
Manual de referència de Cisco IOS

Principals conceptes i comandes per realitzar les PAC i pràctica

PID_00262484

Àlex Macia Pérez
Eduard Lara Ochoa

Temps mínim de dedicació recomanat: 7 hores



Àlex Macia Pérez

Professor col·laborador de la UOC.

Eduard Lara Ochoa

Professor col·laborador de la UOC.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Joan Melià Seguí (2019)

Primera edició: febrer 2019
© Àlex Macia Pérez, Eduard Lara Ochoa
Tots els drets reservats
© d'aquesta edició, FUOC, 2019
Av. Tibidabo, 39-43, 08035 Barcelona
Disseny: Manel Andreu
Realització editorial: Oberta UOC Publishing, SL

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars del copyright.

Índex

Introducció	5
1. Introducció a Cisco IOS	7
1.1. Accés a l'IOS	7
1.2. Modes d'operació	10
1.3. Inspecció de l'estat	11
1.4. Ajuda a l'entrada de comandes	12
1.5. Arquitectura del sistema	16
1.6. Sistema de fitxers	19
2. Configuració de commutadors a Cisco IOS	23
2.1. Seguretat i accés remot	28
2.2. Cas pràctic	32
2.3. Configuració de commutadors: VLAN	34
2.4. Configuració de commutadors: taula MAC	39
3. Configuració d'encaminadors a Cisco IOS	42
3.1. Estructura d'un encaminador (<i>router</i>)	42
3.1.1. Consulta de l'estat de l'encaminador (comanda <i>show</i>)	42
3.2. Configuració d'encaminadors amb Cisco IOS	43
3.2.1. Configuració d'interfícies	43
3.2.2. Configuració d'interfícies Ethernet	44
3.2.3. Configuració d'interfícies sèrie	45
3.2.4. Taula ARP	46
3.3. Encaminament estàtic	48
3.3.1. Ruta per defecte (Default Gateway)	52
3.4. Encaminament entre VLANS	53
3.4.1. Característiques del VLAN Trunking Protocol	55
3.4.2. Estàndard IEEE-802.1Q	56
3.4.3. Exemple d'encaminament entre VLANS	56
3.5. Configuració dels protocols d'encaminament	59
3.5.1. Distància administrativa d'un protocol d'encaminament	60
3.5.2. Encaminament amb OSPF	61
3.5.3. Encaminament amb EIGRP	69
3.6. Xarxes IPv6	75
3.6.1. Tipus d'adreces IPv6	76
3.6.2. Exemple: generació d'adreces <i>Link Local</i>	77
3.6.3. Exemple de configuració d'interfícies Ethernet amb adreces <i>Global Unicast</i>	79

3.6.4.	Exemple d'adreçament estàtic a IPv6	80
3.6.5.	Exemple d'encaminament entre VLANs amb IPv6	83
3.7.	Encaminament amb OSPFv3	87
3.7.1.	Exemple: encaminament amb OSPFv3	87
Bibliografia		91

Introducció

Aquest mòdul serveix com una introducció a l'operació del sistema Cisco IOS, emprat pels dispositius Cisco (encaminadors, commutadors). Si bé aquest sistema operatiu és complex i amb moltes opcions, els conceptes que es presenten aquí són els més bàsics per poder seguir l'assignatura partint des de zero.

Dispositius que es consideren en aquest document

Els exemples de comandes i configuracions que es presenten en aquest mòdul s'han realitzat principalment amb el programa de simulació de xarxes Packet Tracer. És una eina desenvolupada per Cisco i és part dels recursos del seu programa de formació Network Academy.

A l'ajuda del programa podeu trobar, entre altres informacions, la referència completa a les comandes de l'IOS disponibles. Només cal que accediu als continguts de l'ajuda, a Configuring Devices, apartats Router IOS, Router IOS 15 i Switch IOS.

En aquest mòdul ens centrarem principalment en el funcionament de l'IOS que implementen commutadors i encaminadors. Però més enllà del maquinari específic, totes les funcionalitats que es descriuen en el present mòdul apliquen al conjunt de dispositius que treballen sobre un sistema IOS.

Finalment també és important posar de manifest que l'IOS ha esdevingut un estàndard *de facto* per al programari dels dispositius de xarxa i la majoria de les empreses del sector implementen sistemes molt similars, per tant, els següents continguts tenen un abast prou significatiu en relació amb l'extensa varietat de maquinari disponible al mercat.

1. Introducció a Cisco IOS

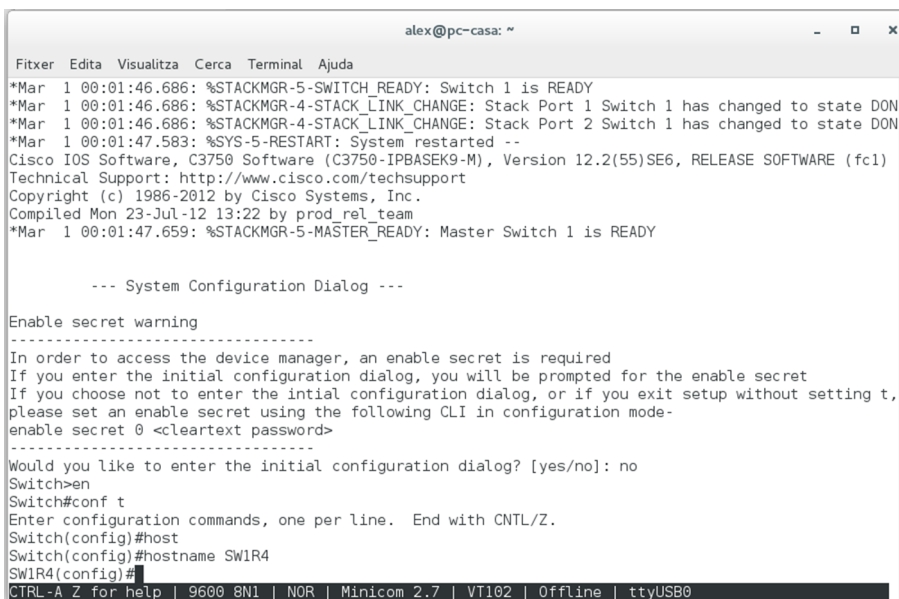
Aquest apartat resumeix l'accés i els modes d'operació de Cisco IOS. A més es fa una breu introducció a l'arquitectura del sistema i al sistema de fitxers dels dispositius Cisco.

1.1. Accés a l'IOS

Cisco IOS (IOS, sigles que fan referència a Internetwork Operating System) és el nom comercial del sistema que integren els dispositius de xarxa de Cisco. Es configura per mitjà d'una interfície de línia de comandes (CLI - Command Line Interface), que diferencia diversos nivells o modes de privilegi i funcionalitat.

El conjunt de comandes disponibles a cada mode és diferent i l'usuari ha de canviar de mode depenent del que vulgui fer. A la figura 1 es mostra un exemple de la interfície de línia de comandes de l'IOS.

Figura 1. Configuració des del CLI



```
alex@pc-casa: ~
Fitxer Edita Visualitza Cerca Terminal Ajuda
*Mar 1 00:01:46.686: %STACKMGR-5-SWITCH_READY: Switch 1 is READY
*Mar 1 00:01:46.686: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 1 Switch 1 has changed to state DON
*Mar 1 00:01:46.686: %STACKMGR-4-STACK_LINK_CHANGE: Stack Port 2 Switch 1 has changed to state DON
*Mar 1 00:01:47.583: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C3750 Software (C3750-IPBASEK9-M), Version 12.2(55)SE6, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Mon 23-Jul-12 13:22 by prod_rel_team
*Mar 1 00:01:47.659: %STACKMGR-5-MASTER_READY: Master Switch 1 is READY

--- System Configuration Dialog ---

Enable secret warning
-----
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the initial configuration dialog, or if you exit setup without setting t,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
-----
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname SW1R4
SW1R4(config)#
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyUSB0
```

Hi ha diverses maneres d'accedir a l'IOS per configurar els diferents dispositius. Les més habituals són:

- Connexió directa per **consola**.
- Accés **remot** per xarxa.

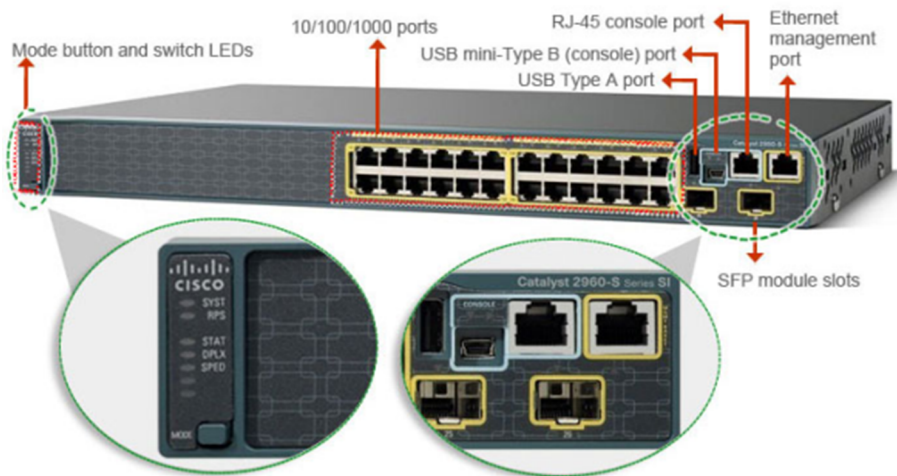
La primera vegada que es configura un commutador o un encaminador, cal connectar-s'hi directament fent servir un **cable de consola**. Tots els dispositius gestionats inclouen un o més ports de gestió, també anomenats ports de consola o *out-of-band*.

Els ports de consola sempre estan separats dels ports de xarxa i indicats clarament. Els podem trobar al panell frontal, al posterior o fins i tot excepcionalment al lateral, i poden tenir diferents formats: **RJ45** (consola o Ethernet de gestió), **RS-232 o DB9**, **USB mini (tipus B)**. A la figura 2 es mostren alguns exemples de ports de gestió d'un commutador.

Out-of-band

Out-of-band, o fora de banda, és un terme heretat de la nomenclatura de les telecomunicacions i fa referència a ports que treballen a part de la banda de freqüències per on es transmeten les dades i la veu.

Figura 2. Panell frontal d'un commutador sèrie CISCO Catalyst 2960



Font: Cisco

La connexió de consola sempre està disponible, encara que la configuració no sigui correcta, estigui incompleta o fins i tot si l'IOS no es pot carregar. És per això que s'utilitza també durant els procediments de recuperació de les diferents situacions de desastre, si l'arxiu de sistema està malmès o no es troba durant el procés d'arrencada, o si hem perdut o oblidat les contrasenyes i cal recuperar l'accés o restablir la configuració de fàbrica.

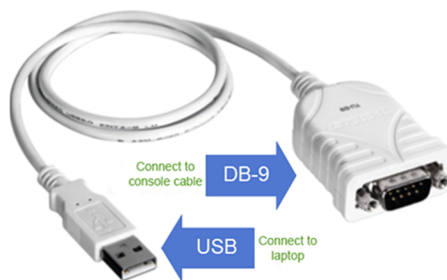
Per completar la connexió física es connecta un cable de consola des del port de gestió del dispositiu que es vol configurar fins al port sèrie d'un ordinador (COM1, COM2...), o alternativament a un port USB fent servir algun adaptador de port sèrie a USB. A les figures 3 i 4 es mostren exemples d'aquests elements.

Figura 3. Cable de consola, sèrie DB-9 a consola RJ-45



Font: https://dcloud-cms.cisco.com/help/connect_console

Figura 4. Adaptador port sèrie (DB-9) a USB



Font: https://dcloud-cms.cisco.com/help/connect_console

Per gestionar les comunicacions pel cable de consola cal algun programa d'emulació de terminal sèrie com per exemple: PuTTY (Windows), minicom (Linux), Kermit (Unix), Z-Term (MacOS). A continuació es mostra la configuració del port sèrie «/dev/ttyS0» des del programa minicom. Aquests són els paràmetres habituals, tot i que la velocitat pot variar entre diferents fabricants:

```

Bits per segon (Baud)      : 9600
Bits de dades              : 8
Paritat                    : no
Bits de parada             : 1
Control de flux            : no

```

D'altra banda, també es pot accedir a l'IOS **per xarxa** fent servir algun protocol de connexió remota, normalment telnet o ssh. Aquest últim funciona sobre comunicacions xifrades i és el mètode recomanat.

A diferència de l'accés per consola que requereix estar físicament al costat del dispositiu, aquest procediment té l'avantatge que es pot fer servir des de qualsevol terminal amb accés a la mateixa xarxa d'aquell, sempre que la configuració de seguretat de la xarxa ho permeti, que el dispositiu tingui establerta la configuració de xarxa i els serveis d'accés remot estiguin actius i correctament configurats.

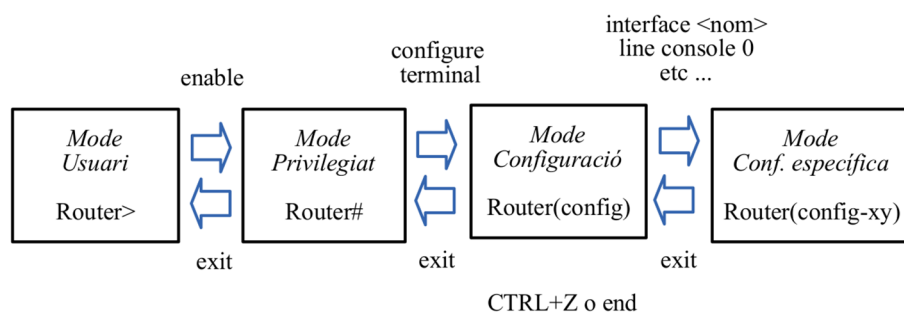
L'accés remot és, per tant, opcional i no sempre estarà disponible o serà necessari configurar-lo. Cal no oblidar que els commutadors no requereixen adreçament de xarxa (adreça IP i porta d'enllaç) per realitzar la seva funció,

o que el fet d'estar disponible remotament suposa un major risc de seguretat. Més endavant es detalla la configuració de l'IOS per permetre l'accés remot tant per telnet com xifrada per ssh.

1.2. Modes d'operació

Un dels aspectes més importants de l'IOS és que aquest s'estructura en un seguit de modes d'operació, als quals s'accedeix de manera seqüencial, per nivells. Depenent del mode d'operació actual, les comandes que es poden executar canvien totalment. En tot moment es pot saber en quin mode estem per la forma del símbol del sistema (*prompt*). L'usuari pot accedir a cadascun dels modes o tornar a un mode anterior, tal com es mostra a la figura 5.

Figura 5. Modes d'operació i comandes de navegació entre modes



El mode usuari és l'inicial en entrar al dispositiu. Només permet executar unes poques comandes de consulta per visualitzar el seu estat. No l'usareu gairebé mai. Es pot passar a mode privilegiat amb la comanda `enable`.

El mode privilegiat permet visualitzar l'estat del dispositiu amb més detall i gestionar els sistemes de fitxers. En ser el punt d'entrada al control del dispositiu, normalment es protegeix amb una contrasenya. També permet executar les comandes `ping`, `telnet` i `ssh`. Es pot avançar al mode de configuració amb la comanda `configure terminal`.

El mode de configuració només permet executar comandes que canvien la configuració general del dispositiu. Per exemple, el nom del *host* o el seu servidor DNS.

Es pot entrar a mode interfície amb la comanda `interface <nom interfície>`. El nom ha de ser complet i accepta espais (per exemple: `interface fastEthernet 0/0`). El mode interfície permet configurar una interfície de xarxa concreta. Per exemple, l'adreça IP. Hi ha un mode associat a cada interfície concreta del dispositiu.

Per retrocedir al mode anterior, s'usa la comanda `exit`. És possible retrocedir directament a mode privilegiat amb `CTRL+Z` o amb la comanda `end`.

Exemple

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet 0/0
Router(config-if)#exit
Router(config)#exit
Router#exit
```

1.3. Inspecció de l'estat

La utilitat principal del mode privilegiat és poder inspeccionar l'estat del dispositiu mitjançant variacions de la comanda `show`. Aquesta comanda té moltes opcions i permet visualitzar dades de tota mena.

Algunes opcions d'utilitat o que es fan servir sovint són:

- `show running-config`: mostra la configuració en execució.
- `show ip interface brief`: mostra un resum de l'estat de les interfícies.
- `show interfaces`: mostra informació detallada de les interfícies de xarxa.
- `show interfaces <nom interfície>`: mostra informació detallada d'una interfície concreta.
- `show cdp neighbors`: permet llistar dispositius Cisco veïns connectats.

Exemple

```
SWP1>
SWP1>
SWP1>enable
SWP1#show running-config
Building configuration...

Current configuration : 2567 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWP1
!
!
```

```
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
  
RINT>enable  
RINT#show ip interface brief  


| Interface             | IP-Address  | OK? | Method | Status                | Protocol |
|-----------------------|-------------|-----|--------|-----------------------|----------|
| GigabitEthernet0/0    | unassigned  | YES | unset  | up                    | up       |
| GigabitEthernet0/0.4  | 192.168.4.1 | YES | manual | up                    | up       |
| GigabitEthernet0/0.10 | 172.10.0.1  | YES | manual | up                    | up       |
| GigabitEthernet0/0.20 | 172.20.0.1  | YES | manual | up                    | up       |
| GigabitEthernet0/0.99 | unassigned  | YES | unset  | up                    | up       |
| GigabitEthernet0/1    | unassigned  | YES | unset  | administratively down | down     |
| Serial0/0/0           | unassigned  | YES | unset  | up                    | down     |
| Serial0/0/1           | unassigned  | YES | unset  | administratively down | down     |
| Vlan1                 | unassigned  | YES | unset  | administratively down | down     |


```

1.4. Ajuda a l'entrada de comandes

Les comandes poden tenir moltes opcions i es construeixen ordenadament. Les opcions disponibles a cada moment depenen de l'opció immediatament anterior i les possibilitats es despleguen per tant en forma d'arbre.

Així, les comandes resultants es componen d'un seguit d'opcions interdependents i que no poden intercanviar la seva posició. Per sort l'IOS incorpora un seguit d'utilitats per facilitar-ne l'ús. Per exemple, l'IOS disposa dels mecanismes següents per facilitar l'entrada de comandes:

- Introduint ? es pot accedir a l'ajuda. Si es fa a mitja comanda, mostra l'ajuda vinculada a les opcions entrades fins al moment (per exemple: `show ip ?`).
- La tecla de tabulador permet autocompletar la introducció d'una comanda.
- No cal introduir el text complet del nom d'una comanda o opció. Si no hi ha ambigüitat en la comanda entrada, el sistema ho resol automàticament (per exemple: en lloc de `configure terminal` es pot escriure `conf t`, o en comptes de `show running-config` es pot escriure `sh run`).

- La comanda `do` permet executar comandes del mode privilegiat des de qualsevol mode de configuració, general o específic. De manera que ens estalvia haver de canviar de mode.

L'ajuda que es mostra fent servir `?` a continuació de cada opció desplega una llista indentada de dues columnes amb el conjunt de noves opcions disponibles. A la primera columna indica el valor concret de l'opció o dels valors possibles, i a la segona columna una descripció breu d'aquesta.

A més, segueix una nomenclatura que també facilita identificar els valors de les opcions disponibles a mesura que es construeix cada comanda.

Si només indica un text o caràcter sense indentació i sense afegir cap descripció, significa que és l'única opció possible:

1) `<0-9>` vol dir un rang de valors possibles, en aquest cas un enter entre 0 i 9.

2) `WORD` fa referència a una paraula qualsevol, sense espais.

3) `LINE` vol dir que es pot escriure una frase amb espais, si s'escau.

4) Els diferents formats d'adreces: MAC, IPv4 i IPv6.

- **adreça IPv4:** A.B.C.D
- **adreça MAC:** H.H.H
- **link-local:** X:X:X:X::X adreça IPv6
- **prefix IPv6:** X:X:X:X::X/`<0-128>`

5) `<cr>` fa referència a *carriage return* i indica que **la comanda està completa** i es pot executar. Mentre no aparegui aquesta opció significa que la comanda necessita més opcions.

L'ús de majúscules també permet diferenciar d'un sol cop d'ull aquelles opcions que són variables.

Exemple

```
Router(config)#enable password ?
  7      Specifies a HIDDEN password will follow
LINE    The UNENCRYPTED (cleartext) 'enable' password
level   Set exec level password

Router(config)#interface GigabitEthernet ?
  <0-9>  GigabitEthernet interface number
Router(config)#interface Giga?
GigabitEthernet
Router(config)#interface Giga ?
```

```

    <0-9> GigabitEthernet interface number
Router(config)#interface Giga 0?
/
Router(config)#interface Giga 0/?
    <0-24> GigabitEthernet interface number
Router(config)#interface Giga 0/1

Router(config-if)#
Router(config-if)#mac-address ?
    H.H.H MAC address
Router(config-if)#mac-address 0001.0001.0001 ?
    <cr>
Router(config-if)#mac-address 0001.0001.0001
Router(config-if)#ipv6 address ?
    WORD General prefix name
    X:X:X:X::X IPv6 link-local address
    X:X:X:X::X/<0-128> IPv6 prefix
    autoconfig Obtain address using autoconfiguration

Router(config)#ip route ?
    A.B.C.D Destination prefix
Router(config)#ip route 192.168.0.0 ?
    A.B.C.D Destination prefix mask
Router(config)#ip route 192.168.0.0 255.255.255.0 FastEthernet 0/0 ?
    <1-255> Distance metric for this route
    <cr>
Router(config)#ip route 192.168.0.0 255.255.255.0 FastEthernet 0/0 20 ?
    <cr>
Router(config)#ip route 192.168.0.0 255.255.255.0 FastEthernet 0/0 20

```

En cas d'error l'IOS mostra informació que ha de servir per poder identificar-ne la causa i fer les correccions necessàries:

- La comanda està incompleta, encara cal afegir alguna opció més.
- La sintaxi no és correcta. És important fixar-se en el marcador «^» que apareix a sota de la comanda i que indica exactament el caràcter on comença a no ser vàlida.
- Si no és cap dels errors anteriors, mostra una breu descripció del problema, per exemple fa referència a un recurs inexistent.

Exemple

```

Router(config)#interface gigabitEthernet
% Incomplete command.
Router(config)#interface gigabitLAN 0/1

```

```

      ^
% Invalid input detected at '^' marker.
Router(config)#interface gigabitEthernet 0
      ^
% Invalid input detected at '^' marker.
Router(config)#interface gigabitEthernet 0/10
%Invalid interface type and number
Router(config)#

```

Per finalitzar amb els diferents mecanismes d'ajuda integrats a l'IOS, cal comentar també les **opcions per cercar i filtrar** la informació de sortida de les comandes show i more. Les operacions disponibles són:

- Cerca: «begin expression» comença a la primera línia on es troba l'expressió.
- Filtre: «include expression» només mostra les línies que contenen l'expressió.
- Filtre: «exclude expression» només mostra les línies que no contenen l'expressió.

L'opció corresponent s'indica a continuació de la comanda precedida per la barra vertical «|», a l'estil d'una redirecció o *pipe* de Linux. Per l'expressió que es vol cercar o filtrar s'usen expressions regulars. Per exemple, podeu consultar només les línies que contenen certa paraula a l'arxiu de configuració `show running-config | include secret`, o consultar la informació del dispositiu a partir de la línia que conté un text concret `show version | begin FastEthernet`.

Exemple

```

SW1#show running-config | include secret
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0

SW1#show running-config | include secret|hostname
hostname SW1
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0

SW1#show version | begin FastEthernet
24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0002.4A86.2754
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02

```

```
...

SW1#show interfaces | include FastEthernet0/([3-5])
FastEthernet0/3 is down, line protocol is down (disabled)
FastEthernet0/4 is down, line protocol is down (disabled)
FastEthernet0/5 is down, line protocol is down (disabled)

SW1#show interfaces | include FastEthernet|duplex
FastEthernet0/1 is down, line protocol is down (disabled)
    Half-duplex, 100Mb/s
FastEthernet0/2 is down, line protocol is down (disabled)
    Half-duplex, 100Mb/s
...
```

1.5. Arquitectura del sistema

Els dispositius de xarxa no deixen de ser ordinadors, però extremadament especialitzats per realitzar la seva tasca. S'hi poden trobar els mateixos components de maquinari a excepció dels perifèrics: processadors, memòries de sistema, unitats d'emmagatzematge, plaques base i en general més ports dels que es poden trobar en un dispositiu d'usuari final. Pel que fa al programari també disposen d'un sistema operatiu (per exemple, Cisco IOS) amb els diferents components de gestió.

El sistema de fitxers s'organitza en diferents memòries de capacitats i prestacions diverses segons l'ús que l'IOS n'ha de fer. La memòria de major capacitat i on es guarda per exemple la imatge de l'IOS (arxiu comprimit del sistema) s'anomena **Flash**. És una memòria de lectura i escriptura i s'hi poden desar imatges de versions actualitzades de l'IOS o còpies dels arxius de configuració. Normalment està integrada a la placa base del dispositiu però alguns models disposen de ranures o ports USB que permeten ampliar-la.

A la memòria principal **RAM** es carreguen el sistema en execució, la configuració en funcionament *running-config*, les estructures de dades i en general tot el necessari perquè l'IOS funcioni, però és volàtil i per tant la informació no es manté quan el dispositiu s'atura.

Per aquesta raó els dispositius també incorporen una memòria d'accés ràpid, de poca capacitat, que es pot escriure i que no és volàtil, anomenada **NVRAM** (RAM no volàtil), on només s'hi guarda la configuració que es carrega a l'arrencada *startup-config*.

També hi ha una memòria **ROM** (només lectura) que conté el sistema d'arrencada anomenat System Bootstrap o monitor de la ROM, que s'encarrega d'inicialitzar el maquinari i localitzar el fitxer amb la imatge del sistema per carregar-lo i arrencar. Aquest inclou una interfície CLI que funciona com a sistema de recuperació *rommon*.

A la taula 1 s'indiquen les diferents memòries que es poden trobar als dispositius i les seves característiques més rellevants.

Taula 1. Tipus de memòries existents als dispositius

Memòria	R/W	Volàtil	Contingut principal
ROM	R	No	Sistema d'arrencada System Bootstrap o monitor de la ROM. Inclou el sistema de recuperació <i>rommon</i> .
FLASH	R/W	No	Imatge comprimida del sistema IOS, tot i que s'hi poden afegir noves imatges o desar configuracions.
NVRAM	R/W	Sí	La configuració d'inici <i>startup-config</i> .
RAM	R/W	No	El sistema en execució i les estructures de dades necessàries per al funcionament, per exemple: <ul style="list-style-type: none"> • La configuració en execució <i>running-config</i> • Els búfers • Taules de sistema

Per tant, el procés d'arrencada dels dispositius consisteix en els següents passos:

- 1) POST (Power-On Self-Test), inicialització i comprovació del maquinari.
- 2) Càrrega del sistema d'arrencada System Bootstrap des de la memòria ROM a la memòria principal (RAM) per executar-lo.
- 3) El sistema d'arrencada localitza la imatge de l'IOS, la descomprimeix i la carrega a memòria per executar-la.
- 4) L'IOS s'executa i copia la configuració d'inici *startup-config* a memòria *running-config*; els canvis a la configuració sempre es realitzen sobre aquesta última.

Durant el procés d'arrencada es mostra un resum de la informació del sistema, tant del maquinari com del programari. Aquesta informació es pot recuperar en qualsevol moment amb la comanda `show version`. A la taula 2 es recullen a tall d'exemple alguns dels paràmetres d'un encaminador Cisco 2901.

Taula 2. Paràmetres de sistema de l'encaminador Cisco 2901

Paràmetre de sistema	Valor
Versió de l'IOS	15.1(4)M4
Arxiu d'imatge del sistema	flash0:c2900-universalk9-mz.SPA.151-1.M4.bin

Paràmetre de sistema	Valor
Mida memòria no volàtil NVRAM	255K
Mida memòria FLASH	249856K (250 MB)
Mida memòria RAM	491520K/32768K (500 MB)
Interfícies de xarxa integrades	2 x GigaEthernet

Exemple

```
Router>
Router>en
Router#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco2901 uptime is 3 minutes, 43 seconds
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

[...]

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO2901/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX15240KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

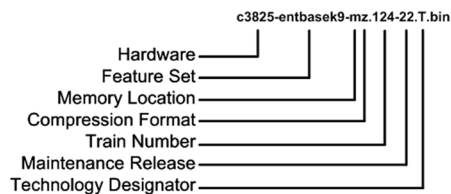
[...]
```

La memòria es mostra amb el format 491520K/32768K; la primera és la memòria RAM que utilitza el sistema i la segona fa referència a la memòria per gestionar els paquets a les cues de sortida (búfers).

Es poden trobar dues grans famílies de publicacions del programari Cisco IOS, versions 12.x o 15.y (aquesta última és la versió actual), tot i que molts dispositius encara implementen versions 12.x. També hi ha altres variants del sistema com IOS XE, que possiblement serà el successor de l'IOS, OS-XR, enfocat a maquinari per a proveïdors de serveis, i NX-OS per a maquinari de centres de dades.

El nom de l'arxiu d'imatge del sistema acostuma a seguir una nomenclatura que també aporta informació rellevant. A la figura 6 es pot observar com s'estructura el nom de la imatge d'un encaminador Cisco 3825.

Figura 6. Estructura del nom de la imatge d'un encaminador Cisco 3825



Font: <https://www.cisco.com/c/en/us/about/security-center/ios-nx-os-reference-guide.html>

1.6. Sistema de fitxers

El sistema de fitxers en general interactua amb la memòria Flash i pot transferir i rebre arxius de l'exterior, per exemple per fer còpies de suport remotes de les configuracions o carregar actualitzacions de l'IOS.

Per a la transferència d'arxius remots es fa servir el protocol TFTP (Trivial File Transfer Protocol), que és una versió lleugera del protocol FTP (File Transfer Protocol) que funciona sobre UDP (port 69) a nivell de Transport. Alguns models admeten també FTP per transferir els arxius o fins i tot HTTP per a la descàrrega d'arxius des dels entorns de gestió web.

El sistema de fitxers també permet l'intercanvi dels arxius de configuració amb les altres memòries d'escriptura RAM i NVRAM del dispositiu.

Algunes comandes de manipulació dels arxius de sistema de fitxers són:

- `dir <memoria>`: llista el contingut de la memòria indicada.
- `mkdir <nom directori>`: crea un nou directori a la memòria Flash.
- `copy <origen> <destí>`: copia el contingut del fitxer origen al destí.
- `del <nom arxiu>`: esborra l'arxiu de la memòria Flash.

Exemple

```
Router#dir ?
WORD      Directory or file name
flash0:   Directory or file name
```

Enllaç d'interès

Sobre les xarxes IOS i NX-OS podeu consultar el següent enllaç: https://www.cisco.com/c/es_es/products/ios-nx-os-software/index.html.

Enllaç d'interès

Al següent enllaç podeu trobar una eina que permet comparar les funcionalitats entre dues versions diferents del sistema per a cada dispositiu: <http://cfn.cloudapps.cisco.com/ITDIT/CFN/jsp/compareImages.jsp>.

Enllaç d'interès

Per a més informació al respecte podeu consultar els enllaços següents: Cisco IOS and NX-OS Software Reference Guide i Understanding Cisco IOS Naming Convention.


```
33591768 bytes copied in 3.952 secs (892458 bytes/sec)
Router#
```

La configuració dels dispositius es basa en dos fitxers especials: el que està desat a memòria no volàtil (*startup-config*) i el que es troba carregat a la memòria RAM i s'usa per a l'operació del dispositiu quan està en marxa (*running-config*). En iniciar el sistema, el fitxer *running-config* es genera copiant a memòria els continguts del fitxer *startup-config*.

Aquests fitxers contenen el text amb la seqüència de comandes IOS que caldria entrar per línia de comandes per arribar a la configuració actual.

Les comandes per consultar-los i manipular-los, en mode privilegiat, són:

- `show <nom fitxer>`: mostra per pantalla el contingut del fitxer.
- `copy <fitxer origen> <fitxer destí>`: copia el contingut del fitxer de configuració origen al fitxer de configuració destí.
- `write`: persisteix els canvis en execució, equivalent a la comanda `copy running-config startup-config`.
- `erase startup-config`: esborra el fitxer de configuració inicial de la memòria no volàtil NVRAM.

Qualsevol canvi en la configuració del dispositiu es fa sempre sobre el fitxer *running-config*. Per tant, si els canvis es volen fer persistents, cal copiar aquest fitxer a *startup-config*.

D'altra banda, amb tot just el procés invers, copiar el fitxer *startup-config* sobre *running-config*, podem desfer canvis actuals i tornar el dispositiu a la configuració inicial. També es pot reiniciar sense desar les noves configuracions i el dispositiu iniciarà sense aquests canvis.

Exemple

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

No files in directory

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RBCN
RBCN(config)#exit
RBCN#
%SYS-5-CONFIG_I: Configured from console by console

RBCN#copy running-config startup-config
```

```
Destination filename [startup-config]?
Building configuration...
[OK]
RBCN#dir nvram:
Directory of nvram:/

   238  -rw-          531          <no date>  startup-config

531 bytes total (237588 bytes free)

RBCN#
RBCN#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
RBCN#dir nvram:
Directory of nvram:/

No files in directory

RBCN#
```

2. Configuració de commutadors a Cisco IOS

La primera vegada que s'accedeix a configurar un encaminador amb IOS, aquest encara no té cap configuració desada a la memòria no volàtil (NVRAM) i s'activa l'assistent de configuració inicial System Configuration Dialog, que permet configurar el dispositiu de manera guiada responnent tot un seguit de preguntes.

Exemple

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

[...]

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

Enter host name [Router]: RBCN

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.

Enter enable secret: itsasecret
```

En general no fareu servir aquest assistent perquè és més lent. Amb una mica de pràctica és molt més fàcil fer les configuracions manualment o carregar un arxiu de configuració i després fer els ajustos necessaris a mà.

Per establir qualsevol configuració cal accedir primerament al mode de configuració, on es pot configurar el **nom del dispositiu** `hostname WORD` i establir una **clau d'accés** a aquest mode per evitar que qualsevol usuari pugui fer modificacions sense autorització. Aquesta clau es pot desar xifrada a l'arxiu de configuració `enable secret LINE` o en text pla `enable password LINE`. Només heu de configurar una de les dues opcions.

El nom del dispositiu no és sensible a majúscules o minúscules i no ha de ser gaire llarg (menys de deu caràcters). Només pot contenir lletres, dígitos i alguns caràcters especials però no pot contenir espais. En tot cas, la recomanació és que els noms comencin sempre per una lletra seguida de lletres o dígitos o guions, si escau.

Un altre aspecte important que cal conèixer a l'hora d'utilitzar l'IOS és que per **desactivar qualsevol configuració** es fa servir la negació de la mateixa comanda `no comanda` en el mateix mode de configuració. Per exemple, per desactivar la clau xifrada d'accés al mode de configuració global haureu d'executar `no enable secret` en aquest mateix mode.

Exemple

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
SW1(config)#enable secret itsasecret
SW1(config)#exit
SW1#
SW1#sh run | include secret|password
no service password-encryption
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#no enable secret
SW1(config)#enable password itsasecret
SW1(config)#ex
SW1#
SW1#sh run | include secret|password
no service password-encryption
enable password itsasecret
SW1#exit

[...]

SW1>en
Password:
SW1#
```

Una altra de les primeres configuracions que haureu de fer és l'adreçament de xarxa del dispositiu. Les adreces IP s'estableixen en el mode de configuració específic de cada interfície. Així, per exemple, en un encaminador cal accedir a la configuració de la interfície `interface <nom interfície>` i a continuació indicar l'adreça i la màscara `ip address A.B.C.D A.B.C.D`.

Enllaç d'interès

La guia de referència de Cisco IOS recomana seguir les directrius del document RFC 1178 «Choosing a Name for Your Computer» per escollir els noms dels dispositius. La podeu consultar a: <https://tools.ietf.org/html/rfc1178>.

Sovint les interfícies dels dispositius estan desactivades per defecte, i en aquest cas cal activar-les amb la comanda `no shutdown`. Si la interfície ja està activa, aquesta comanda no té cap efecte, per tant és una bona pràctica que us acostumeu a **activar sempre les interfícies després de configurar l'adreçament**.

També és possible configurar l'adreçament dinàmic i que automàticament es demanin els paràmetres al servidor DHCP que hi hagi disponible, en aquest cas la comanda és `ip address dhcp`.

Una vegada les adreces estan configurades a l'IOS també teniu disponibles algunes eines d'utilitat per comprovar la connectivitat, com per exemple el clàssic `ping`, la comanda de seguiment de la traça d'una ruta `traceroute` i els clients `telnet` i `ssh` per establir connexions remotes. Totes elles les trobareu tant en mode usuari com en mode privilegiat.

Exemple

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#do sh ip inter brief | include GigabitEthernet0/0
GigabitEthernet0/0    192.168.1.1    YES manual up
R1(config-if)#
R1(config-if)#no ip address
R1(config-if)#ip address dhcp
%DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0 assigned DHCP address 192.168.1.10,
mask 255.255.255.0, hostname Router0

R1(config-if)#
R1(config-if)#do sh ip inter brief | include GigabitEthernet0/0
GigabitEthernet0/0    192.168.1.1    YES DHCP up
R1(config-if)#end
R1#
R1#ping 192.168.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.100, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

R1#exit

...
```

```
R1>traceroute 192.168.1.100
Type escape sequence to abort.
Tracing the route to 192.168.1.100

 1  192.168.1.100  10 msec  0 msec  0 msec
```

Si bé l'adreçament IP és necessari per al funcionament dels encaminadors, i qualsevol interfície activa ha de tenir com a mínim una adreça única en el context corresponent, els commutadors no necessiten cap configuració de xarxa per al seu funcionament normal que es desenvolupa a nivell d'enllaç i es relaciona només amb les adreces físiques (adreces MAC).

Tot i això, per poder accedir remotament a un commutador o per connectar-se des del mateix commutador a un altre dispositiu remotament cal necessàriament que aquest disposi d'adreçament de xarxa. A diferència dels encaminadors, l'adreçament de xarxa dels commutadors no es configura a cap interfície física, sinó a alguna de les interfícies virtuals disponibles `VLAN <id>`, encara que el dispositiu no tingui cap estructura de xarxes virtuals configurada sempre té definida la interfície virtual de la VLAN 1.

Exemple

```
Switch#conf t
Switch(config)#interface vlan 1
Switch(config-if)#
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config-if)#do wr
```

Adicionalment, a l'adreçament del dispositiu pot ser necessari configurar **la porta d'enllaç** de la xarxa `ip default-gateway A.B.C.D` o també el **servidor de noms** `ip name-server A.B.C.D` i el **nom del domini** `ip domain-name WORD`.

En tot cas aquestes configuracions només afecten l'operativa local d'administració, per poder comunicar-se amb equips remots o utilitzar el nom de *host* d'aquests equips en comptes de les corresponents adreces IP, però en cap cas afecten el desenvolupament normal de la funció principal del dispositiu i són opcionals.

Exemple

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
```



```
SW1(config)#ip default-gateway 192.168.1.1
SW1(config)#ip name-server 192.168.1.100
SW1(config)#ip domain-name office.test
SW1(config)#ip domain-lookup
SW1(config)#do wr
Building configuration...

[OK]
SW1(config)#exit
SW1#
%SYS-5-CONFIG_I: Configured from console by console

SW1#ping host1.office.test
Translating "host1.office.test"...domain server (192.168.1.100)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
```

Sovint us passarà que executeu comandes incorrectes o en un mode que no els correspon. En aquests casos, quan l'IOS no troba la comanda, activa la resolució de noms (DNS) per comprovar si hi ha algun *host* amb aquest nom. Aquesta consulta bloqueja el CLI fins que obté resposta del servidor de noms, o si no està configurat, que és el més habitual, fins que passa el temps d'espera, i pot ser exasperant.

Per evitar aquesta situació es pot desactivar la resolució de noms, que es troba activada per defecte, fent servir la negació de la comanda `no ip domain-lookup`.

Exemple

```
Router#cmdnotfound
Translating "cmdnotfound"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#ex
Router#cmdnotfound
Translating "cmdnotfound"
% Unknown command or computer name, or unable to find computer address
```

2.1. Seguretat i accés remot

Anteriorment s'ha explicat com assegurar l'accés al mode privilegiat establint una contrasenya, i de manera anàloga es poden assegurar també els diferents accessos al CLI, per consola `line console 0` o l'accés remot per mitjà de les línies virtuals `line vty <X Y>`. Les línies virtuals determinen el total de **connexions remotes concurrents** disponibles, normalment hi ha fins a **setze línies virtuals** numerades del 0 al 15, i es configuren tantes com calgui, o totes alhora, per exemple per configurar fins a cinc línies concurrents `line vty <0 4>`.

És important destacar que perquè l'accés remot sigui funcional **cal que l'accés al mode de configuració global estigui protegit amb una contrasenya**. En cas contrari l'IOS de Cisco implementa una restricció de seguretat que impedeix accedir al mode de configuració si l'accés al CLI és per alguna de les línies virtuals `line vty`.

Des de la configuració específica de línia es poden activar diferents tipus d'autenticació amb la comanda `login` o desactivar-los amb la corresponent `no login`. Per defecte l'autenticació bàsica sense paràmetres `login` requereix un *password* que es desa en text pla a l'arxiu de configuració, comanda `password` `LINE`.

D'altra banda, es poden definir **usuaris locals** des del mode de configuració global `username WORD [secret|password] LINE` i activar l'**autenticació local** contra aquests des de la configuració de línia `login local`. També són possibles altres mètodes d'autenticació més complexos contra servidors AAA (Authentication Authorization Accounting, per exemple Radius o TACACS+), que queden fora de l'abast d'aquest manual.

Adicionalment es poden filtrar els tipus de comunicacions d'entrada i sortida permeses amb la comanda `transport [input|output] <protocol>`, per exemple per limitar l'accés remot al protocol `ssh` podeu fer servir `transport input ssh`.

Exemple

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable password itsasecret
Router(config)#line console 0
Router(config-line)#password itsasecret
Router(config-line)#login
Router(config-line)#exit
Router(config)#username myuser password 1234
Router(config)#line vty 0 15
Router(config-line)#no login
```

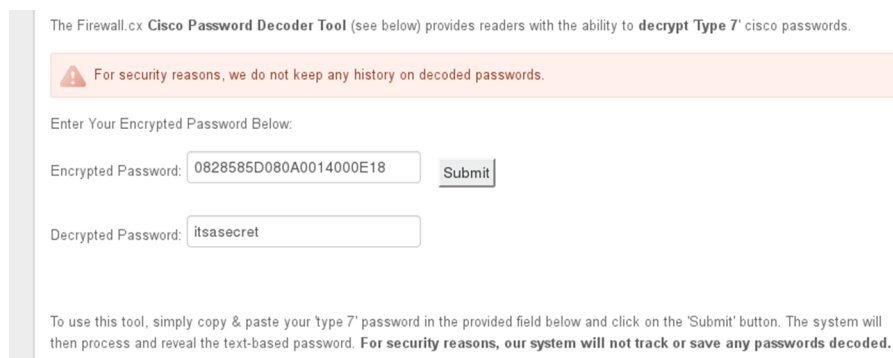
```
Router(config-line)#exit
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
Router(config-line)#login local
Router(config-line)#do wr
Building configuration...

[OK]
```

Com heu pogut veure anteriorment, en alguns casos és possible establir les contrasenyes perquè es guardin xifrades als arxius de configuració `secret` i en d'altres apareixeran sense xifrar `password`. Per aquest motiu l'IOS ofereix la possibilitat de xifrar totes les contrasenyes que no ho estiguin, fent servir la comanda `service password-encryption`.

Cal que tingueu present que el xifratge del servei «password-encryption» és molt feble i hi ha multitud d'eines que permeten desxifrar les contrasenyes que fan ús d'aquest servei. A la figura 7 en podeu veure un exemple, «0828585D080A0014000E18» és el resultat de xifrar la clau «itsasecret».

Figura 7. Clau desxifrada. Servei «password-encryption»



The Firewall.cx Cisco Password Decoder Tool (see below) provides readers with the ability to **decrypt Type 7** cisco passwords.

For security reasons, we do not keep any history on decoded passwords.

Enter Your Encrypted Password Below:

Encrypted Password:

Decrypted Password:

To use this tool, simply copy & paste your type 7 password in the provided field below and click on the 'Submit' button. The system will then process and reveal the text-based password. **For security reasons, our system will not track or save any passwords decoded.**

D'altra banda, l'IOS permet configurar missatges de sistema que es mostren als usuaris en diferents situacions i que es poden fer servir com a informació o advertència, alhora que eviten, per exemple, que en cas d'un accés no autoritzat el responsable pugui al·legar desconeixement.

Per configurar els missatges s'utilitza la comanda `banner`: per exemple, es pot mostrar una advertència just abans de demanar les credencials d'accés al sistema `banner login LINE` o afegir una informació que es mostri sempre que un usuari hi accedeixi, encara que no es requereixi autenticació `banner motd LINE`. Els missatges comencen i acaben indicant el mateix delimitador i poden contenir espais i salts de línia.

Exemple

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#no ena secret
Router(config)#ena password itsasecret
Router(config)#service password-encryption
Router(config)#ex
Router#
Router#sh run | include password
service password-encryption
enable password 7 0828585D080A0014000E18
username myuser password 7 08701E1D5D
password 7 0828585D080A0014000E18
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#banner motd #
Enter TEXT message. End with the character '#'.
This is the Message of the day #

Router(config)#

....

Press RETURN to get started.

This is the Message of the day

Router>
```

Finalment, cal comentar els serveis d'accés remot que implementen els dispositius: telnet i ssh. Pel que respecta al **telnet**, no és necessària cap configuració, el servei està actiu i és funcional en tots els dispositius. Això no evita certs requeriments per poder-lo fer servir que s'han comentat amb anterioritat:

- El dispositiu ha de disposar d'adreçament de xarxa que permeti la comunicació amb els equips remots.
- S'ha d'establir una contrasenya per a l'accés a la configuració global; en cas contrari, cap equip remot no podrà accedir a aquest mode.

El servei **ssh**, adicionalment als requeriments anteriors, per poder funcionar necessita que es generi la parella de claus asimètriques pública-privada amb la comanda `crypto key generate rsa`. L'algoritme per generar les claus és RSA (Rivest-Shamir-Adleman) i cal tenir en compte el següent:

- Abans de generar les claus, el dispositiu ha de tenir configurats el nom de *host* `hostname` i el domini IP `ip domain-name`. El nom de les claus resultants té el format del nom totalment qualificat FQDN (Fully Qualified Domain Name) del dispositiu. `HOSTNAME.DOMAIN-NAME`.
- A l'hora de generar les claus cal indicar-ne la mida en bits. Els valors habituals són 512, 1024 o 2048. A mesura que s'incrementa la mida de les claus també triguen més a generar-se, i depenent del dispositiu les claus de 2048 bits poden trigar minuts o fins i tot hores.
- Per activar la versió 2 del protocol ssh teniu la comanda `ip ssh version 2`.
- També es pot configurar, per exemple, el nombre màxim de temptatives d'autenticació abans que la sessió es desconnecti `ip ssh authentication-retries <0-5>`, i el temps en segons per completar l'inici de sessió `ip ssh time-out <1-120>`.

Exemple

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RBCN
RBCN(config)#enable secret itsasecret
RBCN(config)#ip domain-name example.com
RBCN(config)#crypto key generate rsa
The name for the keys will be: RBCN.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RBCN(config)#ip ssh version 2
*març 1 0:8:26.509: %SSH-5-ENABLED: SSH 1.99 has been enabled

RLAN24 (config)#
RLAN24#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
RLAN24#
```

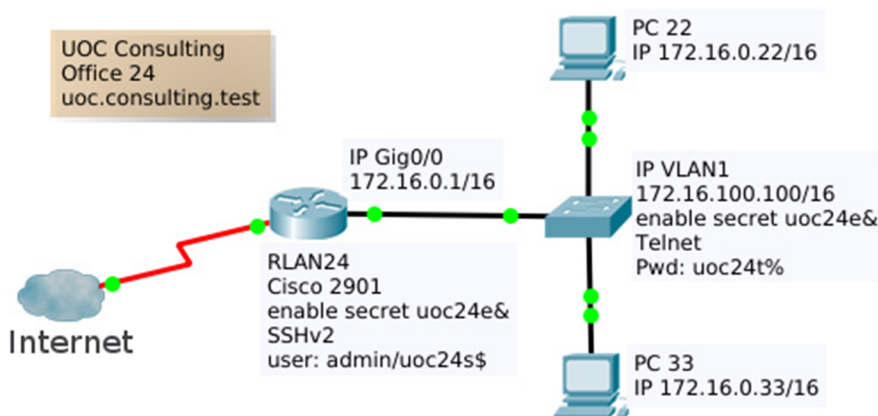
2.2. Cas pràctic

En el cas pràctic següent es proposa configurar l'accés remot per ssh i telnet a un encaminador i a un commutador, respectivament. A l'esquema de la figura 8 es mostren alguns dels dispositius de la xarxa d'una de les oficines de l'empresa fictícia UOC Consulting, amb el domini corporatiu «uoc.consulting.test». En aquesta xarxa els ordinadors es connecten a un commutador, i aquest amb l'encaminador que fa les funcions de porta d'enllaç i dona accés a Internet a la resta de dispositius.

Vegeu també

A l'apartat 3 d'aquest manual es tractarà més detalladament la configuració dels encaminadors.

Figura 8. Esquema xarxa Cas pràctic 1. Oficina 24 UOC Consulting



En aquest mateix esquema es mostra l'adreçament IPv4 i també l'accés remot que cal configurar tant a l'encaminador com al commutador per poder gestionar-los des de qualsevol dels ordinadors de l'oficina. L'encaminador RLAN24 ha d'estar accessible per ssh amb les credencials indicades, mentre que l'accés al commutador serà per telnet fent servir la clau indicada.

Es demana implementar les configuracions indicades a tots els dispositius i comprovar el funcionament dels accessos per ssh i telnet.

A continuació es proposa la solució implementada amb el programari de simulació de xarxes Packet Tracer. S'inclouen les configuracions des de CLI pas a pas dels dos dispositius de xarxa.

Solució. Servei ssh a l'encaminador

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inte gig0/0
Router(config-if)#ip addr 172.16.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#hostname RLAN24
RLAN24(config)#enable secret uoc24e&
RLAN24(config)#ip domain-name uoc.consulting.test
RLAN24(config)#crypto key generate rsa
The name for the keys will be: RLAN24.uoc.consulting.test
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RLAN24(config)#ip ssh version 2
*març 1 0:8:26.509: %SSH-5-ENABLED: SSH 1.99 has been enabled
RLAN24(config)#username admin secret uoc24s$
RLAN24(config)#line vty 0 15
RLAN24(config-line)#no login
RLAN24(config-line)#exit
RLAN24(config)#line vty 0 1
RLAN24(config-line)#transport input ssh
RLAN24(config-line)#login local
RLAN24(config-line)#do wr
Building configuration...
[OK]
RLAN24(config-line)#
```

Solució. Servei telnet al commutador

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip address 172.16.100.100 255.255.0.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#exit
Switch(config)#enable secret uoc24e&
Switch(config)#line vty 0 15
Switch(config-line)#no login
Switch(config-line)#exit
Switch(config)#line vty 0 1
Switch(config-line)#password uoc24t%
```

```
Switch(config-line)#login
Switch(config-line)#do wr
Building configuration...
[OK]
Switch(config-line)#
```

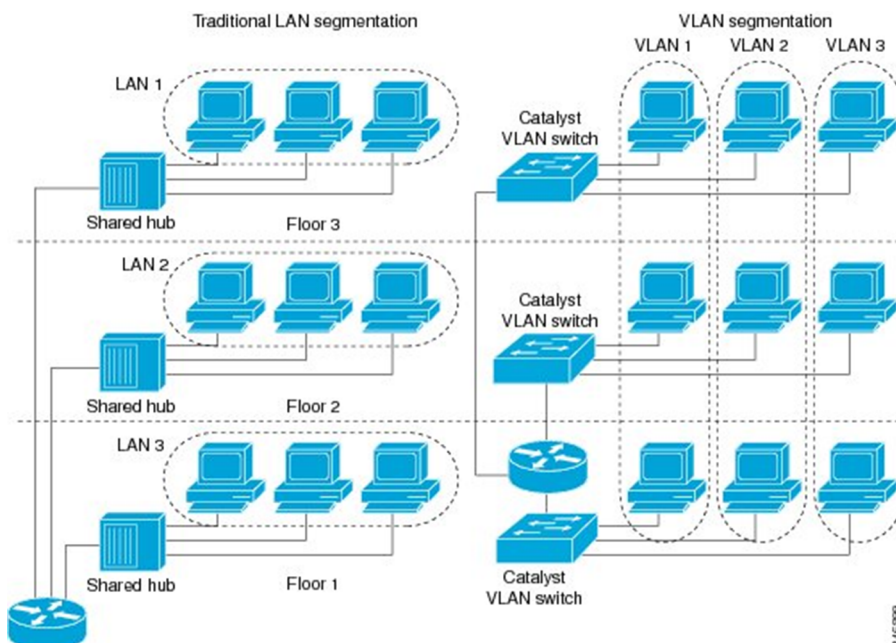
2.3. Configuració de commutadors: VLAN

Una de les principals funcionalitats dels commutadors és la possibilitat de dividir els dispositius d'una xarxa local en segments o grups funcionals més petits sense necessitat de tenir en compte la seva ubicació física, ni haver d'incrementar el maquinari.

Cada segment s'anomena **xarxa virtual** o **VLAN** i té assignat un identificador numèric propi. El terme "virtual" fa referència al fet que, si bé tots els dispositius dins una xarxa local estan connectats entre si fent servir commutadors, o sigui, es pot seguir un camí físic entre dos dispositius qualssevol de la xarxa, els membres d'una xarxa virtual es comporten com si estiguessin sols sense compartir-la amb ningú més.

Per tant, la implementació de xarxes virtuals aporta una major flexibilitat a l'hora d'organitzar els equips d'una xarxa corporativa i garanteix que les comunicacions de cadascuna d'elles estaran aïllades de la resta, ja que el segment de la xarxa que conforma cada VLAN és un domini de difusió independent. Podeu veure'n un exemple a la figura 9.

Figura 9. Comparativa de la segmentació tradicional envers la implementació amb VLAN



Font: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/15-s/lsw-15-s-book/lsw-vlan-cfg-rtg.html>

Per començar, cal identificar clarament en quants segments o grups d'equips es dividirà la xarxa, i a quin grup pertany cada equip. Per implementar des de l'IOS d'un commutador l'esquema de xarxes virtuals cal crear una VLAN per a cada grup i assignar-li un número, des del mode de configuració global amb la comanda `vlan <id>` es crea la VLAN i entra al mode de configuració específic, des d'on opcionalment es pot indicar un nom per a aquesta, `name WORD`.

Els ports dels commutadors on es connecten els equips s'assignen a les VLAN corresponents. Aquests tipus de ports que connecten equips s'anomenen **ports d'accés**. A cada commutador només cal definir les VLAN dels dispositius que es connecten directament als seus ports, tot i que si voleu podeu crear-les totes.

Des del mode de configuració de cada interfície s'estableix el rol d'accés d'aquesta amb la comanda `switchport mode access`, i després s'indica a quina VLAN pertany `switchport access vlan <id>`. **Un port d'accés només pot pertànyer a una VLAN.**

Per verificar la distribució de VLAN dels ports d'un commutador es poden executar les comandes `show vlan` o `show vlan brief`, que mostren a quina VLAN està assignat cada port, o també per consultar informació concreta d'una VLAN `show vlan id <id>` o `show vlan name WORD`.

Normalment és una bona pràctica configurar tots els ports a les diferents VLAN segons els requeriments, i és habitual que diversos ports comparteixin la mateixa configuració. Per facilitar-ne la configuració, l'IOS permet accedir a configurar **rangs de ports** tots alhora amb la comanda `interface range <tipus interfície> <0-9>/<0-48>-<0-48>`.

Exemple

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 5
Switch(config-vlan)#name MANAGE
Switch(config-vlan)#vlan 10
Switch(config-vlan)#name RRHH
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 5
Switch(config-if)#do wr
Building configuration...
```

```
[OK]
Switch(config-if)#end
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Gig0/1, Gig0/2
5 GESTIO	active	Fa0/24
10 RRHH	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10

```
[...]

Switch#
Switch#show vlan id 10
```

VLAN Name	Status	Ports
10 RRHH	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
10	enet	100010	1500	-	-	-	-	0	0

A l'hora de connectar dos commutadors entre ells apareix la necessitat de comunicar dispositius de les mateixes VLAN repartits entre els dos commutadors. En primera aproximació es podria fer servir un port de cada commutador de les diferents VLAN definides per connectar-los entre ells. És fàcil veure que això té l'inconvenient d'haver d'utilitzar tants ports dels commutadors com VLAN estiguin definides per fer aquesta interconnexió, i és un malbaratament de recursos.

Per resoldre el problema anterior es pot configurar un únic port per tal que permeti el trànsit de dades de múltiples VLAN. La comanda en el mode de configuració d'interfície és `switchport mode trunk`, i per a aquests ports anomenats **truncals** es pot configurar el trànsit de les VLAN admeses, indicant un rang inclusiu `switchport trunk allowed vlan <id inicial>-<id final>` o també una llista discreta dels identificadors de VLAN `switchport trunk allowed vlan <id1>,<id2>, ...` També posteriorment es poden afegir o treure VLAN assignades al port troncal `switchport trunk allowed vlan add <id>` o `switchport trunk allowed vlan remove <id>`.

Per poder gestionar el trànsit de dades de múltiples VLAN en un únic port troncal, el commutador que envia les dades pel port troncal prèviament els afegeix la informació de la VLAN a la qual pertany (*tag* o etiqueta). Així, el receptor en rebre les trames extreu aquesta informació per identificar a quina VLAN correspon i les torna a deixar tal com estaven originalment, sense l'etiqueta. A la figura 10 podeu observar com afecten aquests canvis a l'estructura de la trama Ethernet.

Figura 10. Estructura de la trama Ethernet VLAN 802.11q (dot1q)

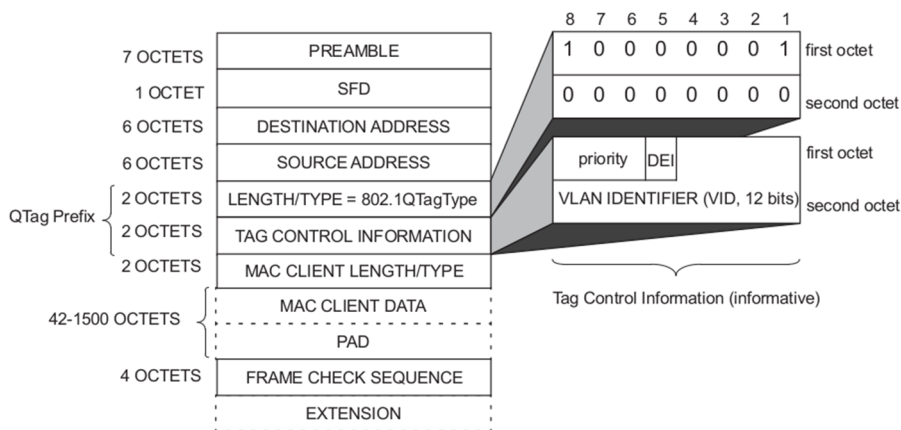


Figure G-1—Example of IEEE 802.3 MAC frame format

Font: https://standards.ieee.org/standard/802_1Q-2014.html

Els ports troncal també accepten trames sense etiqueta. En aquest cas el commutador assigna aquestes dades a la VLAN nativa. Cada port troncal només pot tenir configurada una única VLAN nativa i per defecte és la VLAN 1. Per configurar-la teniu la comanda `switchport trunk native vlan <id>`.

Per a alguns dispositius CISCO també es pot fer servir un altre protocol per encapsular les trames als enllaços troncal anomenat ISL Inter-Switch Link. En aquest cas als ports troncal caldrà establir explícitament el tipus d'encapsulament `switchport trunk encapsulation [isl | dot1q]`. Aquest protocol és propietat de CISCO mentre que la norma 802.1q és l'estàndard utilitzat arreu i per tant el mètode recomanat; a més, ISL està en desús i els nous models no l'implementen.

Qualsevol trama que arribi a un port troncal des de la mateixa VLAN que té configurada el port troncal es transmet per aquest sense etiqueta. És obligatori que els dos ports connectats a l'enllaç troncal tinguin configurada la mateixa VLAN nativa.

Per consultar la informació dels ports troncal teniu la comanda `show interfaces trunk` i per obtenir informació detallada d'una interfície concreta `show interfaces <nom interfície> switchport`.

Exemple

Tagging

El mecanisme d'afegir la informació de la VLAN a les trames s'anomena **tagging** o etiquetatge, raó per la qual aquests ports troncal també s'anomenen **tagged ports**. Els detalls d'implementació de les xarxes virtuals es descriu a la norma IEEE 802.1q, que és l'origen del terme dot1q.

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 99
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 5-20
Switch(config-if)#switchport trunk allowed vlan add 99
Switch(config-if)#do sh int trunk
Port          Mode          Encapsulation  Status        Native vlan
Gig0/1        on            802.1q         trunking      99

Port          Vlans allowed on trunk
Gig0/1        5-99

Port          Vlans allowed and active in management domain
Gig0/1        5,10,20

Port          Vlans in spanning tree forwarding state and not pruned
Gig0/1        5,10,20

```

El fet que l'estructura de les trames de dades es modifiqui als ports troncal implica que aquests ports no són compatibles amb els ports d'accés d'altres commutadors, ni amb els ports d'altres dispositius com ordinadors o encaminadors.

En una xarxa segmentada en diverses VLAN independents caldria un encaminador per a cada VLAN per gestionar les comunicacions amb l'exterior (incloent-hi els dispositius de les altres VLAN), o bé fer servir un port troncal que admet múltiples VLAN connectat a un únic encaminador, però cal configurar el port de l'encaminador per entendre les trames etiquetades que li arriben per aquest enllaç troncal.

Així, per configurar un port d'un encaminador connectat a un port troncal d'un commutador, primerament a partir del port físic de l'encaminador cal crear tantes subinterfícies com VLAN admeti el troncal. La comanda és `interface <nom interfície>.N`, on `.N` és un sufix numèric. És una bona pràctica escollir pel sufix el mateix valor de l'identificador de la VLAN que gestionarà la subinterfície.

Cada subinterfície actuarà com a porta d'enllaç dels dispositius d'una VLAN, per tant tindrà una adreça lògica de la mateixa xarxa. A més, per tal que accepti les dades etiquetades amb la informació de la VLAN, s'hi configurarà

l'encapsulament amb la comanda `encapsulation dot1Q <id>`, tot indicant l'identificador d'aquesta. Hi ha altres solucions a l'encaminament entre VLAN que no es detallaran en aquest manual.

Exemple

```
Router>en
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1.5
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.5, changed state to up

Router(config-subif)#encapsulation dot1Q 5
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#do wr
Building configuration...
[OK]
Router#show ip interface brief

Interface                IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0      unassigned      YES unset  administratively down  down
GigabitEthernet0/1      unassigned      YES unset  up            down
GigabitEthernet0/1.5    192.168.5.1     YES manual  up            down
Vlan1                    unassigned      YES unset  administratively down  down
Router#
```

2.4. Configuració de commutadors: taula MAC

La taula d'adreces MAC és la taula que utilitza el commutador per a la seva funció principal, que és commutar les trames que arriben per un port cap a un dels altres ports de sortida. A la taula MAC s'hi desa informació de les adreces físiques dels dispositius, com per exemple per quin port cal enviar-li les dades, a quina VLAN està i el tipus o origen d'aquesta informació. La taula es pot consultar amb la comanda `show mac-address-table`.

Sense fer cap configuració, el commutador és capaç de gestionar la informació d'aquesta taula de manera automàtica a partir de les adreces origen de les trames que rep pels diferents ports. En aquest cas les dades apareixeran

a la taula com a dinàmiques `DYNAMIC`. Aquesta informació registrada automàticament té caducitat i és volàtil. Si passat cert temps sense utilitzar-se, s'esborra de la taula, i si es reinicia el dispositiu també. El contingut dinàmic també es pot esborrar amb la comanda `clear mac-address-table dynamic`.

Sempre que el commutador rep una trama i ha de decidir a quin port enviar-la, consulta la taula d'adreces MAC. Si el destinatari no hi apareix, l'envia a tots els ports perquè la transmetin esperant trobar-lo, i aquesta trama es difon per tota la xarxa. La majoria d'aquest trànsit serà finalment descartat. Per evitar la difusió de trames per tota la xarxa cercant dispositius que no es troben a la taula d'adreces MAC, es pot afegir informació directament a la taula. Aquestes dades es mostren com a estàtiques `STATIC` a la taula i són permanents, no s'esborren ni tan sols després d'un reinici. La comanda per afegir informació estàtica d'un dispositiu és `mac-address-table static H.H.H vlan <id> interface <nom interfície>`.

Es pot buidar temporalment la taula de totes les entrades dinàmiques o estàtiques amb la comanda `clear mac-address-table`, però cal tenir present que les configuracions estàtiques estan desades a l'arxiu de configuració i, per tant, després de reiniciar tornaran a aparèixer. Per desactivar una entrada estàtica cal fer servir la negació de la comanda `no mac-address-table static H.H.H vlan <id> interface <nom interfície>`.

Aquesta configuració només té sentit fer-la per afegir informació de dispositius rellevants a la xarxa i que siguin destins habituals de les comunicacions, per exemple la porta d'enllaç, un servidor o una impressora.

Exemple

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mac-address-table static 000C.000C.000C vlan 5 interface GigabitEthernet 0/1
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show mac-address-table
          Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0040.0baa.ba19   DYNAMIC     Gig0/1
5       000c.000c.000c   STATIC      Gig0/1
```

```
Switch#clear mac-address-table dynamic
Switch# sh mac-address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
5       000c.000c.000c  STATIC  Gig0/1
```

3. Configuració d'encaminadors a Cisco IOS

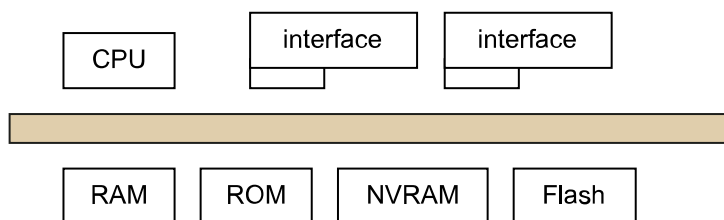
Aquest apartat serveix com una breu introducció a l'operació d'encaminadors amb el sistema Cisco IOS, emprat pels dispositius Cisco. Si bé aquest sistema operatiu és complex i amb moltes opcions, els conceptes que es presenten aquí són els més bàsics per poder seguir els objectius d'aprenentatge de l'assignatura partint des de zero.

3.1. Estructura d'un encaminador (*router*)

Un encaminador (*router*, en anglès) IP és un computador especialitzat en commutar datagrames IP. Depenent de les prestacions que ha d'oferir, la seva estructura interna és més o menys complexa i especialitzada, però per als models de gama baixa, podem pensar en una estructura similar a la d'un PC: CPU, memòria, busos e interfícies de xarxa. Per a l'emmagatzemament de dades és habitual utilitzar memòria ROM, memòria Flash i memòria RAM i RAM no volàtil (NVRAM):

- RAM: codi, taules d'encaminament, búfers, memòria cau ARP, etc.
- NVRAM (no volàtil): fitxer de configuració *startup-config*.
- Flash (no volàtil): imatge de l'IOS.
- ROM (no volàtil): part de la imatge IOS, codi *bootstrap*.

Figura 11. Diagrama de blocs d'un encaminador Cisco



3.1.1. Consulta de l'estat de l'encaminador (comanda `show`)

Podem consultar l'estat d'un encaminador mitjançant variacions de la comanda `show`. Aquesta comanda té moltes opcions i permet visualitzar dades de tota mena, per la qual cosa és molt útil usar l'ajuda per llistar-les (opció `?`).

Depenent del tipus d'informació que volem consultar, la comanda és executable des del mode usuari, o bé necessitem els privilegis del mode privilegiat.

Les opcions que fareu servir més habitualment són:

- `show running-config`: mostra el fitxer de configuració que està actiu a l'encaminador.
- `show startup-config`: mostra el fitxer de configuració que està gravat a la NVRAM.
- `show ip <parameter>`: mostra els paràmetres associats a la configuració del protocol IP.
- `show ip route`: mostra la taula d'encaminament IP.
- `show ip interface brief`: mostra un resum de l'estat de les interfícies.
- `show interfaces`: mostra informació detallada de les interfícies de xarxa.
- `show interface <nom>`: mostra informació detallada d'una interfície concreta.
- `show cdp neighbors`: permet llistar dispositius Cisco veïns connectats.

La taula d'encaminament és una informació que no es considera privilegiada i que pot ser consultada des del mode usuari. No obstant això, el contingut dels fitxers de configuració sí que es consideren privilegiats i només poden ser visualitzats des del mode privilegiat.

3.2. Configuració d'encaminadors amb Cisco IOS

Els següents subapartats introdueixen la configuració genèrica d'interfícies als encaminadors, juntament amb la configuració d'interfícies Ethernet i la configuració d'interfícies sèrie. També s'indica el mètode per consultar la taula ARP.

3.2.1. Configuració d'interfícies

Un encaminador pot tenir diferents interfícies de diferents protocols de nivell 2 (Ethernet, Serial, ADSL). Cada una d'aquestes interfícies es pot configurar només amb una adreça IP.

A nivell bàsic, per configurar una interfície de xarxa només cal indicar la seva adreça IP, la màscara de subxarxa, i activar-la:

- `ip address <adreça IP> <màscara de subxarxa>`: configura l'adreça IP.
- `no shutdown/shutdown`: activa o desactiva la interfície.

La comanda `ip address` permet assignar una adreça IP a una interfície. La configuració de les interfícies es fa des del mode de configuració d'un encaminador.

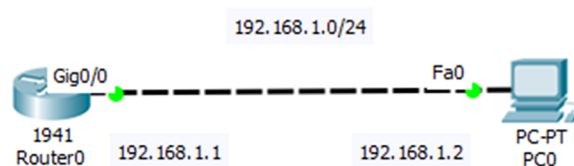
La comanda `no shutdown` és necessària per activar la interfície. Per defecte, en arrancar l'encaminador totes les interfícies estan desactivades. La comanda `shutdown` en el seu defecte desactivaria administrativament una interfície.

3.2.2. Configuració d'interfícies Ethernet

Exemple 1: Configuració d'un enllaç Ethernet entre un encaminador i un ordinador

A la figura 12a es mostra un enllaç Ethernet que connecta la interfície GigabitEthernet0/0 del Router0 i la interfície FastEthernet0 de l'ordinador PC0.

Figura 12a. Enllaç Ethernet entre un encaminador i un ordinador



Les configuracions de les interfícies de l'encaminador i de l'ordinador es mostren a la figura 12b. Per exemple, per configurar la interfície de l'encaminador s'ha fet servir la comanda `ip address`, i per activar-la la comanda `no shutdown`.

Figura 12b. Configuració de les interfícies de l'encaminador Router0 i de l'ordinador PC0

```
Router>enable
Router#configure terminal
Router(config)#interface Gig0/0
Router(config-if)#ip address
192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
```

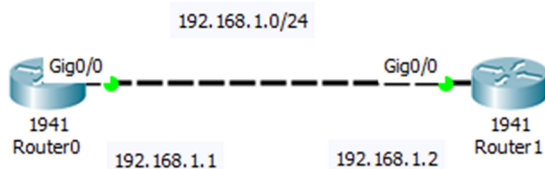
La captura de pantalla mostra la finestra de configuració de l'ordinador PC0. La pestaña 'Config' està seleccionada, i la sub-pestaña 'IP Configuration' està activa. Sota 'IP Configuration', l'opció 'Static' està seleccionada. L'adreça IP està configurada com '192.168.1.2' i la màscara de subxarxa com '255.255.255.0'. Sota 'IPv6 Configuration', l'opció 'Static' està seleccionada, i l'adreça IPv6 està configurada com 'FE80::20A:41FF:FE97:B9E2'.

Un cop configurades les dues interfícies, es pot fer un `ping` amb èxit entre els dos dispositius.

Exemple 2: Configuració Ethernet entre dos encaminadors

A la figura 13a es mostra un enllaç Ethernet que connecta la interfície GigabitEthernet0/0 de Router0 amb la interfície GigabitEthernet0/0 de Router1.

Figura 13a. Connexió Ethernet entre dos encaminadors



A la figura 13b es mostren les configuracions de les interfícies Ethernet dels dos encaminadors, on les comandes `ip address` i `no shutdown` són imprescindibles per fer aquesta tasca. Un cop configurades les interfícies ja s'aconsegueix visibilitat a nivell IP entre els dos equips.

Figura 13b. Configuracions de les interfícies GigabitEthernet de Router0 i Router1

```
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface Gig0/0
Router0(config-if)#ip address
192.168.1.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#
```

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Gig0/0
Router1(config-if)#ip address
192.168.1.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#
```

3.2.3. Configuració d'interfícies sèrie

Les interfícies sèrie estan dissenyades perquè en la situació més normal es connectin a un operador de telecomunicacions per mitjà d'un DCE (es a dir, un mòdem o una Terminació de Xarxa, TR). El DCE és el que normalment dona el rellotge i per tant fixa la velocitat de modulació i de transmissió.

Si es connecten dos ports sèrie d'encaminador (DTE-DTE) s'ha de fer servir un cable sèrie, on un dels dos ports ha d'actuar com a DCE donant el rellotge. En principi, des del punt de vista de l'encaminador qualsevol dels dos pot actuar com a DCE, així que és important saber quin connector del cable marcarà el port que actuarà com a DCE.

Una vegada se sap quin és el port que actua com a DCE, aquest ha d'aportar el rellotge. Aquesta opció s'activa amb la comanda `clock rate Bw`, on `Bw` indica la velocitat (bits per segon) a la qual ha de treballar la línia. Al port DTE no s'ha d'executar aquesta comanda.

Exemple: Configuració d'enllaç sèrie entre dos encaminadors

A la figura 14a es mostra un enllaç sèrie entre la interfície Serial `Se0/1/0` de Router0 i la interfície Serial `Se0/1/0` de Router1. La configuració de les dues interfícies es mostra a la figura 14b. Les interfícies *Serial* es configuren de forma similar a les interfícies *Ethernet* (amb les comandes `ip address` i `no shutdown`), amb la diferència que cal fixar la velocitat de transmissió a la interfície DCE. En aquest cas, la interfície *Serial* de Router0 és la que actua com a DCE i on cal assignar la velocitat amb la comanda `clock rate 4000000`. La interfície *Serial* de Router1 és DTE i no cal fer res més.

Un cop configurat l'enllaç sèrie, els dos encaminadors es poden comunicar a nivell IP.

Figura 14a. Connexió sèrie entre dos encaminadors

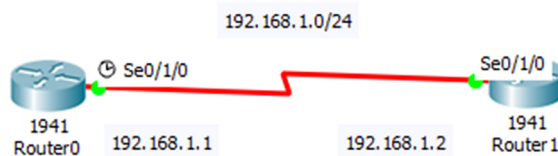


Figura 14b. Configuració de les interfícies sèrie dels dos encaminadors

```
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface se0/1/0
Router0(config-if)#ip address
192.168.1.1 255.255.255.0
Router0(config-if)#clock rate 4000000
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#
```

```
Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface se0/1/0
Router1(config-if)#ip address
192.168.1.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#
```

3.2.4. Taula ARP

Per consultar la taula ARP d'un encaminador es pot fer servir la comanda `show arp`, i per esborrar les entrades es poden fer servir les comandes `clear arp` i `clear arp-cache`.

Exemple: Taula ARP d'un encaminador

La xarxa de la figura 15a està formada per dos ordinadors PC0 i PC1 connectats via Ethernet a un mateix encaminador Router0. Les configuracions de les interfícies dels encaminadors i dels dos ordinadors es mostren a la figura 15b.

Figura 15a. Xarxa formada per dos ordinadors connectats a un encaminador

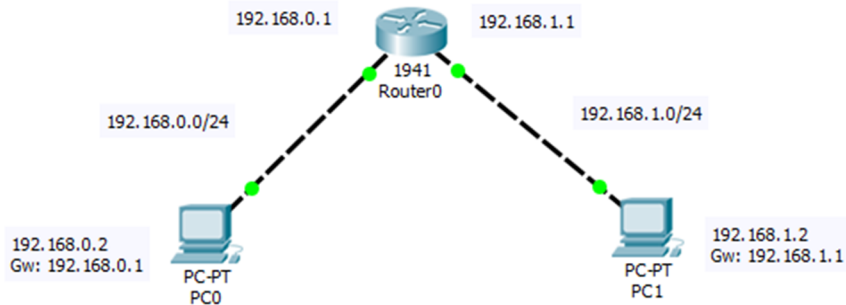


Figura 15b. Configuració dels dos ordinadors PC0 i PC1 i de Router0

```
Router>enable
Router#configure terminal
Router(config)#interface Gig0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface Gig0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)
```

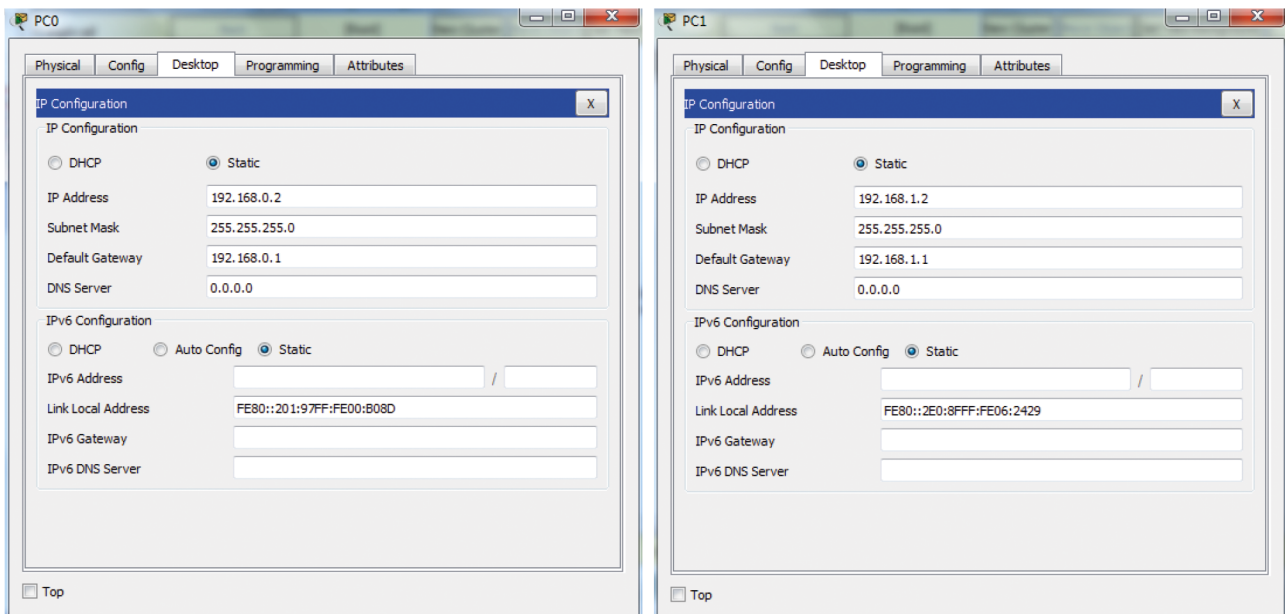
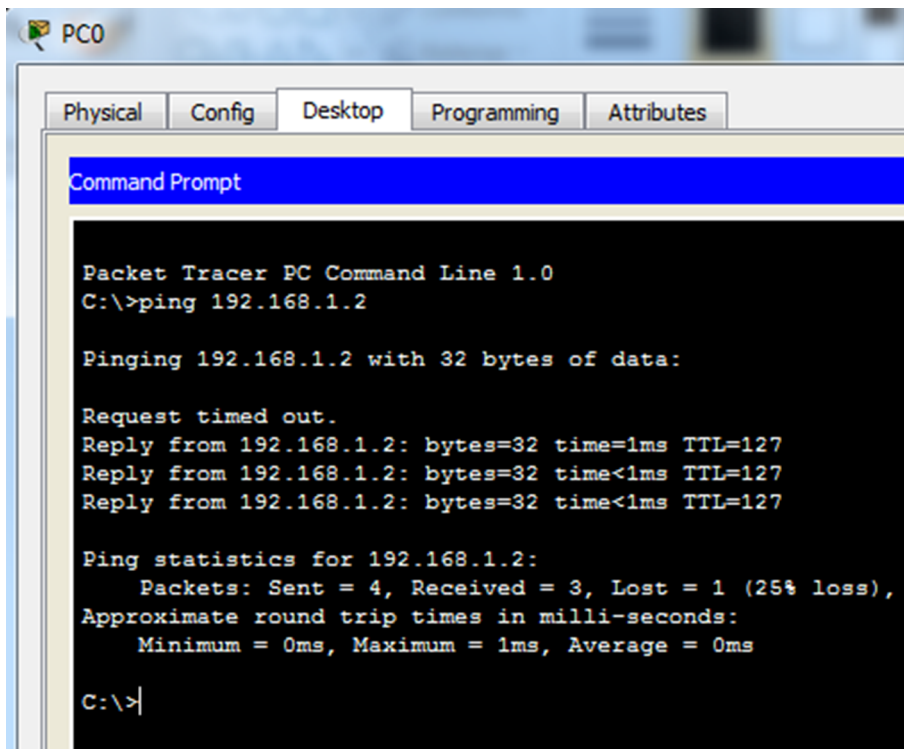


Figura 15c. *Ping* realitzat des de PC0 cap a PC1

Un cop configurades totes les interfícies, des de PC0 es realitza un *ping* cap a l'adreça de PC1 (figura 15c). Aquest *ping* provoca que es facin dues resolucions ARP, una en cada xarxa Ethernet, que permetran a l'encaminador conèixer les adreces MAC de les interfícies dels dos ordinadors. La comanda `show arp` permet visualitzar aquestes adreces MAC i les interfícies de l'encaminador per on s'han après:

```
Router#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.0.1 - 000C.856C.6201 ARPA GigabitEthernet0/0
Internet 192.168.0.2 0 0001.9700.B08D ARPA GigabitEthernet0/0
Internet 192.168.1.1 - 000C.856C.6202 ARPA GigabitEthernet0/1
Internet 192.168.1.2 0 00E0.8F06.2429 ARPA GigabitEthernet0/1
Router#
```

3.3. Encaminament estàtic

Una ruta estàtica és creada per un administrador de forma manual. Per configurar un encaminament estàtic a un encaminador es fa servir la comanda `ip route` en mode de configuració:

```
Router(config)# ip route <IP xarxa destí> <màscara destí> <IP Gateway>.
```

Els paràmetres de la comanda `ip route` són:

- Adreça de la xarxa destinació.
- Màscara associada a aquesta xarxa.
- Adreça de la interfície de l'encaminador o l'adreça del següent salt (*gateway*) per on s'ha d'encaminar el paquet.

Exemple: Encaminament estàtic entre dos encaminadors

La xarxa de la figura 16a està formada per tres subxarxes IP i dos encaminadors, de manera que cada encaminador només està directament connectat a dues subxarxes. Les configuracions de les interfícies dels encaminadors Router0 i Router1 i dels ordinadors PC0 i PC1 es mostren a la figura 16b. En tractar-se d'interfícies Ethernet s'utilitzen bàsicament les comandes `ip address` i no `shutdown`, com hem vist en apartats anteriors.

Figura 16a. Xarxa formada per dos encaminadors i tres subxarxes IP

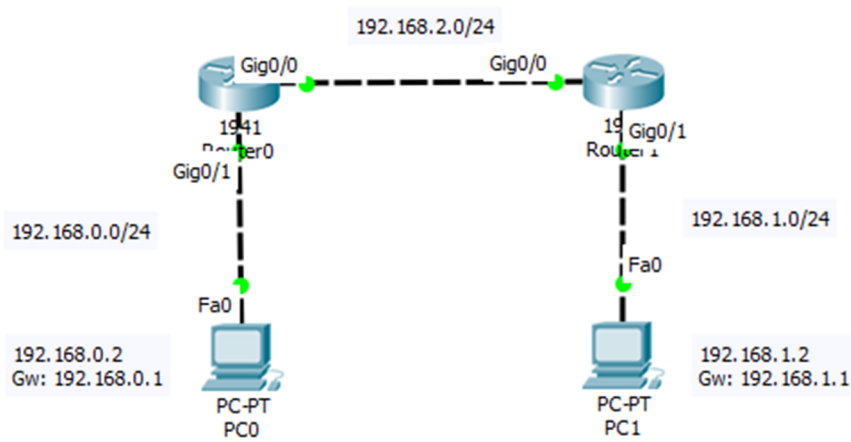


Figura 16b. Configuració de les interfícies dels ordinadors i encaminadors

```
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface Gig0/1
Router0(config-if)#ip address
192.168.0.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface Gig0/0
Router0(config-if)#ip address
192.168.2.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
```

```
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Gig0/0
Router1(config-if)#ip address
192.168.2.2 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface Gig0/1
Router1(config-if)#ip address
192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
```

The figure displays two screenshots of network configuration windows for PC0 and PC1. The PC0 window shows the IP Configuration tab with the following settings: IP Configuration (Static), IP Address: 192.168.0.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.0.1, and DNS Server: 0.0.0.0. The IPv6 Configuration section shows DHCP (Auto Config) selected, IPv6 Address: [empty], Link Local Address: FE80::201:97FF:FE00:B08D, IPv6 Gateway: [empty], and IPv6 DNS Server: [empty]. The PC1 window shows the IP Configuration tab with the following settings: IP Configuration (Static), IP Address: 192.168.1.2, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.1.1, and DNS Server: 0.0.0.0. The IPv6 Configuration section shows DHCP (Auto Config) selected, IPv6 Address: [empty], Link Local Address: FE80::2E0:8FFF:FE06:2429, IPv6 Gateway: [empty], and IPv6 DNS Server: [empty].

És molt important remarcar que quan es configura una interfície d'un encaminador, de manera automàtica s'afegeix una entrada a la seva taula de *routing*, que es correspon amb aquesta xarxa directament connectada.

Figura 16c. Taules de *routing* del Router0 i Router1

```
Router0#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/1
L 192.168.0.1/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
L 192.168.2.1/32 is directly connected, GigabitEthernet0/0
```

```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, GigabitEthernet0/0
L 192.168.2.2/32 is directly connected, GigabitEthernet0/0
```

Si s'executa la comanda `show ip route` al Router0 (tal com mostra la figura 16c), es pot observar que pel fet d'haver configurat les seves interfícies amb les adreces 192.168.0.1 i 192.168.2.1, s'han afegit a la seva taula de *routing* les xarxes directament connectades 192.168.0.0/24 i 192.168.2.0/24 amb el distintiu 'C'. De manera similar, també es pot veure que Router1 té registrades les xarxes 192.168.1.0/24 i 192.168.2.0/24 a la seva taula de *routing* amb el distintiu 'C'.

Per tant, es pot dir que Router0 coneix les xarxes 192.168.0.0/24 i 192.168.2.0/24, però desconeix la xarxa 192.168.1.0/24, i d'altra banda, Router1 coneix les xarxes 192.168.1.0/24 i 192.168.2.0/24, però no la xarxa 192.168.0.0/24. Per a una connectivitat completa cal que tots els encaminadors coneguin totes les subxarxes implicades en l'encaminament dels paquets.

Aquesta problemàtica es pot resoldre de dues maneres:

- Amb encaminament estàtic: un administrador de xarxa afegeix manualment les rutes que són desconegudes per les taules de *routing*.
- Amb encaminament dinàmic: els protocols d'encaminament s'encarreguen de propagar i mantenir aquesta informació entre les taules de *routing* dels dispositius.

Amb encaminament estàtic i per tal que totes les rutes siguin conegudes, s'haurien d'executar les següents comandes `ip route` en els encaminadors corresponents:

```
Router1(config)#ip route 192.168.0.0 255.255.255.0
192.168.2.1
```

```
Router0(config)#ip route 192.168.1.0 255.255.255.0
192.168.2.2
```

3.3.1. Ruta per defecte (Default Gateway)

La ruta per defecte (o Default Gateway) evita que les taules dels encaminadors hagin d'emmagatzemar totes les xarxes destinació d'Internet. Normalment un encaminador només especifica les rutes més properes. La resta de rutes s'indiquen mitjançant una ruta o Gateway per defecte. La ruta per defecte indica a un encaminador que qualsevol paquet que no sàpiga com encaminar (destinació desconeguda), l'encamini per aquesta ruta.

Una ruta per defecte és aquella ruta que té com a xarxa destinació 0.0.0.0 i màscara 0.0.0.0, tal com mostra la taula 3.

Taula 3. Entrada d'una ruta per defecte a una taula de *routing* d'un encaminador

Destinació	Màscara	Gateway	Interfície
0.0.0.0	0.0.0.0	IP Gateway	eth0

En un encaminador Cisco es pot introduir una ruta per defecte a la seva taula de *routing* amb la comanda `ip route`, de la següent manera:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 <IP Gateway>
```

La utilitat de la ruta per defecte s'explica més clarament amb l'algorisme de recerca de ruta, que fa servir l'encaminador a dins de la taula de *routing*, anomenat Longest Prefix Match (recerca pel prefix més llarg), i que es mostra en el codi següent.

```
trobat=false;
```

```

for i=1 to num_files_taula_routing {
    if (@IPdestinacio_datagrama AND Mascara[i] == Destinació[i]) {
        Interface[i] ← Datagrama; //S'encamina el datagrama per la interfície corresponent
        trobat =true;
        break; //Es para la recerca
    }
}
if (!trobat){ //Si no coincideix amb cap entrada de la taula
    descarta_datagrama(); //Es descarta el datagrama
    envia_notificacio(); //S'envia un missatge ICMP d'error
}

```

Un encaminador ordena les entrades de la seva taula de *routing* segons les seves màscares, de més específiques (255.255.255.255) a menys específiques (0.0.0.0), o, dit d'una altra manera, de màscares amb més 1's a màscares amb menys 1's. A causa d'aquesta ordenació, la ruta per defecte, en cas que existeixi, ocuparia sempre l'última entrada en la taula de *routing*.

Quan un encaminador rep un datagrama, extreu la seva adreça IP destinació, i accedeix a la taula de *routing* per iniciar la recerca d'una interfície de sortida. Començant per la primera entrada, va comprovant que l'AND bit a bit entre `IP_destinacio_datagrama` i la màscara de l'entrada sigui igual a la destinació d'aquella entrada. Quan troba una coincidència, deixa la recerca i encamina el paquet per la interfície de l'entrada coincident. Si no troba cap coincidència, aquest paquet es descartaria.

AND bit a bit

AND bit a bit és l'operació lògica binària que permet comprovar la coincidència entre adreces IP a gran velocitat, necessària en qualsevol encaminador, i en especial els que gestionen molts paquets.

Una ruta per defecte evitaria en última instància que el paquet fos descartat, ja que una entrada amb adreça destinació 0.0.0.0 i màscara 0.0.0.0 sempre trobarà coincidència amb qualsevol IP destinació (`IP_destinacio_datagrama AND 0.0.0.0 = 0.0.0.0`).

3.4. Encaminament entre VLANs

Definim una VLAN como una xarxa *broadcast*. Cada un dels ports d'un encaminador és una xarxa *broadcast* per definició i per tant una xarxa IP. Per estalviar ports d'encaminador es poden crear xarxes *broadcast* (xarxes IP) fent servir commutadors que tinguin mòduls programari de nivell 3. Això significa que amb un port d'encaminador connectat a un commutador es poden crear tantes VLANs (xarxes *broadcast*) com el programari del commutador ho permeti. Un commutador Cisco de la gama 2950 permet crear fins a 1024 VLANs.

És evident que si un port d'encaminador ha de suportar N VLANs (N xarxes IP), el port haurà de tenir N adreces IP, una per cada VLAN creada. També es evident que per viatjar des d'una VLAN a una altra s'ha de passar obligatòriament per l'encaminador. És a dir, no es pot anar d'una VLAN a una altra directament per mitjà del commutador, de la mateixa manera que el tràfic *broadcast* de

nivell 2 (per exemple les trames ARP) no es propaguen entre VLANs diferents. Per aconseguir aquesta segmentació de nivell 3 s'utilitza un protocol específic anomenat *trunking*. L'estàndard de *trunking* és el protocol IEEE802.1Q.

Quan encenem un commutador Cisco, tots els ports pertanyen a la VLAN nativa. La VLAN nativa per definició és la VLAN-ID=1. Si es defineix una VLAN per a un ús específic és millor fer servir altres VLAN-ID diferents a 1.

A continuació detallem els passos per realitzar un encaminament entre VLANs:

1) Definició de les VLANs en un commutador:

```
Sw(config)#vlan VLAN-ID //VLAN-ID pot tenir el rang entre 0001 i 1005
Sw (config-vlan)# name VLAN-NAME
Sw (config-vlan)#exit
Sw (config)#
```

2) Assignació de VLANS als ports d'un commutador. S'ha de fer servir la comanda `switchport`:

```
Sw(config)# interface e0/1
Sw(config-if)# switchport mode access //Defineix VLANs en mode estàtic
Sw(config-if)# switchport access vlan VLAN-ID //Assigna el port a la VLAN amb identificador VLAN-ID
Sw(config-if)# exit
```

3) Definició de l'enllaç entre el commutador i l'encaminador com un enllaç de tipus *trunk*. L'enllaç *trunk* és el que pertany a totes les VLANs creades. Ha d'estar assignat a la VLAN nativa (VLAN=1):

```
Sw(config)# interface fastethernet0/1
Sw(config-if)# switchport mode trunk
Sw(config-if)# exit
Sw(config)# exit
```

4) Comandes per comprovar la configuració del commutador:

- `show vlan`: mostra totes les VLANs existents.
- `show vlan VLAN-ID`: mostra paràmetres d'una VLAN determinada.
- `show interfaces IFACE switchport`: mostra el mode administratiu (accés estàtic), el mode d'accés de la VLAN (vlan-id), etc.
- `show interfaces IFACE trunk`: mostra paràmetres d'un enllaç tipus *trunk*.

5) Configuració de l'encaminador perquè entengui les VLANs creades:

L'enllaç de l'encaminador ha de ser de tipus *trunk* i ha de tenir tantes adreces IP com VLANs hagin estat creades. Per això s'han de crear tantes subinterfícies lògiques a la mateixa interfície física com VLANs s'hagin definit. A cada subinterfície se li assignarà una encapsulació dot1q (corresponen al protocol de *trunking* IEEE 802.1Q), juntament amb l'identificador de VLAN-ID. També se li assignarà una IP:

```
R(config)# int fastethernet 0/0
R(config-if)# no ip address
R(config-if)# int fastethernet 0/0.1
R(config-subif)# encapsulation dot1q VLAN-ID2
R(config-subif)# ip address @IP2 MASK2
R(config-subif)# exit
R(config-if)# int fastethernet 0/0.2
R(config-subif)# encapsulation dot1q VLAN-ID3
R(config-subif)# ip address @IP3 MASK3
R(config-subif)# exit
R(config-if)# exit
R(config)# exit
```

A la taula de *routing* hi ha d'haver una entrada per a cada subinterfície i la seva subxarxa IP.

3.4.1. Característiques del VLAN Trunking Protocol

Algunes de les característiques del VLAN Trunking Protocol són:

- Va ser desenvolupat per gestionar la transferència de trames de diferents VLANs en una única línia física o *trunk*.
- Evita enllaçar un cable per cada VLAN entre dos commutadors o entre un encaminador i un commutador.
- Un enllaç *trunk* agrupa múltiples enllaços virtuals sobre un únic enllaç físic (figura 17a), afegint etiquetes especials a les trames per identificar a quina VLAN pertany (figura 17b).

Figura 17a. Exemple de VLAN Trunking Protocol

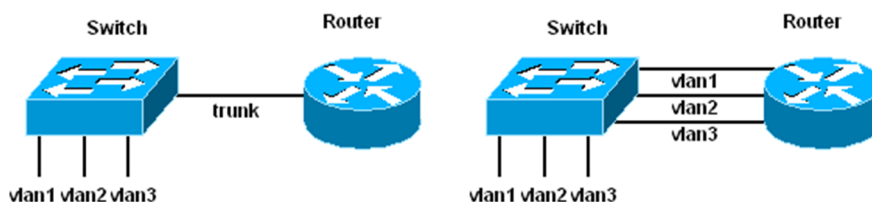
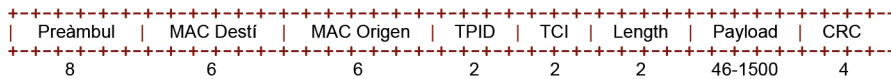


Figura 17b. Etiquetat de la trama Ethernet amb l'estàndard IEEE 802.1Q



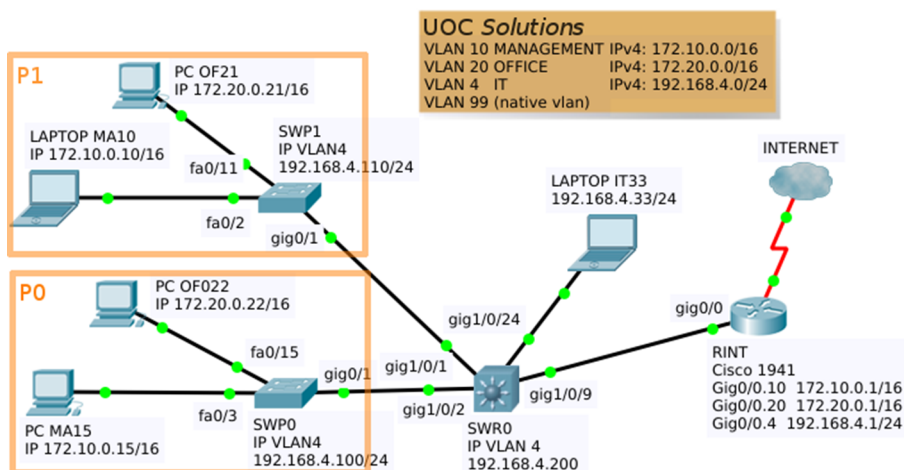
3.4.2. Estàndard IEEE-802.1Q

Afegeix una etiqueta de 4 bytes a la capçalera Ethernet de la trama per indicar a quina VLAN pertany. El *tag* està format pels camps següents (figura 17b):

- TPID (Tag Protocol Identifier): porta el valor 0x8100 quan el *tag* s'ha afegit a una trama Ethernet.
- TCI (Tag Control Information): porta el VLAN ID a la qual pertany la trama.

3.4.3. Exemple d'encaminament entre VLANs

En el següent cas pràctic es proposa configurar la distribució de xarxes virtuals (VLAN) de l'empresa fictícia UOC Solutions, tal com es mostra a la figura 18.

Figura 18. Esquema xarxa **Cas pràctic 2. UOC Solutions**

Les oficines d'aquesta empresa ocupen dues plantes d'un edifici comercial, els equips de cada planta es connecten a un commutador (SWP0 i SWP1), els commutadors de planta es connecten per un enllaç troncal al commutador principal (SWR0), i aquest es connecta també per un enllaç troncal a l'encaminador (RINT) que dona l'accés a Internet.

Els dispositius de la xarxa d'aquesta empresa estan segmentats en tres grups: ordinadors de direcció (VLAN 10), ordinadors d'empleats (VLAN 20) i equiptaments diversos del departament d'informàtica (VLAN 4).

Cada VLAN té assignada una xarxa IPv4 per configurar els seus equips. A l'esquema de la figura 18 s'indiquen les adreces dels equips i dels dispositius de xarxa. S'han posat només uns quants equips a tall d'exemple.

A la taula 4 s'indica la distribució de ports per als dos models de commutadors.

Taula 4. Configuració VLAN de ports dels commutadors UOC Solutions

Dispositiu	Ports d'accés		Ports troncats		VLAN nativa
	Ports	VLAN	Ports	VLAN	
Commutadors SWP0 i SWP1	fa0/1-4	10	gig0/1-2	4 - 99	99
	fa0/5-23	20			99
	fa0/24	4			99
Commutador SWR0	gig1/0/24	4	gig1/0/1-23	4 - 99	99

Es demana configurar la distribució VLAN als commutadors segons els requeriments indicats, i configurar l'encaminador per tal que permeti la comunicació entre tots els equips de les diferents VLAN.

A continuació es proposa la solució implementada amb el programari de simulació de xarxes Packet Tracer. S'inclouen les configuracions des de CLI pas a pas dels commutadors SWP1 i SWR0, i de l'encaminador RINT, i les proves de connectivitat entre els dispositius finals.

Solució. Configuració commutador SWP1

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWP1
SWP1(config)#vlan 4
SWP1(config-vlan)#name IT
SWP1(config-vlan)#vlan 10
SWP1(config-vlan)#name MANAGEMENT
SWP1(config-vlan)#vlan 20
SWP1(config-vlan)#name OFFICE
SWP1(config-vlan)#vlan 99
SWP1(config-vlan)#exit
SWP1(config)#interface range fastEthernet 0/1-4
SWP1(config-if-range)#switchport mode access
SWP1(config-if-range)#switchport access vlan 10
SWP1(config-if-range)#exit
SWP1(config)#interface range fastEthernet 0/5-23
SWP1(config-if-range)#switchport mode access
SWP1(config-if-range)#switchport access vlan 20
```

```
SWP1(config-if-range)#ex
SWP1(config)#interface fastEthernet 0/24
SWP1(config-if)#switchport mode access
SWP1(config-if)#switchport access vlan 4
SWP1(config-if)#exit
SWP1(config)#interface range gigabitEthernet 0/1-2
SWP1(config-if-range)#switchport mode trunk
SWP1(config-if-range)#switchport trunk allowed vlan 4-99
SWP1(config-if-range)#switchport trunk native vlan 99
SWP1(config-if-range)#exit
SWP1(config)#interface vlan 4
SWP1(config-if)#ip address 192.168.4.110 255.255.255.0
SWP1(config-if)#no shutdown
SWP1(config-if)#do wr
Building configuration...
[OK]
SWP1(config-if)#
```

Solució. Configuració commutador SWR0

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWR0
SWR0(config)#vlan 4
SWR0(config-vlan)#name IT
SWR0(config-vlan)#vlan 10
SWR0(config-vlan)#name MANAGEMENT
SWR0(config-vlan)#vlan 20
SWR0(config-vlan)#name OFFICE
SWR0(config-vlan)#vlan 99
SWR0(config-vlan)#exit
SWR0(config)#interface gigabitEthernet 1/0/24
SWR0(config-if)#switchport mode access
SWR0(config-if)#switchport access vlan 4
SWR0(config-if)#exit
SWR0(config)#interface range gigabitEthernet 1/0/1-23
SWR0(config-if-range)#switchport trunk encapsulation dot1q
SWR0(config-if-range)#switchport mode trunk
SWR0(config-if-range)#switchport trunk native vlan 99
SWR0(config-if-range)#switchport trunk allowed vlan 4-99
SWR0(config-if-range)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
SWR0(config-if-range)#
```


Solució. Configuració encaminador RINT

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RINT
RINT(config)#interface gigabitEthernet 0/0.4
RINT(config-subif)#encapsulation dot1Q 4
RINT(config-subif)#ip address 192.168.4.1 255.255.255.0
RINT(config-subif)#no shutdown
RINT(config-subif)#exit
RINT(config)#interface gigabitEthernet 0/0.10
RINT(config-subif)#encapsulation dot1Q 10
RINT(config-subif)#ip address 172.10.0.1 255.255.0.0
RINT(config-subif)#no shutdown
RINT(config-subif)#exit
RINT(config)#interface gigabitEthernet 0/0.20
RINT(config-subif)#encapsulation dot1Q 20
RINT(config-subif)#ip address 172.20.0.1 255.255.0.0
RINT(config-subif)#exit
RINT(config)#interface gigabitEthernet 0/0.99
RINT(config-subif)#encapsulation dot1Q 99 native
RINT(config-subif)#do wr
Building configuration...

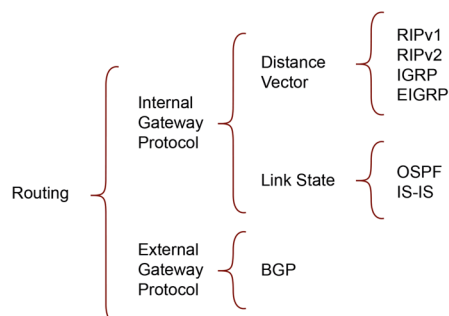
[OK]
RINT(config-subif)#

```

3.5. Configuració dels protocols d'encaminament

Els encaminadors han de construir una taula de rutes per saber on redirigir els paquets que viatgen per la xarxa. Per aconseguir-ho, intercanvien entre si informació sobre les xarxes que tenen directament connectades a les seves interfícies. Perquè un encaminador pugui dur a terme aquest intercanvi, s'ha de configurar un protocol d'encaminament. A la figura 19 es mostra la classificació dels principals protocols d'encaminament.

Figura 19. Classificació dels principals protocols d'encaminament



Per veure la taula de rutes actual d'un encaminador es pot executar, en mode privilegiat, la comanda `show ip route`.

Hi ha diferents tipus de protocols d'encaminament i un dispositiu només pot intercanviar dades amb d'altres amb qui comparteixi algun protocol. Per configurar cada protocol, cal entrar en un mode especial de configuració de rutes, accessible des del mode de configuració amb la comanda `router <nom protocol>`.

3.5.1. Distància administrativa d'un protocol d'encaminament

És una mesura utilitzada als encaminadors Cisco que defineix la fiabilitat d'un protocol d'encaminament. Quan hi ha dues o més rutes cap a una mateixa destinació, de diferents protocols d'encaminament, la distància administrativa ajuda en l'elecció de la millor ruta (la més fiable). Les rutes amb distància administrativa baixa són les més fiables. Per exemple, una ruta OSPF (veure la Secció 2.5.2), amb distància administrativa 110, es considera més fiable que una ruta RIP amb distància administrativa 120. La taula 5 mostra les distàncies administratives per defecte que fan servir els encaminadors Cisco.

Taula 5. Distàncies administratives que utilitzen els encaminadors Cisco

Protocol	Distància administrativa
Directament connectat	0
Ruta estàtica amb Gateway de següent salt	1
Ruta EIGRP resumida	5
BGP externa	20
EIGRP interna	90
IGRP	100
OSPF	110
RIP	120
EGP	140
EIGRP externa	170
BGP interna	200
Desconeguda (descartada)	255

3.5.2. Encaminament amb OSPF

OSPF (Open Shortest Path First) és un protocol d'encaminament d'estat de l'enllaç considerat de porta d'enllaç interna. Fa ús de l'algorisme SPF (anomenat també de Dijkstra), per calcular la ruta més curta (de més baix cost) entre dos nodes. La seva mètrica es denomina *cost*, i té en compte diversos paràmetres com ara l'ample de banda i la congestió dels enllaços.

Per configurar-lo en la seva forma més simple, cal indicar un nombre de procés a la comanda `router`:

```
Router(config): router ospf <process id>
```

Aquest valor process ID no segmenta la xarxa, només serveix com a identificador del procés intern al dispositiu. Per tant, és d'importància local i pot diferir entre encaminadors.

Cal publicar les xarxes connectades a l'encaminador, les quals s'introdueixen amb la comanda `network`:

```
Router(config-router): network 192.168.10.0 0.0.0.255 area 0
```

En aquest cas, però, cal especificar una *wildcard*, que equival a la màscara de subxarxa, però invertint els 1's i els 0's. Per exemple, per publicar la subxarxa 192.168.10.0/24, cal usar com a *wildcard* 0.0.0.255. També cal afegir un paràmetre amb el nombre d'àrea, que és realment el valor que segmenta les zones on es publica OSPF (de manera semblant al nombre de sistema a EIGRP, protocol que veurem al subapartat 3.5.3).

En tots els casos, en mode de configuració de rutes és possible desactivar la publicació en una interfície amb la comanda `passive-interface`:

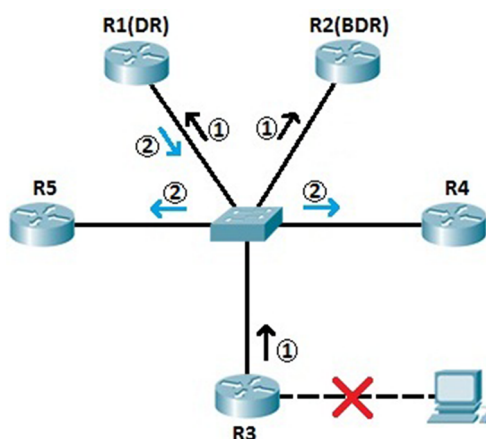
```
Router(config-router): passive-interface <nom interfície>
```

Això evita malbaratar ample de banda en xarxes on no hi ha cap altre encaminador amb el qual intercanviar informació.

Relacions d'adjacència en OSPF: encaminadors DR i BDR

OSPF es basa en establir i mantenir relacions de veïnatge perquè els encaminadors puguin compartir informació d'encaminament i de l'estat de l'enllaç. Cada encaminador s'ha de connectar com a mínim a un encaminador en cada xarxa IP a la qual estigui directament connectat. Però en xarxes multiaccés broadcast (com Ethernet), el nombre de possibles adjacències creix quadràticament amb el nombre d'encaminadors existents (figura 20).

Figura 20. Encaminadors DR i BDR en una xarxa multiaccés Ethernet



La solució consisteix a designar un encaminador que faci de portaveu d'aquella xarxa o segment (Designated Router o DR). Com que aquesta solució representa tenir un únic punt de fallada, es tria un segon encaminador designat com a *backup* per si falla el principal (Backup Designated Router o BDR). Els encaminadors DR i BDR actuen com a punt central per a l'intercanvi d'informació d'encaminament OSPF en una xarxa multiaccés concreta. Cada encaminament només intercanviarà informació (establirà adjacències) amb el DR i el BDR. El DR i el BDR distribuïran informació de topologia a qualsevol altre encaminador dins de la mateixa xarxa multiaccés, reduint considerablement el trànsit OSPF. Quan el DR cau, el BDR es fa amb el control i es tria un altre BDR.

Elecció DR/BDR

En els enllaços de punt a punt, no es tria un DR i un BDR, ja que només hi ha dos encaminadors connectats directament. A les xarxes LAN, s'ha de triar un DR i un BDR que representin la xarxa. S'utilitzen dues regles per triar un DR i un BDR:

- L'encaminador amb la màxima prioritat OSPF es convertirà en un DR. Per defecte, tots els encaminadors tenen una prioritat d'1. Manualment es pot configurar la prioritat OSPF amb la comanda `ip ospf priority <value>`.
- Si no es decideix la prioritat, es triarà l'encaminador amb el *router ID* més alt.

Assignació del *router ID* en un encaminador

Hi ha el següent ordre de precedència en l'assignació del *router ID* en un encaminador:

- És possible assignar manualment el valor a cada procés d'OSPF amb la comanda `router-id X.X.X.X`.
- En cas que no es tingui configurat de forma manual el *router ID*, els encaminadors utilitzen l'adreça IPv4 més alta configurada en les interfícies *loopback* per assignar el *router ID* (sempre que les interfícies no estiguin desactivades).
- Per últim, si no es té configurat el valor de *router ID* de manera manual, o no s'ha configurat cap interfície *loopback* en estat actiu, s'utilitzen les adreces IPv4 de les interfícies físiques com a valor per a aquest paràmetre. També cal que la interfície es trobi en estat actiu.

Paquets d'OSPF

Alguns dels paquets d'OSPF són:

- *Hello*: ajuden a establir i a mantenir relacions d'adjacència amb els encaminadors veïns. Els paquets *Hello* són emesos cada deu segons per la interfície d'un encaminador per indicar que continua actiu i per mantenir i establir relacions de veïnatge. És el temps per determinar si un veí ha caigut o no.
- *LSA* o anunci de l'estat de l'enllaç: anuncien la relació entre l'estat de les interfícies i adjacències d'un encaminador, amb els canvis que es produeixen a la xarxa. Avisen els encaminadors de la xarxa dels canvis de topologia.

Funcionament bàsic d'OSPF

Hem de tenir en compte el següent:

- Mitjançant l'enviament de *LSA*, els encaminadors intercanvien el seu coneixement de la xarxa (mètriques) amb la resta d'encaminadors de la xarxa. Els *LSA* s'envien per *flooding*: es reenvia un missatge per totes les interfícies d'un encaminador, excepte per la qual ha arribat. Si a un encaminador li arriba per segona vegada el mateix *LSA*, llavors el descarta.
- Només s'envien davant canvis de la topologia. Tota la xarxa n'és advertida per mitjà d'un *LSA*.
- Cada encaminador fa servir la informació dels paquets *Hello* i *LSA* rebuts per construir una base de dades topològica de la xarxa.
- A la base de dades topològica se li aplica l'algoritme Dijkstra (SPF) per calcular la ruta més curta cap a una destinació.

- S'obté l'arbre SPF cap a totes les destinacions on l'encaminador arrel és l'encaminador local.
- Se seleccionen les millors rutes de l'arbre SPF i s'insereixen a la taula de *routing*.

Exemple d'encaminament amb OSPFv2

Donada la xarxa de la figura 21a, es vol activar el protocol OSPF als encaminadors Router0 i Router1 per tal que coneguin totes les rutes de la xarxa.

A la figura 21b es mostra la configuració de les interfícies dels dos encaminadors i dels dos ordinadors. S'ha de tenir en compte la velocitat de la interfície serial DCE de Router0 amb la comanda `clock rate`. A la figura 21c es mostra l'activació del protocol OSPF en cada encaminador. S'ha utilitzat la forma completa d'activació, si bé és cert que en aquest cas les comandes `router-id` i `passive-interface` no són necessàries o es podrien ometre. Després de configurar Router1, el seu sistema ja indica que ha contactat i establert una relació d'adjacència amb l'encaminador veí 1.1.1.1 (que és el Router0).

A la figura 21d s'observen les taules de *routing* dels dos encaminadors. Per exemple, Router0 té dues xarxes directament connectades (192.168.0.0/24 i 192.168.1.0/30) i ha après la xarxa 192.168.2.0/24 mitjançant OSPF, amb una distància administrativa de 110 i una mètrica de 65. A la figura 21e es pot veure que la connectivitat entre tots els ordinadors de la xarxa és completa.

Figura 21a. Xarxa formada per tres subxarxes i dos encaminadors.

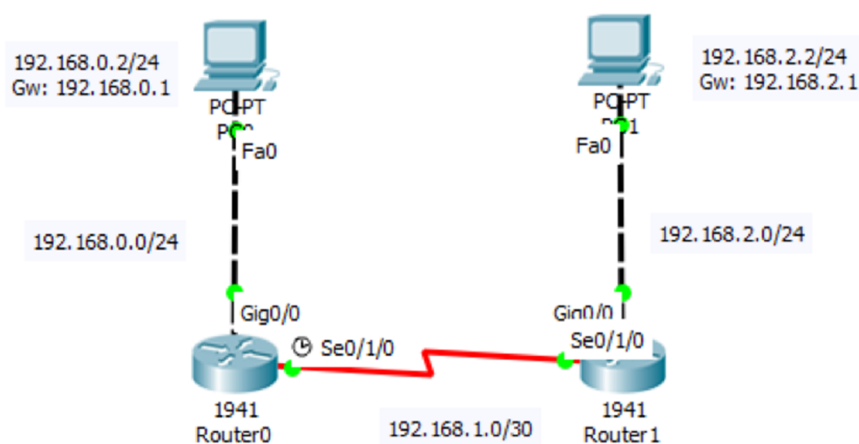


Figura 21b. Configuració de les interfícies dels encaminadors i dels ordinadors

```

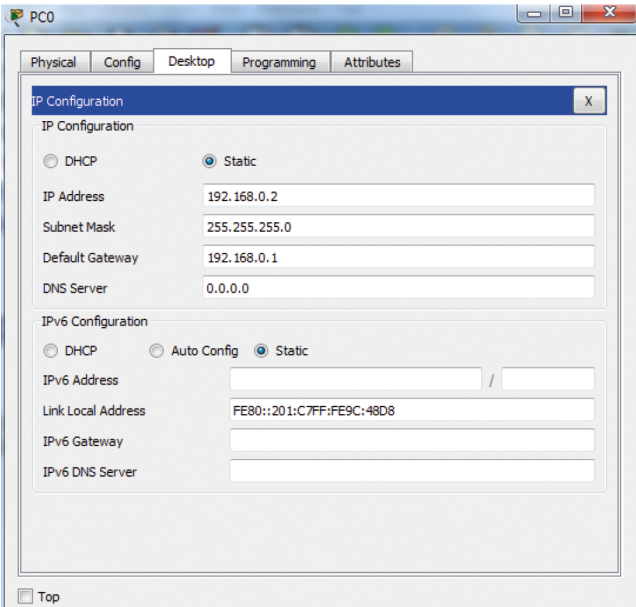
Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface Gig0/0
Router0(config-if)#ip address
192.168.0.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface se0/1/0
Router0(config-if)#clock rate 4000000
Router0(config-if)#no shutdown
Router0(config-if)#ip address
192.168.1.1 255.255.255.252
Router0(config-if)#exit

```

```

Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Gig0/0
Router1(config-if)#ip address
192.168.2.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface se0/1/0
Router1(config-if)#no shutdown
Router1(config-if)#ip address
192.168.1.2 255.255.255.252
Router1(config-if)#exit

```



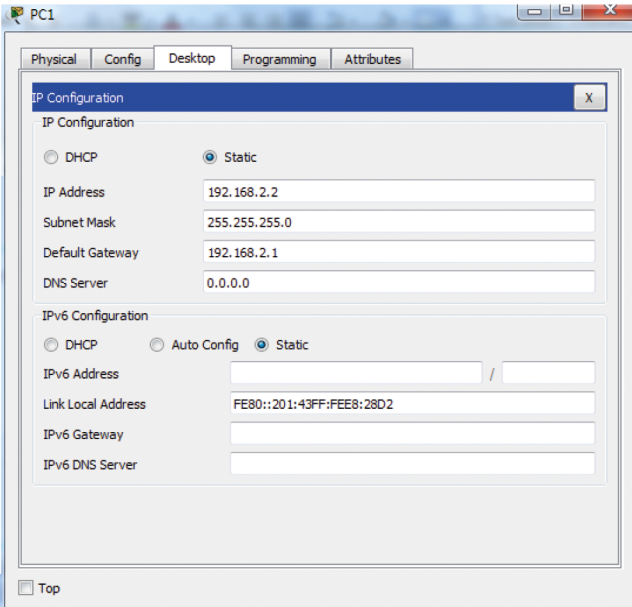


Figura 21c. Activació del protocol OSPF en cada encaminador

```

Router0(config)#router ospf 10
Router0(config-router)#router-id
1.1.1.1
Router0(config-router)#passive-
interface Gig0/0
Router0(config-router)#passive-
interface Gig0/1
Router0(config-router)#network
192.168.0.0 0.0.0.255 area 0
Router0(config-router)#network
192.168.1.0 0.0.0.3 area 0

```

```

Router1(config)#router ospf 10
Router1(config-router)#router-id
2.2.2.2
Router1(config-router)#passive-
interface Gig0/0
Router1(config-router)#passive-
interface Gig0/1
Router1(config-router)#network
192.168.2.0 0.0.0.255 area 0
Router1(config-router)#network
192.168.1.0 0.0.0.3 area 0
00:33:11: %OSPF-5-ADJCHG: Process
10, Nbr 1.1.1.1 on Serial0/1/0
from LOADING to FULL, Loading Done

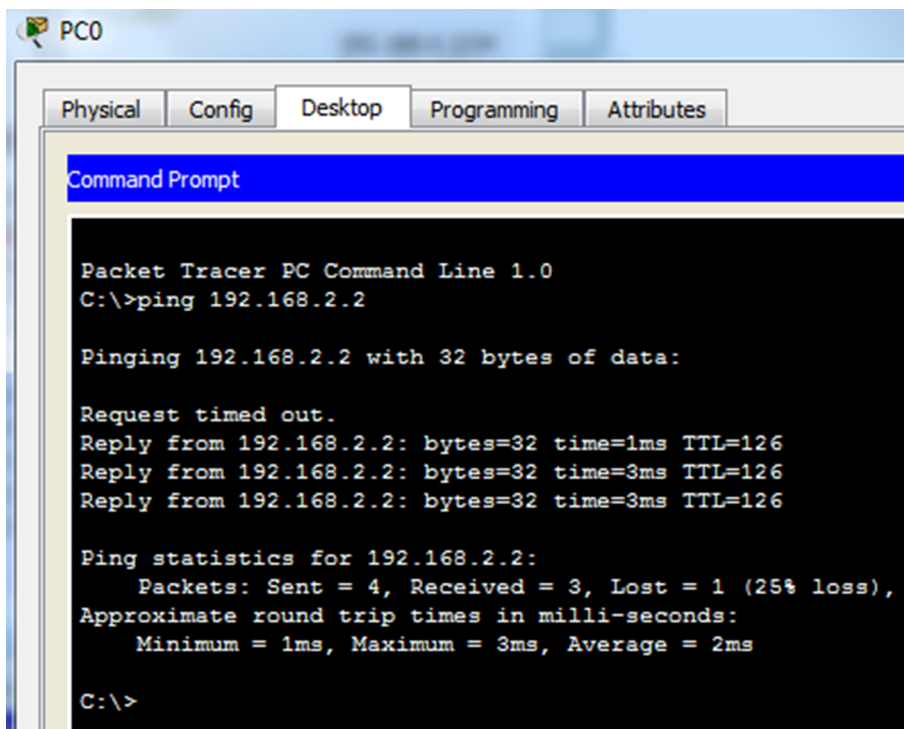
```

Figura 21d. Observació de la taula de *routing* de Router0 i Router1

```
Router0#show ip route
Codes: L - local, C - connected,
S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O
- OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 -
OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2
- IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-
user static route, o - ODR
P - periodic downloaded static
route
Gateway of last resort is not set
192.168.0.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly
connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly
connected, GigabitEthernet0/0
192.168.1.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.1.0/30 is directly
connected, Serial0/1/0
L 192.168.1.1/32 is directly
connected, Serial0/1/0
O 192.168.2.0/24 [110/65] via
192.168.1.2, 00:00:48,
Serial0/1/0
```

```
Router1#show ip route
Codes: L - local, C - connected,
S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O
- OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 -
OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2
- IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-
user static route, o - ODR
P - periodic downloaded static
route
Gateway of last resort is not set
O 192.168.0.0/24 [110/65] via
192.168.1.1, 00:00:00,
Serial0/1/0
192.168.1.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.1.0/30 is directly
connected, Serial0/1/0
L 192.168.1.2/32 is directly
connected, Serial0/1/0
192.168.2.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly
connected, GigabitEthernet0/0
L 192.168.2.1/32 is directly
connected, GigabitEthernet0/0
```


Figura 21e. Comprovació de la connectivitat entre els ordinadors



Comandes d'observació de l'estat d'OSPF

A continuació es mostren una sèrie de comandes que ens poden ajudar a esbrinar l'estat del protocol OSPF un cop activat:

```
Router0#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead	Time	Address	Interface
2.2.2.2	0	FULL/ -	00:00:37	192.168.1.2	Serial0/1/0	

```
Router0#show ip ospf database
```

```
OSPF Router with ID (1.1.1.1) (Process ID 10)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	Checksum	Link count
1.1.1.1	1.1.1.1	366	0x80000005	0x002441	3
2.2.2.2	2.2.2.2	366	0x80000005	0x00b1ac	3

```
Router#show ip ospf
```

```
Routing Process "ospf 10" with ID 1.1.1.1
```

```
Supports only single TOS(TOS0) routes
```

```
Supports opaque LSA
```

```
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
```

```
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
```

```
Number of external LSA 0. Checksum Sum 0x000000
```

```
Number of opaque AS LSA 0. Checksum Sum 0x000000
```

```
Number of DCbitless external and opaque AS LSA 0
```

```
Number of DoNotAge external and opaque AS LSA 0
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0x00d9eb
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

```
Router0#show ip ospf interface
  GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.1/24, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.0.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Serial0/1/0 is up, line protocol is up
  Internet address is 192.168.1.1/30, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
  Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
```

```
Router0#show ip protocols
```

```

Routing Protocol is "ospf 10"

  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.0.0 0.0.0.255 area 0
    192.168.1.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    GigabitEthernet0/1
  Routing Information Sources:
  Gateway         Distance      Last Update
  1.1.1.1         110          00:11:08
  2.2.2.2         110          00:11:08
  Distance: (default is 110)

```

```

Router#debug ip ospf events
OSPF events debugging is on

Router#
00:43:47: OSPF: Rcv hello from 2.2.2.2 area 0 from Serial0/1/0 192.168.1.2
00:43:47: OSPF: End of hello processing
00:43:57: OSPF: Rcv hello from 2.2.2.2 area 0 from Serial0/1/0 192.168.1.2
00:43:57: OSPF: End of hello processing

```

3.5.3. Encaminament amb EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) és un protocol d'encaminament vector distància avançat, propietat de Cisco, que combina els avantatges dels algorismes de vector distància i de l'estat de l'enllaç. EIGRP millora les propietats de convergència i és més fàcil de configurar que OSPF. Fa servir el següent càlcul de mètrica:

$$\text{Mètrica} = [K1 * \text{ample de banda} + ((K2 * \text{ample de banda}) / (256 - \text{carga})) + (K3 * \text{retard}) * [K5 / (\text{confiabilitat} + K4)]$$

Quan K4 i K5 són 0, l'equació de la mètrica queda:

$$\text{Mètrica} = \text{Ample de banda} + \text{retard}$$

Per configurar el protocol EIGRP, cal afegir al final de la comanda `router` un nombre de sistema autònom:

```
Router(config): router eigrp <number sa>
```

El nombre de sistema autònom es fa servir per identificar tots els encaminadors que pertanyen a la xarxa. Només intercanviaran dades els equips configurats amb el mateix valor.

Posteriorment només cal introduir les adreces IP de les xarxes que es volen publicar amb la comanda `network`:

```
Router(config-router): network <ip xarxa> <wildcard>
```

Només es poden posar xarxes directament connectades al dispositiu via alguna interfície. També cal especificar una *wildcard*, que equival a la inversió de la màscara de la xarxa.

Amb la comanda `no auto-summary` s'indica a l'encaminador que no resumeixi les rutes que té:

```
Router(config-router): no auto-summary
```

Per defecte, el protocol EIGRP resumeix automàticament les subxarxes a la xarxa principal de classe cada vegada que travessen una frontera entre dues xarxes principals diferents. La comanda `no auto-summary` desactiva aquest comportament i fa publicitat de les subxarxes. Posem per cas que un encaminador té dues subxarxes 172.16.8.0/24 i 172.16.4.0/24 de classe B i una subxarxa 10.2.0.0/16 de classe A. Quan `auto-summary` està habilitat, l'encaminador anunciarà només la xarxa principal més gran resumida de classe B 172.16.0.0/16 per la seva interfície de classe A. Amb la comanda `no auto-summary` anunciaria les dues subxarxes.

Exemple d'encaminament amb EIGRP entre dos encaminadors

Donada la xarxa de la figura 22a, es vol activar el protocol EIGRP als encaminadors Router0 i Router1 per tal que coneguin totes les rutes de la xarxa.

A la figura 22b es mostra la configuració de les interfícies de tots els dispositius de la xarxa, tenint en compte la velocitat de la interfície serial DCE (comanda `clock rate`).

Per activar el protocol EIGRP en els dos encaminadors (figura 22c) es fan servir les comandes:

- `network` per indicar les xarxes directament connectades a l'encaminador i que prendran part del procés EIGRP.
- `no auto-summary`, que controla que s'anunciïn les xarxes sense resums.

A la figura 22c, després de configurar Router1, el seu sistema ja indica que ha contactat i establert una relació d'adjacència amb l'encaminador veí 192.168.30.1.

A la figura 22d s'observen les taules de *routing* dels dos encaminadors. Per exemple, Router1 ha après la xarxa 192.168.10.0/24 gràcies a EIGRP, la qual té una distància administrativa de 90 i una mètrica de 2172416. La figura 22e mostra que la connectivitat entre tots els ordinadors de la xarxa és completa.

Figura 22a. Xarxa formada per tres subxarxes i dos encaminadors

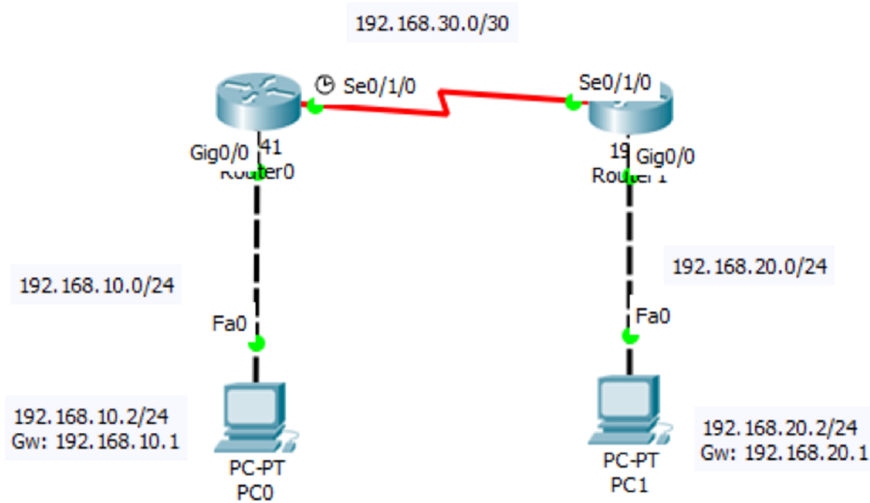


Figura 22b. Configuració de les interfícies dels encaminadors i dels ordinadors

```

Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface Gig0/0
Router0(config-if)#ip address
192.168.10.1 255.255.255.0
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface se0/1/0
Router0(config-if)#clock rate 4000000
Router0(config-if)#no shutdown
Router0(config-if)#ip address
192.168.30.1 255.255.255.252
Router0(config-if)#exit

```

```

Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Gig0/0
Router1(config-if)#ip address
192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface se0/1/0
Router1(config-if)#no shutdown
Router1(config-if)#ip address
192.168.30.2 255.255.255.252
Router1(config-if)#exit

```

Figura 22c. Activació del protocol EIGRP en cada encaminador

```

Router0(config)#router eigrp 10
Router0(config-router)#network
192.168.10.0 0.0.0.255
Router0(config-router)#network
192.168.30.0 0.0.0.3
Router0(config-router)#no auto-summary
Router0(config-router)#exit
Router0(config)#

```

```

Router1(config)#router eigrp 10
Router1(config-router)#network
192.168.20.0 0.0.0.255
Router1(config-router)#network
192.168.30.0 0.0.0.3
Router1(config-router)#no auto-summary
Router1(config-router)#exit
Router1(config)#
%DUAL-5-NBRCHANGE: IP-EIGRP 10:
Neighbor 192.168.30.1
(Serial0/1/0) is up: new adjacency

```

Figura 22d. Observació de la taula de *routing* de Router0 i Router1

```

Router0#show ip route
Codes: L - local, C - connected,
S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O
- OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 -
OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2
- IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-
user static route, o - ODR
P - periodic downloaded static
route
Gateway of last resort is not set
192.168.10.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly
connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly
connected, GigabitEthernet0/0
D 192.168.20.0/24 [90/2172416]
via 192.168.30.2, 00:00:07,
Serial0/1/0
192.168.30.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.30.0/30 is directly
connected, Serial0/1/0
L 192.168.30.1/32 is directly
connected, Serial0/1/0

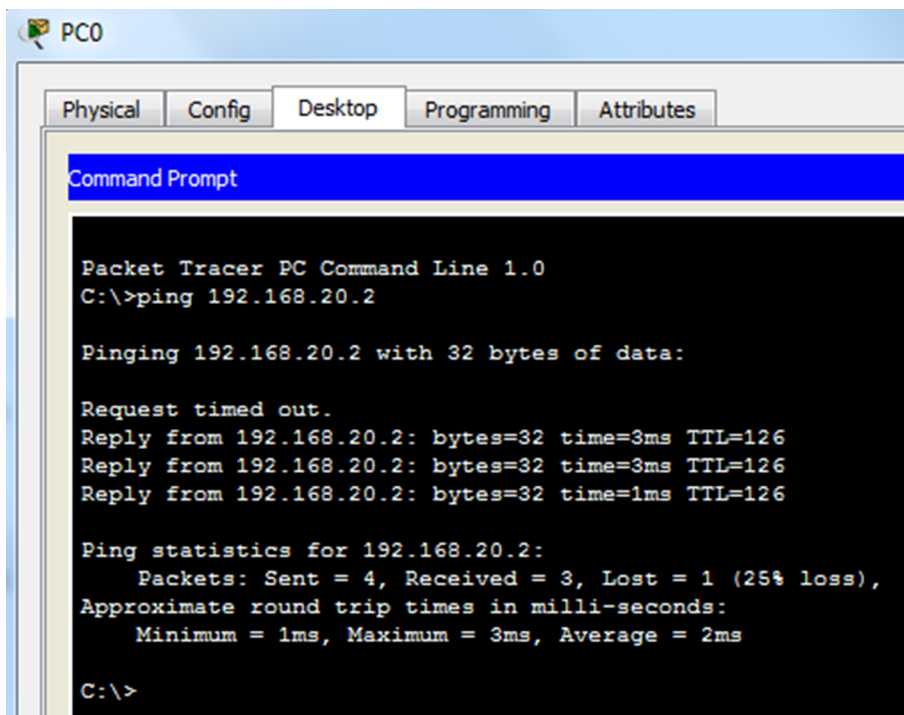
```

```

Router#show ip route
Codes: L - local, C - connected,
S - static, R - RIP, M - mobile,
B - BGP
D - EIGRP, EX - EIGRP external, O
- OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 -
OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2
- IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U -
per-user static route, o - ODR
P - periodic downloaded static
route
Gateway of last resort is not set
D 192.168.10.0/24 [90/2172416]
via 192.168.30.1, 00:00:53,
Serial0/1/0
192.168.20.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly
connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly
connected, GigabitEthernet0/0
192.168.30.0/24 is variably
subnetted, 2 subnets, 2 masks
C 192.168.30.0/30 is directly
connected, Serial0/1/0
L 192.168.30.2/32 is directly
connected, Serial0/1/0

```

Figura 22e. Comprovació de la connectivitat entre els ordinadors



Comandes d'observació de l'estat d'EIGRP

A continuació es mostren una sèrie de comandes que ens poden ajudar a esbrinar l'estat del protocol EIGRP un cop activat:

```
Router#show ip protocols
Routing Protocol is "eigrp 10 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 10
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.10.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1
    Automatic Summarization: disabled
    Automatic address summarization:
      Maximum path: 4
    Routing for Networks:
      192.168.10.0
```



```

192.168.30.0/30
Routing Information Sources:
  Gateway Distance Last Update
  192.168.30.2 90 5195
Distance: internal 90 external 170

```

```

Router1#show ip eigrp interfaces
IP-EIGRP interfaces for process 10

          Xmit Queue Mean Pacing Time Multicast Pending
Interface Peers    Un/Reliable  SRTT  Un/Reliable  Flow Timer  Routes
Gig0/0     0          0/0         1236  0/10         0           0
Se0/1/0    1          0/0         1236  0/10         0           0
Router#

```

```

Router1#show ip eigrp neighbors
IP-EIGRP neighbors for process 10

H Address           Interface      Hold Uptime    SRTT    RTO    Q    Seq
                   (sec)         (ms)          Cnt    Num
0 192.168.30.2      Se0/1/0       12 00:52:10   40     1000   0    3
Router#

```

3.6. Xarxes IPv6

IPv6 és la versió 6 del Protocol d'Internet (IP), dissenyada per substituir l'actual IPv4 a Internet, ja que l'espai d'adreçament d'IPv4 és a punt d'esgotar-se i la IANA està repartint els últims grups d'adreces.

La mida de les adreces IPv6 és de 128 bits, quatre vegades més gran que la mida de les adreces IPv4 de 32 bits.

Les adreces IPv6 es representen en vuit grups de quatre dígit hexadecimals. Per exemple, 2001:0DB8:85A3:08D3:1119:8A2E:0220:AB34 és una adreça IPv6 vàlida.

Si un grup de quatre dígit pren el valor nul "0000", llavors pot ser comprimit amb la notació "::" o ":0:". Per exemple, 2001:1111:1111:0000:2222:2222:2222:2222 és la mateixa adreça que 2001:1111:1111::2222:2222:2222:2222 o l'adreça 2001:1111:1111:0:2222:2222:2222:2222.

Si una adreça IPv6 té més d'una sèrie de grups nuls consecutius, també es pot comprimir amb "::", però sempre respectant que no hi hagi ambigüitats. Per exemple, l'adreça 2001::2222::3333 no és vàlida perquè no queda clar quants grups nuls hi ha a cada costat.

Una altra regla és que els zeros inicials en un grup poden ser omesos. Per exemple, l'adreça IPv6 2001:0111:0222::0333 també es pot representar com a 2001:111:222::333.

IPv6 fa servir la notació de la màscara compacta com ja s'utilitzava a IPv4. Per exemple, l'adreça 2001:20:20:20::1/64 indica que 64 bits és la part de subxarxa i els altres 64 bits representen la part de *host*.

3.6.1. Tipus d'adreces IPv6

Els tipus d'adreces IPv6 poden identificar-se tenint en compte els primers bits de cadascuna:

1) Adreces *Global Unicast* a IPv6

Les adreces *Global Unicast* a IPv6 són l'equivalent a les adreces IP públiques a IPv4. Són adreces úniques al món i es configuren una per cada interfície de *host*. Les adreces IPv6 *Global Unicast* són adreces IPv6 enrutables d'Internet.

Els tres primers bits d'aquestes adreces han de ser els valors 001 en notació binària, per tant el prefix d'aquestes adreces IP sempre tindrà un valor hexadecimal de 2XXX o 3XXX amb una màscara /3, que estableix el Global Routing Prefix.

Una adreça *Global Unicast* IPv6 de 128 bits es pot dividir en les parts següents:

- Prefix Global (3 primers bits).
- Xarxa assignada a les organitzacions (45 bits següents).
- Subxarxa (16 bits següents, per a 2^{16} possibles subxarxes).
- *Host* (64 bits, on cada subxarxa pot suportar 2^{64} nodes).

2) Adreces *Link Local*

Aquestes adreces IPv6 locals permeten la comunicació entre dispositius en un enllaç local. El prefix de l'adreça IPv6 local es FE80::/10, i especifica que aquesta adreça només és vàlida en aquest enllaç físic local.

- Les adreces IPv6 *Link Local* no són enrutables.
- Normalment s'assignen automàticament.
- Només es comunica amb altres interfícies a l'enllaç.
- Poden duplicar-se fora dels enllaços locals, ja que no interferiran entre si.

Es pot generar automàticament a partir de l'adreça MAC de la mateixa interfície amb la comanda:

```
Router(config-if)# ipv6 enable
```

També es poden indicar manualment amb la comanda:

```
Router(config-if)#ipv6 address FE80::1 Link Local
```

3) Adreces *multicast*

Una transmissió *multicast* envia paquets a totes les interfícies que són part del grup *multicast*. El grup ve representat per l'adreça IPv6 destinació del paquet. Les adreces IPv6 *multicast* comencen amb FF (FF00::/8). Les adreces IPv6 *multicast* més importants són:

FF02::1 - Tots els nodes en el segment local de la xarxa.

FF02::2 - Tots els encaminadors en el segment local de la xarxa.

4) Adreces *loopback*

L'adreça *loopback* d'IPv6 és la

0000:0000:0000:0000:0000:0000:0001/128,

que també pot representar-se com a ::1/128. S'utilitza per un node per enviar un paquet IPv6 a si mateix. Una adreça *loopback* IPv6 funciona igual que una adreça *loopback* IPv4 (correspon amb l'adreça 127.0.0.1 d'IPv4). No és assignable a cap interfície física.

5) Adreces *anycast*

Una transmissió *anycast* envia paquets a només una de les interfícies associades amb l'adreça, no a totes les interfícies. Aquesta interfície és normalment la interfície més propera, tal com defineix el protocol de *routing*.

3.6.2. Exemple: generació d'adreces *Link Local*

A la figura 23a es mostra un enllaç Ethernet entre un encaminador i un ordinador. Es pretén fer un *ping* entre ambdós dispositius fent servir només adreces *Link Local* d'IPv6.

A l'ordinador PC0 ja hi ha una adreça *Link Local* configurada per defecte (figura 23c). Per tant, només cal generar una adreça *Link Local* per a la interfície GigabitEthernet0/0 de Router0. Això es fa amb la comanda `ipv6 enable`, com es pot observar a la figura 23c.

A la figura 23b es mostra l'adreça MAC de la interfície GigabitEthernet0/0 de l'encaminador Router0: **0001:4235:D201**. Es pot comprovar observant el resultat de la comanda `show ipv6 interface brief` (figura 23d) que l'adreça *Link Local* IPv6 generada a la interfície Gig0/0 té una part de la seva adreça MAC: FE80::201:42FF:FE35:D201.

Des de PC0 es pot executar un *ping* amb èxit cap a l'adreça *Link Local* de la interfície GigabitEthernet0/0 generada anteriorment (figura 23e).

Figura 23a. Enllaç Ethernet entre un encaminador i un ordinador

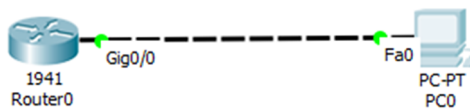


Figura 23b. Adreces MAC de les interfícies de l'encaminador

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	<not set>	<not set>	0001.4235.D201
GigabitEthernet0/1	Down	--	<not set>	<not set>	0001.4235.D202
Vlan1	Down	1	<not set>	<not set>	0010.111A.0678

Hostname: Router

Figura 23c. Configuració de les adreces *Link Local* a l'encaminador i a l'ordinador

```
Router>enable
Router#configure terminal
Router(config)#interface Gig0/0
Router(config-if)#ipv6 enable
Router(config-if)#no shutdown
Router(config-if)#exit
```

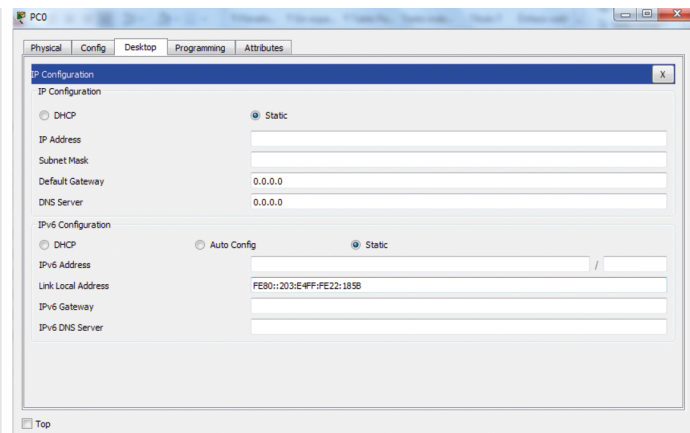
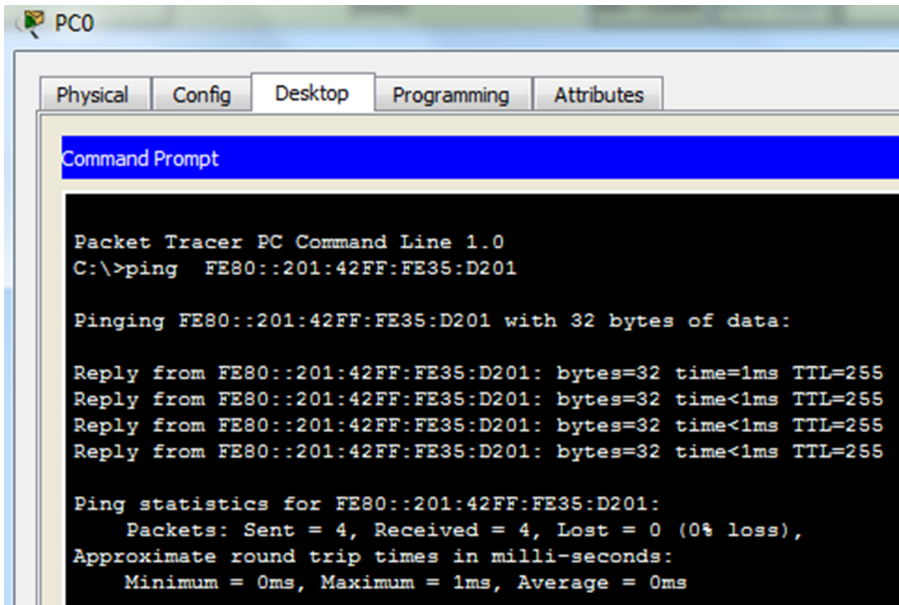


Figura 23d. Resultat de la comanda `show ipv6 interface brief` a l'encaminador

```
Router#show ipv6 interface brief
GigabitEthernet0/0 [up/up]
FE80::201:42FF:FE35:D201
GigabitEthernet0/1 [administratively down/down]
Vlan1 [administratively down/down]
```

Figura 23e. *Ping* realitzat amb adreces *Link Local* entre encaminador i ordinador


```

PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping FE80::201:42FF:FE35:D201

Pinging FE80::201:42FF:FE35:D201 with 32 bytes of data:

Reply from FE80::201:42FF:FE35:D201: bytes=32 time=1ms TTL=255
Reply from FE80::201:42FF:FE35:D201: bytes=32 time<1ms TTL=255
Reply from FE80::201:42FF:FE35:D201: bytes=32 time<1ms TTL=255
Reply from FE80::201:42FF:FE35:D201: bytes=32 time<1ms TTL=255

Ping statistics for FE80::201:42FF:FE35:D201:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

3.6.3. Exemple de configuració d'interfícies Ethernet amb adreces *Global Unicast*

A la figura 24a es mostra un enllaç Ethernet entre les interfícies d'un encaminador i d'un ordinador. Es vol aconseguir connectivitat IP entre ambdós equips fent servir adreces *Global Unicast* d'IPv6, com per exemple les de la xarxa 2001:10:10:10::/64. A la figura 24b es mostra la configuració IPv6 de les interfícies de l'encaminador i de l'ordinador. L'encaminador fa servir la comanda `ipv6 address` per configurar la seva interfície amb una adreça IPv6. Un cop realitzada la configuració es pot fer un *ping* amb èxit entre els dos dispositius (figura 24c).

Figura 24a. Enllaç Ethernet entre un encaminador i un ordinador amb adreçament IPv6

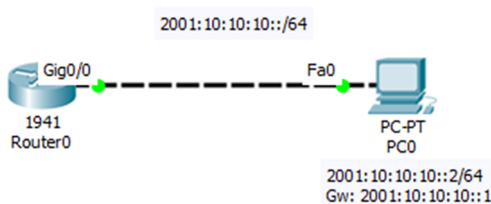


Figura 24b. Configuració de les interfícies dels encaminadors i de l'ordinador

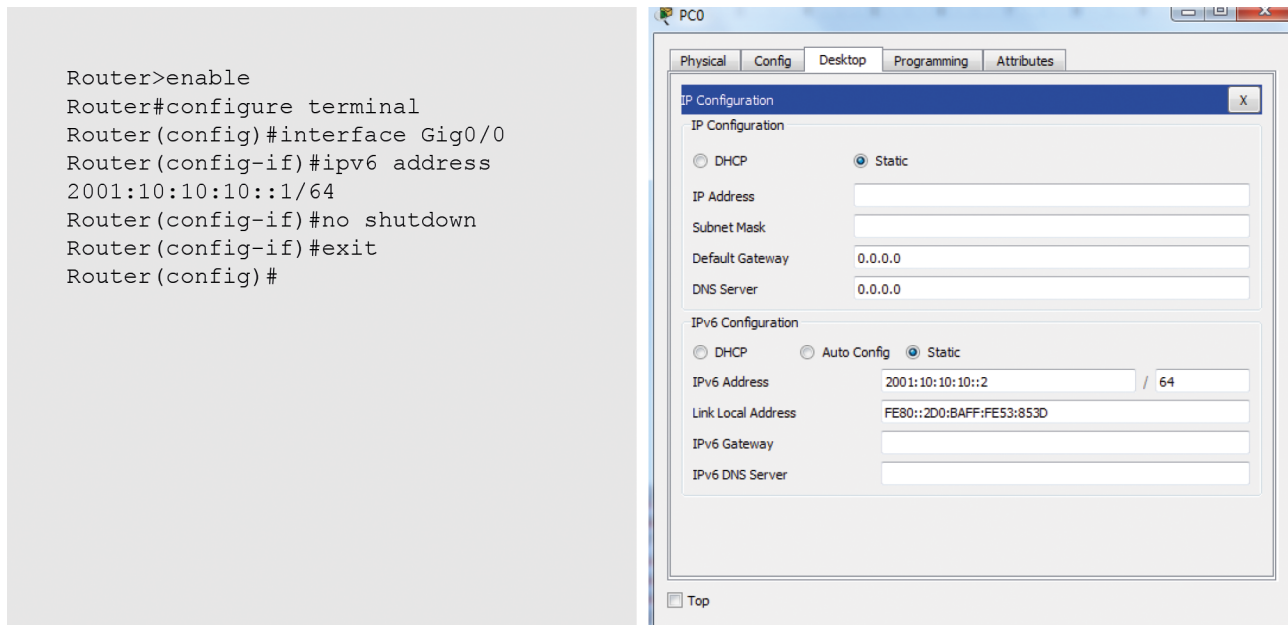
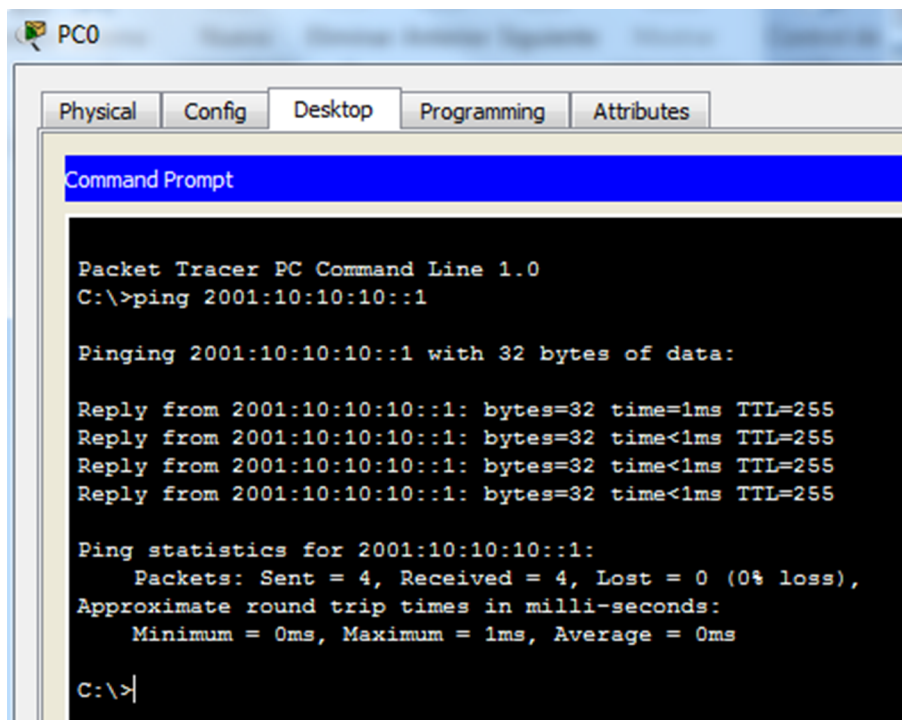


Figura 24c. Comprovació de la connectivitat entre PC0 i Router0

**Comanda IPv6 unicast-routing**

IPv6 unicast-routing és la comanda necessària per habilitar el reenviament de datagrames de unidifusió IPv6. Per deshabilitar el reenviament de datagrames d'unidifusió IPv6, s'ha de fer servir la negació d'aquesta comanda.

Comanda IPv6 route

Es l'equivalent de la comanda `ip route` a IPv4. Serveix per tant per indicar rutes estàtiques a l'encaminador, com per fer conèixer rutes no directament connectades a la taula de routing.

3.6.4. Exemple d'adreçament estàtic a IPv6

Donada la xarxa de la figura 25a, es vol aconseguir visibilitat IP entre els dos ordinadors PC0 i PC1, pertanyents a subxarxes IPv6 diferents. Cada encaminador està directament connectat a dues subxarxes, compartint la subxarxa 2001:20:20:20::/64. A la figura 25b es mostren les configuracions de les interfícies dels encaminadors Router0 i Router1 (amb la comanda `ipv6 address`) i dels ordinadors PC0 i PC1.

Figura 25a. Xarxa formada per dos encaminadors i tres subxarxes IPv6

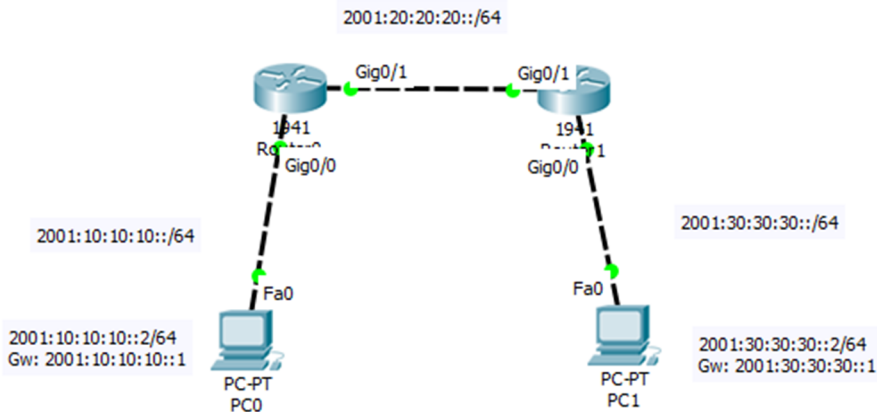


Figura 25b. Configuració de les interfícies dels encaminadors i dels ordinadors

```

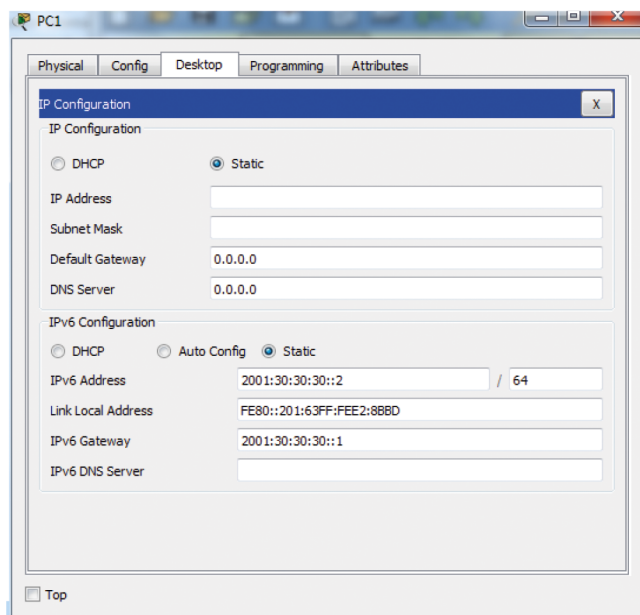
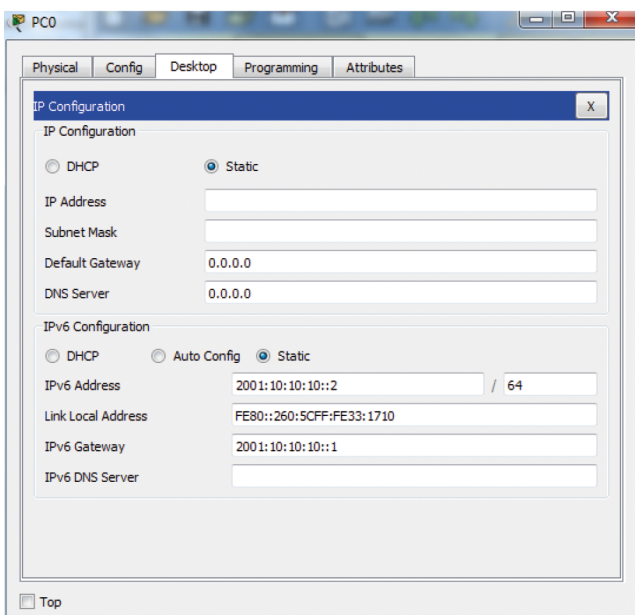
Router0(config)#ipv6 unicast-
routing
Router0(config)#interface
GigabitEthernet0/0
Router0(config-if)#no shutdown
Router0(config-if)#ipv6 address
2001:10:10:10::1/64
Router0(config-if)#interface
GigabitEthernet0/1
Router0(config-if)#ipv6 address
2001:20:20:20::1/64
Router0(config-if)#no shutdown
Router0(config-if)#exit

```

```

Router1(config)#ipv6 unicast-
routing
Router1(config)#interface
GigabitEthernet0/0
Router1(config-if)#no shutdown
Router1(config-if)#ipv6 address
2001:30:30:30::1/64
Router1(config-if)#interface
GigabitEthernet0/1
Router1(config-if)#ipv6 address
2001:20:20:20::2/64
Router1(config-if)#no shutdown
Router1(config-if)#exit

```



La situació és la mateixa que hi havia amb IPv4: Router0 coneix les xarxes 10 i 20 pel fet d'estar directament connectades, però desconeix la xarxa 30, i igualment Router1 coneix les xarxes 20 i 30, però desconeix la xarxa 10. Per tant, perquè els encaminadors de la xarxa coneguin totes les rutes, cal executar les següents comandes `ipv6 route` als encaminadors corresponents:

```
Router0(config)#ipv6 route
2001:30:30:30::/64
2001:20:20:20::2
```

```
Router1(config)#ipv6 route
2001:10:10:10::/64
2001:20:20:20::1
```

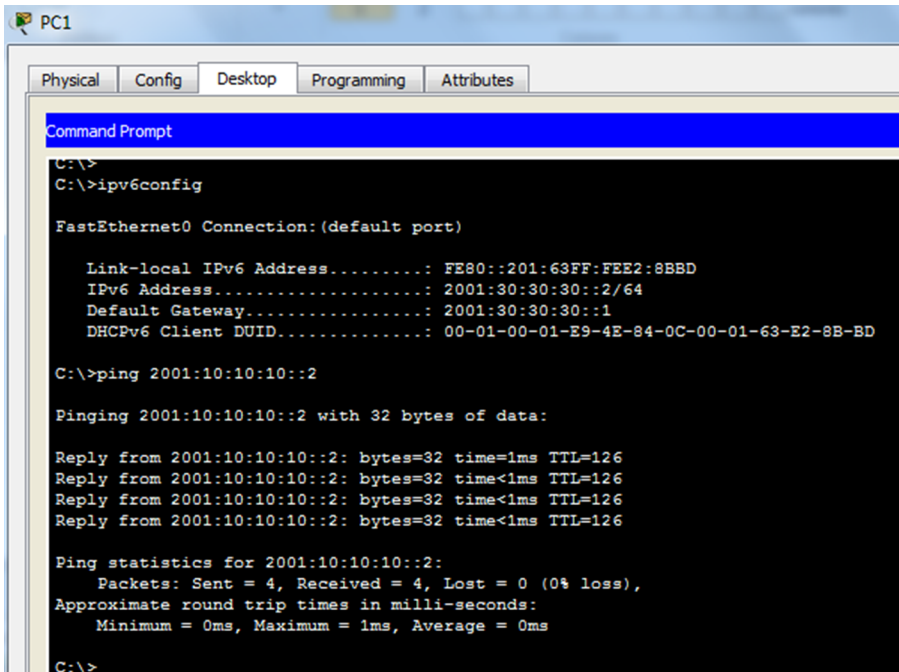
A la figura 25c es mostren les taules de *routing* de Router0 i Router1. S'ha afegit al Router1 la xarxa 10 amb el distintiu S (estàtic), que té una distància administrativa d'1 (molta fiabilitat). Al Router0 s'ha afegit la xarxa 30 de forma estàtica. En aquestes condicions un *ping* entre PC1 i PC0 funciona correctament (figura 25d):

Figura 25c. Taules de *routing* del Router0 i Router1

```
Router0#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local,
S - Static, R - RIP, B - BGP
U - Per-user Static route, M -
MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA -
ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter,
OE1 - OSPF ext 1, OE2 - OSPF ext
2
ON1 - OSPF NSSA ext 1, ON2 - OSPF
NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:10:10:10::/64 [0/0]
  via GigabitEthernet0/0, directly
connected
L 2001:10:10:10::1/128 [0/0]
  via GigabitEthernet0/0, receive
C 2001:20:20:20::/64 [0/0]
  via GigabitEthernet0/1, directly
connected
L 2001:20:20:20::1/128 [0/0]
  via GigabitEthernet0/1, receive
S 2001:30:30:30::/64 [1/0]
  via 2001:20:20:20::2
L FF00::/8 [0/0]
  via Null0, receive
Router0#
```

```
Router1#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local,
S - Static, R - RIP, B - BGP
U - Per-user Static route, M -
MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA -
ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter,
OE1 - OSPF ext 1, OE2 - OSPF ext
2
ON1 - OSPF NSSA ext 1, ON2 - OSPF
NSSA ext 2
D - EIGRP, EX - EIGRP external
S 2001:10:10:10::/64 [1/0]
  via 2001:20:20:20::1
C 2001:20:20:20::/64 [0/0]
  via GigabitEthernet0/1, directly
connected
L 2001:20:20:20::2/128 [0/0]
  via GigabitEthernet0/1, receive
C 2001:30:30:30::/64 [0/0]
  via GigabitEthernet0/0, directly
connected
L 2001:30:30:30::1/128 [0/0]
  via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
Router0#
```


Figura 25d. Ping amb èxit realitzat entre PC1 i PC0



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ipv6config

FastEthernet0 Connection: (default port)

Link-local IPv6 Address.....: FE80::201:63FF:FEE2:8BBD
IPv6 Address.....: 2001:30:30:30::2/64
Default Gateway.....: 2001:30:30:30::1
DHCPv6 Client DUID.....: 00-01-00-01-E9-4E-84-0C-00-01-63-E2-8B-BD

C:\>ping 2001:10:10:10::2

Pinging 2001:10:10:10::2 with 32 bytes of data:

Reply from 2001:10:10:10::2: bytes=32 time<1ms TTL=126
Reply from 2001:10:10:10::2: bytes=32 time<1ms TTL=126
Reply from 2001:10:10:10::2: bytes=32 time<1ms TTL=126
Reply from 2001:10:10:10::2: bytes=32 time<1ms TTL=126

Ping statistics for 2001:10:10:10::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

3.6.5. Exemple d'encaminament entre VLANs amb IPv6

La xarxa de la figura 26a està formada per un encaminador i un commutador amb suport per a VLANs. Es vol segmentar la xarxa en tres VLANs (en aquest cas tres subxarxes IPv6), utilitzant el mòdul de nivell 3 del qual disposa el commutador. En el primer pas s'han de configurar els ordinadors (figura 26b). A continuació s'han de crear les VLANs i assignar-les a cada port corresponent del commutador (figura 26c). S'ha de configurar també el port *trunking* del commutador. Finalment s'han de configurar les subinterfícies de l'encaminador (figura 26c). S'han de definir i configurar tantes subinterfícies lògiques sobre la mateixa interfície física Gig0/1, com el nombre de VLANs definides a la xarxa.

Un cop realitzades totes les configuracions, a la figura 26d es poden observar les entrades, a la taula de *routing* de l'encaminador, corresponents a les diferents subxarxes IPv6 definides sobre la mateixa interfície física.

La connectivitat entre ordinadors és total, com es pot observar a la figura 26e.

Figura 26a. Xarxa segmentada en tres VLANs

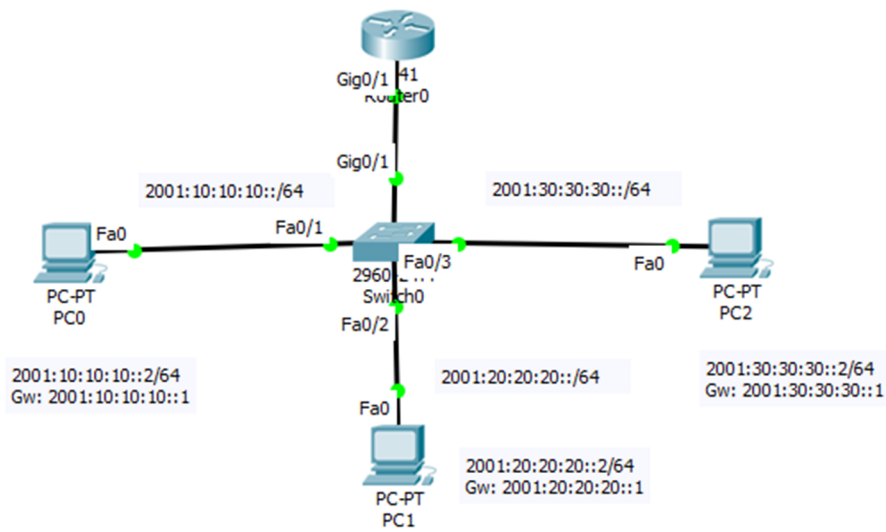


Figura 26b. Configuració dels ordinadors

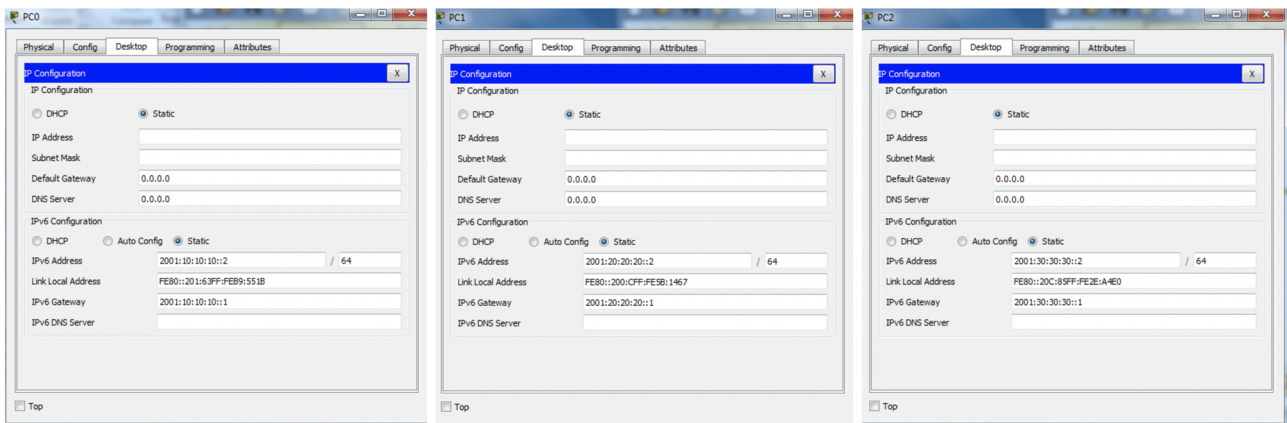


Figura 26c. Configuració del commutador i les subinterfícies de l'encaminador

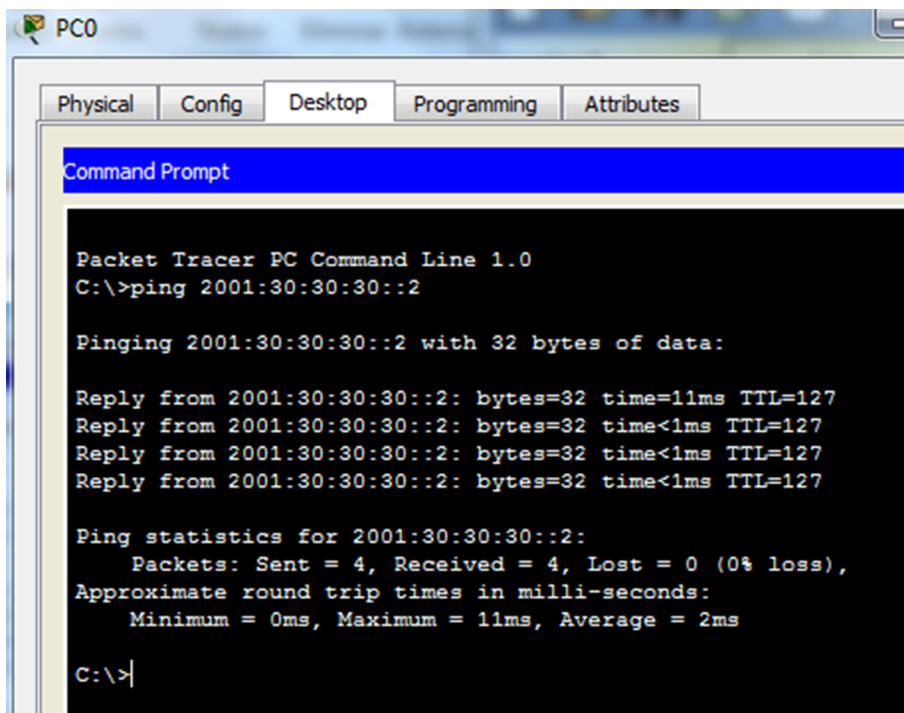
```
Switch>enable
Switch#configure terminal
Switch (config)#vlan 10
Switch (config-vlan)#exit
Switch (config)#vlan 20
Switch (config-vlan)#exit
Switch (config)#vlan 30
Switch (config-vlan)#exit
Switch (config)#interface fa0/1
Switch (config-if)#switchport
mode access
Switch (config-if)#switchport
access vlan 10
Switch (config-if)#exit
Switch (config)#interface fa0/2
Switch (config-if)#switchport
mode access
Switch (config-if)#switchport
access vlan 20
Switch (config-if)#exit
Switch (config)#interface fa0/3
Switch (config-if)#switchport
mode access
Switch (config-if)#switchport
access vlan 30
Switch (config-if)#exit
Switch (config)#interface Gig0/1
Switch (config-if)#switchport
mode trunk
Switch (config-if)#exit
```

```
Router>enable
Router#configure terminal
Router(config)#ipv6 unicast-
routing
Router(config)#interface gig0/1
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface
gig1/0.10
Router(config-
subif)#encapsulation dot1Q 10
Router(config-subif)#ipv6 address
2001:10:10:10::1/64
Router(config-subif)#exit
Router(config)#interface
gig0/1.20
Router(config-
subif)#encapsulation dot1Q 20
Router(config-subif)#ipv6 address
2001:20:20:20::1/64
Router(config-subif)#exit
Router(config)#interface
gig0/1.30
Router(config-
subif)#encapsulation dot1Q 30
Router(config-subif)#ipv6 address
2001:30:30:30::1/64
Router(config-subif)#exit
Router(config)#exit
```

Figura 26d. Taula de *routing* de Router0

```
Router#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route, M - MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:10:10:10::/64 [0/0]
  via GigabitEthernet0/1.10, directly connected
L 2001:10:10:10::1/128 [0/0]
  via GigabitEthernet0/1.10, receive
C 2001:20:20:20::/64 [0/0]
  via GigabitEthernet0/1.20, directly connected
L 2001:20:20:20::1/128 [0/0]
  via GigabitEthernet0/1.20, receive
C 2001:30:30:30::/64 [0/0]
  via GigabitEthernet0/1.30, directly connected
L 2001:30:30:30::1/128 [0/0]
  via GigabitEthernet0/1.30, receive
L FF00::/8 [0/0]
  via Null0, receive
Router#
```

Figura 26e. Comprovació de la connectivitat entre PC0 i PC2



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2001:30:30:30::2

Pinging 2001:30:30:30::2 with 32 bytes of data:

Reply from 2001:30:30:30::2: bytes=32 time=11ms TTL=127
Reply from 2001:30:30:30::2: bytes=32 time<1ms TTL=127
Reply from 2001:30:30:30::2: bytes=32 time<1ms TTL=127
Reply from 2001:30:30:30::2: bytes=32 time<1ms TTL=127

Ping statistics for 2001:30:30:30::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 2ms

C:\>|
```

3.7. Encaminament amb OSPFv3

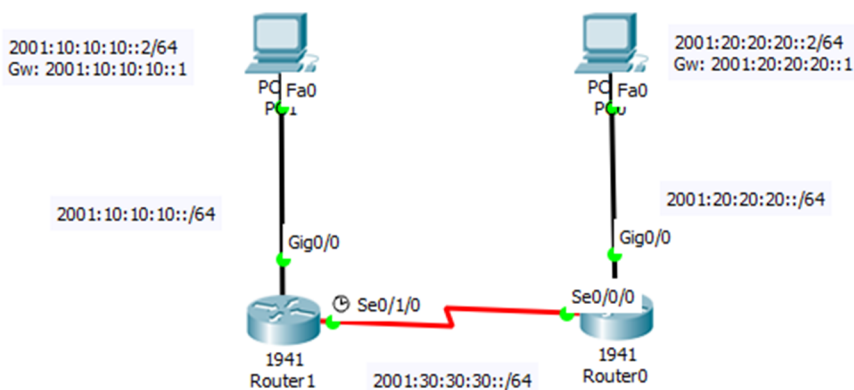
OSPFv3 és la versió del protocol d'encaminament *link-state* OSPF que permet treballar amb adreces IPv6 (OSPFv2 treballa amb adreces IPv4). Hi ha una diferència bàsica molt important sobre la forma de configurar i activar el protocol OSPF entre les dues versions:

- OSPFv2 s'activa en el mode de configuració (`Router(config)#`)
- OSPFv3 s'activa en el mode de configuració específica de cada interfície implicada en el procés OSPF (`Router(config-if)#`)

3.7.1. Exemple: encaminament amb OSPFv3

Donada la xarxa de la figura 27a, formada per només dos encaminadors i tres subxarxes IPv6, l'objectiu final és activar el protocol OSPF versió 3, perquè tots els encaminadors coneguin totes les subxarxes de la xarxa principal i es pugui realitzar un *ping* amb èxit entre els dos ordinadors.

Figura 27a. Xarxa formada per dos encaminadors amb adreçament IPv6



Primer de tot s'han de configurar les interfícies Serial i Ethernet dels encaminadors Router0 i Router1 i les interfícies Ethernet dels ordinadors PC0 i PC1 (figura 27b). Com que es tracta d'adreces IPv6, s'ha de fer servir la comanda `ipv6 address` per configurar totes les interfícies dels encaminadors. A més, a la interfície serial DCE de Router1 s'ha de configurar la velocitat de l'enllaç amb la comanda `clock rate`.

Com es detalla a la figura 27c, l'activació del protocol OSPFv3 es fa a cada interfície de l'encaminador implicada en la transmissió dels paquets *Hello* i *LSA*. S'ha de fer servir la comanda `ipv6 ospf` amb dos identificadors: el del procés OSPF i el de l'àrea.

Un cop activat aquest protocol, es pot comprovar a la figura 27d que les xarxes apreses amb OSPF tenen el distintiu 'O'. A la figura 27e es mostra un *ping* executat amb èxit entre els ordinadors PC0 i PC1.

Figura 27b. Configuració de les interfícies dels encaminadors i dels ordinadors

```

Router>enable
Router#configure terminal
Router(config)#hostname Router1
Router1(config)#interface Gig0/0
Router1(config-if)#ipv6 address
2001:10:10:10::1/64
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface se0/1/0
Router1(config-if)#clock rate 4000000
Router1(config-if)#no shutdown
Router1(config-if)#ipv6 address
2001:30:30:30::1/64
Router1(config-if)#exit
Router1(config)#

```

```

Router>enable
Router#configure terminal
Router(config)#hostname Router0
Router0(config)#interface Gig0/0
Router0(config-if)#ipv6 address
2001:20:20:20::1/64
Router0(config-if)#no shutdown
Router0(config-if)#exit
Router0(config)#interface se0/0/0
Router0(config-if)#no shutdown
Router0(config-if)#ipv6 address
2001:30:30:30::2/64
Router0(config-if)#exit
Router0(config)#

```

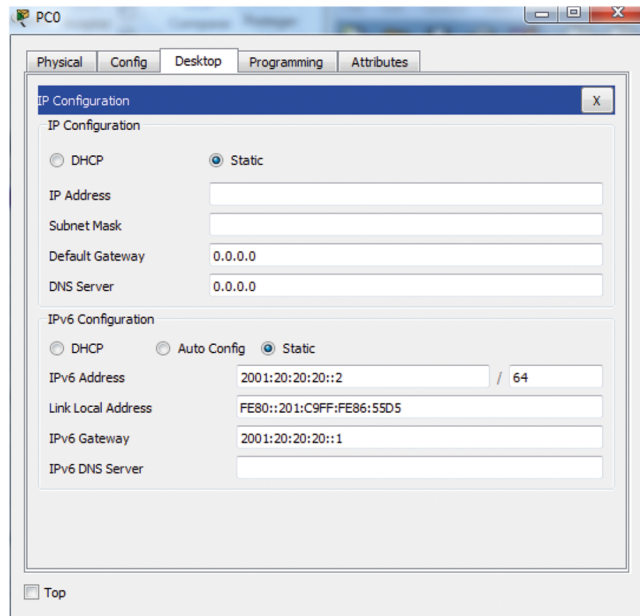
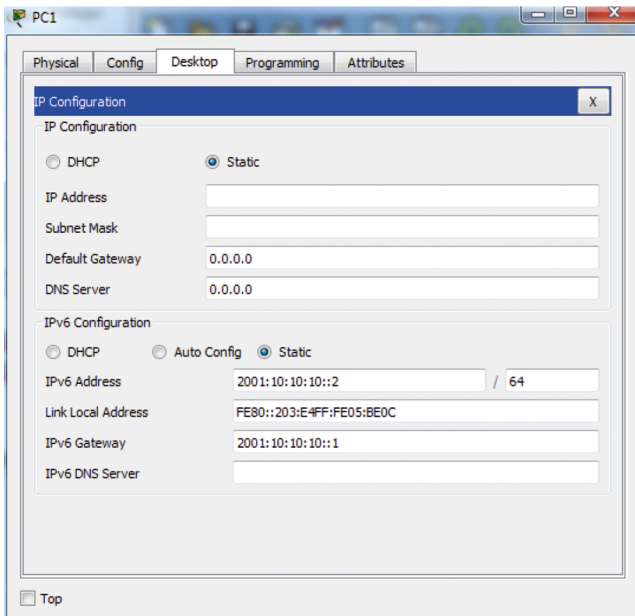


Figura 27c. Activació del protocol OSPFv3 a cada encaminador

```

Router1>enable
Router1#conf term
Router1(config)#ipv6 unicast-
routing
Router1(config)#ipv6 router ospf
100
Router1(config-rtr)#router-id
1.1.1.1
Router1(config-rtr)#exit
Router1(config)#int Gig0/0
Router1(config-if)#ipv6 ospf 100
area 0
Router1(config-if)#exit
Router1(config)#int se0/1/0
Router1(config-if)#ipv6 ospf 100
area 0
Router1(config-if)#exit
Router1(config)#

```

```

Router0>enable
Router0#conf term
Router0(config)#ipv6 unicast-
routing
Router0(config)#ipv6 router ospf
100
Router0(config-rtr)#router-id
2.2.2.2
Router0(config-rtr)#exit
Router0(config)#int Gig0/0
Router0(config-if)#ipv6 ospf 100
area 0
Router0(config-if)#exit
Router0(config)#int se0/0/0
Router0(config-if)#ipv6 ospf 100
area 0
Router0(config-if)#exit
Router0(config)#

```

Figura 27d. Taula de *routing* de Router0 i Router1

```

Router1#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local,
S - Static, R - RIP, B - BGP
U - Per-user Static route, M -
MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA -
ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter,
OE1 - OSPF ext 1, OE2 - OSPF ext
2
ON1 - OSPF NSSA ext 1, ON2 - OSPF
NSSA ext 2
D - EIGRP, EX - EIGRP external
C 2001:10:10:10::/64 [0/0]
  via GigabitEthernet0/0, directly
connected
L 2001:10:10:10::1/128 [0/0]
  via GigabitEthernet0/0, receive
O 2001:20:20:20::/64 [110/65]
  via FE80::20A:41FF:FEDD:E601,
Serial0/1/0
C 2001:30:30:30::/64 [0/0]
  via Serial0/1/0, directly
connected
L 2001:30:30:30::1/128 [0/0]
  via Serial0/1/0, receive
L FF00::/8 [0/0]
  via Null0, receive
Router1#

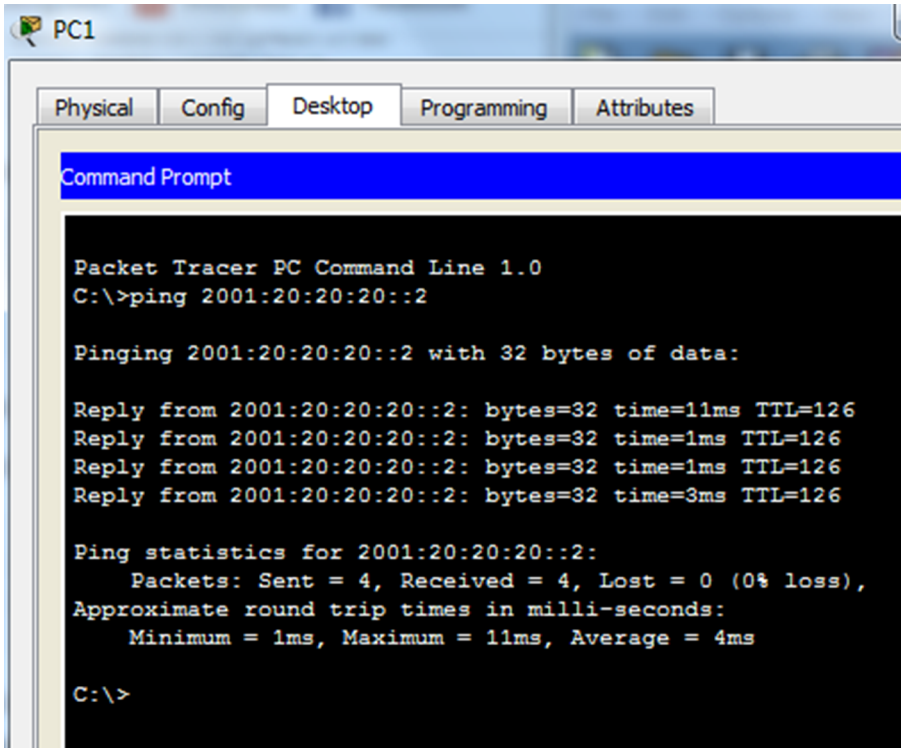
```

```

Router0#show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local,
S - Static, R - RIP, B - BGP
U - Per-user Static route, M -
MIPv6
I1 - ISIS L1, I2 - ISIS L2, IA -
ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter,
OE1 - OSPF ext 1, OE2 - OSPF ext
2
ON1 - OSPF NSSA ext 1, ON2 - OSPF
NSSA ext 2
D - EIGRP, EX - EIGRP external
O 2001:10:10:10::/64 [110/65]
  via FE80::200:CFF:FE99:6901,
Serial0/0/0
C 2001:20:20:20::/64 [0/0]
  via GigabitEthernet0/0, directly
connected
L 2001:20:20:20::1/128 [0/0]
  via GigabitEthernet0/0, receive
C 2001:30:30:30::/64 [0/0]
  via Serial0/0/0, directly
connected
L 2001:30:30:30::2/128 [0/0]
  via Serial0/0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
Router0#

```

Figura 27e. Comprovació de la connectivitat entre PC0 i PC1



The image shows a screenshot of a Packet Tracer PC Command Prompt window. The window title is "PC1" and it has tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, showing a "Command Prompt" window. The text in the Command Prompt is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 2001:20:20:20::2

Pinging 2001:20:20:20::2 with 32 bytes of data:

Reply from 2001:20:20:20::2: bytes=32 time=11ms TTL=126
Reply from 2001:20:20:20::2: bytes=32 time=1ms TTL=126
Reply from 2001:20:20:20::2: bytes=32 time=1ms TTL=126
Reply from 2001:20:20:20::2: bytes=32 time=3ms TTL=126

Ping statistics for 2001:20:20:20::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 4ms

C:\>
```


Bibliografia

Una part dels continguts d'aquest document s'han consultat de la web de Cisco o als materials dels cursos CCNA de Netacad:

<https://www.cisco.com/>

<https://www.netacad.com/>

Adicionalment, alguns dels recursos s'han obtingut del fòrum de la comunitat Cisco, i de les pàgines dels organismes IEEE (Institute of Electrical and Electronics Engineers), responsable dels estàndards de la majoria de tecnologies de xarxa i IETF (Internet Engineering Task Force), responsable dels estàndards d'Internet i la publicació dels documents RFC (Request For Comment):

<https://community.cisco.com/>

<https://standards.ieee.org>

<https://tools.ietf.org/>

