Disseny e implementació de una xarxa sense fils

Informe de disseny e implementació

Director de projecte: Victor Carceler
Alumne: Josep Manel Pulpillo Lopez (EI)
Data: 25 de maig de 2006

CONTINGUT

1 VISIÓ GENERAL DEL PROJECTE

El projecte consisteix en l' aplicació practica i real de les tecnologies sense fils actuals per l' ampliació dels serveis d' accés a la xarxa TCP / IP en una empresa.

Les tecnologies sense fils formen part cada cop mes de la nostra vida quotidiana i naturalment les empreses també incorporen aquestes tecnologies en àrees

Les necessitats de les empreses en temes de seguretat o disponibilitat son mes elevades que en casos particulars, i les tecnologies sense fils varen començar amb certes febleses en aquests àmbits.

Però actualment ja hi ha tecnologia prou desenvolupada i fiable perquè les empreses puguin implementar instal·lacions sense fils de transmissió de dades per ampliar el accés a la seva xarxa local de dades amb la seguretat de que només els usuaris autoritzats tindran accés als recursos disponibles i amb la garantia de que els equips actuals donaran el nivell de qualitat i de rendiment adequat a les expectatives.

Les xarxes sense fils de dades, també conegudes com xarxes "wireless" o Wifi son, una extensió dinàmica de la xarxa local de una empresa, i permet absorbir les necessitats de connexió intermitents, amb solucions senzilles, ràpides i de poc cost d' infrastructura per les necessitats de connexió mòbil dels seus col·laboradors.

El fet de utilitzar el mitja aeri per la seva transmissió es el seu punt mes feble ja que dona una visió de vulnerabilitat en el accés no autoritzat i pèrdua de confidencialitat així com una sensació de manca de garantització de qualitat de servei.

Però les tecnologies actuals ja permeten la implementació de xarxes sense fils segures, fiables i disponibles en entorns empresarials.

Amb l' aplicació practica de les tecnologies de xarxes locals sense fils, aquest projecte pretén explorar aquesta tecnologia dins del entorn empresarial, dissenyant l' implementació d' una xarxa sense fils per a una empresa per ampliar el accés dels seus usuaris i els seus col·laboradors externs a la xarxa corporativa.

2 METODOLOGIA DE TREBALL

La metodologia a seguir en aquest projecte ha estat la de un desenvolupament clàssic (Especificacions anàlisi i disseny / implementació).
Dins de les primeres fases he descrit les especificacions del projecte, determinant els objectius a cobrir i per altra banda he desenvolupat el anàlisi funcional del sistema a construir valorant les necessitats i avaluant l' enfoc mes adient que abarqui els objectius proposats en el les especificacions indicades.

La fase de disseny e implementació ha estat el punt en el qual he definit la tecnologia especifica a utilitzar que complís amb l' anàlisi desenvolupat i també he dissenyat les configuracions necessàries per dur a terme la instal·lació del sistema definit.

Les fases del projecte han estat :

FASE 0: INICI - PLA DE TREBALL

Preparació del pla de treball a seguir, basant se en uns objectius molt genèrics i dissenyant un calendari de fases i tasques a realitzar.

FASE 1: ESPECIFICACIONS INICIALS

Aquesta primera fase ha consistit en la descripció dels requeriments específics que vol cobrir el sistema a desenvolupar,
es centrarà, aquesta fase, en el coneixement i recerca dels productes del mercat mes adients per aplicar a les necessitats descrites.

FASE 2: ANÀLISI FUNCIONAL

Aquesta fase ha estat enfocada al anàlisi de les necessitats especifiques a cobrir i a conèixer les diferents tecnologies que poden donar suport a l' implementació de una solució per als requeriments especificats.

FASE 3: DISSENY E IMPLEMENTACIÓ

En aquest punt s' ha desenvolupat el document de disseny de la solució seleccionada. Aquest document descriu les tecnologies a utilitzar, topologies, configuracions i desenvolupaments, si escau, que s' han seleccionat en la fase anterior.
Cal incloure amb detall, tots els processos i sistemes que han d' intervenir en aquest projecte per poder detectar qualsevol necessitat i trobar-hi les solucions adients.

FASE 4: TEST

Per últim, a la fase de test es prepara un document de casos de test per avaluar el bon funcionament del sistema segons la configuració dissenyada en fases anteriors.
Els processos a realitzar en aquesta fase son bàsicament les proves definides i el lliurament de la documentació final composada per la memòria i la presentació.

3 AVALUACIÓ I SELECCIÓ DE LA TECNOLOGIA

INTRODUCCIÓ

La tecnologia de xarxes inalàmbriques es la que permet la transferència de dades utilitzant radio freqüència en lloc de cable de coure o fibra òptica.

Actualment aquesta tecnologia ja aporta la capacitat de transmetre dades a velocitats properes a les velocitats de transmissió que s' utilitzen habitualment en les xarxes locals de cable i per tant ja es una opció valida per ampliar o complementar les xarxes locals tradicionals (LAN's) o en alguns casos per ser utilitzada com a enllaç sense fils entre edificis o instal·lacions separades pocs quilòmetres.

Les xarxes sense fils actuals treballen en les bandes de 2,4 i 5 GHz que son bandes lliures sense necessitat de demanar llicencia, i això els aporta una flexibilitat molt atractiva.

En aquest projecte no parlarem de les tecnologies de transmissió cel·lular mòbil també conegudes com telefonia mòbil, tot i que actualment amb les tecnologies de 3G, les comunicacions sense fils mòbils i les xarxes sense fils cada cop estan mes a prop i ofereixen serveis de l' altre tecnologia.

TIPUS DE XARXES SENSE FILS

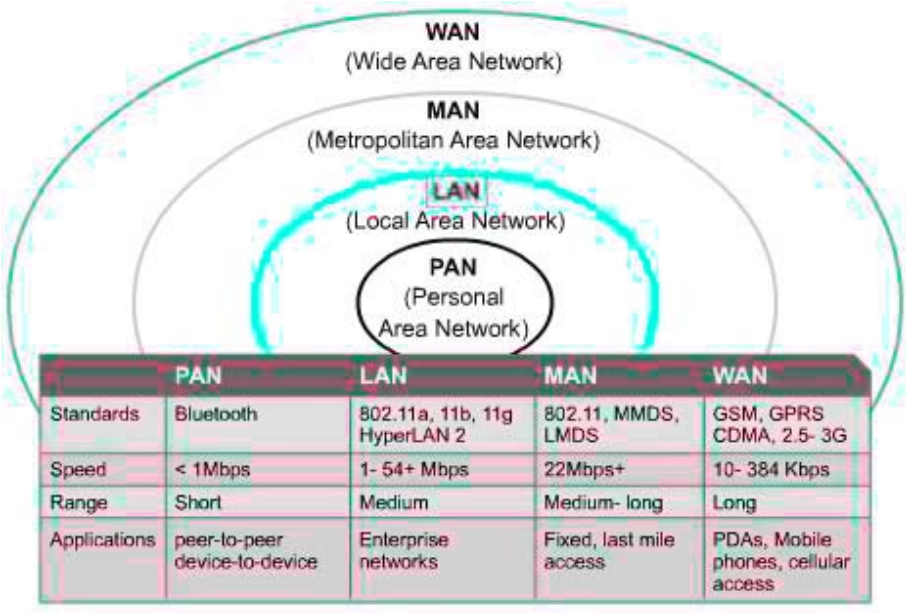
3.1.1 Descripció

L' evolució continua de les xarxes sense fils fa que les tecnologies mes modernes substitueixin les anteriors sense que aquestes hagin pogut desenvolupar tot el seu potencial.

Mirarem de fer una petita descripció de les tecnologies actuals i ens centrarem en les xarxes sense fils d' àrea local (WLAN) que es el focus principal d' aquest projecte.

Les xarxes sense fils s' agrupen en tres grans grups. Les xarxes de curt abast WPAN (Personal) les xarxes de mitja abast WAN (Wireless area networks) i les de gran abast (WMAN) Metropolitan area network.

Les xarxes nomenades WAN (Wide Area Network) son les xarxes de telefonia mòbil en las quals no aprofundirem en aquest projecte.



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HyperLAN 2	802.11, MMDS, LMDS	GSM, GPRS CDMA, 2.5- 3G
Speed	< 1Mbps	1- 54+ Mbps	22Mbps+	10- 384 Kbps
Range	Short	Medium	Medium- long	Long
Applications	peer-to-peer device-to-device	Enterprise networks	Fixed, last mile access	PDAs, Mobile phones, cellular access

3.1.2 Xarxes de curt abast

En les primeres (PAN) el Standard actual son les xarxes bluetooth que operen a curtes distancies.
Treballen en la freqüència de 2.4 Ghz i estan dissenyades per connexions dispositiu a dispositiu a velocitats moderades (1 a 2 Mbits)
La seva arquitectura es arborescent, on un dispositiu actua com a master i pot acceptar fins a un màxim de 7 connexions (esclaus) encara que les transferències es realitzen un a un de forma rotativa

Tot i que hi ha algunes especificacions per mes distancies (Classe 1 fins a 100 mts) s' utilitzen quasi exclusivament per a curtes distancies.
Aquest tipus de xarxa s' ha convertit en l' estàndard de facto en la fabricació de dispositius sense fils de curt abast i s' està introduint en la vida quotidiana en l' automòbil, els dispositius de veu o àudio i en identificació a distancia.

Ell nostre projecte esta focalitzat en l' us de xarxes sense fils en oficines i per tant aquest tipus de xarxes no son les adequades.

3.1.3 Xarxes d' abast metropolità

Es en aquest entorn en el que hi ha mes moviment actualment, ja que les tecnologies cada cop ofereixen mes velocitat de transmissió, mes radi de cobertura i menys consum elèctric.
Aquesta evolució fa que les xarxes WMAN, tot i com el seu nom indica estan dissenyades per gran abast, poden ser una tecnologia a tenir en compte també per a ser utilitzades en les xarxes sense fils locals.
Les tecnologies actualment utilitzades MMDS LMDS son tecnologies punt multipunt utilitzades per difusió de senyal de àudio i vídeo. Treballen en la banda de 27 a 31 Ghz pero poden ser desbancades ràpidament amb noves tecnologies mes rapides i amb mes radi de cobertura com son WiMax o 802.20
Actualment hi ha una lluita entre els fabricants de dispositius per determinar el estàndard de llarg abast mes utilitzat entre WiMax i 802.20.
En el apartat de tecnologies emergents parlarem amb mes detall d' aquestes xarxes

3.1.4 Xarxes de abast local

En aquest àmbit, que es en el que ens centrarem nosaltres, hi ha actualment un estàndard definit per l' organització americana IEEE que es el 802.11, també conegut com Wi-Fi (Wireless Fidelity).

El protocol 802.11 es el que descriu les comunicacions sense fils per xarxes locals (WLAN) i que esta tutoritzat per el organisme internacional IEEEE.

Dins d' aquest grup de treball (802.11) s' han definit diferents Standard en quant al sistemes de transmissió, les bandes, la seguretat … Per això aquests Standard també son coneguts com els 802.11x (no confondre amb 802.1x).

Les especificacions tècniques d' accés al medi es descriuen en els sub protocols 802.11b 802.11g 802.11a.
L' especificació 802.11i descriu els sistemes de seguretat a implementar en xarxes sense fils. El desenvoluparem mes endavant

L' especificació 802.11n parla sobre xarxes sense fils d' alta velocitat, que també descriurem breument en les tecnologies emergents.

L' especificació 802.11e parla sobre els protocols de priorització i qualitat de servei en xarxes sense fils.

DESCRIPCIÓ TECNOLOGIA 802.11

3.1.5 Arquitectura

La arquitectura lògica de 802.11 consisteix en els components :

Conjunt Bàsic de servei(BSS). Descriu L' arquitectura bàsica de comunicació amb un punt d' accés i uns equips clients. Es una arquitectura de infrastructura i també es nomena Cel·la o àrea de cobertura. Un BSS te un identificador que es nomena SSID.

Hi ha un sub component (IBSS) que descriu les comunicacions entre dos equips exclusivament (peer-to-peer) Aquest component també es conegut com AD-HOC.

El component de distribució (DS) determina la distribució dels BSS per definir un domini de cobertura i ofereix els serveis necessaris per la gestió de roaming.

El component ESS consisteix en l' arquitectura coordinada de varis conjunts bàsics de serveis connectats entre si per mitjà de una xarxa de cable i utilitzant el component de distribució de serveis per implementar serveis com el roaming.

3.1.6 Protocols de transmissió

El protocol 802.11b descriu el sistema de comunicació utilitzant tecnologia de transmissió DSSS. Treballa en la banda de 2.4Ghz i pot transmetre dades a una velocitat de fins a 11 Mbps.

El protocol 802.11g treballa en la mateixa banda de freqüències que 802.11b i amb el mateix protocol físic de transmissió (OFDM) que consisteix en una tècnica de divisió ortogonal de freqüències per aconseguir, per una banda majors velocitats de transmissió (fins a 54 Mbps) i compatibilitat amb el equipament que treballa en la banda de 2.4 Ghz.

Aquest protocol permet la coexistència de transmissions de 802.11b i 802.11g sense interferències ja que els dispositius 802.11b poden "veure" les trames 802.11g però no descodificar les.

La banda de 2.4Ghz te, a mes a mes de les transmissions generades per dispositius 802.11b 802.11g altres dispositius que operen també en aquesta banda de i que causen interferències com son els dispositius bluetooh i els dispositius telefònics sense fils.

La especificació 802.11a descriu el sistema de comunicació sense fils utilitzant tecnologia de divisió ortogonal de freqüències (OFDM). Aquest protocol opera en el rang dels 5 GHz aconseguint d' aquesta forma evitar les interferències existents en la banda de 2.4 GHz.

La tecnologia de codificació que utilitza es diu OFDM i consisteix en la divisió de del canal de comunicació en subcanals i la transmissió simultània en 48 dels 52 subcanals, enviant part de les dades en cadascun d' ells. Els subcanals son ortogonals (de freqüències independents entre ells)

Com el medi de transmissió es compartit, aquestes tecnologies utilitzen un sistema de compartició del medi que es diu CSMA/CA (carrier-sense multiple acces collision avoidance). Es un sistema molt similar al utilitzat en les xarxes de cable ethernet .

El protocols CSMA/CA prova de reduir la possibilitat de col·lisió quan s' intenta transmetre en el mitjà compartit. El protocol consisteix en escoltar el medi i si esta ocupat, esperar. Quan es detecta el medi lliure després de d' haver esperat, s' aplica un temps addicional d' espera calculat aleatòriament ja que es molt probable que altres dispositius també estiguin esperant per transmetre.

Addicionalment, aquest protocol envia trames de informació general per informar de que els vol transmetre (RTS / CTS) i de quan tems es necessita transmetre per informar els altres dispositius i ordenar el accés al medi

3.1.7 Seguretat

Les xarxes sense fils son especialment vulnerables als atacs especialitzats degut al seu accés físic i a la seva joventut.

Les seves vulnerabilitats mes importants son :

- Autenticació només per dispositiu. Això permet a persones no autoritzades amb dispositius autoritzats accedir a la xarxa.
- Encriptació simple (WEP) Es un sistema poc efectiu per encriptar dades
- Mala integritat dels missatges. El sistema de integritat (ICV) també es poc segur i fàcilment manipulable

Degut a la poc fiable seguretat presentada per les xarxes sense fils en el seu Standard 802.11, aquestes han estat poc incorporades a les empreses fina a l' aparició del primer esborrany del protocol 802.11i on es defineixen noves tècniques per resoldre les vulnerabilitats detectades.

La primera versió del protocol 802,.11i no finalitzada ja va proposar unes importants millores en la seguretat de les xarxes sense fils enfocades a resoldre les deficiències esposades. Aquesta primera versió o esborrany es coneix com protocol WPA.

Les mesures de seguretat proposades per WPA son :

- Autenticació per usuari utilitzant protocol d' autenticació 802.1x, un protocol d' autenticació ja utilitzat en xarxes de cable basat en servidors d' autenticació RADIUS.
- Encriptació utilitzant sistemes com TKIP (temporal key integrity protocol) per encriptar les transmissions.
- Integritat de missatges (MIC) es el protocol de verificació redundant de integritat de les dades que substitueix a CRC.

El protocol 802.11i (WPA2) ha estat aprovat definitivament amb unes recomanacions encara mes complexes i segures en l' àrea d' encriptació de missatges en el que demana l' us del protocol d' encriptació AES (Advanced Encryption system) tot i que degut a la seva complexitat en els càlculs, es recomanable l' us de dispositius hardware que el implementin.

3.1.8 Procés d' autenticació

El procés d' autenticació 802.1x recomanat per IEEE 802.11i es basa en que el client que demana identificar se, envia les seves credencials a un servidor d' autenticació intermedi (proxy RADIUS) que gestiona el establiment de connexió i enviament de credencials y les passa a un servidor d' identitats que valida les credencials.

El protocol utilitzat per la transferència de les credencials entre el client (suplicant) i el servidor RADIUS es nomena EAP (Extensible authentication protocol) i els servidors RADIUS suporten diferents variacions d' aquest protocol (LEAP, PEAP, EAP-TLS ...)

Tant EAP-TLS com PEAP estan basats en infrastructura de clau publica (PKI) per encriptar les comunicacions entre el client i el servidor RADIUS i garantir l' autenticitat dels participants en el procés d' intercanvi i validació de credencials

3.1.9 Procés d' encriptació

El procés d' encriptació TKIP es el que s' utilitza per l' encriptació del tràfic de dades entre el client i el punt d' accés.

Es basa en el algoritme RC4 per l' encriptació de les dades i utilitza un vector d' inicialització (IV) de 48 bits i en una clau temporal diferent per encriptar cada paquet.

El sistema d' intercanvi del vector d' inicialització i la primera clau temporal es realitza en dos fases.

Per a la garantització de l' integritat dels paquets s' utilitza el algoritme MIC. Aquest algoritme inclou un numero de seqüència al missatge i genera una clau hash de les dades i la seqüència per garantir l' integritat del missatge

COBERTURES

La finalitat de la tecnologia que s' avalua es la conectivitat dins de oficines o espais curts.

Els espais dins d' edificis son molt variats i poden afectar de forma molt important la qualitat de la senyal degut al material del mobiliari, als murs i portes, als sostres, vigues i altres components de construcció.

Amb aquest enfoc, cal seleccionar una tecnologia de abast mitjà amb un ample de banda alt per permetre l' us dels sistemes informàtics gràfics i la transmissió de imatges de forma semblant a les xarxes locals de cable.

El tipus d' antenes a utilitzar han de ser omnidirecionals o de paret (patch walls) per donar una cobertura amplia i general al àrea de treball.

Es difícil avaluar l' àrea de cobertura de forma teòrica perquè, com ja comentava, depèn molt del materials de construcció i per això cal mesurar les cobertures per definir quantes antenes caldrà instal·lar.

ALTRES TECNOLOGIES EMERGENTS

Les noves tecnologies sense fils actuals estan derivant en millorar la capacitat de transmissió de les xarxes sense fils, augmentar el àrea de cobertura i disminuir el consum d' energia, per anar guanyant terreny al cable.

La demanda de ample de banda fa que noves tecnologies sense fils pugnin per succeir el 802.11 actual en les seves tres versions mes conegudes (a,b,g)
Inicialment hi ha dos competidors que son WiMax (802.16) i 802.20. Aquestes dues tecnologies es basen en millorar les mancances de la tecnologia sense fils actual oferint mes ample de banda, mes distancia de cobertura i mes seguretat en les seves comunicacions.

El protocol 802.20 treballa en la banda dels 3.5 GHz i aporta capacitats de 1 Mbps a 15 Km de distancia. Te l' avantatge que s' ha dissenyat des de zero i l ' inconvenient de que es competència de les tecnologies de telefonia mòbil.
Es una tecnologia enfocada a cobrir el àrea d' enllaç amb el usuari final (la darrera milla) competint amb les connexions ADSL per cable,
Un altre característica interessant d' aquesta tecnologia es la seva capacitat de transmissió amb els dispositius en moviment a alta velocitat (fins a 250 Km/h) que la fa atractiva per implementar en trens.

El protocol 802.16 també conegut com WiMax treballa en la banda de 2 GHz a 6 GHz i les seves característiques son similars al protocol 802.20.
WiMax proporciona una cobertura de fins a 50 Kms sense necessitat de vista directa amb les estacions de treball. El ample de banda que pot proporcionar es fins a 70 Mbits/s
També aporta un sistema d' encriptació basat en certificats (tecnologia PKI) que la fa molt atractiva per la seva seguretat.

Un altre tecnologia, en la mateixa línia que les anteriors, sembla que pot ser finalment el nou successor de wifi 802.11. Aquesta tecnologia te com a gran avantatge a les altres dos que es compatible amb el protocol 802.11 ja que es 802.11n.
Aquest nou protocol que ha estat aprovat recentment, aporta una gran ample de banda (300 Mbps) basant se en una tecnologia de transferència simultània per varis canals nomenada MIMO (Multiple input Multiple output).
Aquest protocol te moltes opcions de ser el pròxim protocol de transmissió de dades IP perquè s' ha dissenyat compatible amb els protocols actuals i basa la seva força en la transmissió simultània utilitzant varies antenes.

Però una tecnologia emergent amb moltes possibilitats de futur es la UWB (Ultra Wideband). Aquesta tecnologia es basa en la transmissió de gran quantitat d' informació (500 Mbps) a curtes distancies.

En lloc de la tecnologia tradicional d' emissió, aquesta tecnologia UWB treballa utilitzant un ampli ventall de freqüències a molt baixa potencia, inclòs per sota del soroll de fons de les senyals actuals.

Aquest sistema de treball fa aquesta tecnologia molt adient per a distancies curtes ja que no interfereix amb altres senyals degut al seu ampli espectre de treball i la seva baixa potencia de transmissió. UWB treballa emeten polsos electromagnètics de alta freqüència i molt baixa durada.

En lloc d' utilitzar una senyal portadora, UWB esta composta de series intermitents de polsos que varien l' amplitud, la polaritat i el temps. Utilitzant un esquema de modulació bipolar.

La seva feblesa radica en la correcta detecció de la senyalització que si que esta distorsionada per altres senyals electromagnètiques al mateix espectre.

Cal que el desenvolupament dels receptors de UWB es facin molt sofisticats per poder distingir les distorsions generades per altres fonts d' emissió al voltant. S' utilitzen tècniques de transmissió múltiple i recepció per comparació en temps real per decidir quin valor de transmissió es el correcte.

Es una tecnologia que te les seves aplicacions en la llar i la oficina, per a la transmissió de àudio i vídeo entre equips mòbils.

També te, fins i tot, altres aplicacions gràcies al sistema de transmissió per polsos ja que aquesta característica permet utilitzar la UWB com a sistema de posicionament local.

Els polsos emesos poden utilitzar se per la detecció de objectes que portin un emissor, utilitzant varis receptors al voltant.

SELECCIÓ DEL EQUIPAMENT

3.1.10 Decisions estratègiques

A l' hora de decidir quina tecnologia utilitzar per a fer l' implementació de la xarxa sense fils, he tingut en compte que aquest tipus de tecnologia evoluciona molt ràpidament i que es important seleccionar una tecnologia prou madura per donar un servei adequat, tenint en compte que l' evolució la farà obsoleta aviat.

Sembla que la tecnologia actual mes madura i amb mes productes al mercat es la que compleix l' estàndard 802.11g, recolzada per els protocols de seguretat descrits en el protocol 802.11i que descriuen sistemes d' autenticació i encriptació raonablement segurs.

3.1.11 Estudi de cost

Els objectius econòmics del projecte s' enfoquen en l' inversió d' una partida pressupostaria definida per ampliar els sistemes d' accés a la xarxa de l' empresa.

El pressupost definit en un inici inclou l' inversió necessària per cobrir l' objectiu tecnològic amb el marge de seguretat adequat marcat per la política de seguretat definida pel departament d' informàtica de l' empresa. Això vol dir que es va definir un pressupost per a el equipament inalàmbric tenint en compte que calia assegurar el compliment de les normes de seguretat en el accés a la xarxa, ja que aquestes tecnologies poden donar cobertura àrees no desitjades fora del àmbit físic de les dependències de l' empresa.

L' inversió es va definir en 3000 euros per una seu de pocs elements sense fils, i 8000 euros per la seu central, tenint en compte un promig de 2 equips per una seu petita i 5 elements per una seu gran o per a la seu central.

Dins l' inversió s' inclou l' instal·lació de punts de xarxa a les oficines per a la connexió de les antenes, així com els equipaments sense fils i no s' inclou les

ampliacions de maquinari necessàries per aquells equips portàtils que desitgin utilitzar la xarxa sense fils

El retorn de l' inversió es fa difícil de calcular degut a que es basa en la millora o ampliació de un servei però es pot valorar en :

Cada cop que s' utilitza una sala de reunions i es necessita connexió a xarxa, cal que el departament d' informàtica proveeixi d' un element de xarxa (commutador) i cablejat auxiliar de xarxa per a la connexió.

La disponibilitat de l' informació corporativa en àrees comuns afavoreix la millora en la presa de decisions i optimitza els temps dedicats a reunions amb dades fixes.

Per últim la versatilitat en l' accés a la xarxa des de àrees sense connexió física a la xarxa també millora la qualitat en el servei global informàtic donat a l' empresa

3.1.12 Descripció de la tecnologia

La arquitectura tradicional de les xarxes sense fils consisteixen en un o varis punts d' accés que cobreixen un àrea de connectivitat sense fils.
Aquests punts d' accés son, en realitat, antenes que incorporen la tecnologia de microones per a la transmissió i recepció de dades amb els clients i la tecnologia de gestió de la seguretat i l' accés al mitjà de dades de cable.

Actualment esta apareixen al mercat de les xarxes sense fils una arquitectura que separa les funcions per especialitzacions de forma que els equips encarregats de la gestió de les transmissions per microones no s' encarreguen de cap tractament de les dades.
Hi ha un altre equip especialitzat que realitza la gestió de la configuració i de la seguretat en l' accés de les dades a la xarxa troncal de cable.

Aquesta segona arquitectura aporta una major seguretat en les transmissions de dades i el accés.
Els punts d' accés son equips especialitzats que depenen de un equip de seguretat central que els transfereix la configuració i verifica la identitat i la fiabilitat de les dades transmeses

La empresa Nortel Networks ofereix aquesta tecnologia en forma de uns punts d' accés especialitzats en la part de transmissió sense fils i uns commutadors de seguretat que donen la connectivitat als punts d' accés i gestionen la configuració i la seguretat en l' accés.

3.1.13 Descripció dels equips

Punt d' accés (Acces Point or Acces Port)

Es una antena omnidireccional que te una connexió ethernet per on rep l' alimentació elèctrica i les dades. Utilitza el protocol estàndard d ' alimentació elèctrica a traves d' ethernet (PoE) 802.3af.

Pot treballar en dues modalitats. Connexió directe amb un commutador de seguretat (WSS) o connectat directament a un commutador estàndard. En

aquest segon cas treballa com un equip TCP/IP connectat a la xarxa rebent les dades bàsiques de connexió a xarxa (IP, porta d' enllaç ...) a través del protocol DHCP. Es nomena llavors punt d' accés distribuït (DAP)

En els dos casos, cal que el equip estigui donat d' alta al commutador de seguretat amb la configuració de radio freqüència a utilitzar (radio-profile) especifica per cada antena.

WLAN Access Point 2330

Commutador de Seguretat inalàmbric (WSS)

Es un commutador d' accés a la xarxa de cable (switch) que te dues característiques bàsiques :

- Es un commutador de xarxa que te ports de connexió que serveixen dades i corrent elèctrica, complint el estàndard de potencia elèctrica a traves de ethernet (PoE) per poder alimentar als punts d' accés, que com hem vist reben l' alimentació elèctrica a traves del protocol PoE.
- Conté un software de gestió de la seguretat i de la configuració dels punts d' accés definits per poder :
    - Identificar els punts d' accés que depenen d'ell (tant els connectats directament com els connectats a traves de la xarxa (punts d' accés distribuïts)
    - Descarregar la configuració definida a cadascun d' aquests punts d' accés definits.
    - Gestionar el tràfic entre els punts d' accés i la xarxa tant a nivell de commutador com a nivell de supervisió de paquets TCP

4 DISSENY TOPOLOGIC DE LA XARXA

ESTRATÈGIA TOPOLOGICA

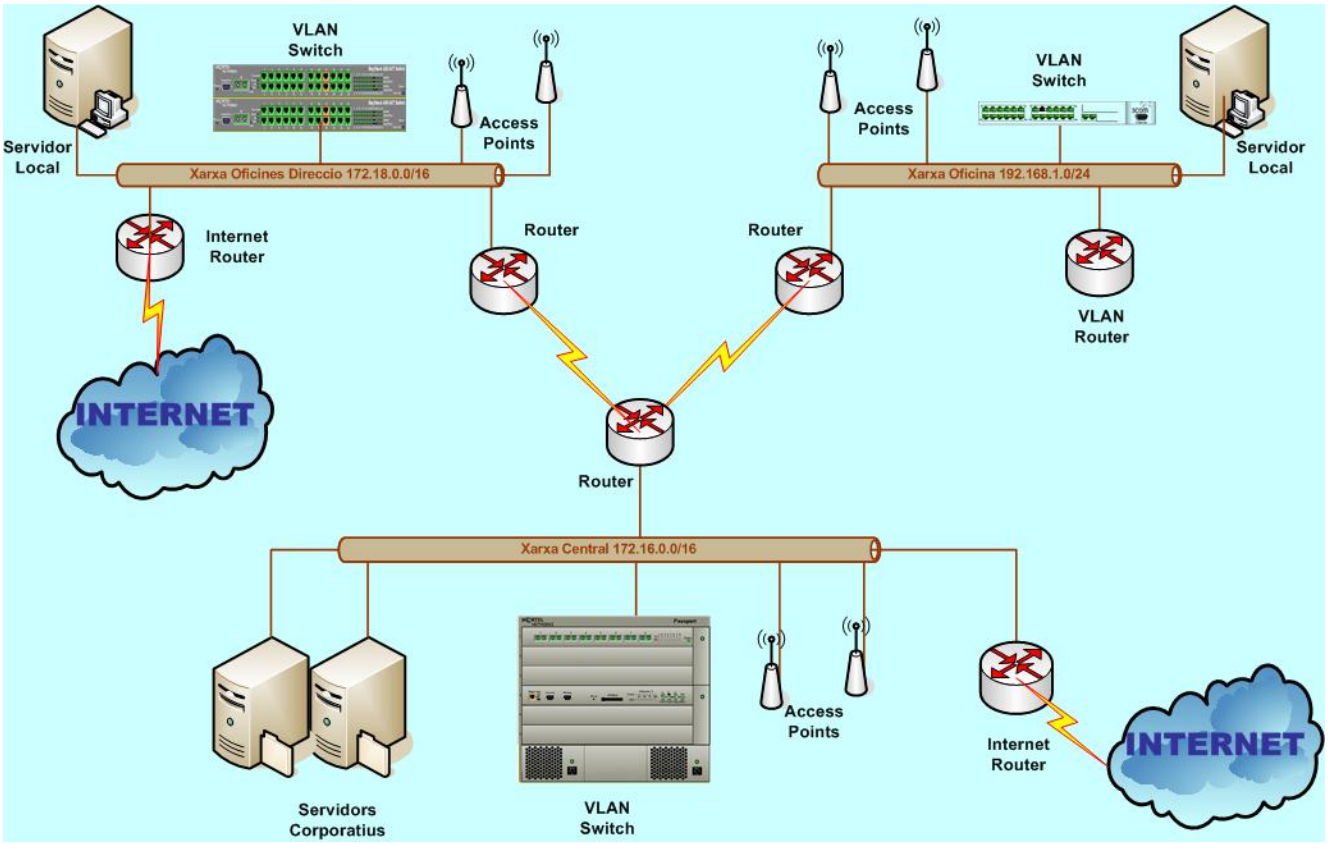
4.1.1 Disseny topologic

L' abast del projecte es la cobertura sense fils en les oficines centrals de l' empresa i en la oficina de direcció general de l' empresa.

La topologia de la xarxa de cable de l' empresa en una topologia en estrella on les oficines centrals tenen instal·lats els servidors centrals i hi ha línies de comunicacions WAN de connexió amb totes les oficines remotes de la companyia.

Aquest projecte pretén ser un model per poder implementar la mateixa solució a totes les oficines de l'empresa que necessitin un accés inalàmbric, però el projecte inicial s' implementa a les oficines centrals i a l' oficina de direcció general que esta separada físicament i connectada amb una línia WAN

El disseny topologic de la solució es el que es veu a la següent figura :



4.1.2 Definició del adreçament

Seguint el model definit en el document d' anàlisi, s' ha decidit l' utilització de xarxes virtuals (VLAN) per separar i així poder tractar en forma especifica els equips connectats a la xarxa sense fils en funció del grup.

Definim un adreçament IP de classe C per cada VLAN definida. Això ens porta a dedicar tres classes C per cada seu de la empresa en la qual es decideix instal·lar el accés inalàmbric.

En l' abast del nostre projecte definim dues seus, la seu central i la seu de direcció general situada en un altre ubicació i, per tant amb un altre adreçament.

La definició dels identificadors (tags) de xarxes virtuals serà el mateix per totes les seus

VLAN 101. Users Indicador de la xarxa virtual dedicada per als equips connectats inalambricament i que tenen nivell de usuaris corporatius.

El adreçament definit per aquests equips serà: **192.168.111.0 / 24 (Central)**

El adreçament definit per aquests equips serà: **192.168.114.0 / 24 (Direcció)**

VLAN 102. Devel Indicador de la xarxa virtual dedicada per als equips connectats inalambricament i que tenen nivell de usuaris cooperadors o de desenvolupament..

El adreçament definit per aquests equips serà: **192.168.112.0 / 24 (Central)**

El adreçament definit per aquests equips serà: **192.168.115.0 / 24 (Direcció)**

VLAN 103. Guest

Indicador de la xarxa virtual dedicada per als equips connectats inalambricament i que tenen nivell de usuaris convidats.

El adreçament definit per aquests equips serà: **192.168.113.0 / 24 (Central)**

El adreçament definit per aquests equips serà: **192.168.116.0 / 24 (Direcció)**

4.1.3 Encaminament

Com hem definit un adreçament específic per aquestes xarxes inalàmbriques, caldrà definir les als encaminadors locals de cada seu perquè les noves xarxes inalàmbriques puguin accedir als serveis de la xarxa, en funció de les seves autoritzacions.

Degut a la pròpia estructura d' adreçament de la seu, a cadascuna de les seus hi ha un equip encaminador central que coneix totes les xarxes locals a la seu.

Per aconseguir que els equips sense fils, amb l' adreçament definit a l' apartat anterior, puguin accedir als serveis disponibles a la xarxa, cal definir una adreça virtual al encaminador per cada VLAN que serà l' adreça de xarxa del encaminador.

Aquest encaminador utilitza un protocol de priorització de rutes e intercanvi d' informació sobre les rutes conegudes amb els altres encaminadors de la xarxa de l' empresa. El protocol utilitzat es OSPF.

Basat en aquest protocol, el encaminador informarà a la resta d' encaminadors de la xarxa que ell te una connexió amb les xarxes virtuals sense fils definides.

DESCRIPCIÓ DE LES AREAS DE COBERTURA

4.1.4 Tipus d' antenes

Bàsicament existeixen dos tipus d' antenes :

- Antenes direccionals

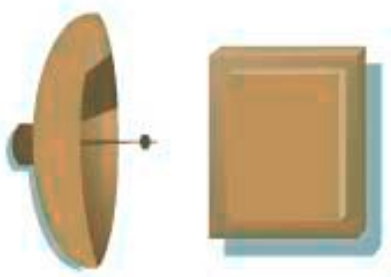
  Son antenes que radien la seva energia de radio freqüència en una direcció determinada predominantment.

  En funció de la seva forma es parla de antenes :

  Yagi (Antena tipus apuntador)

  Parabòliques (Antenes compostes per un plat parabòlic

  Patch (Antenes de Paret)



Directional

- Antenes omnidireccionals

  Son antenes que radien la seva energia en totes direccions de forma aproximadament igual.

  Els tipus mes habituals son :

  -Mastil

  -Dipol

Omnidirectional

Degut a que, en el projecte en qüestió, les àrees de cobertura son zones de curt abast com sales de reunió, el tipus d' antenes mes adient son les antenes

omnidireccionals. Aquest tipus d' antenes tenen un abast mes curt però amb un radi d' acció mes generalitzat.

4.1.5 Interferències

L' espectre d' emissió de radio freqüència utilitzat per les xarxes inalàmbriques es un espectre no regulat.

Això significa que no es d' us exclusiu per a les xarxes inalàmbriques i, per tant, poden haver altres emissors que generin ones que interfereixin amb les generades per els punts d' accés de la xarxa sense fils.

Com a exemple, els telèfons sense fils també treballen a l' espectre de 2,4 Ghz i generen interferències. En particular el protocol de transmissió de dades inalàmbric 802.11b es veu severament afectat per interferències generades per aquests i altres emissors.

A l' hora de decidir l' ubicació dels punts d' accés inalàmbric, es aconsellable evitar altres fonts d' emissió i conèixer els obstacles atenuants de senyal.

Aquests poden ser :

- Telèfons sense fils, forns microones
- Transformadors elèctrics, fluorescents elèctrics o llums de radio freqüència
- Portes tallafocs
- Cartó i paper en quantitat

4.1.6 Àrees de cobertura

Les àrees de cobertura de les antenes depenen del guany de l' antena.

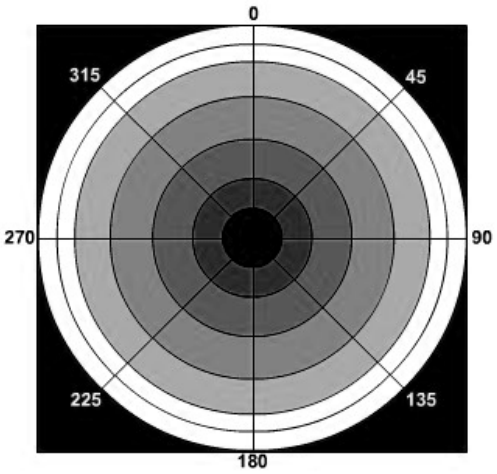
El guany de l' antena es la seva capacitat de enfocar la radiació que transmet en la direcció definida.

Aquest concepte es mesura en dBi

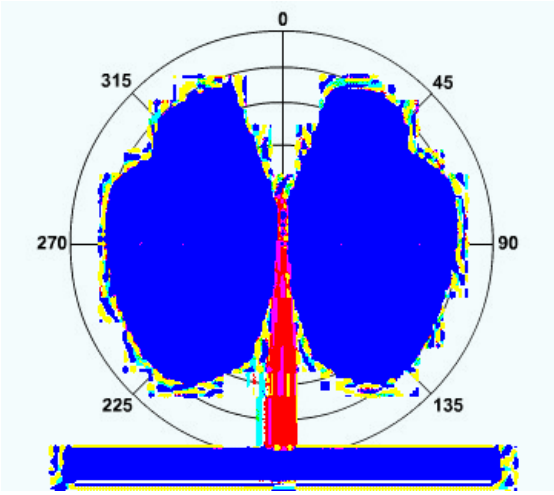
La necessitat de cobertura general en el projecte que s' esta desenvolupant, fa que calgui avaluar les àrees de cobertura generades per antenes omnidireccionals

A partir de un cert guany per una antena omnidireccional, ja no es millora substancialment l' àrea de cobertura, ja que l' antena emet en totes direccions.

Els mapes de cobertura per una antena omnidireccional seria :



Cobertura horitzontal

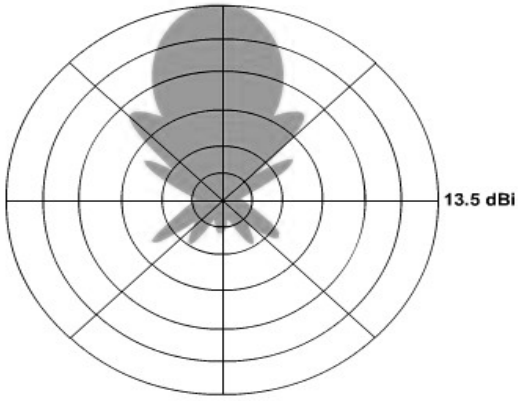


Cobertura vertical

Els dbi de les antenes omnidireccionals es mouen al voltant del 5 o 6 dbi.

En el cas d' antenes direccionals, s' utilitzen antenes de mes guany per que al direccionar la emissió, es pot aconseguir mes abast utilitzant antenes de mes guany.

Las antenes direccionals tenen un àrea de cobertura mes enfocada :



En aquest projecte només es faran servir antenes omnidireccionals.

Si l' àrea a cobrir es massa gran per una sola antena, es pot utilitzar mes d' una, tenint en compte que :

- Les antenes han de solapar el àrea a cobrir
- Per evitar interferències han de treballar en canals diferents.

El sistema de punts d' accés seleccionat decideix de forma automàtica el canal òptim d' emissió fent verificacions continues del estat del espectre i, si detecta alguna font d' emissió que pot ser causant de interferències selecciona un canal diferent.

EQUIPS DE CONTROL DE LA XARXA

4.1.7 Descripció dels equips de control

Els equips de control i gestió de la xarxa sense fils estan formats per dos tipus diferents de equips :

Punts d' Accés (Acces Point AP).

Aquests equips son, en realitat els equips de accés inalàmbric. Son antenes connectades a la xarxa de cable, que reben la configuració dels equips de control i que realitzen les tasques de gestió inalàmbric.

Commutador de control inalàmbric (Wireless Security switch WSS)

Els equips de control son commutadors de xarxa (switches) amb la característica de realitzar la gestió de configuració dels punts d' accés i, per altra banda, treballar com a commutador del tràfic rebut dels punts d' accés que gestionen.

Aquesta estratègia de separació de les funcions especialitzades de gestió de les connexions sense fils i gestió de tràfic de xarxa dona una major robustesa i fiabilitat a la arquitectura proposada.

4.1.8 Alimentació elèctrica

Els punts d' accés son equips que esperen l' alimentació elèctrica a través del mateix cable de dades.

Utilitzen el protocol estàndard (802.3af) d' alimentació elèctrica a traves del cable de dades per rebre la corrent elèctrica (PoE).

Així doncs, es necessari connectar els punts d' accés a un commutador especialitzat que doni connexió ethernet i alimentació elèctrica seguint aquest protocol.

Els commutadors de seguretat (WSS) ofereixen algunes connexions amb aquestes característiques que poden ser utilitzades per els punts d' accés si la connexió dels punts d' accés arriba al mateix armari de comunicacions on es instal·lat el commutador de control.

En cas contrari, quan el punt d' accés s' hagi de connectar a un commutador Standard caldrà :

- Utilitzar un commutador amb capacitats PoE (Power over Ethernet)
- Un injector de corrent que te una connexió d' entrada ethernet i una de sortida Ethernet + PoE

Existeixen alguns equips al mercat amb aquestes característiques :

Els equips **PowerDsine** son connectors PoE que reben una senyal de dades I serveixen una senyal unificada de potencia elèctrica I dades a traves de un cable Ethernet de categoria 5 o superior.

Es fabriquen en models de una connexió sis o dotze, permeten una gran flexibilitat a l' hora de connectar equips que necessiten alimentació elèctrica a traves del cable de dades com es el cas de les antenes a utilitzar.

SISTEMA DE GESTIÓ DEL ADREÇAMENT

4.1.9 Gestor del adreçament

Per a la gestió del adreçament de tots els equips a la xarxa, s' utilitza un servei de assignació dinàmica d' adreces (servei DHCP).

Degut al funcionament per broadcast del sistema d' assignació de IP del servei DHCP, cal crear un servei DHCP per a cada subxarxa o VLAN definida.

En aquest servei es defineixen els rangs de adreces a assignar al rebre una petició i els paràmetres bàsics de xarxa que s' assignaran al client que demana l' adreça IP.

Com en el cas que es defineix actualment es treballa amb diverses VLAN gestionades per un commutador / encaminador central, es aquest equip el que rep les peticions de IP amb protocol DHCP dels equips clients que accedeixin a la xarxa sense fils.

Per tal de re-dirigir aquestes peticions al equip gestor d' adreces dinàmiques central, cal configurar el encaminador per que realitzi tasques de "proxyDHCP".

Aquest servei de "proxy DHCP" recull una petició del client de una VLAN especifica de la xarxa sense fils i realitza una petició d' aquesta adreça al servidor DHCP en nom del equip client.

En el gestor del adreçament s' indiquen també les reserves de IP que es facin per tal de assignar una mateixa IP sempre al mateix equip o per tal de informar de que una adreça IP esta utilitzada sempre per un equip específic.

4.1.10 Adreçament dels equips clients sense fils

Per a cada rang de IP que es vol assignar es defineixen els paràmetres o valors bàsics de descripció de la xarxa que el client DHCP necessita per operar a la xarxa,

Aquests valors son :

El rang d' adreces disponible per servir.

Les adreces a excloure del rang (si hi ha)

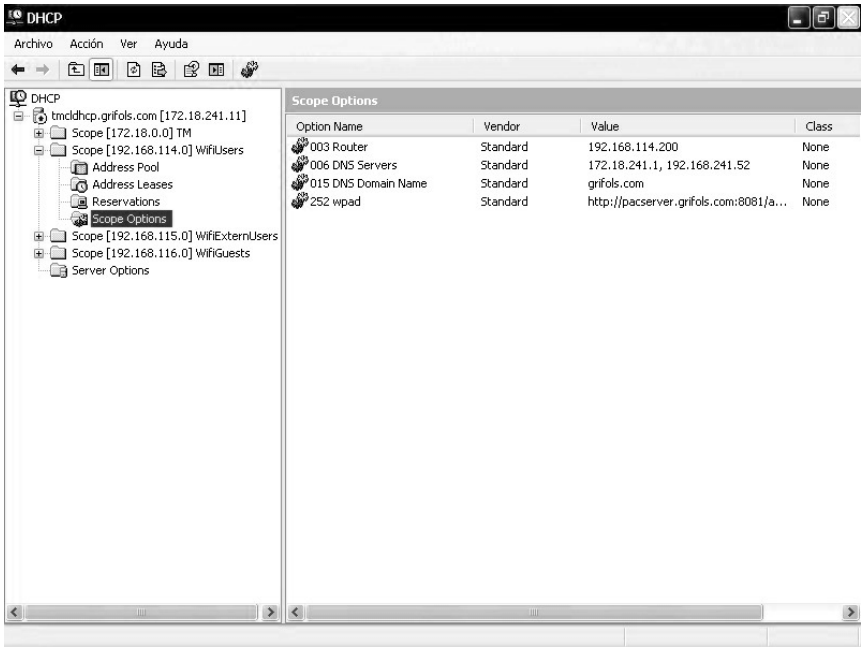
L' adreça de la porta d' enllaç: Per cada rang de IP hem definit l' adreça 200 com adreça IP de la porta d' enllaç d' aquella xarxa.

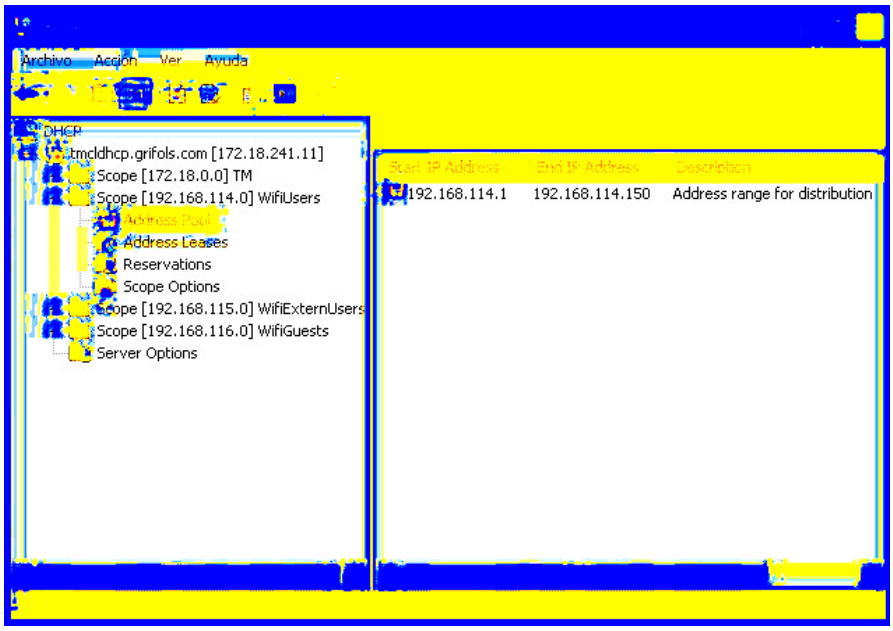
Per exemple, per a la xarxa 192.168.113.0/24 la seva porta d' enllaç es 192.168.113.200 que es l' adreça de la interfície del encaminador a aquesta xarxa.

El servidor o servidors de noms: Cada seu te un servidor local que es el servidor principal de resolució de noms. En el cas de la seu central hi ha dos servidors de noms. També es defineix un servidor secundari de la seu central per utilitzar en cas de caiguda del primari.

Principal : 172.17.241.5 Secundari 192.168.241.52

El nom del domini : S' utilitza com a nom de domini el nom de la empresa.





4.1.11 Adreçament dels punts d' accés

Els punts d' accés son antenes connectades a la xarxa que utilitzen protocol DHCP per rebre l' adreça de accés a la xarxa i els paràmetres bàsics.

Els punts d' accés estan a la xarxa de cable i han de tenir el adreçament específic de la xarxa de cable, es a dir, el mateix adreçament que altres equips en el mateix segment de la xarxa.

Després de la incorporació a la xarxa com a elements de xarxa, descarreguen la configuració dels equips de control de xarxa com ja comentaré mes endavant.

Per raons d' ordenació en l' adreçament, s' ha decidit assignar una IP especifica a cada antena de forma que sigui la mateixa sempre. Això es una reserva de IP.

Per fer això es defineix al servidor de DHCP una entrada per cada antena indicant la seva adreça de hardware o "MAC address". Aquesta es la adreça física assignada per el fabricant i es única.

Quan el servidor DHCP rebi una petició d' adreça de un equip amb una "MAC address" de la qual te una entrada, l' hi assignarà la adreça IP definida per aquella entrada.

4.1.12 Adreçament dels equips de control

Els equips de control inalàmbric s' els hi assigna una adreça IP fixa en el procés de configuració del equip, de forma que no utilitzen el servei DHCP per rebre l' informació de xarxa.

Tan els equips de control com les antenes estan en el mateix tram de xarxa, per tant tenen el mateix adreçament.

Els equips de controls son capaços de treballar amb VLAN's Això ens permetrà definir al port de connexió a la xarxa del equip de control el etiquetatge de les trames per la gestió dels paquets marcats per les diferents xarxes virtuals que des defineixen.

Aquesta part de definició de les xarxes virtuals es descriu mes endavant.

5 DISSENY DE LA SEGURETAT

REQUISITS DE SEGURETAT

Els requeriments del projecte demanen que els processos de seguretat siguin el mes estrictes possibles per garantir que cap intent d' accés a la xarxa sense fils no autoritzat tingui èxit.

Cal emmarcar aquests requisits dins del àmbit del parc informàtic de la empresa, es a dir, cal aconseguir la màxima seguretat possible amb els sistemes sense fils sense haver de substituir tots els equips actuals o fer una inversió excepcional en aspectes no imprescindibles.

Això vol dir que els requisits de seguretat han de marcar un mínim imprescindible de seguretat que estigui en consonància amb els portàtils que actualment utilitza la empresa.

Seguint aquests requisits marcats i tenint en compte que el nivell mínim de seguretat marcat ha de complir el estàndard 802.1x definirem l' estratègia de seguretat.

Els processos de seguretat tenen dos vessants: La física i la lògica.

SERVEIS BÁSICS D' ACCÉS

La seguretat física dels equips sense fils s' ha enfocat en el aspecte de selecció de un equipament que no es pugui manipular, per evitar intents de manipulació física als equips.

Els punts d' accés son antenes que no es poden configurar i que descarreguen la configuració dels equips de control inalàmbric. Per tant si un intrús intenta manipular una antena no pot aconseguir res mes que inutilitzar la. Gràcies al sistema de monitorització descrit mes endavant, el departament d' informàtica detectarà la no disponibilitat de una antena i actuarà en conseqüència.

En quant als equips de control, aquests estan instal·lats als armaris de comunicacions on també estan els equips commutadors.

Aquests armaris estan tancats amb clau i només hi tenen accés les persones autoritzades d' informàtica.

SERVEIS D' AUTENTICACIÓ

El sistema d' autenticació definit segueix l' estandard 802.1x de acceptació de credencials a traves d' un servidor proxy RADIUS amb un sistema de gestió d' usuaris Active Directory.

El procés consisteix en que el client envia les credencials al servidor RADIUS utilitzant un protocol de presentació (handshaking) que es nomena PEAP.

Aquest protocol es basa en l' enviament, per part del servidor, de un certificat de clau publica per encriptar el enviament de les credencials. D' aquesta forma, tota la comunicació de intercanvi i validació de credencials es fa utilitzant PKI i validant el certificat del servidor.

El servidor RADIUS trasllada al servidor d' identificació (Active Directory) les credencials del usuari. S' utilitza un protocol de desafiament resposta desenvolupat per Microsoft (MS-CHAPv2) a partir de un protocol estàndard nomenat CHAP

Quan el servidor RADIUS rep la acceptació de credencials per part del servidor d' identificació, llavors transmet els atributs definits en la política d' acceptació de la connexió. En el nostre cas,, en funció de la pertinença del usuari autenticat a un grup d' usuaris o altre definit en el servidor d' autenticació, el servidor RADIUS enviarà el atribut de etiqueta de xarxa virtual que l' hi correspon al usuari connectat (tag VLAN).

Tot el procés de autenticació que fa el servidor RADIUS, només es realitza amb aquells punts d' accés que s' han autoritzat a fer-ho en el servidor RADIUS, de forma que un punt d' accés no autoritzat, no pot realitzar peticions d' autenticació.

Aquest sistema d' autenticació garanteix que l' usuari que s' identifica es realment qui diu que es, i millora ostensiblement la autenticació per dispositiu que recomana la norma 802.11

SISTEMA D' ENCRIPTACIÓ E INTEGRITAT

El procés d' encriptació es realitza amb totes les trames enviades entre el dispositiu inalàmbric client i el punt d' accés.

Les especificacions del estàndard 802.11i indiquen que es necessari l' utilització de, al menys un dels dos sistemes d'encriptació següents :

- TKIP (Temporary Key Integrity Protocol)
- AES / CCMP (Advanced Encryption protocol.)

Hem decidit l' utilització del primer protocol que es prou segur per encriptar les comunicacions i evitar els intents de desencriptació.

Aquest protocol es basa en un algoritme d' encriptació potent, el RC4. un vector d' inicialització mes llarg (48 bits) i un sistema de generació de claus temporals rotatiu per l' encriptació de les trames variant la clau d' encriptació per evitar els atacs de força bruta.

Per últim, aquest protocol també incorpora un sistema de integritat de trames mes robust que els anteriors (MIC) que es basa en la signatura hash del missatge incloent en la signatura l' adreça origen i un número de seqüència per garantir que no ha estat manipulat.

El protocol d' encriptació AES es un protocol molt mes robust encara que TKIP que te com a petit inconvenient actualment un elevat cost de computació per els processos d' encriptació / desencriptació.

Es molt recomanable tenir hardware addicional per realitzar aquesta tasca. Com que no totes les targetes sense fils actuals incorporen hardware per realitzar

aquests processos, ens hem decantat per l' altre protocol que també es força segur.

SISTEMES DE CONTROL D' ACCÉS

La seguretat lògica en el accés als equips de control es basa en tres punts :

Evitar el accés físic als equips de control per evitar que s' utilitzi de forma no autoritzada el port sèrie de configuració que incorporen ja que tenen.

Desactivar tots els serveis d' accés als equips de control excepte aquell que s' utilitzi per configurar el equip. El servei que deixem activat es ssh per que es el que mes garanteix la seguretat en l' accés. Es un servei encriptat i garanteix que et connectes al equip de control presentant el seu certificat en la connexió.

Per últim, cal configurar el sistema d' identificació en l' accés al sistema de control ja que també es molt important a l' hora de garantir que només el personal autoritzat te les credencials per fer-ho.

Configurem un usuari i una paraula clau d' accés que s' emmagatzema en un sistema de informació confidencial que utilitza l' empresa. El departament d' informàtica te un procediment de canvi periòdic de claus en els sistemes crítics que, a partir d' ara inclourà els equips de control sense fils instal·lats.

6 CONFIGURACIÓ DELS SISTEMAS

CONFIGURACIÓ DEL SISTEMA D' AUTENTICACIÓ

6.1.1 Servidor d' autenticació (RADIUS)

Per a realitzar la autenticació i l' autorització d' accés a la xarxa utilitzem un servidor RADIUS.

El procés d' autenticació recull l' identificació proporcionada per usuari que s' identifica i la valida.. En aquesta instal·lació s' utilitzen identificadors i paraules clau per l' identificació. Aquest sistema d' identificació es diu PEAP (Protected Extensible Access Protocol). El protocol específic que s' utilitza es diu MS-CHAP v2.

Es un protocol de desafiament resposta encriptat desenvolupat per Microsoft.

El procés d' autorització es el que, un cop autenticat l' usuari, en funció de la pertinença a un grup de usuaris definit, de franges horàries o altres condicions, s' autoritza el accés i s' assignen uns atributs, en particular s' assigna la xarxa virtual a la que pertany el equip inalàmbric que s' ha autenticat.

Degut a que la empresa treballa amb un servei de directori actiu de Microsoft (Active Directory), s' ha seleccionat com a servidor Radius el servidor de Microsoft que es nomena IAS (Internet Authentication Service).

L' avantatge principal d' aquest component es que utilitza el servei de directori actiu com a repositori centralitzat de usuaris. El sistema d' autenticació es

basarà en les paraules clau que ja utilitzen els usuaris quan accedeixen a la xarxa sense fils que quan accedeixen als serveis de xarxa de cable (Servidor de fitxers, Sistema de correu electrònic Exchange ...).

Els grups d' autorització utilitzats en el servidor Radius per el accés de la xarxa sense fils es defineixen també al directori actiu.

6.1.2 Configuració del sistema de autorització

El servei d' autorització es basa en la pertinença a un grup d' usuaris per l' assignació dels paràmetres que siguin. En la implementació que es fa, la pertinença a un grup d' usuari serveix per assignar l' identificador de xarxa a la connexió.

S' han definit tres grups d' usuaris al directori actiu :

Wifi_Auth, Wifi_Devel, Wifi_Guest

Els usuaris s' assignaran al grup adient en funció de la xarxa a la que es vulguin incorporar.

Per tant si un usuari es del grup Wifi-Auth se l' assignarà l' atribut Tunnel = Users que es el nom de la xarxa virtual de usuaris de la empresa.

El servidor de control inalàmbric marcarà tots els paquets que transmeti l' equip d' aquest usuari amb la etiqueta de la xarxa virtual corresponent (VLAN Users)

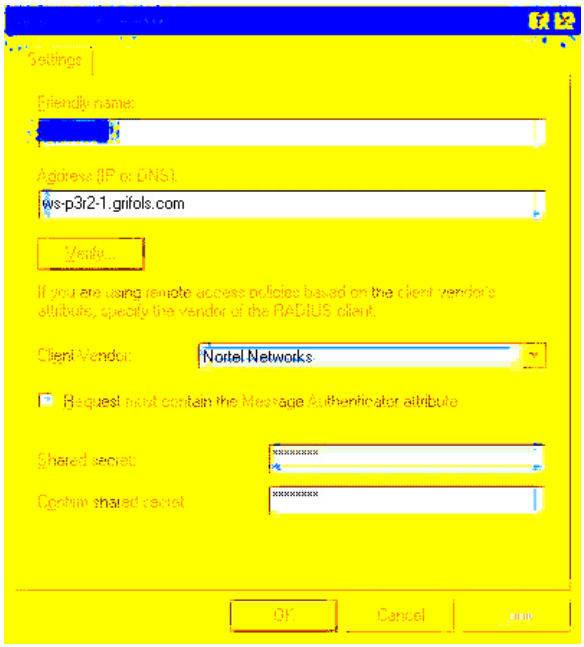
El servidor DHCP assignarà una IP del rang definit per aquesta xarxa virtual.

Després es defineixen unes llistes de control d' accés el equip de control inalàmbric per restringir els serveis accessibles a cada xarxa virtual.

6.1.3 Autenticacio del Client de consulta Radius

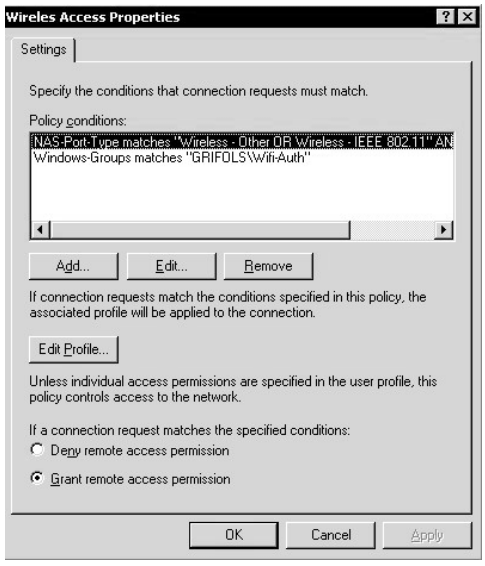
Cal que el equip que fa la consulta sobre la autorització d' accés a la xarxa sense fils sigui conegut per el servidor Radius.

Per això es dona de alta al servidor Radius el equip client que farà consultes, (el servidor de control inalàmbric) i es configura una paraula de pas (passphrasse) que coneixen tots dos i que s' intercanvien en la connexió per verificar l' autenticitat de la consulta



6.1.4 Configuració de les polítiques de Radius

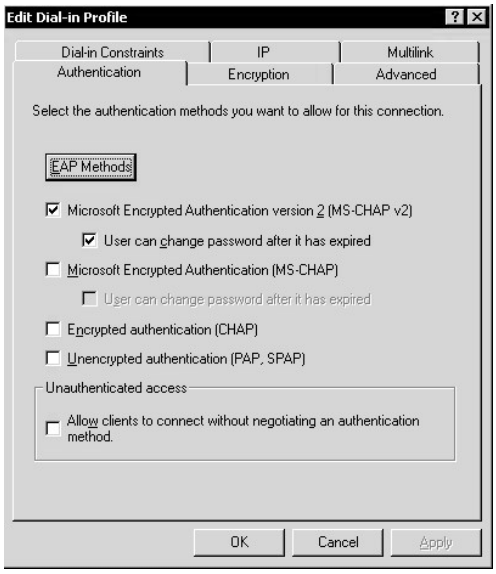
Les polítiques d' autorització a generar al servidor Radius son les que indiquen, per una banda quines han de ser les condicions a complir per que la política es pugui aplicar a la petició rebuda i, per l' altre quins son els mètodes de comunicació a utilitzar i els atributs a retornar en cas de acceptació de la petició d' autenticació rebuda.

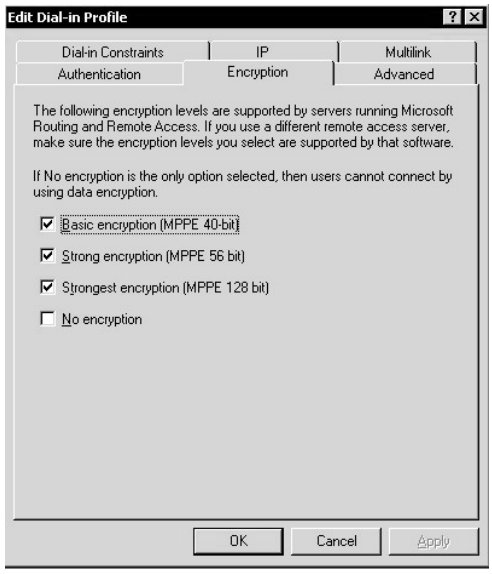


En el nostre cas les condicions a acomplir son :

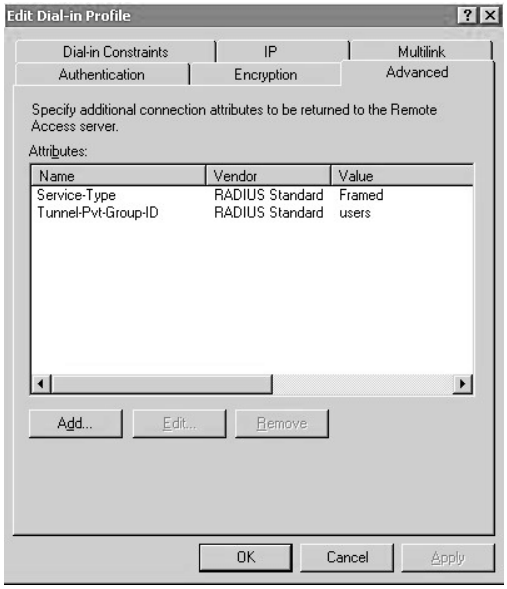
- Una petició d' autenticació que provingui de un client inalàmbric
- El identificador de la petició ha de formar par de un grup de identificadors validats de la base de dades (en aquest cas Active Directory)

Els mètodes d' intercanvi de credencials es defineixen a la política :





Si la política s' acompleix, es a dir el protocol d' intercanvi de claus es correcte, les credencials enviades son valides i les condicions de la política s' acompleixen, llavors el servidor d' autenticació retorna uns atributs definits que, en el nostre cas, indiquen la xarxa virtual a assignar al client autenticat.



CONFIGURACIÓ DEL ADREÇAMENT A LA XARXA

6.1.5 Xarxes virtuals (VLAN's)

La topologia de la xarxa te forma de estrella on l' equip central es un commutador amb capacitats d' encaminament.

En aquest commutador principal hi ha connectat altres commutadors on hi ha els equips d' usuari (PC's impressores ...) o els servidors i encaminadors connectats.

El commutador/encaminador principal utilitza un protocol d' encaminament per informar de les rutes conegudes als altres encaminadors de la xarxa (protocol d'encaminament OSPF).

Les xarxes virtuals es creen en el encaminador principal i es propaguen als commutadors que tenen equips connectats i que pertanyen amb aquestes xarxes virtuals.

Per que el commutador/ encaminador gestioni correctament les xarxes virtuals a crear per les connexions sense fils caldrà :

Crear les VLAN's a cada interfície del commutador per on hi haurà tràfic marcat amb la VLAN que correspon.

A tots els equips commutadors que hi ha entre el commutador central i el equip de control inalàmbric, caldrà activar el marcatge de paquets VLAN i configurar les VLANS a gestionar per tal de fer arribar el tràfic de les VLAN definides al equip de control inalàmbric

Definir el rang de IP's assignat a aquesta VLAN i definir una adreça de encaminador de defecte per cada VLAN.

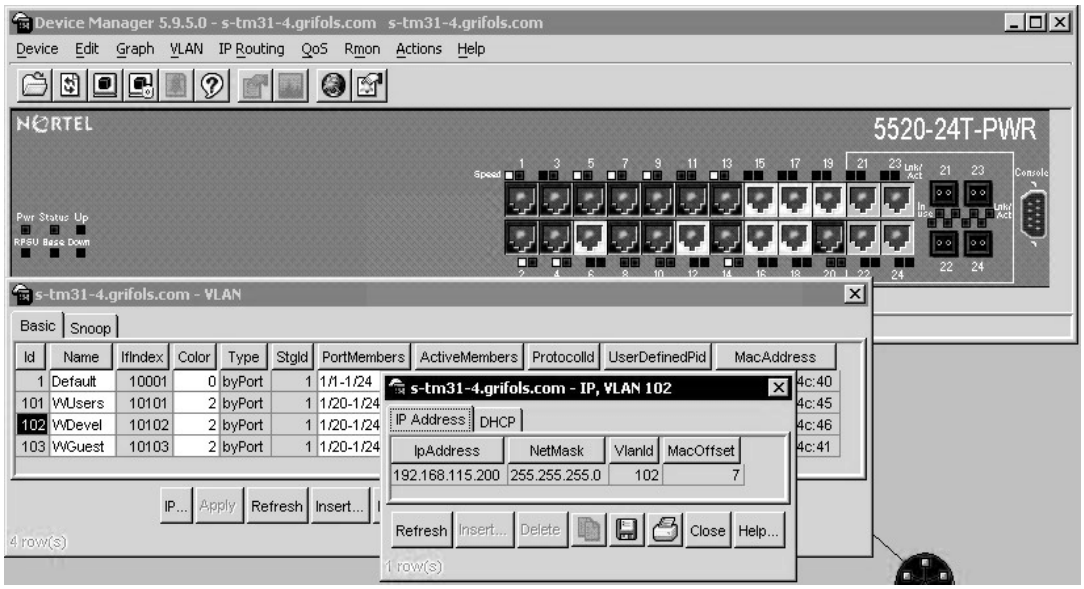
Definir aquestes VLAN a la taula d'encaminament per que es propaguin amb el protocol d' encaminament configurat (OSPF)

Per últim, cal definir un servei proxyDHCP que permeti rebre les peticions de IP generats per els clients de les VLAN's i transmeti aquestes peticions al servidor DHCP on s' han creat els rangs de IP's i atributs a servir.

6.1.6 Assignació d' adreces IP

Es defineixen les xarxes virtuals indicant el identificador que utilitzaran, el adreçament assignat la modalitat de transmissió que es per port i els ports on es propaguen les etiquetes de les VLAN's

Degut a que els commutadors son Nortel, utilitzem una eina gràfica de Nortel :



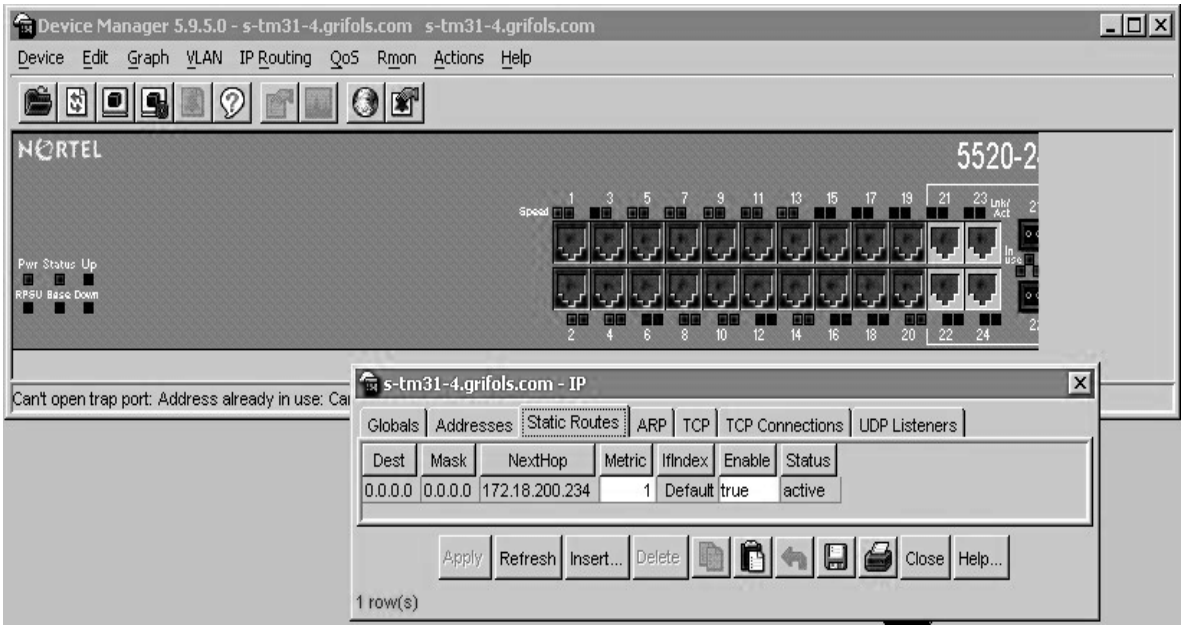
6.1.7 Encaminament

Cal activar el protocol d' encaminament desitjat o escriure les rutes manualment per a les noves xarxes creades.

Aquí fem servir un protocol d' encaminament nomenat OSPF i el que fem es activar aquest protocol per cadascuna de les xarxes creades per que aquestes siguin anunciades a tota la xarxa.

Aquest punt es particularment important per que cal que els encaminadors coneguin com enviar els paquets que pertanyen a aquestes xarxes per arribar als servidors centrals i tornar.

El commutador de la oficina de direcció general no utilitza protocol OSPF i s' ha definit una ruta estàtica cal al encaminador principal que després s' encarrega de informar a la resta de nodes de la xarxa de l' existència de les xarxes sense fils creades utilitzant el protocol OSPF.



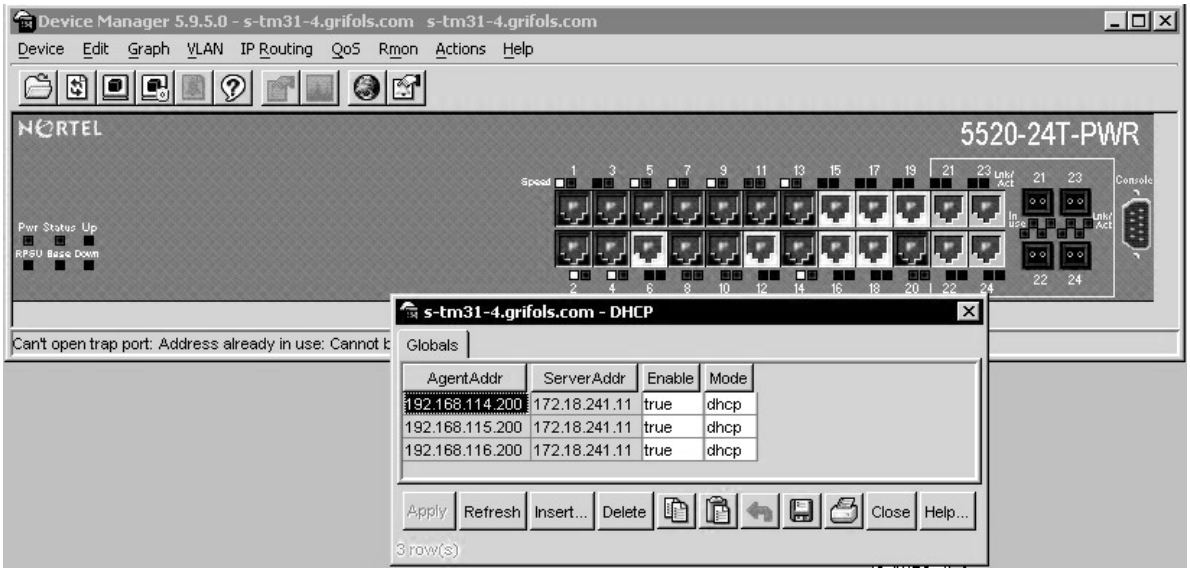
6.1.8 Proxy DHCP

Els clients sense fils demanen la informació de adreçament de xarxa utilitzant protocol DHCP.

Com que aquests equips sense fils, al connectar se a la xarxa s' els assigna una xarxa virtual diferent de la xarxa de defecte, es necessari que el servidor de DHCP, que esta a la xarxa de defecte rebi les peticions de DHCP enviades per aquests equips.

Per això fem servir una característica dels equips de encaminament que es diu proxyDHCP i que consisteix en que el equip encaminador rep la petició DHCP i l' envia al servidor DHCP fent d' intermitjari.

Cal configurar el equip per que sàpiga que per cada adreçament o xarxa de la qual pot rebre una petició DHCP, ha de passar aquesta petició a un servidor de DHCP.



CONFIGURACIÓ DEL SISTEMA D' ACCÉS INALÁMBRIC

6.1.9 Configuració de autenticació amb el servidor

El sistema de control d' accés inalàmbric permet la configuració de un grup de servidors d' autenticació RADIUS per implementar balanceig de carrega en les peticions d' autenticació o per tenir alta disponibilitat en cas de fallada de algun dels servidors d' autenticació RADIUS

Així es configura un grup de servidors d' autenticació i un protocol d' intercanvi de credencials amb els servidors d' autenticació.

El sistema de control també ha de presentar una clau (passphrase) per que el servidor d' autenticació RADIUS el reconegui.

La configuració te els següents passos :

- Creació dels servidors d' autenticació disponibles i la passphrase corresponent per a cadascun d' ells

- Creació del grup de autenticació i assignació dels servidors
- Assignació al perfil de radio del sistema de intercanvi de credencials per al grup d' autenticació :

set radius server ulises address 192.168.241.196 timeout 5 retransmit 3 deadtime 0 key ***************

set radius server w3-tm address 172.18.241.5 timeout 5 retransmit 3 deadtime 0 key ***************

set server group GRUP_SRVRS members ulises w3-tm

set authentication dot1x ssid grifols ** peap-mschapv2 GRUP_SRVRS

6.1.10 Configuració de la senyalització de radio

La configuració del identificador de radio, el sistema d' encriptació i la senyalització de radio es fa utilitzant perfils.

Primerament cal definir un perfil de servei on es defineixen les característiques del accés que es vol posar en marxa.

Nosaltres definim un perfil de servei que inclou l'identificador de xarxa i el sistema d' encriptació a utilitzar

set service-profile crypto-sp ssid-name SSID

set service-profile crypto-sp wpa-ie enable

Un cop definides les característiques del servei utilitzant un perfil, també caldrà crear un perfil de radio amb el sistema de radio freqüència definit i relacionar los.

El sistemes de control inalàmbric tenen un perfil de radio creat per defecte que es el que utilitzem. Aquest perfil inclou la emissió en les tres bandes 802.11 a b g i els paràmetres bàsics de transmissió

```
23x0# show radio-profile default
Beacon Interval: 100 DTIM Interval: 1
Max Tx Lifetime: 2000 Max Rx Lifetime: 2000
RTS Threshold: 2346 Frag Threshold: 2346
Short Retry Limit: 5 Long Retry Limit: 5
Long Preamble: NO Allow 802.11g clients only: NO
Tune Channel: yes Tune Power: no
Tune Channel Interval: 3600 Tune Power Interval: 600
Power Backoff Timer: 10 Channel Holddown: 300
Countermeasures: none Active-Scan: yes
WMM enabled: yes
Service profiles: default-dot1x, default-clear
```

Els equips utilitzats permeten la configuració de un sistema de "auto-tunning" per que el propi punt d' accés decideixi el canal d' emissió i la potencia d' emissió per ajustar se a les necessitats del entorn.

Cada cert temps (3600 seg) el punt d' accés comprova les interferències en els canals disponibles i selecciona el òptim per utilitzar.

set radio-profile webqs-rp enable

Un cop creat el perfil de radio, s' ha d' associar amb un perfil de servei

set radio-profile webqs-rp service-profile crypto-sp

I per últim, aquest perfil de radio s' assigna a tots els punts d' accés que interessi. En aquest cas tots els punts d' accés treballen amb el mateix perfil.

set dap 2 radio 1 radio-profile webqs-rp mode enable

set dap 2 radio 2 radio-profile webqs-rp mode enable

Els dos diferents tipus de radio son les emissions a 2,4 Ghz per els protocols **b,g** i les emissions a 5 Ghz per el protocol **a**

6.1.11 Configuració de VLAN's

Com els punts d' accés treballen a nivell 2, son els encarregats de marcar les trames amb els identificadors de les xarxes virtuals seguint el protocol 802.1q

Es necessari doncs crear els identificadors de les xarxes virtuals i associar los als atributs definits al servidor RADIUS que ens envia per cada nova autenticació de un client a la xarxa.

set vlan 1 port 1 tag 1
set vlan 100 name users
set vlan 100 port 1 tag 100
set vlan 101 name devel
set vlan 101 port 1 tag 101
set vlan 102 name guest
set vlan 102 port 1 tag 102

També cal indicar al commutador de control quins identificadors ha de utilitzar en els ports en els que esta connectat a la xarxa de cable.

En el cas de la configuració mostrada, al port 1 s' assignen les tres xarxes virtuals definides per els clients sense fils (100,101,102) i també s' assigna la xarxa virtual per defecte (1)

6.1.12 Llistes de control d' accés

Per restringir el accés dels usuaris als serveis en funció del grup al que pertanyen, s' utilitzen les llistes de control d' accés de que disposen els equips de control inalàmbric.

La definició de les llistes de control d' accés es fa a partir de les xarxes definides.

Es necessari tenir en compte que hi ha uns serveis mínims als que s' ha de tenir accés per poder treballar i aquests son els serveis de noms (DNS).

Per al cas de la xarxa de convidats, les restriccions definides son les de accés exclusiu a Internet a través del servidor proxy de la empresa.

La configuració de les llistes de control d' accés es fa per tipus de tràfic i per destí / origen

Llavors per restringir el tràfic IP de la xarxa de convidats al servidor de proxy, tant en el tràfic d' anada com en el de tornada caldrà :

set security acl ip internet permit ip 192.168.113.0 0.0.0.255 172.16.254.27 0.0.0.0

set security acl ip internet permit ip 172.16.254.27 0.0.0.0 192.168.113.0 0.0.0.255

CONFIGURACIÓ DELS CLIENTS

Els equips client s' han de configurar per fer servir els mateixos sistemes d' autenticació i encriptació definits als punts d' accés per l' identificació.

Degut a que la major part dels equips clients formen part de l' empresa i estan inclosos al sistema Active Directory de la companyia, s' ha desenvolupat un mètode d' assignació automàtica basant se en l' homogeneïtat de sistemes (Windows).

Hi ha unes especificacions mes generals que permeten l' assignació de les configuracions sense fils als clients a partir de una descarrega de fitxers XML des d'un servidor WEB, però en un cas com aquest de desplegament de un sistema inalàmbric dins d' una empresa es mes pràctic fer les configuracions de clients el mes automàtiques possibles.

6.1.13 Configuració manual dels clients

Els requeriments bàsics per a la configuració sense fils en el cas de sistemes operatius Windows XP es que tinguin instal·lat el service pack 2 per que inclou les funcions necessàries per l' autenticació utilitzant 802.1x i PEAP (Protected Extensible Password) i per l' encriptació amb WPA.

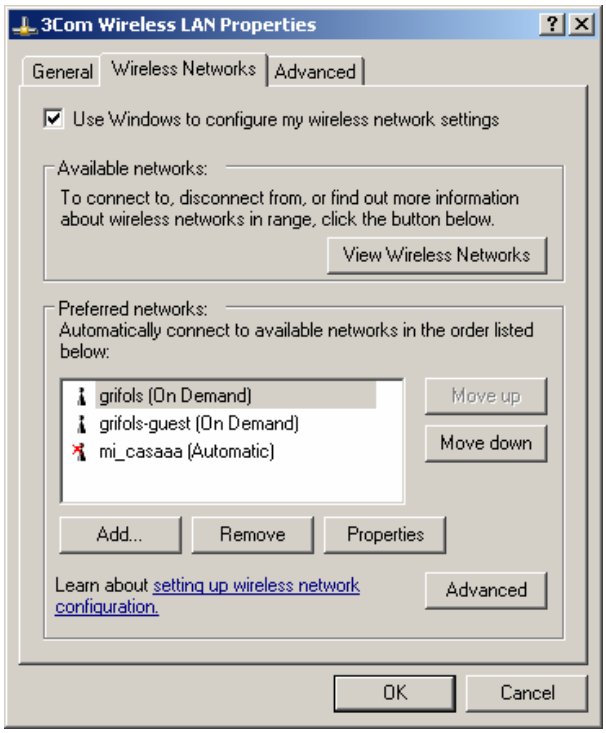
També es necessari que el equip disposi de un dispositiu de radio freqüència que compleixi algun dels estàndards 802.11 a b g

La configuració bàsica es :

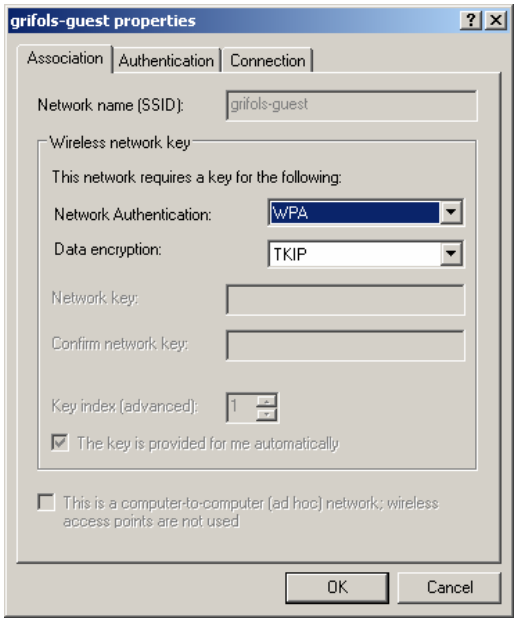
Atributs	**Configuració Local**	**Configuració Visitant**
SSID	**Grifols**	**Grifols-Guest**
Network Authentication :	WPA	WPA
Data Encription :	TKIP	TKIP
Authentication :	Protected EAP	Protected EAP
EAP Properties :		
Validate Server Certificate :	No	No
Authentication Method :	EAP-MSCHAP v2	EAP-MSCHAP v2
Enable Fast Reconnect :	Yes	Yes
Use Windons Logon Name :	Yes	No

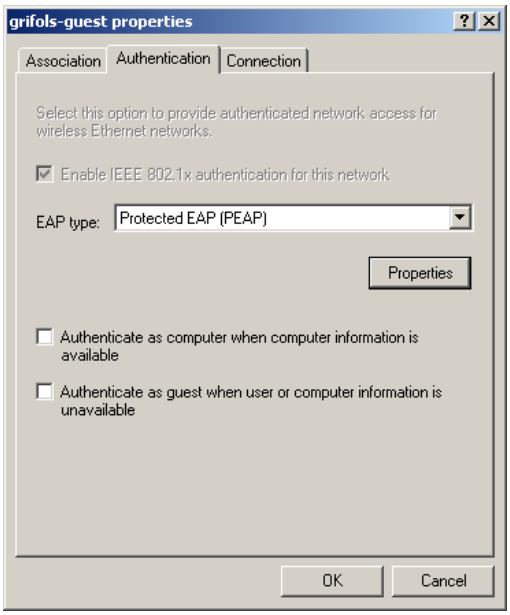
Els passos a seguir al PC son :

Configuració del identificador de xarxa SSID :



Configuració del sistema d' encriptació i d' autenticació

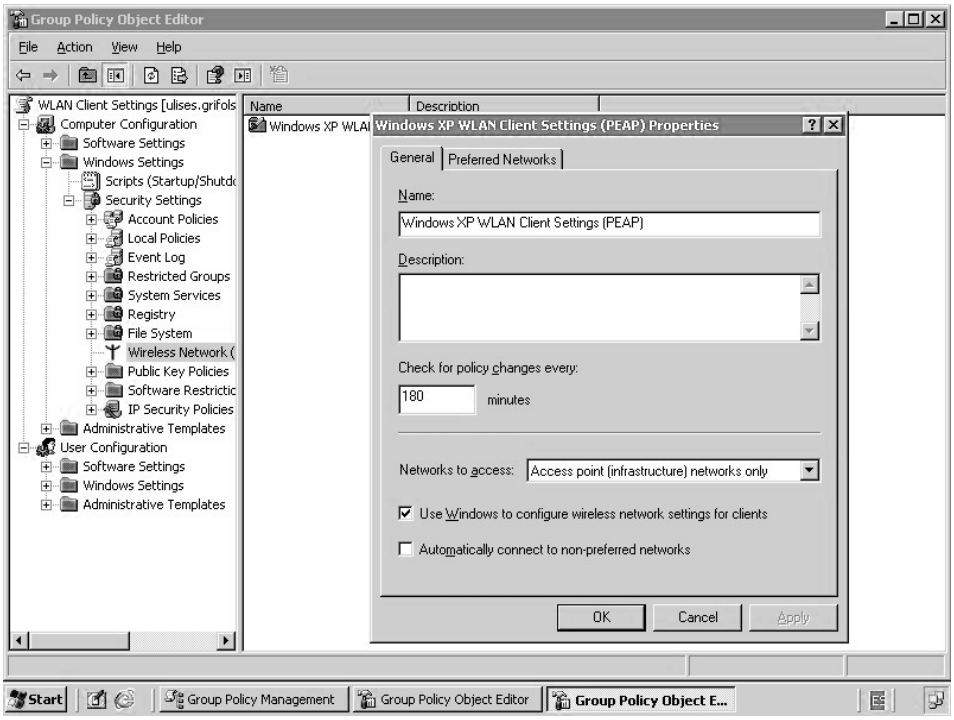


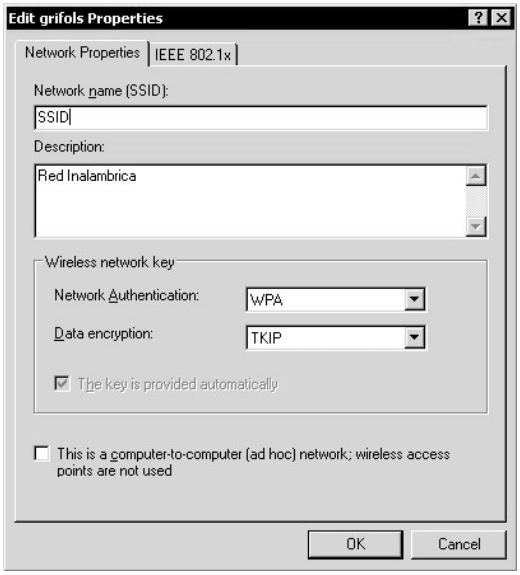


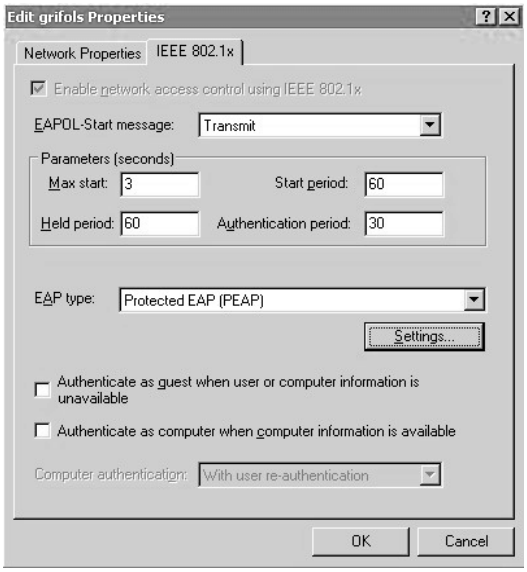
6.1.14 Sistema de configuració automàtica

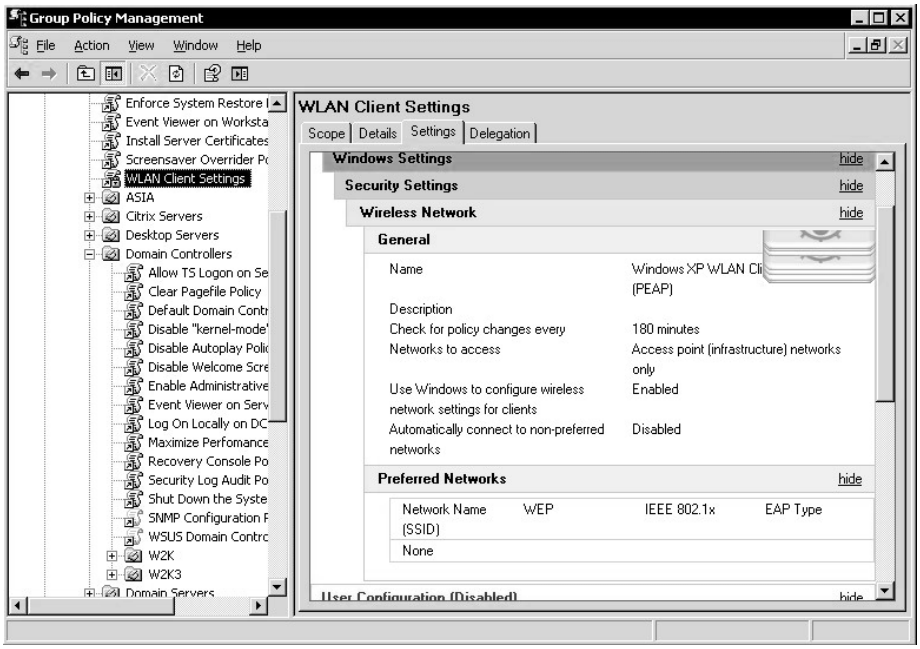
Per evitar que els usuaris hagin de configurar el seus propis portàtils s' ha desenvolupat una política de grup que s' aplica quan el portàtil es connecta a la xarxa de cable un cop (GPO).

Aquesta política es la següent :









7 DISSENY D' IDENTIFICACIÓ D' USUARIS

7.1.1 Sistema de gestió d' usuaris autoritzats

Donat que el servidor d' autenticació RADIUS utilitza la base de dades d' usuaris del Directori Actiu i els grups configurats per autoritzar el accés de les peticions rebudes, el sistema de gestió d' usuaris es basa en el sistema de gestió d' usuaris del Directori Actiu.
Al donar d' alta un usuari de xarxa sense fils al Directori Actiu, caldrà incloure'l al grup d'usuaris adient en funció de les autoritzacions que li corresponguin.

Wifi_Auth : Grup d' usuaris autoritzats de la empresa
Wifi_Devel: Grup d' usuaris externs autoritzat
Wifi_Guest: Grup d' usuaris convidats temporalment.

7.1.2 Gestió automàtica de baixes

Els dos grups de usuaris primers (Auth i Devel) esta format per usuaris de la empresa o que hi col·laboren amb l' empresa de forma habitual.
Per aquests usuaris ja hi ha un protocol establert de altes i baixes que gestiona el propi departament d' informàtica i, per tant, en cas de baixa de la empresa el identificador d' usuari es bloqueja.

En el cas dels usuaris convidats temporalment, s' ha pensat en un sistema de gestió d' usuaris descentralitzat i s' ha cedit autorització d' alta d' usuaris de WiFi a les recepcionistes dels edificis on hi ha xarxa sense fils.
En aquest cas, es necessari desactivar aquest tipus d' usuaris el mes aviat possible un cop han marxat per evitar que poguessin connectar se des de fora de la empresa o cedir les credencials a altres usuaris no autoritzats directament.

Per això s' ha desenvolupat un procés que s' executa diàriament a partir de les 22:00 y que borra els usuaris del servei de connexió sense fils convidats que han estat donat d' alta per les recepcionistes.

8 DISSENY DELS CASOS DE TEST

8.1.1 Introducció

El disseny dels casos de test consisteix en el desenvolupament de un protocol de verificació del correcte funcionament del sistema de connexió sense fils i de que les configuracions realitzades es compleixen tal i com s' ha previst.

Per això desenvolupem un sistema de verificació de dades que indiquin la correcta acció realitzada.

8.1.2 Test del correcte funcionament del sistema

Primer cal garantir el correcte funcionament del sistema de forma que tots els processos implicats en l' accés a la xarxa del equip inalàmbric es comportin segons la forma dissenyada e implementada.

Es per això que el primer cas de test ha de ser la verificació del correcte funcionament de una connexió.

Procés d' autenticació

Verificació de la correcta validació del usuari en el sistema RADIUS.

Per realitzar aquesta tasca es necessari fer una connexió i comprovar al fitxer de missatges del servidor RADIUS que el codi de resposta del procés de validació d' usuari es 0 que significa correcte.

Procés d' assignació de xarxa

Comprovació de la correcta assignació de l' adreça IP en funció del grup d' usuaris al que pertany el usuari.

La comprovació es realitza en el equip client, utilitzant l' ordre de verificació de les dades de xarxa assignades per DHCP (ipconfig /all)

Aquest procés ha de mostrar una IP del rang definit en funció del grup, la porta d' enllaç definida per defecte i els servidors de noms adequats.

Procés de control de accés i encaminament

Verificació de l' accessibilitat de la xarxa

En aquest punt es necessari realitzar una connexió als serveis disponibles dins de la xarxa segons el grup assignat.

El pas mes bàsic serà l' us de l' ordre "traceroute" per comprovar que les trames enviades al servidor a accedir arriben correctament al seu destí.

8.1.3 Test del sistema d' autenticació d' usuari

Per verificar el funcionament correcte realitzem unes proves de autenticació no correctes per veure que el sistema rebutja correctament els processos no vàlids.

El procés d' autenticació d' usuari te dos aspectes a verificar :

1. Que la validació del usuari es realitzi correctament
    a. Utilitzar un usuari no autoritzat
    b. Canvi de paraula clau per que no sigui la correcta
2. Que la assignació de atributs es realitzi correctament
    a. Assignar l' usuari a un grup diferent dins del Active Directory i comprovant que se l' assigna una adreça IP del altre grup
    b. Canviant al servidor RADIUS el valor del atribut que indica la VLAN a assignar per veure que no assigna correctament IP.

Per realitzar les comprovacions sobre la veracitat dels test proposats utilitzem dues eines :

El sistema RADIUS disposa de un fitxer de missatges que es pot activar on queden reflectits els intents erronis de autenticació d' usuaris i el codi d' error retornat per el servidor.

En el equip portàtil client es verifica el procés d' assignació IP i s' observa l' IP assignada (o cap) en funció dels atributs que se l' hi assignen

8.1.4 Test del sistema d' encriptació

El procés de verificació del sistema d' encriptació es complicat per que cal utilitzar un "sniffer" de xarxa sense fils i veure les trames encriptades.

Com a prova aproximada utilitzem dos programaris clients sense fils que donen informació de les xarxes detectades al voltant.

Un client serà el propi programari que ofereix **Windows**. Aquest client mostra, en les finestres de disponibilitat de xarxes el tipus de xarxa que hi ha i el tipus d' encriptació que utilitza.

Un altre client que utilitzem per comprovar que realment s' esta treballant en una xarxa que utilitza el protocol d' encritpació definit (TKIP) es el programa **stumbler.** Aquest programa, de lliure distribució, també mostra les xarxes sense fils disponibles al entorn i les seves característiques d' emissió (Canal, identificador de xarxa, encriptació ...)

8.1.5 Test del sistema d' autenticació dels equips sense fils

Per verificar que la validació del client d' autenticació es realitzi correctament es realitzen dos tests :

a. Canvi de la phassprasse al equip client i comprovació que no es realitza la validació.
b. Canvi de l' adreça IP en el servidor RADIUS i comprovació que no es realitza la validació

La verificació dels missatges de error es pot realitzar en el fitxer de missatges de que disposa el sistema RADIUS que s' ha comentat anteriorment.

8.1.6 Verificació dels sistemes de control d' accés

La verificació del funcionament dissenyat dels sistemes de control d' accés es realitza a partir del sistema de monitorització. D' aquesta forma es realitza una doble vessant en els casos de test ja que es comprova el correcte funcionament del sistema de monitorització i es verifiquen els sistemes de control d' accés definits.

Per comprovar-ho realitzem :

a. Comprovació de la disponibilitat dels serveis d' accés : Amb l' ordre **nmap** podem realitzar un scan dels ports disponibles de un sistema connectat a la xarxa.

   Utilitzant aquest scanner de xarxa veiem que els sistemes de control d' accés només tenen disponibles els ports previstos (SSH, SNMP i SYSLOG)

b. Comprovació de validació errònia en l' identificació del accés al sistema utilitzant SSH.

   A partir del fitxer de log que envia el sistema de control d' accés al servidor de monitorització dels logs centralitzats podem comprovar el missatge de intent s' accés incorrecte.

9 GESTIÓ DE LA DISPONIBILITAT

DISSENY DEL SISTEMA DE MONITORITZACIÓ

L' Empresa utilitza un sistema de monitorització amb una consola centralitzada on es reben els missatges SNMP enviats per els equips de xarxa amb aquests tipus de capacitats.

Per altra banda també es disposa de un sistema de recepció de logs Standard centralitzats (syslog) basat en un servidor Kiwi

El sistema de monitorització centralitzat permet desenvolupar scripts de cerca de mostres en fitxers i en aquesta característica es basa per verificar els missatges que els sistemes envien al servidor syslog centralitzat i decidir, si apareix algun missatge tipificat com advertència, de enviar lo a la consola de monitorització

CONFIGURACIÓ DEL SISTEMA DE ALERTAS

9.1.1 Enviament d' alertes SNMP

El sistema de alertes SNMP o traps es el sistema de monitorització mes estes dins del entorn de sistemes de xarxa.

Aquest sistema es basa en un protocol d' enviament de missatges per part dels equips de la xarxa i una consola receptora dels missatges.

Cada fabricant desenvolupa una definició de les característiques de els seus equips en un fitxer que es nomena MIB (Management Information Database)

La MIB es una base de dades de característiques dels objectes que es poden supervisar per un sistema de monitorització de xarxa. L' us dels SNMP va fer formats Standard de les MIB que permet que qualsevol eina de monitoritzat de SNMP supervisi qualsevol dispositiu definit per una MIB.

Per utilitzar les característiques especifiques dels equips, cal carregar les seves MIB al sistema de monitorització.

Per configurar l' enviament d' alertes SNMP al sistema receptor es defineixen els següents paràmetres :

Cal indicar la versió d' SNMP a utilitzar. En el cas que ens ocupa, s' utilitza la versió 2 de SNMP

set snmp protocol v2c enable

Després es necessari indicar la comunitat a utilitzar :

Set snmp community name dawn read-only

Set snmp community name dusk read-write

Per últim, cal indicar el sistema receptor dels missatges

Set snmp notify target 192.168.241.230 v2c trap

9.1.2 Sistema de log centralitzat (Syslog)

Hi ha definit un protocol de missatges de sistema que es nomena syslog. Aquest protocol defineix un format específic per als missatges generats i un protocol d' enviament d' aquests missatges a un sistema receptor i centralitzador dels missatges (syslog centralitzat).

Els missatges tenen un format específic que indica el moment de la generació i el originador, així com el nivell de gravetat, el component generador del missatge i el text explicatiu del missatge.

Per enviar els missatges al sistema de recepció de missatges d' alerta centralitzat cal definir el nivell de missatges que es volen enviar i si es vol enviar alguna tipificació.

Els nivells de missatges disponibles son :

Debug.	Missatges informatius sobre les operacions del mòdul.
Notice	Missatges informatius de una acció no habitual però no necessàriament alarmant
Warning	Missatge d' advertència de un succés no esperat i potencialment perillós
Error	Missatge de avis de mal funcionament del component indicat
Critical.	Missatge de error greu del component

En el cas que es defineix, el nivell de missatges que s' enviarà es "warning" o un nivell superior.

Set log server 192.168.241.130 severity warning local-facility local enable

CONFIGURACIÓ DELS SERVEIS D' ACCES ALS SISTEMES DE CONTROL

9.1.3 Restricció del accés als equips de control

Els equips d' accés a la xarxa sense fils han de ser segurs per evitar manipulacions no autoritzades.

Els punts bàsics a tenir en compte son :

Mantenir seguretat física en l' accés als equips.

Cal no permetre el accés físic als equips sense fils a personal no autoritzat. Els punts d' accés que s' instal·len a les àrees de treball son la part mes accessible i vulnerable.

Degut a la arquitectura seleccionada, aquests punts d'accés només es poden desconnectar, per tant, en el pitjor dels casos, un atac sobre els punts d' accés deixarà sense cobertura l' àrea però no comprometre la seguretat de la xarxa.

Els equips de control si son vulnerables físicament i per tant han d' estar aïllats del accés físic en armaris de servei o en el centre de comunicacions si escau.

Utilitzar sistemes d' encriptació i paraules clau segurs.

El accés lògic als equips de control ha d' estar restringit per evitar accés no autoritzat i per evitar interceptació de les comunicacions.

El protocol mes recomanat per el accés al sistema de control es ssh. Aquest protocol treballa amb certificats i encripta les comunicacions entre el client que es connecta i el equip de control, fent impossible interceptar les comunicacions.

En el accés, cal utilitzar usuaris personalitzats i paraules clau segures, seguint una bona política de garantització de paraules clau (caducitat, tipus, longitud ..)

Desactivar protocols i serveis no utilitzats

Es important desactivar els protocols no utilitzats o que pugin ser menys segurs.

Cal desactivar doncs, tots els protocols no utilitzats com DNS, DHCP, NTP TFTP etc. També es necessari desactivar els protocols d' accés als equips de control com el TELNET o HTTP ja que les tasques de manteniment i administració dels equips es farà amb SSH i per tant ja no son imprescindibles.

En el nostre cas, que utilitzem el protocol SNMP per supervisar el estat dels equips, es important modificar les paraules d' accés SNMP (community) i utilitzar paraules robustes, ja que aquest protocol no es excessivament segur

Limitar els accessos lògics amb filtres.

Com a darrera mesura de restricció de accés, es recomanable la configuració de filtres de control (ACL) per restringir l' accés als equips de control de forma que només des d' uns equips específics i només amb uns serveis específics es pugui accedir als equips de control.

Els ACL permeten indicar des de quina IP o rang d' IP es pot accedir al equip i quins serveis es poden accedir.

AVALUACIÓ DE MESURES EN FRONT POSSIBLES ATACS

9.1.4 Detecció d' atacs de pillatge

Els equips WSS incorporen un sistema de detecció de altres fons de connexió sense fils per avaluar el seu potencial de risc en quant a la possibilitat de atacs de pillatge (rogue atacs).

Els sistemes treballen en dues formes : passiva i activa.

El sistema de detecció passiu consisteix en que el sistema escolta la xarxa per emissions de oferiment de altres dispositius (beacons) o per enviaments de prova de detecció de xarxa.

En el format actiu, els sistemes envien paquets de prova sense identificador de xarxa (SSID) esperant les respostes de possibles i recollint les.

Si el sistema detecta intents d' atac amb paquets mal formats intencionadament o intents de interrompre el servei (atacs de denegació de servei), pot enviar alertes de intents d' atac utilitzant el sistema de SNMP y el syslog

Un cop recol·lectada l' informació sobre possibles fonts sospitoses de entorpir les comunicacions, el sistema inclou els identificadors (MAC addresses) de les fonts emissores en una llista de equips no grats.

Els sistemes WSS suporten diferents tipus de llistes.

Llista de equips no permesos (per MAC address).

Llista de identificadors no permesos (SSID's)

Llista de equips coneguts i permesos

També es pot implementar una llista de clients no acceptats (client black list) per evitat el accés de clients malintencionats a la xarxa sense fils

9.1.5 Mesures de prevenció

Bàsicament les mesures de prevenció consisteixen generar emissió de paquets a la xarxa per entorpir als dispositius que interfereixen a la xarxa sense fils

Quan es detecta algun dispositiu que genera paquets de forma sospitosa, es pot incorporar aquest equip (la seva "MAC address") a una llista d' atac i activar les mesures de prevenció que generaran tràfic cap aquell dispositiu per evitar o entorpir el enviament de paquets de verificació.

Un altre mesura de prevenció consisteix en enviar avisos SNMP o missatges al syslog quan es detecten intents d' atac o sospites d' intents d' atac.

Alguns exemples poden ser aquests :

Interferències forçades :Quan els equips detecten excessives interferències al canal de transmissió, automàticament son capaços de canviar de canal de transmissió

Spoofing : Enviament de trames sense autenticar als clients substituint la "MAC address" de origen per la del AP. Els equips WSS detecten aquest tipus de

trames amb seva “MAC address” com a adreça de origen, coneixen el intent d’ atac.

SSID Masquerade : El atacant envia presentacions (beacons) amb el identificador de xarxa per tractar de que els clients connectin amb ell. Els equips WSS detecten aquests tipus de trames basant se en una signatura que tenen tots els punts d’ accés i envien alertes

10 EXTENSIBILITAT

L’ implementació d’ aquesta xarxa sense fils s’ ha basat en els requeriments definits de cobertura, seguretat i disponibilitat procurant seleccionar la tecnologia mes madura per a les necessitats descrites i amb mes projecció per tal de migrar a noves versions amb el menor impacte possible.

Però aquesta tecnologia deixa altres àmbits per explorar que poden ser interessants i rics.

El primer i mes immediat es el “roaming” o trasllat dels equips sense fils sense perdre la connexió sense fils. Aquesta opció pot ser interessant en cas de incorporar altres equips portàtils de poc pes i facilitat de transport com poden ser las PDA o els portàtils lleugers.

Es necessari configurar els equips de forma que els punts d’ accés formen un domini de mobilitat

Sembla una aplicació molt interessant per un altre àmbit mes ambiciós e interessant que es la telefonia sense fils IP. A partir d’ alguns equips portàtils amb capacitats de transmissió de veu IP pot ser interessant explorar les possibilitats de definir un sistema de cobertura de telefonia IP sense fils per a les oficines.

Els equips amb els que estem treballant (WSS Nortel) disposen de capacitat de priorització de tràfic i gestió de cues per nivells seguint el estàndard 802.1p. Aquest protocol es basa en el marcatge de paquets en funció del tipus de tràfic i del seu destí per prioritzar lo.

Els punts d’ accés gestionen els paquets a enviar als clients a traves de cues de prioritat i els equips clients que envien tràfic prioritari (veu IP o vídeo) marquen els paquets seguint el protocols 802.1p per que pugui ser prioritzat.

11 BIBLIOGRAFIA

Cisco Structured Wireless-Aware Network (SWAN) Implementation Guide - Cisco Structured Wireless-Aware Network (SWAN) Implementation Guide [Cisco Aironet 1200 Series] - Cisco Systems

Computer Network Design Wireless VPN Local Area Wide Area Basic Network Design UK

Wireless Policy Development (Part One)

VPN - virtual private network resources - vpn solutions clients servers

Michigan Engineering :: Overview of CAEN Wireless

Navini Networks

Wi-Fi Alliance - Knowledge Center - White Papers - www.wi-fi.org

WLANA Learning Center

The Cable Guy

Wi-Fi Planet - The Source for Wi-Fi Business and Technology

Wireless - Products & Services - Cisco Systems

WLANA Wireless LAN Association

Wireless Networking MS

Wi-Fi Protected Access 2 (WPA2) Overview: The Cable Guy - May 2005

Wireless LAN 802.11b Security FAQ

Examining 802.1x and EAP

802.1X Port-Based Authentication HOWTO

802.16e vs. 802.20

IEEE 802.11, The Working Group Setting the Standards for Wireless LANs

Unified 802.11n Wi-Fi Standard to Emerge in Mid-2006

CiudadWireless

Fundamentals of Wireless LAN's (Cisco Networking Academy Program)

Nortel WLAN Security Switch guide (Nortel Networks)

Securing Wireless LAN with PEAP and Passwords (Microsoft)

12 ANNEXOS

ANNEX 1. Configuració equip seu central

```
WS-P3R2-1# show config
# Configuration nvgen'd at 2006-6-15 14:20:10
# Image 4.0.20.0
# Model 2350
# Last change occurred at 2006-6-15 06:07:09
set ip dns domain grifols.com
set ip dns server 192.168.241.52 PRIMARY
set ip dns server 192.168.241.196 SECONDARY
set ip route default 172.16.200.199 1
set ip route default 172.16.200.198 1
set log session enable severity info
set log server 192.168.31.230 severity debug local-facility 7
set timezone Eur 1 0
set summertime Eur-S start first sun apr 2 0 end last sun oct 2 0
set system name WS-P3R2-1
set system ip-address 172.16.19.35
set system countrycode ES
set system location P2-inf
set service-profile crypto-sp ssid-name grifols
set service-profile crypto-sp wpa-ie enable
set service-profile guest-sp ssid-name grifols-guest
set service-profile guest-sp wpa-ie enable
set radius server ulises address 192.168.241.196 timeout 5 retransmit 3 deadtime 0
key ****************
set server group GRIFOLS members ulises
set enablepass password 5223a53dc3a4decdb9b01c59c2e28f0cb15f
set authentication admin rwa local
set authentication console rwa local
set authentication console ** local
set authentication dot1x ssid grifols ** peap-mschapv2 GRIFOLS
set authentication dot1x ssid grifols-guest ** peap-mschapv2 local
set user rwa password encrypted 0214135a
set user rwa attr vlan-name default
set user rwa attr service-type 6
set user user password encrypted 14131d06050a2d24
set user user group GUEST
set user user attr end-date 06/02/24-16:17
```

```
set usergroup GUEST attr vlan-name guest
set radio-profile webqs-rp service-profile crypto-sp
set radio-profile webqs-rp service-profile guest-sp
set dap auto mode disable
set dap auto radiotype 11g
set dap auto radio 1 radio-profile webqs-rp
set dap auto radio 2 radio-profile webqs-rp
set dap 2 serial-id stp1w20b01 model 2330
set dap 2 name AP02-PARETS
set dap 2 fingerprint 5f:34:b6:66:7f:ed:f6:89:ab:29:c6:fc:82:57:89:9a
set dap 2 radio 1 radio-profile webqs-rp mode enable
set dap 2 radio 2 radio-profile webqs-rp mode enable
set dap 3 serial-id stp1w20azn model 2330
set dap 3 name AP03-PARETS
set dap 3 fingerprint 5a:02:f3:36:c2:26:33:db:f0:9a:0f:77:c5:8a:74:15
set dap 3 radio 1 radio-profile webqs-rp mode enable
set dap 3 radio 2 radio-profile webqs-rp mode enable
set port type ap 2 model 2330 poe enable
set ap 2 name AP01-PARETS
set ap 2 radio 1 radio-profile webqs-rp mode enable
set ap 2 radio 2 radio-profile webqs-rp mode enable
set ip https server enable
set ip snmp server enable
set ip telnet server enable
set port poe 2 enable
set snmp notify profile ovo_prf send LinkDownTraps
set snmp notify profile ovo_prf send DeviceFailTraps
set snmp notify profile ovo_prf send PoEFailTraps
set snmp notify profile ovo_prf send APTimeoutTraps
set snmp notify profile ovo_prf send APBootTraps
set snmp protocol v2c enable
set snmp community name public access read-only
set snmp community name private access read-write
set snmp notify target 1 192.168.31.206:162 v2c public trap
set vlan 1 port 1 tag 1
set vlan 100 name users
set vlan 100 port 1 tag 100
```

set vlan 101 name devel

set vlan 101 port 1 tag 101

set vlan 102 name guest

set vlan 102 port 1 tag 102

set spantree enable vlan 1

set spantree enable vlan 100

set spantree enable vlan 101

set spantree enable vlan 102

set interface 1 ip 172.16.19.35 255.255.0.0

set security acl ip portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0 255.255.255.255 eq 67

set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture

commit security acl portalacl

set security acl ip internet permit icmp 192.168.113.0 0.0.0.255 172.16.254.27 0.0.0.0

set security acl ip internet permit icmp 172.16.254.27 0.0.0.0 192.168.113.0 0.0.0.255

set security acl ip internet permit ip 192.168.113.0 0.0.0.255 172.16.254.27 0.0.0.0

set security acl ip internet permit ip 172.16.254.27 0.0.0.0 192.168.113.0 0.0.0.255

set security acl ip internet permit ip 192.168.113.0 0.0.0.255 192.168.241.196 0.0.0.0

set security acl ip internet permit ip 192.168.241.196 0.0.0.0 192.168.113.0 0.0.0.255

commit security acl internet

set security acl map internet vlan 102 out

set ntp enable

set ntp server 192.168.241.2

ANNEX 2. Configuració equip direcció general

WS-MAPFRE-1# show config

Configuration nvgen'd at 2006-6-15 14:21:56

Image 4.0.20.0

Model 2380

Last change occurred at 2006-5-23 08:36:11

set trace aaamsg level 10

set ip dns domain grifols.com

set ip dns enable

set ip dns server 192.168.241.52 SECONDARY

set ip dns server 172.18.241.1 PRIMARY

set ip route default 172.18.200.234 1

set log server 192.168.31.230 severity notice local-facility 7

set timezone Eur 1 0

set summertime Eur-S start first sun apr 2 0 end last sun oct 2 0

set system name WS-MAPFRE-1

set system ip-address 172.18.199.101

set system countrycode ES

set service-profile crypto-sp ssid-name grifols

set service-profile crypto-sp wpa-ie enable

set service-profile guest-sp ssid-name grifols-guest

set service-profile guest-sp wpa-ie enable

set radius server w3-tm address 172.18.241.1 timeout 5 retransmit 3 deadtime 0 key **********

set server group GRIFOLS members w3-tm

set enablepass password 5223a53dc3a4decdb9b01c59c2e28f0cb15f

set authentication admin rwa local

set authentication console rwa local

set authentication console ** local

set authentication dot1x ssid grifols ** peap-mschapv2 GRIFOLS

set authentication dot1x ssid grifols-guest test peap-mschapv2 local

set user rwa password encrypted 0214135a

set user rwa attr vlan-name default

set user rwa attr service-type 6

set user test password encrypted 105a0c0a11

set user test group GUEST

set usergroup GUEST attr vlan-name guest

set radio-profile webqs-rp service-profile crypto-sp

set radio-profile webqs-rp service-profile guest-sp

set dap 2 serial-id stp1w20axm model 2330

set dap 2 name AP01-MAPFRE

set dap 2 fingerprint 89:bb:ca:3f:8b:ed:35:e2:ac:c4:89:07:44:ac:11:35

set dap 2 radio 1 radio-profile webqs-rp mode enable

set dap 2 radio 2 radio-profile webqs-rp mode enable

set dap 3 serial-id stp1w20az6 model 2330

set dap 3 name AP02-MAPFRE

set dap 3 radio 1 radio-profile webqs-rp mode enable

```
set dap 3 radio 2 radio-profile webqs-rp mode enable
set dap 4 serial-id stp1w20b0w model 2330
set dap 4 name AP03-MAPFRE
set dap 4 fingerprint 7f:46:e0:b7:59:ec:8e:9e:da:bd:f9:1b:9f:90:12:13
set dap 4 radio 1 radio-profile webqs-rp mode enable
set dap 4 radio 2 radio-profile webqs-rp mode enable
set dap 5 serial-id stp1w20azv model 2330
set dap 5 name AP04-MAPFRE
set dap 5 fingerprint 9f:ba:a7:c8:89:e8:ae:52:f2:06:15:65:e6:13:e7:a8
set dap 5 radio 1 radio-profile webqs-rp mode enable
set dap 5 radio 2 radio-profile webqs-rp mode enable
set dap 6 serial-id stp1w209sr model 2330
set dap 6 name AP05-MAPFRE
set dap 6 fingerprint 7f:f1:4f:34:47:0b:b8:b8:af:b1:bd:63:7c:b7:86:ef
set dap 6 radio 1 radio-profile webqs-rp mode enable
set dap 6 radio 2 radio-profile webqs-rp mode enable
set dap 7 serial-id stp1w20af1 model 2330
set dap 7 name AP06-MAPFRE
set dap 7 radio 1 radio-profile webqs-rp mode enable
set dap 7 radio 2 radio-profile webqs-rp mode enable
set dap 8 serial-id stp1w20y5q model 2330
set dap 8 name AP08-MAPFRE
set dap 8 radio 1 radio-profile webqs-rp mode enable
set dap 8 radio 2 radio-profile webqs-rp mode enable
set ip https server enable
set ip snmp server enable
set ip telnet server enable
set port 1 name Uplink_to_LAN
set port media-type 1 rj45
set vlan 1 port 1 tag 1
set vlan 101 name users
set vlan 101 port 1 tag 101
set vlan 102 name devel
set vlan 102 port 1 tag 102
set vlan 103 name guest
set vlan 103 port 1 tag 103
set spantree enable vlan 1
```

set spantree enable vlan 101

set spantree enable vlan 102

set spantree enable vlan 103

set interface 1 ip 172.18.199.101 255.255.0.0

set security acl ip portalacl permit udp 0.0.0.0 255.255.255.255 eq 68 0.0.0.0 255.255.255.255 eq 67

set security acl ip portalacl deny 0.0.0.0 255.255.255.255 capture

commit security acl portalacl

set security acl ip intnet permit icmp 192.168.116.2 0.0.0.255 172.16.254.27 0.0.0.0

commit security acl intnet

set security acl ip internet permit icmp 192.168.116.2 0.0.0.0 172.16.254.27 0.0.0.0

set security acl ip internet permit icmp 172.16.254.27 0.0.0.0 192.168.116.2 0.0.0.0

set security acl ip internet permit icmp 192.168.113.0 0.0.0.255 172.16.254.27 0.0.0.0

set security acl ip internet permit icmp 172.16.254.27 0.0.0.0 192.168.116.0 0.0.0.255

set security acl ip internet permit ip 192.168.116.0 0.0.0.255 172.16.254.27 0.0.0.0

set security acl ip internet permit ip 172.16.254.27 0.0.0.0 192.168.116.0 0.0.0.255

set security acl ip internet permit ip 192.168.116.0 0.0.0.255 192.168.241.196 0.0.0.0

set security acl ip internet permit ip 192.168.241.196 0.0.0.0 192.168.116.0 0.0.0.255

commit security acl internet

set security acl map internet vlan 102 out

set ntp enable

set ntp server 192.168.241.2

set ntp server 192.168.241.2