

**TREBALL FINAL DE CARRERA****INTEGRACIÓ DE XARXES TELEMÀTIQUES****Títol**

**Integració en una xarxa d'àrea local , d'un sistema d'autenticació sense fils amb un servidor RADIUS.**

**Alumne:**

**M<sup>a</sup> Teresa Martí Ferrando**

**Consultor:**

**Antoni Morell Pérez**

## Descripció

La xarxa de l' institut està formada per sis aules independents amb ordinadors de sobretaula.

En cadascuna de les aules hi ha un servidor d'aula amb dues targetes de xarxa que dona accés a un servidor Proxy, que filtra entrades i sortides cap a Internet.

Aquest accés a Internet es proporciona mitjançant un router connectat a la línia d' ADSL.

Quan es va fer el disseny de les aules, la utilització dels ordinadors portàtils no estava tan estesa com ho està avui en dia.

El fet que els ordinadors portàtils hagen abaratit els seus costos, ha produït que una gran quantitat d'alumnes acudeixen al centre amb els seus ordinadors portàtils.

Donat que en cadascuna de les aules hi ha una gran quantitat d'ordinadors de sobretaula i la ubicació d'aquests ordinadors portàtils, s'han de sumar als ja existent, el cablejat de cadascuna de les aules es insuficient per a garantir la connectivitat de tots els alumnes.

Com que els ordinadors portàtils d'avui en dia disposen de targeta de xarxa sense fils, sorgeix la idea de posar punts d'accés per a connectar els dispositius portàtil.

En aquest punt, es quan es crea la necessitat d'aquest projecte, l'objectiu del qual és la integració en el sistema d'un punt d'accés sense fils, que permetria als alumnes que porten el seu portàtil propi, connectar-se'l a la xarxa.

Actualment disposem tan sols de dos aules amb un punt d'accés, en el qual es realitza una validació WPA2, i tots els alumnes es connecten amb la mateixa contrasenya.

Però el que es desitja no és tan sols que els alumnes es puguin connectar, sinó poder validar-se en el sistema amb un usuari i una contrasenya, i tindre accés a la xarxa de l'aula corresponent a cada alumne. Així també poder tindre accés al servidor d'aula corresponent i disposar al mateix temps de connectivitat Internet.

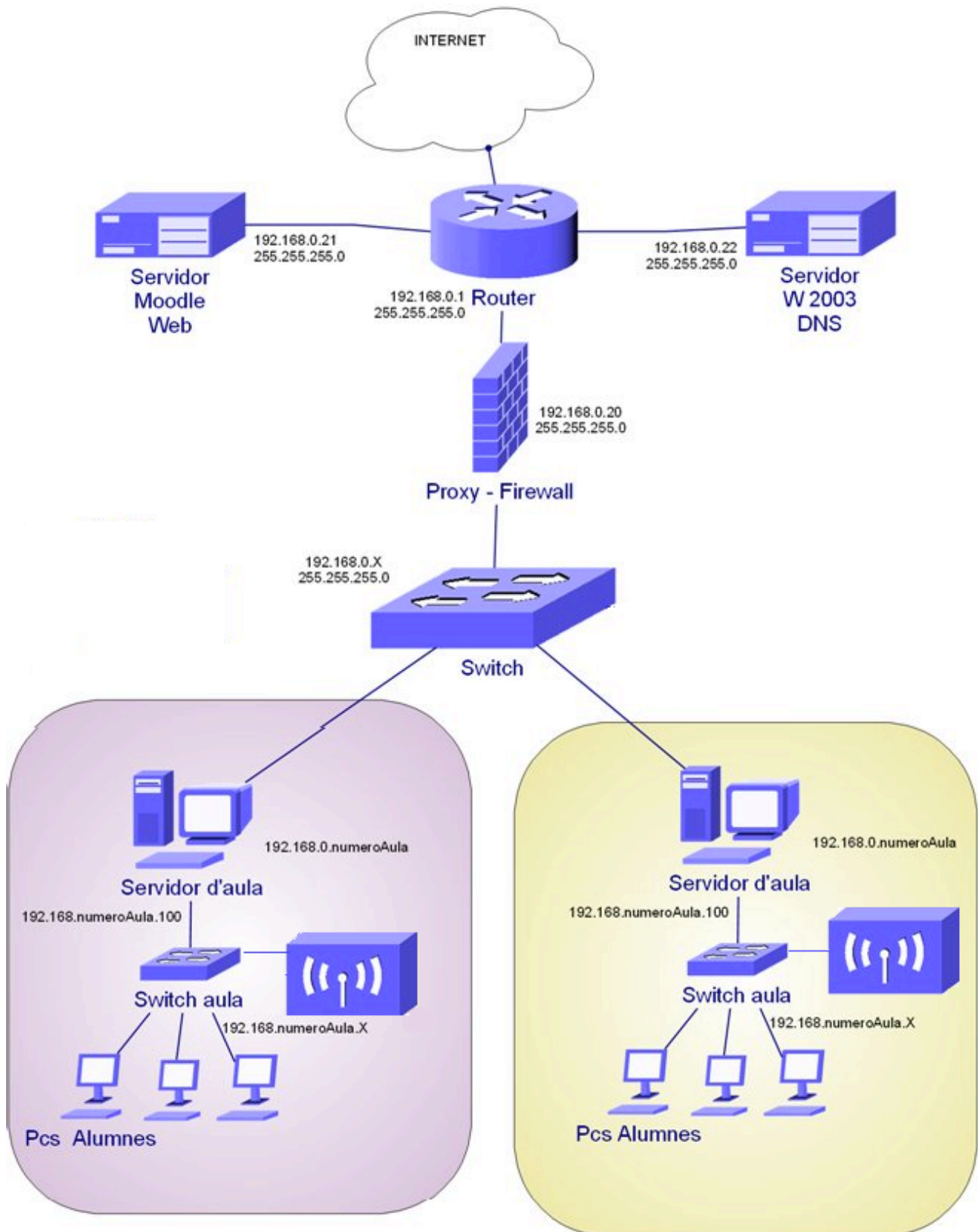
Tots els ordinadors i servidors de l' institut, tenen instal·lat un sistema operatiu Ubuntu. Coexisteixen diverses versions d'aquest sistema operatiu.

Per tal de dur a terme el projecte, caldria configurar un servidor RADIUS, com per exemple, freeRadius.

També caldria instal·lar i configurar algun sistema per a la validació d'usuaris com pot ser un servidor LDAP, per a l'autenticació i validació dels alumnes.

Una vegada instal·lats i configurats el servidor i el punt d'accés, caldria integrar-lo a la xarxa ja existent, fent les modificacions necessaris als servidors d'aula, per tal de que coexisteixen els dos sistemes.

## ESQUEMA D'INTERCONNEIXIÓ DE LA XARXA DE L' INSTITUT



*Figura 0. Esquema Interconnexió de la xarxa de l'institut*

## ÍNDIX DE CONTINGUTS

<b>1</b>	<b>Introducció .....</b>	<b>8</b>
1.1	Justificació i context del projecte.....	8
1.2	Objectiu del projecte.....	9
1.3	Punt de vista i mètode seguit.....	9
1.4	Planificació del projecte.....	10
1.5	Calendari de treball .....	15
<b>2.</b>	<b>Protocols i Software de Xarxes sense fils .....</b>	<b>16</b>
2.1	Introducció.....	16
2.2	Estàndards de xarxes d'àrea local.....	17
2.3	Wep.....	23
2.4	WPA .....	25
2.5	Servidor RADIUS .....	27
2.7	Estudi de Viabilitat .....	30
<b>3.</b>	<b>Configuració del Servidor RADIUS.....</b>	<b>32</b>
3.1	Instal·lació del Sistema Operatiu.....	32
3.2	Configuració de la xarxa .....	35
3.3	Instal·lació i configuració del servidor de DHCP .....	37
3.4	Instal·lació i configuració del servidor DNS.....	38
3.5	Instal·lació i configuració de LDAP .....	41
3.5.1	Components.....	41
3.5.2	Backends.....	41
3.5.3	Característiques i avantatges .....	42
3.5.4	Instal·lació del servidor LDAP i carrega d'informació del directori.....	43
3.5.5	Backend de OpenLDAP .....	43
3.5.6	Control d'accés a LDAP (olcAccess).....	47

3.5.7 Administració gràfica de OpenLDAP .....	48
<b>3.6 Instal·lació i configuració de freeRadius .....</b>	<b>51</b>
<b>3.7 Configuració del Punt d'accés (Access Point) .....</b>	<b>55</b>
<b>4. Integració amb la Xarxa d'Àrea local.....</b>	<b>59</b>
4.1 Descripció de la xarxa de d'institut .....	59
4.2 Integració del Servidor RADIUS i punt d'accés .....	61
4.3 Alta d'elements en el directori ldap.....	63
<b>5. Solucions Integrades amb Ldap i RADIUS. ZeroShell. ....</b>	<b>65</b>
<b>6. Conclusions.....</b>	<b>66</b>
<b>Bibliografia .....</b>	<b>67</b>
<b>Glossari d'acrònims .....</b>	<b>68</b>
<b>ANNEXES.....</b>	<b>70</b>

## Índex de Figures

Figura 0. Esquema Interconnexió de la xarxa de l'institut .....	3
Figura 1. Calendari de treball.....	15
Figura 2.1. Taula d'estàndards 802.11 [1] .....	18
Figura 2.2.Part de la pila de protocols del 802.11, de la capa Física [2] .....	18
Figura 2.3. Exemple de multiplexació SDM en MIMO. [8].....	20
Figura 2.4. Detecció de Canal Virtual en CSMA/CA [2] .....	21
Figura 2.5. Esquema de connexió en mode Ad-Hoc [1].....	22
Figura 2.6. Esquema de connexió en mode Infraestructura [1] .....	23
Figura 2.7. Esquema d'enviament WEP. [1] .....	24
Figura 2.8. Funcionament de AES [4] .....	26
Figura 2.9. Esquema de connexió WPA2-empresarial [1].....	27
Figura 3.1. Instal·lació Ubuntu 10.04. Selecció de l'idioma .....	32
Figura 3.2. Instal·lació Ubuntu 10.04. Selecció de la ubicació .....	33
Figura 3.3. Instal·lació Ubuntu 10.04. Selecció de la distribució teclat .....	33
Figura 3.4. Instal·lació Ubuntu 10.04. Esquema de Particionat del disc .....	34
Figura 3.5. Instal·lació Ubuntu 10.04. Definició Usuari i nom d'equip. ....	34
Figura 3.6. Instal·lació Ubuntu 10.04. Confirmació i copia d'arxius. ....	35
Figura 3.7. Configuració de la interfície gràfica. ....	36
Figura 3.8. Resultat de la recerca d'un usuari al servei de directori .....	47
Figura 3.9. Interfície gràfica LAT.....	49
Figura 3.10. Administració de LDAP amb phpLDAPadmin.....	50
Figura 3.11. Vista gràfica del directori des de phpLDAPadmin.....	50
Figura 3.12. Sortida del test de funcionament de freeRadius .....	54
Figura 3.13. Configuració de l'adreça del Router.....	55
Figura 3.14. Configuració de la xarxa wireless al Router.....	56
Figura 3.15. Configuració de l'associació Router-Server Radius.....	56
Figura 3.16. Configuració de l'autenticació del client sense fils .....	57
Figura 3.17. Selecció del certificat de la CA .....	58
Figura 3.18. Connexió establerta des d'un client.....	58
Figura 4.1. Esquema de la xarxa actual del centre IES Jaume II el Just.....	59
Figura 4.2. Esquema de la xarxa, divisió per aules.....	60
Figura 4.3. Xarxa amb el servidor RADIUS i el Router (AP) .....	62

Figura 4.4. Esquema de la Xarxa del Centre Definitiva .....	63
Figura A1. Preparació Instal·lació Ubuntu12.04 .....	70
Figura A2. Tipus d'Instal·lació Ubuntu12.04 .....	70
Figura A3. Instal·lació Ubuntu12.04, esquema de particionat de disc .....	71
Figura A4. Instal·lació Ubuntu12.04. Selecció zona horaria .....	71
Figura A5. Instal·lació Ubuntu12.04. Selecció teclat .....	72
Figura A6. Instal·lació Ubuntu12.04. Usuari i nom de l'equip. ....	72
Figura A7. Finalització Instal·lació Ubuntu12.04 .....	73
Figura A8. Interfície del sistema ZeroShell .....	78
Figura A9. Finestra de validació en el sistema ZeroShell.....	78
Figura A10. Interfície d'Administració ZeroShell.....	79

## 1 Introducció

### 1.1 Justificació i context del projecte

La tecnologia avança a passos agegantats, i a mesura que es produeix aquest avanç, els costos dels nous dispositius van disminuint.

Aquest fenomen en el qual ens veiem immersos contínuament ha produït que l'ordinador de sobretaula que apareixia a gran nombre de domicilis particulars, s'haja substituït o acompanyat en molts casos, de dispositius portàtils. Aquest fet ha estat donat per què els ordinadors portàtils cada vegada són més econòmics, ofereixen millors prestacions, al mateix temps que aporten al usuari una gran comoditat al poder endur-se'l al treball, a altres domicilis o simplement perquè no ocupen quasi espai.

El context en el qual es situa aquest projecte, és un institut d'educació secundària, on s'imparteixen tres cicles formatius de la família d'Informàtica i Comunicacions. En aquest institut disposem d'un edifici de tres plantes, que està distribuït amb dues aules per planta.

Al igual que en molts centres docents de la comunitat valenciana, els recursos dels quals disposem no són tots els que desitjaria un professor per impartir la docència d'una forma adequada.

En aquestes aules disposem majoritàriament d'ordinadors de sobretaula que es renoven parcialment cada tres o quatre anys.

Si ajuntem aquesta context, a la primera part, es produeix una situació que a primera hora era esporàdica i ara ja és un fet habitual. Cada alumne assisteix a classe amb el seu ordinador portàtil.

Aquesta situació aporta diversos avantatges. Per una part l'alumne se'n porta amb ell, tot el treball que ha fet a classe i pot consultar-lo o continuar-lo a casa. Per l'altra part, la feina de manteniment de l'aula es redueix donat que cada alumne s'ocupa del seu propi ordinador.

També existeix un grup d'alumnes a cadascuna de les aules que segueix utilitzant els ordinadors de sobretaula de l'institut.

Quan es va fer el disseny de les xarxes de les aules no es va tenir en compte, que a més dels ordinadors de sobretaula, podrien connectar-se més usuaris amb els seus portàtils.

És per aquest motiu, que el cablejat d'aula no és suficient per a cobrir totes les necessitats, i



s'ha hagut de instal·lar punts d'accés en algunes de les aules, per a donar cobertura sense fils als ordinadors portàtils.

Encara que es protegeix l'accés a cadascun dels punts amb contrasenya, aquesta qüestió provoca que els alumnes es validen en qualsevol aula, perquè van passant-se les contrasenyes entre ells.

A partir d'ací naix la possibilitat de validar cadascun dels usuaris amb una identificació única, per tal que cada usuari estigui controlat.

## 1.2 Objectiu del projecte

L'objectiu principal del projecte és l'autenticació i validació dels alumnes que assisteixen a l'institut amb el seu portàtil personal, en la xarxa de cadascuna de les aules a les que pertanyen, sense necessitat de connectar-se'l amb un cable.

Com objectius secundaris que es poden assolir pel fet de complir l'objectiu principal, podem destacar, que l'alumne podrà treball exactament igual que si treballés amb un ordinador de sobretaula. És a dir, tindrà connexió amb el servidor d'aula i amb l'exterior. Per tant també gaudirà de la possibilitat de connectar el portàtil a Internet.

## 1.3 Punt de vista i mètode seguit

El punt de vista i el mètode que s'utilitzarà en aquest projecte, serà la divisió en tasques.

Tindrem unes primeres tasques que consistiran en l'anàlisi de tots els elements que intervenen en el projecte. Com per exemple:

- protocols utilitzats
- software que es podria utilitzar en el projecte
- sistemes de connexió sense fils
- esquema d'interconnexió
- sistemes de validació d'usuaris
- estudi de viabilitat, etc..

Les tasques que es duran a terme en segon lloc, seran les de la instal·lació del sistema servidor. Que consistirà en un servidor basat en un sistema de software lliure, com és Ubuntu, i després instal·larem el servidor RADIUS.

Una vegada es tingui el sistema operatiu el servidor, s'instal·larà i configurarà un sistema de validació d'usuaris basat en el protocol LDAP.

En una fase posterior abordarem les tasques d'integració del sistema de la xarxa cablejada, amb els nous usuaris sense fils.

La última fase consistirà en les proves de funcionament, correcció i adaptació de tots els sistemes per a que tot tingui el funcionament esperat.

## 1.4 Planificació del projecte

Fites del projecte que s'han d'assolir	
<i>*Fites que ha de complir el projecte. Fites externes.</i>	
Data	Descripció
29 de febrer	Inici del projecte
7 de març	Decisió del projecte i comunicació al consultor
14 de març	PAC 1 - Lliurament de la planificació del treball
25 d'abril	PAC 2 - Primer lliurament del projecte
30 de maig	PAC 3 - Segon lliurament del projecte
16 de juny	Lliurament de la memòria final
22 de juny	Entrega de la presentació i del codi

Per tal d'aconseguir assolir aquestes fites, després d'analitzar el projecte, podem dividir aquest en 6 tasques principals.

Per tant la planificació vindrà adaptada a cadascuna d'aquaqquests fases i etapes, fent una divisió de tasques i subtasques, per tal de fer un seguiment adequat, i fent possible portar a bon terme els l'objectiu proposats.

### ➤ TASCAS 1: Preparació del projecte.

#### ▲ Subtasca 1.1

Estudi del projecte.

Durada                      4 dies

Objectiu:            Obtenir tots aquells coneixements necessaris quant a seguretat, per tal de poder implantar un sistema sense fils segur.

▲ **Subtasca 1.2**

Proposta del treball final de carrera.

Durada                    2 dies

Objectiu:        Elaborar un document que defineixi les característiques del projecte.

Definició, títol, objectius, etc.

FITA: Proposta TFC acceptada.

▲ **Subtasca 1.3**

Definició del pla del projecte.

Durada                    7 dies

Objectiu:        Elaborar un pla de treball, on es dividirà el projecte en tasques. A més s'obté un diagrama de Gantt on s'especificaran les tasques detallades temporalment.

FITA:PAC 1 Pla de Projecte

➤ **TASCA 2: Anàlisi de protocols, i del software i hardware necessari per al projecte.**

▲ **Subtasca 2.1**

Estudi dels protocols de seguretat sense fils.

Durada                    5 dies

Objectiu:        Fer una recerca dels protocols sense fils utilitzats, així com el diferents tipus de protocols de seguretat.

Producte Resultant: Documentació de protocols sense fils i seguretat.

▲ **Subtasca 2.2**

Anàlisi de diferents dispositius hardware que ens permeten l'accés dels portàtils a la xarxa sense fils.

Durada                    5 dies

Objectiu:        Fer una recerca dels dispositius que més s'adeqüen a les necessitats del projecte.

Producte Resultant:: Documentació amb productes a utilitzar.

▲ **Subtasca 2.3**

Anàlisi de diferents programes que ens poden proveir el servei de RADIUS.

Durada                    5 dies

Objectiu: Fer una recerca dels tipus de programes que hi ha, avantatges i inconvenients de cadascun d'ells.

Producte Resultant:: Programa escollit.

▲ **Subtasca 2.4**

Anàlisi del software necessari per a permetre l'autenticació d'usuaris.

Durada 2 dies

Objectiu: Fer una recerca del tipus d'autenticació que es pot utilitzar.

Producte Resultant:: Software d'autenticació escollit.

➤ **TASCA 3: Implementació del sistema amb Ubuntu**

▲ **Subtasca 3.1**

Analitzar i estudiar tota la infraestructura de la xarxa així com els serveis i protocols Linux a emprar.

Durada 1 dia

Objectiu: Compatibilitzar totes els dispositius hardware i software.

▲ **Subtasca 3.2**

Instal·lació i configuració de Linux

Durada: 1 dia

Objectiu: Preparar un ordinador que tingui la funció de servidor, amb tot el hardware i software necessari per a poder implementar el servidor i fer les proves d'autenticació, autorització i gestió de l'accés als usuaris.

▲ **Subtasca 3.3**

Configuració i Parametrització dels Serveis.

Durada: 12 dies

Objectiu: Instal·lar i configurar el servidor RADIUS així com Openssl i el servei d'autenticació d'usuaris LDAP.

▲ **Subtasca 3.4**

Instal·lació i configuració del punto de accés.

Duració 1 dia

Objectiu: Instal·lar i configurar un punt d'accés en la xarxa, que es pugui comunicar amb el servidor RADIUS de Linux.

▲ **Subtasca 3.5**

Alta i gestió dels usuaris (alumnes) del servei.

Durada                    1 dia

Objectiu: Configurar els clients per a poder fer les proves després.

▲ **Subtasca 3.6**

Configuració dels clients.

Durada                    1 dia

Objectiu:      Configuració d'un client per a que es pugui validar amb el servidor RADIUS.

➤ **TAREA 4: Integració dels clients wireless a la xarxa local cablejada**

▲ **Subtasca 4.1**

Estudi de la configuració de la xarxa.

Duració:      2 dies

Objectiu:      Analitzar i estudiar la infraestructura de l' institut i el nou sistema muntat.

▲ **Subtasca 4.2**

Integració del Servidor RADIUS.

Duració:      4 dies

Objectiu:      Permetre l'accés a la xarxa cablejada des de els portàtils.

▲ **Subtasca 4.3**

Integració del Punt d'accés.

Duració:      3 dies

Objectiu:      Permetre l'accés a la xarxa cablejada des de els portàtils.

▲ **Subtasca 4.4**

Creació dels scripts.

Duració:      3 dies

Objectiu: Facilitar la tasca d'alta d'elements en el directori LDAP.

▲ **Subtasca 4.5**

Alta d'unitats i usuaris.

Duració: 1 dias

Objectiu: Incorporar els alumnes i aules al directori LDAP.

➤ **TASCA 5: Validació del sistema.**

▲ **Subtasca 5.1**

Realització Proves

Durada 7 dies

Objectiu: Provar que es pot accedir amb portàtils des de totes les aules.

▲ **Subtasca 5.2**

Últims ajusts.

Durada 9 dies

Objectiu: Obtenir una presentació que sintetitza tots els punts més importants i representatius del projecte.

FITA: Finalització del projecte tècnic.

➤ **TASCA 6: Elaboració de la memòria , presentació i documentació addicional.**

▲ **Subtasca 6.1**

Confecció de la memòria del projecte

Durada 73 dies

Objectiu: Redactar tot els estudis, i documentar tots els punts que es realitzen per a dur a terme aquest projecte.

FITA: Memòria del projecte.

▲ **Subtasca 6.2**

Preparar la presentació del projecte.

Durada 7 dies

Objectiu: Obtindre una presentació que sintetitza tots els punts més importants i representatius del projecte.

FITA: Presentació del projecte.

## 1.5 Calendari de treball

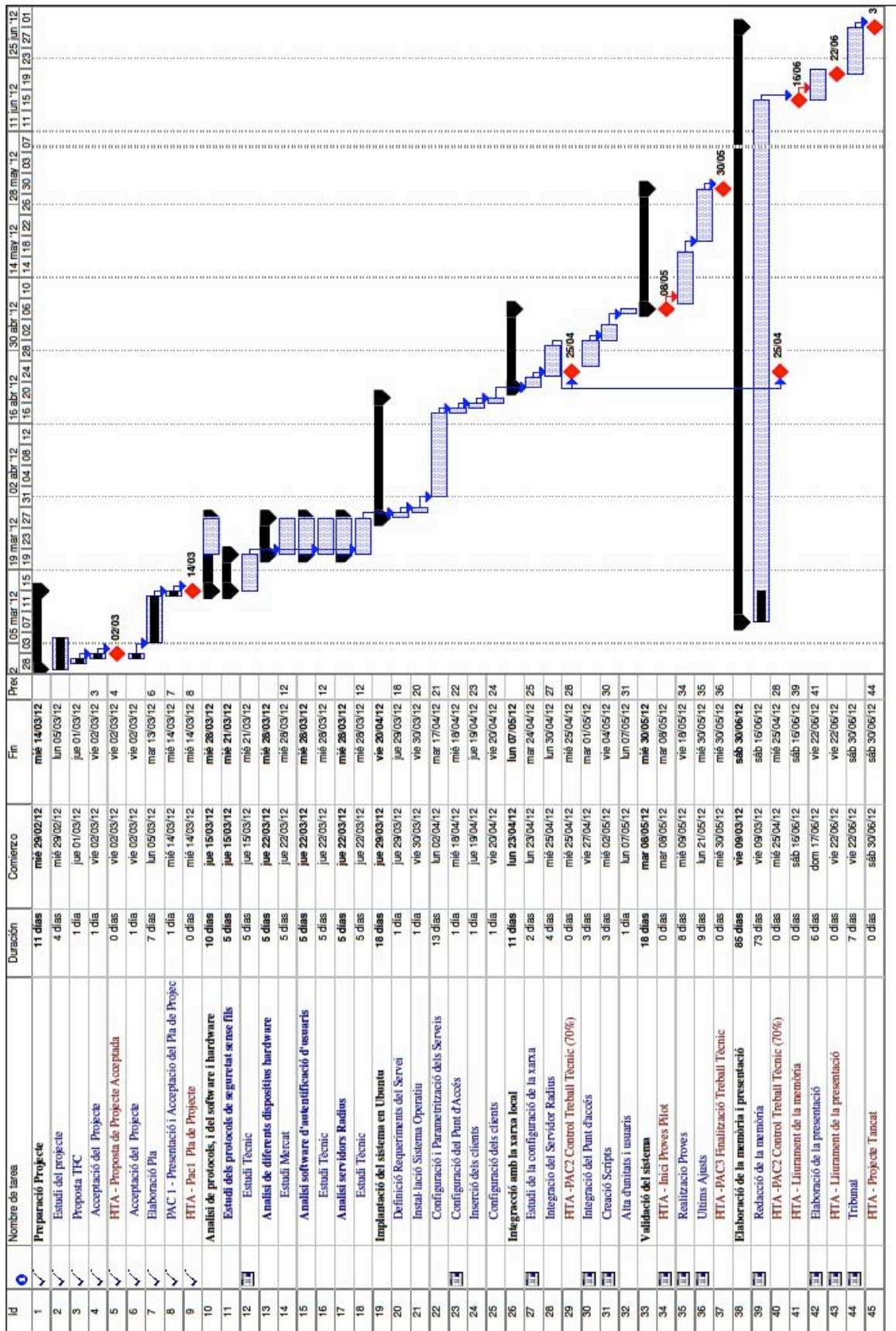


Figura 1. Calendari de treball.

## 2. Protocols i Software de Xarxes sense fils

### 2.1 Introducció

En aquest punt introduïrem diversos conceptes que se considera necessaris per a poder entendre els apartats posteriors dels projecte.

- Autenticació (*authentication*): fa referència al procés per el qual determinem si un usuari té permís per a accedir a un determinat servei de xarxa que vol utilitzar. El procés d'autenticació es realitza mitjançant una validació d'una identitat i uns credencials per part de l'usuari que demanda l'accés.
- Autorització (*authorization*): el que es produeix és la concessió o denegació de serveis específics a un determinat usuari, en base a l'autenticació, els serveis sol·licitats i l'estat actual del sistema.
- Registre (*accounting*, de vegades es tradueix com comptabilitat): es refereix a realitzar un registre del consum de recursos que realitzen els usuaris. El registre pot incloure aspectes de la identitat de l'usuari, la classe de servei prestat, i quan començà i acaba la utilització del servei.
- Protocols PAP (Password Authentication Protocol), que són mètodes de autenticació utilitzats per proveïdors de serveis de Internet (ISPs) accessibles a través de PPP.
- LDAP (Lightweight Directory Access Protocol), un protocol del nivell d'aplicació (sobre TCP/IP) que implementa un servei de directori ordenat, i que té una base de dades que conté noms d'usuaris i les seues contrasenyes.
- EAP (Extensible Authentication Protocol), és un entorn universal d'autenticació emprat freqüentment en xarxes sense fils i connexions punt a punt.
- RADIUS (Remote Authentication Dial-In User Server) és un protocol que ens permet gestionar la "autenticació, autorització i registre" d'usuaris remots sobre un determinat recurs. Les tres "autenticació, autorització i registre" són conegudes com AAA, per el seu significat en anglès "Authentication, Authorization, and Accounting".
- AP (Access Point): Punt d'accés, dispositius que permet connectar a una xarxa cablejada, dispositius sense fils.



- Un Network Access Server (NAS) es un sistema que proporciona accés a la xarxa. En alguns casos també s'anomena Remote Access Server (RAS) o Terminal Server. En general, NAS és un element que controla l'accés a un recurs protegit, que pot ser des d'un simple telèfon per a VoIP o una impressora, fins a l'accés a una xarxa sense fils o a Internet (proporcionat per un ISP).
- **IMS (IP Multimedia Subsystem)** una arquitectura de referència genèrica per tal d'oferir serveis multimèdia sobre infraestructura IP. Es tracta d'un estàndard internacional encara en evolució, que suporta múltiples tipus de tecnologies d'accés, incloent: GSM, GPRS, UMTS, HSDPA, DSL, HFC, Wi-Fi, Wi-Max, Bluetooth, etc. És a dir, el concepte actual de les comunicacions telefòniques i per Internet donarà un canvi radical a curt termini, gràcies a aquesta nova tecnologia que permetrà passar d'un sistema a un altre sense interrompre la connexió, utilitzar més d'un mitjà al mateix temps o compartir-los e intercanviar-los amb altres usuaris.
- **Router.** Terme anglès utilitzat per a designar un **encaminador** o **enrutador**, és un dispositiu de xarxa de nivell 3 del model OSI. Pren la informació del nivell de xarxa (adreça IP) per a prendre les decisions d'encaminament: escollir el camí o ruta més adequada per on reenviar les dades rebudes.

## 2.2 Estàndards de xarxes d'àrea local

El projecte IEEE 802 va ser creat en Febrer de 1980 amb la finalitat de desenvolupar els estàndards per a que tecnologies de diferents fabricants pogueren treball juntes i integrar-se sense cap tipus de problemes. El IEEE ha produït diversos estàndards, protocols o normes per a xarxes d'àrea local.

Els comitès 802 del IEEE es concentren principalment en la interfície física relacionada amb els nivells físics i d'enllaç de dades del model de referència OSI de la ISO.

L'estàndard IEEE 802.11 defineix els dos primers nivells de la capa OSI per a les xarxes d'àrea local sense fils (WLAN).

Els protocols estàndard que permeten la comunicació sense fils són els que es mostren en la figura següent:

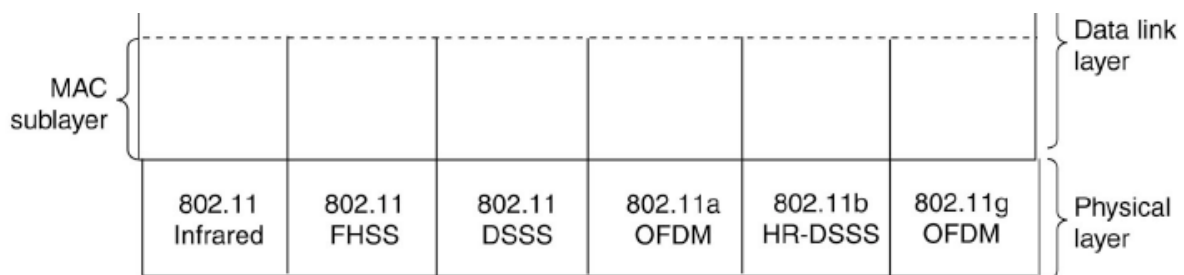
Protocolo	Frecuencia	Alcance aproximado	Velocidad	Otros
802.11a	5GHz	50 metros	54 Mbit/s	Sufre menos interferencias porque no es la banda de los teléfonos móviles y otros electrodomésticos, sin embargo es mucho más sensible a los obstáculos.
802.11b	2,4GHz	100 metros	11Mbit/s	La frecuencia de 2,4 es menos sensible a los obstáculos, pero en esta frecuencia trabajan muchos electrodomésticos que provocan interferencias.
802.11g	2,4GHz	100 metros	54Mbit/s	Las interferencias sufridas son las mismas que en 802.11b
802.11 n	2,4GHz y 5GHz	100 metros	600 Mbps	Aunque el estándar se publicó de forma definitiva en Septiembre de 2009, ya existían anteriormente dispositivos que cumplían un borrador del estándar llamado 802.11 draft n. Los dispositivos de este tipo son compatibles con todos los protocolos anteriores

**Figura 2.1. Taula d'estàndards 802.11 [1]**

Quan es va definir l'estàndard 802.11, l'estàndard 802.3 ja dominava les xarxes d'àrea local, per la qual cosa el 802.11 es va dissenyar de forma que fora compatible amb la 802.3 en la capa d'enllaç de dades.

- **Nivell Físic 802.11**

En la següent figura podem veure totes les variants de la capa física definides per a l'estàndard 802.11.



**Figura 2.2. Part de la pila de protocols del 802.11, de la capa Física [2]**

L'estàndard 802.11- infrarojos utilitza la mateixa tecnologia que els comandaments de control remot de la televisió, però utilitza una transmissió difusa (és a dir, no requereix línia visual directa). Aquest estàndard avui en dia quasi no s'utilitza.

Els altres mètodes utilitzen modulació FDSS y DSSS [2] que usen la banda de 2.4 GHz, que no necessita llicència estatal. Els comandaments de les portes dels garatges també empren aquesta banda, pel que no es pot descartar que algun portàtil aconseguís obrir alguna porta. També utilitzen aquesta banda els telèfon sense fils i els forns microones.

La 802.11a utilitza OFDM (Multiplexació per Divisió de Freqüències Ortogonals) [3] para transmetre fins a 54Mbps en la banda de 5 GHz. Utilitza un sistema de modulació complex basat en la modulació per desplaçament de fase (FSK) [6] per a velocitats de fins 18 Mbps, i modulació QAM [6] per a velocitats majors.

La 802.11b usa una modulació anomenada HR-DSSS (High Rate-DSS) [2]. Utilitza 11 milions de xips per segon per tal d'arribar fins a 11 Mbps en la banda de 2,4 GHz.

En 2001 es va aprovar la 802.11g, que utilitza la modulació OFDM [3] de la 802.11a però la banda de 2,4 GHz de la 802.11b.

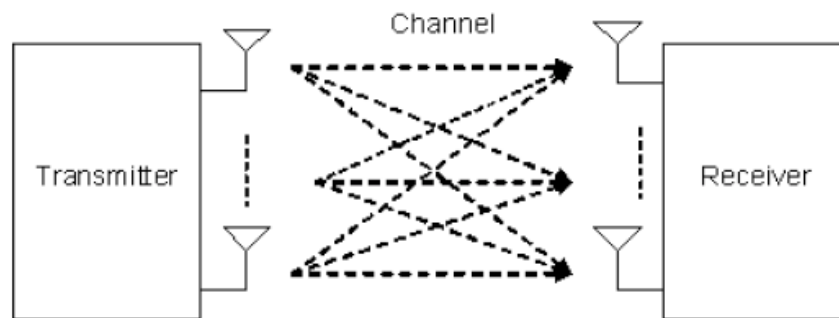
Finalment, la norma IEEE 802.11n es una proposta de modificació per a millorar significativament el rendiment de la xarxa més enllà dels estàndards anteriors amb un increment significatiu en la velocitat màxima de transmissió de 54 Mbps a un màxim de 600 Mbps.

La capa física suporta una velocitat de 300Mbps, utilitzant dos fluxos espacials d'un canal de 40 MHz. L'estàndard 802.11n es basa en agregació Multiple-Input Multiple-Output (MIMO) i la unió d'interfícies de xarxa (Channel Bonding), a més agrega varies trames a la capa MAC.

MIMO utilitza múltiples antenes transmissores i receptors per a millorar les prestacions del sistema. Aquest conjunt d'antenes s'utilitza en funció de la tecnologia en MIMO que s'utilitzarà.

Hi ha principalment tres categories de la tecnologia MIMO [8]:

- **Beamforming:** consisteix en la formació d'un senyal d'ona reforçada pel desfasament en diferents antenes. Els principals avantatges són un major guany de senyal, així com un menor atenuació amb distància. A causa de l'absència de dispersió el beamforming dona lloc a un patró ben definit però direccional. En aquest tipus de transmissions és necessari, l'ús de dominis de beamforming, sobretot en el cas de transmissió d'antenes múltiples.
- **Spatial Multiplexing**(multiplexació per divisió espacial- SDM): consisteix en la multiplexació d'un senyal de gran ample de banda en senyals d'ample de banda més menut d'igual mida, i que es transmet entre les diferents antenes. SDM multiplexa espacialment múltiples fluxos de dades independents. Si aquests senyals arriben amb una separació suficient en el temps que permeti distingir cada una d'elles, s'aconsegueix crear així canals múltiples per a mínim amples de banda. Aquesta és una tècnica molt bona que permet augmentar la velocitat de transmissió, especialment en ambients on hi ha molt de soroll en relació a la senyal. L'inconvenient és que estem limitats pel nombre disponible d'antenes tant en el transmissor com en el receptor.



*Figura 2.3. Exemple de multiplexació SDM en MIMO. [8]*

- **Diversitat de codi:** una sèrie de tècniques utilitzades en mitjans de comunicació que per alguna raó, només podeu utilitzar un únic canal, codificant la transmissió mitjançant espaiat en el temps i la diversitat de senyals disponibles, donant lloc al codi de l'espai-temps. L'emissió des de múltiples antenes basat en principis de ortogonalitat és explotada per augmentar la diversitat del senyal.

La multiplexació espacial es pot combinar amb el Beamforming quan es coneix el canal en el transmissor o amb la diversitat de codi quan no és. La distància física entre les antenes ha de ser gran a l'estació base per permetre múltiples longituds d'ona. L'espaiat entre les antenes de receptor ha de ser de com a mínim 0.3 vegades la longitud d'ona per distingir els senyals clarament.

- **Nivell Enllaç de dades 802.11**

Quant al format de trama que es defineix en aquest nivell, tenim tres tipus de trames diferents.

- Gestió. (Management frame): S'utilitzen per a funcions de gestió, com pot ser la petició d'associació a un punt d'accés, tramés d'autenticació, de prova etc. Aquestes trames venen representades per el seu nom en anglès i tenen a veure en la funció que hi realitzen. Exemples poden ser: Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Authentication, Deauthentication, ...
- Control. (Control frames): Trames de control. Com el seu nom indica serveixen per a controlar la transmissió. Per exemple la trama RTS que és una trama que s'utilitza per a enviar un avís. A part d'aquesta també s'utilitzen, CTS, ACK, QoS, Power Save (PS)-Poll ..
- Dades. (Data frames): Trames que contenen la informació a transmetre. D'aquest tipus són: Data, null data, ...

Típicament una LAN sense fils està formada per un conjunt d'estacions base unides mitjançant algun tipus de cable i un conjunt d'estacions mòbils que es comuniquen amb l'estació base més pròxima. El conjunt d'estacions base forma en realitat un sistema cel·lular en miniatura.

La transmissió es realitza mitjançant ones electromagnètiques no guiades i s'utilitza un protocol CSMA [6]. L'abast de cadascuna de les estacions és limitat. Aquest conjunt de característiques comporten situacions com el problema de l'estació oculta.

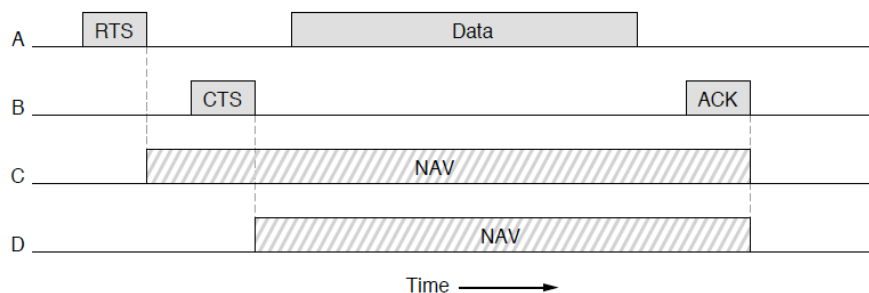
Aquest problema ve donat quan hi ha diverses estacions separades un nombre de metres, i alguna de les estacions queda fora de l'abast d'alguna altra.

Si la que queda fora de l'abast comença a transmetre a una estació del mig i la de l'altra banda també ho fa perquè no ha detectat a la primera, en estar fora de l'abast, es produirien col·lisions que no serien detectades per les estacions més allunyades. Aquest és el problema de l'estació oculta.

Per tot açò la norma 802.11 enlloc d'utilitzar CSMA/CD [2][6], usa 2 modes de funcionament, DCF i PCF [2](de Funció de Coordinació Distribuïda i Funció de Coordinació Puntual).

Quan funciona en mode DCF, la 802.11 usa el protocol CSMA/CA[2][6] (CA = Collision Avoidance o evitació de col·lisions), que se basa en el MACAW [2][7] (Multiple Access with Collision Avoidance for Wireless).

La següent figura mostra com fa el CSMA/CA la detecció del canal virtual.



**Figura 2.4. Detecció de Canal Virtual en CSMA/CA [2]**

El funcionament és el següent:

Quant una estació té una trama per a transmetre, envia abans una xicoteta trama d'avís anomenada RTS (Request To Send). Aquesta trama RTS conté informació sobre la longitud de la trama que vol transmetre i l'estació de destinació.

En rebre la trama RTS la estació de destinació, si està en condicions de rebre la

transmissió, respon amb una altra trama denominada CTS (Clear To Send).

Aquest intercanvi previ de trames produeix la detecció de totes les estacions de que el canal va estar ocupat el temps que es tardí en transmetre la longitud anunciada i així s'evita tant la col·lisió com el problema de l'estació oculta.

L'estàndard IEEE 802.11 defineix el concepte de Conjunt Bàsic de Servei (BSS, Basic Service Set) que consisteix en dos o més nodes sense fils o estacions que se reconeixen una a l'altra i poden transmetre informació entre ells.

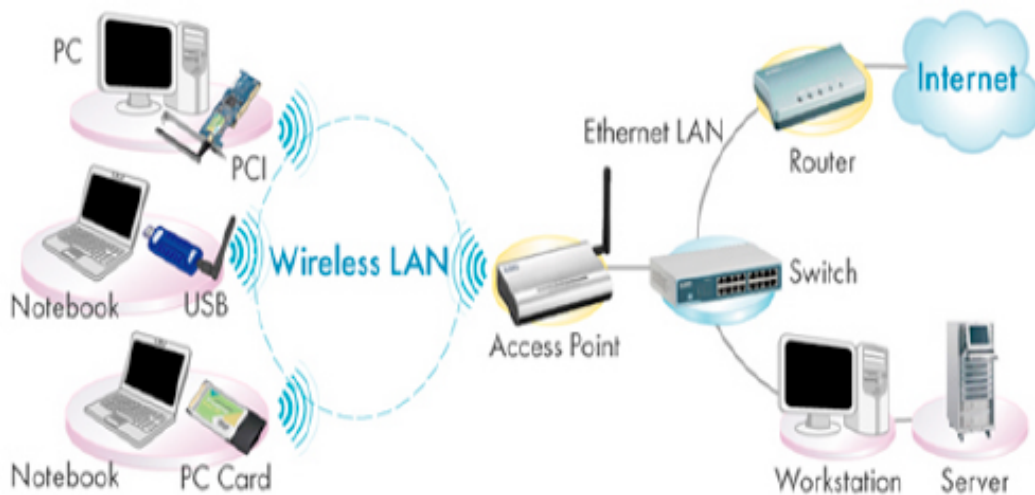
Un BSS pot intercanviar informació de dos modes diferents:

1 – Cada node es comunica amb l'altre node en forma directa i sense cap tipus de coordinació. Aquest mode s'anomena Ad-Hoc o IBSS (Independent Basic Service Set). Aquest mode sols permet la transmissió entre els nodes sense fils. Per tant dificulta la integració d'aquests nodes sense fils en una xarxa cablejada, donat el cas que fora necessari una ampliació de la xarxa.



*Figura 2.5. Esquema de connexió en mode Ad-Hoc [1]*

2 – Existeix un element anomenat AP (Access Point) que coordina la transmissió entre els nodes sense fils. Aquest mode s'anomena mode "Infraestructura" i permet vincular la xarxa sense fils amb la xarxa cablejada ja que el AP actua com a pont entre les dues xarxes. L'existència de diversos AP connectats a un sistema, que pot ser una LAN cablejada es el que anomenen EBSS (Extended Basic Service Set). La tecnologia 802.11 també permet el roaming entre els diferents AP.



*Figura 2.6. Esquema de connexió en mode Infraestructura [1]*

La seguretat és un tema important en les xarxes sense fils ja que, al contrari que en les xarxes cablejades a les que sols tenen accés les persones que físicament poden connectar-se, qualsevol persona del carrer o pisos o edificis veïns poden connectar-se a una xarxa sense fils o veure el contingut dels paquets que circulen per ella si esta no està convenientment protegida.

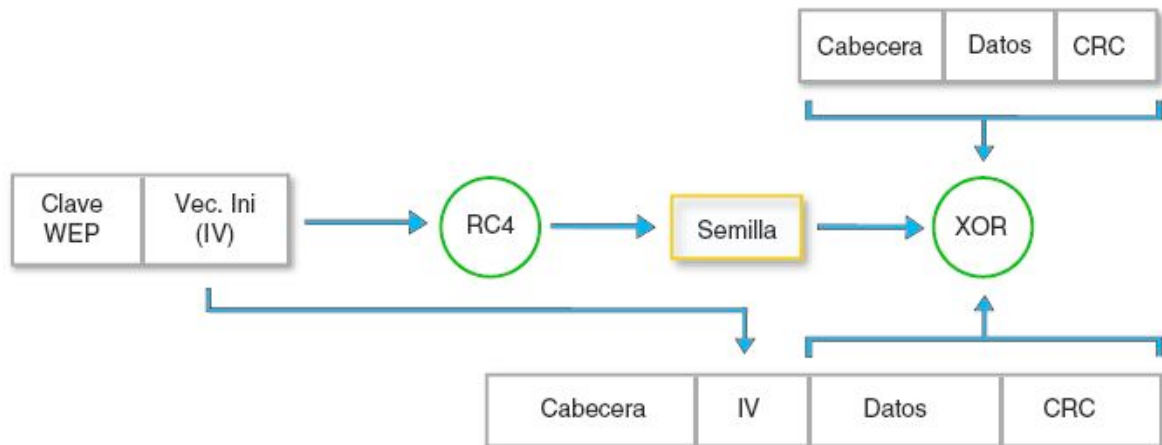
Alguns dels principals protocols estàndard per a proporcionar seguretat en xarxes sense fils IEEE 802.11 son: WEP i WPA.

### 2.3 Wep

WEP (Wired Equivalent Privacy) es el sistema de xifrat estàndard que es va utilitzar en un principi per al xifrat del protocol 802.11. Intenta donar a las xarxes sense fils la seguretat que tenen les xarxes cablejades.

WEP utilitza un algoritme anomenat RC4, que a partir de la clau WEP i d'un vector d'inicialització de 24 bits (que també s'anomena IV), generar una seqüència aleatòria, que s'anomena llavor, i que s'utilitzarà per a xifrar la comunicació amb el punt d'accés. Podem veure un esquema de l'algoritme en la figura 2.7.

El resultat es una trama en la que la capçalera i el vector d'inicialització van sense xifrar i les dades i el CRC van xifrats.



*Figura 2.7. Esquema d'enviament WEP. [1]*

Existeixen dos mètodes a través dels quals un usuari es pot autenticar amb un punt d'accés WEP:

- **Oberta (open):** L'estació pot autenticar-se sense la necessitat d'utilitzar la clau WEP, simplement en sol·licitar l'associació, el punt d'accés donarà per associada a l'estació. Després d'aquest procés d'autenticació l'estació sols podrà comunicar-se amb el punt d'accés si coneix la clau WEP utilitzada per a encriptar la comunicació.
- **Clau compartida (shared key):** Quan una estació envia una sol·licitud de associació al punt d'accés, aquest envia un text sense xifrar a l'estació, que s'anomena «desafio». El punt d'accés sols associarà a les estacions que retornen el text correctament xifrat amb la clau WEP.

Encara que pugui parèixer més segur shared key, no ho és, perquè qualsevol estació sense fils podria capturar tant el paquet de desafio com el mateix paquet xifrat i amb aquest informació associar-se correctament al punt d'accés i començar un atac al nostre punt d'accés. Es recomana utilitzar l'altre mètode d'accés.

Malgrat tot aquestes característiques, aquest sistema de xifrat presenta vulnerabilitats reconegudes com són:

- Debilitat del vector d'inicialització.

El vector d'inicialització es la part que varia de la clau, aquesta variació es produeix per tal que un atacant no pugui recopilar informació xifrada amb una mateixa clau. Però en l'estàndard no s'especifica aquesta variació. Per tant molts fabricants opten per fixar el IV en arrancar la targeta de xarxa i anar incrementant-la poc a poc. Aquesta configuració ocasiona que les primeres combinacions



de IVs i clau secreta es repeteixen molt freqüentment. Cosa que pot provocar el desxifrat dels missatges

- Identificació d'estacions

Aquestes s'identifiquen amb la clau compartida amb el AP, això permet reemplaçar estacions o realitzar atacs de DoS (Denegació de serveis). En aquest tipus d'atac es produeix que un servei o recurs sigui inaccessible als usuaris legítims, ja que es suplanta l'usuari legítim i es nega la comunicació al terminal que intenta connectar-se al AP mitjançant l'enviament de notificacions de des associació.

- Identificació de seqüències pseudoaleatòries iguals.

Ve donat per la debilitat dels algorismes de streaming i del RC4. Aquesta vulnerabilitat serveix per a realitzar atacs actius, com repeticions de paquets, injecció o permutació de bits, injecció de paquets encriptats, etc.

- Vulnerabilitat RC4

Fluhrer, Mantin y Shamir descobrien en agost del 2001 una debilitat del RC4. S'utilitza únicament el primer byte generat per la seqüència pseudoaleatòria amb l'objectiu d'obtenir la clau d'encriptació. A més ell mateix implementaren un sistema pràctic i econòmic per a aconseguir la clau amb la vulnerabilitat del RC4.

## 2.4 WPA

Els estàndards WPA i WPA2 tenen el seu objectiu en fer un procés d'autenticació i xifrat de comunicacions, el més segur possible. En ambdós estàndards es proposen dues solucions per a l'autenticació, una empresarial i l'altra adequada per a xicotetes empreses i per a domicilis particulars:

- **WPA Personal:** Utilitza un mètode d'autenticació que requereix compartir una clau entre totes les estacions de la xarxa. És més apropiat per a xicotetes empreses i per a domicilis particulars, perquè no requereix molta configuració, ni tampoc d'un servidor dedicat a realitzar la tasca.

Existeixen dos tipus d'encriptació en WPA:

- **TKIP (Protocol d'integritat de clau temporal):** És un protocol que a partir d'una clau (que no es la pre compartida) compartida entre el punt d'accés i totes les estacions, genera noves claus diferents per a cada client i renovables cada cert temps. Per tal d'aconseguir-ho, mescla la clau original amb l'adreça MAC i un vector d'inicialització. D'aquesta forma cada estació utilitza una clau independent per a

encriptar la comunicació.

- **AES (xifrat avançat estàndard):** Es un algoritme més robust i complex que TKIP.

La descripció de AES es simple si comptem amb tots els elements. Esta consisteix en dues parts, la primera el procés de xifrat i la segona en el procés de generació de les subclaus o extensió de la clau k. El bloc de xifrat té una longitud de 128 bits, la longitud de la clau K varia de 128, 192 i 256 bits, en cada cas AES té 10,12 i 14 rondes respectivament.

El procés de xifrat consisteix essencialment en la descripció de les quatre transformacions bàsiques de AES: ByteSub, ShiftRow, MixColumns, i AddRoundKey.

Es important mencionar que Aes està basa en Rijndael on les funcions o transformacions són lleugerament diferent en el procés de desxifrat. Per aprofundir més en el tema existeix la referència oficial [5].

En la següent figura es mostra una aproximació del funcionament.

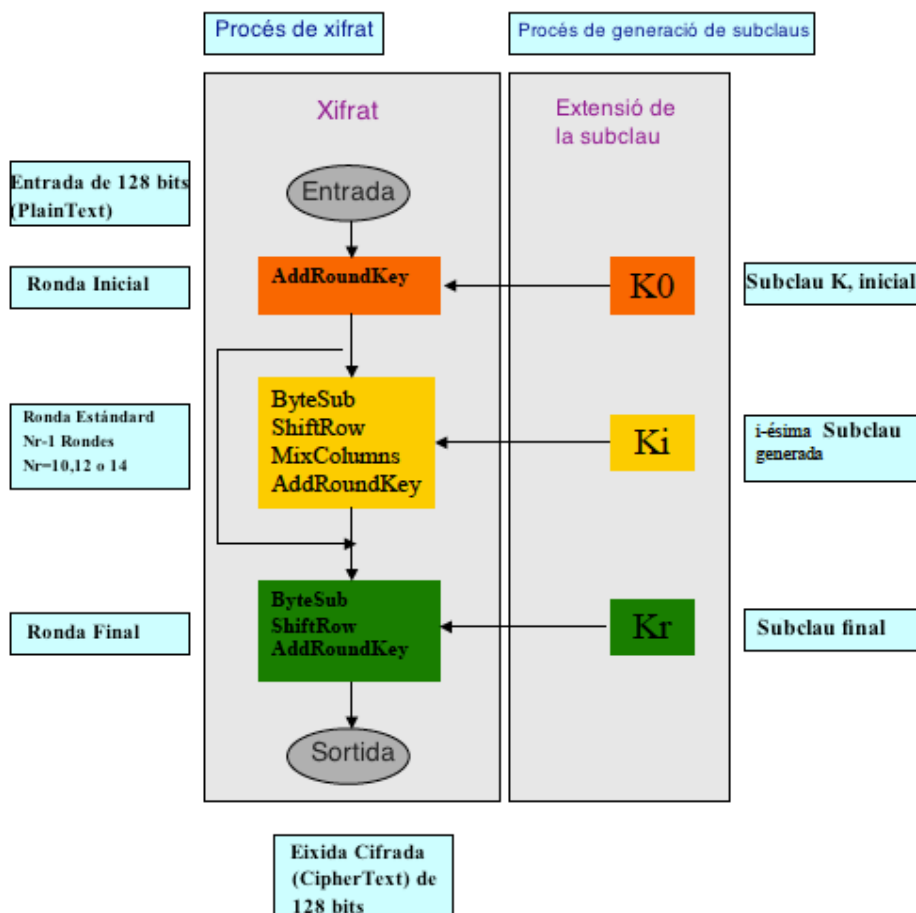


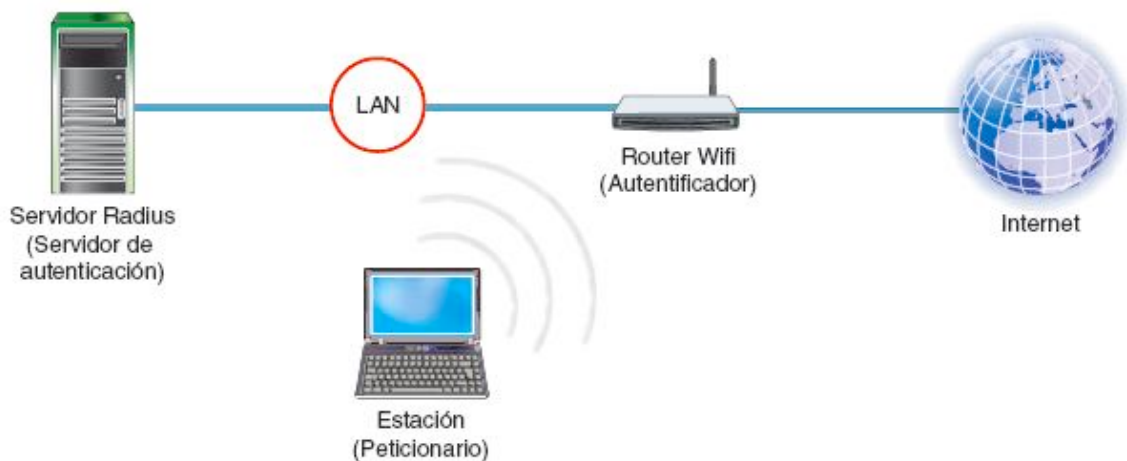
Figura 2.8. Funcionament de AES [4]

Es preferible utilitzar AES que TKIP, per ser aquest més avançat i segur. Com a desavantatge, requereix un maquinari més potent.

- **WPA2 Empresarial:** Requereix de la utilització d'un servidor RADIUS independent, per a gestionar l'autenticació dels usuaris mitjançant un usuari i contrasenya.

La estructura necessària per a poder utilitzar la arquitectura WPA empresarial es la que es mostra en la figura, següent.

Utilitzant la seguretat WPA2 empresarial s'augmenta la seguretat i la flexibilitat, ja que podem modificar la contrasenya d'un usuari o cancel·lar-lo sense que esta acció afecte a la resta d'usuaris. Açò suposa una millora notables respecte a WPA-PSK en xarxes amb molts usuaris.



*Figura 2.9. Esquema de connexió WPA2-empresarial [1]*

## 2.5 Servidor RADIUS

Com ja hem comentat abans RADIUS és un protocol que proporciona autenticació i autorització centralitzada per a l'accés a xarxes de tot tipus.

Al principi es va desenvolupar per donar accés telefònic remot, com indiquen les seues sigles. En l'actualitat s'utilitza per a multitud d'aplicacions.

Un dels principals usos de RADIUS el trobem en empreses que proporcionen accés a Internet o grans xarxes corporatives, en un entorno amb diverses tecnologies de xarxes (incloent mòdems, xDSL, VPNs i per suposat xarxes sense fils) no sols per a gestionar l'accés a la pròpia xarxa, sinó també per a serveis propis de Internet (com e-mail, Web o inclòs dins del procés de senyalització SIP en VoIP).

Una de les utilitzacions de RADIUS que volem destacar, al ser l'objectiu d'aquest projecte, és l'autenticació en xarxes sense fils (Wi-Fi), substituint mètodes més simples de clau compartida clau compartida (pre-shared key, PSK), que son prou limitats a l'hora de gestionar una xarxa, quan aquest arriba a una determinada grandària.

El funcionament és el següent:

Quan un client vol fer ús d'aquests serveis es connecta a un servidor d'accés a la xarxa (**NAS**) [pàgina 16] , que a la vegada es connecta a un servidor de AAA (autenticació, autorització i registre ,típicament RADIUS) preguntant si les credencials proporcionades per el client son vàlides. En base a la seua resposta, NAS li permetrà accedir o no a aquest recurs protegit. El sistema NAS no conte ninguna informació sobre els usuaris que se poden connectar ni les seues credencials, sinó que utilitza esta informació per a enviar-la a RADIUS, i que este li informe sobre els permisos del client.

Un altre avantatge de la utilització de RADIUS es que els seus clients tan sols tenen que implementar el protocol de comunicació amb RADIUS, i no totes les possibilitats de AAA existents (PAP, CHAP, LDAP, kerberos, mySQL, etc.) [glosari]. Per exemple, si tinguérem un punt d'accés, tan sols necessitem implementar una solució NAS que realitzi les consultes a RADIUS.

Un altre avantatge del protocol RADIUS es que, mentre es comunica amb NAS, mai transmet contrasenyes directament per la xarxa (el que es coneix com cleartext), ni tan sols en emprar PAP, sinó que usa algoritmes per a ocultar les contrasenyes como MD5. Malgrat no ser considerat MD5 un sistema de protecció de credencials molt segur, es aconsellable utilitzar sistemes addicionals de protecció per a xifrar el tràfic de RADIUS, com pot ser túnels de IPsec.

Encara que RADIUS és el protocol per a AAA més estes en l'actualitat existeix un altre protocol anomenat DIAMETER, que també ens proporciona control d'errors i comunicacions entre dominis.

Aquest protocol DIAMETER es desenvolupa com una millora respecte de RADIUS, i el seu nom és un joc de paraules respecte a RADIUS (Diametre = 2·Radio). El seu propòsit es donar cobertura a la nova arquitectura IMS (**IP Multimedia Subsystem**) [pàgina 15].

Les característiques principals incloses en el DIAMETER, que superen les limitacions de RADIUS inclouen:

- Operació a través de connexions fiables (TCP / SCTP). RADIUS funciona a través d'UDP que no proporciona connexions fiables, mentre que DIAMETER opera més sobre TCP o SCTP.
- Augment de la longitud dels atributs dels missatges. La longitud del atribut en RADIUS està limitada a un nombre de 255. Aquest nombre s'incrementa en DIAMETER fins a 3 octets .
- Servidor amb capacitat de commutació en cas d'error. La combinació de transport fiable i els missatges de manteniment de connexió, permet que els servidors de sistemes basats en DIAMETER puguin detectar i recuperar-se en cas de fallades de manera eficient.

## 2.6 Conclusions

Analitzada la situació de la qual partim en el institut, les infraestructures de les que disposem i les condicions que es reuneixen, en un centre d'educació secundària, hem d'arribar a la implementació d'una solució que aporti el major nombre de prestacions possible.

També és molt important la seguretat a l'hora d'utilitzar una xarxa sense fils, donat que poden accedir a la xarxa els edificis del carrer veïns al centre.

Vist que aquest projecte està enfocat per a implementar una xarxa sense fils, a la que podran accedir al voltant d'un centenar d'usuaris, cal triar una solució que implementi al màxim un bon nivell de seguretat utilitzant tot el que la tecnologia posa al nostre abast.

I per últim però no menys important el cost material que la solució suposi.

Una solució seria utilitzar un dispositiu que donés cobertura a l'edifici i que utilitzés una validació WPA2 que és més segura que WEP.

L'inconvenient d'aquesta solució és que la contrasenya és única, tots els usuaris tenen la mateixa contrasenya. Això vol dir que no podem restringir l'accés d'un usuari o grups d'usuaris, és a dir, o es connecten tots o no es pot connectar ningun d'ells.

Si el que volem és tenir control sobre quin usuari es pot connectar i quin no, la opció més adequada és WPA2 empresarial amb un servidor RADIUS que s'encarregui de validar quin usuari té accés.

L'elecció de RADIUS en lloc de DIAMETER, ve donada pel condicionament del hardware del dispositiu de connexió sense fils. Com es comentarà a l'estudi de viabilitat, es disposa per al projecte d'un Router sense fils que estava al centre i que suporta RADIUS. Com que no es disposa de dades fiables que permeten garantir el seu funcionament amb un servidor DIAMETER, encara que semblaria la opció més encertada, com hem vist a les seves característiques, ens decantem per l'opció d'un servidor RADIUS.

A més per a complementar aquesta solució, es pot afegir un servei de directori com Ldap, on tinguéssim definits tots els elements que formen part del centre, alumnes, professors, aules etc. De forma que es defineix una validació particular per a cadascun d'ells.

A més aquesta solució, pot venir complementada amb sistemes addicionals que aportin major seguretat com protocols EAP, con autenticació TLS o TTLS, servidors de túnels, etc.

## 2.7 Estudi de Viabilitat

El projecte no disposa de ningun pressupost, donat que en el centre educatiu no hi ha últimament cap ingrés que no sigui els ingressos indispensables per a les despeses de funcionament normals. És a dir que si hi ha alguna partida pressupostària va destinada a factures de llum, material d'oficina, personal de neteja, etc.

No disposem per tant de cap partida per a invertir en el projecte. Aleshores el que farem serà reutilitzar material que tenim al departament d'informàtica del centre.

Bàsicament necessitem un ordinador que pugui fer les funcions de servidor, i en el qual instal·larem el sistema operatiu i tot el programari que s'ha comentat abans.

A més necessitarem un punt d'accés que ens proporcioni accés sense fils als dispositius portàtils.

Els punts d'accés que tenim actualment en el institut no ens ofereixen la possibilitat de connectar amb un servidor RADIUS, però disposem en el centre d'un router wireless de la marca Lynksys, que si que ens ofereix la possibilitat de dirigir les peticions cap al ordinador

que farà les funcions de RADIUS.

Aquest dispositiu no s'utilitza al centre perquè va ser substituït per un altre router amb més prestacions que va vindre de dotació al principi del curs escolar.

No estariem aprofitant totes les prestacions de les quals disposa el router, ja que sols faria la funció de punt d'accés, però en contraprestació, estem utilitzant-lo per a donar un servei de punt d'accés.

Disposem per tant de tot el material necessari per al projecte, a un cost zero.

Per una altra part, els avantatges que ens aportaria són significatius, perquè donaria cobertura segura a tots els alumnes que venen en els seu dispositius portàtils.

Un altres dels avantatges, seria que el manteniment estaria centralitzat en un únic dispositiu, el servidor RADIUS. A més podríem utilitzar aquest servidor amb funcionalitats addicionals com servidor d'adreces IP o servidor de noms.

### 3. Configuració del Servidor RADIUS

#### 3.1 Instal·lació del Sistema Operatiu

Abans de res hem de decidir i descarregar la versió del sistema operatiu a emprar. S'utilitzarà una imatge Desktop de **Ubuntu 10.04 Lucyd Lynx**, ja que es una versió LTS (amb suport a llarg termini). En començar aquest projecte encara no estava disponible la versió 12.04.

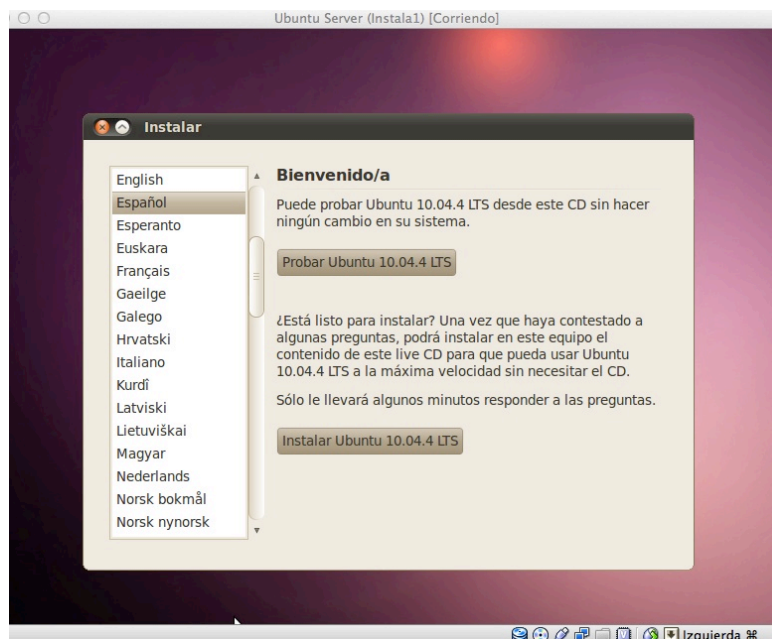
Una vegada descarregada la imatge podem o generar un Cd o fer una imatge auto-arrancable amb un dispositiu usb.

En iniciar el ordenador amb el cd o el dispositiu usb, començarà el procés. La primera pantalla que ens mostrarà serà la de selecció de idioma, seleccionem el que desitgem (espanyol, català, esperanto...) i ens mostra un menú que ens permetrà començar la instal·lació directament o arrancar en mode "live", que es un mode prova que no afecta a res del que està instal·lat a la màquina.

Si seleccionem instal·lar, el procés començarà a continuació.

En el primer pas ens demanarà la selecció de l'idioma de instal·lació.

Seleccionem el idioma que desitgem i polsem Endavant.



*Figura 3.1. Instal·lació Ubuntu 10.04. Selecció de l'idioma*

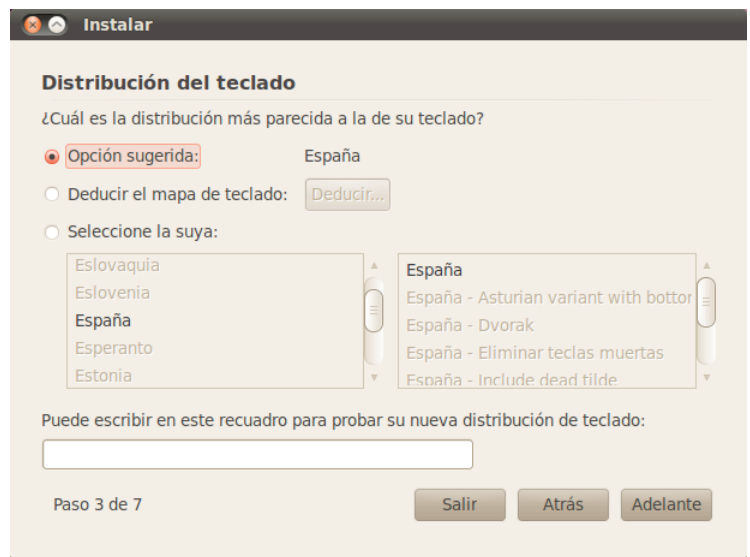
Després caldrà configurar la zona horària, si no sorgeix per defecte triarem Madrid.





*Figura 3.2. Instal·lació Ubuntu 10.04. Selecció de la ubicació*

El següent pas serà seleccionar la distribució del teclat al nostre equip, que per general es España-España. En la part inferior podem provar que funciona correctament polsant sobre tecles com la ñ, la coma, punt i coma...



*Figura 3.3. Instal·lació Ubuntu 10.04. Selecció de la distribució teclat*

En este pas seleccionarem el disc o partició on instal·lar Ubuntu. En el nostre cas disposem d'un disc sencer per al nostre servidor per tant tenim dues opcions "Borrar y usar disco entero" o "Especificar particiones manualmente". Triarem aquesta última per que ens dona la possibilitat de crear les particions de la forma que considerem més escaient. A més el programari d'instal·lació ens proporciona una interfície gràfica que ens permet gestionar les particions.

Cal tenir en compte que les particions que utilitza **GNU/Linux** son un tant diferents i per a poder funcionar i instal·lar el sistema operatiu necessitem almenys dues particions, una per al sistema de fitxers i altra per a l'àrea d'intercanvi que s'anomena **SWAP** i que és semblant a una memòria virtual. Es recomana assignar el mateix espai que memòria **RAM** disposi l'equip. Avui en dia com que els equips disposen de prou memòria aquest valor és aproximat.

A més crearem també una partició addicional /home, on muntarem les dades dels usuaris, per si de cas, calgués reinstal·lar el sistema, no perdérem les dades dels usuaris.

La partició per al sistema de fitxers és la que s'utilitza per a guardar dades, programes etc. Existeixen diferents sistemes que podem triar: **ext2, ext3, ext4 ReiserFS, XFS...** El més estès en **GNU/Linux** es el **ext4**.

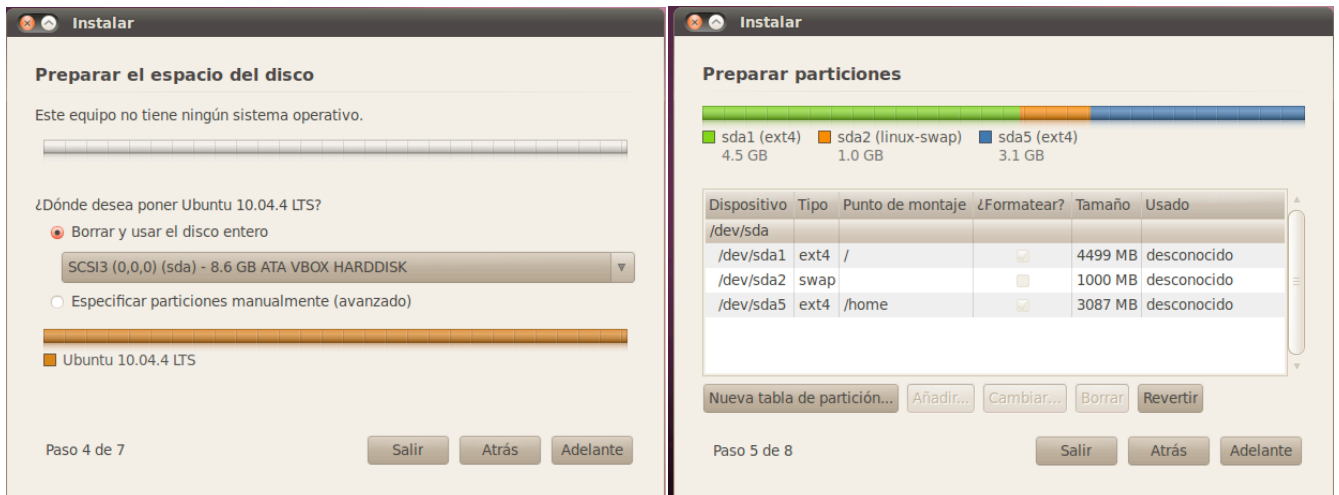


Figura 3.4. Instal·lació Ubuntu 10.04. Esquema de Particionat del disc

Tan sols queda introduir els paràmetres per a la creació d'un usuari que tindrà permisos d'administrador. I a més configurarem el nom de l'equip.

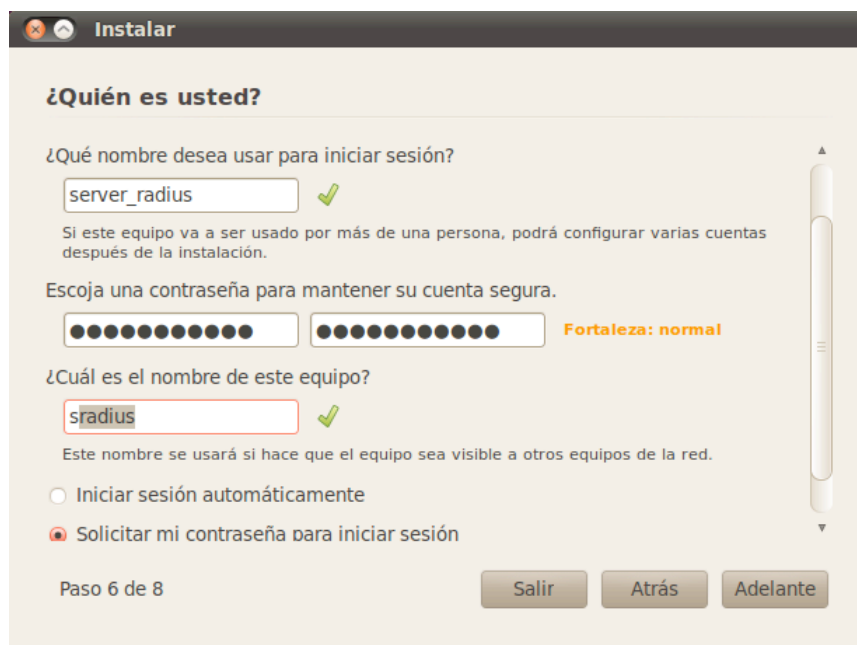
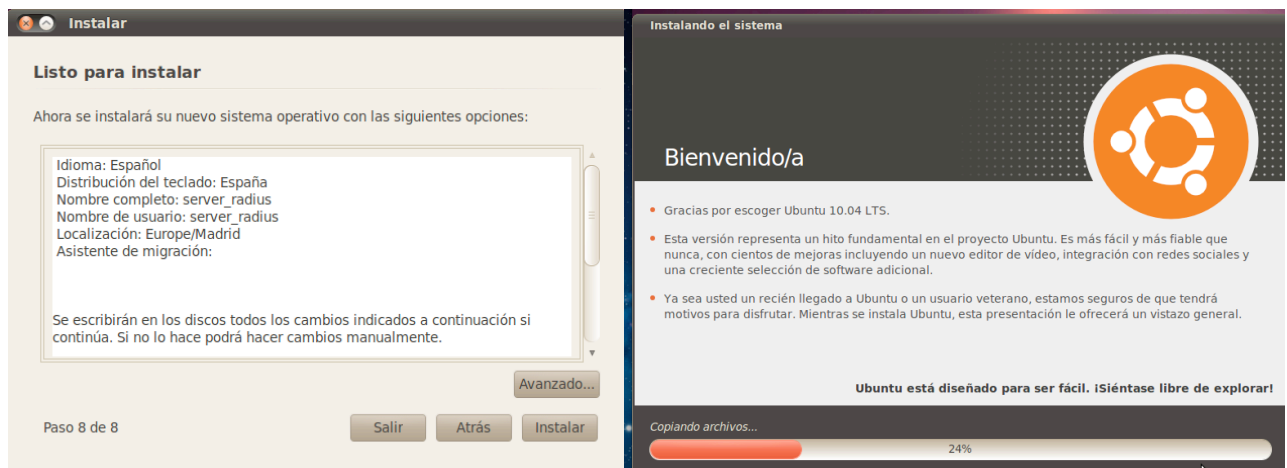


Figura 3.5. Instal·lació Ubuntu 10.04. Definició Usuari i nom d'equip.

Tan sols queda confirmar els paràmetres i que es copien els arxius.



*Figura 3.6. Instal·lació Ubuntu 10.04. Confirmació i copia d'arxius.*

## 3.2 Configuració de la xarxa

Com que el servidor ha de ser accessible per a qualsevol equip de la xarxa haurem de configurar una adreça IP Estàtica

Cal editar el fitxer: **/etc/network/interfaces**

Podeu utilitzar qualsevol de les següents comandes:

```
$ sudo nano /etc/network/interfaces  
$ sudo vi /etc/network/interfaces
```

O si disposeu d'entorn gràfic:

```
$ gedit /etc/network/interfaces
```

Dins del fitxer hem de posar el següent:

```
auto eth0  
iface eth0 inet static  
address 192.168.0.253  
gateway 192.168.0.1  
netmask 255.255.255.0  
network 192.168.0.0  
broadcast 192.168.0.255
```

Després de canviar els paràmetres de xarxa cal executar la següent comanda per tal que els canvis tinguin efecte:

```
$ sudo /etc/init.d/networking restart
```

O també podem apagar i tornar a encendre la interfície de xarxa:

```
$ sudo ifdown eth0  
$ sudo ifup eth0
```

També es podria configurar de forma gràfica a través del network manager, que és un gestor gràfic de configuració de la xarxa.



*Figura 3.7. Configuració de la interfície gràfica.*

### 3.3 Instal·lació i configuració del servidor de DHCP

El protocol de configuració dinàmica de host (DHCP, Dynamic Host Configuration Protocol) és un estàndard TCP/IP dissenyat per a simplificar l'administració de la configuració IP dels equips de la nostra xarxa.

Si disposem d'un servidor DHCP, la configuració IP dels equips pot fer-se de forma automàtica sense necessitat de fer-ho manualment.

Un servidor DHCP és un servidor que rep peticions de clients sol·licitant una configuració de xarxa IP. El servidor respondrà a les dites peticions proporcionant els paràmetres que permeten als clients auto configurar-se.

Perquè un equip sol·liciti la configuració a un servidor, en la configuració de xarxa dels ordinadors cal seleccionar l'opció 'Obtenir direcció IP automàticament'.

El servidor proporcionarà al client almenys els paràmetres següents: Adreça Ip i Màscara de subxarxa.

Opcionalment, el servidor DHCP podrà proporcionar altres paràmetres de configuració com ara la porta d'enllaç o gateway, servidor DNS, duració de la concessió, etc.

Per tal d'instal·lar el servidor DHCP utilitzem la següent comanda des de la consola de root:

```
# apt-get install dhcp3-server
```

Igual que totes les aplicacions en Linux, el servidor DHCP disposa del seu propi arxiu de configuració.

Es tracta de l'arxiu: **/etc/dhcp3/dhcpd.conf**

Este arxiu de configuració consta d'una primera part principal on s'especifiquen els paràmetres generals que defineixen les concessions i els paràmetres addicionals que es proporcionaran al client.

Els rangs d'adreces IP s'especifiquen en seccions que comencen amb la paraula clau 'subnet' seguit de l'adreça de xarxa de la subxarxa, contínuament amb la paraula 'netmask' seguit de la màscara de xarxa. A continuació estarà la llista de paràmetres per a la dita secció tancats entre claus.

Per al nostre cas en concret concedirem IP als clients que es connecten a la xarxa, per sobretot als que es connecten per wifi.

Com que els servidors d'aula i els servidors proxy, moodle, etc tenen adreces de xarxa inferiors a 192.168.0.100, podem configurar el rang d'adreces per als equips portàtils entre la 192.168.0.101 i la 192.168.0.250.

L'editem:

```
$ gedit /etc/dhcp3/dhcpd.conf
```

Si a més de proporcionar l'adreça IP, la màscara i la porta d'enllaç, introduïm els nostre servidor que realitzarà les funcions de dns per tal que resolgui les peticions o un extern en cas alternatiu, l'arxiu de configuració quedaria de la següent forma:

```
// Rango de cesión y parámetros adicionales
subnet 192.168.0.0 netmask 255.255.255.0 {
option routers 192.168.0.1;
option domain-name-servers 192.168.0.253, 80.58.0.33, 8.8.8.8;
range 192.168.0.101 192.168.0.250;
}
```

Després de canviar els paràmetres de xarxa cal executar la següent comanda per tal que els canvis tinguin efecte:

```
$ sudo /etc/init.d/dhcp3-server restart
```

### 3.4 Instal·lació i configuració del servidor DNS

Cada equip i cada servidor connectat a Internet, disposa d'una direcció IP i d'un nom pertanyent a un domini.

Internament, la comunicació entre els PCs es realitza utilitzant adreces IP per això és necessari algun sistema que permeti, a partir dels noms dels PCs, esbrinar les direccions IPs dels mateixos.

Per exemple, quan volem accedir al nostre servidor ldap-radius, en la barra del navegador escrivim: `http://sradius.ieseljust.edu` el nostre PC haurà d'esbrinar quina és la IP corresponent a `www.upv.es` i una vegada que ha esbrinat que la seua IP és 192.168.0.253, podem accedir a tots els serveis que ens proporciona aquest servidor.

Per a facilitar aquesta resolució instal·larem un servidor de DNS (Domain Name Server). En aquest cas instal·larem el més utilitzat en els servidors Linux, el bind9.

```
$ sudo apt-get install bind9
```

Una vegada feta la instal·lació haurem de configurar el servidor. Haurem d'indicar-li quin són els fitxers on implementarem les resolucions directes i les inverses. Aquesta informació es troba al fitxer **/etc/bind/named.conf.local**.

L'editarem i li afegirem les següents línies per a indicar-li la zona de recerca directa e inversa:

```
//Arxiu per a recerques directes
zone "ieseljust.edu" {
    type master;
    file "/etc/bind/ieseljust.db";
};

// Arxiu per a recerques inverses
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.rev";};
```

Una vegada definit on es trobarà la informació de resolució, haurem de crear els arxius Creem l'arxiu **ieseljust.db** on configurarem el zona de cerca directa. Posarem tres alumnes de mostra però en aquest arxiu podríem definir els ordinadors als quals tenim accés per nom, com servidors d'aula, moodle correu, etc.

Editarem l'arxiu **/etc/bind/192.rev** i podríem escriure la configuració de la següent forma:

```
; BIND data file for ieseljust.edu
;
@      IN      SOA    ieseljust.edu. root.ieseljust.edu. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Default TTL
                                IN      NS      dns.ieseljust.edu.
serveraula1  IN      A      192.168.0.101
correu      IN      A      192.168.0.22
www         IN      A      192.168.0.21
proxy       IN      A      192.168.0.20
dns         IN      A      192.168.0.253
sradius     IN      A      192.168.0.253
```

Per últim crearem l'arxiu **192.rev** on configurarem la zona de recerca inversa i que ens

permetrà obtenir la resolució d'un nom, a partir de la seua adreça Ip.

```
;  
; BIND reverse data file for 192.168.0.0  
;  
@      IN      SOA      ieseljust.edu. root.ieseljust.edu. (  
                                1          ; Serial  
                                604800     ; Refresh  
                                86400      ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Default TTL  
                                IN      NS      dns.ieseljust.edu.  
101    IN      PTR      alumne1. ieseljust.edu.  
11     IN      PTR      cliente2. ieseljust.edu.  
22     IN      PTR      cliente3. ieseljust.edu.  
21     IN      PTR      cliente4. ieseljust.edu.  
20     IN      PTR      www. ieseljust.edu.  
253    IN      PTR      dns. ieseljust.edu.  
253    IN      PTR      sradius. ieseljust.edu.
```

Necessitem a més fer unes modificacions en dos fitxers més, per a completar la configuració. Primera modificarem l'arxiu `/etc/resolv.conf` i afegirem aquestes 2 línies:

```
nameserver 127.0.0.1 // per a reconèixer-nos com a servidor dns  
search ieseljust.edu // per a que cerque per defecte en el nostre domini
```

Ara sols ens queda redirigir les peticions que no són dels nostre domini, cap un servidor de noms que tingui la capacitat per a resoldre les peticions externes.

Caldrà per tant modificar l'arxiu `/etc/bind/named.conf.options` i afegim la següent línia:

```
forwarders {  
    192.168.0.254;  
};
```

Per últim sols quedaria reiniciar el servidor per tal que resolgui les peticions de forma com hem configurat:

```
$sudo /etc/init.d/bind9 restart
```



## 3.5 Instal·lació i configuració de LDAP

**OpenLDAP** es una implementació lliure i de codi obert del protocol Lightweight Directory Access Protocol (LDAP) desenvolupada pel projecte OpenLDAP. Està alliberada sota una llicència pròpia OpenLDAP Public License. LDAP es un protocol de comunicació independent de la plataforma, així podem trobar moltes distribucions GNU/Linux que inclou software o suport per a LDAP. Tanmateix aquest protocols està implementat i suportat per altres plataformes com BSD, HP-UX, Mac OS X, Solaris, Microsoft Windows (en moltes de les seues variants, tan en la versió servidor com usuari).

**LDAP** és un servei de directori (on un directori és un conjunt d'objectes que tenen uns determinats atributs ), ordenat de manera lògica i distribuït, per a buscar certa informació en un entorn de xarxa.

Un arbre de directori LDAP pot reflectir límits polítics, geogràfics o organitzacionals. Actualment LDAP tendeix a usar noms DNS per a estructurar els nivells més alts de la jerarquia. A mesura que anem baixant en el directori poden aparèixer entrades que representen persones, unitats organitzacionals, impressores, documents, grups de persones o qualsevol cosa que representa una entrada en l'arbre.

Normalment també s'emmagatzema la informació d'autenticació (usuari i contrasenya) y es utilitzat per a autenticar-se, encara que es possible emmagatzemar altra informació (dades de contacte de l'usuari, ubicació de diversos recursos de la xarxa, permisos, certificats, etc).

### 3.5.1 Components

Bàsicament, OpenLDAP posseeix tres components principals:

- slapd – (slapd, Standalone LDAP Daemon) Dimoni servidor
- Biblioteques que implementen el protocol LDAP
- Programes client i utilitats de gestió: ldapsearch, ldapadd, ldapdelete, entre altres

### 3.5.2 Backends

L'arquitectura del servidor OpenLDAP està dividida entre una secció frontal anomenada **frontend** que s'encarrega de les connexions de xarxes i el processament del protocol, i una

base de dades dorsal o de segon plànol (**backend**) que tracta únicament amb l'emmagatzemament de dades. La arquitectura és modular i existeix una gran varietat de backends disponibles per a interactuar amb altres tecnologies, no tan sols en bases de dades tradicionals.

Existeixen al voltant de 16 backends diferents, proporcionats per la distribució d'OpenLDAP i que s'agrupen en tres categories diferents

- Backends d'emmagatzemament de dates
- Proxy backends
- Backends dinàmics

### 3.5.3 Característiques i avantatges

Es pot considerar LDAP com una base de dades optimitzada per a fer un nombre molt alt de lectures i poques escriptures o modificacions. A més com que està organitzat de forma jeràrquic, es pot també emmagatzemar informació dels usuaris.

Per exemple podem guardar informació com el login, UID, GID, contrasenya, etc. Inclòs podem afegir-li una foto, telèfon de casa i molt tipus d'informació addicional que es necessiti.

En el nostre cas particular ens centrarem en guardar la informació necessària per a un servidor d'autenticació.

Encara que també es podria configurar com un directori compartit o una llibreta d'adreces per a clients de correu electrònic.

Per motius de seguretat es recomanable disposar d'un servidor centralitzat d'autenticació. Durant molt de temps en el mon de Unix s'ha emprat NIS (**Network Information Service**), que és un protocol de servei de directoris client- servidor per a l'enviament de dades de configuració en sistemes distribuïts. Però actualment ja quasi no s'utilitza i es troba en desús. Ara es recomana LDAP per tractar-se d'un sistema més modern i segur.

Entre les implementacions de LDAP més conegudes per a sistemes Linux/Unix tenim OpenLDAP que a més es pot integrar amb clients Windows.

Anem a veure com podem muntar un servei centralitzat d'autenticació amb OpenLDAP.

### 3.5.4 Instal·lació del servidor LDAP i carrega d'informació del directori

En primer lloc, instal·larem el dimoni servidor **slapd**, i a més instal·larem el paquet **ldap-utils** que conté els serveis LDAP de gestió:

```
$ sudo apt-get install slapd ldap-utils
```

Per defecte **slapd** està configurat amb les opcions mínimes que permeten arrancar i executar el dimoni **slapd**.

L'exemple de configuració ve definit com `dc=ejemplo, dc=com`. Aquest nom ha de coincidir amb el nom de domini del servidor. En el nostre cas particular, donat que la màquina té el nom de domini complet (FQDN) `sradius.ieseljust.edu`, el sufix serà `dc=ieseljust, dc=edu`.

Per tant fixarem l'arrel del directori LDAP, **dc=ieseljust,dc=edu** que serà la que ens proporcionarà el nostre servidor `sradius.ieseljust.edu`, con IP: 192.168.0.253.

### 3.5.5 Backend de OpenLDAP

**OpenLDAP** utilitza un directori independent (`/etc/ldap/slap.d/cn = config`) que conte l'arbre d'informació de directori, (Directory Information Tree, DIT). El **cn = config DIT** s'utilitza per a configurar dinàmicament el **slapd** dimoni, el que permet la modificació d'esquemes, índex, ACL, etc. sense parar el servei.

Com que la configuració és mínima, haurem de carregar configuracions addicionals per tal de poder carregar després el frontend. Per tant farem una càrrega inicial que sigui compatible amb la llibreta d'adreces i amb comptes Posix (aquest comptes permeten l'autenticació de varies aplicacions, des de clients Linux de la nostra xarxa, com aplicacions web, clients de correu, ssh, etc.).

El LDAP Data Interchange Format (LDIF) és un format que s'utilitza per a la importació i exportació de dades independentment del servidor LDAP que s'estigui utilitzant.

Cada servidor LDAP té una o diverses maneres d'emmagatzemar físicament les seues dades en el disc, per açò que LDIF proveeix una manera d'unificar la manera de tractar les dades i així poder migrar d'un servidor a un altre sense importar que classe d'implementació és.

El format LDIF és simplement un format de text ASCII per a entrades LDAP, que té la manera següent:

```
dn: <nom distinguit>
<nom_tribut>: <valor>
<nom_tribut>: <valor>
<nom_tribut>: <valor>
```

Utilitzarem la comanda `ldapadd`, que ens permetrà afegir la informació del fitxer, que tenen un format LDIF, al nostre servidor Ldap.

```
$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f backend.ieseljust.ldif
```

El fitxer `backend.ieseljust.ldif` conté la següent informació:

```
# Load dynamic backend modules
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module olcModulepath: /usr/lib/ldap
olcModuleload: back_hdb.la

# Database settings
dn: olcDatabase={1}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcSuffix: dc=ieseljust,dc=edu
olcDbDirectory: /var/lib/ldap
olcRootDN: cn=admin,dc=ieseljust,dc=edu
olcRootPW: radius
olcDbConfig: set_cachesize 0 2097152 0
olcDbConfig: set_lk_max_objects 1500
olcDbConfig: set_lk_max_locks 1500
olcDbConfig: set_lk_max_lockers 1500
olcDbIndex: objectClass eq
olcLastMod: TRUE
olcDbCheckpoint: 512 30
olcAccess: to attrs=userPassword by dn="cn=admin,dc=ieseljust,dc=edu" write by anonymous auth by self write by * none
olcAccess: to attrs=shadowLastChange by self write by * read
olcAccess: to dn.base="" by * read
olcAccess: to * by dn="cn=admin,dc=ieseljust,dc=edu" write by * read
```

Una vegada que ja hem posat el backend (és a dir tot allò que fa referència a la base de dades) podem introduir les dades relatives al frontend.

La informació en LDAP s'emmagatzema mitjançant objecte que son construïts a partir de classes definides en els esquemes. Anem a analitzar el fitxer anterior:

```
dn: cn=admin,dc=ieseljust,dc=edu
```

```
objectClass: organizationalRole
objectClass: simpleSecurityObject
cn: admin description: LDAP administrator
userPassword: admin
```

Elements del fitxer frontend:

- En primer lloc tenim el nom unívoc (Distinguished Name) de l'objecte: "cn=admin, dc=ieseljust,dc=edu". Sempre anirà acompanyat del sufix que hem especificat en la configuració (en aquest cas "dc=ieseljust,dc=edu").
- L'objecte tindrà els atributs de les classes 'organizationalRole' i 'simpleSecurityObject'. Aquestes classes es troben definides en els esquemes '/etc/ldap/schema/' que es carreguen per LDAP en iniciar-se. Un objecte pots estar compost per tantes classes auxiliars (per exemple simpleSecurityObject) i abstractes (per exemple top) com es necessiti però sols pot haver una de tipus estructural (organizationalRole en aquest cas).
- Finalment es llisten els atributs, en aquest cas, 'cn', 'description' i 'userPassword'.

Tots els objectes en LDAP segueixen sempre aquesta estructura, que es prou diferent de les típiques bases de dades relacionals (SQL). Una altra diferència important respecte a aquestes bases de dades, és que LDAP està optimitzat per a realitzar consultes de lectura molt ràpides, per això LDAP s'utilitza en entorns on les dades no es modifiquen freqüentment.

L'arxiu que conté tota aquesta informació s'anomena frontend.ieseljust.ldif i conte la següent informació:

```
//Crear el nodo raiz
dn: dc=ieseljust,dc=edu
objectClass: top
objectClass: dc
Object objectclass: organization
o: ieseljust org
dc: ieseljust
description: LDAP ieseljust
# Usuario administrador
dn: cn=admin,dc=ieseljust,dc=edu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: radius
```

```
dn: ou=people,dc=ieseljust,dc=edu
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=ieseljust,dc=edu
objectClass: organizationalUnit
ou: groups

dn: uid=maite,ou=people,dc=ieseljust,dc=edu
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: maite sn: marti
givenName: maite cn: maite marti
displayName: maite marti
uidNumber: 2000
gidNumber: 2000
userPassword: password
gecos: maite marti
loginShell: /bin/bash
homeDirectory: /home/maite
shadowExpire: -1
shadowFlag: 0
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
mail: mmarti@ieseljust.edu
postalCode: 46410 l: Valencia
o: ieseljust edu
mobile: +34 (0)7 xx xx xx xx
homePhone: +34 (0)1 xx xx xx xx
title: System Administrator
initials: NE

dn: cn=radius,ou=groups,dc=ieseljust,dc=edu
objectClass: posixGroup
cn: radius
gidNumber: 2000
```

Com podem veure en aquesta configuració he creat dues unitats organitzatives, “groups” i “people”, el compte de l’administrador, un usuari “maite” i un element dins del grup “groups”.

Ara tan sols queda afegir aquestes entrades al directori LDAP, amb la següent comanda:

```
$ sudo ldapadd -x -D cn=admin,dc=ieseljust,dc=edu -W -f frontend.ieseljust.ldif
```

Que ens proporciona la següent sortida:

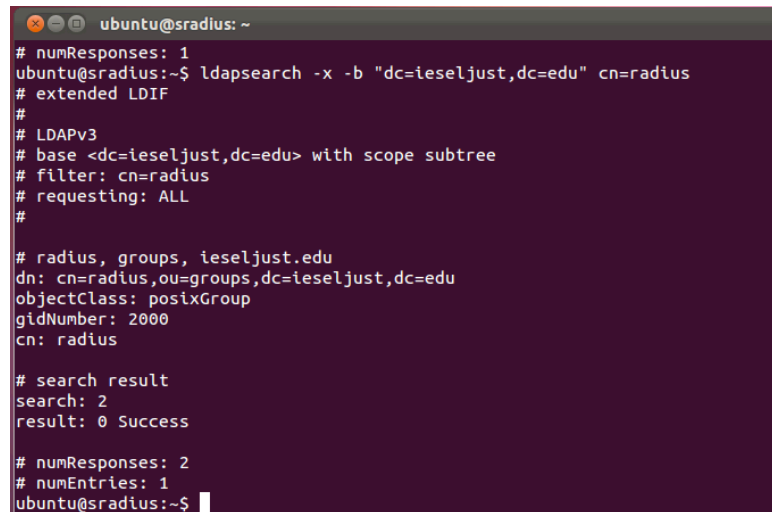
```
ubuntu@ubuntu@sradius:/etc/ldap$ sudo ldapadd -x -D
cn=admin,dc=ieseljust,dc=edu -W -f frontend.ieseljust.ldif
Enter LDAP Password:
adding new entry "dc=ieseljust,dc=edu"
adding new entry "cn=admin,dc=ieseljust,dc=edu"
adding new entry "ou=people,dc=ieseljust,dc=edu"
adding new entry "ou=groups,dc=ieseljust,dc=edu"
adding new entry "uid=maite,ou=people,dc=ieseljust,dc=edu"
adding new entry "cn=radius,ou=groups,dc=ieseljust,dc=edu"
```

Podem comprovar que el contingut s'ha introduït correctament amb la utilitat `ldapsearch` que serveix per a realitzar recerques dins del directori.

Executem una recerca en el directori utilitzant els següents modificadors:

- `-x`: no utilitzarà el mètode d'autenticació SASL, es el per defecte.
- `-b`: base en la qual es realitzarà la recerca.

```
$ ldapsearch -x -b "dc=ieseljust,dc=edu" cn=radius
```



```
ubuntu@sradius: ~
# numResponses: 1
ubuntu@sradius:~$ ldapsearch -x -b "dc=ieseljust,dc=edu" cn=radius
# extended LDIF
#
# LDAPv3
# base <dc=ieseljust,dc=edu> with scope subtree
# filter: cn=radius
# requesting: ALL
#
# radius, groups, ieseljust.edu
dn: cn=radius,ou=groups,dc=ieseljust,dc=edu
objectClass: posixGroup
gidNumber: 2000
cn: radius
# search result
search: 2
result: 0 Success
# numResponses: 2
# numEntries: 1
ubuntu@sradius:~$
```

*Figura 3.8. Resultat de la recerca d'un usuari al servei de directori*

### 3.5.6 Control d'accés a LDAP (olcAccess)

L'autenticació requereix accés al camp de la contrasenya. Aquest camp no deuria d'estar accessible per defecte.

També, s'ofereix la possibilitat que els usuaris puguin canviar la seua contrasenya amb el comandament `passwd` o alguna altra utilitat, per tant "`shadowLastChange`" necessita ser

accessible una vegada que el usuari s'hagi autenticat.

Per a tot això s'utilitzen les llistes de control d'accés, que el que fan es concedir o denegar permisos a alguns usuaris, per tal que puguin llegir, escriure o tindre control total.

Per tal de veure quines llistes de control d'accés tenim definides en el nostre directori, disposem d'una utilitat anomenada **ldapsearch**.

Si utilitzem la comanda que apareix a continuació, ens mostrarà que la llista de control d'accés que tenim aplicada, és la bàsica. Els usuaris autenticats, tenen permís de lectura, mentre que l'usuari administrador té permís tan de lectura com d'escriptura.

```
$ ldapsearch -xLLL -b cn=config -D cn=admin,cn=config -W olcDatabase=hdb olcAccess
```

```
Enter LDAP Password:
dn: olcDatabase={1}hdb,cn=config
olcAccess: {0}to attrs=userPassword,shadowLastChange by
dn="cn=admin,dc=ieseljust,dc=edu" write by anonymous auth by self write
by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=ieseljust,dc=edu" write by * read
```

### 3.5.7 Administració gràfica de OpenLDAP

Existeixen varies ferramentes gràfiques que faciliten l'administració d'OpenLDAP, com per exemple qq, JXplorer, LAT, phpLdapAdmin.

De totes aquest s'ha escollit dues per la seua popularitat i facilitat d'utilització, LAT (Ldap Administration Tools) i phpLdapAdmin.

Amb els dos programes gràfics han sorgit una sèrie d'inconvenients, amb els fitxers .xml i altres problemes de compatibilitat, que provocaven que sols es pogués llegir al servei de directori i no es podia escriure.

Després de dues setmanes de fer intents per solucionar-ho, es va arribar a la conclusió que eren unes incompatibilitats no resoltes amb la versió 10.04 del sistema operatiu Ubuntu.

Aleshores com que ja havia sorgit la nova versió d'Ubuntu la 12.04, es va procedir a la instal·lació tan del sistema operatiu, com de la resta de serveis que s'ha mencionat als apartats anteriors.



Aquesta instal·lació està documentada a l'annex I d'aquest document.

El principal inconvenient ha estat, el retard que ha sofert el projecte respecte de les previsions inicials.

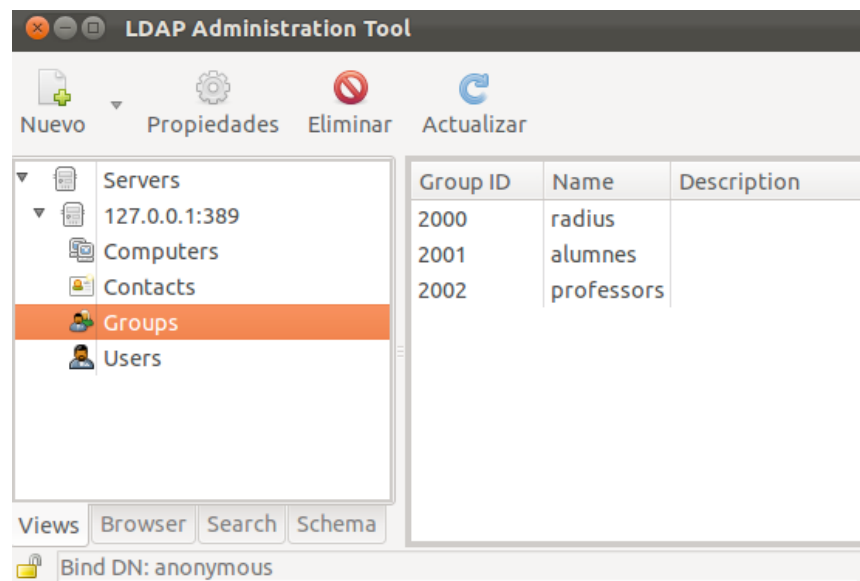
Una vegada comentat aquest incident, es continua sense cap problema amb la instal·lació dels dos programes d'administració gràfica del servei de directori, que s'havia comentat al principi d'aquest apartat.

El primer és un programa que es connecta a l'adreça Ip i port del servidor directament, mentre que el segon utilitza una interfície web per tal de connectar-se i necessita també d'un servidor apache que instal·la el programa mateix, per tal de funcionar.

Per instal·lar LAT:

```
$ sudo apt-get install lat
```

Ja no fa falta cap configuració addicional. Simplement l'executem i posem l'adreça del servidor a qui es connecta.



*Figura 3.9. Interfície gràfica LAT*

Per a instal·lar la segona ferramenta haurem d'executar la següent comanda:

```
$ sudo apt-get install phpldapadmin
```

editar `/etc/phpldapadmin/config.php` i cal canviar on apareix `dc=example,dc=com` per el

domini a configurar

```
$servers->setValue('server','base',array('dc=ieseljust,dc=edu'));  
$servers->setValue('login','bind_id','cn=admin,dc=ieseljust,dc=edu');
```

Una vegada canviat açò accedim al programa a través del navegador, posant l'adreça IP o el nom del servidor <http://sradius.ieseljust.edu/phpldapadmin>

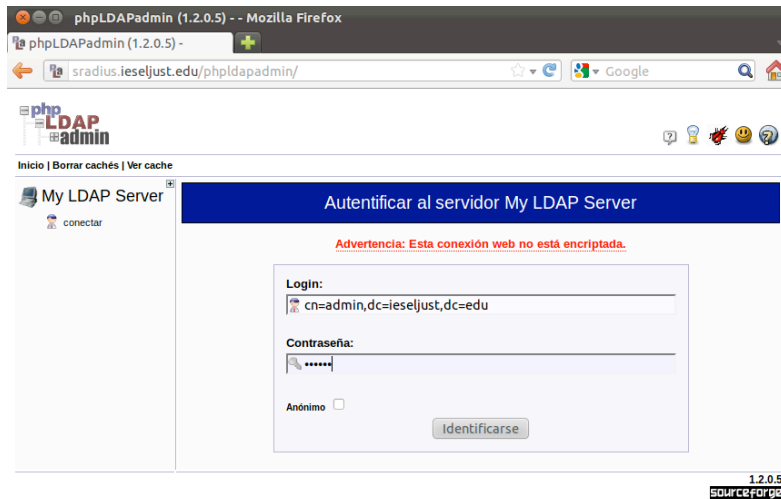


Figura 3.10. Administració de LDAP amb phpLDAPAdmin

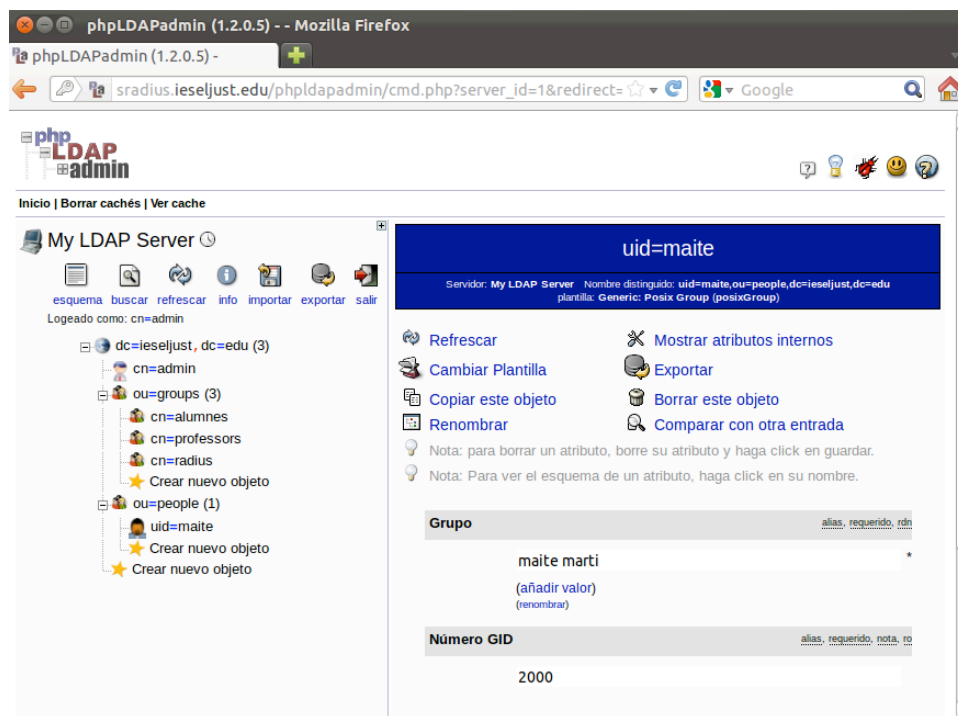


Figura 3.11. Vista gràfica del directori des de phpLDAPAdmin

### 3.6 Instal·lació i configuració de freeRadius

FreeRadius és un conjunt de programes, modulars i lliures que es distribueixin sota llicència GNU General Public License, versió 2 i es gratuït tan la seua descàrrega com la seua utilització.

La suite inclou un servidor RADIUS, un llibreria de client RADIUS amb llicència BSD (Berkeley Software Distribution) , una llibreria PAM (Pluggable Autenticacion Library), un mòdul d'Apache, i unes quantes utilitats i llibreries de desenvolupament relacionades amb RADIUS.

FreeRadius es el més populars dels servidors de RADIUS, amb codi obert i el més utilitzat a tot el mon.

Suporta la majoria dels protocols d'autenticació i el servidor porta un software d'administració per web, que està basat en php, que s'anomena dialupadmin.

És la base en molt productes comercial com sistemes encastats, que suporten aplicacions de RADIUS, com Control d'Accés a la xarxa i WiMax.

El primer que farem és instal·lar-lo, amb la següent comanda:

```
$ sudo apt-get install freeradius
```

Una vegada feta la instal·lació serà necessària la configuració d'uns quants fitxers.

El primer serà editar el fitxer **/etc/freeradius/eap.conf** i assegurar-nos que hem posat les contrasenyes en md5.

```
eap {
    default_eap_type = md5
}
```

Ara haurem d'especificar totes les dades relatives al nostre servidor LDAP. Per tant ara configurarem el fitxer **/etc/freeradius/modules/ldap**.

```
ldap {
    server = "sradius.ieseljust.edu"
    identity = "cn=admin,dc=ieseljust,dc=edu"
    password = admin
    basedn = "dc=ieseljust,dc=edu"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
    ldap_connections_number = 5
    timeout = 4
    timelimit = 3
    net_timeout = 1
    tls {
        start_tls = no
    }
    dictionary_mapping = ${confdir}/ldap.attrmap
    edir_account_policy_check = no
}
```

Després haurem d'especificar que s'haurà de fer la validació per ldap i per tant especificarem que s'utilitzi el mòdul ldap en els processos d'autenticació i autorització.

Caldrà editar el fitxer **/etc/freeradius/sites-available/default** i des comentar les línies de ldap i ha de quedar tota la part de "authorize" de la següent forma:

```
authorize {
    preprocess
    auth_log
    chap
    mschap
    digest
    suffix
    eap {
        ok = return
    }
    ldap
    expiration
    logintime
    pap
}
```

A més també haurem de des comentar en la secció "authenticate" les línies que fan referència a ldap.

El mateix que hem fet abans ho haurem de fer al fitxer:

**/etc/freeradius/sites-available/inner-tunnel**

```
authorize {
  chap
  mschap
  suffix
  update control {
    Proxy-To-Realm := LOCAL
  }
  eap {
    ok = return
  }
  ldap
  expiration
  logintime
  pap
}
authenticate {
  Auth-Type PAP {
    pap
  }
  Auth-Type CHAP {
    chap
  }
  Auth-Type MS-CHAP {
    mschap
  }
  unix
  Auth-Type LDAP {
    ldap
  }
}
eap}
```

Existeix un fitxer anomenat **/etc/freeradius/clients.conf** on es defineixen totes les credencials dels dispositius que es validen en el servidor RADIUS, com són per exemple, els punts d'accés. Podem definir tant equips individuals com xarxes senceres.

Una possible configuració d'aquest fitxer seria:

```
client 192.168.0.253 {
  secret = testing123
  shortname = ApRadius}
client 192.168.0.0 {
  secret = testing123
  shortname = informatica}
```

Per tal de que el servidor llegeixi el fitxer anterior haurem de comprovar que en el fitxer **/etc/freeradius/radiusd.conf** aparegui la següent línia:

```
$INCLUDE clients.conf
```

La configuració sencera d'aquest fitxer la podem trobar a l'annex2.

Una vegada hem canviat tots els fitxers, caldrà fer algunes passes més. Primer haurem d'instal·lar un mòdul que fa falta per a la comunicació entre el servidor freeradius i LDAP:

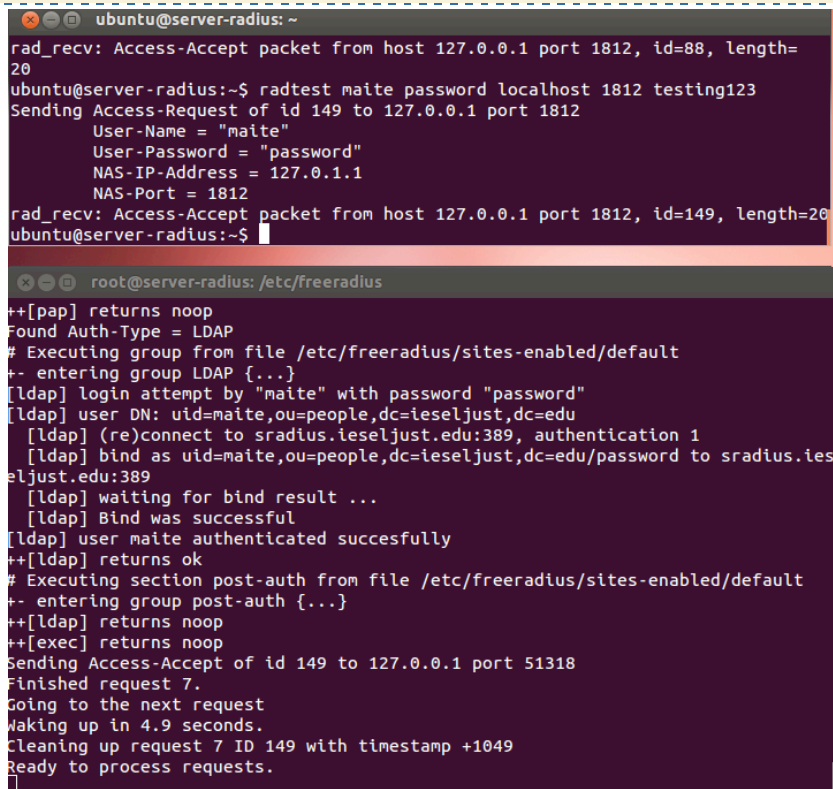
```
$ sudo apt-get install freeradius-ldap
```

Després deuríem reiniciar el servei, però el que farem serà aturar el servei i engegar-lo en mode depuració, per a poder veure si funciona correctament, i ens mostra la següent sortida:

```
$ sudo /etc/init.d/freeradius stop
$ sudo freeradius -X
  Listening on accounting address * port 1813
  Listening on authentication address 127.0.0.1 port 18120 as server inner-tunnel
  Listening on proxy address * port 1814
  Ready to process requests.
```

Una vegada tot configurat i en marxa podem provar que el servidor RADIUS valida contra el servidor ldap. Executem la següent comanda i comprovem que el servidor ens contesta, validant l'accés.

```
$ radtest maite password localhost 1812 testing123
```



```
ubuntu@server-radius: ~
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=88, length=20
ubuntu@server-radius:~$ radtest maite password localhost 1812 testing123
Sending Access-Request of id 149 to 127.0.0.1 port 1812
  User-Name = "maite"
  User-Password = "password"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=149, length=20
ubuntu@server-radius:~$

root@server-radius: /etc/freeradius
++[pap] returns noop
Found Auth-Type = LDAP
# Executing group from file /etc/freeradius/sites-enabled/default
+- entering group LDAP {...}
[ldap] login attempt by "maite" with password "password"
[ldap] user DN: uid=maite,ou=people,dc=ieseljust,dc=edu
[ldap] (re)connect to sradius.ieseljust.edu:389, authentication 1
[ldap] bind as uid=maite,ou=people,dc=ieseljust,dc=edu/password to sradius.ieseljust.edu:389
[ldap] waiting for bind result ...
[ldap] Bind was successful
[ldap] user maite authenticated succesfully
++[ldap] returns ok
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
+- entering group post-auth {...}
++[ldap] returns noop
++[exec] returns noop
Sending Access-Accept of id 149 to 127.0.0.1 port 51318
Finished request 7.
Going to the next request
Waking up in 4.9 seconds.
Cleaning up request 7 ID 149 with timestamp +1049
Ready to process requests.
```

*Figura 3.12. Sortida del test de funcionament de freeRadius*

### 3.7 Configuració del Punt d'accés (Access Point)

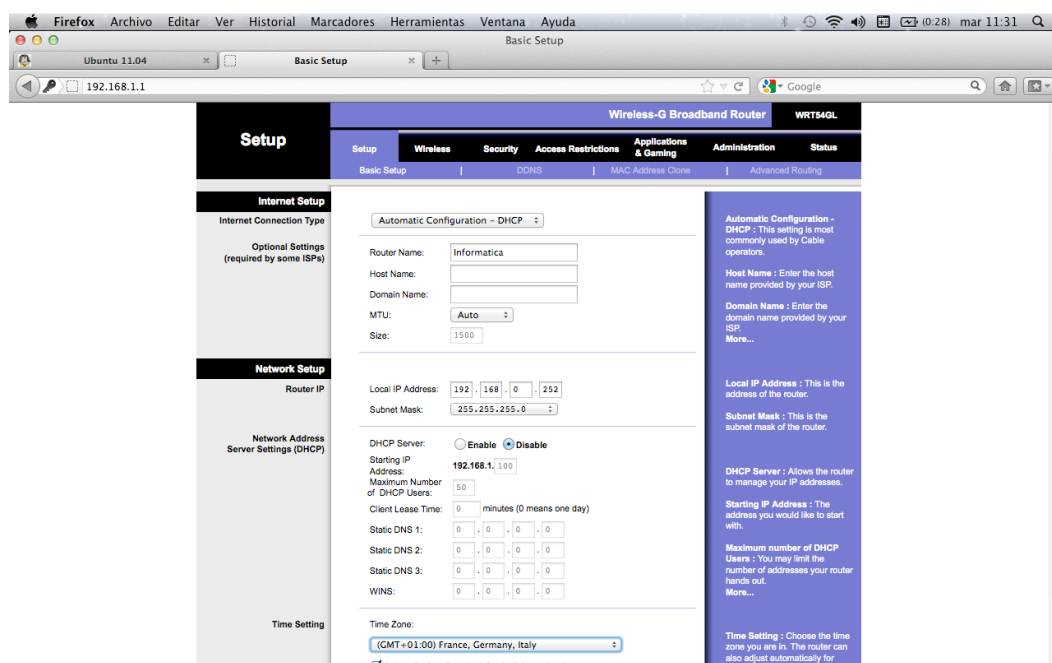
Disposem d'un router Lynksys, en el centre que farà les funcions de punt d'accés. El model és WRT54GL, és compatible amb les normes 802.11b/g/n, opera en la banda de freqüència de 2,4Ghz.

Encara que aquest dispositiu disposa de servidor dhcp, s'ha preferit configurar el ordenador que fa de servidor RADIUS, com a servidor dhcp, perquè poder fer una configuració específica, s selectiva i a més aportem més seguretat.

Per defecte el router ve configurat de fàbrica amb l'adreça 192.168.1.1, amb nom d'usuari en blanc i la contrasenya "admin".

Els paràmetres d'Internet és deixarem conforme estan, perquè no emprarem aquesta funcionalitat del router. Tan sols li configurarem un nom al dispositiu: Informatica, i deixarem obtenir una adreça dhcp.

Pel que fa a la xarxa interna, i com és convenient tenir identificats els dispositius més importants, li assignarem una Ip estàtica: 192.168.0.252 i a més el configurarem per a que no siga servidor dhcp.



**Figura 3.13. Configuració de l'adreça del Router**

El segon pas serà configurar el nom de la xarxa (ESSID- radius), seleccionar el canal que utilitzarà, en el nostre cas el més adequat és el 11.

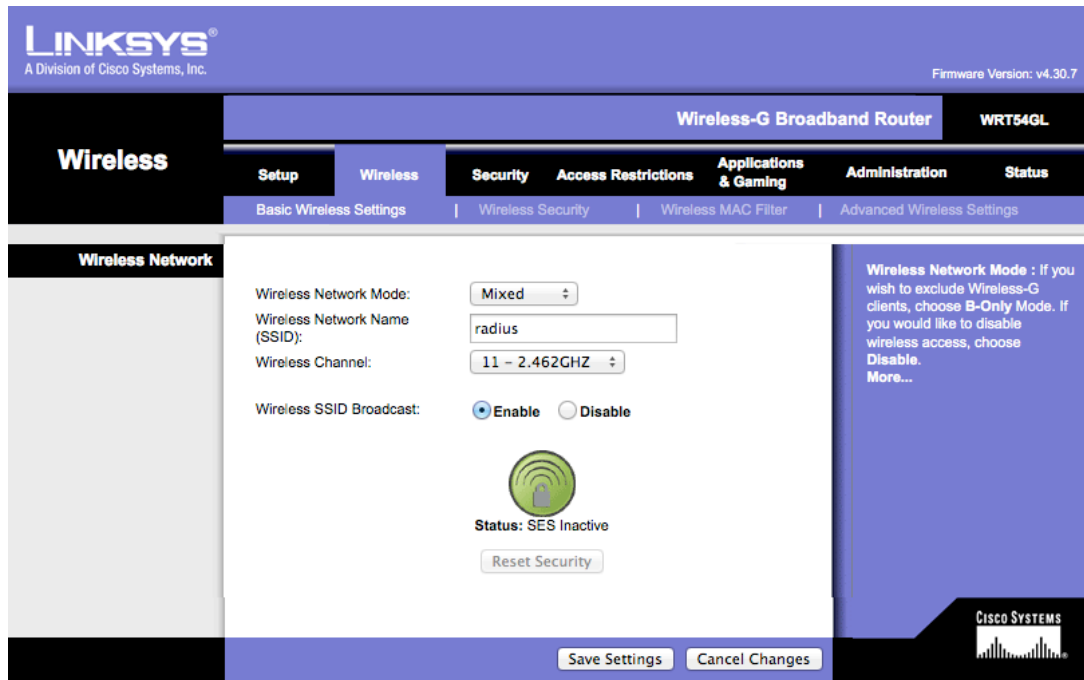


Figura 3.14. Configuració de la xarxa wireless al Router.

seleccionar el mètode de autenticació WPA i posar les dades del servidor RADIUS, que és el lloc on redirigirem les peticions.

A més hem de posar la "shared key" es correspon amb la que està definida a l'arxiu clients.conf de FreeRadius.

Després caldrà salvar els canvis i reiniciar el router que fa de punt d'accés.

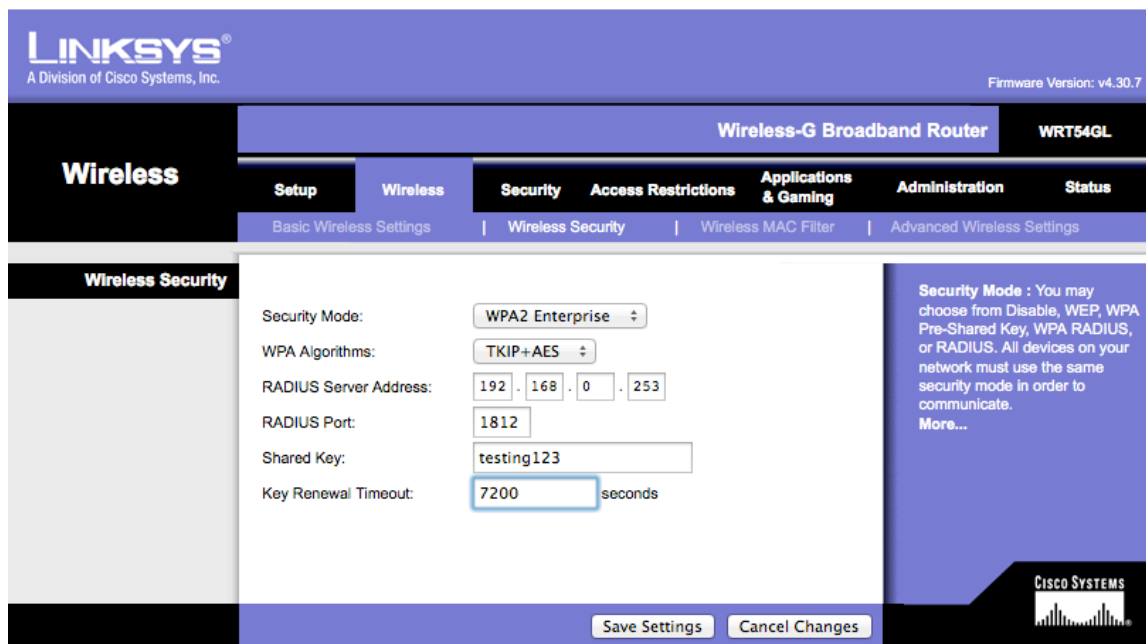


Figura 3.15. Configuració de l'associació Router-Server Radius



### 3.8 Configuració del Client

Una vegada que ja hem configurat el servidor RADIUS i el punt d'accés, ens quedarà configurar un client que disposi d'una connexió sense fils.

Utilitzem un client Linux amb una versió d'Ubuntu 10.04.

El primer que haurem de fer serà detectar totes les xarxes sense fils. En la llista apareix la nostra amb ESSID = radius.

Sol·licitem la connexió i ens apareix la següent finestra de configuració.



*Figura 3.16. Configuració de l'autenticació del client sense fils*

Els paràmetres que més s'adeqüen a la configuració, tal i com hem implementat en els punts anteriors el servidor Ldap i el servidor RADIUS, son els següent:

Tipus d'autenticació TLS a través d'un túnel (configurat al fitxer inner-tunnel del servidor freeradius).

Cap certificat, per què no en tenim cap generat per una Autoritat certificadora. Donat el cas que en tinguéssim, podríem escollir-lo en aquesta finestra.

Autenticació interna PAP, tal i com teníem configurat el servidor.

I l'usuari i contrasenya que havien creat al servei de directori.

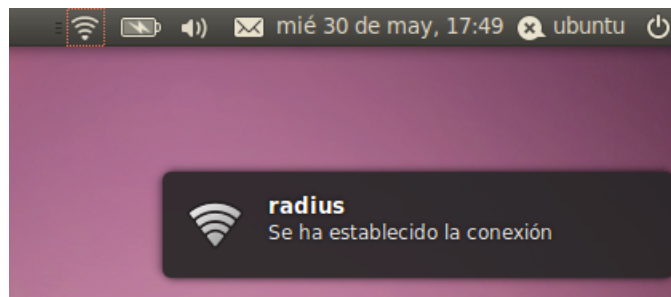
A continuació, ens mostrarà una pantalla on podem triar un certificat, generat per una Autoritat certificadora o Ignorar l'advertència.

Com que no s'ha generat cap certificat triarem l'opció d'Ignorar.



*Figura 3.17. Selecció del certificat de la CA*

En la següent figura podem apreciar, que s'ha acceptat la validació i hem establert la connexió amb el punt d'accés, validant-nos amb l'usuari creat al directori actiu.



*Figura 3.18. Connexió establerta des d'un client*

## 4. Integració amb la Xarxa d'Àrea local

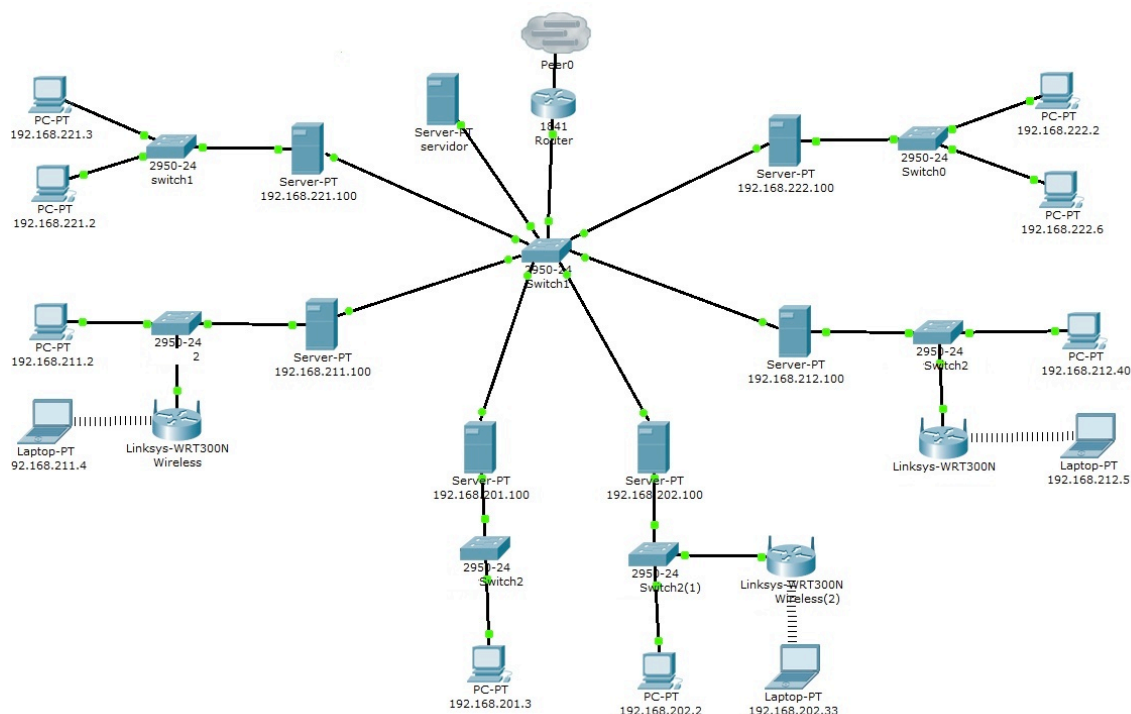
### 4.1 Descripció de la xarxa de d'institut

En aquest projecte es pretén modificar la forma d'accedir a la xarxa del centre a través de les connexions sense fils. Per tant cal redissenyar la configuració actual de la xarxa, per tal d'integrar els nous elements que formaran part de la xarxa.

Actualment a les aules del centre els ordinadors dels alumnes poden accedir als recursos de la xarxa de dues formes:

**-Cablejada:** Les aules estan cablejades de forma que en cada lloc de treball l'estudiant disposa d'una roseta on es pot connectar un ordinador mitjançant un cable de par trenat.

**-Sense Fils:** Per poder accedir a la xarxa amb els portàtils que disposen de targeta sense fils, el que es fa actualment, és accedir a un punt d'accés o *router* que pot estar o no en la mateixa aula, i introduir la contrasenya WPA2 establida en el dispositiu d'accés, per connectar-nos.



*Figura 4.1. Esquema de la xarxa actual del centre IES Jaume II el Just*

Cada aula està dotada a més, d'un commutador al qual van connectat tots els equips cablejats i el punt d'accés.

Les aules disposen també, d'un ordinador del professor, el qual té instal·lades dos targetes de xarxa. Aquest ordinador actua com a servidor d'aula i realitza la funció de interconnexió, entre la xarxa de l'aula i el *Router* que dona accés a Internet.

Una altra de les funcions del servidor d'aula és de servidor DHCP , és a dir, assignar adreces IP, i a cada aula s'assigna un rang diferent d'adreces. D'aquesta forma es separen les diferents aules en diferents xarxes.

En la figura 4.1 podem veure un esquema de l'estructura actual de la xarxa del centre. Es pot observar com els equips portàtils es connecten sense fils, als punt d'accés que els correspon de les seves aules sabent prèviament la contrasenya per poder validar-se. Aquests punts d'accés o *routers* es connecten al *switch* de la seva classe. Ara be també es podria donar la situació que es connectaren d'una aula en una altra, només assabentant-se de la contrasenya.

Si ara ens fixem en la part superior esquerra de la figura 4.1, podem veure el server amb la IP 192.168.221.100,(aquest seria un dels equips professor), aquest, mitjançant dues targetes de xarxa, es connecta al *switch* del aula, (el de la seva esquerra) i aquest a la vegada, connecta amb els equips cablejats del aula.

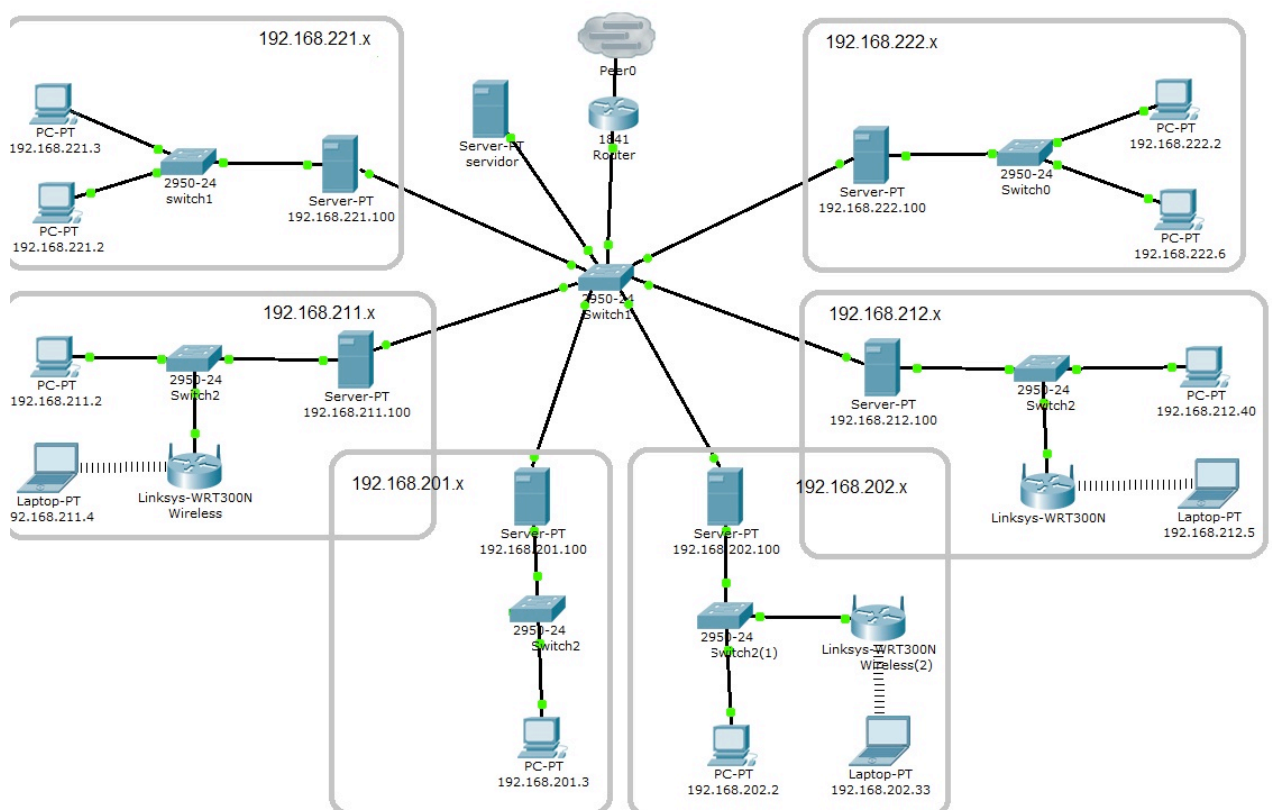


Figura 4.2. Esquema de la xarxa, divisió per aules

Per l'altra banda l'equip del professor es connecta al *switch* central de “*el centre de càlcul o sala de servidors*”. Al *switch* central és on es connecten tots els ordinadors del professors i servidors del centre, així com el *router* que subministra accés a Internet al centre.

En la figura 4.2 podem apreciar millor la divisió de xarxes i aules del centre.

Les xarxes de cada aula tenen diferents IP's segons on esta situada l'aula. En total hi han 6 aules.

Soterrani 192.168.201.x i 192.168.202.x

Planta baixa 192.168.211.x i 192.168.212.x

Primer pis 192.168.221.x i 192.168.222.x

La xarxa a la que pertanyen els servidors d'aula és la 192.168.0.x on x és el número d'aula.

## 4.2 Integració del Servidor RADIUS i punt d'accés

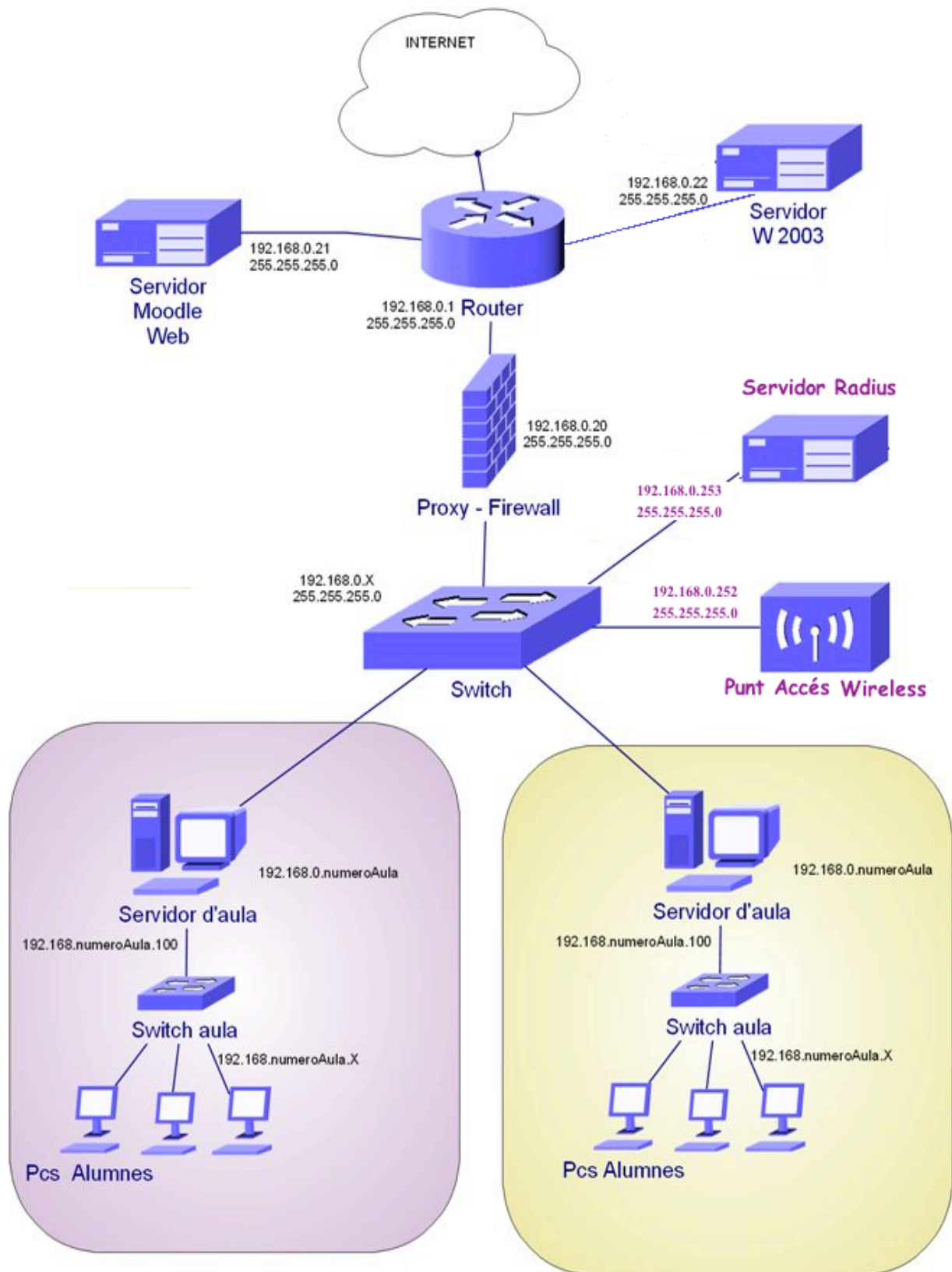
Una vegada descrita l'estructura de la xarxa del centre, explicarem on anem a connectar els nous dispositius per a integrar-los a la xarxa amb els mínims canvis i de la forma més òptima.

Tant el servidor RADIUS, com el Router, han estat configurats per a pertànyer a la xarxa 192.168.0.0, donat que hem configurat el servidor RADIUS amb l'adreça 192.168.0.253 i el Router amb l'adreça 192.168.0.252.

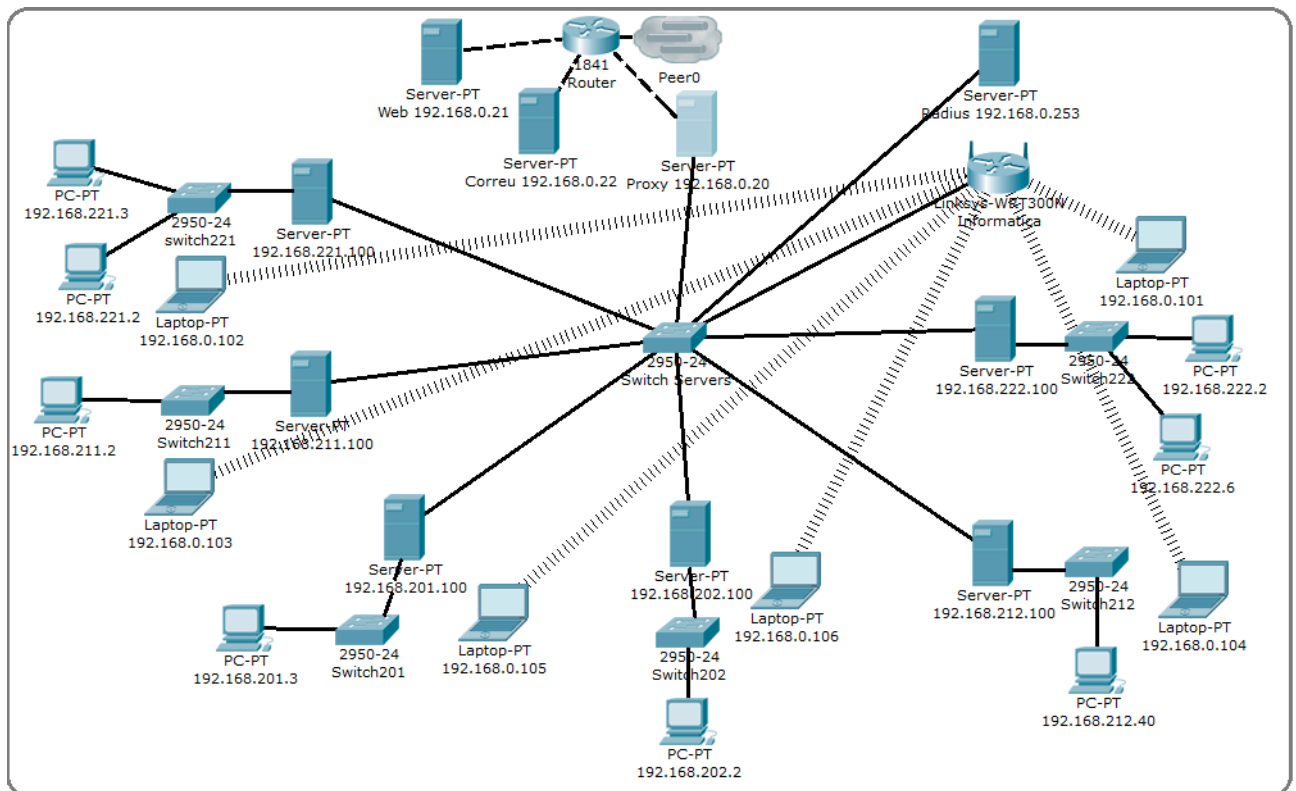
Llavors connectarem els dos dispositius al *switch* central, on ja estaven connectats els servidors d'aula. L'esquema del centre es quedaria tal i com podem veure a la següent figura 4.3

El següent pas seria la desconexió dels AP que hi ha en algunes de les aules, per a deixar únicament en funcionament el Router que hem integrat, amb funció de punt d'accés.

Ara ja no importa des d'on es connecti un equip portàtil, ja que es validaran tots amb el servidor RADIUS. L'esquema detallat d'interconnexió amb tots el dispositius existents, inclòs els portàtils, es pot observar a la figura 4.4.



*Figura 4.3. Xarxa amb el servidor RADIUS i el Router (AP)*



*Figura 4.4. Esquema de la Xarxa del Centre Definitiva*

Explicarem ara com queda el procés de connexió dels equips portàtils.

- En sol·licitar la connexió amb el router-AP, ens demanarà un usuari i una contrasenya.
- Una vegada introduït, es procedirà a la validació amb el servidor Radius.
- El servidor comprovarà els paràmetres introduïts, amb el servei de directori.
- Si la informació és correcta, se li assignarà a l'equip client una adreça IP.
- Ja pot disposar dels serveis de xarxa que li siguin permesos.

Tan sols queda per dir que aquests nous elements que s'han incorporat, el servidor Radius i el Router-AP es situaran en un habitacle destinat als servidors, anomenat centre de càlcul i que esta en la planta baixa.

S'ha comprovat que des del centre de càlcul hi ha bona cobertura i arriba el senyal, tan a la primera planta com a la segona.

### 4.3 Alta d'elements en el directori ldap

Encara que hem instal·lat ferramentes gràfiques, per tal de facilitar les tasques d'administració del servei de directori LDAP, el procés d'inserció d'alumnes, és una tasca un tant costosa.

És per això que s'ha cregut convenient automatitzar aquesta tasca, en previsió que tots el principis de curs lectiu, hi ha moltes tasques, i no es pot dedicar el temps suficient a aquesta feina.

El procediment es pot realitzar de distintes formes. La manera que s'ha considerat més adient ha estat la següent:

- Donem d'alta cadascun dels grups, que s'ubicaran de manera fixa a una aula.
- Des de la secretaria del centre, se'ns proporciona un llista d'alumnes amb les dades que nosaltres sol·licitem. Nom, cognom1, cognom2, adreça, telèfon, grup, mail.
- Crearem un script, que llegint del fitxer proporcionat, generi el fitxer amb el format LDIF, necessari per a poder-se introduir en el servei de directori.
- Executarem la instrucció de càrrega.

Una altra alternativa seria:

- Des de la secretaria del centre, se'ns proporciona un llista d'alumnes amb les dades que nosaltres sol·licitem. Nom, cognom1, cognom2, adreça, telèfon, grup, mail.
- Generem el fitxer en format ldif, mitjançant un script.
- Obrim la utilitat phpLDAPadmin i efectuem la importació de dades, seleccionant aquest fitxer.

Ens hem decantat per la primera opció en efectuar més accions desateses.

Els scripts que realitzen aquestes tasques es poden trobar a l'annex3.



## 5. Solucions Integrades amb Ldap i RADIUS. ZeroShell.

ZeroShell es una distribució Linux [16], que no està basada en cap altra, per a servidors i dispositius encastats, que proporciona molts de serveis de xarxa que s'utilitzen avui en dia. Es un Firewall gratuït que proporciona algunes de les característiques dels equips més complexos, quan a seguretat.

Les seues principals característiques son:

- Balanceig de línies i tolerància a falles amb connexions múltiples d'internet
- Connexions UMTS y HSDPA utilitzant mòdems 3G
- **Servidor de autenticació radius**
- “Captative Portal”. Portal de validació web per a xarxes. L'usuari s'haurà de validar abans de poder navegar.
- QoS (Qualitat de Servei). Permet configurar el tràfic de la xarxa per a garantir un mínim ample de banda.
- HTTP Proxy transparent.
- Punto de accés wireless
- Host to Lan VPN. VPN client
- Lan to Lan VPN. VPN entre servidors
- Router con accés dinàmiques i estàtiques
- Soport de lan Virtual
- Filtre de paquets, inclòs en tràfic P2P
- Traducció d'adreces (NAT)
- TCP/UPD Port Forwarding per a la publicació de servidors interns
- Servidor DNS multi zona
- Client PPPoE per a la connexió xDSL
- Client DNS dinàmic
- Autenticació Kerberos 5
- Autenticació LDAP, NIS y RADIUS
- Sincronització amb Active Directory
- Entitat certificadora X509

ZeroShell es una distribució “Live CD”. Això significa que no es necessari instal·lar-lo en el disc dur per a que funcioni, ja que es capaç de funcionar des de el CD-ROM. Lògicament la base de dades de configuració, que conté les dades de la xarxa, pot ser emmagatzemada en tot tipus de discs fins a un USB.

Disposa d'un sistema d'actualitzacions on-line, i es pot descarregar per a formats de targetes Compact Flash per a instal·lar-la en dispositius encastats.

En l'annex 4 hem incorporat més informació al voltant d'aquest sistema, donat que en si mateix podria ser la base per a un altre projecte.

## 6. Conclusions

El projecte ha estat força interessant, tant en els seus principis, quan estava en la fase d'estudi, com al final en la fase d'implantació.

La implantació dels sistema al centre ens ha proporcionat nombrosos avantatges, encara que també cal destacar que la seua posta en funcionament no ha estat una tasca senzilla, sobretot pel que fa a la instal·lació i configuració de LDAP.

La planificació ha estat molt endarrerida, sobretot pel entrebanc que ha suposat el desenvolupament del projecte en la versió 10.04 d'Ubuntu. Això ha provocat que s'haguera d'instal·lar el sistema operatiu de nou, en la seua versió 12.04. A més tot el que es portava fet del projecte tècnic, es va tenir que repetir. És a dir, vaig tornar a instal·lar i configurar els servei de DHCP i DNS.

Una vegada superats tots els entrebancs i el sistema en marxa, quant ja estava quasi finalitzant les proves, fent una recerca al voltant d'una informació del projecte, vaig ensopegar amb el ZeroShell.

Tant em va sorprendre les seues característiques i tot el que comportava, que vaig decidir dedicar-li, una menció en aquest projecte, perquè en un mateix sistema estaven integrats tots els serveis necessaris per a dur a terme aquest projecte.

Com que ja no quedava temps per estudiar-lo a fons, no se si de veritat aporta totes aquestes funcionalitats i si el sistema es comporta de manera estable. Si més no es curiós, que no fa falta cap mena d'instal·lació i l'espai en disc necessari és molt reduït. La seua administració es pot realitzar mitjançant un navegador de qualsevol equip que estigui connectat a la mateixa xarxa.

Suposo que el meu projecte, aportarà major funcionalitat al poder configurar qualsevol cosa a la mida de les nostres necessitats sense dependre de cap desenvolupador en concret, sent també tot el programari opensource.

## Bibliografia

- [1] **“Seguridad Informatica”** CESAR SEOANE RUANO. McGraw-Hill / Interamericana De España, S.A., 2010
- [2] **“Redes.de.Computadoras” 4ta.ed** ANDREWS. S. TANENBAUM Pearson Educación, México, 2003. Es pot consultar el llibre en format digital en:  
**“<http://es.scribd.com/doc/63969188/Redes-de-Computadoras-4ta-ed-Andrews-S-tanenbaum-Printice>”**
- [3] **“Orthogonal Frequency Division Multiplexing (OFDM)”**  
[http:// www.complextoreal.com/chapters/ofdm2.pdf](http://www.complextoreal.com/chapters/ofdm2.pdf)
- [4] **“AES Advanced Encryption Standard Versión 2005, Principiantes”**, José de Jesús Angel Angel 2005  
[http://www.criptored.upm.es/guiateoria/gt\\_m117i.htm](http://www.criptored.upm.es/guiateoria/gt_m117i.htm)
- [5] **“The Design of Rijndael”**, J. Daemen, V. Rijmen, Springer Verlag 2001
- [6] **“Comunicaciones y redes de computadores” 7 th Edition. William Stallings**, Pearson Prentice Hall
- [7] **“MACAW: A Media Access Protocol for Wireless LANs,”** V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, in *Proceedings of ACM SIGCOMM*, pp. 212-225, 1994
- [8] **“Telemática y Sistemas de Transmisión de Datos”** Estándares del Nivel Físico. Juan Manuel Orduña Huertas. Universitat de València  
<http://informatica.uv.es/iiguia/TSTD/apuntes/tema6.pdf>
- [9] **“Internet Working with TCP/IP - Volumen I; Principles, Protocols and Architectures. - Second Edition”** Douglas E. Comer. Prentice Hall International
- [10] <http://bulma.net/body.phtml?nIdNoticia=1991>
- [11] <https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html>
- [12] <http://www.marblestation.com/?p=735>
- [13] <http://www.padl.com/OSS/MigrationTools.html>
- [14] <http://olsacupy.berlios.de/v0.1/html/openldap-autenticacion-usuarios-configuracion.html>
- [15] <https://help.ubuntu.com/community/LDAPClientAuthentication#Troubleshooting>
- [16] <http://www.zeroshell.net/es/>

## Glossari d'acrònims

**AAA** *Authentication, Authorization, and Accounting*

Autenticació, Autorització i Comptabilització

**AP** *Access Point*

Punt d'Accés

**AES** *Advanced Encryption Standard*

Estàndard de Xifrat Avançat

**BSS** *Basic Service Set*

Conjunt de Serveis Bàsics

**DHCP** *Dinamyc Host Protocol*

Protocol de Configuració Dinàmica d'Equips

**DNS** *Domain Name Server*

Servidor de Noms de Domini

**ESS** *Extended Service Set*

Conjunt de Serveis Extensos

**IAS** *Internet Authentication Service*

Servei d'Autenticació d'Internet

**IBSS** *Independent Basic Service Set*

Conjunt de Serveis Bàsics Independents

**IEEE** *Institute of Electrical and Electronics Enginneers*

Institut d'Engeniers Elèctrics i Electrònics

**IP** *Internet Protocol*

Protocol d'Internet

**LAN** *Local Area Network*

Xarxa d'Àrea Local

**LDAP** *Lightweight Directory Access Protocol*

Protocol Lleuger d'Accés al Directori

**LDIF** *LDAP Data Interchange*

Format d'Intercanvi de Dades del LDAP

**MAC** *Media Access Control*

Control d'Accés al Medi

**NAS**      *Network Access Server*

Servidor d'Accés a la Xarxa

**RADIUS**    *Remote Authentication Dial-In User Server*

Servidor Remot d'Autenticació

**RAS**      *Remote Access Server*

Servidor Remot d'Accés

**SSH**      *Secure Shell*

Shell Segur

**VoIP**      *Voice over IP*

Veü sobre IP

**SSL**      *Secure Socket Layer*

Capa Connexió Segura

**TCP**      *Transport Control Protocol*

Protocol de Control de Transport

**TKIP**      *Temporal Key Integrity Protocol*

Protocol d'Integritat de Clau Temporal

**TLS**      *Transport Layer Security*

Capa de Transport Segura

**VPN**      *Virtual Private Network*

Red Privada Virtual

**WEP**      *Wired Equivalent Privacy*

Privacitat Equivalent al Cable

## ANNEXES

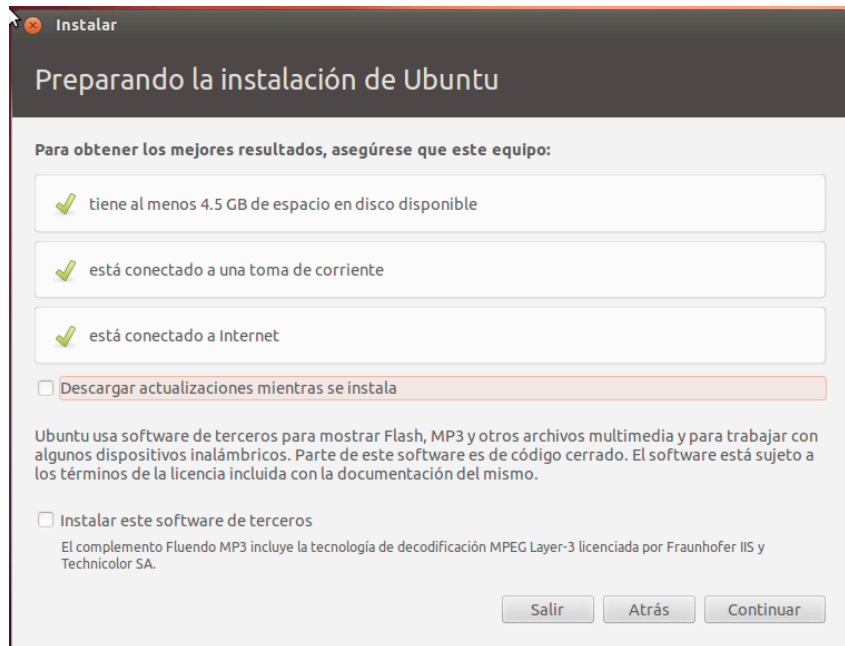
### Annex1

#### Documentació de la instal·lació de la versió de Ubuntu 12.04

La instal·lació varia un poc, però no hi ha cap canvi substancial.

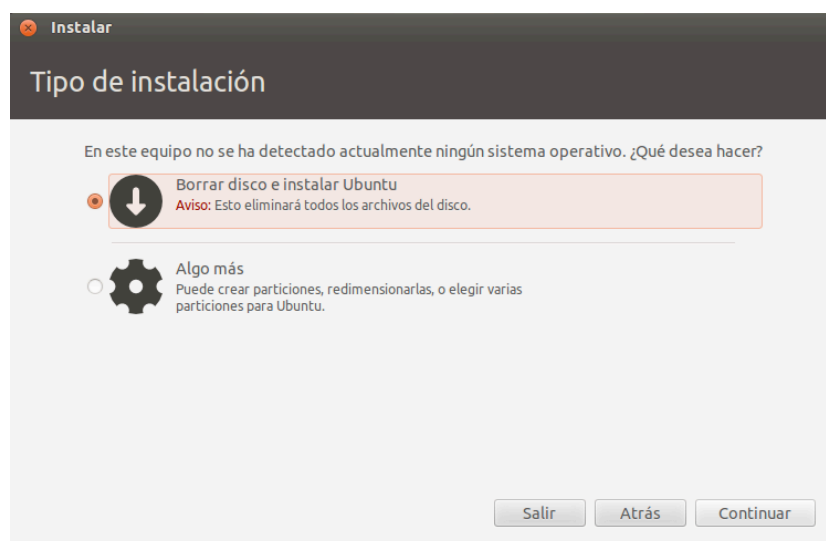
En la primera pantalla d'instal·lació, el programa testeja els requisits necessaris per a la instal·lació i ens mostra un primer informe, per si no complim algun punt, poder solucionar-ho.

No és el nostre cas, on apareix tot en verd i podem polsar en continuar.



**Figura A1. Preparació Instal·lació Ubuntu12.04**

En la següent pantalla detecta que no tenim instal·lat cap sistema operatiu, al haver format el disc dur i ens dona l'opció de fer les particions manuals o automàtiques. Triarem la segona opció.



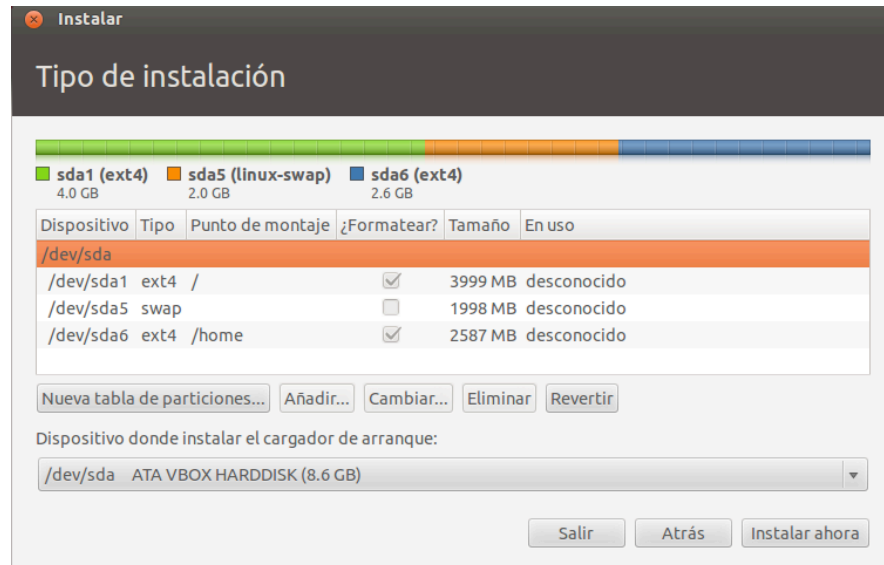
**Figura A2. Tipus d'Instal·lació Ubuntu12.04**

I polsarem continuar.

Les particions seran semblants a les que havíem explicat en el procés inicial d'instal·lació.

Muntarem una partició per al sistema /, altra per a les dades d'usuari /home i una per a l'àrea d'intercanvi.

I després seleccionarem "Instalar ahora".



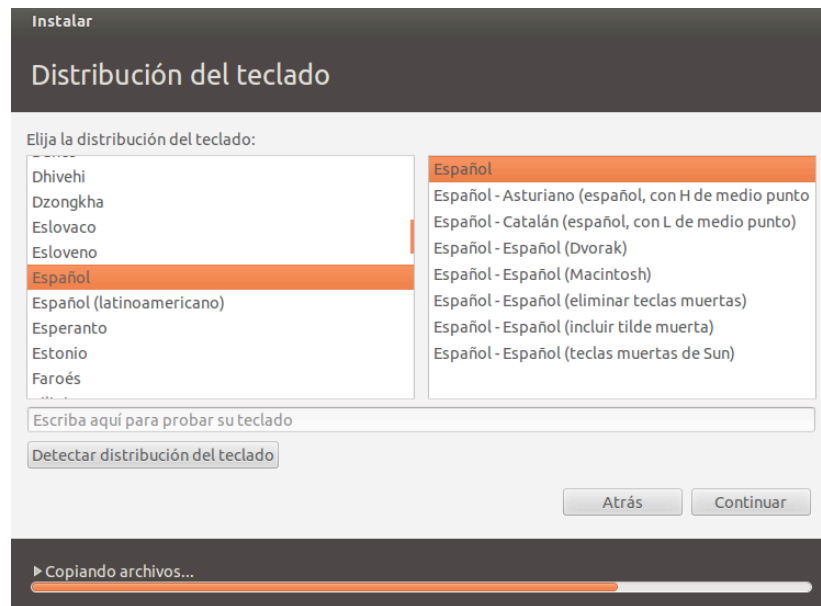
*Figura A3. Instal·lació Ubuntu12.04, esquema de particionat de disc*

Comença la còpia d'arxius i ens demana que seleccionem la zona horària. Triarem la de Madrid i continuarem.



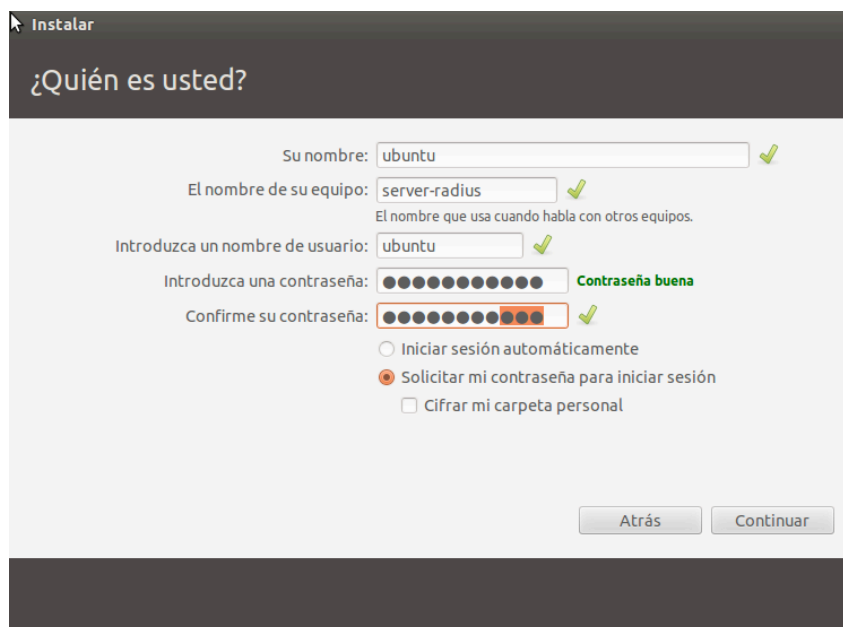
*Figura A4. Instal·lació Ubuntu12.04. Selecció zona horaria*

Triem la configuració del teclat i Continuem.



**Figura A5. Instal·lació Ubuntu12.04. Selecció teclat**

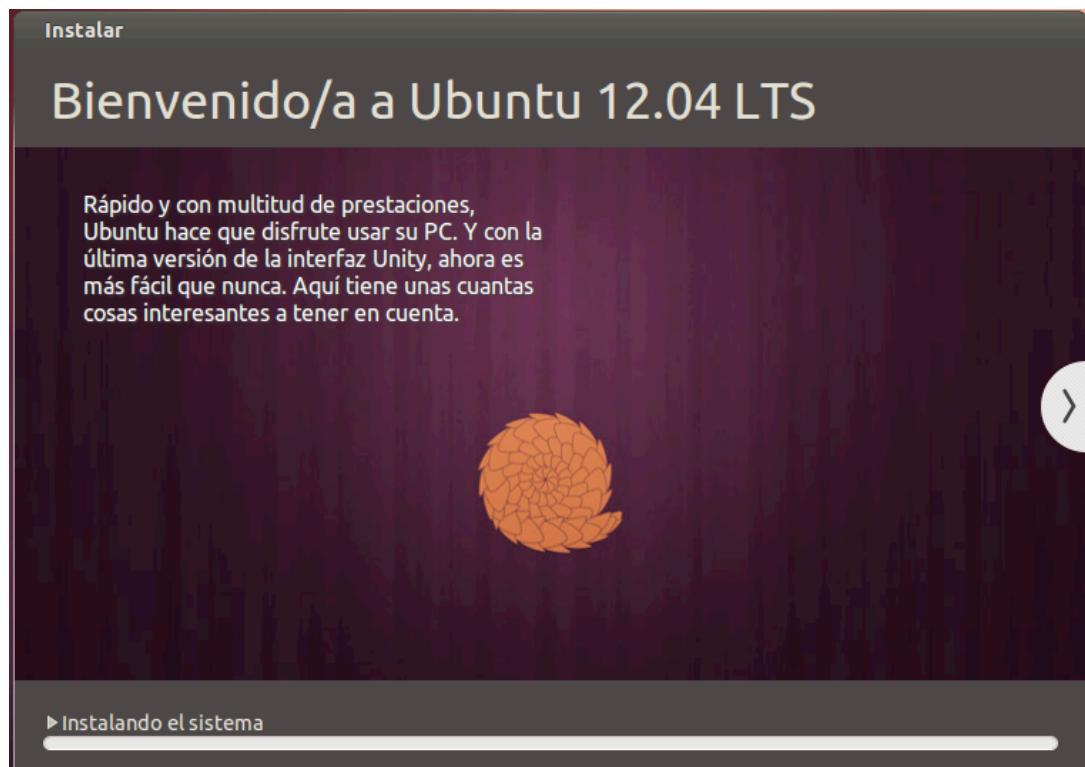
Ara introduïrem un usuari que tindrà privilegis d'administrador i li posarem el nom a l'equip. Triarem a més una contrasenya segura, i continuarem.



**Figura A6. Instal·lació Ubuntu12.04. Usuari i nom de l'equip.**



I ja s'instal·la el sistema.



*Figura A7. Finalització Instal·lació Ubuntu12.04*

## Annex2

### Fitxer configuració /etc/freeradius/radiusd.conf

```
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius
radacctdir = ${logdir}/radacct
name = freeradius
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}
db_dir = ${raddbdir}
libdir = /usr/lib/freeradius
pidfile = ${run_dir}/${name}.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 1024
listen {
    type = auth
    ipaddr = *
    port = 0 }
listen {
    ipaddr = *
    port = 0 type = acct }
hostname_lookups = no
allow_core_dumps = no regular_expressions
    = yes extended_expressions
    = yes log {
    destination = files
    file = ${logdir}/radius.log
    syslog_facility = daemon
    stripped_names = no
    auth = no
    auth_badpass = no
    auth_goodpass = no }
checkrad = ${sbindir}/checkrad
security {
    max_attributes = 200
    reject_delay = 1
    status_server = yes }
proxy_requests = yes
$INCLUDE proxy.conf
$INCLUDE clients.conf
thread pool {
```

```
start_servers = 5
max_servers = 32
min_spare_servers = 3
max_spare_servers = 10
max_requests_per_server = 0 }
modules {
    $INCLUDE ${confdir}/modules/
    $INCLUDE eap.conf }
instantiate {
    exec
    expr
    expiration
    logintime }
$INCLUDE policy.conf
$INCLUDE sites-enabled/
```

## Annex3

### Creació dels grups, com unitats organitzatives

```
#!/bin/bash
domini="dc=ieseljust,dc=edu"
pass="curs2012"
destinacio="grups.ldif"

while read line
do
echo "dn: ou=$line,$domini " > $destinacio
echo "objectClass: organizationalUnit" >> $destinacio
echo "ou: $line" >> $destinacio
ldapadd -x -D cn=admin,$domini -w $pass -f $destinacio #> /tmp/null 2>&1
if [ $? -eq 0 ]; then
echo "Grup $line insertat"
else
echo "No s'ha pogut crear el grup. Pot ser perquè:"
echo "Ja existeix la unitat organitzativa"
fi

done < "grups.txt"
```

### Creació dels usuaris

```
#!/bin/bash
domini="dc=ieseljust,dc=edu"
pass="curs2012"
destinacio="usuaris.ldif"
while read line
do
nom=`echo $line | cut f1 -d`,`"
cognom1=`echo $line | cut f2 -d`,`"
cognom2=`echo $line | cut f3 -d`,`"
adreça=`echo $line | cut f4 -d`,`"
telefon=`echo $line | cut f5 -d`,`"
grup=`echo $line | cut f6 -d`,`"
mail=`echo $line | cut f7 -d`,`"

echo "dn: uid=$nom$cognom1,ou=$grup,$domini" > $destinacio
echo "objectClass: posixAccount" >> $destinacio
echo "objectClass: shadowAccount" >> $destinacio
echo "objectClass: inetOrgPerson" >> $destinacio
echo "uid: =$nom$cognom1" >> $destinacio
echo "sn: $cognom2" >> $destinacio
echo "cn: $usuari $cognom1" >> $destinacio
echo "mail: $mail" >> $destinacio
```

```
uid=`echo ldapsearch -xLLL -b $domini "objectClass=inetorgperson" | grep "uidNumber" | cut -d: -f 2
| tail -1`
uid=`expr $uid + 1`
echo "uidNumber: $uid" >> $destinacio
echo "gidNumber: 1000" >> $destinacio
echo "homeDirectory: /home/$nom$coognom1" >> $destinacio
ldapadd -x -D cn=admin,$domini -w $pass -f $destinacio #> /tmp/null 2>&1
if [ $? -eq 0 ]; then
echo "Usuari $nom$coognom1 insertat"
else
echo "No s'ha pogut crear l'usuari =$nom$coognom1. Pot ser perquè:"
echo "No existeix la unitat organitzativa"
echo "O perquè l'usuari ja existeix"
fi
ldapsearch -xLLL -b $domini uid=$nom$coognom1

done < "alumnes.txt"
```

## Annex4

### ZEROSHELL

Interfície en arrancar el sistema:



Figura A8. Interfície del sistema ZeroShell

Si la configurem per obtenir una adreça IP, després ens podem connectar des del navegador d'altra màquina. Tan sols posant la IP, i l'usuari per defecte "Admin", sense contrasenya.

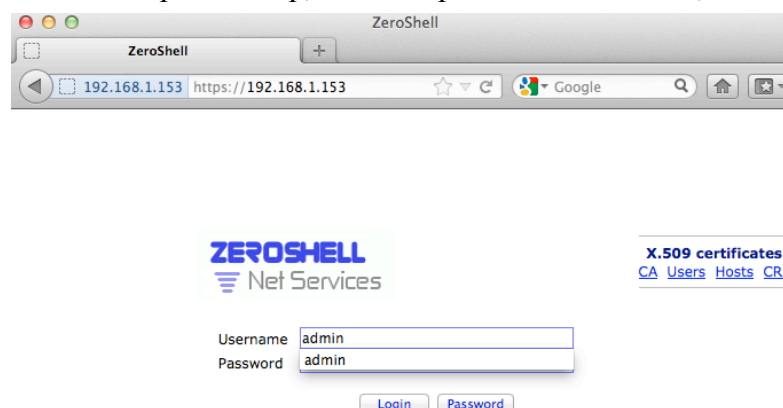
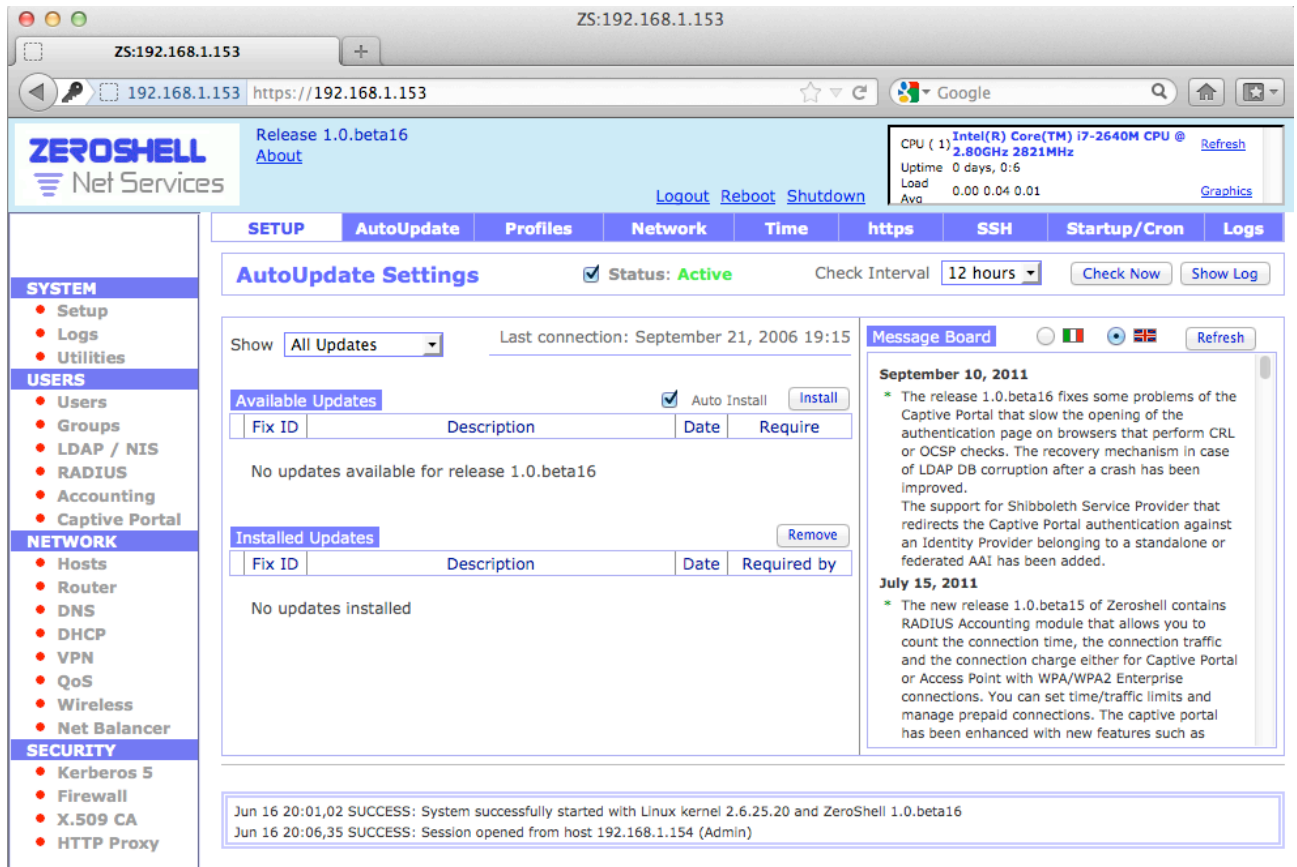


Figura A9. Finestra de validació en el sistema ZeroShell

Com podem veure a la següent figura, en el menú de l'esquerra tenim tots els paràmetres que podem configurar. Entre ells els que ens feien falta en aquest projecte RADIUS i LDAP.



*Figura A10. Interfície d'Administració ZeroShell*