taula d'encaminament
ip link show                   # estat dels adaptadors (UP/DOWN, MAC)
```

> **Ubuntu 24.04:** `ifconfig` forma part del paquet `net-tools`, no instal·lat per defecte. Cal usar `ip addr show`.

`ip neigh` -- Consulta la taula ARP/NDP (associació IP ↔ MAC):

```
ip neigh show                 # mostra la taula ARP (IPv4) i NDP (IPv6)
ip neigh flush dev enp3s0      # buida la caché ARP d'una interfície
```

> **Ubuntu 24.04:** `arp` forma part de `net-tools`. L'eina moderna equivalent és `ip neigh`.

`ss` -- Connexions de xarxa actives i ports en escolta:

```
ss -tulnp                     # ports TCP/UDP en escolta amb PID i nom
 ↪  del procés
ss -tp                         # connexions TCP actives
ss -s                          # resum estadístic
```

`nmap` -- Escàner de xarxa; descobreix hosts actius i ports oberts:

```
sudo apt install nmap          # instal·lació si no és present
nmap -sn 192.168.1.0/24        # descobrir hosts actius a la xarxa
nmap 192.168.1.10              # escaneig de ports d'un host
nmap -sV 192.168.1.10          # detectar versions dels serveis
```

`tcpdump` / Wireshark -- Captura i anàlisi de paquets de xarxa:

```
sudo apt install tcpdump       # instal·lació si cal
sudo tcpdump -i enp3s0 -n      # captura trànsit de la interfície
 ↪  enp3s0
sudo tcpdump -i wlp2s0 -n      # captura trànsit Wi-Fi
sudo tcpdump -i enp3s0 host 192.168.1.10  # filtra per adreça IP
sudo tcpdump -i enp3s0 -w captura.pcap    # desa la captura per
 ↪  analitzar amb Wireshark
```

Wireshark és la versió gràfica; permet visualitzar i analitzar els protocols de cada trama en detall. Instal·lació: `sudo apt install wireshark`.

Eines específiques per a WLAN (Ubuntu 24.04)

Eina	Paquet	Descripció
`nmcli device wifi`	`network-manager` (instal·lat per defecte)	Gestió completa de Wi-Fi: llistar, connectar, desconnectar
`iw`	`iw` (instal·lat per defecte)	Eina moderna per a interfícies Wi-Fi: stats, scan, link
`iwconfig`	`wireless-tools` (**no per defecte**)	Eina antiga; usar `iw` o `nmcli`
`iwlist scan`	`wireless-tools` (**no per defecte**)	Escaneig de xarxes; substituït per `nmcli device wifi list`
`wpa_cli`	`wpasupplicant`	Gestió del dimoni wpa_supplicant
`rfkill`	`rfkill` (instal·lat per defecte)	Activar/desactivar ràdios Wi-Fi i Bluetooth

```
# Exemples pràctics amb Ubuntu 24.04
nmcli device wifi list                    # llistar xarxes disponibles
nmcli device wifi connect "SSID" password "clau"  # connectar a una
 ↪  xarxa
nmcli connection show --active             # connexions actives
iw dev wlp2s0 scan                         # escaneig de xarxes (baix
 ↪  nivell)
iw dev wlp2s0 link                        # estat de l'associació actual
rfkill list                               # estat dels dispositius ràdio
rfkill unblock wifi                          # desbloquejar Wi-Fi si
 ↪  estava bloquejada
```

Eines físiques i d'anàlisi de l'espectre:

- **Comprovadors de cables** (*cable tester*): verifica la continuïtat i el crimpat dels cables Ethernet.
- **Analitzadors Wi-Fi** (apps mòbils com Wi-Fi Analyzer, o `nmcli`/`iw` en terminal): mostren els canals ocupats i la potència del senyal de les xarxes properes.

5.5. Resolució i documentació

Criteris 5.5, 5.6, 5.7, 5.8 -- Localitza la causa; restitueix el funcionament; soluciona disfuncions de programari; elabora l'informe.

Resolució d'incidències de maquinari

Quan la causa és maquinari defectuós o deteriorat, les accions habituals són:

- Substituir el cable Ethernet (provar primer amb un cable conegut com a bo).
- Substituir la targeta de xarxa (NIC) del dispositiu afectat.
- Substituir el port del switch (canviar el cable a un port diferent).
- Substituir el switch o el punt d'accés si el problema afecta múltiples ports.
- Actualitzar o reinstal·lar el controlador (*driver*) de la NIC.

Resolució d'incidències de programari / configuració

Problema	Solució (Ubuntu 24.04)
Adreça IP incorrecta	`nmcli connection modify` o editar Netplan i `sudo netplan apply`
DNS no funciona	`resolvectl status`; configurar DNS a Netplan o via `nmcli`
No pot connectar a Wi-Fi	`nmcli device wifi list`; verificar SSID, contrasenya i mode de seguretat
VLAN mal configurada	Revisar assignació de ports i VID al switch
Firewall bloqueja la connexió	`sudo ufw status`; revisar i modificar les regles `ufw`
Servei de xarxa aturat	`sudo systemctl restart NetworkManager`
Adreça 169.254.x.x (APIPA)	`nmcli device reapply enp3s0` o revisar el servidor DHCP
Wi-Fi bloquejada per programari	`rfkill list`; `rfkill unblock wifi`
Firmware desactualitzat	Actualitzar el firmware de l'AP; `sudo apt upgrade` per als drivers

Reinstal·lació / reconfiguració de serveis de xarxa (Ubuntu 24.04):

```
# Reiniciar NetworkManager
sudo systemctl restart NetworkManager

# Reiniciar una interfície de xarxa
sudo ip link set enp3s0 down && sudo ip link set enp3s0 up

# Desconnectar i reconnectar una connexió gestionada per nmcli
nmcli connection down "nom-connexio"
nmcli connection up "nom-connexio"

# Renovar l'adreça DHCP (via nmcli, mètode recomanat a Ubuntu 24.04)
nmcli device reapply enp3s0

# Aplicar canvis de Netplan (configuració persistent)
sudo netplan apply

# Netejar la caché DNS de systemd-resolved
sudo resolvectl flush-caches
resolvectl statistics
```

> **Nota:** A Ubuntu 24.04, `dhclient` i `ifup`/`ifdown` **no estan instal·lats per defecte**. La gestió DHCP la fa directament NetworkManager o systemd-networkd.

Gestió del tallafoc amb `ufw` (Ubuntu 24.04):

```
sudo ufw status verbose        # estat del tallafoc
sudo ufw enable                # activar el tallafoc
sudo ufw allow 22/tcp          # permetre SSH
sudo ufw deny 23/tcp           # bloquejar Telnet
sudo ufw allow from 192.168.1.0/24  # permetre tota la xarxa local
sudo ufw reset                 # restablir totes les regles
```

Ubuntu 24.04 inclou `ufw` (*Uncomplicated Firewall*) com a front-end simplificat per a `nftables` (que ha substituït `iptables` com a backend del nucli Linux).

Elaboració de l'informe d'incidències

Documentar les incidències és fonamental per al manteniment i la millora de la xarxa. Un informe d'incidència ha d'incloure:

1. **Data i hora** de detecció i resolució.
2. **Descripció de la incidència**: símptomes observats, dispositius i usuaris afectats.
3. **Classificació**: incidència física o lògica; gravetat (crítica, alta, mitjana, baixa).
4. **Anàlisi i diagnòstic**: passos seguits, eines utilitzades i proves realitzades.
5. **Causa arrel identificada**: descripció clara de l'origen del problema.
6. **Solució aplicada**: accions realitzades per resoldre la incidència.
7. **Verificació**: comprovació que la solució ha estat efectiva.
8. **Recomanacions**: mesures preventives per evitar que es repeteixi.

Eines de documentació i diagramació de xarxes:

- **draw.io / diagrams.net**: eina gratuïta per crear diagrames de xarxa.
- **Cisco Packet Tracer**: simulació i documentació de topologies.
- **LibreOffice Draw / Impress**: per a documentació en entorns d'oficina.
- **Markdown / wikis internes**: per a documentació tècnica estructurada.

Versions d'aquest document

- HTML - 0225.html
- PDF - 0225.pdf
- ODT - 0225.odt
- MD - 0225.md