Administració de xarxa d'un institut 1x1

Administració de xarxes i de sistemes operatius

Autor: Antoni Anguera Atset

Consultor: Miguel Martín Mateo

Tutor extern: David Jordan Casals

Gener de 2013

Aquesta obra està subjecta a una llicència de [Reconeixement-NoComercial-CompartirIgual 3.0 No adaptada de Creative Commons]

Resum

Aquest projecte s'ubica a l'institut Guillem Català de Manresa amb una oferta formativa d'ESO, batxillerat i cicles formatius de grau mitjà i superior. El volum d'alumnes és proper al miler i els alumnes de 1r., 2n. i 3r. d'ESO segueixen el programa 1x1 que dota a cada alumne d'un ordinador per treballar el currículum amb suport digital. Si es tenen en compte els ordinadors dels professors, les aules d'informàtica, els dispositiu mòbils i els portàtils dels alumnes de cicles formatius, la xarxa del centre té una càrrega aproximada de 400 màquines.

Per satisfer les necessitats de connectivitat a internet, el departament d'ensenyament va proveir el centre amb un estructura força rígida, assignava una XDSI de 6Mb per tot el centre i dues ADSL de 8Mb per a les aules del projecte 1x1. També cal afegir a aquesta infraestructura una altra línia ADSL de 8Mb contractada pel centre, més tota la infraestructura de cablatge que havia fet el propi centre prèvia al desplegament del projecte 1x1. El resultat global és una xarxa força caòtica que utilitzava maquinari i programari privatiu i és insuficient per cobrir les necessitats de connectivitat del centre. L'altre problema destacable era l'ús que els alumnes del projecte 1x1, i la resta en general, feien de l'accés a internet. Tot i que el sistema disposa d'un filtre, aquest acabava sent inoperant, ja que els alumnes se'l saltaven navegant per *proxys* transparent o accedint als mateixos continguts per mitjà del protocol segur, quan el domini ho permetia, que no es podia filtrar.

A partir de la situació descrita, vaig decidir fer un TFM amb l'objectiu de millorar aquesta situació. Es tracta de reestructurar tota la xarxa per entendre-la com una unitat, i no com a pedaços afegits. Millorar la connectivitat a internet i aconseguir que el suport informàtic sigui una eina pedagògica més, i no el protagonista d'una lluita diària per aconseguir continguts acadèmics.

Globalment la solució proposada es basa en la segmentació de tota la xarxa en espais amb entitat pròpia, com cadascuna de les aules ordinàries, aules d'informàtica, secretaria, sala de professors... per associar-la a una VLAN. Per un altre costat s'ha dotat a tota aquesta xarxa de servidors per fer-la completament operativa i dotar-la de les eines necessàries per a la docència i la gestió del centre.

Aquest projecte s'organitzat en un bloc de disseny que es reflexa en aquesta memòria i unes pràctiques del TFM que han servit per implementar el projecte. He hagut de posar un èmfasi especial en la programació de tasques, ja que s'havia d'afectar el mínim possible el funcionament habitual del centre.

El desenvolupament del projecte ha seguit una seqüenciació piramidal. He començat per la connectivitat a l'exterior amb els *routers*, després substituir els *switch* de capçalera per un servidor de xarxa amb funcionalitats ampliades i mica en mica crear i distribuir les diferents *VLAN's* per tots els espais de l'institut. El bloc menys crític el formen els servidors i serveis que suposen una ampliació de les funcionalitats existents, ja que no s'ha hagut de substituir cap dispositiu previ.

Índex de continguts

0 Introducció

La finalitat última d'aquest projecte és dotar a l'institut Guillem Catà de Manresa d'una estructura informàtica suficient per suportar la càrrega de tots els clients del centre i oferir-los la fluïdesa necessària per desenvolupar les activitats d'ensenyament-aprenentatge còmodament utilitzant les eines informàtiques disponibles.

Per aconseguir aquest ambiciós objectiu a la xarxa informàtica del Guillem Catà, he incidit sobre 3aspectes:

- Reestructurar totes les successives actuacions que s'havien fet a la xarxa per dotar-la d'una entitat cohesionada, oposada al conjunt de blocs inicials.
- Migrar el maquinari i programari privatiu a servidors basats en programari lliure.
- Dotar a la nova xarxa de més funcionalitats per fer-la més àgil i operativa
- Dotar a la infraestructura dels elements de control i monitorització per poder auditar el seu funcionament.

Aquests objectius es concreten amb la següent infraestructura i serveis:

- Instal·lar un balanceig de càrrega per *routers* que permeti el control i la monitorització de cadascun d'ells per separat.
- Traslladar la pàgina web i l'aula virtual (Moodle) del servidor extern a un de propi al centre per accelerar la seva connectivitat i reduir el trànsit cap a internet.
- Instal·lar un servidor DHCP per facilitar la connexió dels clients a la xarxa.
- Instal·lar un servidor DNS que permeti el registre de peticions a internet, per tal de permetre auditar l'accés que en facin els alumnes si fos necessari.
- Disposar d'un filtre de continguts d'internet realment eficaç, flexible i que es pugui configurar a temps real.
- Segmentar la xarxa en unitats diferenciades que permetin configuracions i accessos a internet distints.
- Configurar cada aula i espai amb una VLAN per facilitar el control de les polítiques d'accés a internet dels alumnes.
- Disposar per tot el centre d'un sistema Wi-Fi que permeti simultàniament l'accés restringit a internet dels usuaris visitants o alumnes i un accés lliure pel personal docent.
- Instal·lar un servidor de fitxers Samba i d'impressió.
- Disposar de servidors de còpies de seguretat per el sistema tolerant a fallades amb notificació per e-mail en cas d'error.
- Integrar arquitectura i serveis de xarxa que s'han superposat al llarg del temps

Aquest és un projecte d'administració de xarxa, de configuració, migració i aplicació de serveis àmpliament utilitzats i difosos. El seu gran èxit és que realment és operatiu i actualment està en producció i oferint un bon servei. Però no hi trobarem cap desenvolupament espectacular ni cap aplicació que marqui tendència.

Tot i això m'agradaria remarcar que aquest projecte té dos elements propis i originals que segura-

ment no es troben en d'altres xarxes, o si més no amb la solució aplicada.

Monitorització del treball dels routers.

El balanceig de càrrega per routers és una eina molt utilitza en entorns de programari lliure. En aquest cas recau sobre el servidor **FW-1** que alhora fa les funcions de tallafocs per impedir els atacs de l'exterior als equips de la LAN. L'aspecte propi és que cadascun d'aquests 4 routers actuals (el sistema permet l'ampliació d'una forma molt simple) és l'únic equip de la seva VLAN i per tant es monitoritza el seu treball i rendiment d'una forma molt simple analitzant el transit de la VLAN amb eines com *ipitraf* i *vnstat*.

Commutació de la política d'accés a internet.

La única forma que els alumnes no se saltin les restriccions dels filtres d'internet és treballar amb el sistema de les llistes blanques. És a dir per defecte tot l'accés a internet està prohibit, i només es permeten aquells dominis que es considerin vàlids.

De vegades aquesta política no és viable, ja que el professor pot requerir que els seus alumnes disposin d'un accés lliure a internet. Aquest accés lliure ha de ser per un temps limitat i per una aula concreta.

La solució aplicada és la següent:

El servidor de xarxa té dues instàncies del programa Squid funcionant, i que treballen per ports diferents, el 3128 i el 3228. L'Squid que treballa pel port 3128 i amb la configuració de les seves ACL permet només l'accés a llistes blanques, i en canvi la instància del port 3228 treballa per llista negra i té un accés molt més permissiu.

D'aquesta forma quan es vol permetre l'accés a internet de l'aula, el professor des del ordinador de l'aula executa un script (es fa gràficament perquè està programat amb *gambas*) que detecta la VLAN a la que pertany l'aula i per IPTABLES dirigeix totes les peticions a *l'Squid* permissiu. Per evitar descuits, cada canvi d'hora es restaura la configuració inicial.

Contingut de la memòria.

D'una banda aquesta memòria inclou la descripció i configuració del sistema. Per facilitar la seva lectura i compressió, scripts i fitxers de configuració apareixen segmentats i sovint incomplerts. El motiu és destacar els elements més importants o característics.

En un segon bloc de la memòria apareixen els mecanismes de verificació, monitorització i control del sistema.

Estudi de viabilitat.

Com a tal aquest estudi no s'ha fet. El motiu és que es parteix d'una instal·lació que ja està feta la qual es sotmet a un procés de migració i dotació de nous serveis.

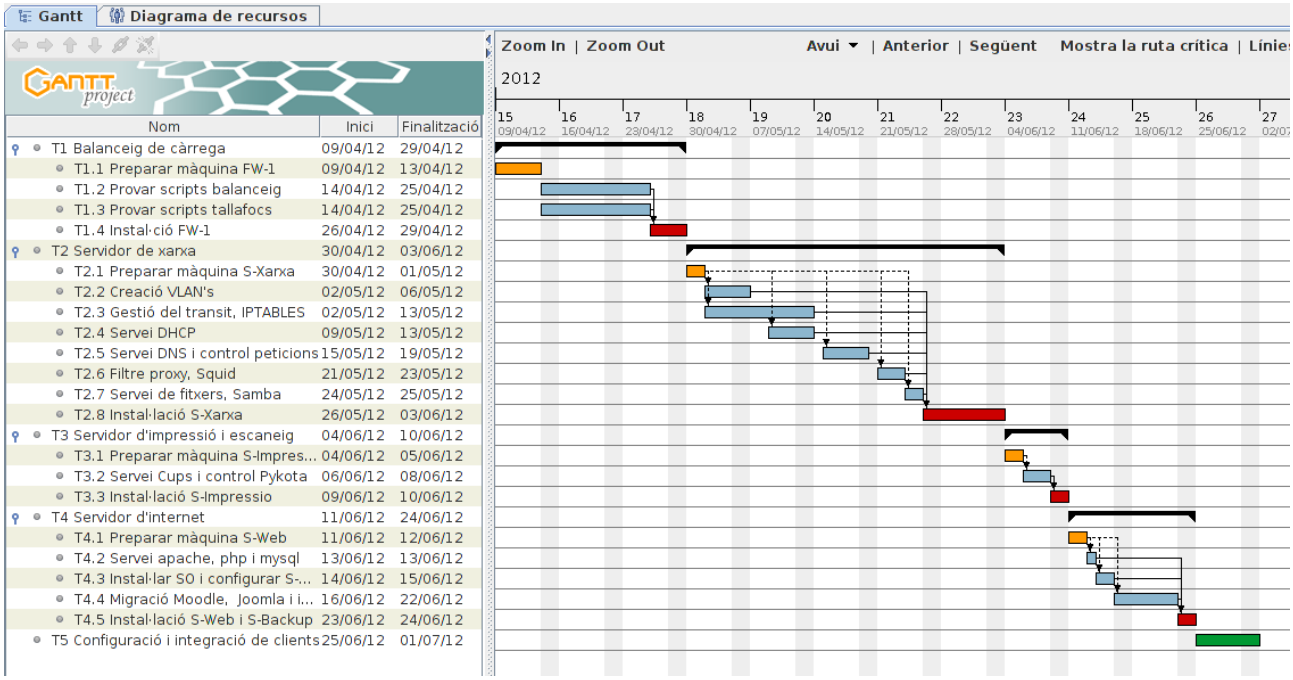
Hi ha però el cost del servidor Web i ampliacions de memòria de servidors que el centre ja disposava.

També s'ha hagut de comprar 2 *switchs* programables, però el seu cost no és massa significatiu, el preu unitari està als voltants de 120€.

Respecta als punts d'accés la dotació del departament preveia 2 punts per aula. He deixat les aules amb un sol punt i he aprofitat el restant per d'altres espais no coberts.

Programació de tasques.

Aquest ha estat un aspecte crític, ja que s'havia de conviure amb l'activitat quotidiana del centre i alhora implementar el procés de migració.



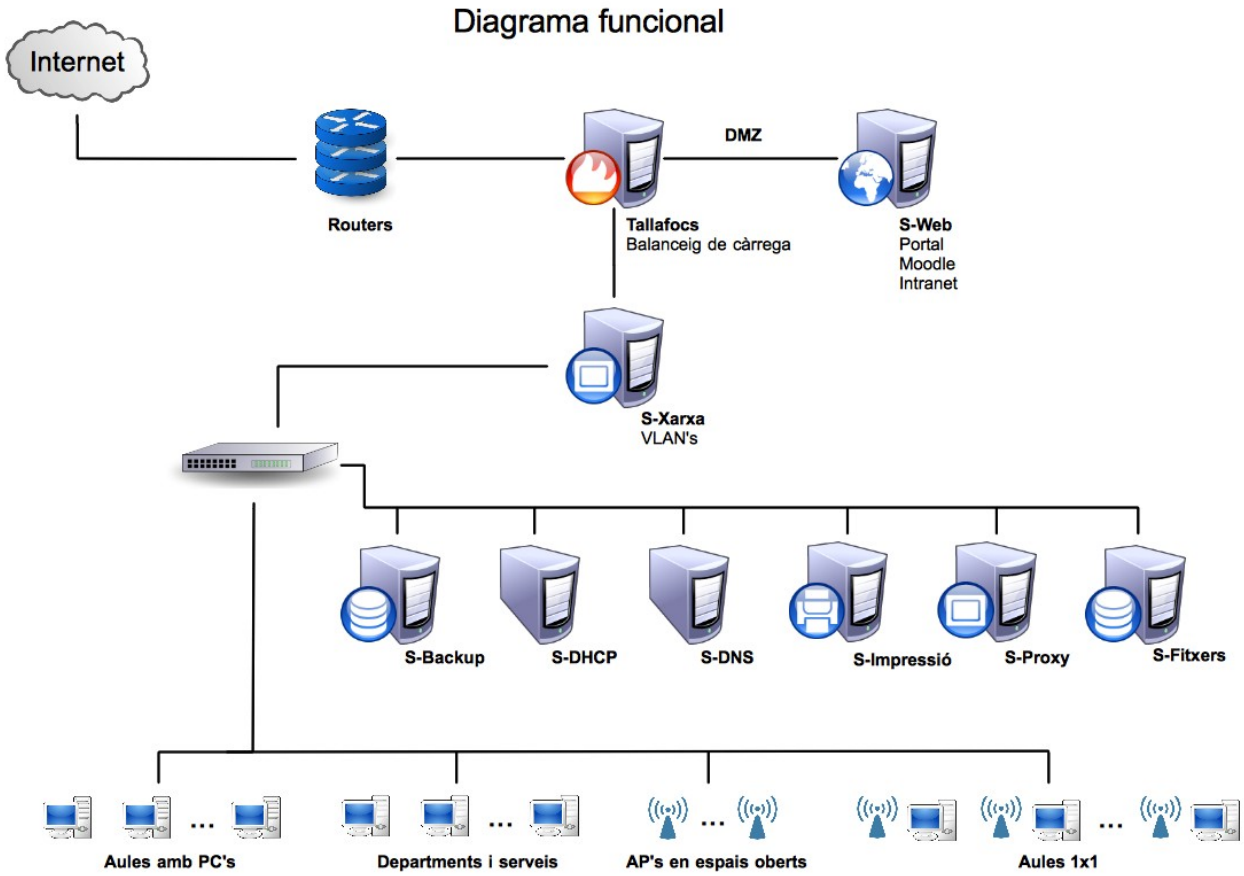
Nom	Inici	Finalització
T1 Balanceig de càrrega	09/04/12	29/04/12
T1.1 Preparar màquina FW-1	09/04/12	13/04/12
T1.2 Provar scripts balanceig	14/04/12	25/04/12
T1.3 Provar scripts tallafocs	14/04/12	25/04/12
T1.4 Instal·ció FW-1	26/04/12	29/04/12
T2 Servidor de xarxa	30/04/12	03/06/12
T2.1 Preparar màquina S-Xarxa	30/04/12	01/05/12
T2.2 Creació VLAN's	02/05/12	06/05/12
T2.3 Gestió del transit, IPTABLES	02/05/12	13/05/12
T2.4 Servei DHCP	09/05/12	13/05/12
T2.5 Servei DNS i control peticions	15/05/12	19/05/12
T2.6 Filtre proxy, Squid	21/05/12	23/05/12
T2.7 Servei de fitxers, Samba	24/05/12	25/05/12
T2.8 Instal·lació S-Xarxa	26/05/12	03/06/12
T3 Servidor d'impressió i escaneig	04/06/12	10/06/12
T3.1 Preparar màquina S-Impres...	04/06/12	05/06/12
T3.2 Servei Cups i control Pykota	06/06/12	08/06/12
T3.3 Instal·lació S-Impressio	09/06/12	10/06/12
T4 Servidor d'internet	11/06/12	24/06/12
T4.1 Preparar màquina S-Web	11/06/12	12/06/12
T4.2 Servei apache, php i mysql	13/06/12	13/06/12
T4.3 Instal·lar SO i configurar S-...	14/06/12	15/06/12
T4.4 Migració Moodle, Joomla i i...	16/06/12	22/06/12
T4.5 Instal·lació S-Web i S-Backup	23/06/12	24/06/12
T5 Configuració i integració de clients	25/06/12	01/07/12

Les tasques que requerien aturar el funcionament de la xarxa les he realitzat en períodes de vacances o bé en caps de setmana.

1 Arquitectura de xarxa

1-1 Diagrama funcional

Conceptualment es parteix del la següent arquitectura:



Aquest diagrama requereix de concreció, el punt més crític és el tallafoc, ja que ha de discriminar el transit en funció de l'origen, el destí i el port dels paquets, per encaminar-lo per la ruta òptima.

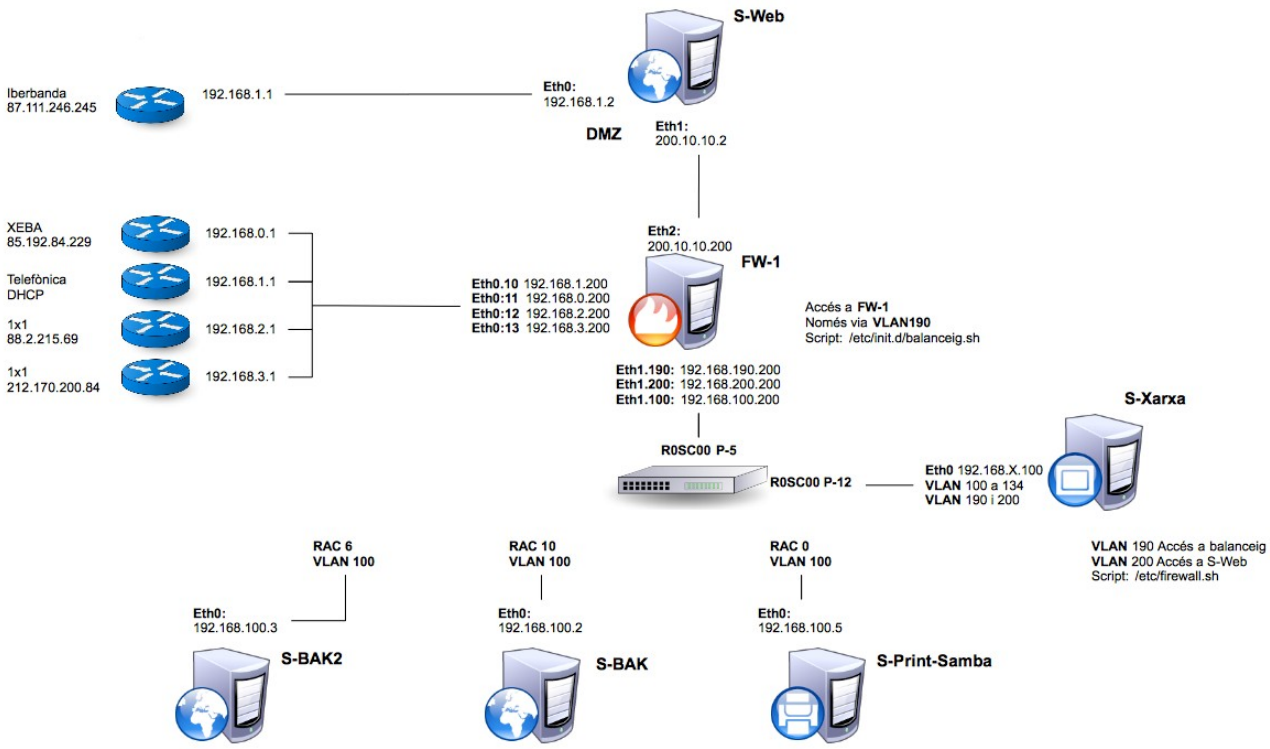
El segon punt d'interès és l'agrupament de serveis en servidors. Per optimitzar l'arquitectura no és necessària una relació directe entre servei i servidor. Una situació de compromís que compartís serveis afins en una mateixa màquina seria l'òptima.

Els equips es divideix en tres nivells, el tallafocs té en d'altres la funció d'interconnectar-los. Els nivells són:

- Nivell 1 Màquines exposades a l'exterior, S-Web, *routers* i Tallafocs
- Nivell 2 Servidors interns de la xarxa
- Nivell 3 Clients de la xarxa

1-2 Disseny de xarxa

El disseny de la xarxa de servidors es concreta en el següent esquema:

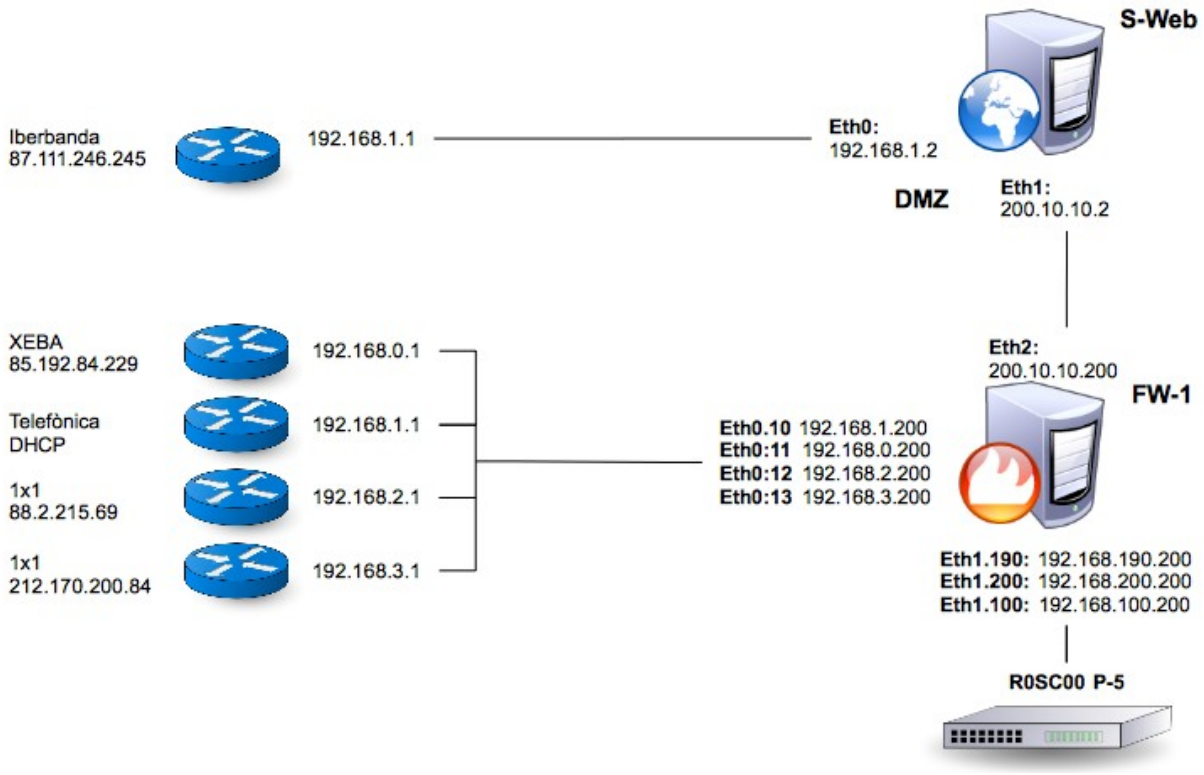


La instal·lació completa compta amb tota l'estructura de *Rac's*, s*witch's* i els punts d'accés per permetre la connectivitat a tots els clients.

Per facilitar les tasques de disseny i estudi divideixo l'arquitectura de xarxa en els mateixos 3 nivells del diagrama conceptual.

1-2-1 Nivell 1

En aquest nivell es troben les màquines exposades directament a *internet*.



Routers

Els *routers* s'agrupen en dos blocs. El primer el forma el *router* d'iberbanda que permet la connectivitat del servidor web a *internet*, i el segon grup de 4 permet la connexió a *internet* de la resta de clients de la xarxa.

Segons el primer diagrama funcional, i aparentment el més lògic, tots els *routers* passen pel tallafocs, en canvi a la solució definitiva el *router* del servidor web no. Els motius són els següents:

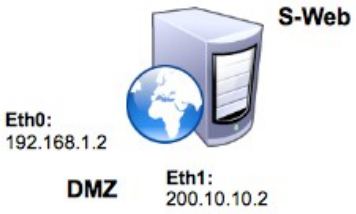
- La seva funcionalitat és molt diferent de la resta, no està destinat a fer balanceig de càrrega.
- Si es combina amb la resta de *routers* el disseny de les regles d'*iptables* del tallafocs es complica, cal discriminar orígens diferents per adreçar al destí correcte.
- Les funcions de tallafocs pel S-Web es poden fer al mateix *router*, ja que admet la redirecció selectiva per ports.
- El servidor web continua sent visible des de l'exterior encara que hi hagin problemes a la xarxa interna.

Els 4 *routers* destinats al balanceig de càrrega disposen d'una VLAN independent per cadascun d'ells. Podrien estar tots a la mateixa, però el fet de separa-los facilita molt les tasques de control. D'aquesta forma mirant el trànsit per cadascuna de les VLAN es controla directament el treball que fa cada *router*.

Servidor Web

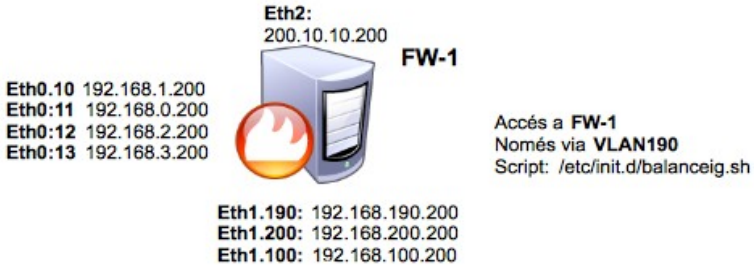
Un dels objectius de disposar d'un servidor web a les pròpies instal·lacions és la millora de l'accés a *internet*. Es tracta de:

- Reduir el nombre de peticions *d'internet* que surten pels *routers*.
- Dotar de gran velocitat l'accés a l'entorn educatiu propi, el ***Moodle***, que copa un percentatge molt alt de la quota d'accés a *internet*



Per aquests motius es dota al servidor amb dues interfícies de xarxa. Eth0 es configura amb els paràmetres per accedir a *internet* extern, i Eth1 amb els paràmetres per accedir a la xarxa interna

Tallafocs

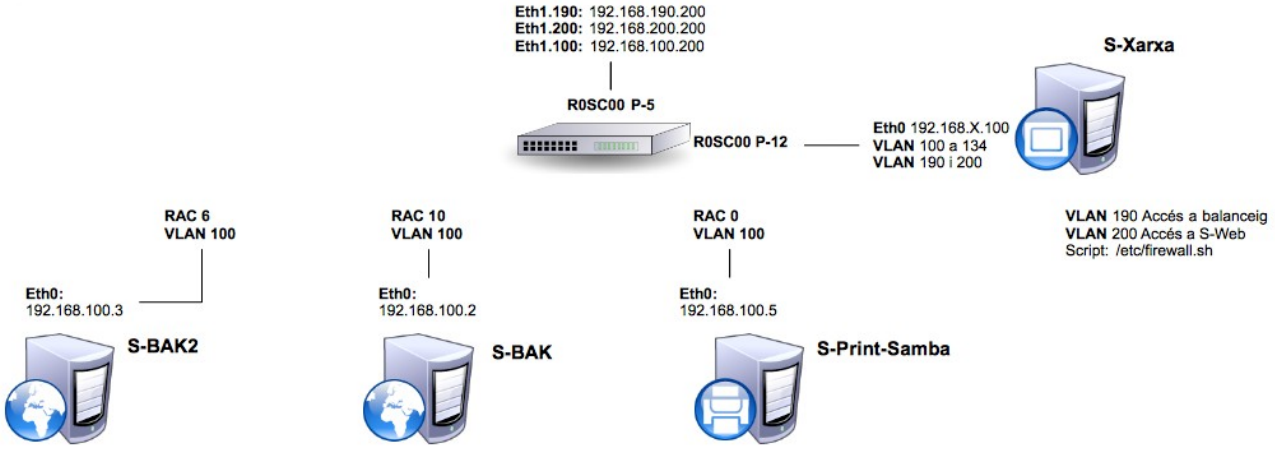


El tallafocs disposa de tres interfícies de xarxa per gestionar tot el transit. La utilització de *VLAN's* permet ajustar les polítiques de xarxa als requisits del sistema amb molta facilitat i fiabilitat.

- Eth2: No conté *VLAN's* i permet l'accés al propi servidor web amb la màxima velocitat que permet la xarxa local, en aquest cas 1Gb
- Eth1: Enllaça amb la xarxa interna LAN, i per facilitar la gestió del trànsit es divideix en 3 *VLAN's*
    - Eth1.190: Aquesta interfície és la única que permet l'accés al propi tallafocs per tasques administratives.
    - Eth1.200: Recull tot el transit que té com a destí el propi servidor web
    - Eth1.100: Permet l'accés entre el servidor web i els servidors interns, imprescindible per poder fer còpies de seguretat.
- Eth0: És la interfície que connecta amb els routers que fan balanceig de càrrega per servir totes les peticions *d'internet* a excepció de les destinades al propi servidor web del centre.

1-2-2 Nivell 2

En aquest nivell s'ubiquen els servidors de la pròpia LAN, que no estan directament exposats a *internet*, l'accés sempre és via tallafocs.



El resultat final d'aquest disseny coincideix força amb el primer diagrama funcional. La diferència principal està en l'agrupament de **serveis** i **servidors**.

S-Xarxa

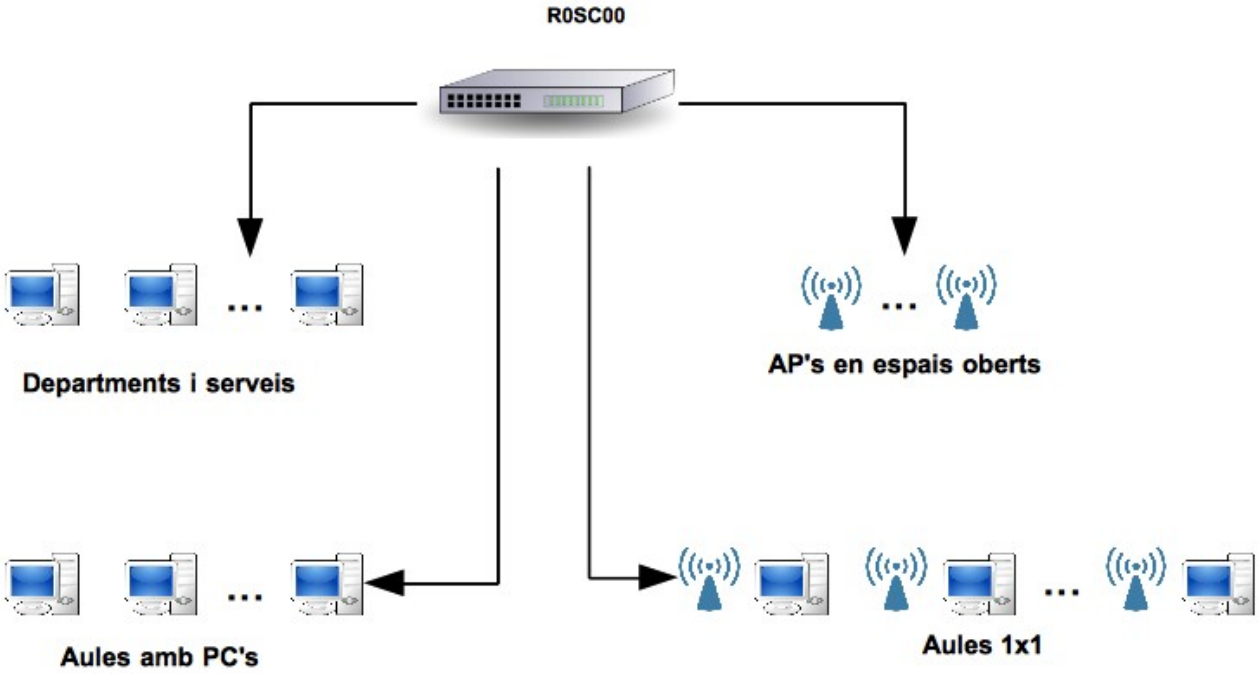
Aquest és el servidor clau del segon nivell de xarxa. Gestiona tot el transit de la LAN i fiscalitza l'accés a *internet*. Disposa d'una sola interfície de xarxa amb diverses *VLAN's*. Aquestes s'organitzen de la següent forma:

- VLAN 100: Permet l'accés a la resta de servidors de la LAN
- VLAN 190: Permet l'accés al balanceig de càrrega
- VLAN 200: Permet l'accés al servidor web
- VLAN 101-134: Donen servei als diferents clients de la xarxa organitzats en *VLAN's*

Aquest servidor que treballa com a ***proxy* transparent** discrimina les peticions *d'internet*. Per la VLAN 190 envia totes les peticions d'internet a excepció de les destinades a domini *inskta.cat*, que és el domini propi del centre ubicat al servidor web local. Les peticions del domini inskta.cat es dirigeixen a la VLAN 200 per evitar el pas pels *routers* i accedir al servidor web a velocitat de LAN.

1-2-3 Nivell 3

Aquest és el nivell del clients, per tant l'arquitectura de xarxa és molt simple. Es redueix a la distribució de les *VLAN's* pels diferents *RAC's* i espais del centre.



La distribució de les diferents *VLAN's* es fa per línies troncals entre *RAC's* o fins i tot entre diversos *switch's* en un mateix RAC.

Cada aula 1x1 disposa d'un punt d'accés propi i d'un ordinador connectats a la mateixa VLAN. Aquesta configuració facilita el treball d'alumnes amb portàtil com pot ser el control remot d'ordinadors amb l'aplicació ***iTalc*** o les polítiques d'accés a *internet* que són independents per cada aula.

2 Regles de xarxa

Es tracta de totes les regles que controlen o encaminen les comunicacions a diferents destins. Aquest treball es fa bàsicament a nivell d'*iptables*, tot i que hi ha una aplicació, l'*squid*, que també fiscalitza el transit que té com a destí *internet*.

Els servidors que contenen aquestes regles són **S-FW1**, el tallafocs que controla la comunicació amb l'exterior i balanceja els routers , i **S-Xarxa** que bàsicament gestiona el transit de la LAN i fa les funcions d'un *proxy* transparent.

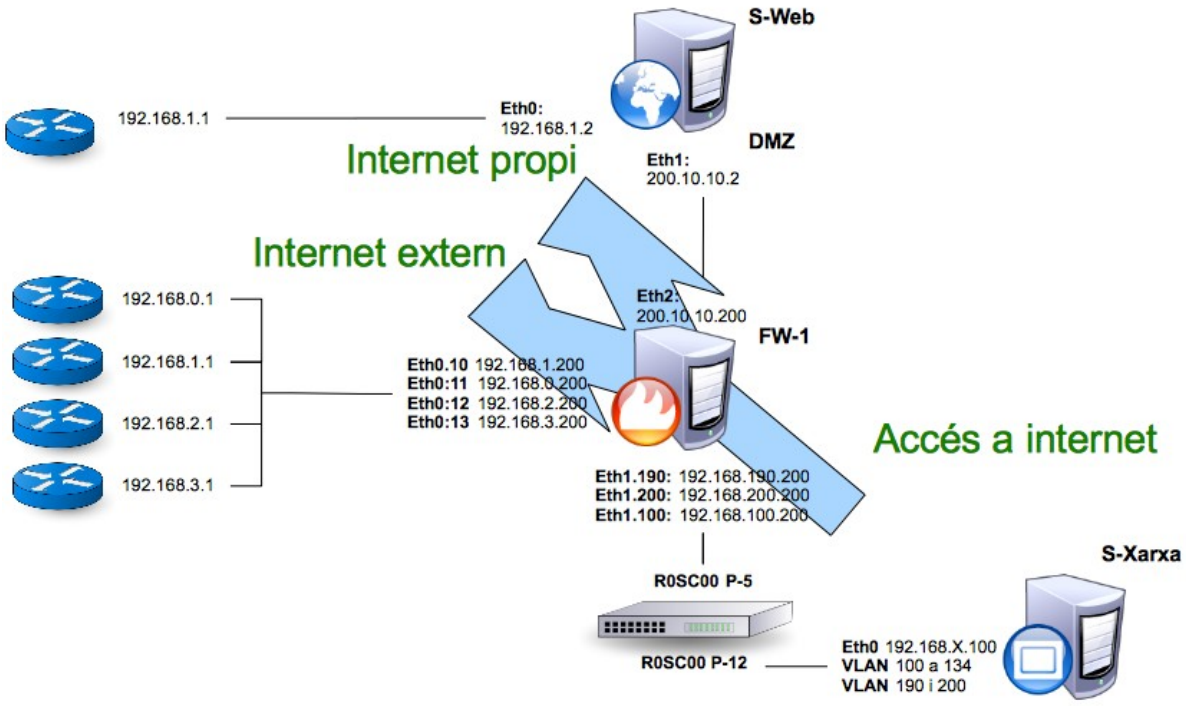
2-1 Tallafocs, S-FW1

Les funcions d'aquest tallafocs són quatre.

1. Protegir la xarxa interna dels atacs externs.
2. Discriminar els dos tipus d'accés a *internet*.
3. Balancejar o repartir les peticions *d'internet* per tots els *routers* disponibles.
4. Permetre fer còpies de seguretat del S-Web a servidors de la LAN.

Compta amb tres interfícies de xarxa organitzades de la següent forma.

- Eth0, disposa de 4 *VLAN's* que es corresponen a cadascun dels *routers*
- Eth1, disposa e 3 VLAN per accedir a diferents seccions de la LAN
    - Eth1.100 comunica amb els servidors interns
    - Eth1.190 accedeix a internet extern
    - Eth1.200 accedeix a internet propi
- Eth2, Accedeix al S-Web propi



L'*script* que conté totes aquestes regles és **blanceig.sh**. Les línies que blinden el tallafocs i la LAN de l'exterior són:

```
############ IPTABLES ############
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X

# Per defecte el FORWARD no està permès i s'hauran de validar una a una les connexions
# Per defecte tampoc es pot entrar al tallafocs

iptables -P FORWARD DROP
iptables -P INPUT DROP
```

La política per defecte és el DROP i aquestes línies deixen el tallafocs completament aïllat però inoperant. Caldrà editar una a una totes les connexions que es vulguin permetre.

Accés a internet extern.

La següent secció permet el retorn de les peticions fetes a *internet* des de la LAN per cadascuna de les *VLAN's* que el **S-FW1** hi té un *router*. Per la interfície Eth1.190 es reben les peticions d'accés a *internet* extern per part del *proxy* transparent, en aquest cas **S-Xarxa**.

```
# Per cadascuna de les VLAN que van al router permet el retorn dels paquets demanats a la LAN
# Permet que surtin tots els protocols i tots els port.
#
iptables -A FORWARD -i eth0.10 -o eth1.190 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0.11 -o eth1.190 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0.12 -o eth1.190 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0.13 -o eth1.190 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1.190 -o eth0.10 -j ACCEPT
iptables -A FORWARD -i eth1.190 -o eth0.11 -j ACCEPT
iptables -A FORWARD -i eth1.190 -o eth0.12 -j ACCEPT
iptables -A FORWARD -i eth1.190 -o eth0.13 -j ACCEPT
```

Accés a la internet pròpia

Les següents línies permeten les connexions al propi servidor web. S'emmascaren les peticions que surten per Eth2 (la interfície que connecta directament amb el S-Web) i permetem el retorn de les peticions fetes pels ports 80, 443 i 22.

```
######### Secció de tallafocs entre S-Web de la DMZ i la LAN ###############
iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
iptables -A FORWARD -i eth2 -o eth1.200 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth1.200 -o eth2 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth1.200 -o eth2 -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -i eth1.200 -o eth2 -p tcp --dport 22 -j ACCEPT
```

Accés dels servidors de copies de seguretat

```
# Acces dels servidors de backups a S-Web
iptables -A FORWARD -i eth1.100 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1.100 -p tcp --dport 22 -j ACCEPT
```

Accés a *internet* del propi tallafocs

S'ha de permetre fins i tot l'accés a *internet* del propi S-FW1, ja que amb la política per defecte del DROP, ni aquest accés és permès.

```
##### Accés al propi tallafocs ######
#Permet les connexions local. Cas contrari no van ni els ping a la seva propia eth
iptables -A INPUT -i lo -j ACCEPT
# Per accedir-hi remotament només ho podem fer des de la VLAN 190
iptables -A INPUT -i eth1.190 -j ACCEPT
# Permet que entrin d'internet la resposta a les peticions  generades de la propia màquina
iptables -A INPUT -i eth0.10 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0.11 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0.12 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -i eth0.13 -m state --state RELATED,ESTABLISHED -j ACCEPT
```

2-1-1 Balanceig de càrrega

En una xarxa on es disposen de diferents *routers* per fer l'accés a *internet*, en aquest cas n'hi ha quatre, és gairebé imprescindible que hi hagi una màquina que actuï com si fos un únic *router*. Aquesta màquina és el **S-FW1**, que fa les funcions de balanceig de càrrega.

La programació d'aquestes funcions estan incloses en el mateix script que conté les regles del tallafocs, **balanceig.sh**

L'script comença inicialitzant les variables que s'utilitzaran per la configuració de la xarxa.

```
#!/bin/bash
### BEGIN INIT INFO
# Provides: Institut Guillem Catà
# Required-Start:    $syslog
# Required-Stop:     $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Balanceig de càrrega i tallafocs per DMZ
# Description:
#
### END INIT INFO
############ CONF GRAL ############
# Crea i/o borra el registre de logs
echo > /var/log/adsl_watchdog.log
# Defineix les variables per configurar les interfícies de xarxa
# i els paràmetres de càrrega per router
adsl_ifaces=(eth0.10 eth0.11 eth0.12 eth0.13)
adsl_ips=(192.168.1.200 192.168.0.200 192.168.2.200 192.168.3.200)
adsl_gws=(192.168.1.1 192.168.0.1 192.168.2.1 192.168.3.1)
adsl_weight=(1 1 1 1)
adsl_upload=(256 256 256 256)
```

- **adsl_ifaces**, llista de les interfícies amb *routers* associats.
- **adsl_ips**, ip de les interfícies.
- **adsl_gws**, ip dels *routers*.

- **adsl_weight**, ponderació de la càrrega pels diferents *routers*
- **adsl_upload**, factor de càrrega de cada *router*

La secció següent configura les interfícies de xarxa, es creen les taules d'encaminament i es genera la variable *multipath* per fer el salt entre les *adsl* disponibles.

```
#
# Configura cadascuna de les interfícies definides a les variables
#
for ((n=0;n<${#adsl_ifaces[@]};n++)); do
        # Es creen i configuren les diferentes vlan
        vconfig add ${adsl_ifaces[n]%%.*} ${adsl_ifaces[n]##*.} &>/dev/null
    ifconfig ${adsl_ifaces[n]} ${adsl_ips[n]} netmask 255.255.255.0 up
    # Borra les configucions, taules i càrregues anteriors
    ip route flush table adsl$((n+1)) 2>/dev/null
    ip rule del from ${adsl_ips[n]} table adsl$((n+1)) 2>/dev/null
    tc qdisc del dev ${adsl_ifaces[n]} root 2>/dev/null
    # limita el cabal d'accés als routers per no saturar-los.
    # Sense aquesta línia baixa la velocitat d'accés després de 2-3h de funcionar
    tc qdisc add dev ${adsl_ifaces[n]} root tbf rate ${adsl_upload[n]}kbit latency 50ms burst 1540
    # Carrega la taula d'encaminamemt “adsl$n” copia la tabla main y canvia default gateway
    while read line ;do
        test -z "${line##default*}" && continue
        test -z "${line##nexthop*}" && continue
        ip route add $line table adsl$((n+1))
    done < \
    <(/sbin/ip route ls table main)
    ip route add default table adsl$((n+1)) proto static via ${adsl_gws[n]} dev ${adsl_ifaces[n]}
    # Crea la regla d'encaminament per sortir per aquesta taula si té aquesta source address
    ip rule add from ${adsl_ips[n]} table adsl$((n+1))
    # Es guarda per generar els salts entre els diferents adsl
    multipath="$multipath nexthop via ${adsl_gws[n]} dev ${adsl_ifaces[n]} weight ${adsl_weight[n]}"
done
```

Es genera la taula d'encaminament amb la variable *multipath* i s'emmascaren els paquets per poder sortir de la LAN

```
#
# Es genera default gw con amb la variable multipath a la taula main
#
ip route del default 2>/dev/null
ip route add default proto static $multipath
# Netegem la cache d'encaminament
ip route flush cache

############ NAT ############
# S'emmascara cada connexió per cadascuna de les interfícies disponibles
# funció imprescindible per poder sortir a l'exterior
for ((n=0;n<${#adsl_ifaces[@]};n++)); do
    iptables -t nat -A POSTROUTING -o ${adsl_ifaces[n]} -j MASQUERADE
done
```

La darrera secció de *l'script* gestiona les marques dels paquets. És imprescindible que cada client que sol·licita una petició d'accés a *internet* se li assigni un *router*, i que aquest es mantingui al llarg de la *vida* de la connexió.

```
############ CONNTRACK ############
# Restaura la marca de la cadena PREROUTING abans d'enrutar-la.
iptables -t mangle -A PREROUTING -j CONNMARK --restore-mark

# CONNTRACK pel multipath
# Es crea una taula personalitzada per marcar els paquets
iptables -t mangle -N my_connmark
# Per aquesta nova taula passen els paquets que encara no s'han marcat
# Es tracta de paquets que inicien una sessió
iptables -t mangle -A FORWARD -m mark --mark 0 -j my_connmark
# Després d'encarrilar el paquet, s'elimina la marca per futures reutilitzacions.
iptables -t mangle -A FORWARD -j MARK --set-mark 0x0

# Gestiona la taula creada my_conmark per cada connexió.
iptables -t mangle -A my_connmark -o eth1 -j RETURN
for((n=0;n<${#adsl_ifaces[@]};n++)); do
        #asocio una marka a cada interfaz
        iptables -t mangle -A my_connmark -o ${adsl_ifaces[n]} -j MARK --set-mark 0x$((n+1))
        iptables -t mangle -A my_connmark -i ${adsl_ifaces[n]} -j MARK --set-mark 0x$((n+1))
done
# Guarda la marca per després poder fer el –restore-mark a PREROUTING
iptables -t mangle -A my_connmark -j CONNMARK --save-mark

# S'encaminen els paquets per la taula que li correspongui
for ((n=0;n<${#adsl_ifaces[@]};n++)); do
        ip ru del fwmark 0x$((n+1)) table adsl$((n+1)) 2>/dev/null
        ip ru add fwmark 0x$((n+1)) table adsl$((n+1))
done
```

2-1-2 Control de routers

El balanceig de càrrega presenta el problema de la caiguda d'una línia o *router*. En aquesta situació el sistema continua enviant els paquets per un *router* no operatiu i un grup de clients perd la connectivitat.

La solució passa per executar *l'script* **multipath.sh**, que des de *crontab* i amb una freqüència de 5 minuts, testeja la sortida de cadascun dels *routers* i torna a calcular la configuració de salts actius en aquell moment.

Aprofitem les variables i constants definides en *l'script* inicial de balanceig de càrrega. Degut a que es tornen a calcular els salts, cal reiniciar la variable *multipath.*

```
#!/bin/bash
# Carrega les variables de l'script de balanceig
source /etc/balanceig.sh loadvars
#De A a M són servidors DNS de referència global que accepten ping's
root_dnservers="B C D E F I J K L M"

multipath_total=0
# Inizialitza la variables per borrar el valor eredat de firewall.sh
multipath=""
```

El pas següent és verificar el funcionament dels *routers*. El mètode emprat és el del *ping*, però amb un doble llaç de forma que si no obtenim resposta d'un *router* repetim la prova però a un altre servidor, per evitar donar un *router* caigut quan el què realment falla és el servidor de test.

Per detectar els *routers* caiguts utilitzem el mètode invers, és a dir, generem una nova variable de salts que conté només *routers* vàlids, posteriorment aquesta cadena la compararem amb la cadena actual del sistema. Aquest mètode té l'avantatge que és vàlid tant per donar *routers* de **baixa** com d'**alta** al sistema.

```
for((n=0;n<${#adsl_ifaces[@]};n++)); do
  pong=0
  for letter in $root_dnservers; do
    if(ping -n -c1 -W2 $letter.root-servers.net -I ${adsl_ips[n]} &>/dev/null);then
       pong=1
      multipath="$multipath nexthop via ${adsl_gws[n]}  dev ${adsl_ifaces[n]} weight ${adsl_weight[n]}"
       let multipath_total+=1
        break
      fi
  done
      ##Cada connexió caiguda es registra al fitxer de logs
      if [[ $pong == 0 ]];then
            echo `date`" la conexion con ${adsl_gws[n]} esta down" >> /var/log/adsl_watchdog.log
   fi
done
```

En el darrer bloc es compara la ruta vàlida del sistema amb la ruta generada a partir de la detecció de *routers* actius, variable *$multipath.*

```
#Si es comprova que tots els routers han caigut se surt i ni es fa res
test -z "${multipath}" && exit 1

# Inicialitzem la variable $route amb el multipath actual
while read line ;do
      test -z "${line##default*}" && begin=1
      test "$begin" == 1 && route="$route ${line}"
done < \
<(/sbin/ip route ls)

# Generem la ruta del multipath, que varia en funció si n'hi ha un o més d'un actius
if [[ $multipath_total > 1 ]];then
      route_multipath=" default  proto static${multipath}"
else
      route_multipath=${multipath#nexthop }
      route_multipath=${route_multipath% weight*}
      route_multipath=" default ${route_multipath/ dev/ dev} proto static"
fi
# Es comparen el 2 multipath i només s'actualitza si són diferents
if [[ "$route" != "$route_multipath" ]];then
      ip route chg default proto static $multipath
      ip route flush cache
      echo `date`" Canvi de default gateway a $multipath" >> /var/log/adsl_watchdog.log
fi
```

2-2 Servidor de xarxa, S-Xarxa

El servidor de xarxa fiscalitza el transit que circula per la xarxa i restringeix l'accés a *internet* de les adreces no permeses. També dirigeix totes les peticions del domini propi al servidor web.

Les regles de configuració de les *iptables* (es carreguen per amb *l'script* **firewall**.**sh**) és la següent:

- Per defecte habilita el FORWARD, això implica que el transit estarà permès per tot arreu.
- Accepta el transit des de *VLAN's* a sortides d'internet que no siguin pel port 80.
- Permetre l'accés a algun dispositiu de xarxa (impressores), que no formi part de la VLAN però que s'hi hagi d'accedir.
- Permetre l'accés lliure d'algunes màquines a internet
- Dirigeix les peticions del port 80 d'internet al *proxy*, a excepció de de totes les peticions que tinguin com a destí el propi del centre, inskta.cat
- Denegar tota la resta de peticions per cadascuna de les *VLAN's* que no s'hagin permès anteriorment.

Al principi de *l'script* de configuració de les *iptables* es netegen totes les possibles regles anteriors, i s'accepte per defecte tot el transit de la cadena FORWARD.

```
#!/bin/bash

iptables -F
iptables -X
iptables -Z
iptables -t nat -F

iptables -P FORWARD ACCEPT
```

A continuació acceptem totes les peticions que tinguin com a destí una URL que s'hi accedeixi per un port que no sigui el 80 i que es vulgui permetre. En el següent llistat hi figuren algunes de les acceptades com UOC, SAGA ... que s'hi ha d'accedir via port 443.

```
### IOC i UOC
iptables -A FORWARD -s 192.168.0.0/16 -d cv.uoc.edu -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/16 -d ioc.xtec.cat -p tcp --dport 443 -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/16 -d cambridgelms.org -p tcp --dport 443 -j ACCEPT
### Studenconsult
iptables -A FORWARD -s 192.168.0.0/16 -d studentconsult.com -p tcp -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/16 -d studentconsult.com -p udp -j ACCEPT
iptables -A FORWARD -s 192.168.0.0/16 -d media.us.elsevierhealth.com -p tcp -j ACCEPT
### SAGA
iptables -A FORWARD -s 192.168.0.0/16 -d saga.xtec.cat -p tcp --dport 443 -j ACCEPT
```

També s'ha de permetre l'accés a impressores o servidors d'impressió que no estan a la mateixa VLAN que el client.

```
#### Permet imprimir a la HP de Fusteria
iptables -A FORWARD -s 192.168.0.0/16 -d 192.168.102.205 -j ACCEPT
```

Es permet l'accés lliure a *internet* pel port 443 d'algunes màquines particulars que s'identifiquen a partir de la seva adreça MAC.

```
#
# Mac de profes per permetre tot el port 443
#
# Àlex
iptables -A FORWARD -p tcp --dport 443 -m mac --mac-source 00:26:5e:57:33:34 -j ACCEPT
# David
iptables -A FORWARD -p tcp --dport 443 -m mac --mac-source 00:1e:4c:02:26:94 -j ACCEPT
# Toni
iptables -A FORWARD -p tcp --dport 443 -m mac --mac-source 60:33:4b:04:b9:d5 -j ACCEPT
# Albert
iptables -A FORWARD -p tcp --dport 443 -m mac --mac-source 1c:ab:a7:af:e6:59 -j ACCEPT
```

Es dirigeix totes les peticions d'accés a *internet* via port 80 i que siguin diferents del domini propi (**inskta.cat**) al *proxy*. Les peticions amb destí al servidor web propi es millor dirigir-les al propi servidor que no carregar més el *proxy*.

```
#
# Redireccions de VLAN's
#
### Redirecciono VLAN 103 Comerç a l'Squid
iptables -t nat -A PREROUTING -s 192.168.103.0/24 ! -d 200.10.10.2 -p tcp --dport 80 -j REDIRECT --to-port 3128
### Redireccio VLAN Aula0.13 a Squid llista Blanca
iptables -t nat -A PREROUTING -s 192.168.107.0/24 ! -d 200.10.10.2 -p tcp --dport 80 -j REDIRECT --to-port 3128
#
```

Finalment es deneguen totes les peticions que no s'han acceptat prèviament amb un DROP.

```
#
# Denegar totes les peticions no acceptades previament
#
### Denega peticions comerç, VLAN 103
iptables -A FORWARD -s 192.168.103.0/24 -j DROP
### Denega peticions wifi ktalliure VLAN 105
iptables -A FORWARD -s 192.168.5.0/24 -j DROP
```

3-Serveis de xarxa

Els serveis de xarxa doten al sistema de les funcionalitats necessàries per fer-lo operatiu. Gestionen les diferents *VLAN's*, proporcionen els paràmetres necessaris per poder connectar els equips a la xarxa, resolen noms i fan de *proxy* amb el filtratge de continguts.

3-1 Creació de les VLAN's

La creació de *VLAN's* és imprescindibles en xarxes amb molts equips. En el nostre cas el nombre d'equips que s'hi poden connectar és més de 400, si la xarxa fos de classe C només disposaríem de 255 adreces menys 2 (*broadcast* i xarxa).

No només hi ha la qüestió de l'impediment físic si no la possibilitat d'utilitzar polítiques diferents per diferents grups de clients. La utilització de diferents xarxa facilita molt aquesta tasca, ja que aplicar una determinada política per tots els equips d'una mateixa xarxa és molt més simple que particularitzar per equips concrets.

Quan dins d'una mateixa xarxa uns equips han de tenir unes polítiques i els altres unes altres cal identificar-los, per l'adreça IP o MAC, i assignar a aquestes màquines polítiques personalitzades. Evidentment no és el mateixdirigir-se a una IP que a tot el marge d'IP d'una xarxa, la quantitat d'equips que cobreixes és molt més gran.

3-1-1 Configuració de VLAN's

El procés de configuració és molt simple. Només requereix un parell de passos:

- Instal·lar el paquet *vlan*
- Editar el fitxer *interfaces*

En aquest fragment del fitxer *interfaces* es veu la configuració de les *VLAN's* pels ordinadors de direcció i pels ordinadors de la sala de professors.

```
# Targeta física per a totes les VLAN
auto eth0

# Configuracio VLAN 101 Direccio
auto eth0.101
iface eth0.101 inet static
        address 192.168.101.100
        netmask 255.255.255.0

#Configuracio VLAN 102 Profes
auto eth0.102
iface eth0.102 inet static
        address 192.168.102.100
        netmask 255.255.255.0
```

3-2 Servei DHCP

Aquest servei configura dinàmicament els paràmetres del protocol IP que requereixen les màquines que es connecten a la xarxa i reserva adreces per les màquines que tinguin una IP estàtica (servidors, impressores...)

3-2-1 Configuració del servei DHCP

La configuració del servei també és molt simple i només s'ha de tenir en compte que cal configurar-lo per treballar a diferents *VLAN's*

Aquest procés es fa en 3 passos

- Instal·lació del paquet *isc-dhcp-server*
- Indicar la relació de totes les interfícies al fitxer i*sc-dhcp-server*
- Editar el fitxer de configuració *dhcpd.conf*

En el fitxer de configuració s'ha d'editar una *subnet* per cadascuna de les *VLAN's* que s'hagi de donar servei, a més dels paràmetres habituals. En el següent fragment del fitxer de configuració s'hi veuen els paràmetres per la VLAN de direcció i la sala de professors.

```
#
# VLAN de direcció
#
subnet 192.168.101.0 netmask 255.255.255.0 {
        range 192.168.101.20 192.168.101.50;
        option routers 192.168.101.100;
        option broadcast-address 192.168.101.255;
        option domain-name-servers 192.168.101.100;
}
#
# VLAN Profes
#
subnet 192.168.102.0 netmask 255.255.255.0 {
        range 192.168.102.20 192.168.102.50;
        option routers 192.168.102.100;
        option broadcast-address 192.168.102.255;
        option domain-name-servers 192.168.102.100;
}
```

3-3 Servei DNS

Sovint aquest servei és extern en es xarxes local. El més habitual seria utilitzar un servidor DNS *d'internet*. En aquest cas no és possible utilitzar-ne un d'extern i els motius són:

- El domini propi de l'institut té una adreça pública per l'accés de l'exterior del centre i una de privada per l'accés de dins la LAN
- Millora l'accés a *internet* ja que guarda en memòria les adreces dels dominis sol·licitats i les successives peticions no requereixen peticions externes per resoldre el nom.
- Permet la fiscalització dels accessos a *internet* dels alumnes, ja que el servei registra les peticions que cada client fa.

3-3-1 Configuració del servei DNS

La configuració no és excessivament complexa però cal anar en compte amb les zones pròpies que es creïn, és a dir que resolgui correctament en nom del servidor Web del propi centre (inskta.cat). Per defecte el servei assignaria la IP pública fet que enviaria tot el transit pel routers de "sortida" i tornarien a entrar pel *router* del propi servidor, en lloc de viatjar per la LAN accelerant de forma molt considerable la velocitat d'accés.

La configuració del servei requereix dels següents passos:

- Instal·lar el paquet bind9
- Editar el fitxer resolv.conf per dir-li que resolgui ell mateix els noms
- Editar els fitxers de configuració
- Crear les zones pròpies, tant per resolució directa com inversa

Després d'instal·lar el paquet i modificar el fitxer ***resolv-conf*** per tal que sigui ell mateix qui resolgui els noms editem el fitxer named.conf.options per indicar-li quins seran els servidors externs que haurà de consultar cas que ell no sàpiga resoldre. El següent és un fragment del fitxer amb la configuració dels *forwarders*.

```
options {
        directory "/var/cache/bind";

         forwarders {
              8.8.8.8;
              213.176.161.16;
         };
```

En el fitxer de configuració *named.conf.loca*l es defineixen les zones internes, és a dir el nom que ha de resoldre per a la nostra LAN. En el següent requadre es veu la configuració de la zona inskta.cat

```
zone "inskta.cat" {
        type master;
        notify no;
        file "/etc/bind/db.inskta";
};
```

En aquest fitxer de configuració se li indica qui conté la configuració de la zona nova que hem definit. En aquest cas és el fitxer **db.inskta**, que creem a partir del model **db.local**.

El contingut d'aquest fitxer inclou els paràmetres necessaris per identificar el domini amb una adreça IP. El seu contingut és:

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     inskta.cat. root.inskta.cat. (
                      201109201       ; Serial
                       604800         ; Refresh
                        86400         ; Retry
                       2419200         ; Expire
                       604800 )       ; Negative Cache TTL
;
@       IN      NS      inskta.cat.
@       IN      A       200.10.10.2
;@      IN      AAAA    ::1

www     IN      A       200.10.10.2
```

3-4 Proxy

El servei de *proxy* el presta l'***squid***, però en aquest cas la configuració és més complexa de l'habitual. Un dels objectius del projecte és filtrar de forma fefaent l'accés a *internet* per part de l'alumnat, però també cal disposar d'algun mecanisme per obrir l'accés a *internet* quan el professor de l'aula ho estimi convenient.

El repte és que el mateix *squid* es comporti de dues formes diferents, i a voluntat del professor, es pugui escollir una forma restrictiva o bé permissiva. La forma de treball restrictiva es basa en llista blanca, on només estan permeses les adreces que hi figuren. La forma permissiva treballa amb llista negra, és a dir, que per defecte tot està permès menys el què figura a l'esmentada llista.

Aquest funcionament dual s'aconsegueix llaçant dues instàncies del mateix *squid* però utilitzant en cada cas un fitxer de configuració diferent. Cadascuna d'aquestes instàncies escolta un port diferent, i les *iptables* dirigeixen a una o altra instància en funció de si es treballa de forma permissiva o restrictiva.

3-4-1 Configuració del servei proxy

Després d'instal·lar el paquet *squid* editem el primer fitxer ***squid.conf***. La primera instància del *proxy* escolta el port 3128 i treballa en mode transparent.

```
#
# Squid normally listens to port 3128
http_port 3128 transparent
```

Per tal que sigui operatiu cal configurar dos paràmetres més.

- *acl*, llista de control d'accés
- *http_access*, o política d'accés a internet

De *acl* n'hi han de dos tipus. En un primer cas la llista serveix per indicar un destí a *internet*. i en un segon cas aquesta llista especifica un conjunt de clients de la xarxa.

El següent gràfic mostra un fragment del fitxer *squid.conf.*

```
# acl llista blanca només URL permeses
# acl llista negra, URL no permeses
acl llistablanca dstdomain "/etc/squid3/llistablanca.txt"
acl llistanegra dstdomain "/etc/squid3/llistanegra.txt"

# acl de diferents espais del centre
acl aula013 src 192.168.107.0/24
acl comerc src 192.168.103.0/24
acl ktalliure src 192.168.5.0/24
acl 2ESOn1 src 192.168.110.0/24
acl 2ESOn2 src 192.168.111.0/24
acl 2ESOn3 src 192.168.112.0/24
acl 3ESOn1 src 192.168.113.0/24

# acl amb llista d'ordinadors personalitzats
acl profesktalliure arp "/etc/squid3/mac_profes.txt"
acl profesfusteria arp "/etc/squid3/mac_profesfusteria.txt"
acl mac_culturals arp "/etc/squid3/mac_culturals.txt"
```

La informació que contenen aquestes *acl's* és la següent:

- acl llistablanca dstdomain "/etc/squid3/llistablanca.txt"
    - Es tracta d'una acl que té per nom llista blanca i que el seu contingut s'ubica en el fitxer de text llistablanca.txt i conté totes les URL permeses
- acl aula013 src 192.168.107.0/24
    - Es tracta d'una acl que té per nom aula013 referencia tots els ordinadors d'una aula determinada, l'aula 0.13, podem assegurar que es tracta d'aquest espai ja que la VLAN que distribueix el *switch* correspon al marge de IP indicat
- acl profesktalliure arp "/etc/squid3/mac_profes.txt"
    - Es tracta d'una acl de nom profesktalliure que conté les adreces MAC d'ordinadors de profes a qui s'aplicarà una política diferencia d'el lloc on s'hagin connectat.

Definides les llistes cal aplicar una política d'accés a *internet*. La següent imatge és un fragment del fitxer de configuració amb la concreció d'aquestes polítiques.

```
http_access allow profesfusteria
http_access allow fusteria !llistanegra
http_access allow profesktalliure
http_access allow aula013 llistablanca
http_access allow comerc !llistanegra
http_access allow ktalliure llistablanca
http_access allow 2ESOn1 llistablanca
http_access allow 2ESOn2 llistablanca
http_access allow 2ESOn3 llistablanca
```

- *http_access allow* profesfusteria
    - En aquest cas la *acl* **profesfusteria**, que és una llista d'adreces MAC, té l'accés completament permès. És a dir que podrien navegar per tot arreu
- *http_access allow* comerc !llistanegra
    - En aquest cas els equips de la acl comerç, tenen marge de ip's 92.168.103.0/24 tindran accés a *internet* sempre que la URL no coincideixi amb alguna de la llista negra

Amb combinacions de *acl's* i polítiques d'accés, es pot configurar un filtre d'accés a *internet* molt personalitzat, aplicant polítiques a grups d'equips o a equips de forma individual.

3-4-2 Configuració del segon squid

El primer que cal canviar és el port que escolta *l'squid*. Cal canviar-lo del port per defecte ja que no hi poden haver dues instàncies del mateix programa que escoltin el mateix port.

```
# Squid normally listens to port 3128
http_port 3228 transparent
```

Un altre paràmetre que no pot coincidir és el **número de procés**. Se li defineix el fitxer on es guardarà l'esmentat paràmetre.

```
#  TAG: pid_filename
#       A filename to write the process-id to.  To disable, enter "none".
#
#Default:
pid_filename /var/run/squid_llistanegra.pid
```

Per tal que la velocitat d'accés a la *cache* sigui òptima, s'ha d'utilitzar un directori diferent al de la primera instància.

```
#Default:
cache_dir ufs /var/spool/squid_llistanegra 10000 16 256
```

Per arrancar aquest segon *squid*, a la crida se li ha d'especificar quin és el fitxer de configuració.

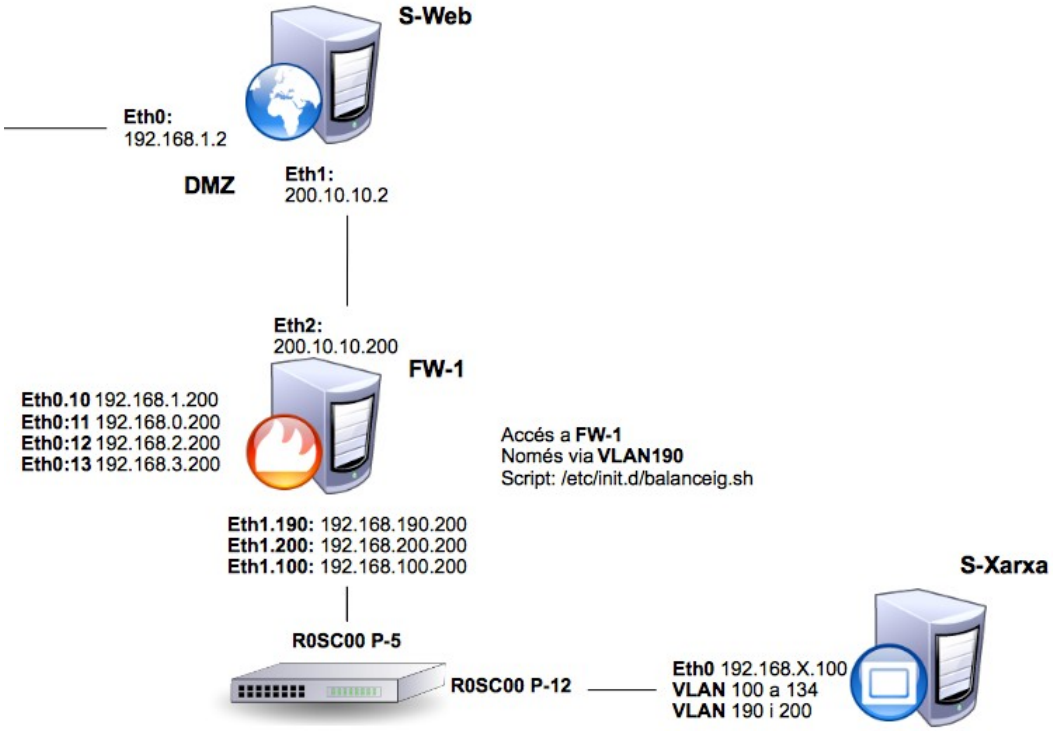
- /usr/sbin/squid -f /etc/squid/squid_llistanegra.conf

4- Servidor d'internet, S-Web

És el servidor *d'internet* que hostatge el portal de l'institut i l'aula virtual Moodle. Amb dos objectius clars.

- Proporcionar la màxima velocitat al treball amb l'aula virtual dins l'institut
- Millorar l'accés general a *internet*

Duran les hores lectives es produeix una gran concurrència d'alumnes que accedeixen a l'aula virtual. El fet de tenir el servidor *d'internet* accessible des de la LAN proporciona un accés molt ràpid al *Moodle* i redueix un transit que hauria de sortir pels *routers*. Aquesta situació també es repeteix, tot i què en un menor grau, amb el portal de l'institut.



L'accés al servidor es fa per dues vies. Per Eth0 el S-Web es connecta a un *router* exclusiu i d'aquí a l'exterior. En canvi per Eth1 el S-Web es connecta a la LAN. Abans els paquets circulen per FW-1 que actua de tallafocs permeten només el retorn dels paquets que s'han sol·licitat des de la LAN.

4-1 Configuració

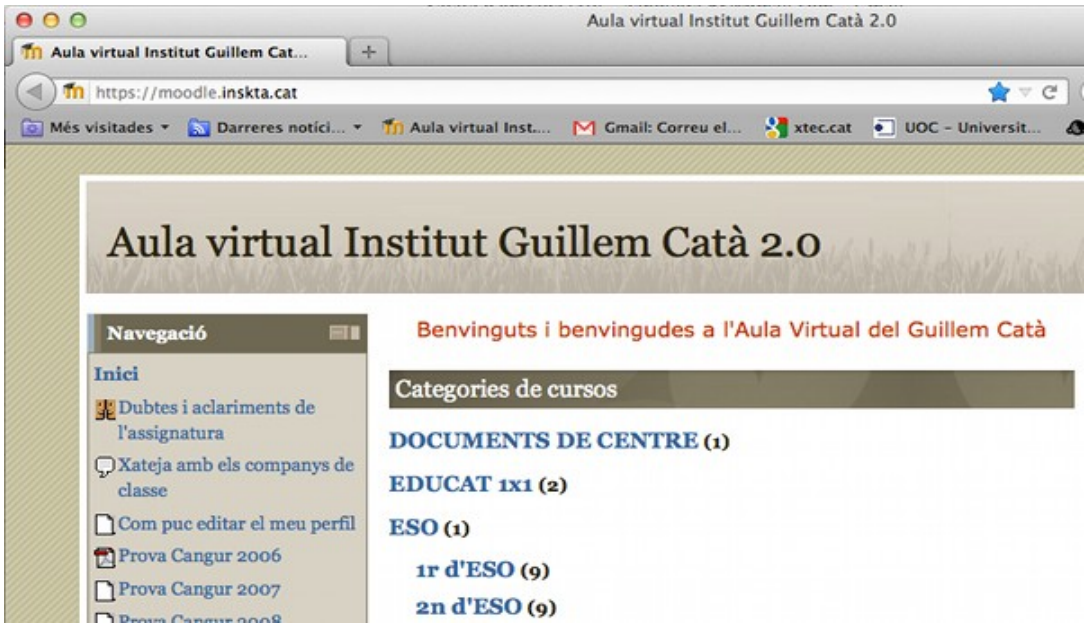
El sistema operatiu del servidor és *Debian Squeeze* i se li afegeixen els paquets de:

- Apache
- PHP
- MySQL

Imprescindibles per funcionar els gestors de continguts. Tant l'aula virtual (*Moodle*) com el portal (*Joomla*) basen el seu funcionament en aquest tres serveis.

Els portal és accessible a l'adreça *http://inskta.cat,* i treballa pel port 80

L'aula virtual és accessible a l'adreça *https://moodle.inskta.cat.* Al contenir informació personal d'alumnes i professors treballa pel port 443 i es configura com a subdomini *moodle.inskta.cat*.



4-1-1 Configuració de l'apache

La configuració per defecte de *l'apache* dirigeix el domini a /var/www. En el nostre cas no ens interessa, ja que es vol que l'arrel del domini es situï a /var/www/portal que és on s'ubica el portal de l'institut.

L'altre aspecte a considerar és que amb la configuració bàsica es podria accedir a totes les carpetes que pengessin del directori /var/www. En el nostre cas el *Moodle* s'ubica a:

- /var/www/moodle

Això vol dir que s'hi podria accedir fàcilment des de http://inskta.cat/moodle, cosa que no ens interessa per 2 motius.

- Es podria accedir a d'altres llocs que no interessés ex: /var/www/privat1
- No s'utilitzaria la certificació SSL

Fragment del fitxer /etc/apache2/sites-available/default

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        ServerName inskta.cat
        DocumentRoot /var/www/portal
        <Directory />
                Options FollowSymLinks
                AllowOverride All
        </Directory>
        <Directory /var/www/portal>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride All
                Order allow,deny
                allow from all
        </Directory>
```

Les modificacions que s'han aplicat són:

- S'afegeix la directiva **ServerName inskta.cat**
- DocumentRoot passa a /**var/www/portal**
- La directiva Directory és a **/var/www/portal**

El cas del *Moodle* és una mica més complicat per tractar-se d'un entorn segur i per tant s'han de configurar correctament les claus SSL. Per accedir-hi com a subdomini els paràmetres de configuració són semblants als del portal.

Fragment del fitxer /etc/apache2/sites-available/default

```
<IfModule mod_ssl.c>

NameVirtualHost *:443

<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/moodle
        ServerName moodle.inskta.cat
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/moodle>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>

        SSLEngine on

        SSLCertificateFile    /etc/ssl/certs/server.crt
        SSLCertificateKeyFile /etc/ssl/private/server.key

        SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
```

Afegim l'accés al certificat i la clau.

- SSLCertificateFile   /etc/ssl/certs/server.crt
- SSLCertificateKeyFile /etc/ssl/private/server.key

Per arrancar el servei ens calen un parell de coses:

- Habilitar el mòdul ssl de l'apache: **a2enmod ssl**
- Habilitar el nou lloc: **a2ensite default-ssl**

Després de recarregar el servei ja apareix el nou lloc lloc *ssl* habilitat

```
lrwxrwxrwx 1 root root   26 27 jul  2011 000-default -> ../sites-available/default
lrwxrwxrwx 1 root root   30 19 jun 13:45 default-ssl -> ../sites-available/default-ssl
```

4-2 Certificats digitals

L'opció correcta per treballar amb entorns segurs seria utilitzar certificats digitals signats per entitats competents. En el nostre cas i per temes econòmics ens auto-certifiquem.

El proces és el següent:

Primer cal disposar de la clau digital que generem

- openssl genrsa -des3 -out server.pkey 2048

La clau requereix una frase de pas que es pot eliminar per evitar que la requereix cada vega que s'inicia el servei.

- openssl rsa -in server.pkey -out server.key

Amb la clau anterior generem una petició de certificat. Aquest procés sol·licita informació de l'empresa certificadora, que serà visible pels navegadors.

- openssl req -new -key server.key -out server.csr

El darrer pas és auto signar-nos el certificat

- openssl x509 -req -days 400 -in server.csr -signkey server.key -out server.crt

La informació del certificat vista pel navegador és la següent

4-3 Procés d'importació

Abans del procés de migració el portal de l'institut i el *Moodle* estaven ubicats al servei de *hosting* de l'empresa CDmon.

Degut al canvi de nomenclatura del Departament d'ensenyament de la Generalitat, a més de la ubicació, també s'ha canviat el domini. Inicialment la nomenclatura era:

- IES Guillem Catà

D'aquí se'n va treure el domini **ieskta.cat**

Amb la nova nomenclatura som:

- INS Guillem Catà

El nou domini contractat és **inskta.cat**

La migració ha implicat:

- Copiar directoris que es posen a
    - Pel portal /var/www/portal
    - Pel moodle 2, /var/www/moodle i /var/moodledata
- Canviar dominis
- Importar bases de dades
- Modificar fitxers de configuració

El fet de canviar el domini implica canviar tots els enllaços del portal i del *Moodle*, aquests es troben a la base de dades. Del servei de *hosting* s'han importat copies de les bases de dades (que estan en format text) i a partir d'aquest fitxers i amb l'editor *sed* es modifiquen totes les cadenes de text:

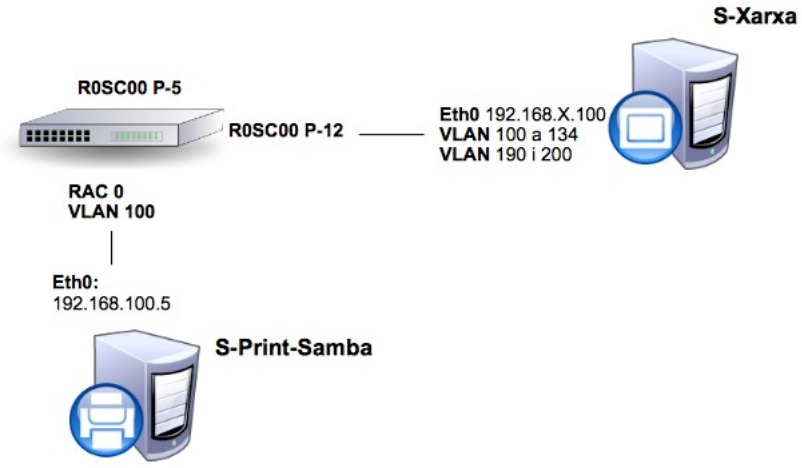
- sed -i 's@http://ieskta.cat/moodle@https://moodle.inskta.cat@g'
- sed -i 's@http://ieskta.cat@http://inskta.cat@g'

Les bases de dades les importem amb les comandes:

- mysql --password=XXX --user=root moodle2 < bdmoodle2.bak.sql

5- Servidor d'impressió i fitxers

La funcionalitat d'aquest servidor és gestionar les impressions i proporcionar un servei de fitxers. Les aplicacions que els ofereixen són **CUPS** i **Samba**. El servei d'impressió també utilitza Samba per poder tenir clients Windows, i aquest és un argument més pel qual s'integren els dos serveis en una mateixa màquina.



La connexió a la xarxa es fa per la VLAN100 que conté els servidors de la LAN i és accessible per tots els clients via S-Xarxa.

5-1 Configuració

El sistema operatiu del servidor és Debian Squeeze i se li afegeixen els paquets de:

- Cups
- Samba

Amb aquestes aplicacions podem compartir fitxers, gestionar impressores i fins i tot compartir impressores per mitjà de Samba. Però el que no es pot aconseguir és portar un control de les impressions que fa cadascun dels usuaris.

Cups disposa de gestió d'usuaris i permisos, amb lo qual es pot determinar qui imprimeix i qui no, però en la majoria de casos no és capaç de comptar les pàgines impreses. Sobretot si aquest comptatge no és per *hardware*, que és quan la pròpia impressora que retorna el nombre de pàgines impreses.

5-1-1 Servidor de fitxers

La configuració del servei de fitxers és molt simple. Després d'instal·lar el paquet de samba i dependències només cal seguir aquests 4 passos:

- Editar el fitxer de configuració *smb.conf*
- Donar d'alta al sistema els usuaris
- Afegir aquest usuari al servei Samba
- Crear la carpeta compartida en el servidor

El següent procés de configuració és per a l'usuari *secretaria*, que disposa del recurs compartit *secretaria*. El procés s'ha de repetir per cada recurs compartit.

1. Al fitxer de configuració *smb.conf* hi afegim la secció de secretaria

```
#
# Configuració del recurs compartit secretaria
#
[secretaria]
path=/home/samba/secretaria
browseable=yes
comment=share
writable=yes
public=yes
guest ok = no
```

2. Donem d'alta al sistema l'usuari secretaria, no cal que disposi de carpeta /home
    - adduser --no-create-home secretaria
3. Fem que aquest usuari del sistema passi a ser usuari samba
    - smbpasswd -a secretaria
4. Creem la carpeta compartida i li donem els permisos per l'usuari *secretaria*

5-1-2 Servidor d'impressió

Aquest servei és més complex, ja que el sistema no només gestiona les impressions si no que també registra el nombre de pàgines impreses per cada usuari. Això s'aconsegueix encadenant el procés de ***Cups*** amb ***Pykota***, que és un projecte de control d'impressions escrit en *python*. Els dos processos s'encadenen per mitjà de *sockets*.

Per a la instal·lació del servei es segueix el següent procés:

- Instal·lació de Cups
- Edició dels fitxers de configuració
- Instal·lació de la base de dades postgresql
- Instal·lació de paquets de python
- Instal·lació del paquet pkpgcounter
- Instal·lació de l'aplicació Pykota
- Configuració d'usuaris i impresores

La configuració de Cups és molt simple, utilitza el sistema d'autenticació *Basic* i no fixa restriccions ni força l'autenticació d'usuaris. Aquest procés es reserva per Pykota.

El paràmetres principals del fitxer *cupsd.conf* són:

```
# Default authentication type, when authentication is required...
DefaultAuthType Basic

# Restrict access to the server...
<Location />
  Order allow,deny
Allow from all
</Location>

<Location /printers/Ricoh>
   Order allow,deny
   Allow from all
</Location>

<Location /printers/RicohWindows>
   Order allow,deny
   Allow from all
</Location>
```

En aquests paràmetres es configura una autenticació ***Basic***, és a dir, que només hi accediran usuaris del sistema per configurar el servei i les impressores seran accessibles per tothom. Les impressores *Ricoh* i *RicohWindows* són realment la mateixa impressora amb dues cues d'impressió diferents, ja que els usuaris que hi accedeixin des d'ordinadors amb S.O. Windows només ho poden fer com a recurs compartit de Samba.

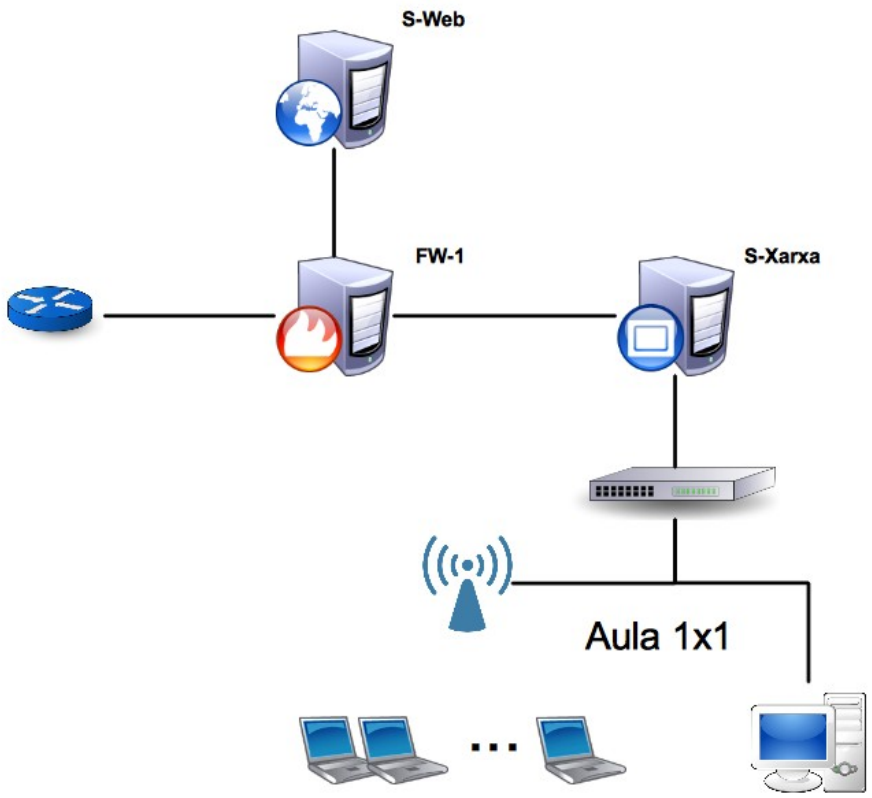
Per a la instal·lació del Pykota es segueix el procés:

- Descarregar-se el paquet pykota-1.26_fixes_official.tar.gz del projecte http://pykota.com
- Descomprimir i executar el *setup.py*
- Crear una base de dades a *postgresql* a partir de la seva plantilla *pykota-postgresql.sql*
- Copiar el *cupspykota* al *backend* del cups per tal que aquest el pugui utilitzar
- Crear l'usuari del sistema pykota per poder gestionar l'aplicació
- Copiar i modificar els fitxers de configuració i administració *pykota.conf* i *pykotadmin.conf*

A partir d'aquest punt ja es poden crear usuaris i impressores amb les funcions de *pykota* per crear les seves pròpies cues d'impressió.

6- Configuració d'aules 1x1

Les aules 1x1 disposen d'un ordinador del professor i un punt d'accés on es connecten els portàtils dels alumnes.



Cada aula pertany a una VLAN pròpia que li permet aplicar una política d'accés a *internet* independent de la resta d'aules.

La navegació per *internet* està configurada de la següent forma:

- L'ordinador del professor té accés lliure pel port 80
- Els portàtils dels alumnes només tenen accés a les URL's validades pel port 80
- Tant alumnes com el professor només naveguen pel port 443 a les URL validades
- La resta de ports estan restringits per tothom
- A voluntat del professor es pot commutar l'accés restringit dels ordinadors per una navegació lliure pel port 80

6-1 Mecanisme de commutació

El mecanisme es basa en la redirecció, que es fa a **S-Xarxa**, de les peticions del port 80 a un *squid* que treballa amb llista blanca, només té permeses algunes pàgines, a un segon *squid* que treballa amb llista negra on tot està permès a excepció de les URL d'aquesta llista negra.

Per poder canviar el tipus d'accés dels alumnes a *internet* a l'escriptori de l'ordinador del professor es disposa d'un enllaç a l'aplicació de commutació.

L'aplicació només fa la crida a un script que permet (**permetre.sh**) o un altre que restringeix

(**denegar.sh**) l'accés a *internet*. Aquesta aplicació està programada amb gambas i té la següent aparença:

En el cas de pitjar "Denegar Internet"

Si el que es pitja és "Permetre Internet" la imatge és la següent

Com que cada aula pertany a una VLAN diferent i *l'script* ha de ser el mateix per totes les aules, primer cal identificar a quina pertany. Les adreces de l'ordinador del professor són:

- 192.168.**106** a **125**.19

L'script de l'ordinador del professor busca quin és aquest 3r. octet i fa una crida al S-Xarxa per tal que executi un script que amb la dada d'aquest tercer octet dirigeix a *l'squid* adequat les peticions d'aquesta VLAN.

```
#!/bin/sh

rang=`ifconfig  | grep 'inet addr:'| grep -v '127.0.0.1' | cut -d: -f2 | awk '{ print $1}' | cut -d. -f3;`
ssh root@192.168.$rang.100 sh /home/super/deny.sh $rang
```

La variable "rang" agafa el valor del tercer octet de l'adreça IP i li passa a *l'script deny.sh* del S-Xarxa. Si es vol permetre, *l'script* és pràcticament igual i només canvia la crida que es fa a *l'script* del S-Xarxa, canvia deny.sh per allow.sh.

6-2 Servidor de xarxa

Aquest servidor també té dos scripts (allow.sh i deny.sh) que són pràcticament iguals, la única diferència és la redirecció de peticions, al port 3128 o al 3228.

```
#!/bin/bash

iptables -t nat -L > tempotables
awk -v OFS=" " '$1=$1' tempotables > tempotables2
linia=0;
contingut=`grep "192.168.$1.0/24" tempotables2`
while read line
        do
                if [ "$line" != "$contingut" ]
                        then
                                linia=$(($linia+1))
                        else
                                linia=$(($linia+1))
                                break
                fi
        done < tempotables2
linia=$(($linia-2))
iptables -t nat -R PREROUTING $linia -s 192.168.$1.0/24 ! -d 200.10.10.2 -p tcp --dport 80 -j
REDIRECT --to-port 3228
rm tempotables && rm tempotables2
```

A la taula nat *d'iptables*, dirigim les peticions de cadascuna de les *VLAN's* del centre a un o l'altre *squid*. L'objectiu dels scripts simplement és de fer un canvi (funció *replace* d'*iptables*) d'aquesta redirecció per canviar la política d'accés a *internet* d'una determinada aula.

La forma de treball és la següent:

- Llista la taula nat al fitxer *tempotables.*
- Canvia les tabulacions del fitxer *tempotables* per espais al fitxer *tempotables2.*
- Busquem la línia que s'haurà de modificar de la taula nat, la variable que li passem identifica la VLAN (3r. octet de l'adreça IP). Aquest línia la carreguem a la variable *contingut*.
- Recorrem tot el fitxer tempotables2 per localitzar la línia en qüestió.
- Corregim el desplaçament de dues línies
- Modifiquem la línia amb el paràmetre -R (*replace*) d'iptables, en funció de si es vol restringir o permetre l'accés aquest port serà el 3128 o el 3228

7 Còpies de seguretat

En el sistema es genera informació que és de vital importància pel funcionament del centre com són:

- Documents de direcció i secretaria
- Portal del centre que es va actualitzant amb noves notícies
- Cursos de *Moodle* amb l'activitat educativa del centre

Les còpies de seguretat es gestionen amb scripts que s'executen automàticament amb el cron.

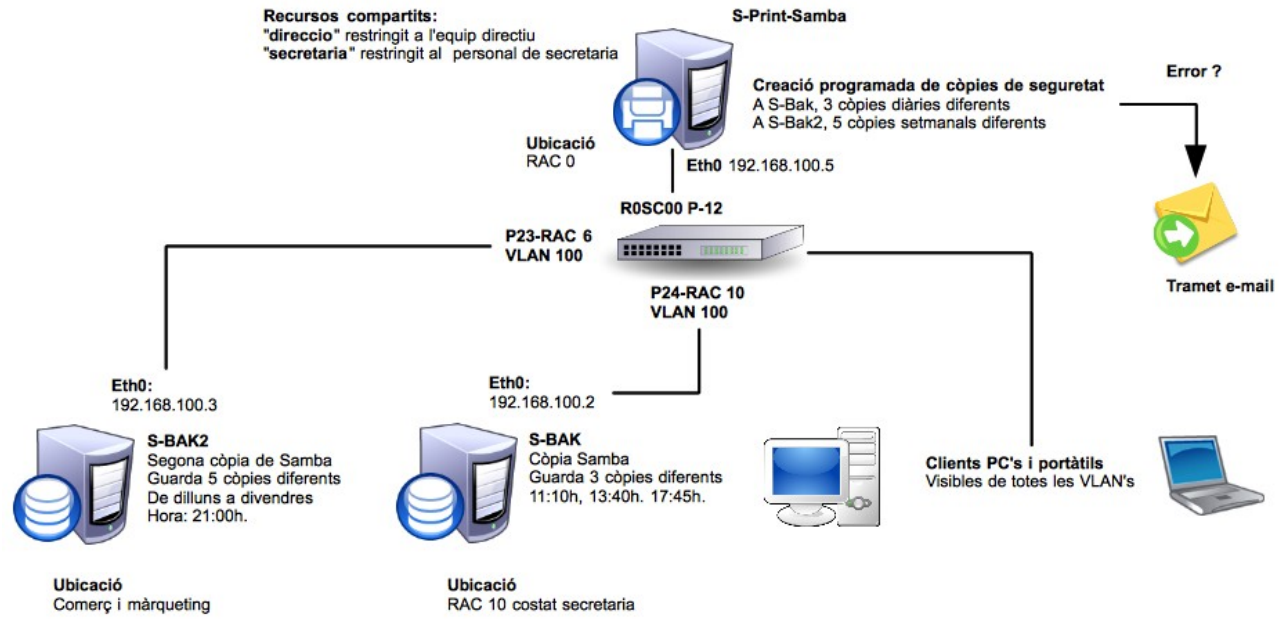
La còpia de seguretat dels fitxers és molt simple i es basa amb la comanda *rsync*, el cas del portal i del *Moodle* és una mica més complicada ja que apart d'utilitzar un sistema de fitxers també disposa de base de dades.

7-1 Còpia de seguretat del servidor de fitxers

La còpia de seguretat es fa en dos servidors diferents ubicats en llocs diferents. En el primer servidor de còpies de seguretat S-Bak es guarden 3 còpies diferents que es fan a mig matí, al migdia i al final de la tarda. L'objectiu d'aquestes còpies és disposar de tres entorns que a més de ser còpies de seguretat permetin recuperar dades que es puguin haver esborrat de forma involuntària.

En el segon servidor de seguretat es guarden 5 còpies diferents corresponents als cinc dies laborables. La redundància de còpies també té per finalitat recuperar dades que s'hagin pogut esborrar de forma involuntària.

El mecanisme de còpies de seguretat incorpora un element de protecció, la detecció d'errors en el propi procés de còpia de seguretat. Si falla el servidor de fitxers tothom se n'adona, ja que l'utilitzen constantment, però no passa el mateix amb el servei de còpies de seguretat. Si caiguessin els servidors de còpies o hi hagués qualsevol fallada o tall a la xarxa seria molt difícil que algú se n'adonés. El sistema disposa de mecanisme de detecció d'errors i en cas de produir-se s'envia un e-mail als responsables del sistema.



Al servidor de fitxers es disposa de quatre scripts per fer les còpies de seguretat. Tots són pràcticament iguals, la raó de tenir-ne quatre de diferents és per simplificar-los, ja que fan còpies a destins diferents i hores diferents, que es poden organitzar molt fàcilment amb el *crontab*. Aquests són:

- copia_samba_mati.sh
- copia_samba_migdia.sh
- copia_samba_tarda.sh
- copia_samba_setmanal.sh

Els tres primers són molt semblants.

```
#!/bin/bash

#
# Script copia seguretat samba mati
#
rm /var/log/samba.log && touch /var/log/samba.log
rsync -a --delete /home/samba/ -e ssh root@192.168.100.2:/samba/mati 2> /var/log/samba.log

if test -s /var/log/samba.log; then
        cat /var/log/samba.log | mutt -s "Error al fer la copia de SAMBA" admin2@inskta.cat
admin1@inskta.cat
else
        echo "No hi han hagut errors" >> /var/log/samba.log
fi
```

Aquest és el de matí i el seu funcionament és el següent:

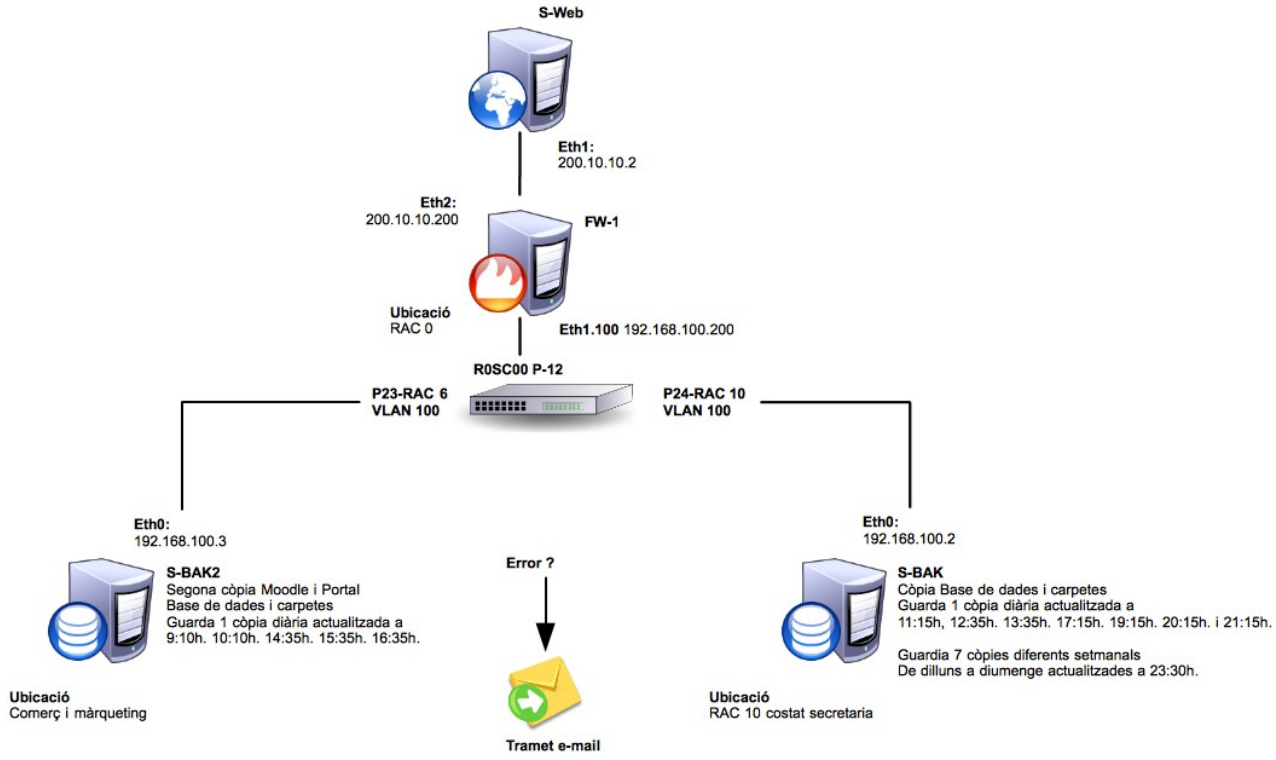
- Borra i regenera un fals registre de *logs*
- Amb la comanda *rsync* i el protocol *ssh* s'actualitza la carpeta remota on es guarden les còpies de seguretat. Si es genera algun error en l'execució de la comanda *rsync*, aquest es dirigeix a fitxer de *logs*
- Es comprova que el fitxer de *logs* estigui buit, cas contrari s'ha produït un error que mutt el tramet als responsables del sistema. Les adreces que hi figuren són fictícies.

L'*script* de còpia setmanal és idèntic en quan a mètode de fer la còpia i detecció d'error només diferencia que té una línia per cada dia de la setmana i el mecanisme d'identificar-lo és per la variable DIA que es carrega amb un nombre que correspon al dia de la setmana. Amb condicionals executem la comanda *rsync* al destí pertinent.

```
DIA=$(date +%u)

#Dilluns posem la còpia a la carpeta de dilluns
if [ "$DIA" = "1" ]; then
rsync -a --delete /home/samba/ -e ssh root@192.168.100.3:/dades/samba_setmana/dilluns 2>
/var/log/samba.log
fi

#Dimarts posem la còpia a la carpeta de dimarts
if [ "$DIA" = "2" ]; then
rsync -a --delete /home/samba/ -e ssh root@192.168.100.3:/dades/samba_setmana/dimarts 2>
/var/log/samba.log
fi
```

7-2 Còpia de seguretat del servidor Web

Aquestes còpies es realitzen als mateixos servidors de còpies de seguretat que el servei de fitxers. Es tracta de servidors ubicats a la pròpia LAN. Per tant el tallafocs ha de permetre aquesta comunicació però en canvi s'ha d'evitar que es pugui accedir a qualsevol màquina de la LAN. Si s'entra a una màquina o servidor d'aquesta LAN es podria accedir a la resta amb molta facilitat.



La solució passa per canviar el mètode de treball del procés de còpies de seguretat. No es pot enviar els fitxers via *rsync* del servidor Web al servidor de còpies de seguretat. Si obrim aquesta via també quedarà oberta per possibles intrusions. El procés s'ha de fer a la inversa, el servidor de còpies de seguretat fa la crida al servidor Web per sincronitzar les carpetes de fitxers, o les bases de dades.

D'aquesta forma el tallafocs pot bloquejar la comunicació del Servidor Web a la LAN però permetre les comunicacions dels servidors de copies de seguretat al servidor Web. Només cal executar les comandes *rsync* en mode invers.

El procés s'executa en dos llocs.

- Al servidor Web s'han de fer còpies de les dues bases de dades
- Als servidors de còpies de seguretat es faran sincronitzacions de carpetes i bases de dades amb el servidor Web.

L'script de còpies de seguretat del servidor és el següent:

```
#!/bin/bash

#
# Script per a la còpia de seguretat del Moodle
#
rm /var/log/backup_moodle.log && touch /var/log/backup_moodle.log
#
# Bolcat de les bases de dades
#
# Bolcat de la base de dades del Moodle al fitxer /root/bdmoodle2.bak.sql
mysqldump --opt --password=ubuntu99 --user=root moodle2 > /root/bdmoodle2.bak.sql 2>>
/var/log/backup_moodle.log
# Bolcat de la base de dades del portal Joomla al fitxer /root/j15.bak.sql
mysqldump --opt --password=ubuntu99 --user=root j15 > /root/j15.bak.sql 2>>
/var/log/backup_moodle.log
```

L'*script* simplement fa un bolcat de les bases de dades a dos fitxers *sql*. Com que en aquest procés també es pot produir error, s'utilitza el mateix mètode per detectar-lo, la possible sortida d'error es redirigeix a un falç fitxer de *logs*, que posteriorment en verificarà i si és necessari tramet *e-mail* als responsables del sistema.

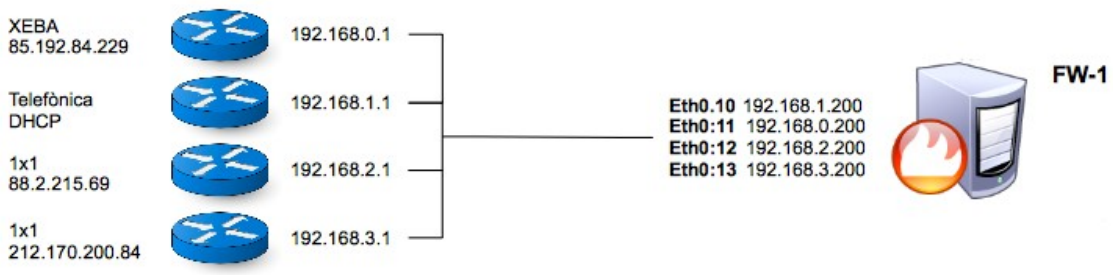
```
#Copia les bases de dades del S-Web
rsync -a --delete /-e sss root@inskta.cat:/root/bdmoodle2.bak.sql /dades/bd 2>>
/var/log/backup_moodle.log
rsync -a --delete -e ssh root@inskta.cat:/root/j15.bak.sql /dades/bd 2>> /var/log/backup_moodle.log
#
# Copia de seguretat de les carpetes i fitxers
#
# Moodle
rsync -a --delete -e ssh root@inskta.cat:/var/www/moodle/ /dades/moodle 2>>
/var/log/backup_moodle.log
rsync -a --delete -s ssh root@inskta.cat:/var/moodledata/ /dades/moodledata 2>>
/var/log/backup_moodle.log

#
# Copia de seguretat de les carpetes i fitxers
#
# Portal
rsync -a --delete -e ssh root@inskta.cat:/var/www/portal/ /dades/portal 2>>
/var/log/backup_moodle.log
```

7-3 Autorització de connexions

La copia de fitxers entre servidors es fa pel protocol *ssh*, que requereix de *contrassenya*. en processos automatitzats el requeriment de *contrassenya* és inviable. Per evitar que a cada connexió es demani la *contrassenya* amb *ssh-keygen* generem les calaus públiques i privades per aconseguir el reconeixement entre servidors sense la sol·licitud d'aquesta *contrassenya*.

8 Verificació i mesura del balanceig de càrrega

L'esquema inicial amb les IP públiques teòriques dels nostres routers són:



Les mesures per avaluar i verificar el funcionament del balanceig de càrrega s'orienten, primer a comprovar el correcte funcionament dels *routers*, després a comprovar el repartiment de paquets pels diferents *routers* i finalment a estudiar el transit que suporta per avaluar possibles ampliacions, o una possible reducció del nombre de *routers* si el volum de trànsit fos reduït.

8.1 Verificació del funcionament dels routers

Des de FW-1 que fa de tallafocs i balanceig de càrrega, executem la comanda

- ping -I eth0.10 google.com

o

- ping -I 192.168.1.200 google.com

Per cadascun dels routers.

```
aanguera — super@S-Xarxa: ~ — ssh — 96×54
root@S-Fw1:~# ping -c2 -I eth0.10 google.com
PING google.com (74.125.230.225) from 192.168.1.200 eth0.10: 56(84) bytes of data.
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=1 ttl=55 time=239 ms
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=2 ttl=55 time=69.3 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 69.357/154.629/239.902/85.273 ms
root@S-Fw1:~# ping -c2 -I eth0.11 google.com
PING google.com (74.125.230.225) from 192.168.0.200 eth0.11: 56(84) bytes of data.
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=1 ttl=45 time=91.8 ms
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=2 ttl=45 time=85.0 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 85.043/88.436/91.830/3.406 ms
root@S-Fw1:~# ping -c2 -I eth0.12 google.com
PING google.com (74.125.230.225) from 192.168.2.200 eth0.12: 56(84) bytes of data.
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=1 ttl=51 time=73.2 ms
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=2 ttl=51 time=72.4 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 72.422/72.834/73.247/0.492 ms
root@S-Fw1:~# ping -c2 -I eth0.13 google.com
PING google.com (74.125.230.225) from 192.168.3.200 eth0.13: 56(84) bytes of data.
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=1 ttl=55 time=59.9 ms
64 bytes from par08s10-in-f1.1e100.net (74.125.230.225): icmp_req=2 ttl=55 time=60.4 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 59.915/60.187/60.460/0.366 ms
root@S-Fw1:~#
```

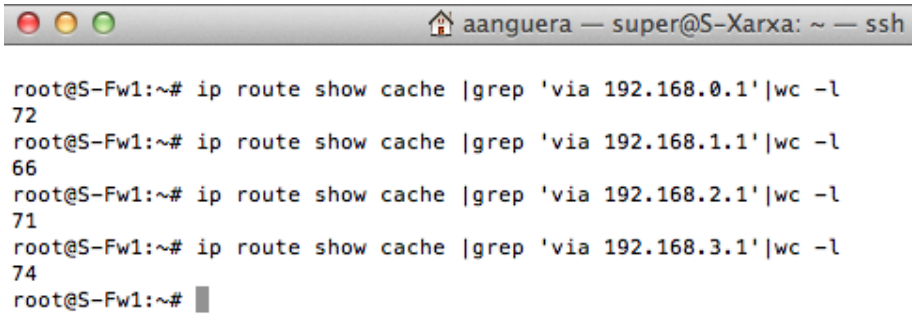
Des del tallafocs es pot verificar que tots els *routers* són operatiu.

8.2 Repartiment de paquets

Per verificar el repartiment de paquets pels diferents *routers* mirem la memòria *cache* de les taules associades a cadascun dels *routers*. Utilitzem la comanda:

- ip route show cache

Per facilitar la tasca de comprovació afegeixo a la instrucció un filtre (grep) per cadascun dels *routers* que tenim, i la comanda "wc" per comptar les línies associades a cada *router*. D'aquesta forma es pot comprovar la quantitat de paquets que s'envien a cadascun dels *routers*.



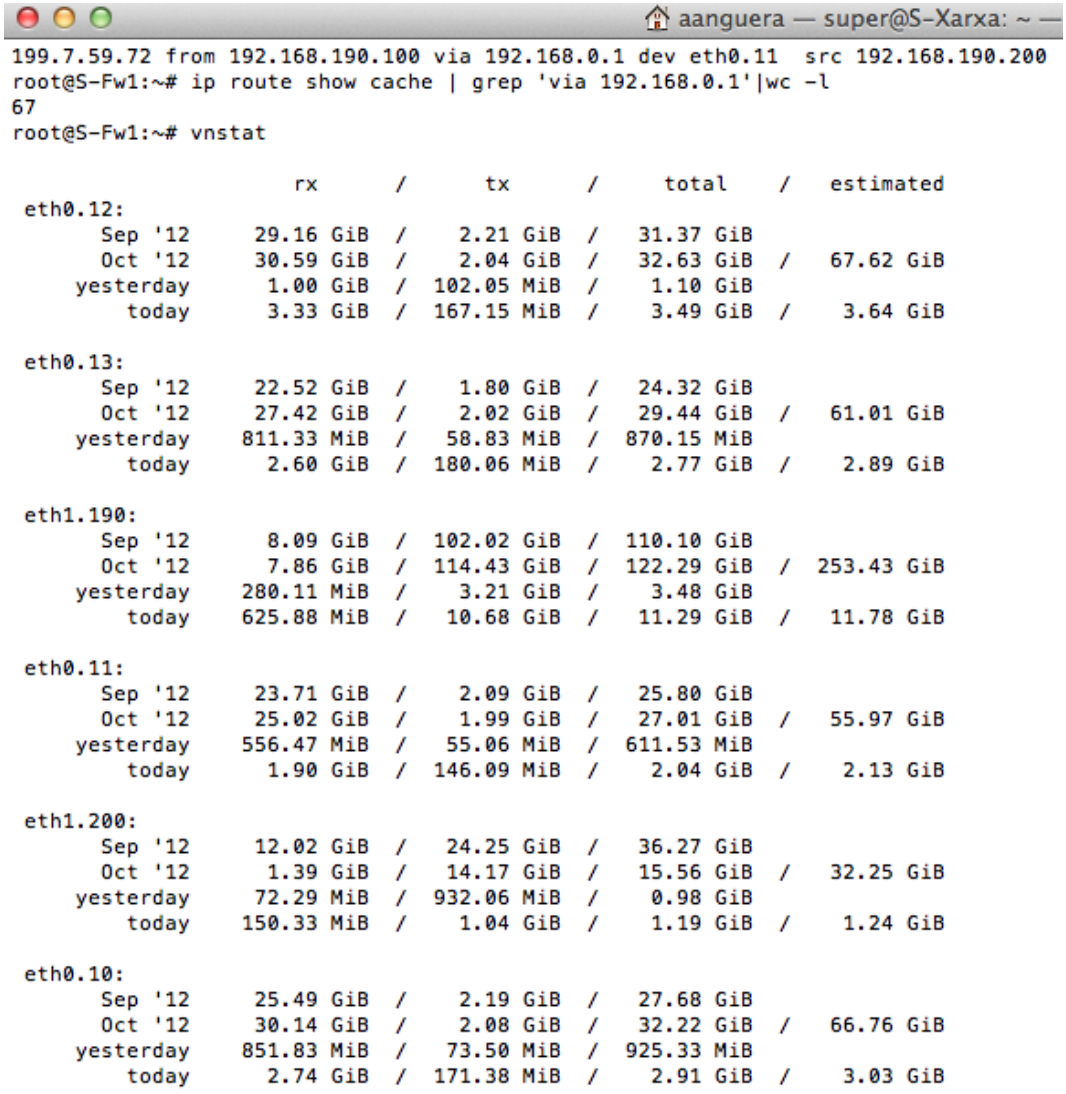
A la imatge es pot comprovar com el nombre de paquets que es reparteixen pels 4 *routers* és força equitatiu, per tant el seu funcionament és òptim.

8.3 Totals de consum d'internet

A banda del repartiment de paquets també podem verificar el transit per cadascun dels routers amb la comanda *iptraf*.

Una altra font d'informació important a tenir en compte és el total de consum en un període determinat. L'aplicació *vnstat* manté un registre i estadística del consums de xarxa consultable de terminal.

Aquest càlcul estadístic és possible gràcies a que cada *routers* disposa d'una VLAN amb dedicació exclusiva. Les interfícies de xarxa connectades als *routers* van de la eth0.10 a la eth0.13. Els consums acumulats a mig mes d´octubre són els de la figura.



Comparant el volum de descàrrega acumulat fins a mig octubre es pot constatar que varien entre els 25 i 30Gb, és a dir, que amb aquest registre també es constata que el treball és força uniforme per a cadascun dels 4 *routers*.

9 Verificació del tallafocs

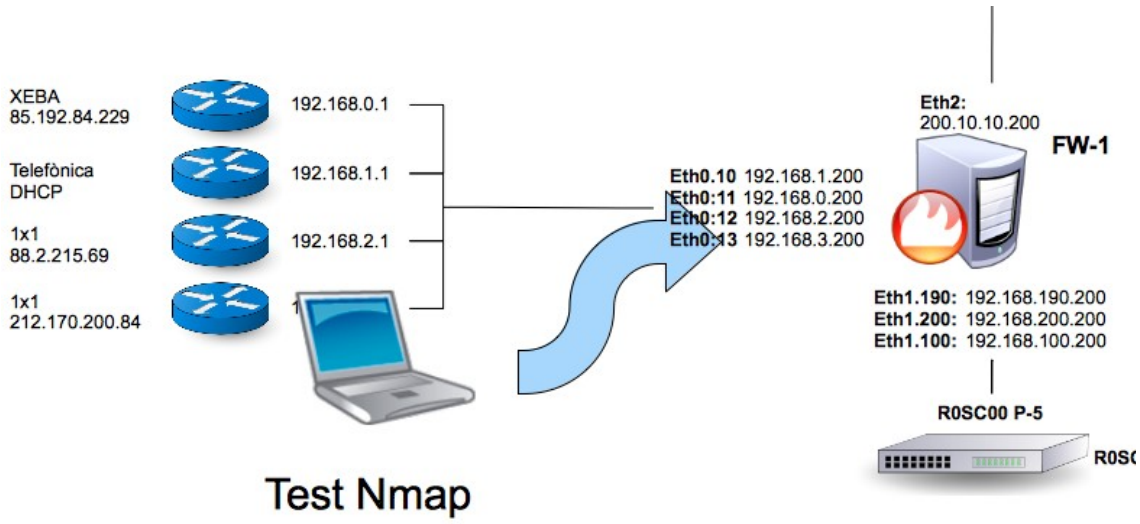
La mateixa màquina FW-1 que fa les funcions de balanceig de càrrega també realitza la funció de tallafocs. Les proves de resistència es fan amb l'aplicació *Nmap*.

De les 3 interfícies de xarxa del tallafocs, només Eth1 dóna accés a la LAN. La interfície Eth0 accedeix al banc de 4 *routers* que balancegen la càrrega de sortida a internet i Eth2 accedeix a la DMZ, on hi ha el servidor Web del propi centre.

Els atacs de prova es fan des de les dues línies que tenen accés internet, Eth0 i Eth2.

9.1 Atac des del banc de routers

En aquest primer cas es col·loca un portàtil amb l'aplicació *Nmap* a les diferents VLAN's associades a cadascun dels *routers*. Des del portàtil es fan atacs al propi tallafocs i als servidors que hi han al seu darrera.



Per aquesta prova es configura el portàtil amb una IP de la banda del router 192.168.1.1, per atacar al tallafocs i als equips del seu darrera

```
root@bt:~# ifconfig eth0 192.168.1.11
root@bt:~# route add default gw 192.168.1.200
root@bt:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=6.79 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.67 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.679/4.236/6.794/2.558 ms
root@bt:~# ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
^C
--- 192.168.1.200 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms
```

En aquestes proves es pot veure com el portàtil pot veure al *router*, però en canvi no veu al tallafoc

(192.168.190.200), aquest no respon ni als *pings*.

El pas següent és intentar atacar als equips que hi ha darrera del tallafocs, i el primer pas és comprovar-ne la seva existència.

Amb la comanda *nmap* s'intenta rastrejar tots els equips que hi pugui haver a la LAN 192.168.190.0, el resultat d'aquest rastreig és nul pel fet que el tallafocs només permet la comunicació de dins la LAN cap a l'exterior.

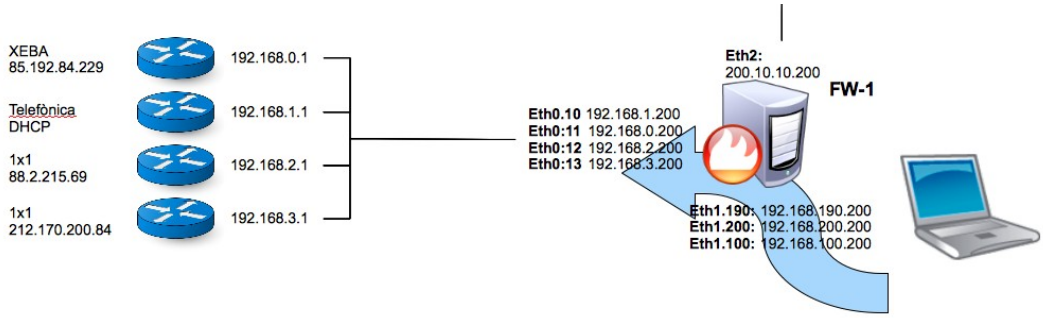
```
root@bt:~# nmap -sP -PA 192.168.190.0/24

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-10-22 10:32 CEST
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.23 seconds
root@bt:~# nmap -sP -PA 192.168.190.200

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-10-22 10:33 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.10 seconds
root@bt:~# nmap -sP -PA 192.168.190.100

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-10-22 10:34 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.12 seconds
root@bt:~#
```

Ara l'atac es dirigeix al propi tallafocs per verificar-ne els ports oberts i les seves possibles vulnerabilitats.

```
root@bt:~# nmap -v -A -p1-65535 192.168.1.200

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-10-22 10:43 CEST
NSE: Loaded 63 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 10:43
Scanning 192.168.1.200 [1 port]
Completed ARP Ping Scan at 10:43, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:43
Completed Parallel DNS resolution of 1 host. at 10:43, 13.00s elapsed
Initiating SYN Stealth Scan at 10:43
Scanning 192.168.1.200 [65535 ports]
SYN Stealth Scan Timing: About 2.23% done; ETC: 11:06 (0:22:40 remaining)
SYN Stealth Scan Timing: About 4.74% done; ETC: 11:05 (0:21:26 remaining)
SYN Stealth Scan Timing: About 93.72% done; ETC: 11:06 (0:01:26 remaining)
Completed SYN Stealth Scan at 11:06, 1366.99s elapsed (65535 total ports)
Initiating Service scan at 11:06
Initiating OS detection (try #1) against 192.168.1.200
Retrying OS detection (try #2) against 192.168.1.200
NSE: Script scanning 192.168.1.200.
Initiating NSE at 11:06
Completed NSE at 11:06, 10.00s elapsed
Nmap scan report for 192.168.1.200
Host is up (0.00020s latency).
All 65535 scanned ports on 192.168.1.200 are filtered
MAC Address: 00:1E:0B:D5:66:D0 (Hewlett Packard)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.20 ms 192.168.1.200


NSE: Script Post-scanning.
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1394.29 seconds
        Raw packets sent: 131119 (5.772MB) | Rcvd: 1 (28B)
root@bt:~#
```

En el resultat es veu com tots els ports estan tancats i la vulnerabilitat del tallafocs des del costat dels *routers* és molt baixa.

Per assegurar-se que l'aplicació *nmap* sigui capaç de saltar-se un tallafocs, sempre i quan aquest ho permeti, es repeteix la prova, però aquesta vegada des de dins la LAN cap al banc de *routers*.



El resultat és el següent.

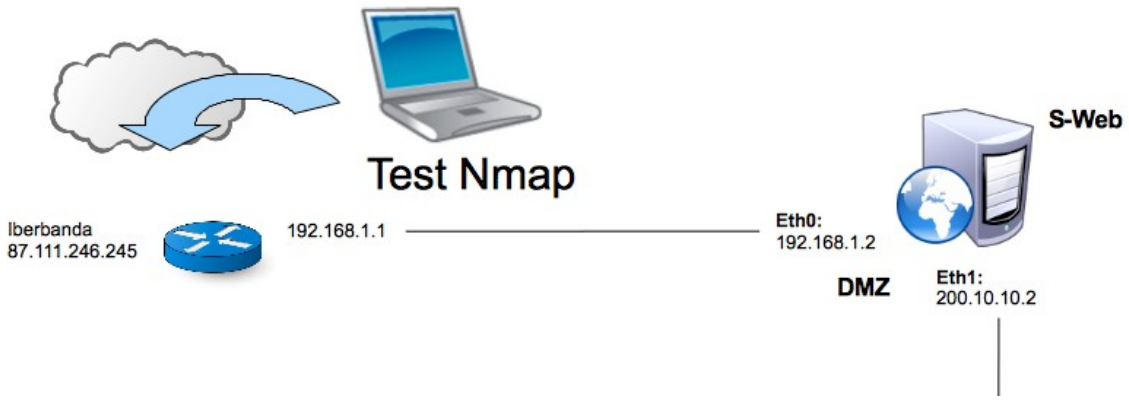
```
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:26:22:49:ba:a3
          inet addr:192.168.100.34  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::226:22ff:fe49:baa3/64 Scope:Link

root@bt:~# nmap -sP -PA 192.168.1.0/24

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-10-22 10:20 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0022s latency).
Nmap scan report for 192.168.1.200
Host is up (0.00028s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.06 seconds
```

Es pot comprovar que amb una IP (192.168.100.34) d'un marge diferent al que es rastreja, la comanda *nmap* detecta el propi tallafocs i el *router* que té al darrera.

Aquestes proves contrasten que efectivament el tallafocs realitza la seva funció de tallar la connexió de l'exterior a la LAN, però permet que de dins la LAN s'accedeixi a l'exterior.

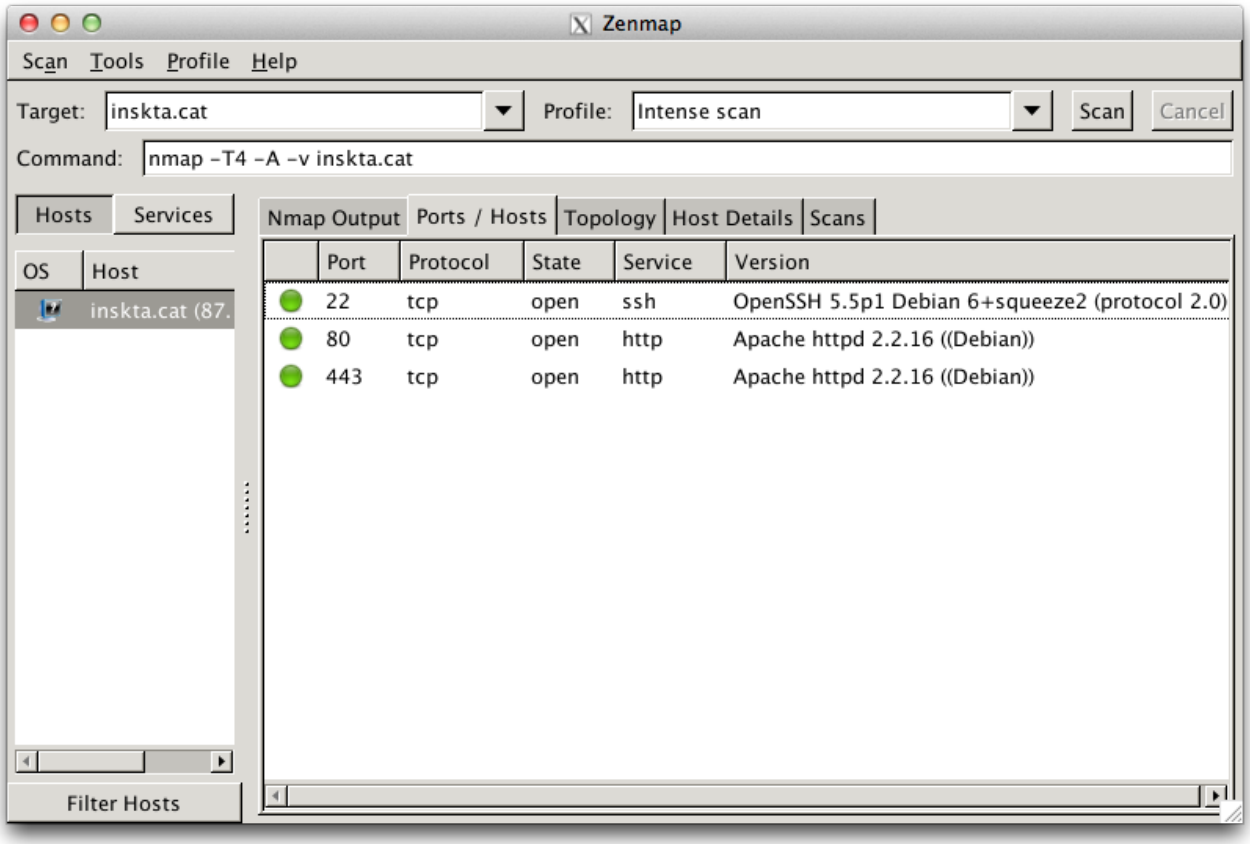
9.2 Atac des de la DMZ

En aquest cas es fan dos atacs, el primer des de l'exterior contra tot el servidor i el segon des de dins el propi servidor cap a la LAN.



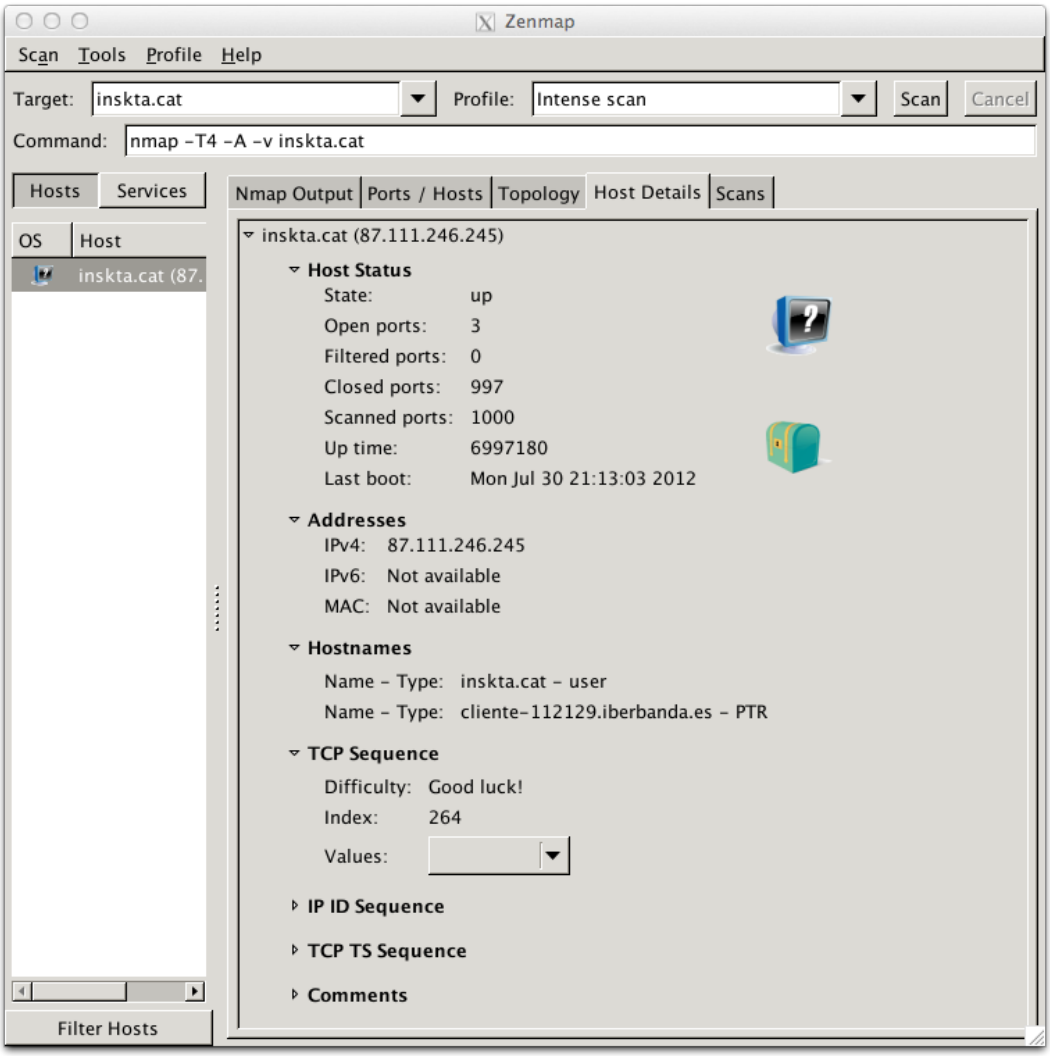
Aquest atac el llenço des de l'exterior, amb la versió *Zenmap* que disposa d'entorn gràfic, contra el domini amb la següent instrucció

- nmap -T4 -A -v inskta.cat

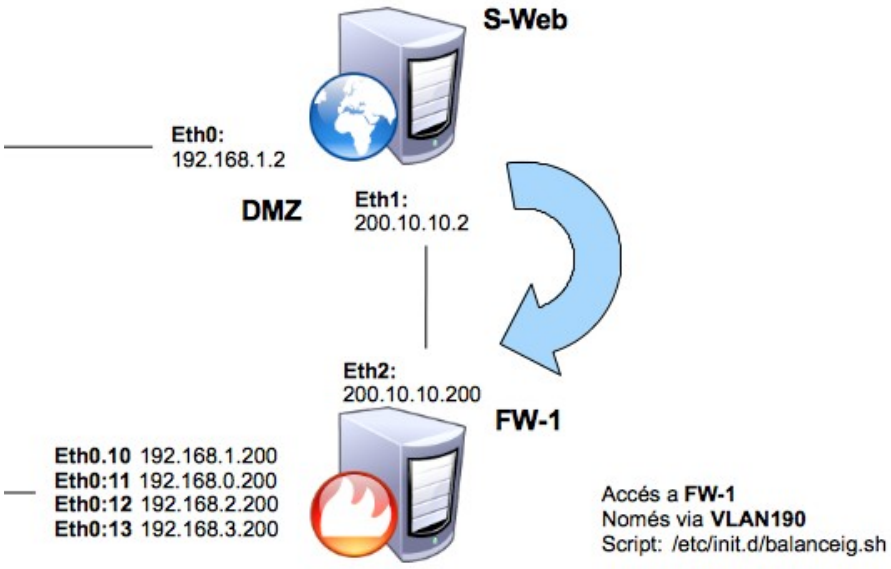


En el resultat es comprova que només hi ha aquests 3 ports oberts.

Si es miren els detalls del host, també es pot observar que disposa d'una bona protecció contra seqüències TCP.

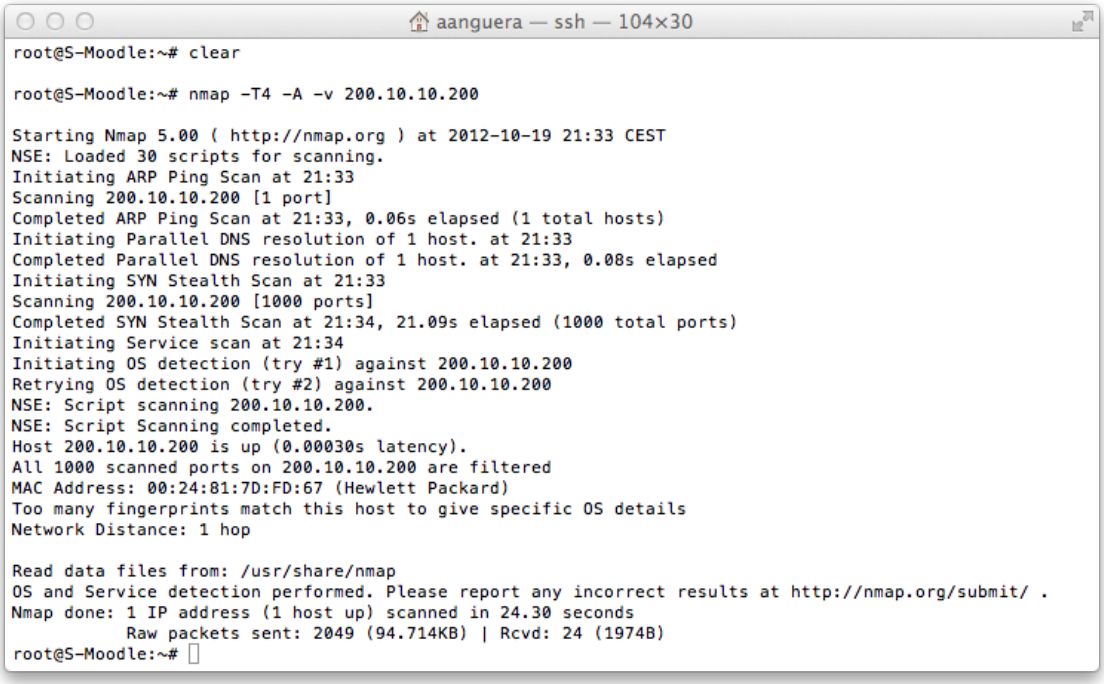


Situats al propi servidor llancem un atac contra el tallafocs per veure el seu comportament.



En aquest cas es pot veure que tots els ports estan filtrats, des del servidor Web de la DMZ no es pot accedir al tallafocs.

Aquest tallafocs està completament tancat des de l'exterior. Només s'hi pot accedir des de dins la LAN.

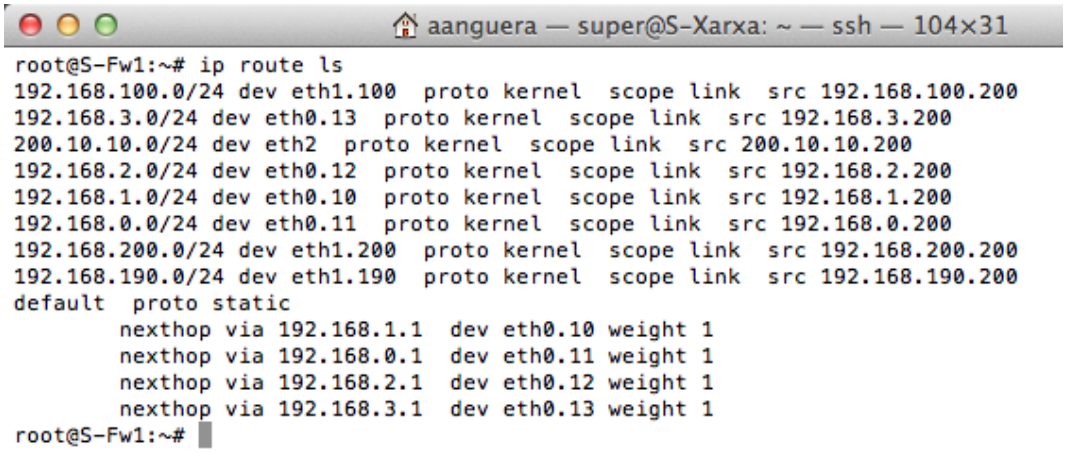


10 Tolerància a fallades de routers

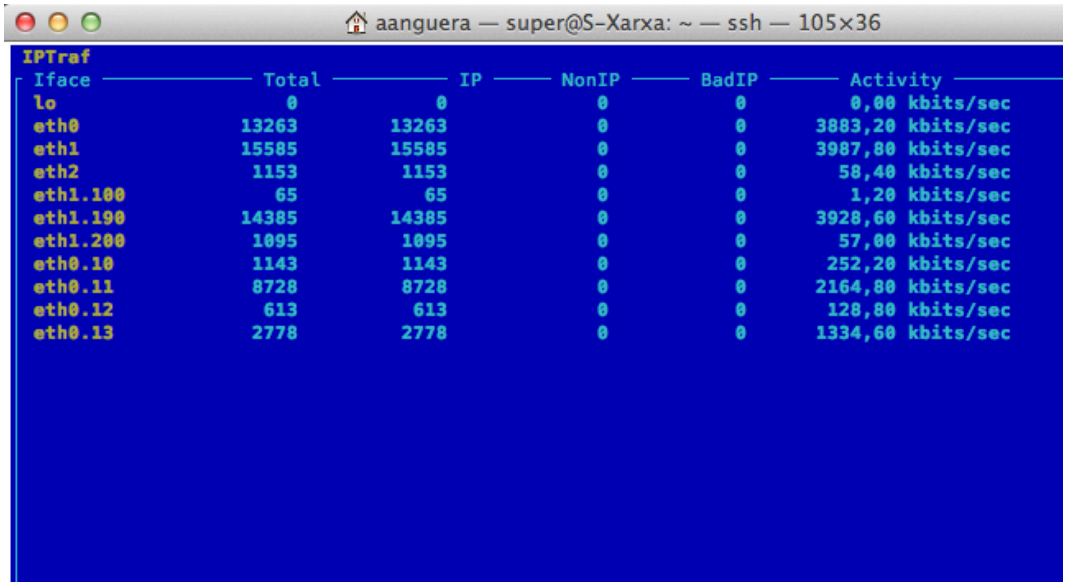
El sistema de balanceig de *routers* reparteix les peticions d'accés a internet pels diferents *routers* del balanceig de càrrega. Si un dels *routers* deixa de funcionar o perd la línia, totes les peticions que s'adrecin a aquest es perden. Per aquest motiu el sistema ha de ser capaç de modificar el sistema d'encaminament per saltar-se el *router* o els *routers* que no són operatius. De la mateixa matera també ha de permetre recuperar de la llista d'encaminament els *routers* que tornin a ser operatius.

10.1 Tots els routers operatius

Amb tots els routers operatius la taula d'encaminament és la següent,



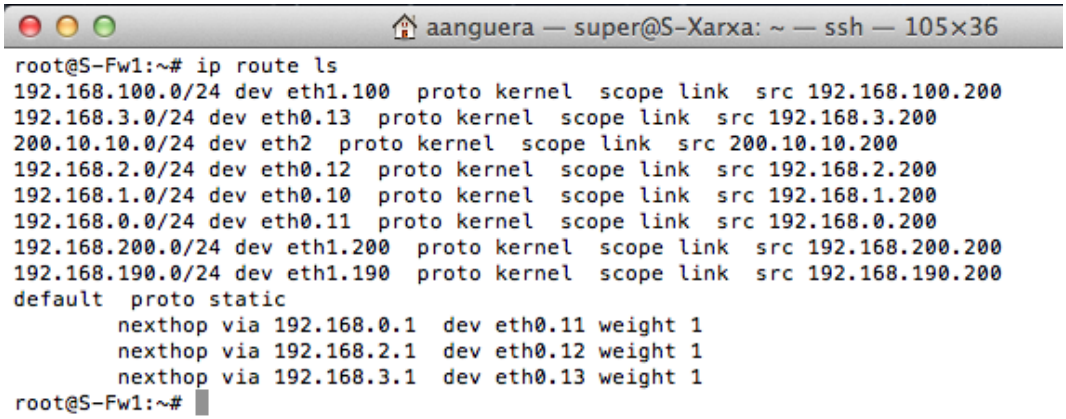
El transit per les VLAN's associades als *routers* és,



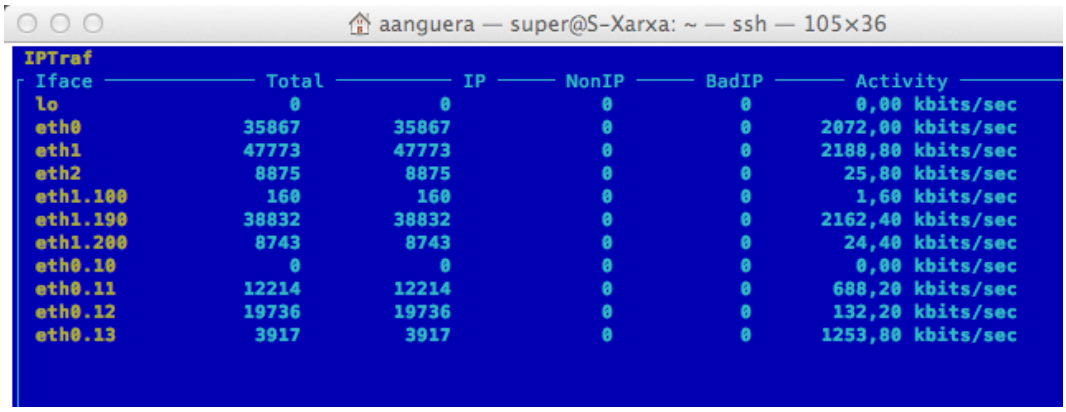
A les VLAN's de la eth0.10 a la eth0.13 s'observa que totes les línies associades als *routers* suporten tràsnit.

10.2 Falla un primer router

En aquest cas s'apaga un router per simular l'averia d'una línia.

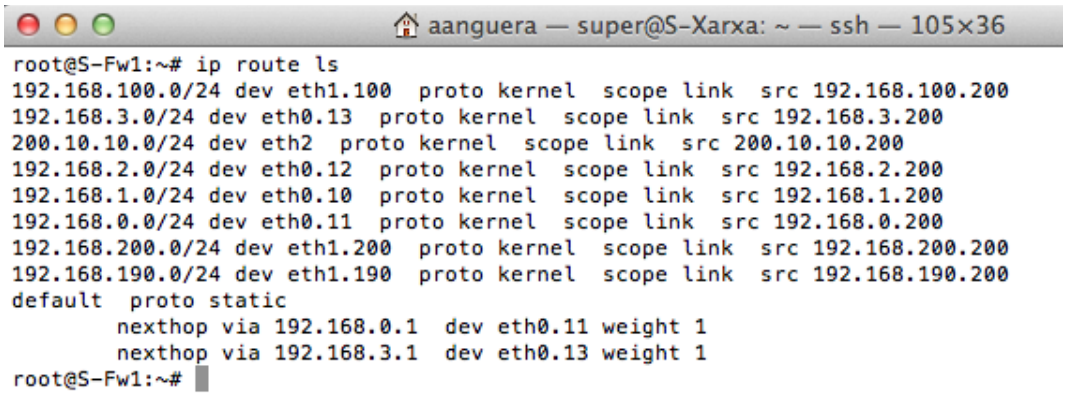


A la taula d'encaminament es pot comprovar que ja no hi ha el router 192.168.1.1, que és el que s'ha apagat. Evidentment el transit associat a la seva VLAN (eth0.10) és zero.

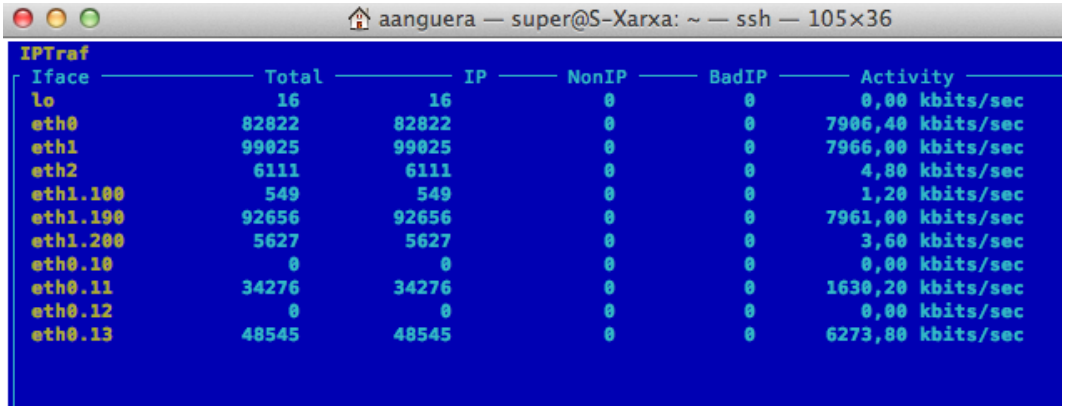


10.3 Falla un segon router

Al cap de poc temps d'apagar el segon router s'actualitza la taula d'encaminament amb els dos únics routers actius.

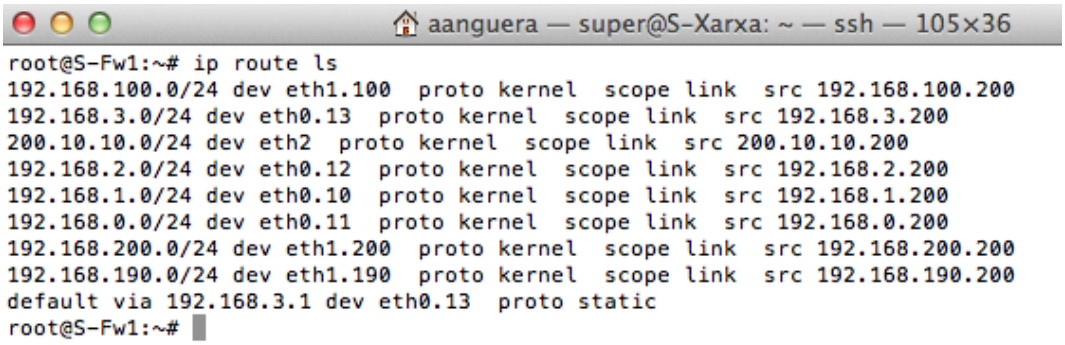


Pel què fa referència al transit, aquest es limita a les dues *VLAN's* associades a *routers* operatius. També es pot comprovar com el trànsit pels *routers* que queden actius augmenta, han de gestionar les peticions que abans es desviaven pels *routers* apagats.

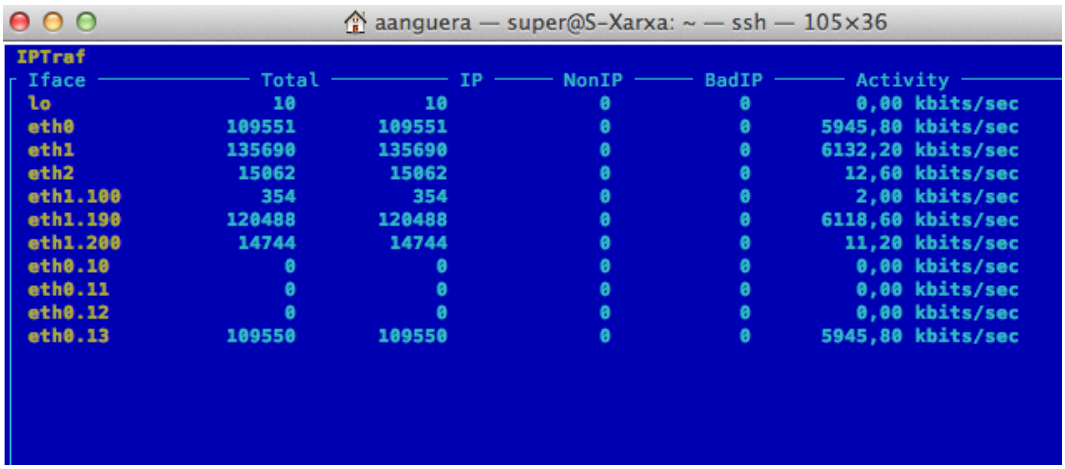


10.4 Falla un tercer router

En aquest cas ja només queda un *router* operatiu i no es poden fer els salts de *routers*, a la comanda de *ip route ls*, no apareix el salt sinó l'únic *router* actiu.



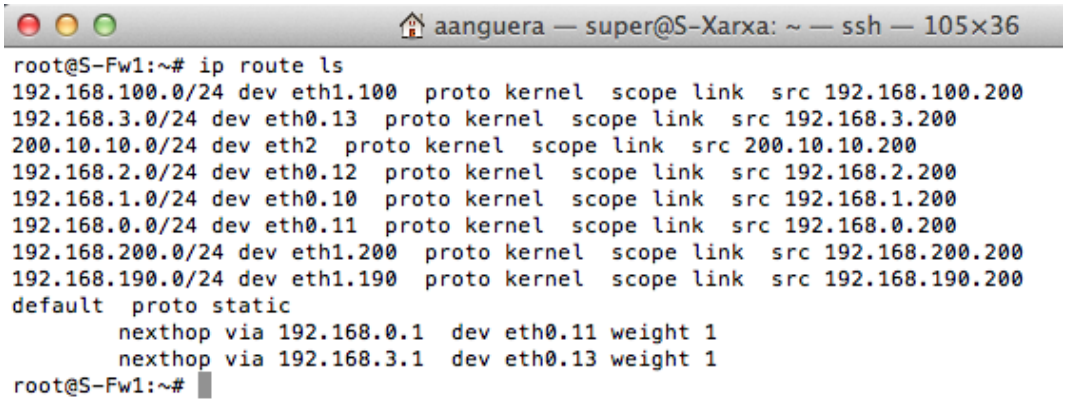
Tot el trànsit de sortida a internet només passa pel *router* 192.168.3.1, i la seva VLAN eth0.13 associada és la única que manté l'activitat. També es pot veure com el *router* pràcticament arriba al límit de la seva capacitat (aproximadament 8Mb/s) ja que ha de suportar el trànsit de tot el centre.

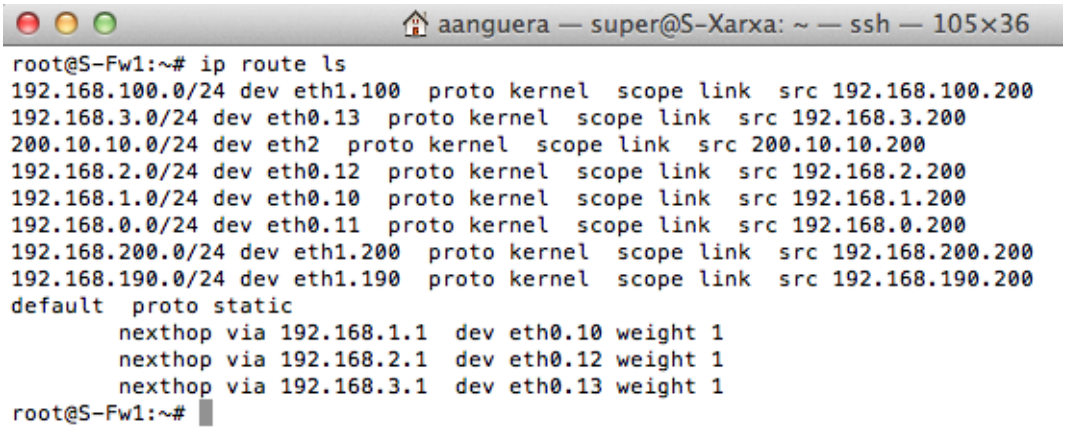


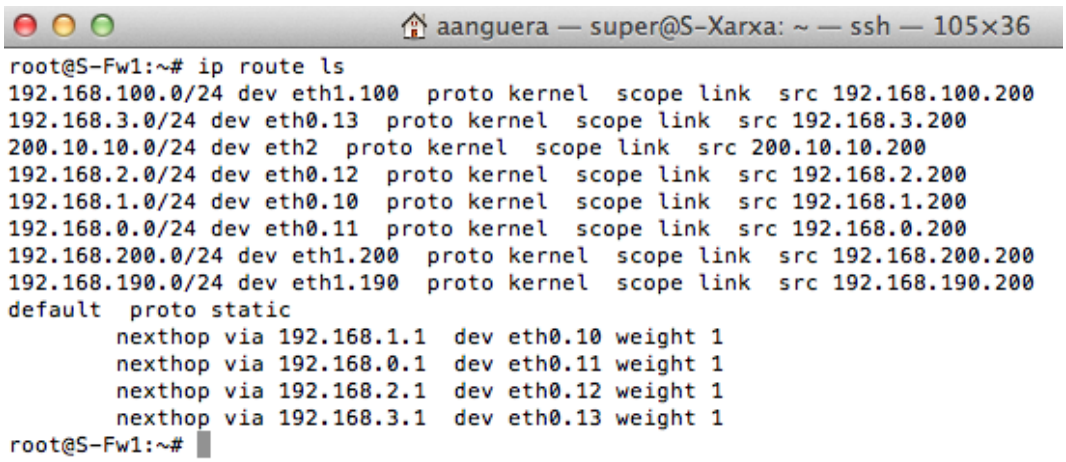
10.5 Recuperació de routers

En mateix procés que treu els routers caiguts de la taula d'encaminament també els hi afegeix en cas de recuperació. El procés seguit va ser anar-los engegant progressivament un a un, tot i que també suportaria l'arrencada simultània de tots ells.

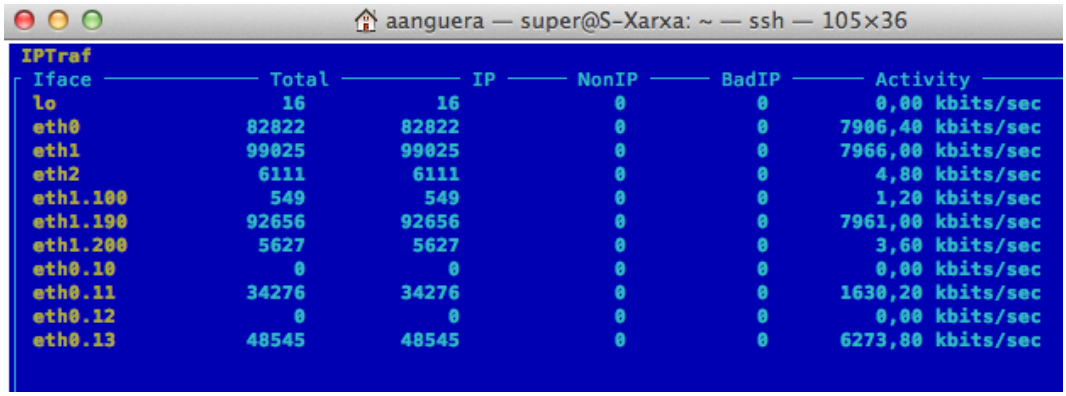
La imatge successiva de la recuperació dels routers a la taula d'encaminament és la següent:

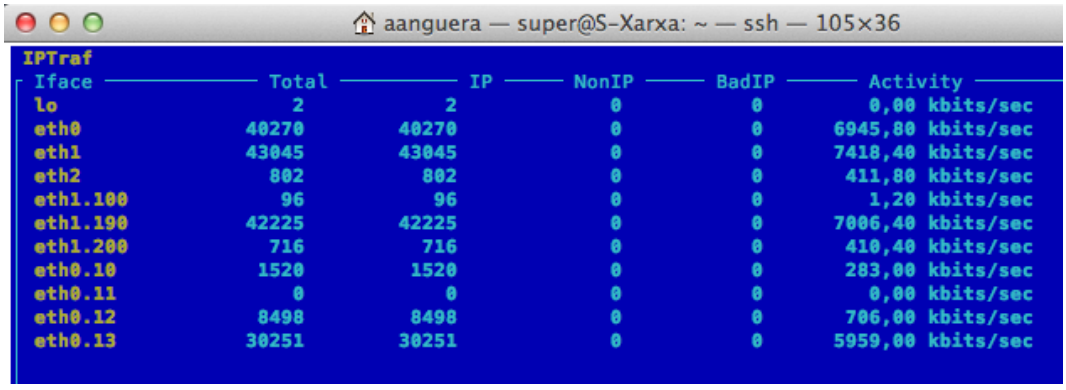


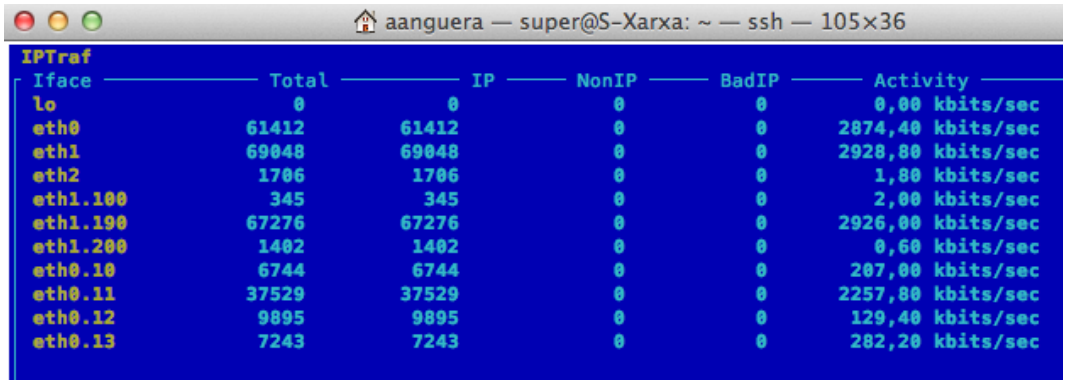




La progressiva recuperació del transit de les VLAN's associat a cadascun del routers és:





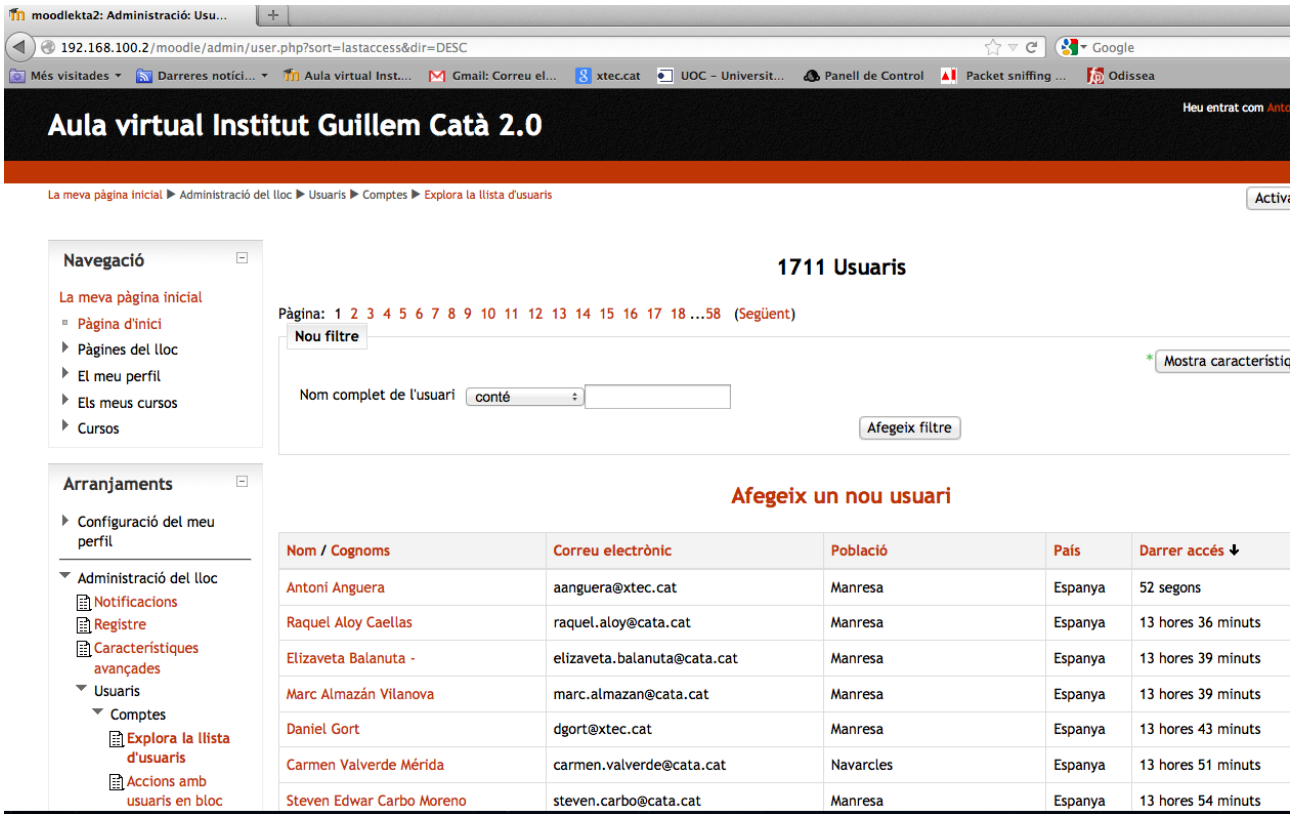


11 Còpia de seguretat del Moodle

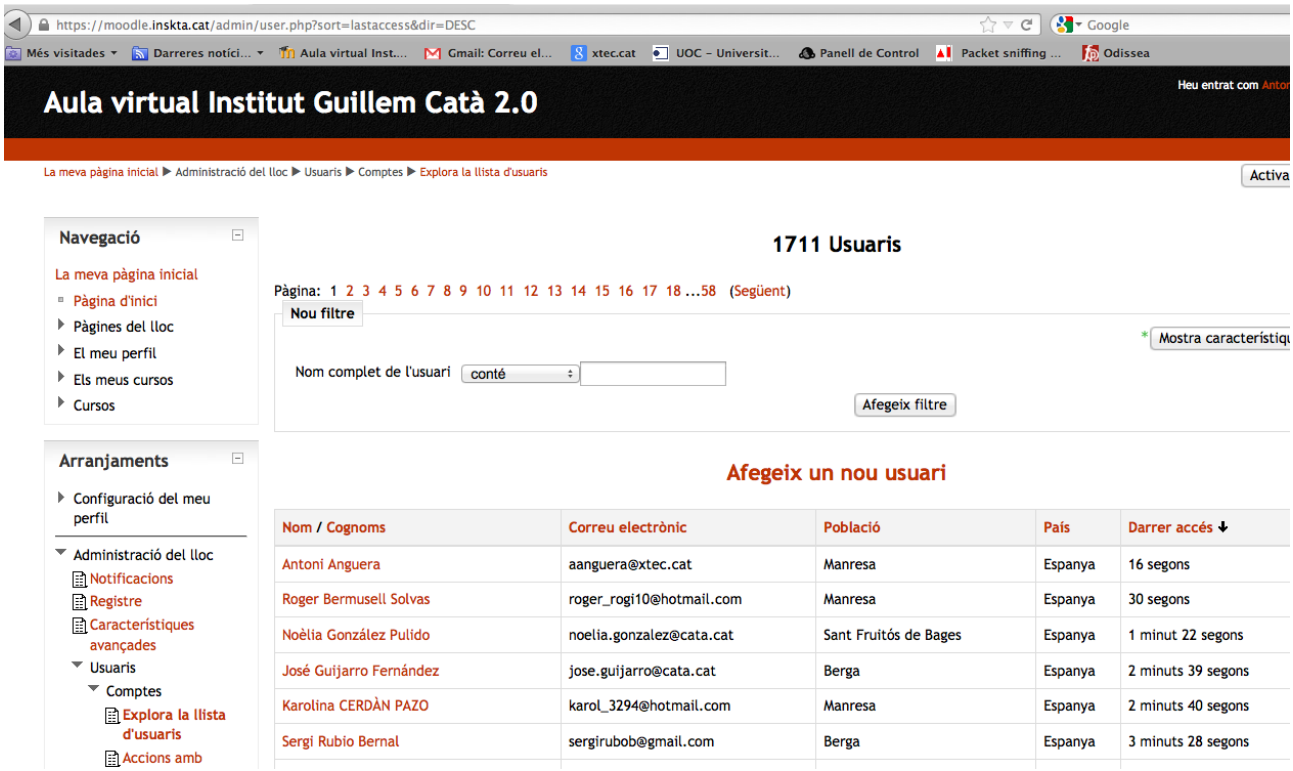
Aquest és un procés de vital importància pel centre. L'entorn virtual d'aprenentatge *Moodle* conté molta informació, des de material elaborat pel professorat fins a treballs d'alumnes que no es poden perdre.

En el primer servidor de còpies de seguretat, a part de guardar els fitxers i les bases de dades del Moodle es fa una restauració de l'entorn a partir de la copia de seguretat. A part de la generació de e-mails en cas de produir-se errors en el procés de còpia de seguretat, podem verificar manualment l'estat d'aquesta còpia.

En aquest cas s'accedeix a la còpia restaurada del Moodle al servidor de còpies de seguretat (192.168.100.2), podem verificar que fa unes 13h. que s'ha fet aquesta còpia ja que coincideix amb els darrers usuaris registrats, molt separat apareix el meu accés per comprovar el funcionament de la còpia.



Podem contrastar la còpia del *Moodle* amb la del servidor de producció. A la barra de navegació es comprova que accedim per protocol https al domini inskta.cat i que els darrers accessos del sistema són seguits.



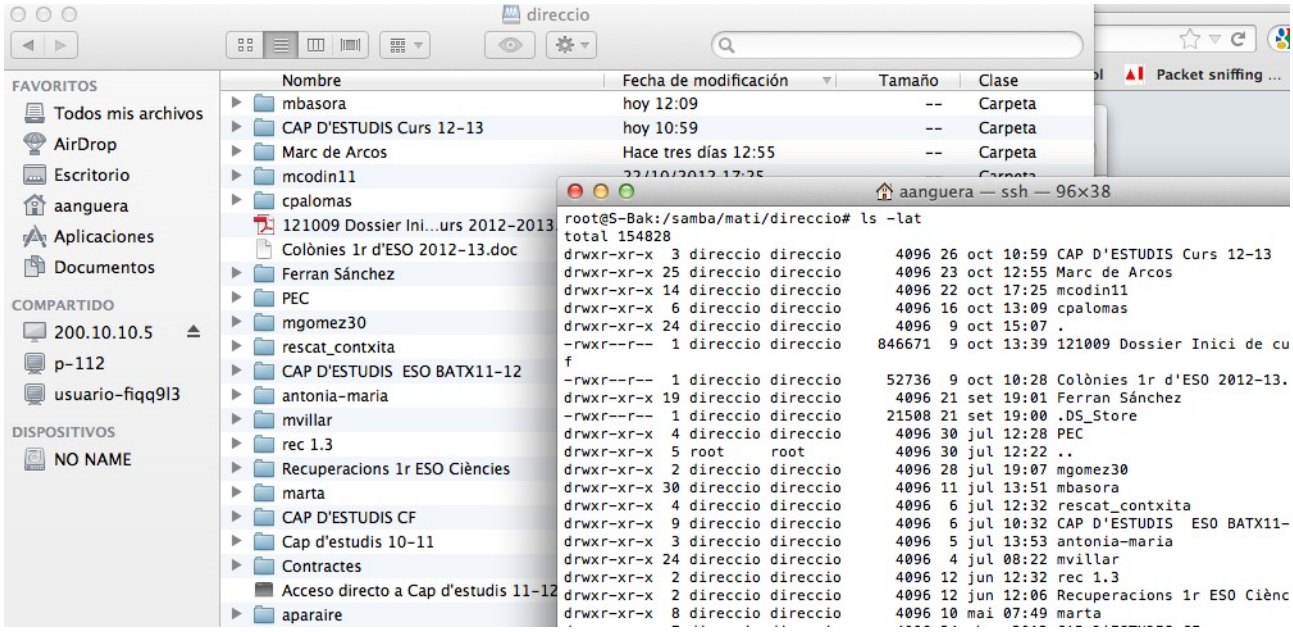
12 Còpia de seguretat del servidor de fitxers Samba

Del servei de fitxers Samba també es fa una còpia de seguretat. Per verificar-ne el seu funcionament obro un finestra amb el recurs *direccio*, que a la següent imatge es mostra ordenat per data de modificació. El darrer recurs modificat és la carpeta

- mbasora (modificat a data d'avui a les 12:09h.)

Aquesta carpeta al moment de verificar la còpia de seguretat encara no s'havia actualitzat, però si que estava actualitzada al servidor de còpies de seguretat la carpeta

- CAP D'ESTUDIS Curs 12-13 (modificat a data d'avui a les 10:59h.)



Amb aquestes proves es demostra que són operatius els serveis de protecció i seguretat. La resta de serveis (servidor Web, gestió de xarxa, proxy, servei DNS...) es comproven per la pròpia dinàmica del centre, si no funcionessin, els usuaris no podrien treballar.

13 Conclusions

Els objectius proposats a l'inici del TFM s'han assolit. Ara es disposa d'una xarxa unificada amb uns serveis (DHCP, DNS, Samba, impressió, Web...), completament operatius i una navegació per internet molt més fluïda de la inicial. Es disposa de la possibilitat de registrar els accessos a internet que realitza un determinat alumne, o la quantitat de fulls que s'imprimeixen, però manca facilitat d'accés a aquest registre.

Respecte al registre d'accés a internet pel servei DNS, aquest genera uns fitxers de *logs* que només els pot consultar un administrador del sistema (per la incomoditat de treballar amb fitxers de text), aquests també són llarguíssims, ocupen molt d'espai al disc i s'han d'esborrar amb periodicitat per no saturar el disc del servidor.

Respecte a la consulta de pàgines impreses (CUPS + Pykota), aquestes es registren en una base de dades PostgreSQL, i el treball directe amb taules tampoc és del tot fàcil. Altra vegada es requereix d'un administrador del sistema per fer consultes.

La millora en el registre podria fer amb una configuració diferent en l'accés a internet, on el client es registres en una base de dades amb usuari i clau.

Respecta a la seguretat amb el treball a internet aquest ha millorat molt. Els clients passen per dos filtres abans no accedeixen a internet. El primer que es troben és el servidor de xarxa (pels clients és la passarel·la), i aquest no obté l'accés directe als *routers* sinó que ho fa pel balanceig de càrrega que també té les seves regles.

El servidor Web de la DMZ també està protegit, i des d'aquest no es pot accedir a la LAN del centre. Però hi ha un petit forat de seguretat. Si bé és cert que del servidor Web no s'accedeix a la LAN si que ho pot fer a dues màquines concretes. Aquest són els servidors de còpies de seguretat que estan ubicades dins la LAN. Per tant si des del servidor Web accedim als servidors de còpies de seguretat, des d'aquest podríem arribar a la resta de màquines de la LAN.

La solució d'aquest forat no es massa complicada, però encara no està resolta i afecta la fase de disseny. La qüestió és:

- qui sol·licita les còpies de seguretat?

Actualment és el servidor Web qui ho fa, per tant aquest disposa de ruta al servidor de còpies de seguretat. En canvi si fos el servidor de còpies de seguretat qui les sol·licités, es podria permetre només el transit entre servidor Web i còpies de seguretat si prèviament qui l'ha sol·licitat és el servidor de còpies de seguretat. Aquest mecanisme tallaria d'arrel la possibilitat d'accés del servidor Web a la LAN.

També m'agradaria agrair el suport i ajuda rebut. Sense aquest hauria estat molt més feixuc configurar tots els punts d'accés, RAC's, ordinadors d'aules, impressores... de la xarxa de l'institut.

14 Webgrafia

Informació genèrica

- http://www.wikipedia.org/

Configuració dels servidors:

- http://www.debian.org/

Configuració de xarxa

- http://wiki.debian.org/NetworkConfiguration

Servidor Web:

- http://www.apache.org/

Servidor proxy i filtre de continguts

- http://www.squid-cache.org/

Servidor cups i registre d'impressions:

- http://www.cups.org/
- http://www.pykota.com/

Bloc d'informació de balanceig de càrrega

- http://bourneagainshell.blogspot.com.es/2008/05/de-como-conectar-13-adsls-en-balanceo.html

Registre d'activitat de xarxa

- http://humdi.net/vnstat/
- http://iptraf.seul.org/