INTEGRACIÓN REDES TELEMÁTICAS
CONSULTOR: JOSE LOPEZ VICARIO

Diseño de una red dinámica: Vivero de Empresas

Trabajo fin de carrera

Miguel Ángel Martín Sánchez

14/06/2013

IT Telecom. Telemática

ÍNDICE

1 DESCRIPCION DEL PROYECTO 4
2 OBJETIVO DEL PROYECTO 5
3 EDIFICIO 6
4 ARQUITECTURA BÁSICA 7
4.1 Conmutación 7
4.2 Encaminamiento 10
4.3 Internet 11
5 ARQUITECTURA LÓGICA 12
5.1 Plan de direccionamiento IP, VLANs y VRFs 13
5.1.1 Direccionamiento IP 13
5.1.2 VLANs 14
5.1.3 VRFs 16
6 SERVICIOS DE RED 18
6.1 Identificación de equipos 18
6.2 Topología de árbol 18
6.3 Configuración básica puertos en los conmutadores 19
6.3.1 Puertos de acceso 19
6.3.2 Puertos troncales 21
6.3.3 Enlaces agregados 21
6.4 Configuración básica puertos de encaminamiento 21
6.5 Autenticación en red 22
6.5.1 RADIUS 22
6.5.2 Autenticación 802.1X para acceso a la red 23
6.5.3 Autenticación sin suplicante (MAC) 25
6.6 Otros servicios 26
6.6.1 LDAP 26
6.6.2 DHCP 27
7 PRESUPUESTO 28
7.1.1 Viabilidad económica del proyecto 30
8 CONCLUSIONES 32
9 ANEXOS 33
9.1 Anexo I. Planificación del trabajo 33
9.2 Anexo II. Glosario 35

9.3 Anexo III. Enlaces documentación utilizada.....36
10 ÍNDICE DE ILUSTRACIONES 39
11 ÍNDICE DE TABLAS.....40

1 DESCRIPCION DEL PROYECTO

El presente documento describirá el diseño de una red cableada en un edificio de oficinas destinado a vivero de empresas.

En este documento se realizará la descripción del diseño de la solución de asignación dinámica de recursos de red empleando sistemas estandar.

Queda fuera del alcance todo lo relacionado con la infraestructura fisica, se presupone que el edificio del supuesto ya cuenta con canalizaciones, cableado, armarios para equipamiento, etc.

Para este fin se describirá que conjunto de protocolos y tecnicas se deben emplear al configurar la electrónica de red y con que medios se ha de contar para dar los servicios de red óptimos.

2 OBJETIVO DEL PROYECTO

El objetivo del proyecto es el diseño de la red de un vivero de empresas donde todas las tomas de red se configuren de forma dinámica dependiendo del equipo que se conecte a ella. De esta forma se puede compartir la infraestructura de red entre todas las empresas pero separando todo el tráfico de red según la empresa por medio de redes virtuales diferentes.

El objetivo principal de construir una red dinámica y auto-provisionada es sobre todo reducir los costes de operación y mantenimiento de una red de estas características.

Un vivero de empresas proporciona una infraestructura a pequeñas empresas para el inicio de su actividad. Las instituciones publicas son las que, normalmente, proporcionan estos servicios por un tiempo determinado a estas empresas, esto supone un reto para los administradores de red que tienen que ir configurando continuamente los sistemas de comunicaciones para dar servicio a esas empresas.

Las tareas más comunes de operación y administración serian la configuración de los puertos de red dependiendo de quien se conecte en cada momento a cada toma (para asegurar que las redes de cada empresa son independientes).

Uno de los problemas con los que se pueden encontrar es la utilización de salas de reuniones comunes o despachos compartidos, esta topología de tomas de acceso haría que los administradores de red cambiasen continuamente la confirmación de los puertos y las empresas dependerían de estos para la utilización de los recursos de red en cada momento.

La propuesta incluye el uso de redes virtuales independientes para cada empresa, es decir, utilizar la infraestructura de red de forma conjunta pero independizando una red de otra. En la parte de conmutación se utilizarán redes de área local virtuales (VLAN) y en la parte de enrutamiento se utilizarán múltiples instancias de enrutamiento y envío virtuales (multi-VRF).

Una red “inteligente” que cambie la configuración del puerto automáticamente en función de que empresa conecta el dispositivo, sin necesidad de que un administrador cambie la configuración de red, asegurando que la red de cada empresa sea totalmente independiente del resto es el objetivo de este proyecto.

3 EDIFICIO

El edificio del proyecto será habilitado por una institución pública para el uso como vivero de empresas y de esta forma proporcionar servicios a emprendedores en su inicio de actividad por el periodo de 24 meses.

El supuesto edificio del proyecto constará de varias plantas, despachos y zonas comunes donde se podrá dar servicio a un total de cincuenta pequeñas empresas.

Se cuenta con todas las infraestructuras de canalizaciones y cableados para montar la red del supuesto, así como armarios donde instalar la electrónica de red y los servidores.

Cada empresa estará en una red separada y podrá disponer de hasta 29 equipos conectados a la red simultáneamente, esto se tendrá en cuenta en el plan de direccionamiento del proyecto y se crearan 50 redes con mascara 27, reservando una dirección de cada subred para puerta de enlace de cada segmento.

Para el dimensionamiento de los equipos de conmutación se ha realizado una tabla que, se adjunta a continuación, a modo de resumen del reparto de puertos por planta:

Plantas	Puertos
Planta 0	192
Planta 1	384
Planta 2	384

Tabla 1: Resumen de puertos

Ha de tenerse en cuenta que aunque se prevea un edificio para 50 empresas de hasta 29 equipos por empresa no se pretende provisionar 1450 puertos, sino que se cuenta con que la mayoría de empresas serán de tamaño reducido, no llegando a los 29 equipos. De esta forma se reducen los costes y no se sobredimensiona la red.

Otro de los aspectos a tener en cuenta es que en la actualidad se tiende a la virtualización de equipos, por lo que en un solo puerto podría haber varias máquinas virtuales (VM), esto quiere decir que una empresa puede montar un servidor donde aloje sus maquinas virtuales y habría que entregar una ip diferente a cada una de ellas aunque se conecten al mismo puerto.

La previsión es de un total de 960 puertos, ahorrando un total de 490 de los 1450, lo que supone un ahorro económico importante de mas de 23000€.

4 ARQUITECTURA BÁSICA

Se han valorado varios fabricantes de electrónica de red profesionales, se ha elegido Enterasys por se muy competitivo en el tipo de entornos propuestos. Otros fabricantes como Cisco o Juniper tienen mayor peso a nivel de enrutamiento en operadoras o interconexión de sedes de empresas, pero en nuestro caso se evalúa la red de área local.

Revisando graficas a que evalúan funcionalidades, arquitectura, innovación, etc, vemos un buen posicionamiento de Enterasys:

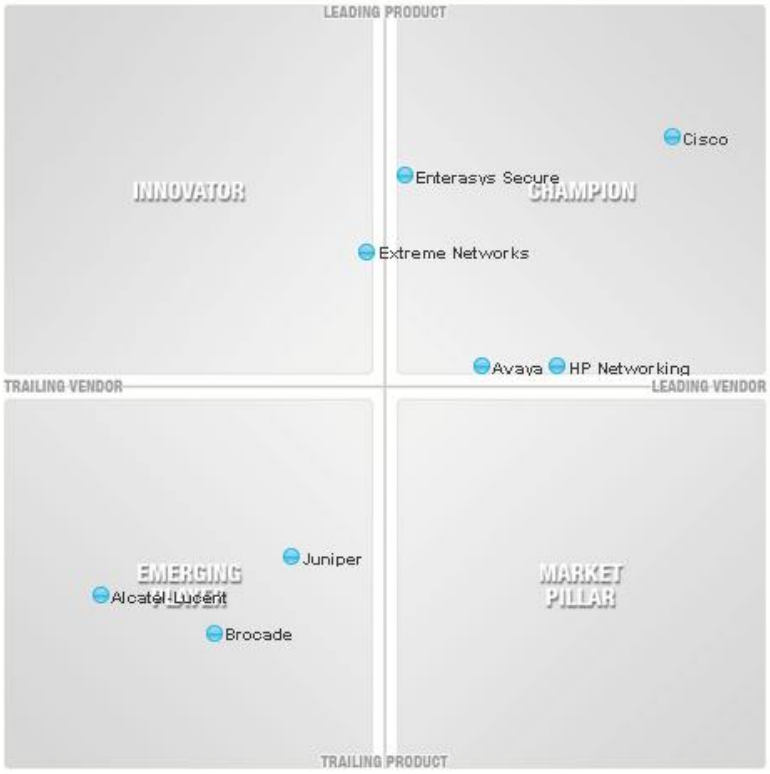

Ilustración 1 Comparativa fabricantes

Se ha valorado también el factor económico, en el sector de las redes de área local empresariales Enterasys también es una opción competitiva que ofrece las mismas o más funcionalidades y rendimientos que otros fabricantes a un precio mas reducido.

4.1 Conmutación

La solución de conmutación propuesta estará formada por un diseño a tres capas: acceso, distribución y núcleo. La capa distribución y núcleo estará formada por dos conmutadores modulares chasis S1 del fabricante Enterasys con capacidad de puertos a 10G.

Se ha elegido este equipamiento de gama alta por sus prestaciones para núcleo y distribución y poseer la tecnología VSB.

Para ello se ha estudiado la tecnología VSB (*Virtual Switch Bonding)*¸ esta tecnología del fabricante Enterasys permite que dos entidades de conmutación diferentes formen una única entidad virtual de conmutación. Esto multiplica la capacidad de la red permitiendo la utilización de todos los enlaces al no necesitar protocolos de eliminación de bucles de red. Tambien simplifica la gestión y configuración de los equipos al gestionarse con una sola dirección IP. Los dos chasis S1 estarán configurados en modo *Virtual Switch Bonding*.

Otra de las ventajas de estos los conmutadores Enterasys S1 es la capacidad de multicapa, es decir, además de ser conmutadores pueden iniciar instancias de encaminamiento por lo que no será necesario la adquisición de enrutadores adicionales. Así pues al disponer de capacidad de enrutamiento además de distribución pueden formar la capa del núcleo. Se encargarán de concentrar todos los enlaces troncales de la capa de acceso.

En esta capa de conmutación también se conectarán equipos de servicios de red: dos servidores redundantes que darán los servicios de DHCP, LDAP, RADIUS y enrutadores de proveedores de Internet.

Se utilizará la tecnología de apilamiento (*stack*) en los equipos de acceso, esta tecnología permite la agregación de varios equipos como una entidad de conmutación virtual. Enterasys permite conectar hasta ocho unidades formando una pila.

Así pues la capa de acceso estará formada por tres pilas de conmutadores B5 de Enterasys con capacidad de puertos 10/100/1000 eléctricos y 10G ópticos. Estos se configurarán como *stack*, es decir, conmutadores apilados. Se conectarán a la capa de distribución/núcleo mediante dos enlaces de 10G formando un enlace agregado de 20G. En esta capa se conectarán los usuarios finales de la red y otros dispositivos (ordenadores, impresoras, servidores de empresas, etc.).

Gracias a la funcionalidad de *stack* que permite el apilado de conmutadores en una única unidad virtual y la funcionalidad *Virtual Switch Bonding* y la agregación de enlaces la red estará libre de bucles, por lo tanto no habrá enlaces bloqueados por *Spanning-Tree* y no será necesario configurar este protocolo.

Los equipos que formen la red se repartirán en tres salas de comunicaciones repartidas en diferentes plantas del edificio.

A continuación se muestra el esquema físico de la red del edificio:

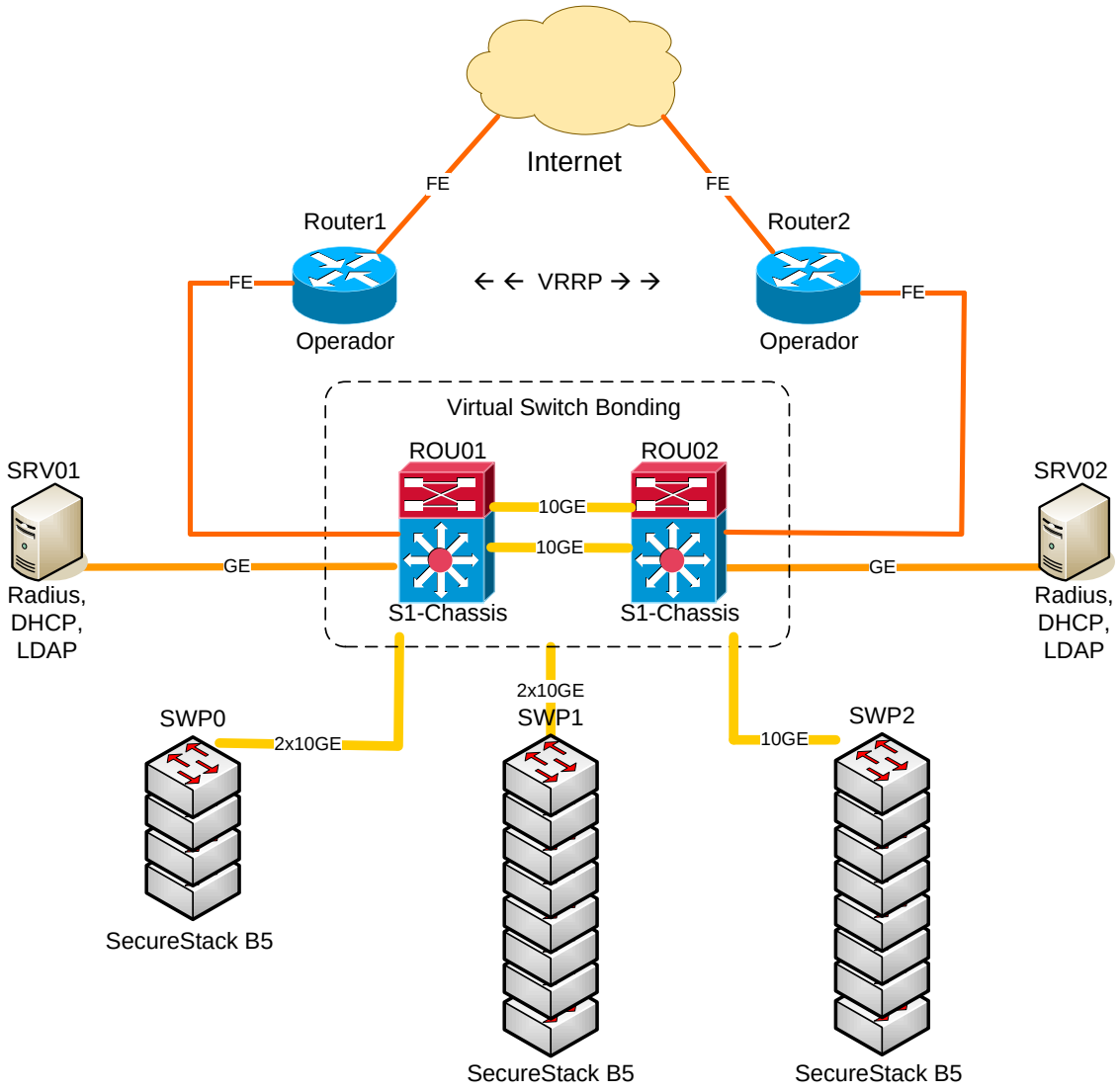

Ilustración 2 Diagrama de red del edificio

Debido a la complejidad de dar servicio en un único edificio a múltiples empresas prestando alta disponibilidad se ha elegido esta arquitectura física con dos equipos de distribución/núcleo.

Para dar mayor estabilidad a la red el diseño presenta equipos redundados; ante el posible fallo de uno de ellos la red no se vería afectada. Al igual que con los equipos se ha propuesto un diseño con enlaces redundantes. En todo momento se ha intentado reducir al máximo los costes, pero sin que esto afecte a la buena prestación del servicio.

4.2 Encaminamiento

La solución de encaminamiento propuesta estará formada por un diseño que busca la sencillez y la seguridad. Ya que se dispone de dos Enterasys S1 formando un equipo virtual con funcionalidades de encaminamiento, se propone utilizar estos equipos como puerta de enlace para todas las redes del edificio y conexión a Internet.

Para tal efecto se configurarán múltiples instancias de enrutamiento virtual (VRF). La tecnología VRF (Virtual Routing and Forwarding) permite la creación de múltiples tablas de rutas independientes dentro de un único enrutador.

En el enrutador del proyecto, se configurarán diferentes enrutadores virtuales, donde cada uno tendrá su propia tabla de rutas totalmente independiente y no compartida con los otros enrutadores virtuales en el mismo dispositivo. Esto significa que aunque todos las redes estén enrutadas por el mismo equipo, las empresas quedaran aisladas entre si al no existir ruta de una a la otra. Esto difiera de las arquitecturas de encaminamiento comunes, donde si se utiliza un solo encaminador habría que crear filtros o reglas para que una empresa no tuviera conectividad con la otra (lo que complicaría la operación y administración) o utilizar un router por cada empresa, lo que ofrecería las mismas prestaciones que la tecnología VRF pero incrementaría los costes del proyecto y el mantenimiento.

Los Enterasys S1 disponen la funcionalidad de multi-VRF por lo que se propone la creación de un enrutador virtual por cada empresa, es decir una VRF por empresa formando una instancia de encaminamiento separada y una VRF global. De esta forma no habrá conectividad entre subredes sin la necesidad de crear listas de acceso, simplificando el diseño.

En la todas las VRFs se configurará la ruta por defecto apuntando a una dirección de la VRF global (Internet) y a su vez la VRF global tendrá como ruta por defecto la ip de interconexión con los enrutadores del proveedor de servicios que proporcione acceso a Internet.

La solución propuesta utiliza los propios dispositivos de conmutación de la capa distribución/núcleo, de esta forma se ahorra en costes y simplifica el diseño al contar con menos dispositivos. Al utilizar la tecnología multi-VRF no necesitamos tener un enrutador por cada empresa para tener separadas las redes en un solo equipo y sin necesidad de configurar filtros entre redes se ofrece la misma funcionalidad.

A continuación se muestra un esquema del sistema de VRFs del enrutador:

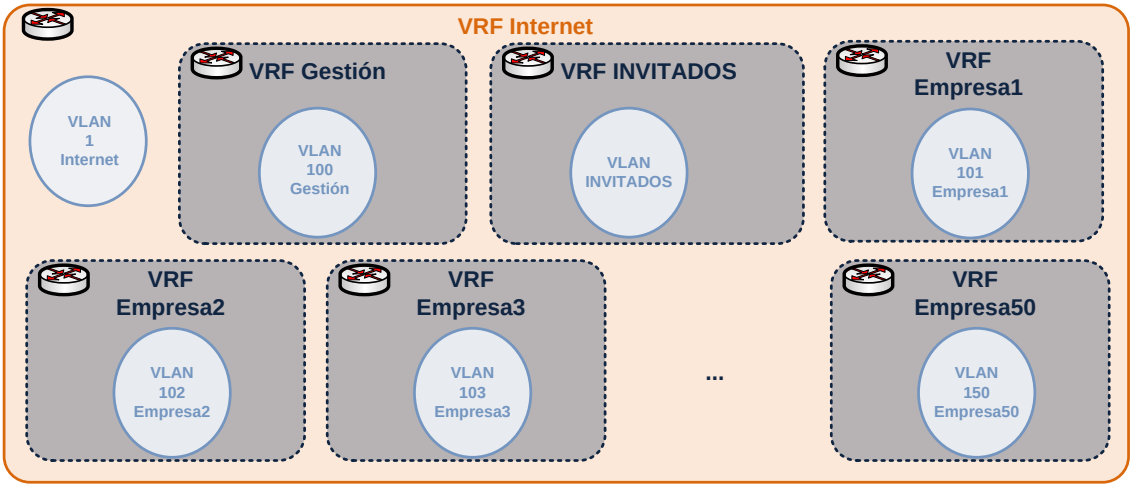

Ilustración 3 Diagrama de VRFs

4.3 Internet

Es acceso a Internet propuesto es una solución para empresas con dos líneas en dos enrutadores diferentes para ofrecer alta disponibilidad. La solución de las operadores de este tipo suelen constar de la instalación de dichos enrutadores en las instalaciones del cliente, en este caso se conectarían uno a cada S1 en la misma VLAN para el intercambio de mensajes del protocolo VRRP. De esta forma la ruta por defecto de la red seria la ip virtual que forman los dos equipos del operador.

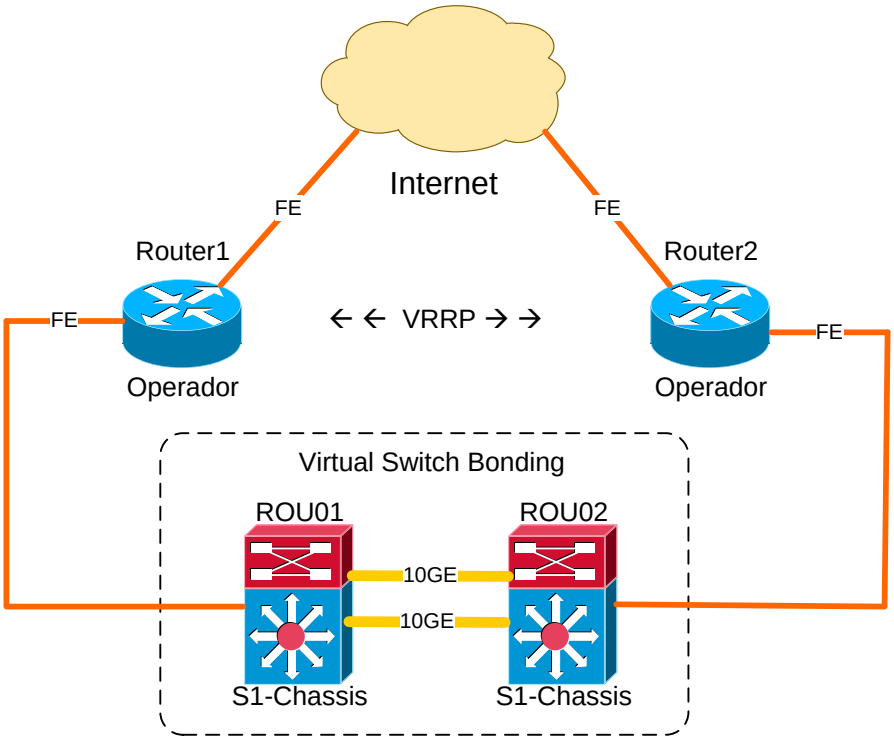

Ilustración 4 Conexión a Internet

5 ARQUITECTURA LÓGICA

En el siguiente esquema se muestra de manera gráfica la solución lógica de red propuesta para el edificio:

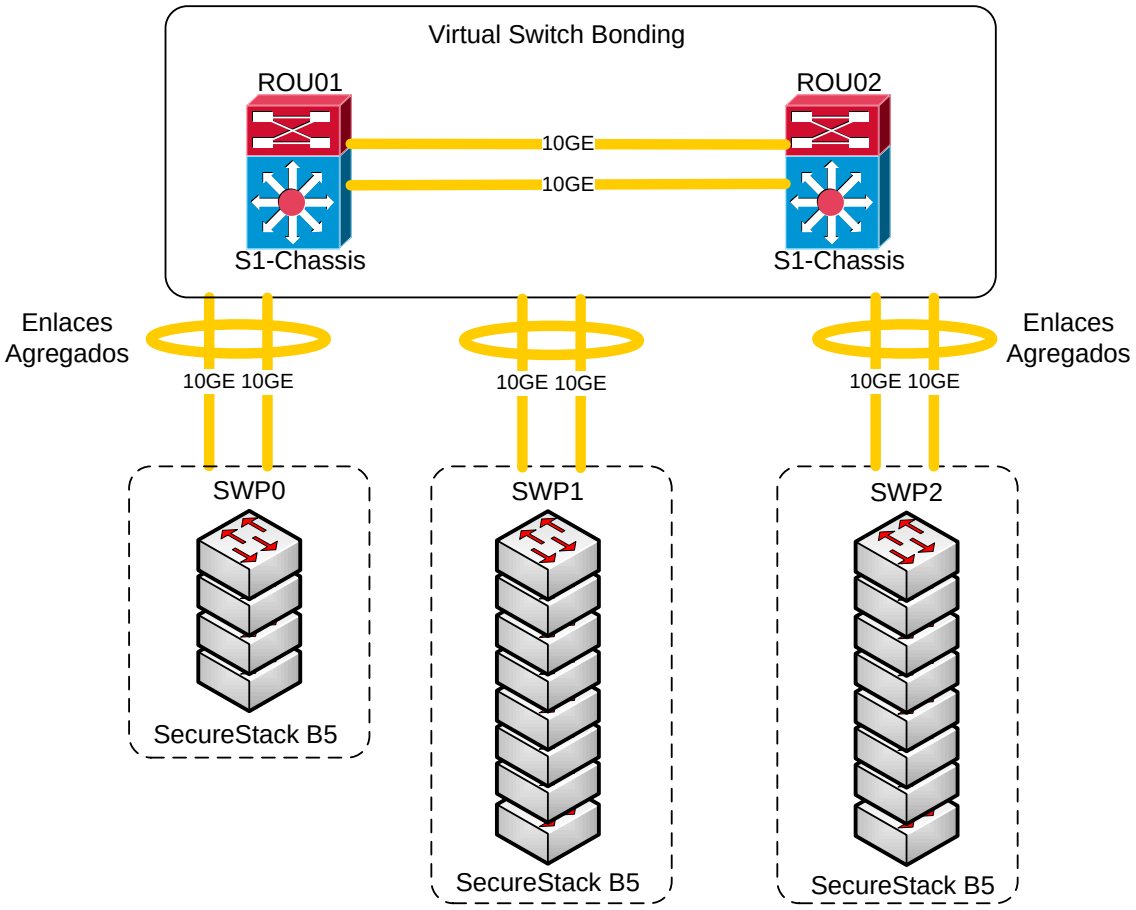

Ilustración 5 Esquema lógico

La red de área local (LAN) se dividirá en 53 entornos virtuales o VRF de acuerdo a la clasificación de empresas y servicios existentes en la red. La división quedará de la siguiente forma:

-Entorno Empresas. Englobará los usuarios corporativos de las empresas.

-Entorno Global (Internet)

-Entorno Gestion. Englobará la VLAN de gestión de la red donde estarán la electrónica de red y los servidores.

-Entorno Invitados. Red de invitados

Con esta división la electrónica de red podrá gestionar de manera independiente el tráfico de enrutamiento.

En cada entorno se configurará las puertas de enlace de las VLANs definidas y las rutas necesarias. No habrá enrutamiento entre VRF a excepción de la ruta por defecto hacia la global que proporciona acceso a Internet.

En la capa de acceso se configurará el acceso de usuarios a través de autenticación 802.1x. También se conectarán las impresoras y servidores este tipo de dispositivos si no disponen de suplicante 802.1x se autenticarán vía dirección MAC.

5.1 Plan de direccionamiento IP, VLANs y VRFs

5.1.1 Direccionamiento IP

El direccionamiento IP de la red del edificio y servicios estará dividido en dos partes:

-Empresas

-Servicios Comunes

La parte Empresas corresponderá a todos los usuarios y servicios que requieran conectividad con la red para los usuarios de las diferentes empresas.

La parte de los Servicios Comunes engloba el direccionamiento de la infraestructura y servicios de red y acceso a Internet.

Las subredes asignadas son las siguientes:

Descripción	Subred	Marcara	Puerta de Enlace	Broadcast
Gestión	192.168.100.0	255.255.255.248	192.168.100.1	192.168.100.7
Internet	192.168.1.0	255.255.255.248	192.168.1.1	192.168.1.7
Invitados	192.168.2.0	255.255.255.0	192.168.2.1	192.168.2.255
Empresa1	192.168.101.0	255.255.255.224	192.168.101.1	192.168.101.31
Empresa2	192.168.102.0	255.255.255.224	192.168.102.1	192.168.102.31
Empresa3	192.168.103.0	255.255.255.224	192.168.103.1	192.168.103.31
Empresa4	192.168.104.0	255.255.255.224	192.168.104.1	192.168.104.31
Empresa5	192.168.105.0	255.255.255.224	192.168.105.1	192.168.105.31
Empresa6	192.168.106.0	255.255.255.224	192.168.106.1	192.168.106.31
Empresa7	192.168.107.0	255.255.255.224	192.168.107.1	192.168.107.31
Empresa8	192.168.108.0	255.255.255.224	192.168.108.1	192.168.108.31
Empresa9	192.168.109.0	255.255.255.224	192.168.109.1	192.168.109.31
Empresa10	192.168.110.0	255.255.255.224	192.168.110.1	192.168.110.31
Empresa11	192.168.111.0	255.255.255.224	192.168.111.1	192.168.111.31
Empresa12	192.168.112.0	255.255.255.224	192.168.112.1	192.168.112.31
Empresa13	192.168.113.0	255.255.255.224	192.168.113.1	192.168.113.31
Empresa14	192.168.114.0	255.255.255.224	192.168.114.1	192.168.114.31
Empresa15	192.168.115.0	255.255.255.224	192.168.115.1	192.168.115.31
Empresa16	192.168.116.0	255.255.255.224	192.168.116.1	192.168.116.31
Empresa17	192.168.117.0	255.255.255.224	192.168.117.1	192.168.117.31
Empresa18	192.168.118.0	255.255.255.224	192.168.118.1	192.168.118.31

Empresa19	192.168.119.0	255.255.255.224	192.168.119.1	192.168.119.31
Empresa20	192.168.120.0	255.255.255.224	192.168.120.1	192.168.120.31
Empresa21	192.168.121.0	255.255.255.224	192.168.121.1	192.168.121.31
Empresa22	192.168.122.0	255.255.255.224	192.168.122.1	192.168.122.31
Empresa23	192.168.123.0	255.255.255.224	192.168.123.1	192.168.123.31
Empresa24	192.168.124.0	255.255.255.224	192.168.124.1	192.168.124.31
Empresa25	192.168.125.0	255.255.255.224	192.168.125.1	192.168.125.31
Empresa26	192.168.126.0	255.255.255.224	192.168.126.1	192.168.126.31
Empresa27	192.168.127.0	255.255.255.224	192.168.127.1	192.168.127.31
Empresa28	192.168.128.0	255.255.255.224	192.168.128.1	192.168.128.31
Empresa29	192.168.129.0	255.255.255.224	192.168.129.1	192.168.129.31
Empresa30	192.168.130.0	255.255.255.224	192.168.130.1	192.168.130.31
Empresa31	192.168.131.0	255.255.255.224	192.168.131.1	192.168.131.31
Empresa32	192.168.132.0	255.255.255.224	192.168.132.1	192.168.132.31
Empresa33	192.168.133.0	255.255.255.224	192.168.133.1	192.168.133.31
Empresa34	192.168.134.0	255.255.255.224	192.168.134.1	192.168.134.31
Empresa35	192.168.135.0	255.255.255.224	192.168.135.1	192.168.135.31
Empresa36	192.168.136.0	255.255.255.224	192.168.136.1	192.168.136.31
Empresa37	192.168.137.0	255.255.255.224	192.168.137.1	192.168.137.31
Empresa38	192.168.138.0	255.255.255.224	192.168.138.1	192.168.138.31
Empresa39	192.168.139.0	255.255.255.224	192.168.139.1	192.168.139.31
Empresa40	192.168.140.0	255.255.255.224	192.168.140.1	192.168.140.31
Empresa41	192.168.141.0	255.255.255.224	192.168.141.1	192.168.141.31
Empresa42	192.168.142.0	255.255.255.224	192.168.142.1	192.168.142.31
Empresa43	192.168.143.0	255.255.255.224	192.168.143.1	192.168.143.31
Empresa44	192.168.144.0	255.255.255.224	192.168.144.1	192.168.144.31
Empresa45	192.168.145.0	255.255.255.224	192.168.145.1	192.168.145.31
Empresa46	192.168.146.0	255.255.255.224	192.168.146.1	192.168.146.31
Empresa47	192.168.147.0	255.255.255.224	192.168.147.1	192.168.147.31
Empresa48	192.168.148.0	255.255.255.224	192.168.148.1	192.168.148.31
Empresa49	192.168.149.0	255.255.255.224	192.168.149.1	192.168.149.31
Empresa50	192.168.150.0	255.255.255.224	192.168.150.1	192.168.150.31

Tabla 2: Subredes

En la tabla anterior se muestra la dirección IP que se configurará en cada VLAN como puerta de enlace de la subred.

5.1.2 VLANs

La segmentación de la red en VLANs se realizará basándose en los tipos de servicios y usuarios que vayan a acoger. Los grupos de VLAN serán los siguientes:

-Gestión – Vlan ID 100

-Empresas – Vlan ID 101-150

-Internet – Vlan ID 1

-Invitados – Vlan ID 2

El plan de VLANs adecuado a la solución técnica propuesta será el siguiente:

Descripción	Identificador VLAN	Nombre VLAN
Gestion	100	Gestion
Internet	1	Internet
Invitados	2	Invitados
Empresa1	101	Empresa1
Empresa2	102	Empresa2
Empresa3	103	Empresa3
Empresa4	104	Empresa4
Empresa5	105	Empresa5
Empresa6	106	Empresa6
Empresa7	107	Empresa7
Empresa8	108	Empresa8
Empresa9	109	Empresa9
Empresa10	110	Empresa10
Empresa11	111	Empresa11
Empresa12	112	Empresa12
Empresa13	113	Empresa13
Empresa14	114	Empresa14
Empresa15	115	Empresa15
Empresa16	116	Empresa16
Empresa17	117	Empresa17
Empresa18	118	Empresa18
Empresa19	119	Empresa19
Empresa20	120	Empresa20
Empresa21	121	Empresa21
Empresa22	122	Empresa22
Empresa23	123	Empresa23
Empresa24	124	Empresa24
Empresa25	125	Empresa25
Empresa26	126	Empresa26
Empresa27	127	Empresa27
Empresa28	128	Empresa28
Empresa29	129	Empresa29
Empresa30	130	Empresa30
Empresa31	131	Empresa31
Empresa32	132	Empresa32
Empresa33	133	Empresa33
Empresa34	134	Empresa34

Empresa35	135	Empresa35
Empresa36	136	Empresa36
Empresa37	137	Empresa37
Empresa38	138	Empresa38
Empresa39	139	Empresa39
Empresa40	140	Empresa40
Empresa41	141	Empresa41
Empresa42	142	Empresa42
Empresa43	143	Empresa43
Empresa44	144	Empresa44
Empresa45	145	Empresa45
Empresa46	146	Empresa46
Empresa47	147	Empresa47
Empresa48	148	Empresa48
Empresa49	149	Empresa49
Empresa50	150	Empresa50

Tabla 3: VLANs

5.1.3 VRFs

En red de área local del edificio no se utilizará *routing* dinámico en los equipos de distribución. El *routing* se limitará a la configuración de rutas estáticas.

La LAN estará dividida lógicamente en VRFs. Cada VRF tendrá una ruta por defecto apuntando hacia el núcleo. Por lo tanto, cada VRF agrupará el tráfico de los dispositivos conectados a sus VLANs y lo encaminará a Internet de ser necesario. El resto de dispositivos de los demás VRFs tendrán como puerta de enlace la dirección IP de la interfaz VLAN configurada en el equipo de núcleo a la que pertenezcan.

Las VRFs irán asociadas a las VLAs y son las siguientes:

VRF	VLAN-ID	Subred
Gestion	100	192.168.100.0/29
Internet	1	192.168.1.0/29
Invitados	2	192.168.2.0/24
Empresa1	101	192.168.101.0/27
Empresa2	102	192.168.102.0/27
Empresa3	103	192.168.103.0/27
Empresa4	104	192.168.104.0/27
Empresa5	105	192.168.105.0/27
Empresa6	106	192.168.106.0/27
Empresa7	107	192.168.107.0/27
Empresa8	108	192.168.108.0/27
Empresa9	109	192.168.109.0/27
Empresa10	110	192.168.110.0/27

Empresa11	111	192.168.111.0/27
Empresa12	112	192.168.112.0/27
Empresa13	113	192.168.113.0/27
Empresa14	114	192.168.114.0/27
Empresa15	115	192.168.115.0/27
Empresa16	116	192.168.116.0/27
Empresa17	117	192.168.117.0/27
Empresa18	118	192.168.118.0/27
Empresa19	119	192.168.119.0/27
Empresa20	120	192.168.120.0/27
Empresa21	121	192.168.121.0/27
Empresa22	122	192.168.122.0/27
Empresa23	123	192.168.123.0/27
Empresa24	124	192.168.124.0/27
Empresa25	125	192.168.125.0/27
Empresa26	126	192.168.126.0/27
Empresa27	127	192.168.127.0/27
Empresa28	128	192.168.128.0/27
Empresa29	129	192.168.129.0/27
Empresa30	130	192.168.130.0/27
Empresa31	131	192.168.131.0/27
Empresa32	132	192.168.132.0/27
Empresa33	133	192.168.133.0/27
Empresa34	134	192.168.134.0/27
Empresa35	135	192.168.135.0/27
Empresa36	136	192.168.136.0/27
Empresa37	137	192.168.137.0/27
Empresa38	138	192.168.138.0/27
Empresa39	139	192.168.139.0/27
Empresa40	140	192.168.140.0/27
Empresa41	141	192.168.141.0/27
Empresa42	142	192.168.142.0/27
Empresa43	143	192.168.143.0/27
Empresa44	144	192.168.144.0/27
Empresa45	145	192.168.145.0/27
Empresa46	146	192.168.146.0/27
Empresa47	147	192.168.147.0/27
Empresa48	148	192.168.148.0/27
Empresa49	149	192.168.149.0/27
Empresa50	150	192.168.150.0/27

Tabla 4: VRFs

6 SERVICIOS DE RED

6.1 Identificación de equipos

Para la electrónica de red se ha elegido al fabricante Enterasys entre otras cosas que se comentan en el documento por su desarrollo en autenticación 802.1x, existen numerosos ejemplos y casos de implantaciones con este fabricante. Se han evaluado otros fabricantes como Juniper o Cisco, pero los equipos de las gamas equivalentes presentaban precios más elevados y puesto que disponen de las mismas funcionalidades se elige Enterasys como la más competente para el proyecto.

A continuación se muestra una tabla con el equipamiento de red:

Nucleo		
Equipo	**Part Number**	**Descripcion**
ROU01	S1-Chassis	Chasis S1
ROU02	S1-Chassis	Chasis S1
Planta 0		
Equipo	**Part Number**	**Descripcion**
SWP0	Stack B5	4 unidades x48 puertos RJ45
Planta 1		
Equipo	**Part Number**	**Descripcion**
SWP1	B5K125-48	8 unidades x48 puertos RJ45
Planta 2		
Equipo	**Part Number**	**Descripcion**
SWP2	B5K125-48	8 unidades x48 puertos RJ45

Tabla 5: Identificación de equipos

En el apartado "Materiales" aparece una tabla más detallada con todos los componentes necesarios para el despliegue de red, así como su precio estimado según webs del mercado.

6.2 Topología de árbol

En una red convencional se encontraría una topología de árbol y habría que utilizar algún protocolo que evitase bucles en la red. En la solución propuesta no seria necesario la utilización del protocolo *Spanning Tree*, los equipos del núcleo de la red están libres de bucles gracias a la funcionalidad *Virtual Switch Bonding*, esta tecnología permite que los dos equipos de núcleo se comporten como uno solo, es decir, tendríamos un único equipo virtual como núcleo de la red, no habría necesidad de bloquear ningún enlace para evitar bucles, aprovechando todos los puertos troncales. A esto habría que unir la agregación de enlaces para poder tener puertos de respaldo entre los equipos de núcleo y los equipos de acceso.

A continuación se muestra un esquema explicativo que muestra la base de esta tecnología:

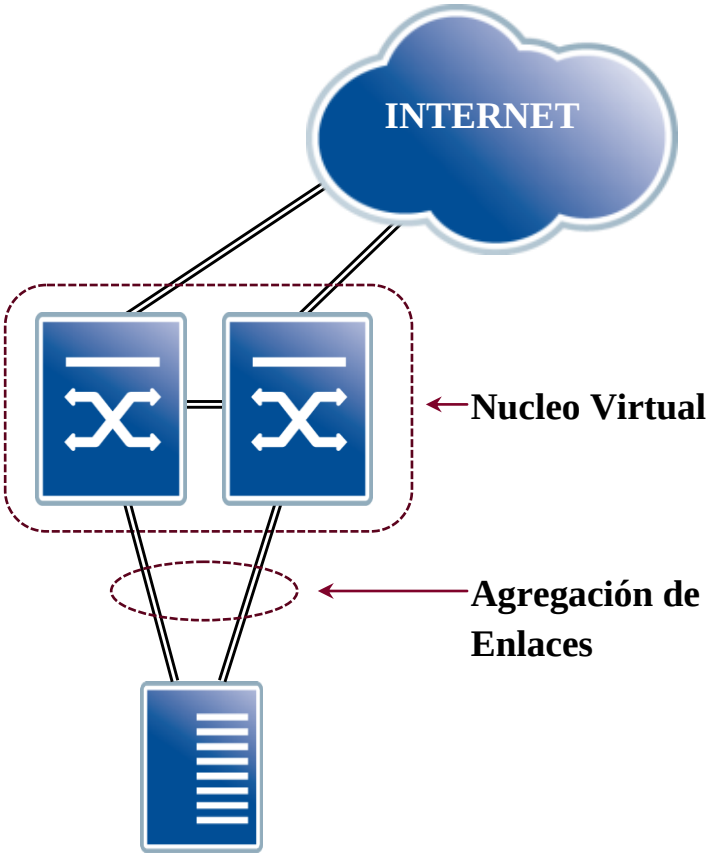

Ilustración 6 Nucleo Virtual

6.3 Configuración básica puertos en los conmutadores

Existen varios tipos de puertos en los conmutadores que se configurarán de forma diferente en función del equipo que haya conectado al otro extremo. Podemos distinguir entre:

-Puertos de acceso: puertos donde se conectan los ordenadores, impresoras, servidores, etc.

-Puertos troncales: puertos de interconexión entre dispositivos de red.

-Enlaces agregados: puertos troncales agregados funcionando como un puerto lógico.

6.3.1 Puertos de acceso

Se considera puertos de acceso a aquellos en los que se conectan:

-Usuarios.

-Otros dispositivos: impresoras, servidores, etc.

En general se considera puertos de acceso a todos los puertos donde se conecten dispositivos que requieran una única VLAN para sus comunicaciones.

Este tipo de puertos será configurado teniendo en cuenta las siguientes consideraciones:

-El puerto será configurado específicamente como acceso, deshabilitando la capacidad de negociar el modo de operación, como no es necesario configurar el protocolo *Spanning Tree*, no es necesario que se negocien los estados de dicho protocolo en cada puerto. Así pues, se configurará el mecanismo de detección y bloqueo de *Bridge Protocol Data Units*, si se detectase una BPDU en algún puerto significaría que el usuario ha conectado un conmutador. Para impedir esto se habilitará el protocolo Enterasys *Spanguard* que bloqueará los puertos por donde se reciban los paquetes de BPDU.

-Todos los puertos forzarán un proceso de autenticación para permitir el acceso a la red del dispositivo conectado. Por esto, se configurarán todos los parámetros 802.1x y de control de acceso a red identificados en el apartado específico.

-Los puertos de usuarios deben negociar dinámicamente el modo de transmisión y la velocidad por lo que se deben configurar en modo automático estos parámetros, (dúplex y velocidad).

-Los puertos de acceso de dispositivos tales como las impresoras se configurarán por defecto en modo automático aunque se deberán seguir las pautas de configuración impuestas por el fabricante del dispositivo.

-Para simplificar la administración de red se configurará la descripción del puerto indicando la roseta de la siguiente forma: ROSETA-XXX.

-Existen protocolos de conmutación que ofrecen información relevante de la configuración de los dispositivos de red. Si un usuario malintencionado capturase el trafico de red de su puerto y lo analizase podría extraer información sobre la configuración de red por lo que para estos puertos se deshabilitará cualquier protocolo de este tipo. Algún ejemplo de estos protocolos son el *Cisco Discovery Protocol*, el *Cabletron Discovery Protocol* o el *Link Layer Discovery Protocol*, estos protocolos anuncian información como el nombre del conmutador, su dirección de gestión, etc.

-Aunque con la introducción de conmutadores en lugar de concentradores ya se ha reducido el problema de las tormentas de difusión, se habilitará la protección contra dichas tormentas en estos puertos usando la funcionalidad *Broadcast Suppression* de Enterasys.

En el apartado de referencias externas se mencionan documentación que considerá algunos de estos puntos como buenas practicas al configurar una red de área local.

6.3.2 Puertos troncales

Los puertos troncales son aquellos que unen dos dispositivos de red, es decir por donde se transporta mas de una VLAN. Estos puertos se consideran puertos 802.1Q, este es el estándar que permite que un mismo medio físico transporte múltiples redes virtuales sin interferir unas con otras.

Las pautas de configuración serán las siguientes:

-La velocidad y modo de transmisión en las conexiones en fibra óptica vendrán determinadas por el SFP utilizado.

-Se configurará la descripción del puerto con los datos del dispositivo remoto y la interfaz remota "EQUIPO _ REMOTO – PUERTO _ REMOTO".

-El puerto será configurado específicamente como un enlace 802.1Q deshabilitando la capacidad de negociar el modo de operación.

-En los dos extremos del enlace 802.1Q se permitirán solo las VLAN específicas que vayan a circular por el enlace.

-Se habilitará un mecanismo de detección de enlaces unidireccionales en los enlaces de fibra óptica.

-Se habilitará la protección contra tormentas de difusión con el mismo mecanismo que los puertos de acceso (*Broadcast Suppression*).

Ha de tenerse en cuenta que estos puertos físicos de fibra óptica, serán los que formen los enlaces agregados.

6.3.3 Enlaces agregados

Los enlaces entre conmutadores serán siempre de puertos agregados, para ello se utilizara el protocolo LACP (*Link Aggregation Control Protocol*), definido en el estándar 802.ad, permite agrupar puertos de características similares en un único enlace lógico. Configurado de forma activa, permitirá a los puertos negociar la agregación. De esta forma y al no contar con puertos bloqueados se aprovecharían todos los puertos troncales de 10G de la red.

6.4 Configuración básica puertos de encaminamiento

Los equipos de núcleo al ser multicapas tienen la capacidad de conmutar y encaminar. Por lo tanto no se configurará ningún puerto como puerto exclusivo de encaminamiento, se configurará el nivel de encaminamiento de todas las redes virtuales y se asignará la VLAN correspondiente a cada puerto y el equipo internamente realizara las tareas de encaminamiento en función de las tablas de rutas.

6.5 Autenticación en red

A nivel general, los usuarios del vivero de empresas tendrán que autenticarse para poder acceder a la red. Esto quiere decir que cuando un dispositivo sea conectado a la red, desencadenará una serie de mecanismos que mediante diversos protocolos concedan el acceso a la red al dispositivo y se le asignen los recursos necesarios.

La norma IEEE 802.1X es utilizada para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1) y permitirá la autenticación de dispositivos que se conecten a los puertos de los conmutadores. Este mecanismo se realizará estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla (asignando el acceso de modo restringido). Para los conmutadores elegidos esta norma se basa en el protocolo de autenticación extensible (EAP),

Todos los puertos de red tendrán aplicadas técnicas de autenticación, a excepción de los puertos troncales y los asignados a servicios de red (Internet, Radius, DHCP, etc).

Las técnicas de autenticación que se aplicarán en la red cableada serán las siguientes:

-Autenticación 802.1X para los usuarios.

-Autenticación MAC para todos los dispositivos que no dispongan de suplicante 802.1x (por ejemplo algunas impresoras).

Cuando un usuario conecte un dispositivo a la red, el conmutador iniciará el proceso de autenticación 802.1X. En el caso de que la autenticación sea correcta, se concederá acceso de red al dispositivo. El servidor Radius validará el acceso, previa consulta con el servidor LDAP y asignará al dispositivo la VLAN correspondiente a la empresa del vivero y esto desencadenara la provisión de otra serie de recursos de red.

En el caso de que la autenticación 802.1X sea fallida, se iniciará el proceso de autenticación por MAC. El servidor LDAP, tendrá definida una lista de direcciones MAC permitidas. Tan solo los dispositivos que estén dados de alta en esa lista podrán acceder mediante este tipo de autenticación.

Finalmente si el dispositivo no logra completar ningún proceso de autenticación será aislado en la VLAN de invitados, negando el acceso a los servicios que pueda tener cada empresa del vivero y permitiendo únicamente el tráfico WEB hacia Internet.

En los siguientes puntos se detallan los diferentes tipos de autenticación y elementos necesarios que habrá en la red.

6.5.1 RADIUS

El protocolo RADIUS (*Remote Authentication Dial-In User Server*) permite la autenticación y autorización de acceso a la red.

Cuando se conecte un dispositivo a un puerto *ethernet*, el conmutador solicitará al dispositivo por medio de un *software* llamado suplicante (instalado en el dispositivo en los casos de autenticación 802.1X) las credenciales de acceso a la red o la dirección MAC (dirección física de la tarjeta de red) sin son dispositivos sin capacidad 802.1X. Esta información se transfiere desde el conmutador que toma el rol de cliente RADIUS

o NAS (Network Access Server) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.

El servidor RADIUS comprueba que la información es correcta utilizando el esquema de autenticación PEAP. Se elige PEAP ya que el sistema operativo mas extendido es Microsoft Windows y el suplicante que tiene integrado utiliza autenticación IEEE 802.1X con PEAP (EAP-MSCHAPv2), además los sistemas unix disponen de suplicante con las mismas especificaciones.

Para comprobar que las credenciales son las correctas el servidor RADIUS hará una consulta LDAP al directorio montado en el proyecto. Si las credenciales son aceptadas, el servidor autorizará el acceso a la red y le asignará al dispositivo la VLAN correspondiente a la empresa por medio de los atributos RADIUS descritos en el RFC3580.

La red dispondrá de un servicio de RADIUS estará compuesto por dos servidores, al contar con dos servidores se puede ofrecer alta disponibilidad. Se ha optado por duplicar el servicio al ser un servicio crítico y así se proponen dos servidores para dar redundancia.

Realizarán las siguientes funciones:

-Autenticación y acceso a red. Los conmutadores de planta serán sus clientes, estos lanzaran el proceso de autenticación cuando el dispositivo se conecte al puerto

-Asignación dinámica de VLAN según tipo de usuario/dispositivo.

Un ejemplo de mapeo empresa/VLAN seria: Grupo LDAP=Empresa1→VLANID=101.

Se propone la instalación del *software* libre FreeRADIUS, para ello se instalará el sistema operativo linux CentOS en cada uno de los servidores HP elegidos y sobre ellos se instalara el servicio RADIUS.

Se ha decidido utilizar FreeRADIUS al ser libre y de codigo abierto, disponer de multiples ejemplos de configuración (incluiuda alta disponibilidad) en Internet y ser compatible con el sistema operativo utilizado en los dos servidores.

Existen multitud de servidores radius en el mercado de fabricantes como Alcatel, Microsoft, Juniper, etc, pero debido a que se opta por la adquisicion de unicamente dos servidores, la forma de aprovechar los recursos existentes sin incrementar los costes es la utilizacion del servicio FreeRADIUS.

6.5.2 Autenticación 802.1X para acceso a la red

El proceso de autenticación de los dispositivos del vivero de empresas se basa en el estándar IEEE 802.1X, que hace uso de tres entidades lógicas:

-Suplicante o cliente 802.1X: es un software instalado en los terminales que desean acceder a la red (PCs de los usuarios).

-Autenticador: son los elementos intermedios entre el cliente y el servidor de autenticación. Son los conmutadores Enterasys. Estos equipos solicitan al usuario sus credenciales, para poder asignar por medio del suplicante una VLAN. Para poder enviar estas credenciales a los servidores RADIUS, los autenticadores (NAS) deben tener configuradas las direcciones IP de los dos servidores RADIUS para asegurar la alta disponibilidad de este servicio.

-Servidor de autenticación: los servidores RADIUS (FreeRADIUS) del vivero de empresas que validarán la identidad de los usuarios, consultando el directorio LDAP a que empresa corresponden.

El proceso de autenticación de un usuario final consta de los intercambios de información que se muestran en la siguiente figura:

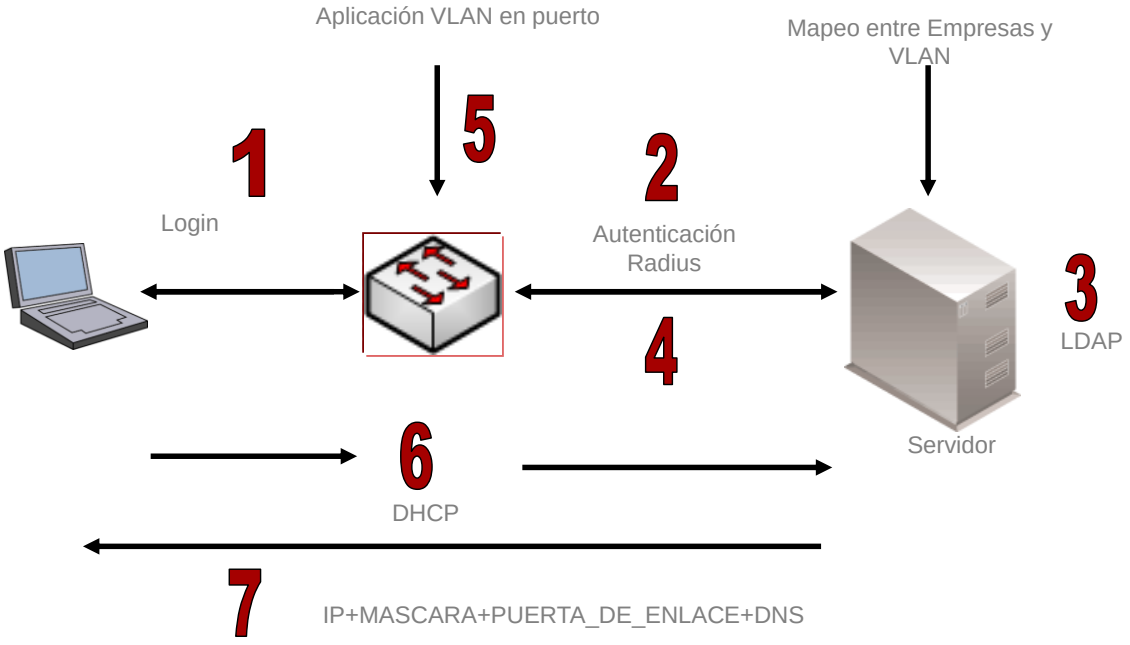

Ilustración 7 Proceso de autenticación

1. Al conectar el usuario el dispositivo a la red, el autenticador (conmutador) al que está conectado solicita autenticación al usuario. El usuario introduce el nombre de usuario asignado a su empresa y contraseña. Estos parámetros son enviados por el autenticador al servidor RADIUS.

2. El servidor RADIUS recoge usuario y contraseña y hace una consulta LDAP al directorio de empresas.

3. El servidor LDAP valida o deniega el acceso y se lo comunica al RADIUS.

4. El RADIUS comunica al autenticador (conmutador) la respuesta del LDAP. En caso de autenticación positiva, el autenticador activa el puerto de usuario

asignándolo a la VLAN correspondiente a su empresa. Aquí finaliza la autenticación 802.1X.

5. El equipo de usuario, ya en su VLAN, lo que desencadena la obtención dinámica de dirección IP, solicitando ésta por DHCP.

6. Los conmutadores al disponer de capa de encaminamiento, reenvían la petición DHCP mediante "DHCP Relay" (RFC 1541) al servidor DHCP, según la VLAN a la que se haya asignado al usuario.

7. El servidor DHCP responde con una dirección IP de la VLAN de la empresa del usuario. Además se le hace entrega de la dirección de su puerta de enlace predeterminada y las direcciones de los servidores de resolución de nombres (DNS del proveedor de acceso a Internet).

Como se ha mencionado el autenticador y el servidor de autenticación se comunican utilizando el protocolo RADIUS.

El suplicante 802.1X y el autenticador se comunican utilizando el protocolo EAP. Este protocolo establece los procedimientos necesarios para el intercambio de mensajes de autenticación, existiendo diversos métodos EAP. Como se menciona anteriormente en la red del vivero de empresas se empleará únicamente PEAP-MSCHAPv2 como método EAP.

El servidor RADIUS indica en su respuesta a los conmutadores el identificador de VLAN que le corresponde al usuario autenticado mediante los atributos especificados en la RFC3580:

-Tunnel-Type=VLAN (13)

-Tunnel-Medium-Type=802

-Tunnel-Private-Group-ID=VLANID

Se configurará en el RADIUS un mapeo que permita asignar a cada grupo del LDAP (un grupo por empresa) los atributos radius correspondientes asociados a la VLAN de la empresa.

Un ejemplo de mapeo empresa/VLAN seria: Grupo LDAP=Empresa1→VLANID=101.

6.5.3 Autenticación sin suplicante (MAC)

Todos los dispositivos que se conecten a la red del vivero, deberán autenticar contra el servidor RADIUS, el problema es que algunos dispositivos no disponen de suplicante 802.1X, por ello habrá que hacer una excepción y para todos estos la autenticación se realizará por la dirección MAC. Solo habría que hacer esta excepción a dispositivos que no dispongan de sistema operativo unix o Windows, como podrían ser las impresoras.

Para llevar a cabo la autenticación de estos dispositivos se identificarán por su dirección MAC. Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en las tarjetas de red en su momento de fabricación.

En este caso habría que crear una entrada LDAP y en lugar de utilizar el nombre de usuario se utilizaría la dirección MAC.

6.6 Otros servicios

Hasta ahora se han ido comentando los servicios de red necesarios para la provisión y concesión de acceso, en este apartado se habla mas en profundidad de estos servicios (LDAP y DHCP) así como el servicio de acceso a Internet deseado proporcionado por el operador correspondiente.

6.6.1 LDAP

Para que el manejo de los usuarios de las empresas sea más fácil y ordenado se propone la instalación de un servicio LDAP (Lightweight Directory Access Protocol) en los mismos servidores donde se instala el servicio RADIUS. LDAP es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. Es decir el directorio LDAP será la base de datos donde se almacenen los usuario y contraseñas de acceso a la red y será el RADIUS el que realice consultas a esta base de datos.

Este directorio estará compuesto por un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. Este conjunto de objetos serán las empresas y dentro de cada objeto empresa habrá varios objetos usuario.

Este seria un ejemplo de LDAP:

Grupo LDAP	Usuario
Empresa1	id-01-01
Empresa1	id-01-02
Empresa1	id-01-03
Empresa1	id-01-04
Empresa1	id-01-05
Empresa1	id-01-06
Empresa1	id-01-07
Empresa1	id-01-08
Empresa1	id-01-09
Empresa1	id-01-10
…	…
Emresa50	id-50-01
…	…

Tabla 6: Ejemplo grupo LDAP

El administrador utilizara cualquier herramienta de acceso a LDAP para cambiar las contraseñas a los usuarios periódicamente por seguridad, cuando estos las pierdan o

cuando la empresa abandone el vivero. Esta será la única tarea de administración de la red cuando esté puesta en producción.

Se propone la instalación del *software* libre OpenLDAP en modo alta disponibilidad, para ello se instalará y configurará en el sistema operativo linux CentOS de cada uno de los servidores HP y se integrará con el servicio RADIUS.

Se ha decidido utilizar OpenLDAP al ser libre y de codigo abierto, disponer de multiples ejemplos de configuración (incluiuda alta disponibilidad) en Internet y ser compatible con el sistema operativo utilizado en los dos servidores.

Existen multitud de servidores LDAP en el mercado de fabricantes como IBM, Microsoft, Novell, etc, pero debido a que se opta por la adquisicion de unicamente dos servidores, la forma de aprovechar los recursos existentes sin incrementar los costes es la utilizacion del servicio OpenLDAP.

6.6.2 DHCP

Para la gestión y concesión de los servicios de red se decide la instalación y configuración del servicio DHCP (Dynamic Host Configuration Protocol).

El protocolo DHCP permitirá a los clientes de la red obtener sus parámetros de configuración automáticamente: dirección IP, puerta de enlace y servidor de nombres. Se trata de protocolo de tipo cliente/servidor. En los servidores HP se instalarán y configurarán los servicios DHCP de CentOS, estos poseerán una lista de direcciones IP dinámicas por cada VLAN y las irán asignando a los clientes según sus peticiones. Se configurarán en modo alta disponibilidad

Un ejemplo de configuración de grupos de direccionamiento:

Grupo	Subred	Marcara	Rango	Puerta de Enlace	DNS
Empresa1	192.168.101.0	255.255.255.224	192.168.101.2-30	192.168.101.1	8.8.8.8
…	…	…	…	…	…
Empresa50	192.168.150.0	255.255.255.224	192.168.150.2-30	192.168.150.1	8.8.8.8

En todo momento los servidores llevaran el control de las direcciones IP entregadas, haciendo una relación del dispositivo que la posee y la duración del alquiler de la dirección.

Se ha decidido utilizar el DHCP nativo de CentOS en modo alta disponibilidad por ser el un servicio disponible como paquete en el sistema operativo.

Existen multitud de servidores DHCP en el mercado de fabricantes como Infoblox, Microsoft, Synologic, etc, pero debido a que se opta por la adquisicion de unicamente dos servidores, la forma de aprovechar los recursos existentes sin incrementar los costes es la utilizacion del servicio dhcpd de CentOS.

7 PRESUPUESTO

A continuación se hace un desglose de todo el material necesario en el proyecto:

Nucleo			
Equipo	**Part Number**	**Descripcion**	**Precio**
ROU01	S1-Chassis	Chasis S1	$2.637,00
ROU01	S1-Mount-kit	Kit de montaje en rack	$281,00
ROU01	S1-FAN	Ventiladores	$459,00
ROU01	SSA-AC-PS-1000W	Fuente de alimentacion	$1.179,49
ROU01	SSA-AC-PS-1000W	Fuente de alimentacion	$1.179,49
ROU01	SK5208-0808-F6	Tarjeta controladora "Fabric" x8 SFP+	$25.483,00
ROU01	SOTK2268-0212	Modulo de expansion x10 RJ45 + 2x SFP+	$4.571,00
ROU01	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
ROU01	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
ROU01	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
ROU01	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
ROU01	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
ROU02	S1-Chassis	Chasis S1	$2.637,00
ROU02	S1-Mount-kit	Kit de montaje en rack	$281,00
ROU02	S1-FAN	Ventiladores	$459,00
ROU02	SSA-AC-PS-1000W	Fuente de alimentacion	$1.179,49
ROU02	SSA-AC-PS-1000W	Fuente de alimentacion	$1.179,49
ROU02	SK5208-0808-F6	Tarjeta controladora "Fabric" x8 SFP+	$25.483,00
ROU02	SOTK2268-0212	Modulo de expansion x10 RJ45 + 2x SFP+	$4.571,00
ROU02	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
ROU02	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
ROU02	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
ROU02	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
ROU02	10GB-SR-SFPP	Puerto Multi Modo 10G	$1.118,00
Planta 0			
Equipo	**Part Number**	**Descripcion**	**Precio**
SWP0	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00
SWP0	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00
SWP0	B5G124-48	switch x48 RJ45	$3.040,00
SWP0	B5G124-48	switch x48 RJ45	$3.040,00
SWP0	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP0	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP0	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP0	STK-CAB-2M	Cable de stack 2 metros	$276,00
SWP0	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
SWP0	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
Planta 1			
Equipo	**Part Number**	**Descripcion**	**Precio**
SWP1	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00
SWP1	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00

SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	B5G124-48	switch x48 RJ45	$3.040,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP1	STK-CAB-5M	Cable de stack 5 metros	$546,00
SWP1	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
SWP1	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
Planta 2			
Equipo	**Part Number**	**Descripcion**	**Precio**
SWP2	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00
SWP2	B5K125-48	switch x48 RJ45 + 2x SFP+	$4.053,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	B5G124-48	switch x48 RJ45	$3.040,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-SHORT	Cable de stack corto	$158,00
SWP2	STK-CAB-5M	Cable de stack 5 metros	$546,00
SWP2	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
SWP2	10GB-LR-SFPP	Puerto Mono Modo 10G	$2.544,00
Servidores			
Equipo	**Part Number**	**Descripcion**	**Precio**
SRV01	647339-B21	HP ProLiant DL120 G7	$1023,00
SRV02	647339-B21	HP ProLiant DL120 G7	$1023,00
		TOTAL DOLARES	$176705,96
		TOTAL EUROS	135931,06€

Tabla 7: Materiales

A continuación se detalla los trabajos y su coste:

Servicios	Días
Dirección del proyecto	9
Análisis de requisitos	30
Diseño	25
Instalación física equipamiento	2
Configuración electrónica de red: conmutación y encaminamiento	5
Configuración Servidores: SO, Radius, LDAP, DHCP, DNS	3
Configuración autenticación mediante 802.1x	2
Pruebas	2
Documentación	13
TOTAL:	188
TOTAL SERVICIOS (HORA=35€):	25480,00€

Tabla 8: Servicios

A continuación se resume el presupuesto del proyecto:

Concepto	Precio
Materiales	135931,06€
Servicios	25480,00€
TOTAL:	**161411,06€**

Tabla 9: Presupuesto

7.1.1 Viabilidad económica del proyecto

Para la evaluación de viabilidad económica del proyecto se tienen en cuenta los siguientes indicadores:

-Inversión del proyecto= 161411.06€

-Coste de operación y mantenimiento de red anual= 60000€

Se plantea cobrar a cada empresa por el servicio de red 160€ al mes, esto incluiría el servicio de red local y el acceso a Internet. Por lo que se calcula:

Concepto	Precio
1 empresa al mes por servicios de red	160 €
1 empresa al año por servicios de red	1.920 €
50 empresas en 1 año	96.000 €

Tabla 10: Calculo ingresos anuales

Por lo que el retorno de la inversión seria:

Concepto	Coste
Inversión del proyecto	161.411,06 €
Ingresos anuales por servicios de red	96.000 €
Retorno de la inversión	**1 año y 8 meses**

Tabla 11: Retorno de la inversión

Si se tienen en cuenta otros factores como el coste de la operación y el mantenimiento estimado de la red y se quiere ver la viabilidad del proyecto a 5 años se tendría:

Inversión del proyecto	Coste 2014	C-2015	C-2016	C-2017	C-2018	Total 5 años
161.411,06 €	60.000 €	60.000 €	60.000€	60.000€	60.000€	**461.411€**
	Ingresos 2014	I-2015	I-2016	I-2017	I-2018	Total 5 años
	96.000 €	96.000€	96.000€	96.000€	96.000€	**480.000€**
	Balance 2014	B-2015	B-2016	B-2017	B-2018	
Inversión+Coste-Ingresos	-125.411€	-89.411€	-53.411€	-17.411€	**18.588€**	

Tabla 12: Viabilidad a 5 años

8 CONCLUSIONES

En el trabajo de fin de carrera se plantea el diseño de red para un vivero de empresas público. El objetivo es diseñar una red profesional, robusta, segura y con un coste mínimo de operación.

Se ha querido plantear como ofrecer a pequeños emprendedores una red de la altura de una gran empresa a un coste adecuado. En estos momentos toda empresa debe contar con una red que permita interconectar a sus empleados o sus dispositivos de forma segura.

Se ha diseñado la red de forma teórica, especificando protocolos, tecnologías y servicios, eligiendo a Enterasys como fabricante de la electrónica de red por los casos de éxito publicados, información sobre redes dinámicas y precios competitivos con otros fabricantes de la misma gama de equipos.

Para los servicios se ha estudiado entre diferentes *software* y se ha visto que existen soluciones profesionales gratuitas y libres, no todo en una solución profesional tiene porque incrementar costes de materiales.

Se ha visto que la solución teórica propuesta puede llegar a ser viable, no se pretende sacar unos beneficios elevados, sino dar un servicio desde una administración pública a emprendedores y que este servicio no sea deficitario.

En resumen, se ha aprendido a evaluar entre fabricantes de electrónica de red, software de pago y libre, se han comparado tecnologías, servicios de red y los concentos podrán ser utilizados en un futuro ámbito laboral.

9 ANEXOS.

9.1 Anexo I. Planificación del trabajo

En este anexo aparecen detalladas todas las tareas con su duración, su fecha de inicio y fecha de fin. Se han tomado como hitos referenciales las entregas marcadas por la asignatura.

Nombre de tarea	Duración	Comienzo	Fin
Diseño de una red dinámica: Vivero de Empresas	**77 días**	**vie 01/03/13**	**lun 17/06/13**
PEC 1: Entrega de la planificación del trabajo	**9 días**	**vie 01/03/13**	**mié 13/03/13**
Investigación del diseño de redes de empresas	2 días	vie 01/03/13	lun 04/03/13
Elección del tipo de red para el proyecto	1 día	mar 05/03/13	mar 05/03/13
Comunicación al consultor: título, objetivos y resumen	1 día	mié 06/03/13	mié 06/03/13
Creación documento base del proyecto	5 días	jue 07/03/13	mié 13/03/13
PAC 2 : Primera entrega del proyecto	**30 días**	**jue 14/03/13**	**mié 24/04/13**
Recopilación de requisitos	10 días	jue 14/03/13	mié 27/03/13
Identificación de elementos necesarios	2 días	jue 28/03/13	vie 29/03/13
Investigación de tecnologías a emplear	3 días	lun 01/04/13	mié 03/04/13
Identificar necesidades reales	5 días	jue 04/04/13	mié 10/04/13
Boceto de diseño	5 días	jue 11/04/13	mié 17/04/13
Documentación Primera entrega	5 días	jue 18/04/13	mié 24/04/13
PAC 3 : Segunda entrega del proyecto	**25 días**	**jue 25/04/13**	**mié 29/05/13**
Diseño Conmutación	4 días	jue 25/04/13	mar 30/04/13
Diseño Enrutamiento	3 días	mié 01/05/13	vie 03/05/13
Diseño Autenticación	8 días	lun 06/05/13	mié 15/05/13
Integración infraestructura	5 días	jue 16/05/13	mié 22/05/13
Maquetación documentación	5 días	jue 23/05/13	mié 29/05/13
Entrega de la memoria final	**13 días**	**jue 30/05/13**	**lun 17/06/13**
Revisión documentación	4 días	jue 30/05/13	mar 04/06/13
Conclusiones	4 días	mié 05/06/13	lun 10/06/13
Memoria final	5 días	mar 11/06/13	lun 17/06/13

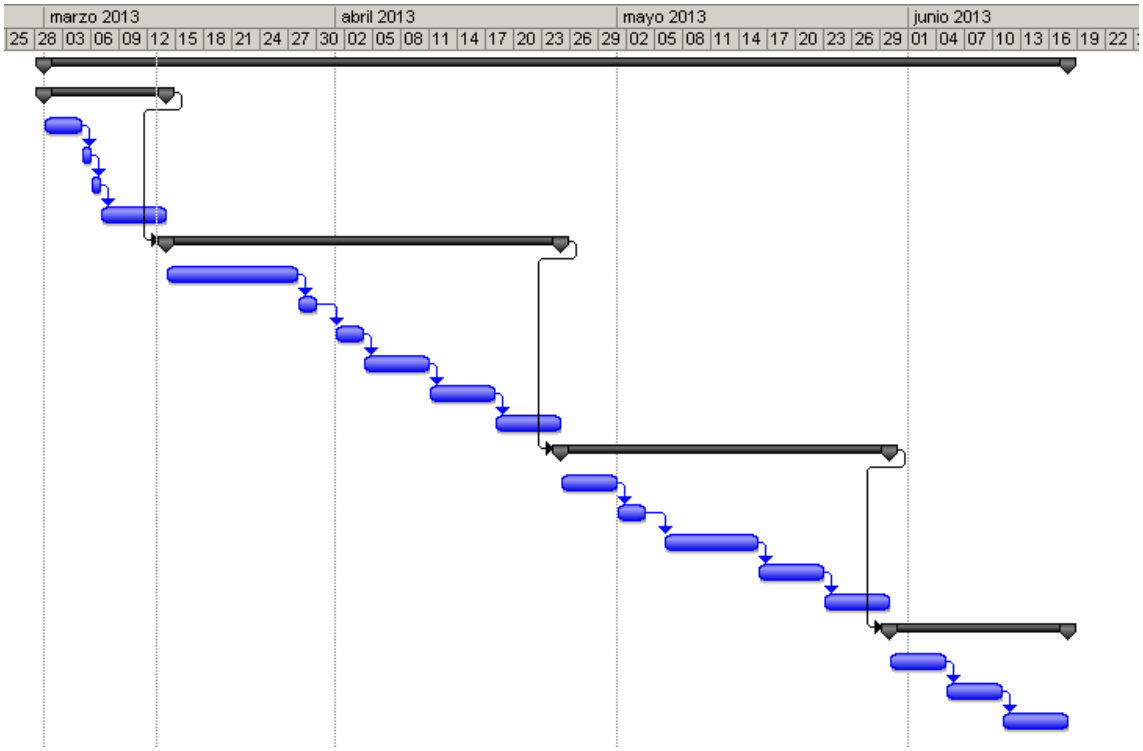

Ilustración 8 Diagrama de Gantt

9.2 Anexo II. Glosario

VLAN: Red de Área Local Virtual.

VRF: Enrutador Virtual y de reenvío

VM: Maquina virtual

DHCP: Protocolo de configuración dinámica de *host*

LDAP: Protocolo Ligero de Acceso a Directorios

RADIUS: Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP

NAS: Servidor de Acceso a la Red

LACP: Protocolo de control de agregación de enlaces

VRRP: Protocolo de redundancia de enrutadores virtuales

MAC: Dirección de control de acceso al medio

LAN: Red de area local

BPDU: Paquetes de control de bucles de red

EAP: Protocolo de autenticación extensible

PEAP: Protocolo de autenticación extensible protegido

PPP: Protocolo punto a punto

DNS: Sistema de nombres de dominio

9.3 Anexo III. Enlaces documentación utilizada

Conmutación:

GET IEEE 802®: LOCAL AND METROPOLITAN AREA NETWORK STANDARDS http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

Conceptos de diseño Enterasys:

Data Center Networking – Connectivity and Topology Design Guide
http://www.enterasys.com/company/literature/datacenter-design-guide-wp.pdf

Integrating Physical and Virtual Networking:
http://www.enterasys.com/company/literature/integrating_phy_virt_net-tsbrief.pdf

Conmutador virtual:

Enterasys Virtual Switch Bonding:
http://www.enterasys.com/company/literature/datacenter-fabric-tsb.pdf

Equipos S-Series:

Datasheet: http://www.enterasys.com/company/literature/s-ds.pdf

DHCP:

RFC2131: http://tools.ietf.org/html/rfc2131

LDAP:

http://tools.ietf.org/html/rfc4511

802.1x:

http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

Eliminación Spanning-Tree:

http://www.networkworld.com/community/node/38338

Apilación de conmutadores en uno virtual (stack):

http://www.enterasys.com/products/security-enabled-infrastructure/securestack-bseries.aspx

Protocolos de descubrimientos de vecinos:

http://redesciscoccna2.blogspot.com.es/2008/01/cisco-dicovery-protocol-cdp.html

http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.pdf

Seguridad ante tormentas de difusión:

http://sobek.su/Docs/univercd/cc/td/doc/product/lan/cat6000/ios127xe/config/bcastsup.htm

802.1Q conmutación con redes virtuales:

http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf

802.1ad Agregación de enlaces:

http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf

RFC3580 asignación dinámica de VLAN:

http://tools.ietf.org/html/rfc3580

RFC1541 asignación dinámica de IP:

http://tools.ietf.org/html/rfc1541

Sistema operativo CentOS:

http://www.centos.org/modules/tinycontent/index.php?id=3

10 ÍNDICE DE ILUSTRACIONES

Ilustración 1 Comparativa fabricantes 7

Ilustración 2 Diagrama de red del edificio 9

Ilustración 3 Diagrama de VRFs 11

Ilustración 4 Conexión a Internet 11

Ilustración 5 Esquema lógico 12

Ilustración 6 Nucleo Virtual 19

Ilustración 7 Proceso de autenticación 24

Ilustración 8 Diagrama de Gantt 34

11 ÍNDICE DE TABLAS

Tabla 1: Resumen de puertos 6
Tabla 2: Subredes 14
Tabla 3: VLANs 16
Tabla 4: VRFs 17
Tabla 5: Identificación de equipos 18
Tabla 6: Ejemplo grupo LDAP 26
Tabla 7: Materiales 29
Tabla 8: Servicios 30
Tabla 9: Presupuesto 30
Tabla 10: Calculo ingresos anuales 30
Tabla 11: Retorno de la inversión 31
Tabla 12: Viabilidad a 5 años 31