PROYECTO AIRC

Contenidos

- Esquema de cableado
  - Horizontal
  - Vertical
- Diseño lógico de la red
- Fichero de configuración:
  - DNS
  - DHCP
  - Red/Encaminamiento
  - Cortafuegos

- Interconexión de redes
  - ISP
  - Comunicación (seguridad y aspectos legales)
- Planificación
- Presupuesto

Introducción

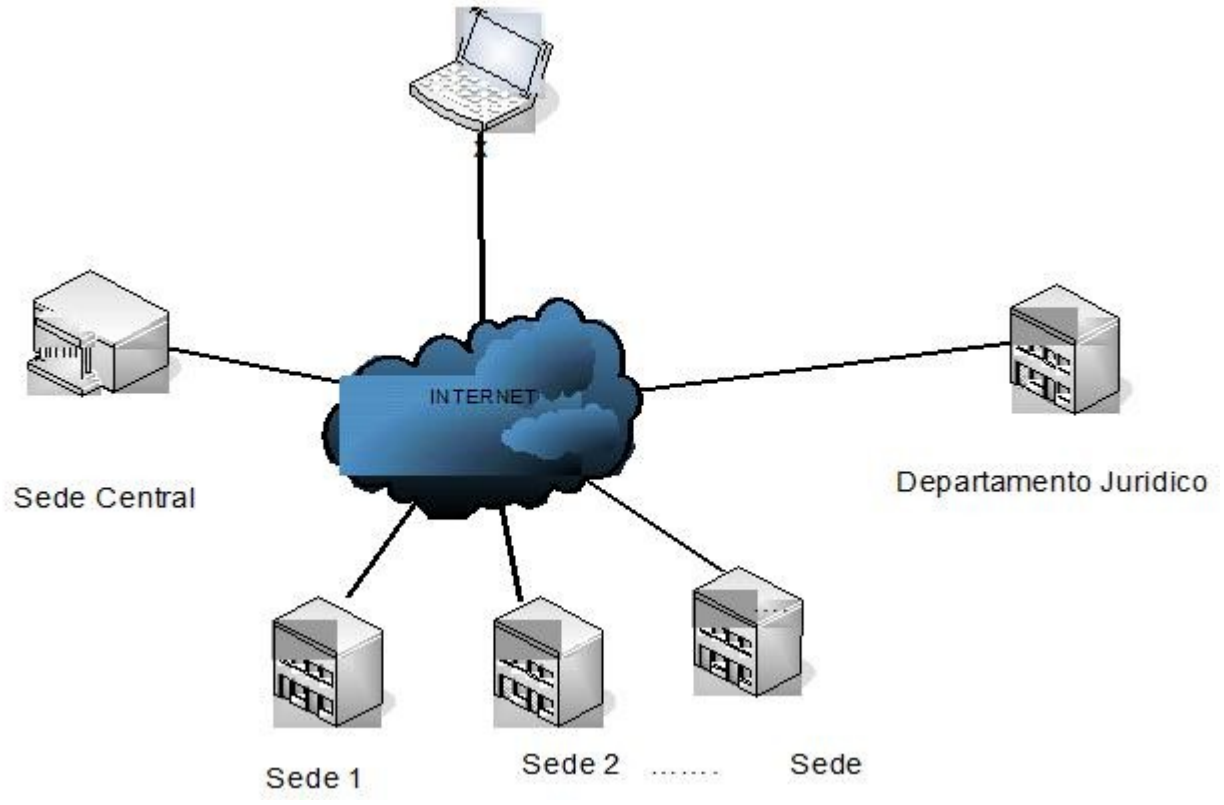
El objetivo es crear el diseño de red para la interconexión de los sistemas informáticos de una empresa con sede cental en Alicante y supermercados situados en varias provincias.

Partimos de una situación inicial en la cual la empresa no dispone de ningún tipo de red anterior, y nuestra tarea será la de diseñar la red de los supermercados así como la iterconexión de todos estos a la sede central.

Por otra parte se van a ofrecer una serie de servicios externos, en primer lugar un servicio de venta on-line que residirá en la sede cental y por otro lado una intranet de gestión para el personal de la empresa desde donde podrán gestionar pedidos, suministros, turnos de los repartidores, etc.

En la empresa se encuentan 6 tipos de trabajadores: dependientes, administrativos, contabilidad, generentes de supermercado, técnicos informáticos y dirección.
En cuanto a la organización, en la sede de Alicante primera planta trabaja toda la dirección, el departamento de contabilidad y en la planta baja el servicio de informática así como también disponemos de un departamento jurídico pero está ubicado en un edificio externo.
Al margen de la oficina central, en cada supermercado trabajan 15 personas: 3 repartidores, 9 dependientes, 2 administrativos y un gerente.

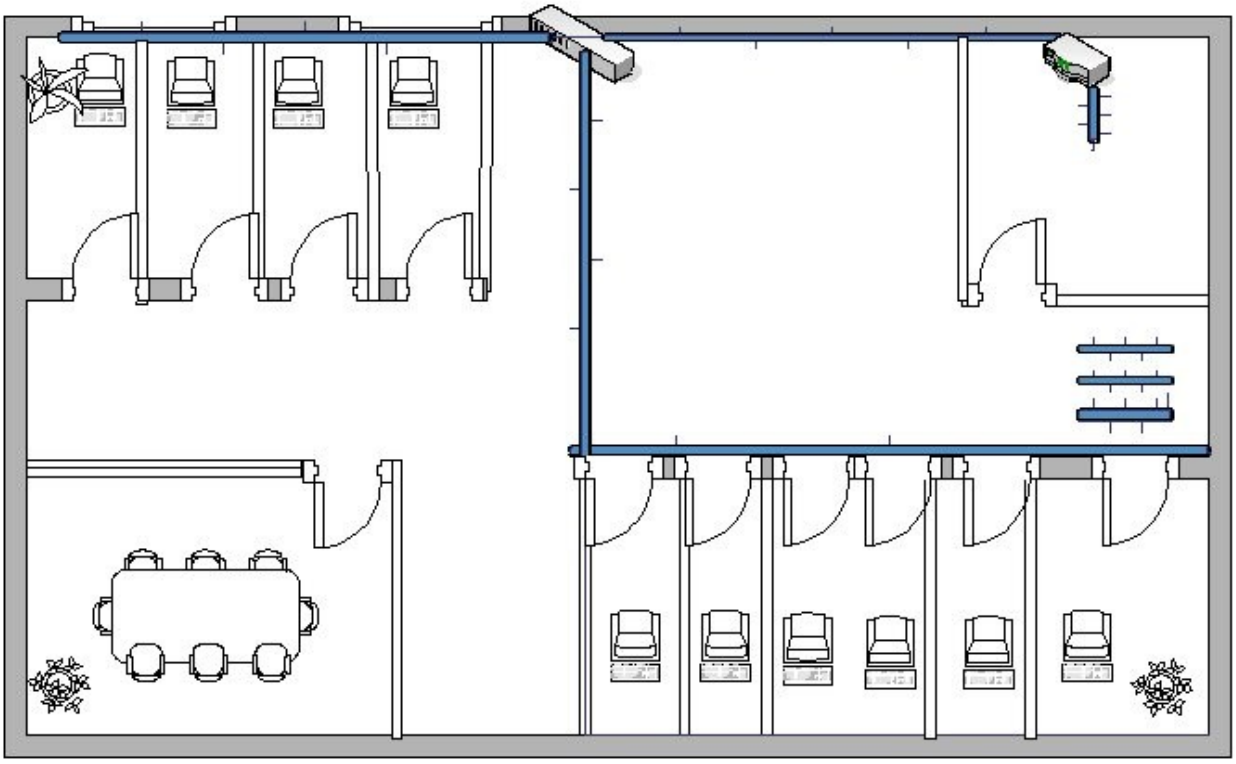
El diseño general de nuestra solución será algo de este estilo.



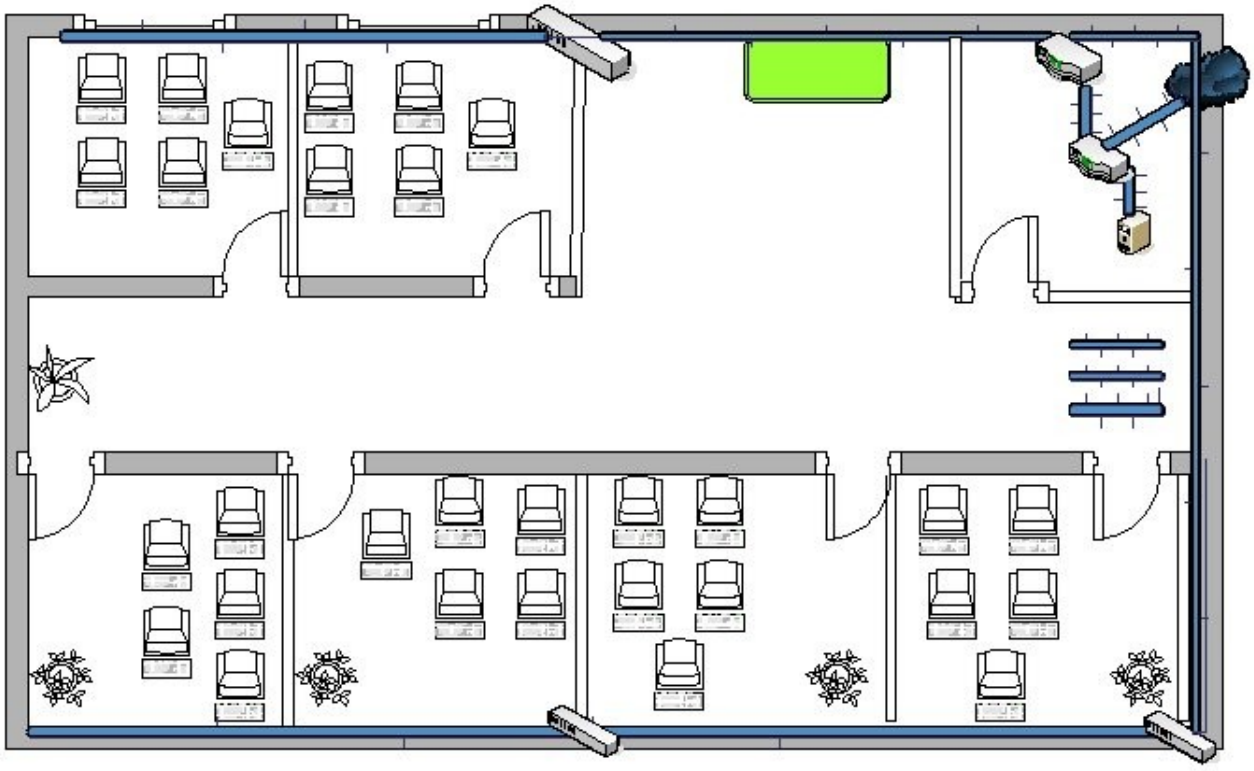
Distribución física

Plano de la primera planta, donde irá situado dirección y el departamento de contabilidad.

En esta planta cada directivo tiene un despacho además de existir una sala de juntas para hacer reuniones, cada cable UTP saldrá de la máquina del usuario hasta el switch de 24 puertos.



La planta de abajo es donde reside el servicio de informática, ellos mantienen el enlace a internet y los servidores.



Vamos a utilizar estos dispositivos:

Broadband Router

Switch 24 puertos 10/100/1000Mbps

MODEM – Router ADSL 4 puertos

Boradband Router

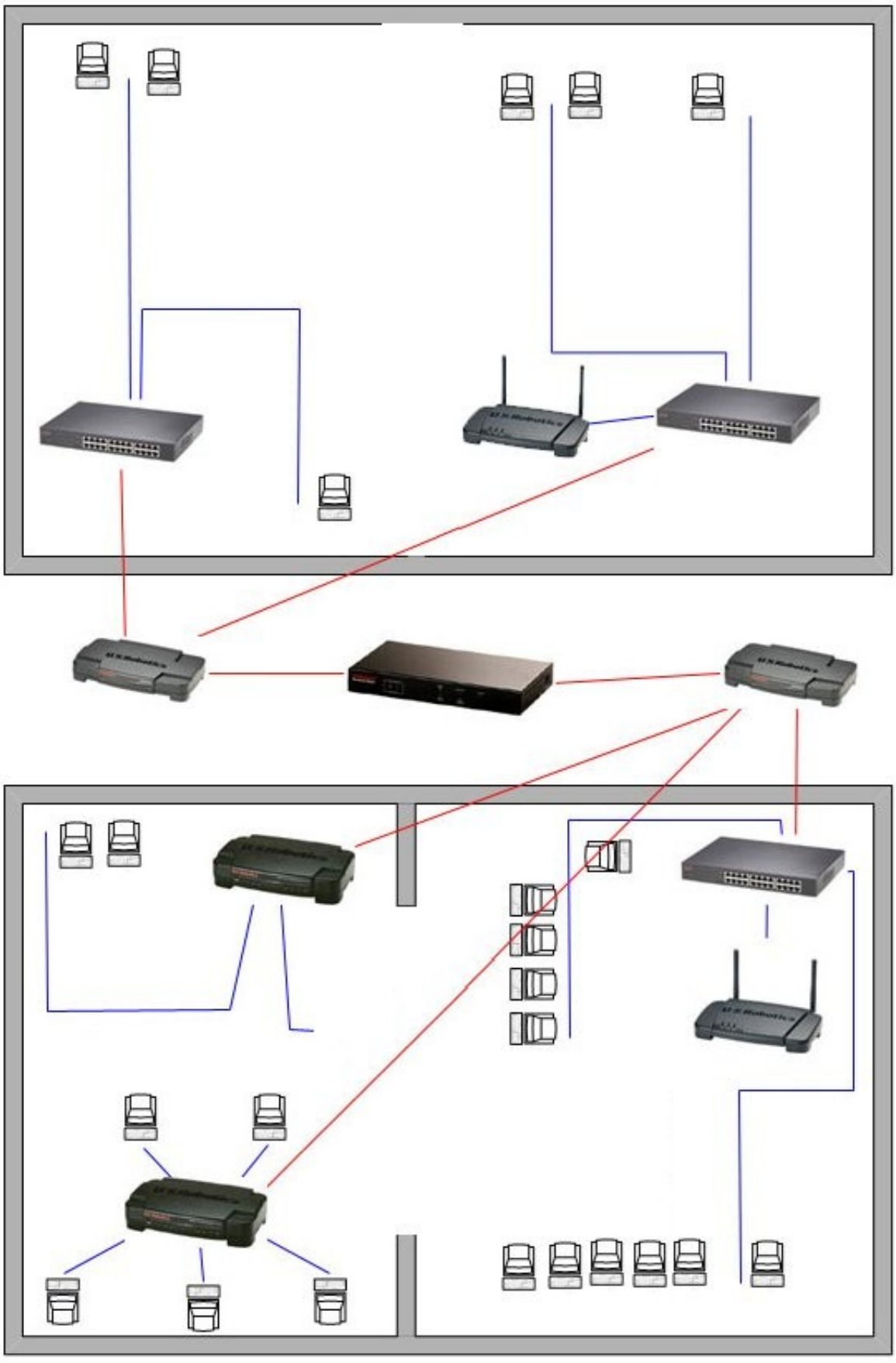
Router – punto de acceso 10/100Mbps 802.11g

Punto de acceso 10/100Mbps 802.11g

Tarjeta de red PCI 10/100Mbps

Tarjeta de red PCMCIA

Sin atender estrictamente a la disposicón física de las máquinas, este sería un esquena a nivel de dispositivos de red de las dos plantas, switchs, routers, puntos de acceso inalámbricos.



Diseño Estructurado

Introducción

Una vez analizados los requisitos de la empresa el siguiente paso es decidir la topología que mejor se adapte a nuestro caso. En concreto, vamos a emplear una topología de estrella extendidausando Ethernet 802.3 ya que actualmente es la tecnología dominante, ampliamente extendida.

El cableado físico es uno de los componentes más importantes a considerar cuando se diseña una red. En esta fase de diseño debemos decidir el tipo de cableado a utilizar y la estructura global.

La conexión consta de un MDF que se encargará de interconectar la red Internet con los distintos routers internos de la LAN. Éste MDF irá situado en un armario en la planta baja de la sede principal.

Los elementos intermedios de conexión se denominan IDF y dentro de éstos elementos encontramos dos tipos: HCC (Conexión cruzada horizontal) y VCC (Conexión cruzada vertical).

Los VCC se encargarán de conectar los HCC con el MDF, estableciendo la conexión vertical del cableado.

Cableado horizontal

Para el cableado horizontal usaremos Cable UTP categoría 5e. La distancia máxima es menor de 100 m. A la hora de seleccionar el cableado hemos de tenido en cuenta que la red queremos que nos va a durar de 7 a 10 años por la calidad del cable, esto debe ser una prioridad aunque nos vaya a costar un poco mas caro.

Al ser una red nueva emplearemos conexiones Ethernet 10/100 (fast ethernet), debido a su buena relación calidad/precio , su alta disponibilidad , facilidad de instalación y mantenimiento.

Usaremos switchs de 24 puertos para asegurar cualquier necesidad próxima de puestos de trabajo, ya que los 144 puestos que nos proporcionan los 8 switchs es superior a la cifra de trabajadores actual (70). Colocaremos 6 HCC, repartidos entre la dirección, el departamento, de contabilidad, el servicio de informática y servidores.

Dos de ellos irán situados en la primera planta, uno para la dirección y otro para el departamento de contabilidad, ya que la cifra de trabajadores en cada uno de ellos, no

supera los 12 trabajadores. El resto en la planta baja donde podemos encontrar el servicio de informática (necesitaremos 2 switches), y el cpd con los servidores, otros dos.

Organización en la sede central

Los tabajadores irán en dos plantas, por un lado en la primera planta nos podemos encontrar al depar

Cableado vertical

Para el cableado vertical usaremos cable de fibra óptica. Teniendo en cuenta que el cableado nos tiene que durar 7 aprox años.

Colocaremos dos de VCC, uno por planta. La forma de conectar los VCC será, el VCC de la planta baja lo pondremos en el MDF, y el otro estará colocadosen su correspondiente IDF.
Tendremos un VCC que conecte el HCC de los directivos con el Router del MDF y un segundo HCC que conectera en router de la planta baja con los tecnicos informaticos.

Diseño Lógico de la red

El esquema de direccionamiento IP es algo que se debe diseñar prestando atención a cómo está dispuesta la organización de la empresa, tanto a nivel lógico como físico.

Es muy importante que esté documentado y archivado por posibles cambios en el futuro o reestructuraciones.

Usaremos una distribucción de direcciones IP basandonos utilizando ips de clase A por su sencilla manipulación.

Uno de los parámetros que nos va a venir bien conocer dada una dirección IP es la ubicación física de éstas, por lo tanto vamos a crear un esquema en el cual se utilizara el segundo octeto para indicar la ubicación, es decir, si es la sede central, o qué supermercado, también dentro de cada edificio se utilizara el tercer octeto para indicar a qué departamento se refiere.

El tráfico entre el departamento jurídico y la sede central se realizará mediante una vpn con IPSec, para que el tráfico vaya cifrado, ya que aparte de la Intranet mediante HTTPS, se utilizan otros mecanismos como un programa a medida que realiza peticiones para la obtención de datos, así como el trasiego de correos electrónicos con información privada.

Supermercados

Usaremos direccionamiento privado en las sedes con el sistema que hemos comentado para la sede centrla, y tendremos un enlace que nos comunicará con Internet y a su vez podremos acceder a la intranet de la central mediante HTTPS (usando la capa de seguridad SSL).

Como hemos comentado usaremos cable categoria 5e, y será importante tener en cuenta que en los supermercados el cableado de estar lo más alejado posible de motores o cualquier otra fuente que pueda inducir ruido en el cableado. Supondremos que ningún supermercados es de más de 100m, pero si en un futuro hubiera alguno habria que tener en cuenta situación de los dispositivos de interconexión.

Direccionamiento

10.1.X.X -> sede central

10.10.X.X -> primer supermercado

10.11.X.X -> segundo supermercado

10.12.X.X -> tercer supermercado

etc

dentro de la sede central tendremos:

En la planta baja al servicio de informático con su subred:

10. 1.2.X Servicio de informática

10.1.100.X Servidores

En la primer planta tenemos:

10.1.3.X Dirección

10.1.4.X Departamento de contabilidad

Supermercados

En cada supermercado trabajan 15 personas: 3 repartidores, 9 dependientes, 2 administrativos y un gerente.

Usaremos este direccionamiento:

10.Y.2.1 Gerente

10.Y.3.X Repartidores

10.Y.4.X Dependientes

10.Y.2.X Administrativos

Ficheros de configuración

DNS

El Domain Name System (**DNS**) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos (técnicamente, este archivo aún existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts).

El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo HOSTS no resultara práctico y en 1983, Paul Mockapetris publicó los RFCs 882 y 883 definiendo lo que hoy en día ha evolucionado al DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y 1035).

básicamente para configurar el servidor DNS tenemos que modificar dos ficheros:

Para configurar los parámetros del servidor de DHCP tendremos que tocar varios ficheros, en primer lugar el fichero /etc/host.conf

```
# Buscar los nombres primero en el fichero /etc/hosts y después mediante búsqueda DNS
order hosts, bind
# No disponemos de máquinas con múltiples direcciones IP
multi on
# Comprobacion ante falseamiento de direcciones (ip spoofing)
nospoof on
# Alerta de los intentos de falseamiento de direcciones
alert on
```

De esta manera podremos configurar el fichero /etc/hosts con algunos host de los cuales queramos evitar que se produzcan peticiones DNS (quizá para mejorar el rendimiento con alguna máquina que usemos con frecuencia).

Ahora nos vamos a encargar del fichero /etc/named.conf, que es el fichero principal de nuestro servidor de DNS

```
options {
        // las tablas de Dns irán situadas en este directorio
        directory "/var/named";

        // Las peticiones que no se puedan resolver las reenviamos al servidor
              //Dns de nuestro ISP
        forwarders {
               ISP_DNS_IP;
        };


};


zone "." {
        type hint;
        file "root.cache";
};

zone "localhost" {
        type master;
        file "localhost";
        allow-update { none; };
        allow-transfer { secundarios; };
        allow-query { 127.0.0.1; };
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "localhost.rev";
        allow-update { none; };
        allow-transfer { secundarios; };
        allow-query { 127.0.0.1; };
};



// Fichero DNS ppal
zone "airc.es" {
        type master;
        file "airc.es.db";
        allow-transfer { 127.0.0.1; };
};


// Consulta inversa para las direcciones privadas
zone "1.10.IN-ADDR.ARPA" {
        type master;
        file "10.1.rev";
        allow-transfer { 127.0.0.1; };
};
```

Por motivos de seguridad montaremos este servicio en una jaula, para de esta manera ante un incidente en el sistema, el impacto será mucho menor.
No cmentaré la configuración extra que supone montar un servicio en una jaula porque considero que no es el objetivo de este trabajo.

Para manejar tanto las consultas recibidas desde la red interna y las recibidas desde la red externa utilizaremos **vistas de dns**:

```
acl internal { 10.1.2/24 10.1.1/24 ;};
View internal {
        math-clients { internal; };
        zone “airc.es” {
                type master;
                files “db.airc.interna”;
        };
};
View external {
        math-clients { any; };
        zone “airc.es” {
                type master;
                files “db.airc.externa”;
        };
};
```

fichero principal:

```
airces.   300   IN   SOA   dns.airc.es. root.dns.airc.es. (
                  2004031004                    Número de serie
                  10800                 Segundos tras los que los secundarios deben conectarse al primario
                  3600                  Si hay error, reintenta cada 3600 segundos
                  3600000               Si no lo consigue tras este tiempo, que deje de responder a consultas
                  300 )                 Mínimo para guardar datos en cachés.

300   IN   A     10.1.100.22
300   IN   NS    dns.airc.es.
300   IN   NS    srvdns.airc.es.
300   IN   MX    10 correo.airc.es.
www       300   IN   A     10.1.100.45
web   300   IN   CNAME www.airc.es.
correo    300   IN   A     10.1.100.66
```

en cuanto a la resolución inversa

```
1.10.in.addr.arpa. IN SOA dns.sede.airc.es.
root.sede.airc.es. (
1 ;Serial
604800 ;Refresh
86400 ;Retry
2419200 ;Expire
604800 ) ;Negative cache TTL
; Servidor DNS
30.172.in-addr.arpa. IN NS dns.airc.es.

; Servidor intranet
100.56 IN PTR srvIntranet.airc.es.
100.57 IN PTR srvExtranet.airc.es.
3.1 IN PTR routerVCC1.airc.es.
4.3 IN PTR routerVCC1.airc.es.
1.1 IN PTR routerMDF.airc.es.
2.2 IN PTR routerMDF.airc.es.
3.4 IN PTR dns.airc.es.
```

DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Este protocolo para la condiguración dinámica de los parámetros TCP/IP de las máquinas es el que vamos a usar para implementar nuestro esquema lógico planteado lineas arriba y de esta manera será más fácil su mantenimiento.

Tendremos para cada subred un bloque en el dhcpd.conf similar a esto:

```
# dhcpd.conf
#default-lease-time 600;
#max-lease-time 7200;

subnet 10.1.4.0 netmask 255.255.255.224{
        range 10.1.4.1 10.1.4.255;
        option domain-name "airc.es";
```

```
        option domain-name-servers 10.1.100.22;
        option routers 10.1.4.1 ;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.1.4.255;
}
```

Podríamos asignar Ips fijas dependiendo de la máquina en cuestión basandonos en su dirección MAC, por ejemplo imaginemos que en la subred 25 tenemos ciertas máquinas con dirección fija (un servidor no puede cambiar su ip dinámicamente si queremos ofrecer algún servicio)

```
 subnet 10.1.3.0 netmask 255.255.255.224{
        option domain-name "airc.es";
        option domain-name-servers 10.1.100.22;
        option routers 10.1.3.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.1.31;
        host PCA1 {
                hardware ethernet  54:61:4E:F3:7D:08;
                fixed-address 10.1.3.34;
        }
        host PCA2 {
                hardware ethernet  54:61:4E:BE:49:D3;
                fixed-address 10.1.3.35;
        }
}
```

Ahora presentamos los ficheros configuración para los parámetros de enrutamiento asi como de los de cortafuegos, iptables.

Securización de los servidores: cortafuegos

Vamos a crear un fichero de configuración de iptables, suponiendo que fuera una debian lo situaríamos en /etc/init.d/ y lo añadiriamos al runlevel que toque,

```
#!/bin/bash
#
# Fichero de configuración iptables para MercAIRC
if [ ! -x /sbin/iptables ]; then
exit 0
fi

start()
{
echo "Iniciando IPTables.."

# limpiamos...
clearall


#reglas para poder establecer comunicaciones TCP y tráfico de salida

iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j
ACCEPT
iptables -A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

# aceptamos conexiones mediante ssh de la red de administración
iptables -A INPUT -s $RED_ADM -d SERVER -p tcp --dport 22 -j ACCEPT

# permitimos puerto 80
iptables -A INPUT -d server -p tcp --dport 80 -j ACCEPT

# permitimos puerto 443
iptables -A INPUT -d server -p tcp --dport 443 -j ACCEPT

# aceptamos samba en la red local
iptables -A INPUT -p udp -m udp -s network/24 --dport 137 -j ACCEPT
iptables -A INPUT -p udp -m udp -s network/24 --dport 138 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp -s network/24 --
dport 139 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp -s network/24 --
dport 445 -j ACCEPT

# reglas para el tráfico de localhost
iptables -A INPUT -d server -s 127.0.0.1 -j ACCEPT
```

```
# protección de syn flood
iptables -A INPUT –p tcp --syn -m limit --limit 5/second -j ACCEPT

#logeamos los logs para su posterior analisis, añadimos el prefijo
#Dropped: para facilitar la tarea de búsqueda en los logs
iptables -A INPUT -j LOG --log-prefix "Dropped: "

# no permitimos nada mas a esta up
iptables -A INPUT -d server -j REJECT

# bloqueamos cualquier otro tipo de trafico
iptables -A INPUT -j REJECT
iptables -A FORWARD -j REJECT



echo "IPTables iniciado ok..."

}

clearall()
{
iptables -F
iptables -X
echo "Reglas de IPTables limpiado..."
}


case "$1" in
restart|start)
start
;;
stop)
clearall
;;
*)
echo "Usage: $0 {start|stop|restart}"
exit 1
esac

exit 0
```

Los routers deberian llevar reglas que permitan el forwarding, además de que realizarán NAT inverso para los servidores, de igual manera añadiríamos los casos para poder lanzarlo con start, stop etc, y añadirlo en el init.d y el runlevel que toque.

#este prodría ser un script para los enrutadores

```
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables --flush
```

```
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
iptables -P OUTPUT ACCEPT
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT


#NAT
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE

iptables --append FORWARD --in-interface eth1 -j ACCEPT
iptables --append FORWARD --in-interface eth2 -j ACCEPT

# ssh
iptables -A INPUT -s 10.1.2.0/24 -p tcp --dport 22 -j ACCEPT

#dns
iptables -A FORWARD  -p udp --sport 53 -j ACCEPT


# NAT inverso para los servidores 80 y 443
#iptables -A INPUT -p tcp -dport 80 -j ACCEPT
iptables -A FORWARD  -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD  -p tcp --dport 80 -j ACCEPT
#iptables -A INPUT -p tcp -dport 443 -j ACCEPT
iptables -A FORWARD  -p tcp --sport 443 -j ACCEPT
iptables -A FORWARD  -p tcp --dport 443 -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to  10.1.100.45:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.1.100.45:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 10.1.100.45:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 10.1.100.45:443
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to 10.1.100.45:443
iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 443 -j DNAT --to 10.1.100.45:443

# logeo de paquetes
iptables -A INPUT -m tcp -p tcp -j LOG
iptables -A OUTPUT  -m tcp -p tcp -j LOG
iptables -A INPUT -m udp -p udp -j LOG
iptables -A OUTPUT  -m udp -p udp -j LOG
iptables -A FORWARD -m tcp -p tcp -j LOG
iptables -A FORWARD  -m udp -p udp -j LOG

echo 1 > /proc/sys/net/ipv4/ip_forward
```

Red y encaminamiento

Es muy importante configurar correctamente cada router de la red con la IP que le toca y las rutas adecuadas.
Básicamente es plasmar en configuración la estructura de direccionamiento IP que hemos planteado en la estructura lógica expuesta más arriba.

Vamos a suponer que estamos utilizando routers en linux, de esta manera utilizaremos la instrucción ip para configurarlos, como también para el firewall supondremos que utilizamos máquinas Linux con Netfilter y expondremos las reglas iptables para su correcta configuración.
De esta manera crearemos una configuración general, que luego podrá ser adaptada a cualquier tipo de tecnología.

Sede Alicante

Router MDF:

#Interfaces directas del router principal

ip addr add 10.1.1.0/24 broadcast 10.1.1.255 dev eth1 #Planta baja
ip addr add 10.1.3.0/24 broadcast 10.1.1.255 dev eth2 #Planta 1
ip addr add 10.1.100.0/24 broadcast 10.1.1.255 dev eth3 #servidores

//Planta Baja
ip route add 10.1.1.0/24 via 10.1.1.1
ip route add 10.2.1.0/24 via 10.1.2.1
ip route add 10.100.2.0/24 via 10.1.100.1

//Planta Primera
ip route add 10.1.3.0/24 via 10.1.3.1
ip route add 10.1.4.0/24 via 10.1.4.1

ip route add 0.0.0.0/0 via IP_ISP

• **Router VCC 1:**

ip addr add 10.1.1.0/24 broadcast 10.1.1.255 dev eth0
ip addr add 10.1.2.0/24 broadcast 10.1.2.255 dev eth1

ip route add 0.0.0.0/0 via 10.1.1.1

• **Router VCC 2:**

ip addr add 10.1.3.0/24 broadcast 10.13.255 dev eth0
ip addr add 10.1.4.0/24 broadcast 10.1.4.255 dev eth1

ip route add 0.0.0.0/0 via 10.1.0.3

Delegaciones

• **Router VCC**

ip addr add 10.X.2.0/24 broadcast 10.X.2.255 dev eth0
ip addr add 10.X.3.0/24 broadcast 10.X.3.255 dev eth1
ip addr add 10.X.4.0/24 broadcast 10.X.4.255 dev eth2
ip addr add 10.X.5.0/24 broadcast 10.X.5.255 dev eth3

ip route add 0.0.0.0/0 via IP_ISP

Seguridad: Consideraciones legales

Un tema muy importante, por lo vital que son los datos y su seguridad para una empresa, son las medidas de seguridad, ya no solo ante una pérdida, interceptación, etc, sino también por el compromiso legal al que estamos obligado.

En concreto nos interesan dos de las normativas legales sobre sistemas informáticos que nos afectan directamente:

a) Ley Orgánica 19/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)
b) Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automátizados que contengan datos de carácter personal.

Ya que con toda seguridad nuestra empresa almacenará y transferirá por la red datos de este tipo, otro tipo de normativas como la LSSI o la LISI no las trateremos en este trabajo.

La normativa a cumplir viene directamente relacionada por la naturaleza de los datos que manejamos, concretamente se ha dividido en 3 niveles:

Niveles de seguridad
- Básico: datos de carácter personal
- Medio: datos de infracciones administrativas, penales, servicios financieros, o personales que permitan evaluación de la personalidad del individuo
- Alto: datos de ideología, religión, creencias, raza, salud, vida sexual y política

En nuestro caso estaríamos en el caso Medio, ya que trataremos con datos de carácter personal y además de servicios financieros (nóminas de empleados, cuentas de proveedores, etc)

Vamos a ver qué normas debemos cumplir para cumplir la ley al trabajar con este tipo de datos:

Nivel básico
- Documento de seguridad con normativa básica
- Mecanismos de actualización y revisión de normativa
- Documento de obligaciones y funciones del personal
- Medidas para informar al personal sobre la normativa
- Registro de incidencias
- Relación de usuarios y procedimientos de ident / auten

- Renovación periódica de contraseñas y almacenamiento ininteligible
- Mecanismos para evitar intrusiones no autorizadas
- Control de soportes (inventario)
- Control de salidas de soportes
- Copias de respaldo, al menos semanalmente

Como vemos va desde algo tan lógico como guardar una copia de seguridad de los datos, como mantener un documento de seguridad o registrar las incidencias que ocurran.

Pero vamos a ver además de todo lo visto para el nivel básico que otras normas debemos cumplir al estar catalogados los datos con los que trabajará la empresa de “nivel medio”:

- Documento de seguridad ampliado
- Designación de responsables de seguridad
- Consignación de recuperación de incidencias
- Autorización escrita del responsable para recuperar ficheros
- Identificación unívoca de usuarios
- Limitación de accesos no autorizados reincidentes
- Control de acceso físico
- Registro de entrada y salida de soportes
- Mecanismo para impedir recuperaciones de información almacenada en soportes
- Auditorías informáticas cada 2 años
- Pruebas con datos ficticiose actualización y revisión de normativa
- Documento de obligaciones y funciones del personal
- Medidas para informar al personal sobre la normativa
- Registro de incidencias
- Relación de usuarios y procedimientos de ident / auten
- Renovación periódica de contraseñas y almacenamiento ininteligible
- Mecanismos para evitar intrusiones no autorizadas
- Control de soportes (inventario)
- Control de salidas de soportes
- Copias de respaldo, al menos semanalmente
- Cifrado de la información en los soportes
- Transmisión cifrada de datos

De todo este listado, cuando diseñamos la red nos afecta directamente solo algunos de ellos, como por ejemplo la transmisión de información de forma cifrada, o el almacenamiento de ciertos datos importantes como las passwords de igual forma cifradas. Así como también saber que necesitaremos métodos de autenticación basadas en usuario/password y log de éstas (esto nos afectará en cuanto a la manera de disponer los servidore, así como también en la manea que habrá que tratar la información a la hora de ser transferida).

ISP

Algo que no debemos olvidar es nuestra conexión a internet.

Para los supermercados contrataremos una linea T1 o equivalente (1544 kbps), y en la central tendremos un enlace T3 o equivalente (44736 kbps)para tener un acceso rápido a Internet para todos los trabajadores, y para que los servidores puedan servir el servicio de venta onlinea, así como sportar todas las operaciones que se realizan mediante la Intranet, desde cualquier punto de la sede o cualquier supermercado, los cuales accederán mediante HTTPS para así usar un canal cifrado.

Presupuesto

Tenemos pensado una serie realizar el proceso en una serie de días, en concreto hemos calculado que para desplegar el cableado, dejar configurados los sistemas de red, configuración de Intenet necesitaremos de dos a tres días por cada supermercado, y para la central necesitaremos también unos tres días para cada planta.

En cuanto al presupuessto se detalla lo que costará (sin tener en cuenta el precio de los servidores que servirán la intranet y el servicio de venta online, necesitaremos servidores de bases de datos, web, correo, dhcp y dns).

Jueves 19:00-21:00

San Vicente (ALICANTE)

MERCAIRC
UA
San Vicente (ALICANTE)

San Vicente de Raspeig, Viernes 11 de enero de 2008

Producto	Cant.	Precios	Total
Hardware			
US Robotics Broadband Router	1	70,74 €	70,74 €
US Robotics Switch 24 puertos 10/100/1000Mbps	3	322,88 €	968,64 €
US Robotics Router ADSL 4 puertos 10/100Mbps	3	79,00 €	237,00 €
US Robotics BroadBand Router 8 puertos	5	149,50 €	747,50 €
US Robotics Router + Punto de Acceso 10/100Mbps	1	139,50 €	139,50 €
US Robotics Punto de Acceso 10/100Mbps	3	149,50 €	448,50 €
US Robotics Tarjeta Red PCMCIA 10/100Mbps	30	46,00 €	1.380,00 €
US Robotics Tarjeta Red PCI 10/100Mbps	10	41,00 €	410,00 €
Cableado			
Cable UTP cat5 10/100Mbps 1350 metros	4	68,39 €	273,56 €
Fibra Multimodal por 30 metros	3	128,91 €	386,73 €
Conectores RJ45 Macho 25u	10	10,00 €	100,00 €

Conectores RJ45 Hembre 25 u	10	10,00 €	100,00 €
Conectores Fibra Macho FO MM LC (900 um) unidad	20	5,00 €	100,00 €
Conectores Fibra Hembra FO MM LC (900 um) unidad	20	5,00 €	100,00 €
Canaleta Plástica CP-6015 por metro	50	2,00 €	100,00 €
Esquinas canaleta	20	4,00 €	80,00 €
Mano de Obra			
Instalaciónes eléctricas por horas 5 personas	60	14,50 €	4350,00 €
Configuración Hardware por horas 3 personas	30	20,00 €	1800,00 €
Desplazamiento	16	35,50 €	568,00 €
		TOTAL	12.810,07 €

* Al total se le añadirá un 16% de IVA

** Mantenimiento Adicional 90€/mes más desplazamientos

Planificación

La duración de la implantación esta pensada para realizar el proceso en tres semanas:

En primer lugar se cableará cada supermercado dependiendo del plano de este, se desplazarán los instaladores, y se realizará la puesto en marcha de los dispositivos hardware de red.

Se realizará la implantación sobre la sede central, instalando las tarejtas de red en las máquinas cliente, pasando cableado e interconectando cada dispositivo de red, situando y configurando los routers, las reglas de enrutamiento, servidores, etc.

Despliegue de la apicación de comercio eléctrónico que será responsabilidad del servicio de informática.

Se realizarán diferentes pruebas para comprobar que todo funciona correctamente.

Bibliografía

http://es.wikipedia.org/wiki/Dns

http://es.wikipedia.org/wiki/DHCP

http://es.wikipedia.org/wiki/Iptables

http://www.cse.msu.edu/~minutsil/iptables.html

http://blogs.ua.es/airc