Pràctiques Xarxes: Laboratori 2

César Fernàndez, Enric Guitart, Carles Mateu

March 11, 2025

Commutació bàsica

Els conceptes sobre els que es treballarà en aquest laboratori són:

- Commutació bàsica nivell 2 (Taules d'encaminament, domini de *broadcast* i *flooding*).
- Configuració de ports
- Diagnòstics
- Seguretat de nivell 2

1 Conceptes preliminars

1.1 Commutació bàsica

- Documentació

  OS6250 : AOS 6.6.1.R01 OS6250 Network Configuration Guide.pdf → Cap. 2

  OS6450 : os_nt_665_revA.pdf → Cap. 2

  OS6600 : OS66_Network_Configuration_Guide_Rev_E.pdf → Cap. 3

  OS7000 : OS7_Network_Configuration_Guide_Rev_G.pdf → Cap. 2

Per defecte (configuració inicial o de fàbrica) els equips de xarxa de nivell 2 tenen configurat un sol domini de *broadcast* (VLAN) i tots els ports de l'equip pertanyen a aquest domini.

Els equips d'usuari (PC) que es connectin als ports de l'equip de xarxa tindran connectivitat a nivell 2 sense haver de fer cap configuració addicional. En rebre el primer paquet de dades dels equips d'usuari l'equip de xarxa els afegirà a les taules d'encaminament de nivell 2 per poder gestionar la commutació.

Per què els equips d'usuari tinguin connectivitat (connectivitat a nivell d'aplicació) caldrà una correcta configuració en els protocols superiors a nivell 2.

Per visualitzar l'estat dels ports de l'equip de xarxa tenim dues comandes:

- Visualitzar únicament l'estat dels ports:

  `-> show interfaces [ethernet | fastethernet | gigaethernet] [`*slot*`[/`*port*`[-`*port2*`]]] port`

- Visualitzar l'estat dels ports i el domini de *broadcast* al que estan associats:

  `-> show vlan [`*vid*`] port [`*slot/port* `|`*link_agg*`]`

Per la gestió de la taula d'encaminament de nivell 2 tenim les següents comandes:

- Visualitzar la taula d'encaminament de nivell 2:

  `-> show mac-address-table [permanent | reset | timeout | learned] [`*mac_address*`] [slot` *slot* `|`*slot/port*`] [linkagg` *link_agg*`] [`*vid*`]`

- Visualitzar estadístiques de la taula d'encaminament de nivell 2:

  `-> show mac-address-table count [`*mac_address*`] [slot` *slot* `|`*slot/port*`] [linkagg` *link_agg*`] [`*vid*`]`

- Visualitzar el temps de vigència de les adreces de nivell 2:

  `-> show mac-address-table aging-time [vlan` *vid*`]`

- Afegir o modificar una entrada en la taula d'encaminament de nivell 2:

  `-> mac-address-table [permanent | reset | timeout]` *mac_address* `{`*slot/port* `| linkagg` *link_agg*`}` *vid* `[bridging | filtering]`

- Eliminar una entrada de la taula d'encaminament de nivell 2:

  `-> no mac-address-table [permanent | reset | timeout | learned] [`*mac_address* `{`*slot/port* `|` *link_agg*`}` *vid*`]`

- Modificar el temps de vigència de les adreces de nivell 2:

  `-> mac-address-table aging-time` *seconds* `[vlan` *vid*`]`
  `-> no mac-address-table aging-time [vlan` *vid*`]`

1.2 Configuració de ports

- Documentació

  OS6250 : AOS 6.6.1.R01 OS6250 Network Configuration Guide.pdf → Cap. 1

  OS6450 : os_nt_665_revA.pdf → Cap. 1

  OS6600 : OS66_Network_Configuration_Guide_Rev_E.pdf → Cap. 1

  OS7000 : OS7_Network_Configuration_Guide_Rev_G.pdf → Cap. 1

La configuració dels ports en l'equipament de xarxa ens permet visualitzar, establir i/o modificar les característiques i funcionalitats de les interfícies *ethernet* de l'equip. Els principals paràmetres als que es pot accedir per configuració són:

- Velocitat (fixa o negociada).
- Cablejat (MDI o MDIX).
- Mode de funcionament (*full-dupex*, *half-duplex* o auto).
- Limitar el trànsit de *broadcast* i *multicast*.
- Habilitar o deshabilitar la interfície.
- Inicialitzar els comptadors d'estadístiques.

Les comandes de configuració de les interfícies (ports) totes tenen el prefix:

`-> interfaces [ethernet | fastethernet | gigaethernet]` *slot*`[`*/port*`[`*-port2*`]] ....`

La comanda continuarà amb la característica o funcionalitat a configurar:

- Establir la velocitat de treball del port:

  `-> .... speed {auto | 10 | 100 | 1000 | 10000 | max {10 | 100 | 1000}}`

- Habilitar l'auto negociació:

  `-> .... autoneg {enable | disable | on | off}`

- Tipus de cablejat:

  `-> .... crossover {auto | mdix | mdi | disable}`

- Mode de funcionament:

  `-> .... duplex {full | half | auto}`

- Habilitar la interfíce:

  `-> .... admin {up | down}`

- Habilitar el control de *broadcast* i *multicast*:

  `-> .... flood`
  `-> .... flood multicast` (sol es pot especificar *slot*)
  `-> .... flood rate` *Mbps*

- Inicialitzar els comptadors d'estadístiques de nivell 2:

  `-> .... no l2 statistics`

Per visualitzar informació de les interfícies hi ha també un prefix comú:

`-> show interfaces [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]] ....`

- Si no s'afegeix cap altre paràmetre a la comanda s'ens mostrarà detallada de les interfícies especificades.
- Visualitzar les capacitats de les interfícies i la configuració actual:

  `-> .... capability`

- Visualitzar el control de flux configurat:

  `-> .... flow [control]`

- Mostrar informació de paquets Rx/Tx:

  `-> .... accounting`

- Mostrar informació de paquets i bytes Rx/Tx:

  `-> .... counters`

- Mostrar informació de paquets erronis:

  `-> .... counters errors`

- Visualitzar els paràmetres configurats:

  `-> .... status`

- Visualitzar l'estat dels ports:

  `-> .... port`

- Visualitzar l'estat del control de *broadcast* i *multicast*:

  `-> .... flood rate`

- Visualitzar estadístiques de trànsit:

  `-> .... traffic`

Control de flux

El control de flux és un mecanisme per evitar la saturació dels *buffers* dels equips de xarxa. Per què aquest mecanisme sigui efectiu ha d'estar configurat tant en l'equip transmissor com en l'equip receptor. El seu funcionament és el següent:

- **Receptor**
  - Si un equip detecta que en un port té el *buffer* de recepció ple envia trames de notificació (*pause frame*) cap a l'equip transmissor per indicar-li una situació de saturació en el port.
  - Les trames que no poden ser encabides en el *buffer* són descartades
- **Transmissor**
  - Si un equip rep trames de notificació de saturació (*pause frame*) per un port espera un temps abans de continuar amb la transmissió de paquets per aquell port

Les comandes per configurar el control de flux són:

- Configurar l'enviament de *pause frame*:

  `-> interfaces [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]] flow {enable | disable | on | off}`

- Configurar el control de flux en transmissió:

  `-> flow [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]]`
  `-> no flow [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]]`

- Configurar el temps d'espera abans de reprendre les transmissions:

  `-> flow [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]] wait [time]`*microseconds*
  `-> flow [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]] no wait [time]`

- Visualitzar l'estat del control de flux:

  `-> show interfaces [ethernet | fastethernet | gigaethernet]` *slot*`[/`*port*`[-`*port2*`]] flow [control]`

  (el temps s'estableix en l'autonegociació que ha d'estar habilitada)

1.3 Diagnòstics

- Documentació

  OS6250 : AOS 6.6.1.R01 OS6250 Network Configuration Guide.pdf → Cap. 35

  OS6450 : os_nt_665_revA.pdf → Cap. 43

  OS6600 : OS66_Network_Configuration_Guide_Rev_E.pdf → Cap. 26

  OS7000 : OS7_Network_Configuration_Guide_Rev_G.pdf → Cap. 29

Els equips de xarxa proporcionen algunes utilitats que permeten diagnosticar els possibles problemes que puguin aparèixer en el seu funcionament. Principalment aquestes utilitats/eines ens permetran capturar trànsit i també consultar l'estat dels recursos de l'equip.

Port Mirroring

Port mirroring copia tot el trànsit d'entrada i sortida d'un port o ports a un altre port que actua com a mirall. El port mirall pot emprar-se per analitzar el trànsit del port o ports originals sense interrompre el servei.

Les comandes emprades per *port mirroring* són:

- Configurar *port mirroring*:

  `-> port mirroring` *port_mirror_sessionid* `source` *slot/port*`[-`*port2*`] [`*slot/port*`[-`*port2*`]...] destination` *slot/-port*
  `[bidirectional |inport |outport] [unblocked` *vlan_id*`]`

- Habilitar o deshabilitar *port mirroring*:

  `-> port mirroring` *port_mirror_sessionid* `{enable | disable}`

- Eliminar *port mirroring*:

  `-> no port mirroring` *port_mirror_sessionid*

- Visualitzar les configuracions de *port mirroring*:

  `-> show port mirroring status [`*port_mirror_sessionid* `]`

Port Monitoring

Port monitoring permet capturar trànsit d'un port i emmagatzemar-lo en el sistema d'arxius de l'equip de xarxa. Per cada paquet sol es capturen els primers 64 bytes. Si no s'especifica el nom de l'arxiu on emmagatzemar les dades es desa a: `/flash/pmonitor.enc`. La mida de l'arxiu s'especifica en blocs de 16 Kbytes i la mida màxima de l'arxiu és de 160 Kbytes. El format de l'arxiu és *Network General Sniffer Network Analyzer Format*.

Per dur a terme el *port monitoring* es disposa de les comandes:

- Configurar *port monitoring*:

  `-> port monitoring` *port_monitor_sessionid* `source` *slot/port* `[{no file | file` *filename* `[size` *filesize*`] | [overwrite {on | off}]}][inport | outport | bidirectional] [timeout` *seconds*`][enable | disable]`

- Pausar, reprendre o deshabilitar una sessió:

  `-> port monitoring` *port_monitor_sessionid* `{disable | pause | resume}`

- Eliminar una sessió:

  `-> no port monitoring` *port_monitor_sessionid*

- Visualitzar l'estat de *port monitoring*:

  `-> show port monitoring status [`*port_monitor_sessionid*`]`

- Visualitzar l'arxiu de captura:

  `-> show port monitoring file [`*port_monitor_sessionid*`]`

Switch Health Monitoring

Finalment els equips proporcionen comandes per monitoritzar la utilització dels recursos de que disposen per dur a terme la seva tasca i també per configurar llindars que en superar-se activin l'enviament d'alarmes.

Per la monitorització de recursos s'empren les comandes:

- Visualitzar les estadístiques de tots els recursos de l'equip:

  `-> show health [`*slot/port*`] [statistics]`

- Visualitzar les estadístiques d'un recurs:

```
-> show health all {memory | cpu | rx | txrx}
```

- Visualitzar els llindars establerts per les alarmes:

```
-> show health threshold [rx | txrx | memory | cpu | temperature]
```

- Visualitzar l'interval de les mesures:

```
-> show health interval
```

- Establir els llindars per les alarmes:

```
-> health threshold {rx percent | txrx percent | memory percent | cpu percent | temperature degrees ]
```

- Establir l'interval de les mesures:

```
-> health intervalseconds
```

- Inicialitzar les estadístiques :

```
-> health statistics reset
```

1.4 Seguretat nivell 2

- Documentació

OS6250 : AOS 6.6.1.R01 OS6250 Network Configuration Guide.pdf → Cap. 3

OS6450 : os_nt_665_revA.pdf → Cap. 3

OS6600 : OS66_Network_Configuration_Guide_Rev_E.pdf → Cap. 3

OS7000 : OS7_Network_Configuration_Guide_Rev_G.pdf → Cap. 4

Mitjançant la seguretat de nivell 2 es pot controlar quins dispositius poden accedir als ports dels *switchs*. En el cas d'Alcatel s'anomena LPS (**L***earned* **P***ort* **S***ecurity*) i permet actuar sobre tres paràmetres de restricció:

- El temps en el que el port fa aprenentatge
- La quantitat màxima d'adreces MAC permeses en un port
- Una llista d'adreces MAC permeses en un port

Les comandes emprades per la seguretat a nivell 2 són:

- Activar, desactivar o eliminar la seguretat:

```
-> port-security slot/port [enable | disable]
-> no port-security slot/port
```

- Restringir l'aprenentatge:

```
-> port-security shutdown minutes
-> port-security slot/port maximum number
-> port-security slot/port mac mac_address
-> port-security slot/port no mac mac_address
-> port-security slot/port mac-range [low mac_address | high mac_address | low mac_address high mac_address]
```

- Especificar l'acció que es pendrà en complir-se la restricció:

```
port-security slot/port violation {restrict | shutdown}
```

- Restablir un port bloquejat per una restricció:

  `port-security` *slot/port* `release`

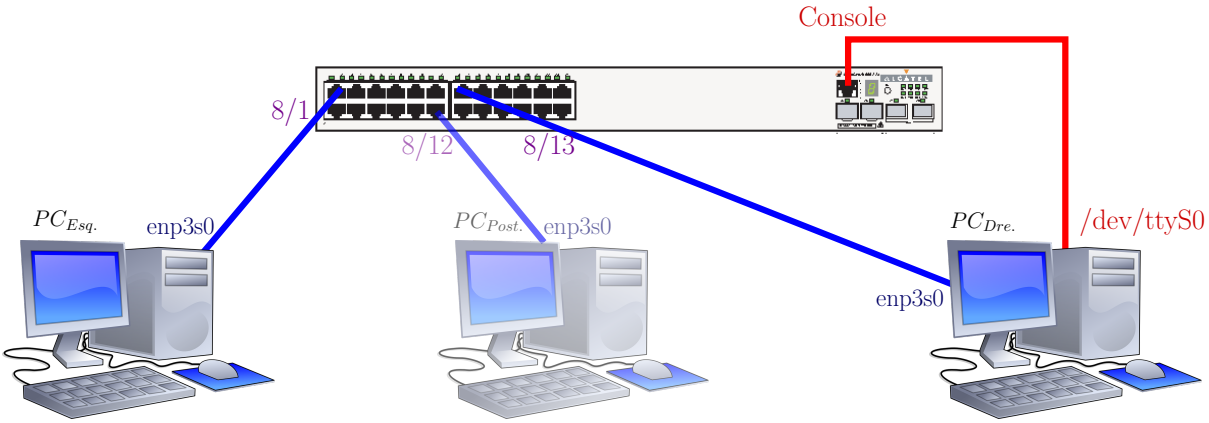
- Visualitzar l'estat de la seguretat:

  `show port-security [`*slot/port* `|` *slot* `| config-mac-range]`
  `show port-security shutdown`

2 Laboratoris

2.1 Commutació bàsica

- **Escenari**



- **Tasques**

1. Elimineu la configuració existent en l'equip de xarxa:

```
-> rm /flash/working/boot.cfg
-> rm /flash/certified/boot.cfg
-> reload
```

2. Configureu una adreça IP, de la mateixa xarxa, en cada equip d'usuari:

```
$ sudo ifconfig enp3s0 192.168.20.(10 + Nº PC) up
```

3. Comproveu l'estat dels ports del *swtich*:

```
-> show interfaces port
-> show interfaces status
-> show vlan port
```

4. Comproveu la connectivitat entre els equips d'usuari:

```
$ ping IP-PC_veï
```

5. Visualitzeu la taula d'encaminament de nivell 2 del *switch* i constateu que les MAC corresponen amb els PC d'usuari:

```
-> show mac-address-table
$ ifconfig enp3s0
$ ip link show enp3s0
```

6. Empreu l'aplicació `wireshark` per capturar el trànsit en cada equip d'usuari.

7. Configureu el *switch* per què $PC_{Esquerra}$ no pugui enviar paquets a la xarxa:

```
mac-address-table mac_PC_esquerra 8/1 1 filtering
```

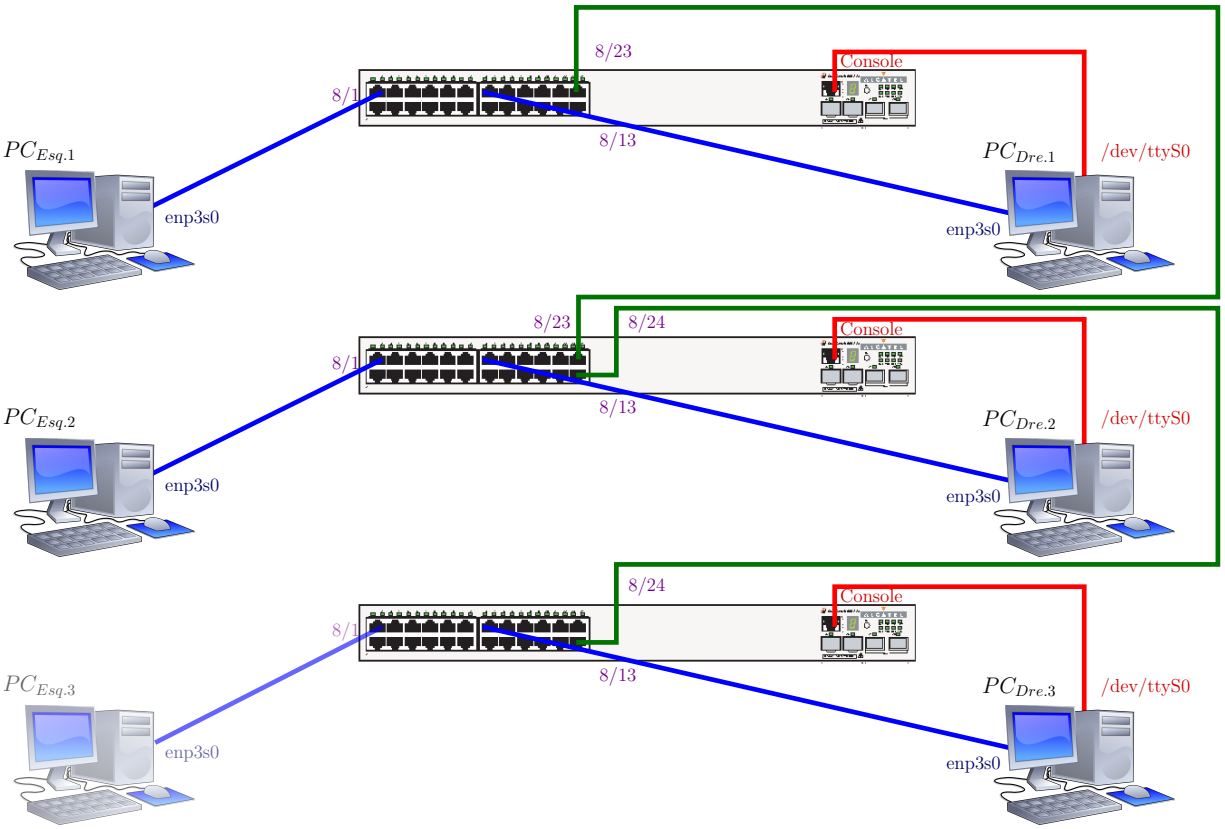
8. Empreu l'aplicació `wireshark` per analitzar què està passant si PC_{Dreta} vol enviar paquets a $PC_{Esquerra}$.

9. Que passa si canviem $PC_{Esquerra}$ de port? Analitzeu el comportament.

10. Connecteu els *switch* de cada *rack* i comproveu la connectivitat entre tots els PC.

2.2 Domini de *broadcast*

- **Escenari**



- **Tasques**

1. Elimineu els protocols que poden enviar trànsit a la xarxa:

```
-> amap disable
-> gmap disable
-> vlan 1 stp disable
```

2. Comproveu que teniu connectivitat entre tots els PC del *rack*.

3. Un cop constatat que teniu connectivitat deixeu d'enviar trànsit a la xarxa.

4. En $PC_{Esq.2}$ elimineu l'entrada de la taula ARP (**A***ddress* **R***esolution* **P***rotocol*) de $PC_{Dre.2}$ i en $PC_{Dre.2}$ la de $PC_{Esq.2}$:

```
$ arp -a
$ arp -d <IP_PC>
$ arp -a
```

5. En tots els PC endegueu *wireshark* i captureu trànsit de la interfície que teniu connectada al *switch* (`enp3s0`).

6. Des de $PC_{Esq.2}$ feu 5 `ping` a $PC_{Dre.2}$ i des de $PC_{Dre.2}$ 5 `ping` a $PC_{Esq.2}$:

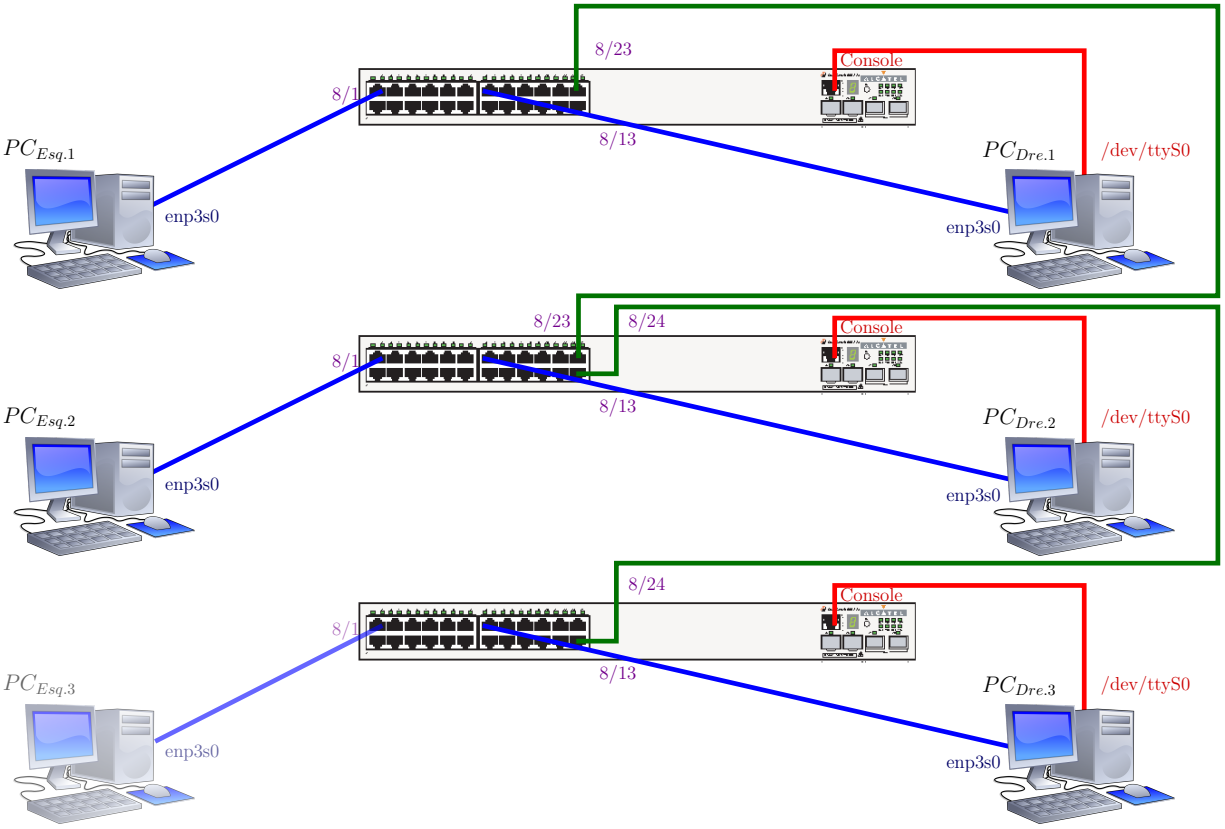
```
$ ping -c 5 <IP_PC>
```

7. Quins paquets heu rebut? Analitzeu les adreces de nivell 2 dels paquets rebuts.

2.3 *Flooding*

El *flooding* es produeix quan un *switch* desconeix l'adreça destí d'un paquet de nivell 2 i, per assegurar connectivitat, l'envia per tots els ports menys per el que l'ha rebut.

- **Escenari**



- **Tasques**

1. Comproveu que teniu connectivitat entre tots els PC del *rack*.
2. Un cop constatat que teniu connectivitat deixeu d'enviar trànsit a la xarxa.
3. Comproveu les taules ARP de $PC_{Esq.2}$ i $PC_{Dre.2}$ per assegurar-vos que coneixen $PC_{Dre.2}$ i $PC_{Esq.2}$ respectivament.
4. Esborreu les taules d'encaminament de nivell 2 de tots els *switch*:

   ```
   -> no mac-address-table learned
   ```

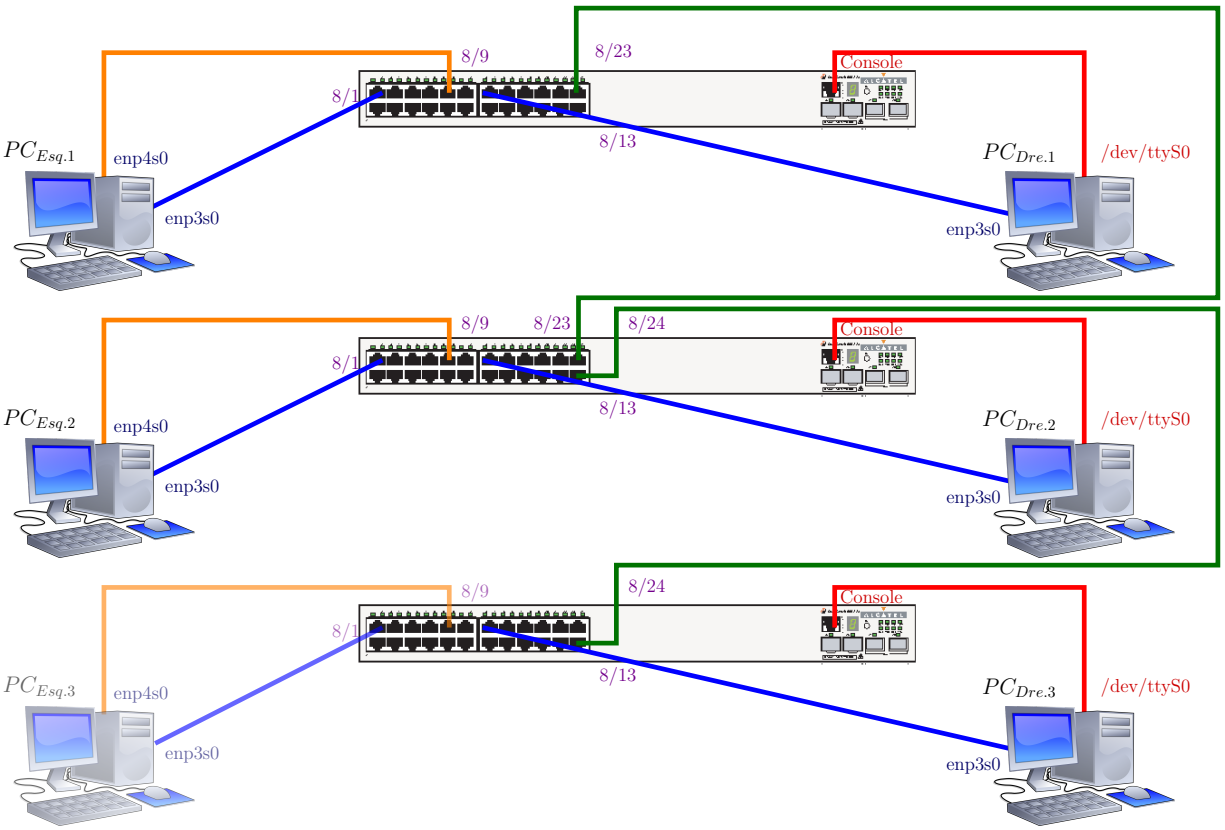
5. En tots els PC endegueu *wireshark* i captureu trànsit de la interfície que teniu connectada al *switch* (`enp3s0`).
6. Des de $PC_{Esq.2}$ feu 5 `ping` a $PC_{Dre.2}$:

   `$ ping -c 5` *<IP_PC>*

7. Quins paquets heu rebut? Analitzeu les adreces de nivell 2 dels paquets rebuts.

2.4 *Port Mirroring*

- **Escenari**



- **Tasques**

1. Comproveu que teniu connectivitat entre tots els PC del *rack*.

2. Un cop constatat que teniu connectivitat deixeu d'enviar trànsit a la xarxa.

3. Feu els següents `ping` continuats:
   - $PC_{Dre.1} \rightarrow PC_{Dre.2}$
   - $PC_{Dre.2} \rightarrow PC_{Dre.3}$
   - $PC_{Dre.3} \rightarrow PC_{Dre.1}$

4. En els PC_{Esq} endegueu `wireshark` sobre la interfície `enp3s0` i analitzeu el trànsit capturat. Podeu veure el trànsit dels `ping` dels $PC_{Dre.}$? Justifiqueu el resultat.

5. Atureu la captura de `wireshark` i activeu la interfície `enp4s0` dels PC_{Esq}:

   `$ ifconfig enp4s0 up` ó `$ ip link set dev eth0 up`

6. En els equips de xarxa configureu el port 9 com a mirall del port de $PC_{Dre.}$:

```
-> port mirroring 9 source 8/13 destination 8/9
-> port mirroring 9 enable
```

7. Connecteu la interfície `enp4s0` dels PC_{Esq} al port 9 del seu equip de xarxa.

8. En els PC_{Esq} endegueu `wireshark` sobre la interfície `enp4s0` i analitzeu el trànsit capturat.

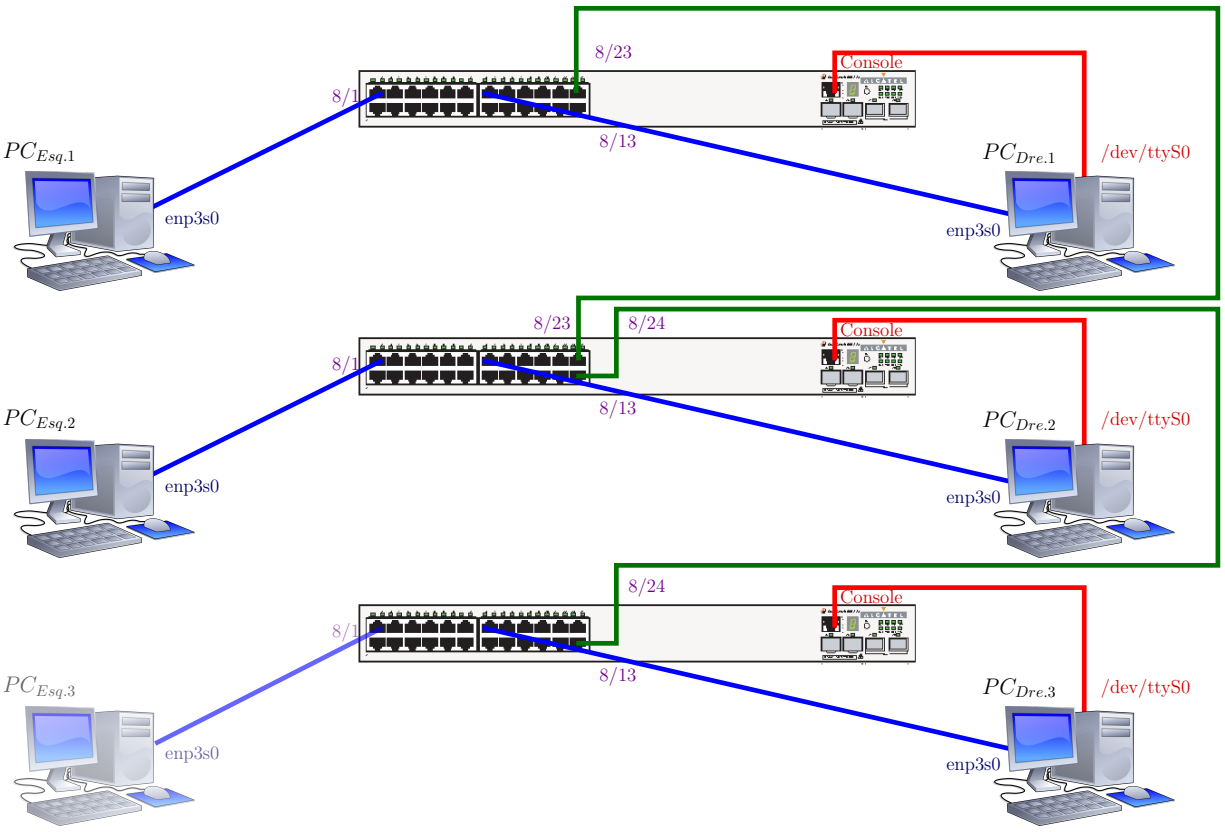
9. Afegiu els següents `ping` continuats:
   - $PC_{Esq.1} \rightarrow PC_{Esq.2}$
   - $PC_{Esq.2} \rightarrow PC_{Esq.3}$
   - $PC_{Esq.3} \rightarrow PC_{Esq.1}$

10. Podeu veure en `wireshark` aquest segon trànsit de la xarxa? Justifiqueu la resposta.

11. Elimineu la sessió de *port monitoring* i finalitzeu els `ping`.

2.5 *Port Monitoring*

- **Escenari**



- **Tasques**

1. Comproveu que teniu connectivitat entre tots els PC del *rack*.
2. Un cop constatat que teniu connectivitat deixeu d'enviar trànsit a la xarxa.
3. En els equips de xarxa configureu la monitorització del port dels $PC_{Esq.}$ durant 5 minuts:

   ```
   -> port monitoring 1 source 8/1 file pcEsq timeout 300 enable
   ```

4. Feu els següents `ping` continuats:
   - $PC_{Esq.1} \rightarrow PC_{Dre.2}$
   - $PC_{Esq.2} \rightarrow PC_{Dre.3}$
   - $PC_{Esq.3} \rightarrow PC_{Dre.1}$
5. Passats uns minuts atureu la monitorització:

   ```
   -> port monitoring 1 disable
   ```

6. Visualitzeu el contingut de l'arxiu de les captures:

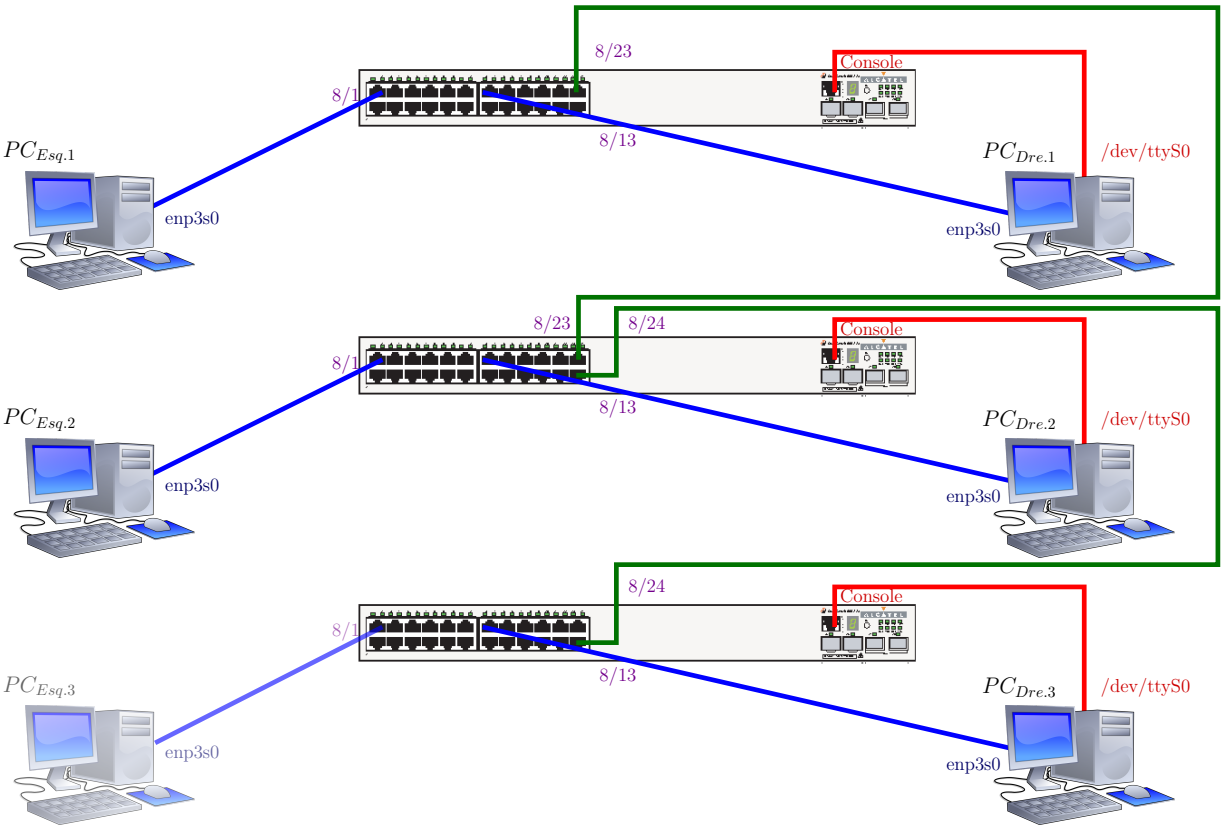
   ```
   -> show port monitoring file 1
   ```

7. Elimineu la sessió:

   ```
   -> no port monitoring 1
   ```

2.6 *Seguretat de nivell 2*

- **Escenari**



- **Tasques**

1. Consulteu en els manuals del equips de xarxa quins són els paràmetres per defecte de LPS.

2. Activeu la seguretat de nivell 2 en els ports d'interconnexió dels *switchs*.

3. Des de cada PC feu *ping* a la resta de PCs del grup i analitzeu el resultat de la prova.

4. En els ports que heu activat la seguretat, establiu un màxim de 3 adreces MAC

5. Repetiu des de cada PC el *ping* a la resta de PCs del grup i analitzeu els resultats.

6. En els ports que heu activat la seguretat, establiu l'acció `shutdown` en cas de `violation`

7. Torneu a fer *ping* des de cada PC a la resta de PCs del grup i analitzeu els resultats.

8. Configureu en cada *switch* els paràmetres de seguretat adients per què en el port 1 sol es pugui connectar $PC_{Esq.}$ i en el port 13 $PC_{Dre.}$.

9. Comproveu que teniu connectivitat amb tots els PCs del grup.

10. Invertiu en cada *switch* les connexions dels PCs, repetiu la prova de connectivitat i analitzeu el resultat.