UNIVERSIDAD DE ALCALÁ

Escuela Politécnica Superior

Grado en Ingeniería Telemática

Trabajo Fin de Grado

Infraestructuras de comunicaciones para interconexión de sede remota en red mallada

David del Rey Buitrago

Director: José Javier Martínez Herraiz

TRIBUNAL:
Presidente:

Vocal 1º:

Vocal 2º:

CALIFICACIÓN: .....
FECHA: .....

Índice

Índice de Figuras

Resumen

Este trabajo fin de grado pretende dar una visión completa, tanto teórica como práctica, de las distintas tareas a realizar para la dotación de un sistema de comunicaciones completo a cualquier edificio, sede, oficina que demande tales servicios.

Por sistema de comunicaciones completo nos referimos a todo lo relacionado con:

- Subsistema de cableado estructurado: Hace referencia al aspecto físico del sistema de comunicaciones.
- Subsistema de acceso: Hace referencia al componente/s que nos permite comunicar internamente dentro del edificio todos los dispositivos conectados al sistema de comunicaciones
- Subsistema de enrutamiento: Hace referencia al componente/s que nos permiten comunicar el edificio con el resto de edificios/sedes de nuestra organización.

Abstract

This project try to provide a complete view, both theoretical and practical, of the different tasks to perform for the provision of a complete communications system to any building, home, office that requires such services.

For complete communications system we mean everything related to:

- Structured cabling subsystem: Refers to the physical aspect of the communication system.

- Subsystem Access: Refers to the components which allows us to communicate internally within the building all the devices connected to the communications system

- Subsystem Routing: Refers to the components that allow us to communicate the building with other buildings or locations of our organization.

Palabras Clave

Comunicaciones, cableado estructurado, switches, routers, ToIP, NAC.

Motivación

Mediante la lectura de este trabajo se pretende dotar al lector, no solo de los conceptos teóricos básicos para abordar el diseño y configuración de un sistema de comunicaciones completo, sino de las nociones prácticas mínimas para poder llevarlo a cabo con equipamiento real de mercado, abarcando desde el diseño del sistema hasta la monitorización del mismo.

Resumen Extendido

El objetivo principal del trabajo consiste en proporcionar los conocimientos y las herramientas adecuadas para poder abordar la dotación de las infraestructuras y equipamientos básicos para la creación del sistema de comunicaciones a una nueva sede. Para conseguir este objetivo el trabajo está divido en 3 grandes bloques, cada uno de los cuales abarca un subsistema distinto, los cuales tienen una estructura similar:

1. Acercamiento teórico: normativa que aplica, técnicas y tendencias de diseño

2. Aplicación práctica: ejemplos de implementación real, referencias a distintos fabricantes, scripts de configuración…

3. Herramientas: mostrar las distintas herramientas que ayudan a la definición, configuración, gestión de cada uno de las partes del diseño del sistema de infraestructura de comunicaciones.

El principal resultado de este trabajo será una memoria donde queden plasmados todos los condicionantes a tener en cuenta a la hora de diseñar, acometer y gestionar una infraestructura de comunicaciones. La memoria estará dividida en 3 grandes subsistemas, en analogía a las capas/protocolos del modelo TCP/IP, estos son:

- Subsistema de cableado estructurado: Hace referencia al aspecto físico del sistema de comunicaciones. → Capa física y elementos pasivos del sistema de comunicaciones

- Subsistema de acceso: Hace referencia al componente/s que nos permite comunicar internamente dentro del edificio todos los dispositivos conectados al sistema de comunicaciones → Capa de enlace de datos [subcapa MAC]

- Subsistema de enrutamiento: Hace referencia al componente/s que nos permiten comunicar el edificio con el resto de edificios/sedes de nuestra organización. → Capa de Red o Internet [IP]

Cada uno de estos subsistemas se abordarán a lo largo del proyecto desde un enfoque teórico, que defina una serie de conceptos básicos a tener en cuenta, pero también desde en enfoque eminentemente práctico, incluyendo esquemas de configuración básica de los distintos agentes que forman parte del sistema de comunicaciones.

Además el trabajo incluirá las referencias básicas a los principales fabricantes de elementos de comunicación y a algunas herramientas que nos permitan realizar la definición y posterior gestión de nuestro sistema.

Se utilizará una metodología propia de los proyectos de infraestructura, muy ligados a las distintas capas que componen la torre de protocolos. Para ello se divide el proyecto en 3 grandes subproyectos: Infraestructura física, Nivel de Acceso, Nivel enrutado. Para cada uno de los 3 subproyectos se seguirá la misma metodología:

Acercamiento teórico a la realidad a tener en cuenta para el diseño del nivel en concreto.

Implementación/Configuración física

Herramientas de apoyo.

De esta forma conseguiremos abordar los objetivos del proyecto, de una forma más progresiva, pudiendo incluso solapar trabajos de uno y otro subproyecto.

1. Memoria del Trabajo Fin de Grado

1.1. Introducción

En el escenario actual de comunicaciones globales se hace necesario que cualquier nueva sede, edificio, oficina, tenga que disponer de un sistema de comunicaciones, tanto para las comunicaciones internas dentro del edificio [comunicación de unos ordenadores con otros, acceso servicios de impresión en red, servicios de videocolaboración entre empleados del edificio, acceso aplicaciones internas], como para las comunicaciones de ese edificio con el mundo exterior [comunicación dentro de un campus cerrado, comunicación con el resto de oficinas de la organización a la que pertenece, comunicación con el mundo].

Es por ello que, en paralelo a la apertura de una sede nueva haya que pensar en la realización de una serie de tareas que permitan la comunicación de los empleados de la misma con el resto del mundo.

En el ámbito académico es muy frecuente hablar de la torre de protocolos OSI, para referirnos a como se establecen los distintos niveles y los protocolos que deben de regir toda comunicación entre dos dispositivos a través de una red de comunicaciones. Los niveles de la torre OSI son 7.

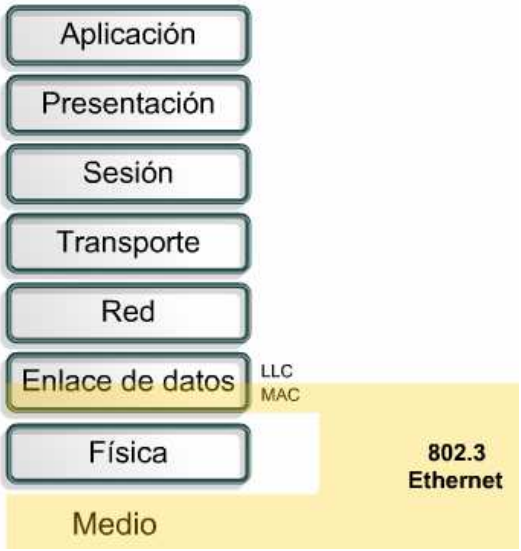


Figura 1 – Torre OSI

La experiencia nos indica que el estándar final que ha adoptado la industria es el protocolo TCP/IP, que básicamente soporta la torre de comunicaciones con 4 niveles. La relación entre ambos modelos se observa en la Figura 2.

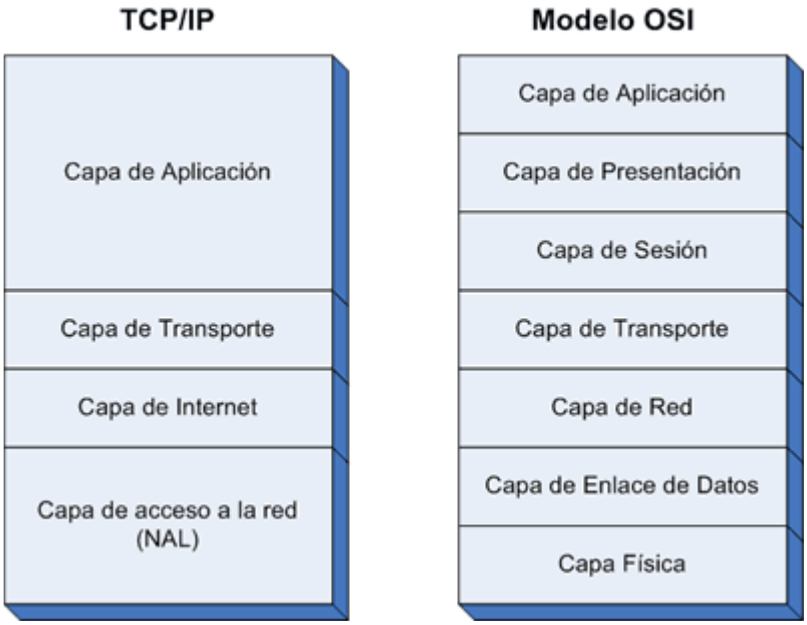


Figura 2 – Relación OSI – TCP/IP

Básicamente, y en lo que respecto a la organización de este trabajo, vamos a ver como se aborda el diseño y la configuración de cada una de las capas, hasta la capa de red (modelo OSI) o capa de Internet [IP] (modelo TCP/IP). Los trabajos de las capas superiores en el modelo TCP/IP son realizadas principalmente por la propia tarjeta de red del dispositivo que se conecta a la red y por la propia aplicación que necesita comunicarse.

Así pues, por hacer una analogía de los distintos subsistemas que se analizan en este trabajo, tendremos que:

- Subsistema de cableado estructurado: Hace referencia al aspecto físico del sistema de comunicaciones. → Capa física y elementos pasivos del sistema de comunicaciones
- Subsistema de acceso: Hace referencia al componente/s que nos permite comunicar internamente dentro del edificio todos los dispositivos conectados al sistema de comunicaciones → Capa de enlace de datos [subcapa MAC]
- Subsistema de enrutamiento: Hace referencia al componente/s que nos permiten comunicar el edificio con el resto de edificios/sedes de nuestra organización. → Capa de Red o Internet [IP]

Cada uno de estos subsistemas se abordarán a lo largo del proyecto desde un enfoque teórico, que defina una serie de conceptos básicos a tener en cuenta, pero también desde en enfoque eminentemente práctico, incluyendo esquemas de

configuración básica de los distintos agentes que forman parte del sistema de comunicaciones.

1.2. Infraestructura de Cableado Estructurado

Un sistema de cableado estructurado es la infraestructura de cable destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor.

Un sistema de cableado estructurado es físicamente una red de cable única y completa, con combinaciones de cables de cobre (pares trenzados), cables de fibra óptica, bloques de conexión, cables terminados en diferentes tipos de conectores y adaptadores.

El beneficio más directo del cableado estructurado es que permite la administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos, aportando además la garantía de transmitir un amplio espectro de señales eléctricas que dan cobertura a casi cualquier necesidad de comunicación entre un origen y un destino dentro del ámbito de cobertura del cableado estructurado, es decir, soporta una amplia gama de productos de telecomunicaciones sin necesidad de ser modificado.

Utilizando este concepto, resulta posible diseñar el cableado de un edificio con un conocimiento muy escaso de los productos de telecomunicaciones que luego se utilizarán sobre él.

La norma garantiza que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años, esta afirmación puede parecer excesiva, pero si se tiene en cuenta que entre los autores de la norma están precisamente los fabricantes de estas aplicaciones, la credibilidad a tal afirmación debe ser completa.

Un sistema de cableado estructurado puede soportar los siguientes sistemas:

1. **Sistemas de Voz.**
    a. Centralitas (PABX), distribuidores de llamadas (ACD)
    b. Teléfonos analógicos, digitales, Telefonía sobre IP (ToIP), etc.

2. **Sistemas Telemáticos.**
    a. Redes locales.
    b. Conmutadores de datos.
    c. Controladores de terminales.
    d. Líneas de comunicación con el exterior, etc.

3. **Sistemas de Control.**
    a. Alimentación remota de terminales.
    b. Calefacción, ventilación, aire acondicionado, alumbrado, etc.
    c. Protección de incendios e inundaciones, sistema eléctrico, ascensores
    d. Alarmas de intrusión, control de acceso, vigilancia, etc.

En definitiva, un sistema de cableado estructurado se caracteriza por ser:

- Fiable.
- Flexible.
- Modular.
- Sencillo de administrar.
- Integrador, de sistemas de voz, telemáticos y de control.

1.2.1. Normativa

Los estándares de cableado actualmente vigentes son:

- Estándar americano: **ANSI/EIA/TIA-568-B**. Es el más extendido, sustituye al ANSI/EIA/TIA-568-A que quedó obsoleto con 2001

- Estándar europeo/mundial: **ISO/IEC 11802**

Son sustancialmente iguales. Las diferencias son menores en cuanto a terminología, tipología de cables aprobados y especificación entre categorías de cableado (EIA/TIA-586 habla de categoría mientras que ISO/IEC 11802 habla de clase).

Se va a realizar un resumen de la normativa ANSI/EIA-568B, que nos dará una muy buena visión de que partes componen un sistema de cableado estructurado y que aspectos de interés son necesarios tener en cuenta en el diseño del mismo.

En primer lugar, la normativa define un Sistema de Cableado Estructurado como un Sistema de Cableado diseñado en una jerarquía lógica que adapta todo el cableado existente, y el futuro, en un único sistema. Un sistema de cableado estructurado exige una topología en estrella, que permite una administración sencilla y una capacidad de crecimiento flexible.

Entre las características generales de un sistema de cableado estructurado destacan las siguientes:

- La configuración de nuevos puestos se realiza hacia el exterior desde un nodo central, sin necesidad de variar el resto de los puestos. Sólo se configuran las conexiones del enlace particular.

- La localización y corrección de averías se simplifica ya que los problemas se pueden detectar a nivel centralizado.

- Mediante una topología física en estrella se hace posible configurar distintas topologías lógicas tanto en bus como en anillo, simplemente reconfigurando centralizadamente las conexiones.

Una solución de cableado estructurado se divide en una serie de subsistemas.

Cada subsistema tiene una variedad de cables y productos diseñados para proporcionar una solución adecuada para cada caso. Los distintos elementos que lo componen son los siguientes:

- Repartidor de Campus. (CD; Campus Distributor)
- Cable de distribución (Backbone) de Campus.
- Repartidor Principal o del Edificio. (BD; Building Distributor)
- Cable de distribución (Backbone) de Edificio.
- Subrepartidor de Planta. (FD; Floor Distributor)
- Cable Horizontal.
- Punto de Transición opcional. (TP; Transition Point)
- Toma ofimática. (TO)
- Punto de acceso o conexión.

La siguiente figura muestra una distribución típica de los distintos elementos.

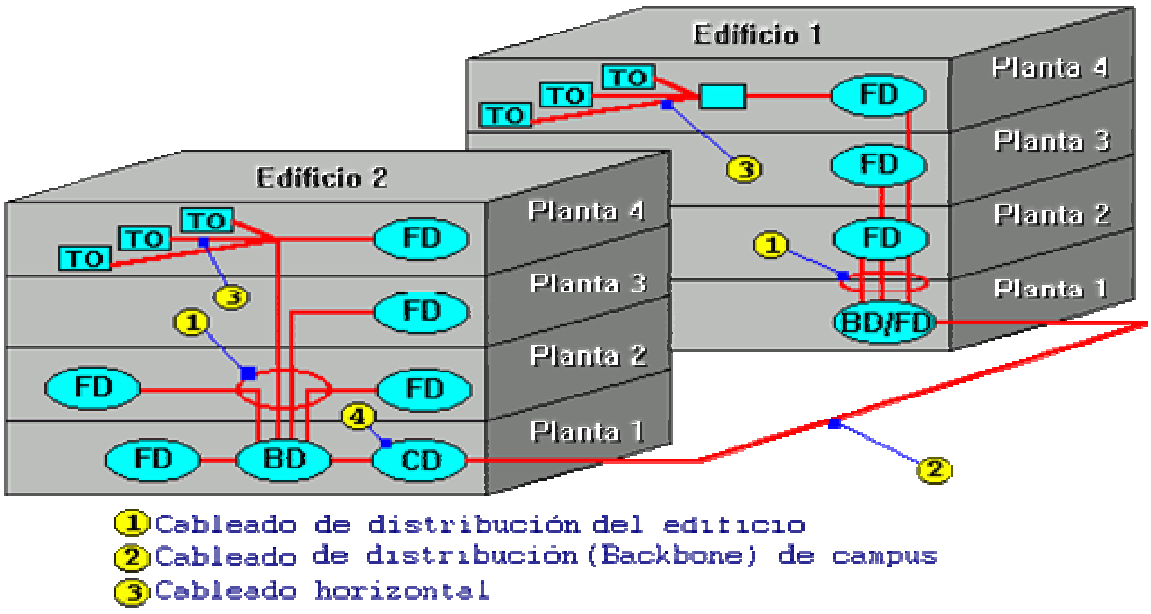


Figura 3 – Subsistemas de un Sistema de Cableado

Un sistema de cableado estructurado se puede dividir en cuatro Subsistemas básicos.

- Subsistema de Administración.
- Subsistema de Distribución de Campus.
- Subsistema Distribución de Edificio.
- Subsistema de Cableado Horizontal.

Los tres últimos subsistemas están formados por:

- Medio de transmisión.
- Terminación mecánica del medio de transmisión, regletas, paneles o tomas.
- Cables de interconexión o cables puente.

Los dos subsistemas de distribución y el de cableado horizontal se interconectan mediante cables de interconexión y puentes de forma que el sistema de cableado pueda soportar diferentes topologías como bus, estrella y anillo, realizándose estas configuraciones a nivel de subrepartidor de cada planta.

Los repartidores conectados juntos forman una estructura jerárquica tal como se muestra en la siguiente figura.

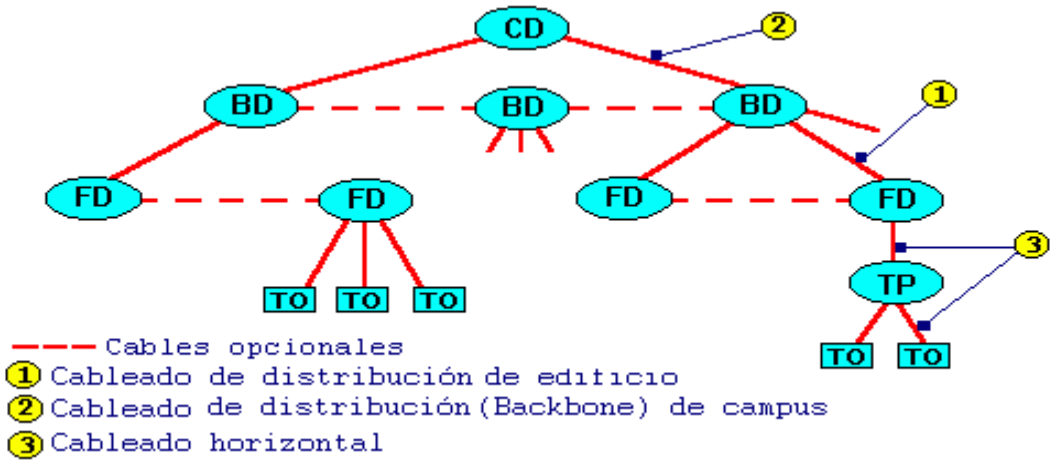


Figura 4 – Estructura Jerárquica Sistema Cableado Estructurado

Esta forma jerárquica proporciona al sistema de cableado de un alto grado de flexibilidad necesario para acomodar una variedad de aplicaciones, configurando las diferentes topologías por la interconexión de los cables puentes y los equipos terminales.

El repartidor de Campus se conecta a los repartidores de edificio asociados a través del cable de distribución del campus o backbone de campus.

El repartidor de edificio se conecta a sus subrepartidores vía el cable de distribución del edificio o backbone de edificio

A continuación se describirán cada uno de los cuatro subsistemas antes mencionados.

Subsistema de Administración

Incluye todos los cuartos de distribución donde se establece una transición en el cableado, mediante el uso de terminadores mecánicos del medio de transmisión, regletas o paneles.

Podemos distinguir dos tipos de cuartos de distribución:

1. **Cuarto de Entrada de Servicios**. Consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto ó espacio de entrada. El cuarto de entrada puede incorporar el backbone que conecta a otros edificios en situaciones de campus.
2. **Cuarto de Telecomunicaciones**. Consiste en el área de un edificio utilizado para el uso exclusivo de equipamiento asociado con el sistema de cableado de telecomunicaciones. Su función principal es la interconexión entre el cableado de distribución horizontal con el cableado de distribución de edificio y los equipos de telecomunicación.

Los elementos incluidos en este subsistema son entre otros:

- Armarios repartidores.
- Equipos de comunicaciones.
- Sistemas de Alimentación Interrumpida (SAI/UPS).
- Cuadros de alimentación.
- Tomas de tierra.

Armarios Repartidores

Los armarios repartidores de planta (FD) deberán situarse, siempre que haya espacio disponible, lo más cerca posible de la(s) vertical(es).

En la instalación de los repartidores de edificio (BD) y de campus (CD) debe considerarse también su proximidad a los cuadros de acometida de los cables exteriores.

En el caso de instalarse equipos de comunicaciones será necesario instalar una acometida eléctrica y la ventilación adecuada.

Los repartidores de planta (FD) deberán estar distribuidos de manera que se minimicen las distancias que los separan de las rosetas, a la vez que se reduzca el número de ellos necesarios.

Equipos de Comunicaciones

Los cuartos de distribución contendrán todos los equipos de comunicaciones asociados al cableado estructurado con el fin de facilitar la administración, gestión y control de los mismos.

Los equipos de comunicaciones más comunes son los asociados a la voz, Centralita y a los datos de área local, concentradores o switches y routers, pero pueden incorporarse otros dispositivos asociados al control ambiental, a la seguridad, al audio, televisión, alarmas y sonido. De hecho telecomunicaciones incorpora todos los sistemas de bajo voltaje que transportan información en los edificios.

El tratamiento del diseño de esta capa de equipos de comunicaciones, así su interconexión, serán tratados en el capítulo 2.3 de este proyecto

Sistemas de Alimentación Interrumpida

Los cuartos de distribución que contengan equipamiento electrónico, deberán estar provistos de un sistema de alimentación ininterrumpida independiente o general para todo el edificio con el fin de evitar pérdidas de información o de disponibilidad ante caídas transitorias de corriente.

Para el cálculo de potencia a dimensionar del sistema SAI se debe computar el consumo de cada uno de los equipos electrónicos a proteger incrementando dicho resultado en un 30%.

Cuadros de Alimentación

Los cuartos técnicos deberán estar dotados de un sistema de alimentación eléctrica independiente con diferencial para protección.

El estándar establece que debe haber un mínimo de tres tomas de corriente de 220V de C.A. con óptima toma de tierra y deben ser circuitos separados de 15 a 20 amperios con protección por magneto-térmico.

Tomas de Tierra

La toma de tierra es imprescindible para el buen funcionamiento de la red y la protección de los equipos asociados.

El cable de toma de tierra será conducida por el camino más corto posible hasta el pozo de tierra, debiendo ser la impedancia del conjunto inferior a 5 ohmios.

El sistema de tierra deberá estar unido a la tierra del edificio en solo un punto, con la tensión Tierra-Neutro siempre inferior a 1,5 V.

Dicha toma será la tierra general de la instalación eléctrica, para efectuar las conexiones de todo el equipamiento electrónico según las especificaciones de ANSI/TIA/EIA-607.

Subsistema de Distribución de Campus

El cableado exterior posibilita la conexión entre los distintos edificios, cableado de distribución de campus, cuyos extremos son los cuartos de entrada de servicios.

Los cuartos de entrada de servicios constan de los cables, hardware de conexión, dispositivos de protección y hardware de transición necesarios para conectar las instalaciones de los servicios externos con el subsistema de distribución de edificio.

El tipo de cableado habitual en la interconexión de campus es la fibra óptica, ya sea monomodo o multimodo, en función de la distancia, con blindaje y protección antihumedad y antiroedores.

El cableado exterior puede ser subterráneo o aéreo. El tendido aéreo es desaconsejable con carácter general debido a su efecto antiestético en este tipo de sistemas.

Con respecto a los cables de exterior subterráneos, deben ir canalizados para permitir un mejor seguimiento y mantenimiento, así como para evitar roturas involuntarias o por descuido, más frecuentes en los cables directamente enterrados.

Si se considerase probable incrementar a medio plazo el número de cables tendidos de exterior deben realizarse arquetas a lo largo del trazado para facilitar el nuevo tendido, sin necesidad de realizar calas de exploración.

Si la zona empleada para el tendido puede verse afectada por las acciones de roedores, humedad o cualquier otro agente externo, debe especificarse el cable de exteriores para considerar estos efectos.

En la realización de canalizaciones de exterior debe estudiarse si es necesario solicitar algún permiso administrativos para la realización de dicha obra, debido a no ser los terrenos empleados propiedad de la institución promotora de la canalización exterior.

Subsistema de Distribución de Edificio

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones.

El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.

El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y la sala de equipamiento.

En este componente del sistema de cableado ya no resulta económico mantener la estructura general utilizada en el cableado horizontal, sino que es conveniente realizar instalaciones independientes para la telefonía y datos.

Esto se ve reforzado por el hecho de que, si fuera necesario sustituir el backbone, ello se realiza con un costo relativamente bajo, y causando muy pocas molestias a los ocupantes del edificio.

El backbone telefónico se realiza habitualmente con cable telefónico multipar. Para definir el backbone de datos es necesario tener en cuenta cuál será la disposición física del equipamiento. Normalmente, el tendido físico del backbone se realiza en forma de estrella, es decir, se interconectan los gabinetes con uno que se define como centro de la estrella, en donde se ubica el equipamiento electrónico más complejo.

El backbone de datos se puede implementar con cables UTP o con fibra óptica.

En el caso de decidir utilizar UTP, el mismo será de categoría 6 y se dispondrá un número de cables desde cada gabinete al gabinete seleccionado como centro de estrella.

Actualmente, la diferencia de coste provocada por la utilización de fibra óptica se ve compensada por la mayor flexibilidad y posibilidad de crecimiento que brinda esta tecnología. Se construye el backbone llevando un cable de fibra desde cada gabinete al gabinete centro de la estrella. Si bien para una configuración mínima Ethernet basta con utilizar cable de 2 fibras, resulta conveniente utilizar cable con mayor cantidad de fibra, 6 a 12, ya que la diferencia de costos no es importante y se posibilita por una parte disponer de conductores de reserva para el caso de fallo de algunos, y por otra parte, la utilización en el futuro de otras topologías que requieren más conductores, como FDDI o sistemas redundantes a fallos.

La norma EIA/TIA 568-B prevé la ubicación de la transmisión de cableado vertical a horizontal, y la ubicación de los dispositivos necesarios para lograrla, en habitaciones independientes con puerta destinada a tal fin, ubicadas por lo menos una por piso, denominadas armarios de telecomunicaciones. Se utilizan habitualmente armarios o

gabinetes estándar de 19 pulgadas de ancho, con puertas, de aproximadamente 60 cm. de profundidad y de una altura entre 1.5 y 2 metros.

En dichos gabinetes se dispone generalmente de las siguientes secciones:

- Acometida de los puestos de trabajo: 2 cables UTP llegan desde cada puesto de trabajo.
- Acometida del backbone telefónico: cable multipar que termina en regletas de conexión o en "patch panels"
- Acometida del backbone de datos: cables de fibra óptica que se llevan a una bandeja de conexión adecuada, o UTP Categoría 6 terminado en regletas de conexión o en "patch panels".
- Electrónica de la red de datos: Switches, Routers y otros dispositivos necesarios.
- Alimentación eléctrica para dichos dispositivos.
- Iluminación interna para facilitar la realización de trabajos en el gabinete.
- Ventilación a fin de mantener la temperatura interna dentro de límites aceptables.

Si se realiza integralmente el cableado de telecomunicaciones, con el objetivo de brindar servicio de transmisión de datos y telefonía, existen por lo menos dos alternativas para la interconexión de las verticales de telefonía con el cableado horizontal a los puestos de trabajo:

1. Utilizar regletas (bloques de conexión) que reciben los cables de la vertical por un extremo y los de los puestos de trabajo por el otro, permitiendo la realización de las "cruzadas" de interconexión.
2. Utilizar "patch panels" para terminar las verticales telefónicas y en el cableado horizontal que se destinará a telefonía, implementando las cruzadas con los cables de parcheo ("patch cords").

Esta alternativa, de coste mayor, es la más adecuada tecnológicamente y la que responde más adecuadamente a este concepto de cableado estructurado, ya que permite con la máxima sencillez convertir una boca de datos a telefonía y viceversa.

Subsistema de Cableado Horizontal

Se extiende desde el repartidor de planta (FD) hasta el punto de acceso o conexión pasando por la toma ofimática.

Está compuesto por:

- Cables horizontales.
- Terminaciones mecánicas (regletas o paneles) de los cables horizontales (en repartidores de Planta).
- Cables puentes en el Repartidor de Planta.
- Punto de acceso.

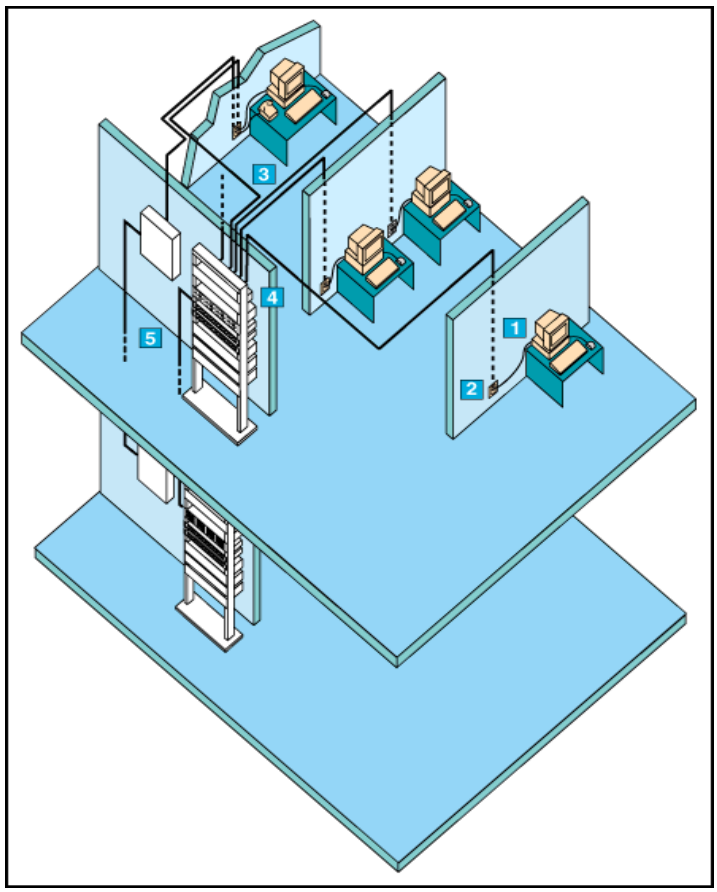


Figura 5 – Elementos cableado horizontal

1.- Latiguillo de puesto.
2.-Toma ofimática o punto de acceso. (TO)
3.- Cableado Horizontal.
4.- Repartidor de Planta (FD).
5.- Cableado vertical.

Cableado Horizontal

El cableado horizontal ha de estar compuesto por un cable individual y continuo que conecta el punto de acceso y el distribuidor de Planta. Si es necesario puede contener un solo punto de transición entre cables con características eléctricas equivalente.

La siguiente figura muestra la topología en estrella recomendada y las distancias máximas permitidas para cables horizontales.

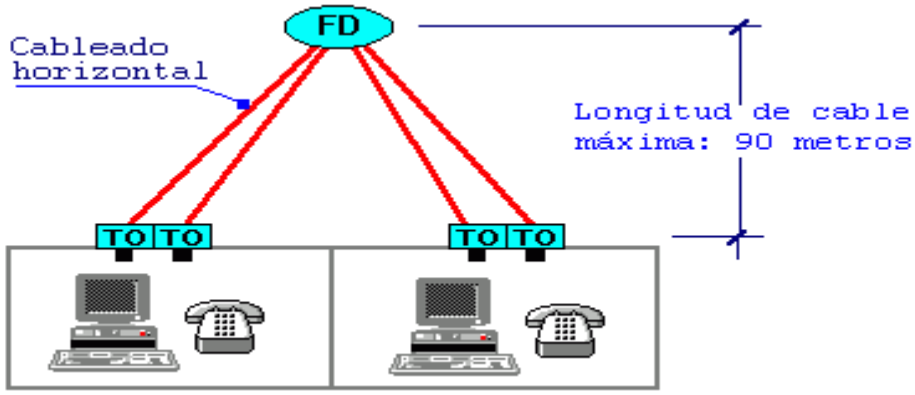


Figura 6 – Detalle Cableado Horizontal

El cableado horizontal consiste de dos elementos básicos:

Cable Horizontal y Hardware de Conexión. Proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones.

Estos componentes son los "contenidos" de las rutas y espacios horizontales.

Rutas y Espacios Horizontales. También llamado "sistemas de distribución horizontal". Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y lo constituyen las canalizaciones dispuestas a tal fin.

Estas rutas y espacios son los "contenedores" del cableado horizontal.

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. En inglés: Work Area Outlets (WAO).
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empalme (patch) y cables de empalme (patch-cords) utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

- Canalizaciones mediante tubos rígidos o flexibles, bandejas de chapa perforada y canaletas con tapa.

La máxima longitud para un cable horizontal ha de ser de **90 metros** con independencia del tipo de cable. La suma de los cables puente, patch cords y cables de equipos no deben sumar más de 10 metros que constituyen la distancia máxima de **100 metros** que establece la norma.

Se recomiendan los siguientes cables y conectores para el cableado horizontal:

- Cable de par trenzado no apantallado (UTP) de cuatro pares de 100 ohmios, Categoría 5e mejorada, terminado con un conector hembra modular de ocho posiciones para EIA/TIA 568, conocido como RJ-45.
- Cable de par trenzado apantallado (STP) de dos pares de 150 ohmios terminado con un conector hermafrodita para ISO 8802.5, conocido como conector LAN.

Los cables se colocarán horizontalmente en la conducción empleada y se fijarán en capas mediante abrazaderas colocadas a intervalos de 4 metros.

Terminaciones mecánicas

Los paneles y regletas son las terminaciones mecánicas de los extremos del cable que llegan a los armarios repartidores.

Para cada tipo de cable existe su panel o regleta asociada.

Los módulos de regletas deberán permitir especialmente:

- La interconexión fácil mediante cables conectores (patch cords) y cables puente o de interconexión entre distintas regletas que componen el sistema de cableado estructurado.
- La integridad del apantallamiento en la conexión de los cables caso de utilizarse sistemas apantallados.
- La prueba y monitorización del sistema de cableado.

Los módulos de regletas se deben unir en el momento del montaje a un porta etiquetas que permita la identificación de los puntos de acceso, de los cables y de los equipos.

Cables de parcheo

Son lo latiguillos de cableado mediante los cuales se realiza las asignaciones en los paneles de distribución. Estas “cruzadas” de interconexión facilitan los procesos de administración dado que los cambios, los traslados, las altas o las bajas se concretan en poner o quitar “patch cords”.

Deberán ser cables certificados en la misma categoría que el cableado que pretende interconectar, siendo elementos críticos por su incidencia en la impedancia total del cableado y su repercusión en el rendimiento del sistema.

La longitud máxima para los “patch cords” es de 3 metros, siempre y cuando el lobe total no exceda de 100 metros.

Punto de acceso

El extremo del cableado horizontal del lado del área de trabajo. Su terminación está mecanizada en módulos hembra RJ45 insertados en rosetas de superficie o empotradas en pared o suelo.

Todos los adaptadores, filtros o acopladores usados para adaptar equipamiento electrónico al sistema de cableado estructurado, deben ser ajenos al punto de acceso o roseta, y está fuera del alcance de la norma 568-B.

Cada área de trabajo deberá ser provista de al menos 2 puntos de acceso con el fin de poder proveer voz y datos.

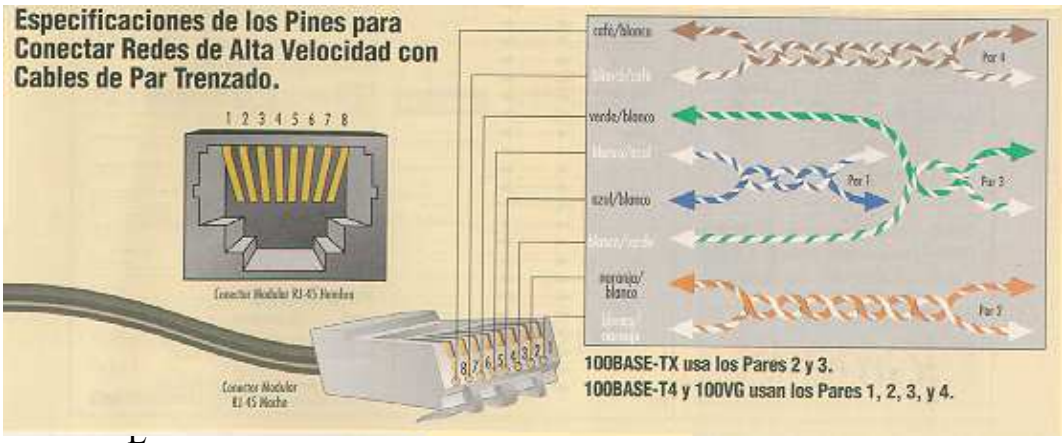


Figura 7 – Especificación Pares RJ45

La norma EIA/TIA 568 especifica dos configuraciones de conexión para el cable UTP de 4 pares los códigos de conexión 568 A y 568 B las diferencias básicas entre uno y otro radican en que en el 568 A el par #2 del cable (naranja) termina en los contactos 3 y 6 y el par #3 del cable (verde) en los contactos 1 y 2 mientras que el 568 B solo intercambia estos dos pares. El par #1 y #4 no varían de una configuración a otra.

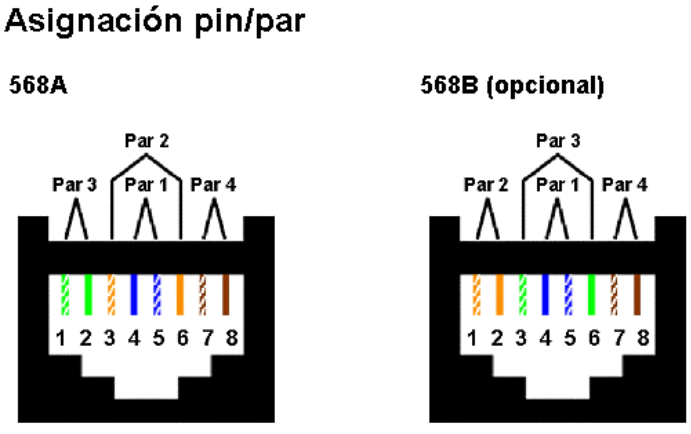


Figura 8 – Asignación de pares

El cable de unión entre la roseta y el equipo de comunicaciones del usuario deberá ser de las mismas características que el resto del cableado, certificado en la misma categoría.

Al igual que los cables de parcheo de los repartidores, estos también son elementos críticos por su incidencia en la impedancia característica pudiéndose degradar el rendimiento de la instalación sino se utilizan cables de calidad.

La longitud máxima de los latiguillos de puesto es de 7 metros, siempre y cuando la distancia total no exceda de 100 metros.

Nueva Generación de Estándares de Cableado: 568-C.0

El Instituto Nacional de Estándares Americanos (ANSI) da una vida útil de los documentos reconocidos de 5 años. El primer documento de la serie 568-B, la 568-B.3 Estándar para Componentes de Cableado en Fibra Óptica", fue publicado en marzo del 2000.

En el año 2008 apareció una nueva revisión del estándar la 568-C.1, que sin modificar la nomenclatura que se venía utilizando para los distintos subsistemas de la versión 568-B, si que planteaba un estándar de cableado de Telecomunicaciones Genérico.

La revisión 568-C.2 fue aprobada a finales de 2009.

La serie 568-B había nacido para cubrir las necesidades de cableado estructurado en edificios comerciales, principalmente dedicado a oficinas, pero al final había sido utilizado para cubrir todo tipo de edificios: aeropuertos, escuelas, estadios…

La nueva generación 568-C intenta dar cobertura a esta necesidad.

Entre las novedades:

- Se modifican los radios de cobertura del cable flexible del patch cord
- Categoría 6A ha sido incluida como tipo de medio reconocido
- Se incluye la recomendación de fibra óptica 50/125 láser optimizada 850 nm como fibra multimodo para edificios comerciales
- Dejan de estar reconocidos como medios: Cableado 150Ω-STP, Categoría 5 y coaxial de 50-Ω y 75-Ω
- Se incluye la nomenclatura ISO 11801 (OM-1, OM-2…) como nomenclatura madre de los distintos tipos de fibras ópticas reconocidas.

- Además, el estándar está preparado para convertirse en el fundamento de otros estándares a desarrollar en el futuro, como pueden ser **estándares de cableado estructurado para el Data Center.**
- En este sentido es el "germen" de los estándares y recomendaciones para todas las **Green Data Center Solutions**:
    - Guía de pasillos Fríos y calientes para mejor la eficiencia energética.
    - Construcción de redes ópticas con menos materias primas (menos peso y volumen)
    - Cableado para la automatización de algunos servicios dentro del Data Center: seguridad, climatización, iluminación…

1.2.2. Tendencias de Diseño

Cuando se afronta el cableado estructurado de un edificio con varias plantas una de las primeras decisiones de diseño que se plantean es la realización de una instalación centralizada o una instalación descentralizada o por planta.

De forma gráfica las opciones son las siguientes:

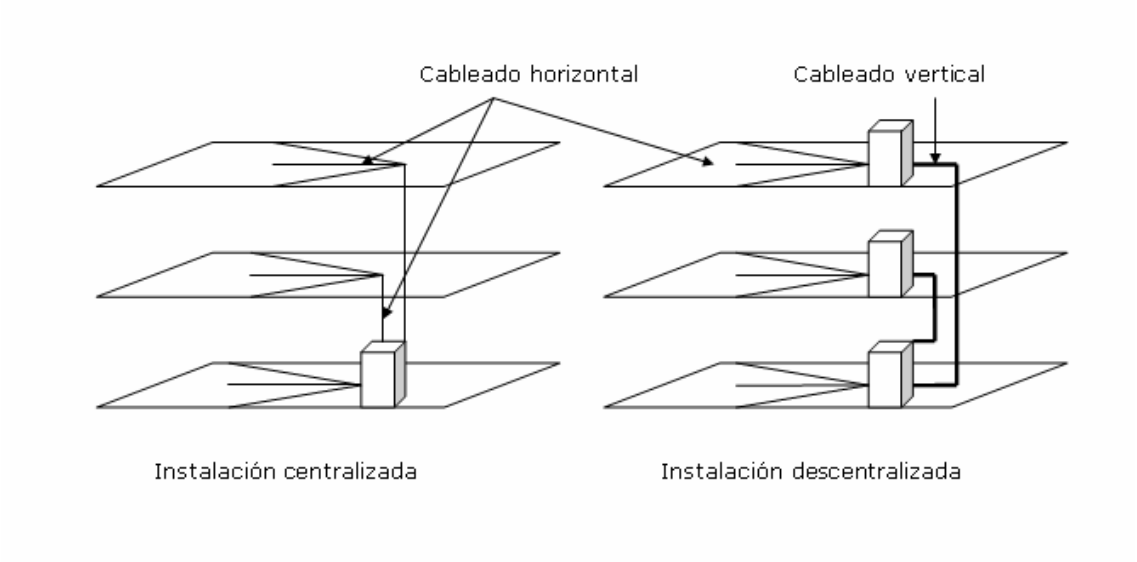


Figura 9 – Diseño Cableado Estructurado

Las características de cada tipo de instalación son:

- **Instalación centralizada**. Consiste en el tendido del cableado de todos los puntos del edificio a un único cuarto de comunicaciones. Se utiliza en los siguientes casos:
    - Edificios de varias plantas con canalizaciones suficientes, siempre que no se supere la distancia máxima.
    - Edificios de una o dos plantas.

    - Ventajas:
        - Facilidad de Gestión – Todo el cableado termina en un mismo cuarto de comunicaciones, con lo que la gestión del mismo es mas sencilla.
    - Inconvenientes:
        - Es necesario que las canalizaciones verticales del edificio sean lo suficientemente anchas como para contener todo el cableado horizontal.

- **Instalación descentralizada o por planta**. Consiste en la instalación de varios armarios de cableado, cada uno de los cuales da servicio a una zona concreta. Es una instalación que se debe evitar, pues son más difíciles de gestionar. Se utilizan en los siguientes casos:
    - Cuando por las dimensiones del edificio no es posible respetar la distancia máxima de 90 metros.
    - Edificios antiguos en los que la canalización disponible no es suficiente para realizar el tendido del cableado de forma centralizada.
    - Edificios en los que sería posible acometer un cableado centralizado, pero que por necesidades organizativas –una unidad independiente- sea conveniente desde el punto de vista de gestión mantener una infraestructura independiente.

Elementos Cableado Estructurado

Cableado en Cobre

El cableado de cobre se realiza con los siguientes elementos:

- Cables de cobre trenzados de 4 pares
- Cables multipar.
- Paneles
- Tomas de usuario
- Latiguillos
  - Voz. RJ11
  - Datos. RJ45. Categoría 6 y Categoría 6ª

En la siguiente tabla se detallan las características en lo que a frecuencia de transmisión y características específicas de las distintas categorías de cableado que se utilizan actualmente en las instalaciones reales:

Categoría	Especificación	Observaciones
3	Hasta 16MHz	Clase C. Compatible RJ45
5E	Hasta 100MHz	Clase D. Compatible RJ45
6	Hasta 250MHz	Clase E. Compatible RJ45
6A	Hasta 500MHz	10Gigabit Ethernet. Compatible RJ45. Mejora el Alien Crosstalk
7	Hasta 600MHz	Clase F. Conectores TERA y GG-45 (compatible RJ45). Cable apantallado

Figura 10 – Categorías Cableado en Cobre

Cada una de las categorías indicadas tiene un servicio asociado, y permite la transmisión a unas velocidades determinadas. En la siguiente tabla se muestras para los servicios básicos demandados actualmente si las distintas categorías lo soportan.

Servicios	Cat 3	Cat5E	Cat6	Cat6A	Cat7
Voz analógica/digital	Sí	Sí	Sí	Sí	Sí
10/100 Base T	No	Sí	Sí	Sí	Sí
Telefonía sobre IP (con POE)	No	Sí	Sí	Sí	Sí
1000Base T Gigabit Ethernet	No	Sí	Sí	Sí	Sí
10Gigabit Ethernet (hasta 100m)	No	No	No	Sí	Sí

Figura 11- Servicios Soportados por categoría cableado cobre

A destacar lo siguiente:

- Categoría 3, utilizada solo para servicios de voz tradicional (analógica o digital), mediante la instalación de cables multipar en cableados de campus o verticales, típicamente con 10, 25,50 o 100 pares.

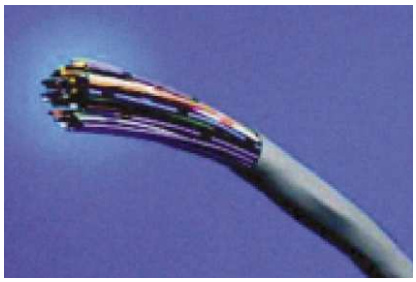


Figura 12 – Cable Cobre Multipar

- Utilización de ToIP. Debido a las limitaciones en lo que a calidad, retardo... del servicio de ToIP sobre una red datos, se recomienda que este servicio sea montado sólo a partir de cableados estructurados de categoría 5E.
- Para velocidad de transmisión de 10Gbps (hasta 100 metros), es necesario cableado a partir de 6A.

Existe además otra clasificación de los tipos de cables de cobre, en función de la metodología utilizada en su construcción y el grado de apantallamiento frente a radiaciones que poseen. Así tenemos:

- Cable UTP (Unshielded Twisted Pair), Par Trenzado NO Apantallado.
- Cable F/UTP (Foiled Unshielded Twisted Pair) Par Trenzado NO Apantallado Individualmente, Cable apantallado con lámina. Otras denominaciones: FTP.
- Cable S/FTP (Shielded Foil Twisted Pair) Par Trenzado Apantallado Individualmente con lámina, Cable con pantalla trenzada). Otras denominaciones: STP.

Además de la construcción es preciso atender a la cubierta del cable que es la que protege al cable frente a la intemperie. El tipo de cubierta dependerá del lugar donde se instale el cableado: exterior o interior. Existe una recomendación adicional para la cubierta del cable: LSZH (Low Smoke, Zero Halogen, Sin emisión de humos y con cero halógenos).

Un aspecto importante es la terminación de todo el cableado dentro de los armarios repartidores de cableado, esto es los **paneles**.

Por referencia histórica referenciamos los paneles ATT 110, paneles utilizados con cableado cat. 3 para la terminación de cableados de voz, bien de centralita, bien de la horizontal de voz de cualquier instalación. Actualmente en desuso.

Figura 13 – Paneles ATT 110 - Voz

Todas las instalaciones se terminan actualmente en paneles con conector RJ45. Comentar que la categoría final del cableado de una instalación viene determinada por todos los elementos que componen la instalación: cables, conectores, cajas y paneles. Es por ello que encontraremos paneles categoría 3, 5E y 6.

Figura 14- Paneles RJ45 – Cat 6

Cableado en Fibra óptica

Las fibras ópticas son medios de transmisión fabricados a partir de un cristal de silicio modificando las características ópticas de los materiales que las componen.

La fibra óptica es una guía de ondas dieléctrica que opera a frecuencias ópticas.

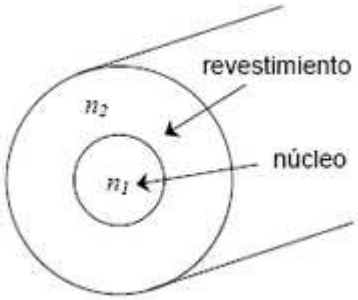


Figura 15 – Estructura Fibra óptica

Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total.

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

En cableado estructura se utilizan básicamente dos tipos de fibras:

- Fibras Multimodo: Los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 Km., es simple de diseñar y económico.

  Según el sistema ISO 11801 para clasificación de fibras multimodo según su ancho de banda se incluye el formato OM3 (multimodo sobre láser) a los ya existentes OM1 y OM2 (multimodo sobre LED).

  - OM1: Fibra 62.5/125 μm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores

  - OM2: Fibra 50/125 μm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores

- OM3: Fibra 50/125 μm, soporta hasta 10 Gigabit Ethernet (300 m), usan láser (VCSEL) como emisores.

- Fibras Monomodo: Sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 Km. máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s).

Las fibras son muy frágiles por lo que se organizan en cables para su protección. Debido a su fragilidad la fibra óptica es difícil de instalar y de delicado mantenimiento en el puesto de usuario

Las pérdidas de la fibra óptica son muy bajas, comparadas con los cables de cobre. Las pérdidas típicas de una fibra óptica son:

- Fibra multimodo: 3.2 dB/Km@850nm y 0.8dB/Km@1310nm
- Fibra monomodo: 0.35 dB/Km@1310nm y 0.25dB/Km@1550nm

En la siguiente figura se intentan resumir las características de los dos tipos de fibras:

Fibra Multimodo	Fibra Monomodo
Bajo precio	Alto Precio
Altas pérdidas	Bajas pérdidas
Electrónica barata	Electrónica cara

Figura 16 – Características Tipos de Fibra

En lo que respecto a los conectores, existen múltiples tipologías, que han ido apareciendo y desapareciendo a lo largo de la historia, a medida, que la tecnología en lo

que a velocidad de propagación ha ido avanzado. Los tipos de conectores que existen (o han existido son)

- FC, que se usa en la transmisión de datos y en las telecomunicaciones.
- FDDI, se usa para redes de fibra óptica.
- LC y MT-Array que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC se usa en redes de edificios y en sistemas de seguridad.

En la siguiente figura se aprecian gráficamente los distintos tipos de conectores:

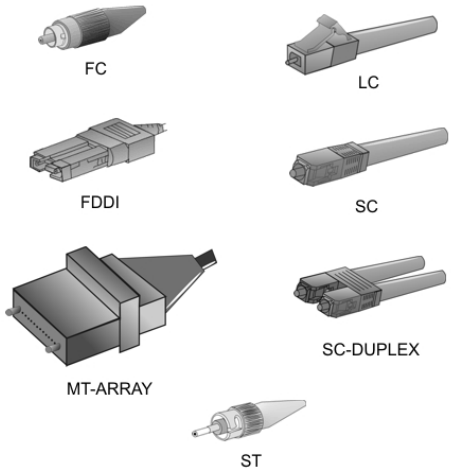


Figura 17 – Tipos conectores Fibra óptica

Actualmente, el conector tipo LC, en su forma LC duplex [transmisión y recepción por fibras separadas], es el que se ha implantado como estándar de facto dentro de los cableados estructurados de fibra óptica.

Figura 18 – Conector Fibra LC Duplex

Los cables de fibra se organizan en cables para protegerlos mecánicamente. Protegen las fibras que se encuentran en su interior y además proporciona suficiente consistencia mecánica para que pueda manejarse en las mismas condiciones de tracción,

compresión, torsión y medioambientales que los cables de conductores. Para ello incorporan elementos de refuerzo y aislamiento frente al exterior.

Canalización Horizontal y cajas de usuario

Como norma general se deberá dimensionar la sección de la canalización horizontal para un 50% de ocupación, en previsión de posibles aumentos del número de puntos de cableado. Además las bandejas que conduzcan el cableado eléctrico y el cableado de voz/datos deben ir separadas, con trazados perpendiculares

La canalización de todo el cableado en el subsistema horizontal, de usuario, se puede realizar de diversas formas:

- Falso Suelo: Cajas empotradas en el falso suelo
- Falso Techo: Las bajantes hasta las cajas de usuario suelen ir por las paredes o en columnas dedicadas a este propósito.
- Canaleta vista perimetral: Cuando no queda otro remedio, se coloca una calaneta en la que se pueden integrar las cajas de usuario

En las siguientes figuras se muestras los distintos tipos de canalización

Figura 19 – Canaliz. Horiz. Falso Suelo

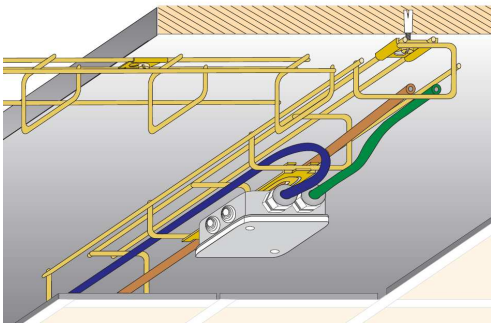


Figura 20 – Canaliz. Horiz. Falso Techo

Figura 21 – Canal. Horiz. Canaleta

Podemos emplear la siguiente fórmula para intentar calcular la sección (mm^2) que debería tener nuestra canalización (rejiband o canaleta) en función del número de cables que queremos que contenga:

- Scanalización (mm2): sección de la canalización.
- Scable(mm2): sección del cable. Para categoría 6 considerar 7.5 mm de diámetro, lo que lleva a 44.2 mm2. A efectos de dimensionamiento se considerará que cada módulo de usuario tendrá 3 cables.
- Ncables: número de cables en esa sección.

$$Scanalizacion(mm2) = 98.2xNcables = 294.6xNmodulos\_usuario$$

En lo que respecta a las cajas de usuario, por comodidad, se intentará, que en la medida de lo posible sean compartidas con los módulos de electricidad (conectores sucko), de forma que con una solo caja se tengan los servicios de electricidad y de telecomunicaciones. Es por esto que se indicaba al inicio de esta apartado la total coordinación que debe de existir entre la sección de arquitectura, de quien debería de depender el cableado de electricidad, y la sección de telecomunicaciones de quien depende el cableado de telecomunicaciones.

Para los usos actuales se recomiendan cajas con 4 conectores eléctricos tipo sucko y 4 tomas de datos (para la utilización de servicios de voz y/o datos), siguiendo el siguiente esquema.

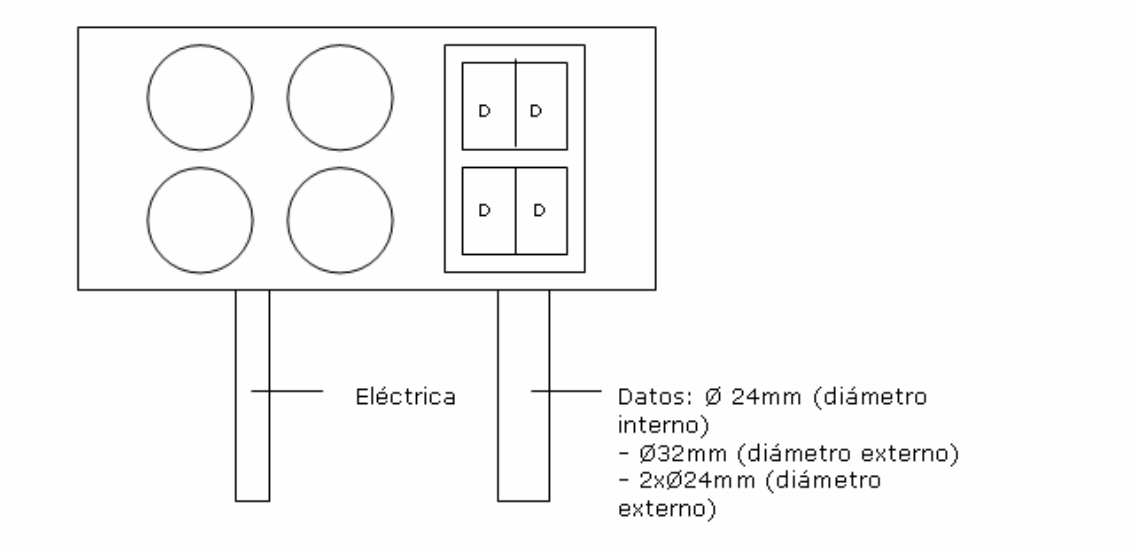


Figura 22 – Caja Usuario: electricidad y datos

En las siguientes figuras aparecen varios modelos comerciales que pueden encontrarse en el mercado.

Figura 23 – Cajas de Usuario - Modelos

Herramientas Diseño

Mediante este apartado se pretende dar una visión de las distintas herramientas que nos ayudan en la realización del diseño de este subsistema. Básicamente utilizaremos dos tipos de herramientas:

- Herramienta tipo CAD para el diseño de la capa física.
- Herramienta diseño Red para el layout de los armarios

Herramienta CAD

Al estar la capa física tan ligada a la estructura física del edificio que la contiene, parece que tiene sentido la utilización de herramientas relacionadas con la arquitectura para la definición, representación de los elementos que componen la capa física. Se utilizan básicamente herramientas de diseño, donde se puedan cargar los planos de planta sobre los que se diseñará la infraestructura de cableado estructurado. Para la realización de este trabajo se ha utilizado la herramienta Autocad 2007®.

La herramienta está pensada para trabajar en capas: canalizaciones, electricidad, climatización, mobiliario, sistema de comunicaciones.

En la siguiente figura se aprecia la gestión de capas de Autocad 2007®.

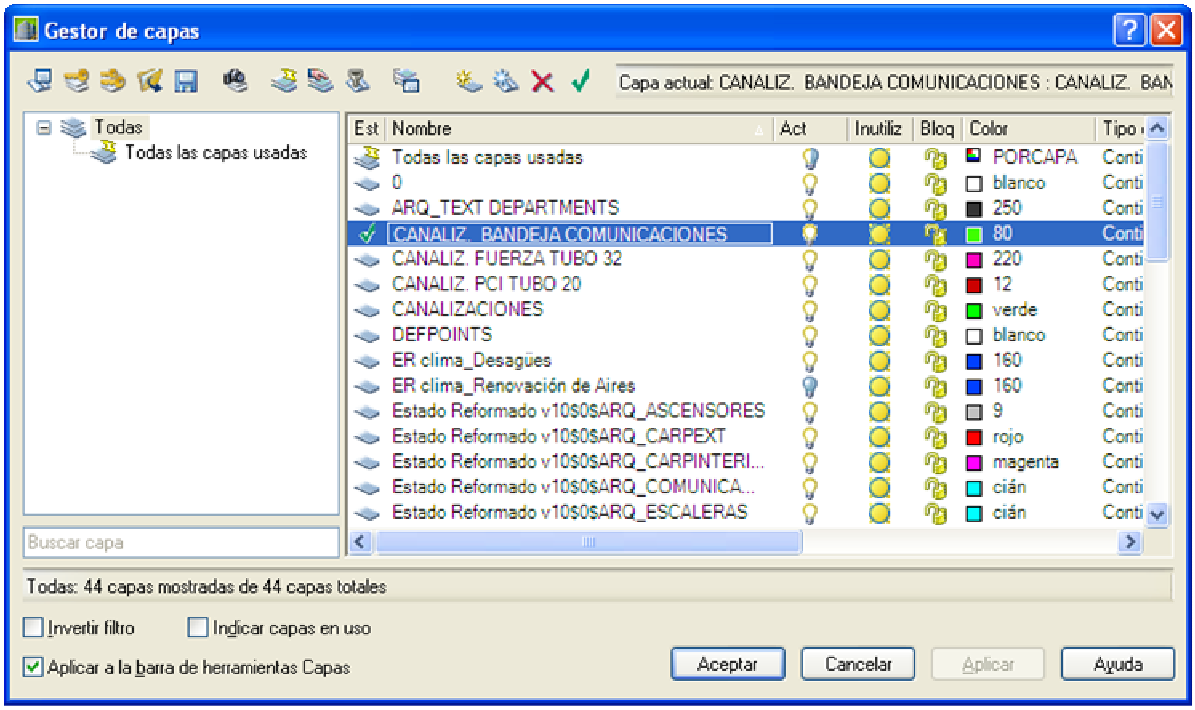


Figura 24 – Gestión Capas Autocad 2007

Simplemente desactivando las capas (icono bombilla) se pueden eliminar del plano todos los elementos no deseados. En nuestro caso, la capa básica que utilizaremos para el diseño de cableado estructurado será la capa de Telecomunicaciones.

El aspecto que tendrá un plano con todos los elementos de comunicaciones: rejillas, bandejas, tubos, canalizaciones, rosetas usuario es el siguiente:

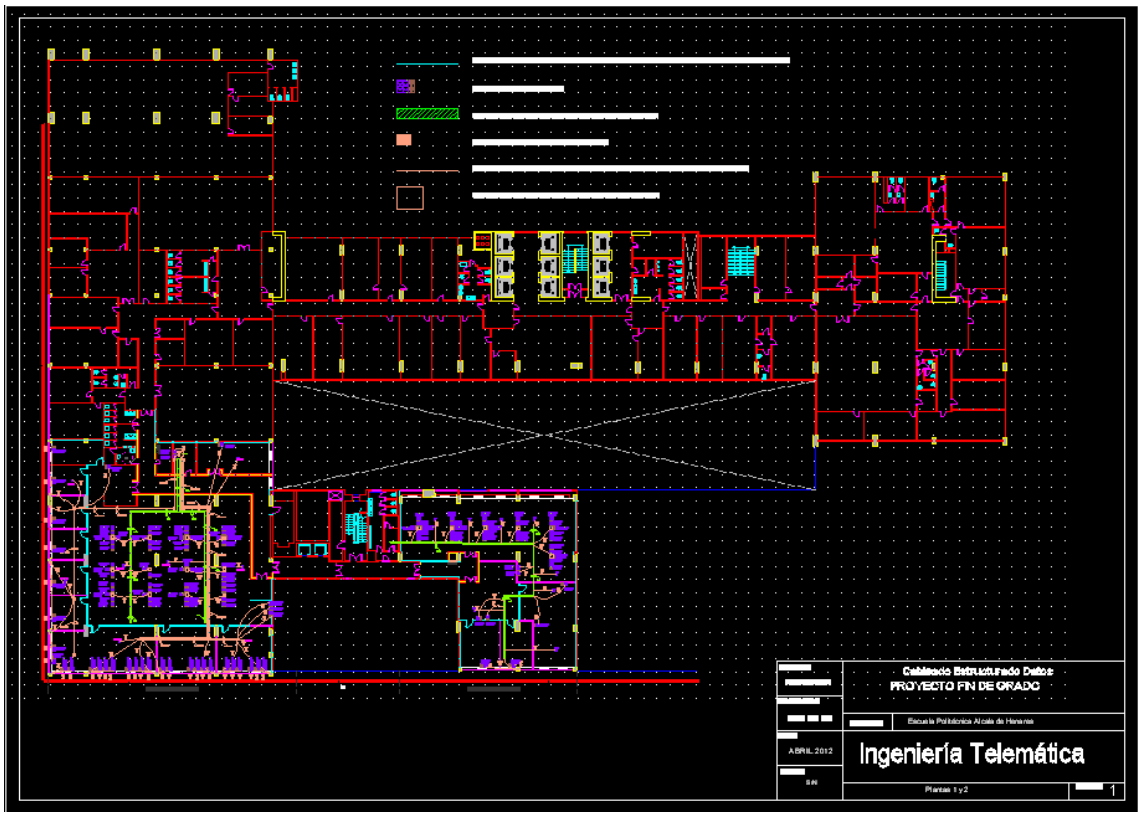


Figura 25- Plano trabajo Autocad 2007

Herramienta Diseño Red

Otro de los aspectos importantes en el diseño del subsistema de cableado estructurado es el diseño de los layout de los frontales de los armarios de comunicaciones, de cara a preparar la disposición de los elementos de cableado estructurado y definir las posiciones donde se ubicarán switches, routers o cualquier otro elemento que tenga que ver con el sistema de comunicaciones de la oficina.

Los elementos a tener en cuenta serán: paneles cableado voz, paneles cableado datos, pasahilos, bandejas de fibra óptica, switches, routers,…

La definición de este layout se puede realizar simplemente con una **hoja Excel**, definiendo las distintas Us de los armarios y los elementos que se albergarán en ellos. …

	A	B	C
1			
2		ARMARIO R1	ARMARIO R2
3	"UR"		
4	1	PANEL DE 4 ENLACES LC F.O. 10GB	TAPA
5	2	PASAHILOS DE CEPILLO ABIERTO	TAPA
6	3	PANEL DE 50 PARES CAT-3 TELEFONIA	TAPA
7	4	PASAHILOS DE CEPILLO ABIERTO	TAPA
8	5	PANEL DE 24 TOMAS CAT-6 (A001-A024)	PANEL DE 24 TOMAS CAT-6 (C001-C024)
9	6	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
10	7	PANEL DE 24 TOMAS CAT-6 (B001-B024)	PANEL DE 24 TOMAS CAT-6 (D001-D024)
11	8	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
12	9	PANEL DE 24 TOMAS CAT-6 (A025-A048)	PANEL DE 24 TOMAS CAT-6 (C025-C048)
13	10	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
14	11	PANEL DE 24 TOMAS CAT-6 (B025-B048)	PANEL DE 24 TOMAS CAT-6 (D025-D048)
15	12	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
16	13	PANEL DE 24 TOMAS CAT-6 (A049-A072)	PANEL DE 24 TOMAS CAT-6 (C049-C072)
17	14	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
18	15	PANEL DE 24 TOMAS CAT-6 (B049-B072)	PANEL DE 24 TOMAS CAT-6 (D049-D072)
19	16	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
20	17	PANEL DE 24 TOMAS CAT-6 (A073-A096)	PANEL DE 24 TOMAS CAT-6 (C073-C096)
21	18	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
22	19	PANEL DE 24 TOMAS CAT-6 (B073-B096)	PANEL DE 24 TOMAS CAT-6 (D073-D096)
23	20	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
24	21	PANEL DE 24 PUNTOS CAT-6 WIFI (WF01-WF08)	TAPA
25	22	PASAHILOS DE CEPILLO ABIERTO	TAPA
26	23		
27	24		
28	25		
29	26		
30	27		
31	28		
32	29	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
33	30	SWITCH CISCO CATALYST 3750X	SWITCH CISCO CATALYST 3750X
34	31	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
35	32	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
36	33	SWITCH CISCO CATALYST 3750X	SWITCH CISCO CATALYST 3750X
37	34	PASAHILOS DE CEPILLO ABIERTO	PASAHILOS DE CEPILLO ABIERTO
38	35		
39	36		
40	37		
41	38		
42	39		
43	40		
44	41		
45	42		
46			
47			

Figura 26- Layout armarios cableado - Excel

Otra de las herramientas que se puede utilizar para la definición de estos layout es el Microsoft Visio, en concreto para la realización de este proyecto se ha utilizado Microsoft Visio 2003 ®

A partir de un layout en blanco insertaremos un componente bastidor donde podremos ir colocando los distintos elementos que conformarán el layout de nuestro armario.

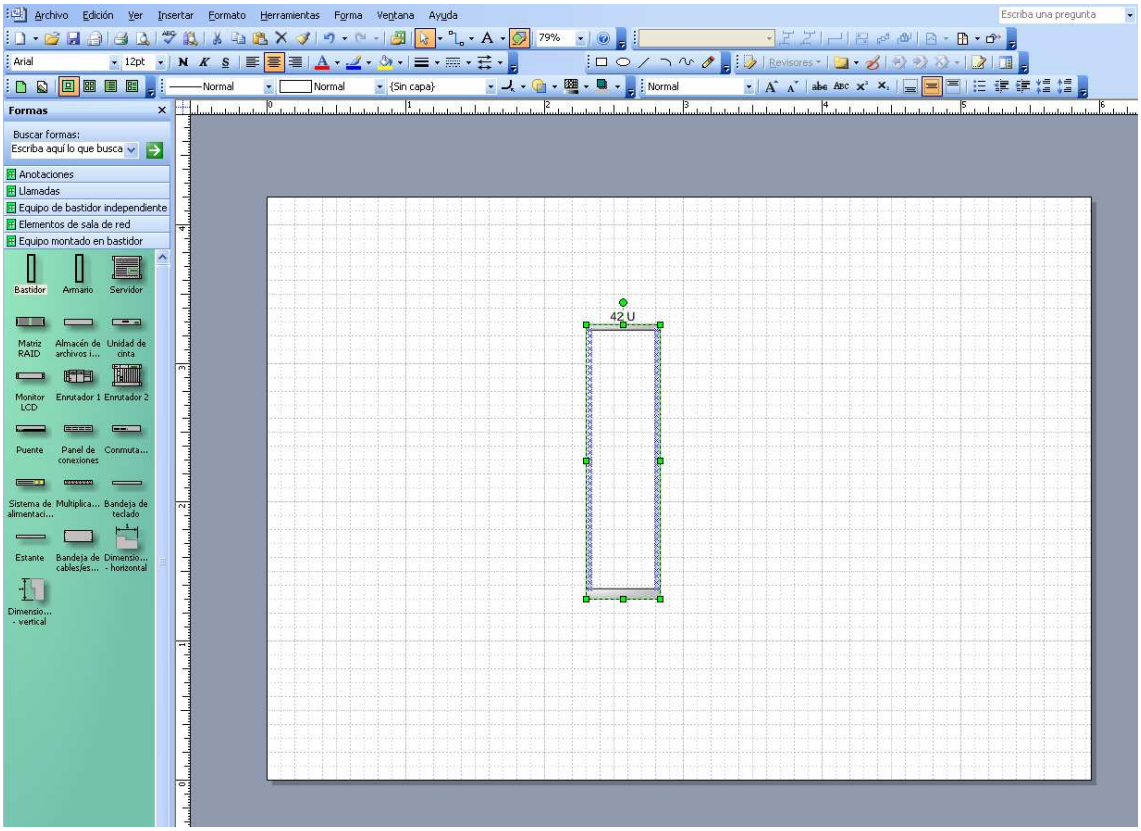


Figura 27- Layout armarios cableado - Visio

El layout de un frontal de armario completo tiene el siguiente aspecto:

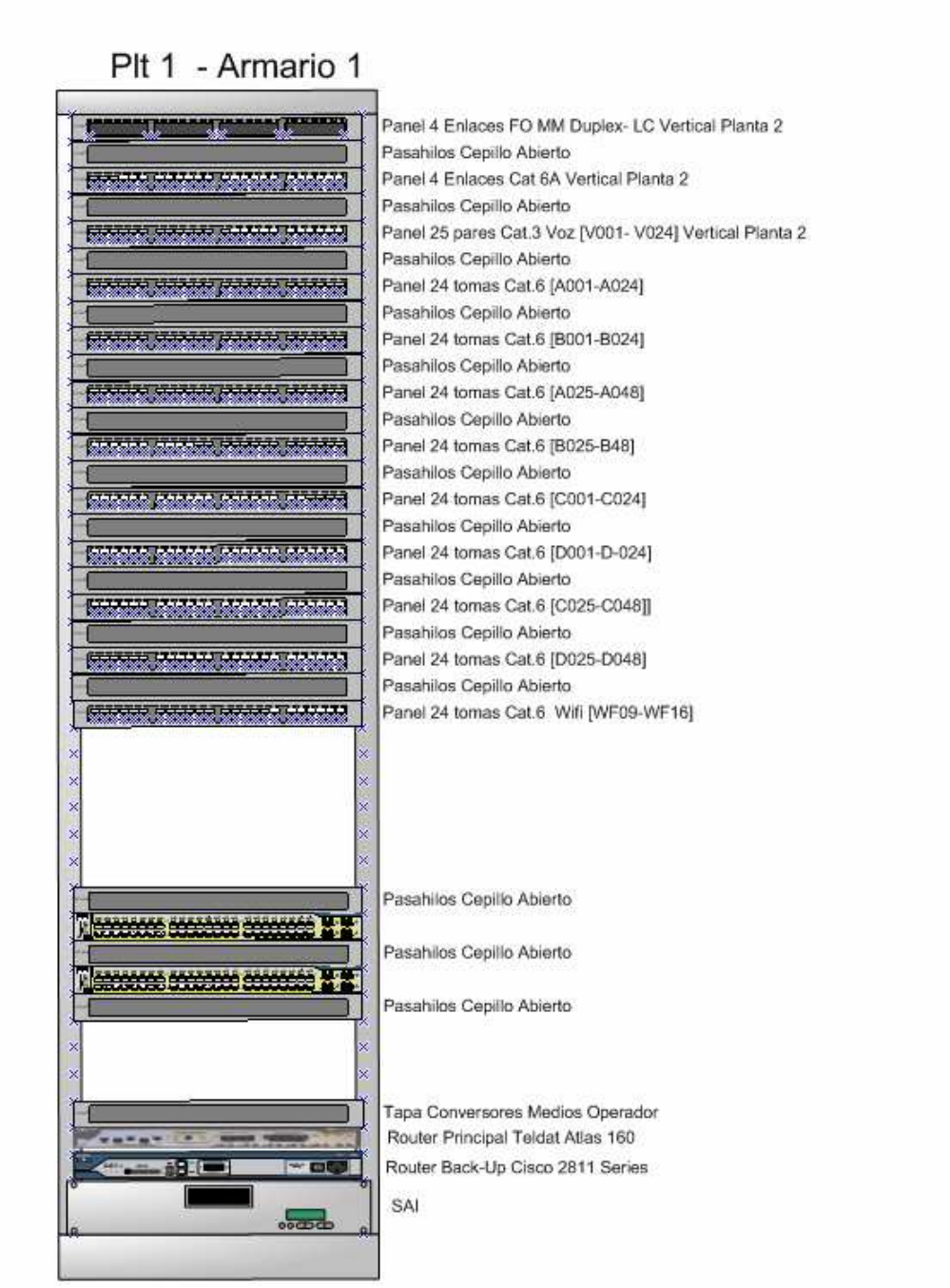


Figura 28- Layout armarios cableado – Visio 2

Es sencillo encontrar en Internet los ficheros de formas para Visio (*.vss) de los distintos fabricantes:

Cableado: systimax, brand-rex…

Electrónica nivel 2: HP, Cisco, Avaya,..

Electrónica nivel 3: Cisco, Teldat,…

1.2.3. Aplicación Práctica

En este apartado se pretende dar una visión práctica que aplique todo lo indicado anteriormente a la instalación de un sistema de cableado estructurado que permita soportar la infraestructura básica de comunicaciones necesarias en una oficina para dotarla de una red de área local con conexión a una red de área extensa.

Para intentar simplificar el caso práctico se presupone que todo el estudio previo de canalizaciones, altura de falsos techos, altura de los suelos técnicos, conducciones de electricidad, cajas empotradas a colocar … se han realizado ya en coordinación con la sección de arquitectura que esté ejecutando la obra civil.

Indicar que, aunque no aparezcan reflejadas en este proyecto, estas reuniones con los arquitectos son muy importantes, y deben poder realizarse, en el momento en el que se está definiendo el proyecto en su conjunto, de forma que una de las partes de la obra civil que se esté realizando sea la realización de la infraestructura de comunicaciones, y se vea como una parte del total de la obra, y no como un anexo posterior [si esto último ocurre suele haber poco margen de maniobra para corregir posibles deficiencias].

1.2.3.1. Estudio Práctico Infraestructura cableado

En el estudio práctico se pretende dotar a una oficina de dos plantas de la infraestructura de comunicaciones necesaria, para permitir la interconexión vía red LAN de los usuarios (capítulo 1.3 de este documento), y permitir la conexión de estos a una red WAN mallada, multiservicio para la conexión con sus sistemas centrales y con otras sedes de la compañía (capítulo 1.4 de este documento).

Ambas plantas se encuentra comunicadas mediante un patinillo central a través de las dos zonas habilitadas como cuartos técnicos.

La distribución de puntos de cableado por plantas es la siguiente:

- **Planta 1:**

Se pretende dotar la zona con una densidad alta de puestos de trabajo, incluyendo puestos cableados para usuarios finales y puntos de cableado para la conexión de puntos de acceso wifi.

El número total de puntos es el siguiente:
- Puntos de cableado usuario: 38
- Puntos de cableado para conexión APs wifi: 8

- **Planta 2:**

Se pretende dotar la zona con una densidad alta de puestos de trabajo, incluyendo puestos cableados para usuarios finales y puntos de cableado para la conexión de puntos de acceso wifi.

El número total de puntos es el siguiente:
- Puntos de cableado usuario: 88
- Puntos de cableado para conexión APs wifi: 8

Se pretende dotar a todo el edificio de un sistema de telefonía basada en ToIP, mediante la instalación de terminales IP conectados a la red. Es por ello que se diseña la infraestructura de red, pensando solo en conectividad para dispositivos IP (ordenadores, escáneres en red, impresoras en red, teléfonos IP…), sin realizar una distinción de voz/ datos ni en la instalación ni en el etiquetado.

La acometida desde la calle, para acceso de las líneas (fibras, cobre, pares..) de los operadores termina en el cuarto técnico habilitado en la primera planta.

Todo el cableado del subsistema horizontal será de categoría 6ª, lo que nos permitirá dotar a la infraestructura de comunicaciones de capacidad suficiente para la conexión de dispositivos de red hasta con 1 Gbps de velocidad.

Se instalará un subsistema de cableado vertical de comunicación entre plantas, compuesto de cableado de cobre categoría 6ª, lo que nos permitirá enlaces entre plantas de hasta 10 Gpbs, y también cableado en fibra multimodo OM3, lo que nos permitirá también conseguir velocidades de transmisión de 10 Gbps y alcances de unos 300 metros

1.2.3.2. Distribución de cableado

Como se ha comentado en este estudio práctico aparecen 3 subsistemas de cableado estructurado: 2 subsistemas de cableado horizontal de planta, 1 subsistema de cableado vertical de comunicaciones entre plantas.

Todo el cableado horizontal de las plantas 1 y 2 tiene una categoría 6A

La distribución del cableado en cada planta tiene las siguientes características.

- Planta 1:

  La distribución del cableado horizontal en la Planta 1 se realizar a través del falso suelo utilizando rejilla del tipo Rejibad (color verde) para la distribución de cableado principal en la planta y tubo corrugado grapado al suelo (color naranja) para llegar a las cajas de usuario.
  Las dimensiones de los elementos de distribución horizontal son:

  - Rejilla Rejiband:
    - Rejilla Principal Distribución Central: 300mm x 60 mm
    - Rejillas Secundarias: 100mm x 60 mm
  - Tubos Corrugados: 21, 32 y 40 mm en función del número de cables que soporta.

Un detalle del plano de cableado estructurado horizontal se aprecia en la siguiente figura:

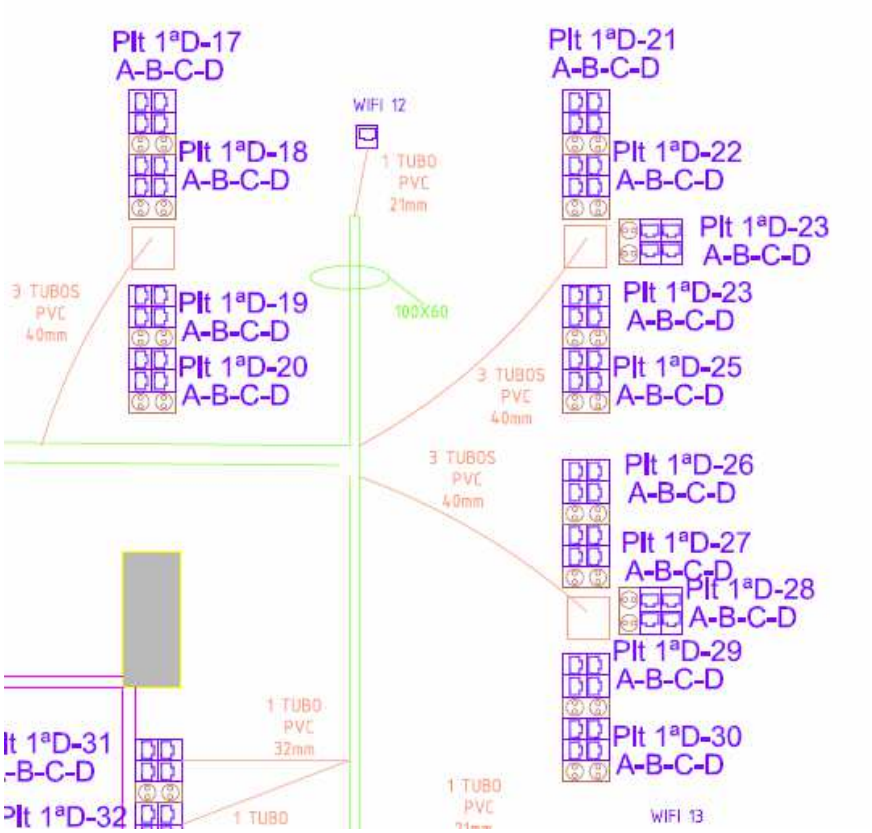


Figura 29 – Detalle Cableado Estructura Horizontal Plata 1

La forma en la que llegan los cables en los puestos de usuario se realiza de dos formas distintas:

- En la zonas centrales de planta, mediante columnas de suelo donde se insertarán los mecanismos RJ45 y los conectores eléctricos Sucko.
- En las zonas de pared directamente colocando las cajas empotradas en el falso suelo

En las siguientes figuras se aprecian las cajas de usuario seleccionadas

Figura 30 – Cajas usuario zonas pared

Figura 31- Cajas de usuario columnas centrales

- Planta 2:

  La distribución del cableado horizontal en la Planta 1 se realizar a través del falso suelo utilizando rejilla del tipo Rejibad (color verde) para la distribución de cableado principal en la planta y tubo corrugado grapado al suelo (color naranja) para llegar a las cajas de usuario.
  Las dimensiones de los elementos de distribución horizontal son:

  - Rejilla Rejiband:
    - Rejilla Principal Distribución Central: 300mm x 60 mm
    - Rejillas Secundarias: 200mm x 60 mm
    - Rejillas Finales: 100mmx60mm

  - Tubos Corrugados: 21, 32, 40 y 50 mm en función del número de cables que soporta.

Las cajas de usuario son las mismas que las utilizadas en la planta 1.

Un detalle del plano de cableado estructurado horizontal se aprecia en la siguiente figura:

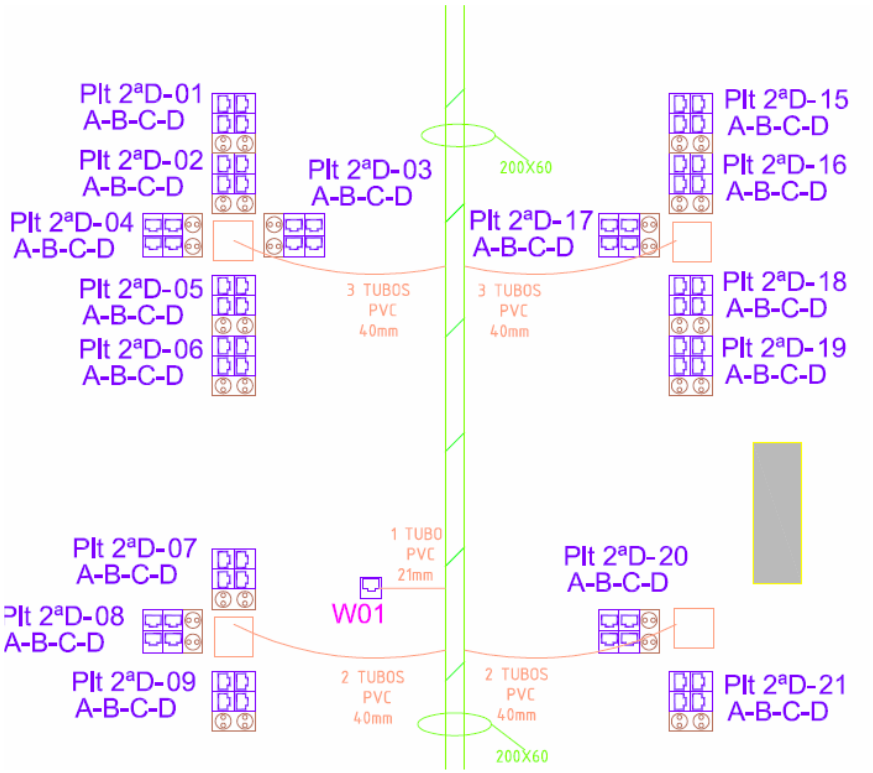


Figura 32- Detalle cableado estructurado Plata 2

La nomenclatura a utilizar será la siguiente:

- Para los puestos de usuario: Plt 1ªD-07-A, es decir, punto 7-A de datos de la planta 1ª.
- Para los puntos de conexión de los APs wifis: WIFI XX, un literal consecutivo donde:
  i. XX = 1 a 8 → Planta 1
  ii. XX = 9 a 16 → Planta 1

Además del cableado de subsistema horizontal, es necesario comunicar ambas plantas, para ello utilizaremos un subsistema de cableado vertical. Se utilizará el patinillo interior del edificio que comunica ambos cuartos técnicos para comunicar ambos cuartos de comunicaciones con:

- Una manguera de 25 pares categoría 3, para uso de servicios analógicos. Pese a que el sistema de telefonía a implantar es tecnología ToIP, es posible que se tenga que dotar a la oficina de algún servicio analógico (fax analógico, teléfono analógico emergencias, líneas Adel sobre par de cobre independiente de la infraestructura de red WAN…)

- 4 enlaces de cobre categoría 6ª, para la interconexión de la electrónica de nivel 2, con velocidades de hasta 10 Gbps en el entorno de los 100m.
- 4 enlaces de fibra óptica multimodo OM3, terminada en conectores Duplex LC, con capacidad de transmisión de hasta 10 Gpbs, para ser utilizados en caso necesario.

Layout Frontal Armarios Comunicaciones

Uno de los aspectos más importantes a la hora de diseñar un sistema de cableado estructura es realizar un layout del frontal de los armarios de comunicaciones y un esquema de la distribución del cableado vertical.

Una buena distribución de todos los elementos es básica para mantener el orden y la limpieza en los cuartos de comunicaciones.

En este layout se deberá hacer notar de una forma gráfica la disposición de los paneles de cableado, indicando claramente los paneles que corresponden a las tomas de usuario, a las tomas wifi, a los paneles de operador y a los paneles del cableado del subsistema vertical de cableado. En capítulos sucesivos se irán completando estos layouts con la información de los dispositivos de nivel 2 y de nivel 3, así como cualquier elemento susceptible de ser enracado en los armarios de comunicaciones.

Layout Frontal Armario Planta 1

Dado el número de puntos cableado es suficiente con un solo armario de 42 U de alto para dar cobertura a todos los paneles de cableado estructurado horizontal, vertical y wifi, a la electrónica nivel 2 necesaria y a la electrónica nivel 3.

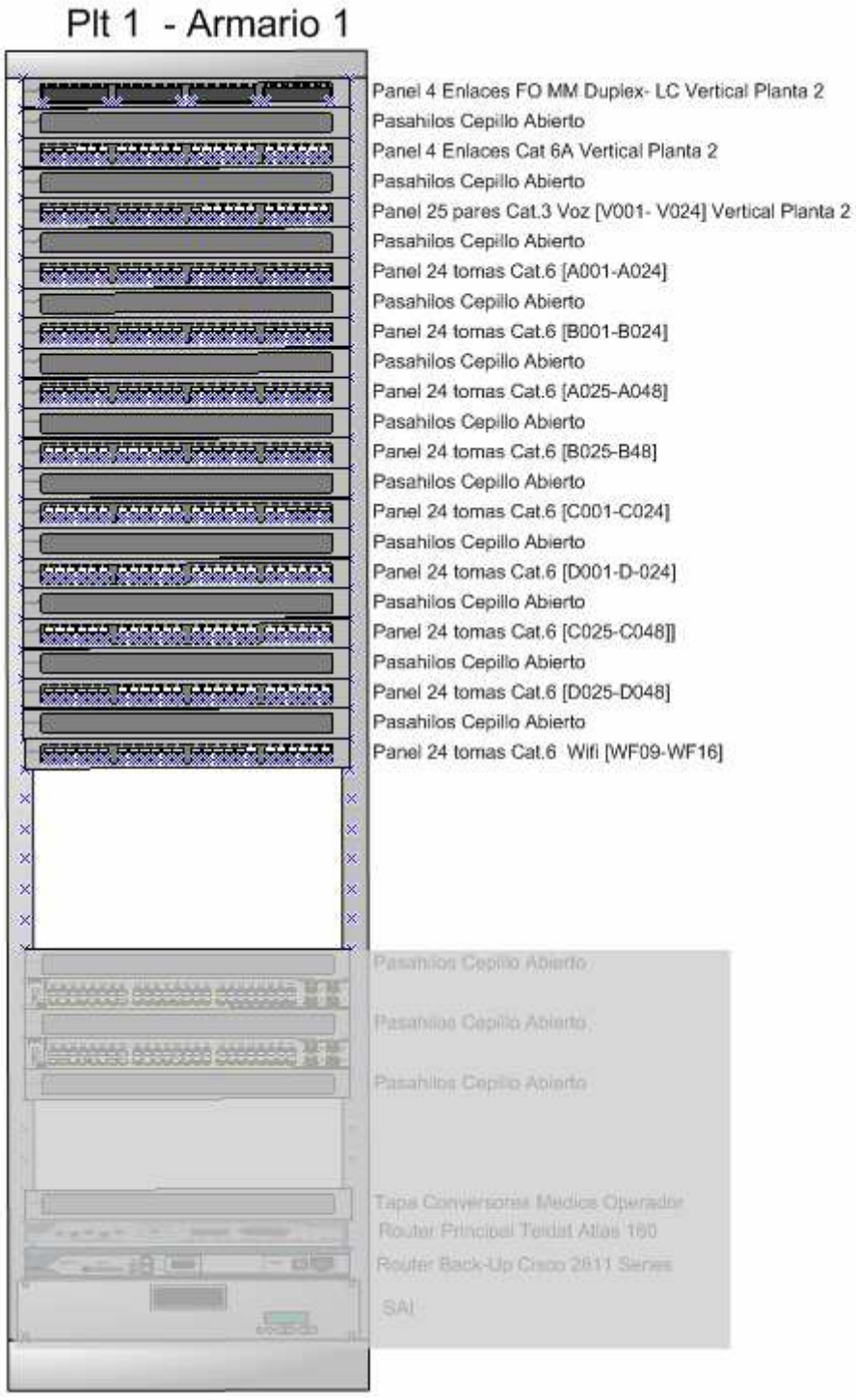


Figura 33 – Layout Frontal Armario Planta 1 Cableado Estructurado

Layout Frontal Armario Planta 2

Debido al alto número de puntos de cableado serán necesarios 2 armarios de 42U de alto para dar cobertura a todos los paneles de cableado estructurado horizontal, vertical y wifi, a la electrónica nivel 2 necesaria y a la electrónica nivel 3.

En uno de los armarios estarán conectadas todas las tomas de cableado etiquetadas como A y B. En el otro armario estarán todas las tomas de cableado etiquetadas como C y D.

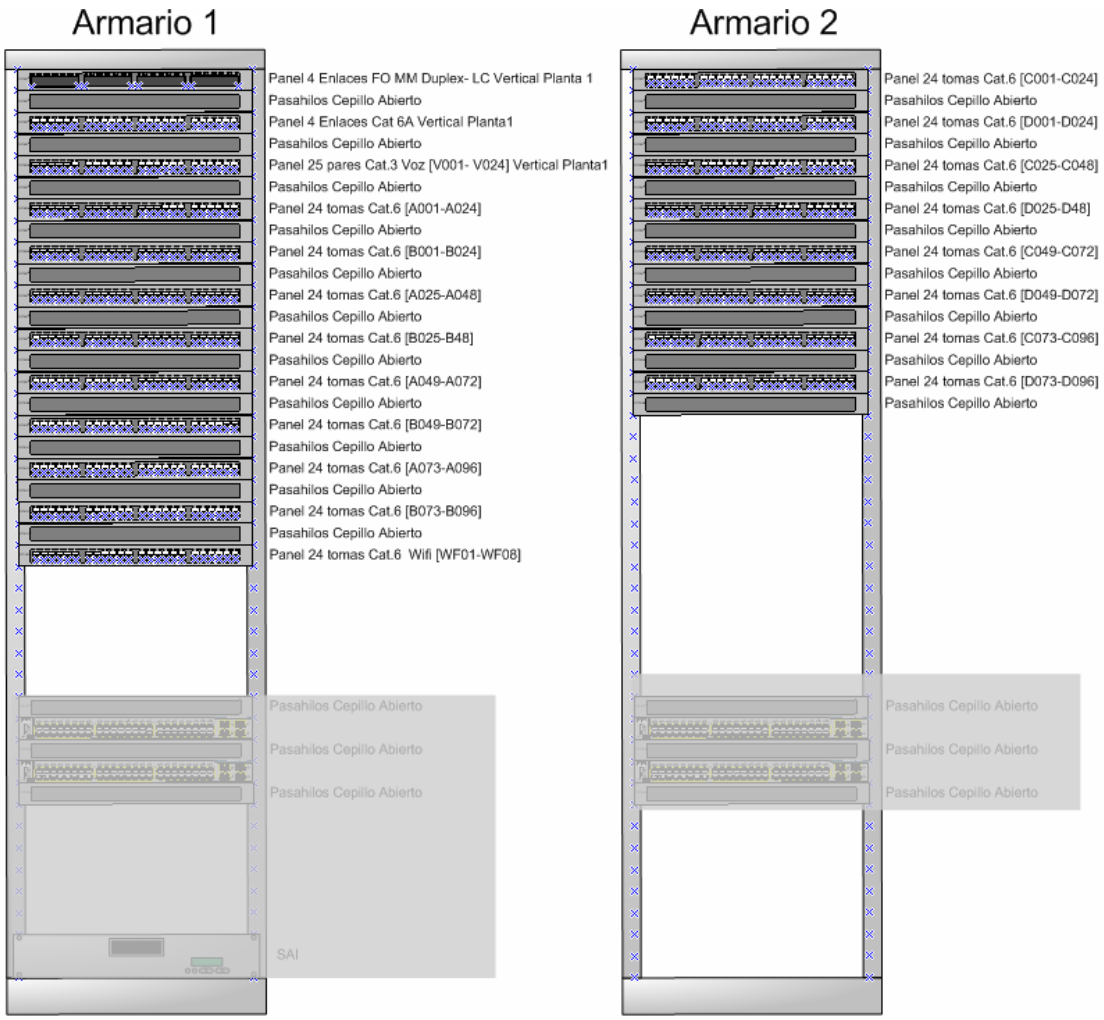


Figura 34- Layout Frontal Armarios Planta 2 Cableado Estructurado

Algunos detalles de los frontales:

- Se aprecia los paneles de interconexión entre plantas de fibra óptica, de cobre categoría 6ª y de cobre categoría 3.

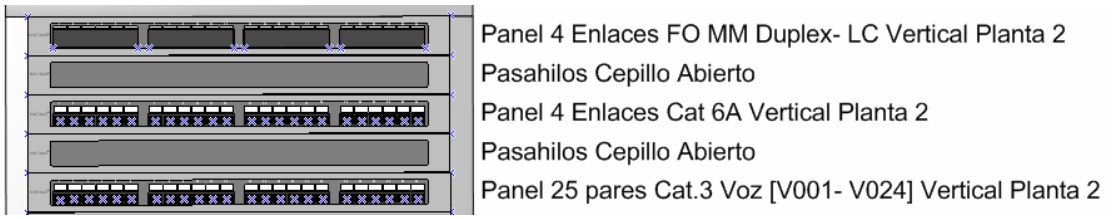


Figura 35 – Detalle Frontal Armario cableado – Subsistema Vertical

- Paneles donde se impactan los puntos de red donde se colocarán los puntos de acceso wifi.

Figura 36- Detalle panel cableado puntos de red para APs Wifi

Layout Distribución Subsistemas Vertical

Mediante este layout se pretende dar una visión en planta del subsistema de cableado vertical. Se puede apreciar los enlaces de cobre (cat 3, y cat 6ª) y el enlace de Fibra óptica OM3, así como la distribución de los puntos de cableado del subsistema horizontal sobre los armarios.

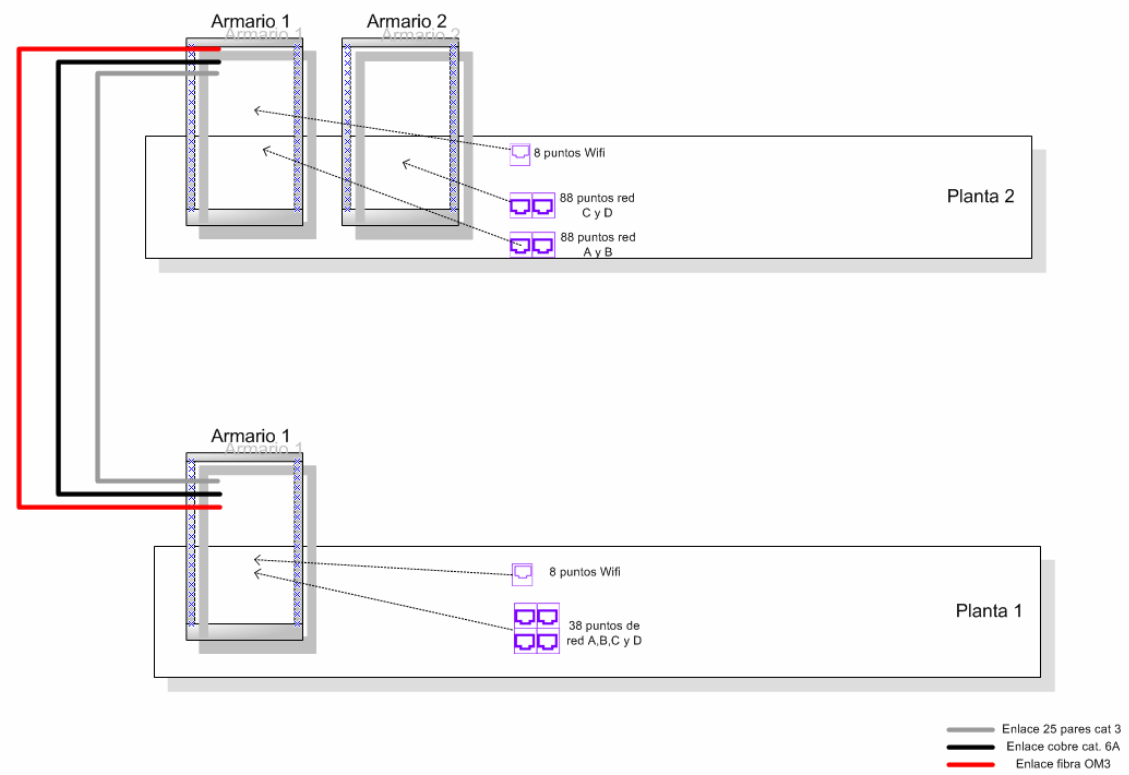


Figura 37 – Layout Distribución Subsistema cableado vertical

1.2.3.3. Planos

La realización de los planos se realiza frecuentemente con programas de diseño de arquitectura (tipo CAD). En concreto para la realización de este proyecto de cableado se ha utilizado AutoDesk Arquitectural Desktop 2007®.

Sin embargo para la visualización de los planos por parte de todo el personal técnico que debe trabar con ellos se utiliza preferentemente el formato Adobe PDF.

Los planos que se van a mostrar a continuación son:

- Plano AutoDesk Planta 1
- Plano AutoDesk Planta 2
- Plano Adobe PDF Planta 1
- Plano Adobe PDF Planta 1
- Layout Frontal Armario Planta 1
- Layout Frontal Armarios Planta 2
- Layout Distribución Subsistema cableado Vertical

Plano AutoDesk Planta 1

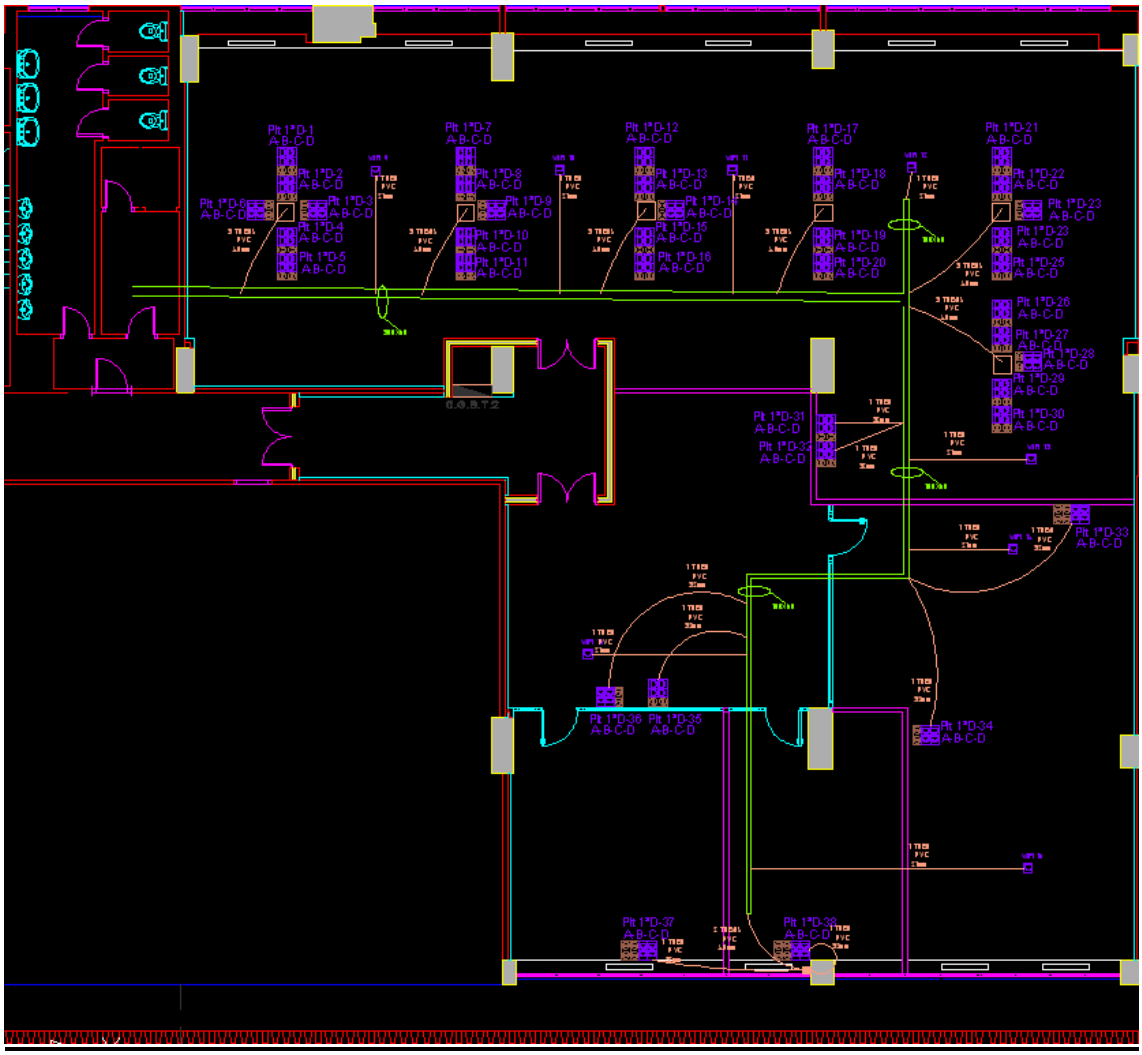


Figura 38 - Plano AutoDesk Planta 1

Plano AutoDesk Planta 2

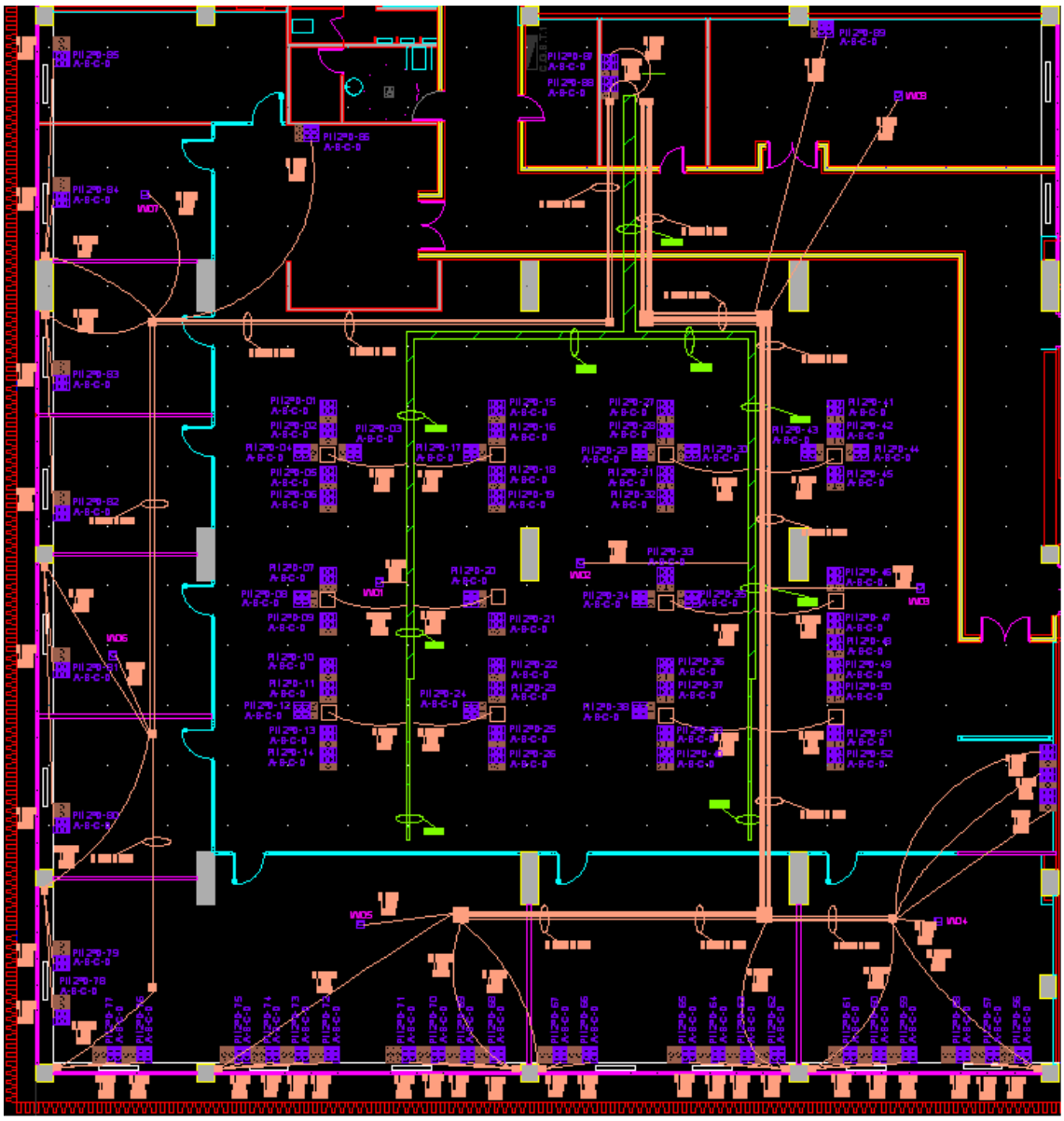


Figura 39 - Plano AutoDesk Planta 2

Plano Adobe PDF Planta 1

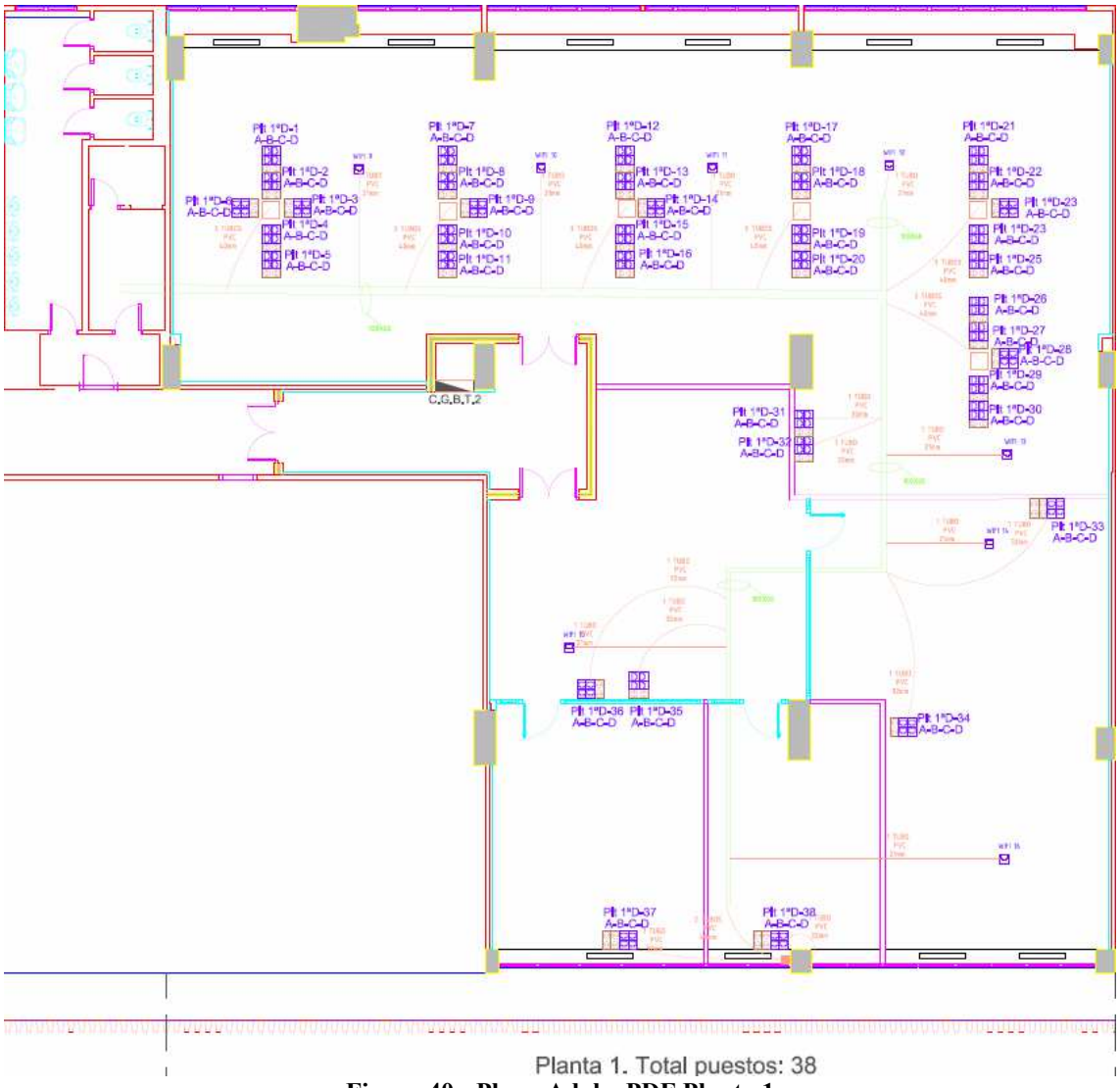


Figura 40 - Plano Adobe PDF Planta 1

Plano Adobe PDF Planta 2

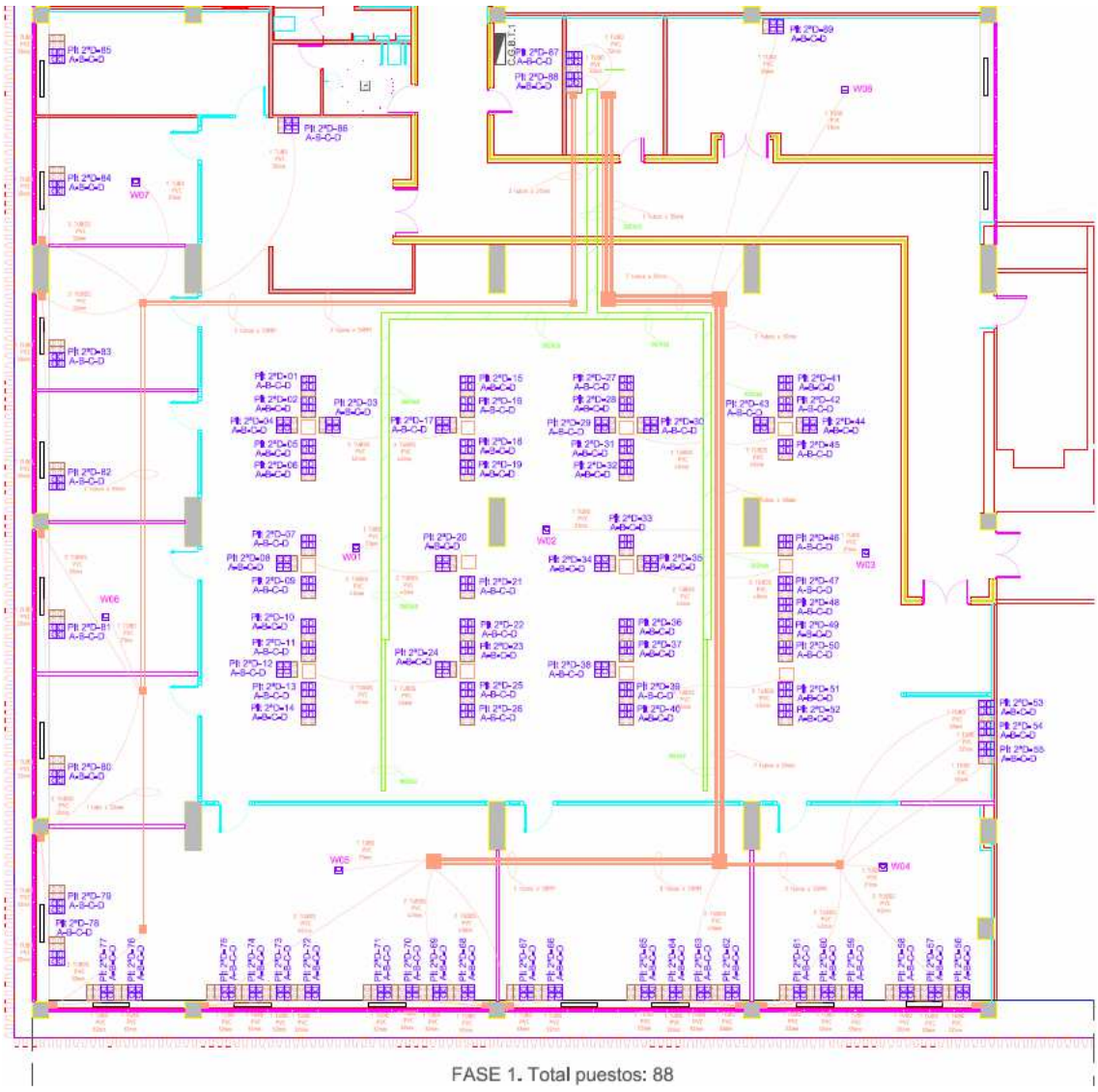


Figura 41- Plano Adobe PDF Planta 2

Layout Frontal Armario Planta 1

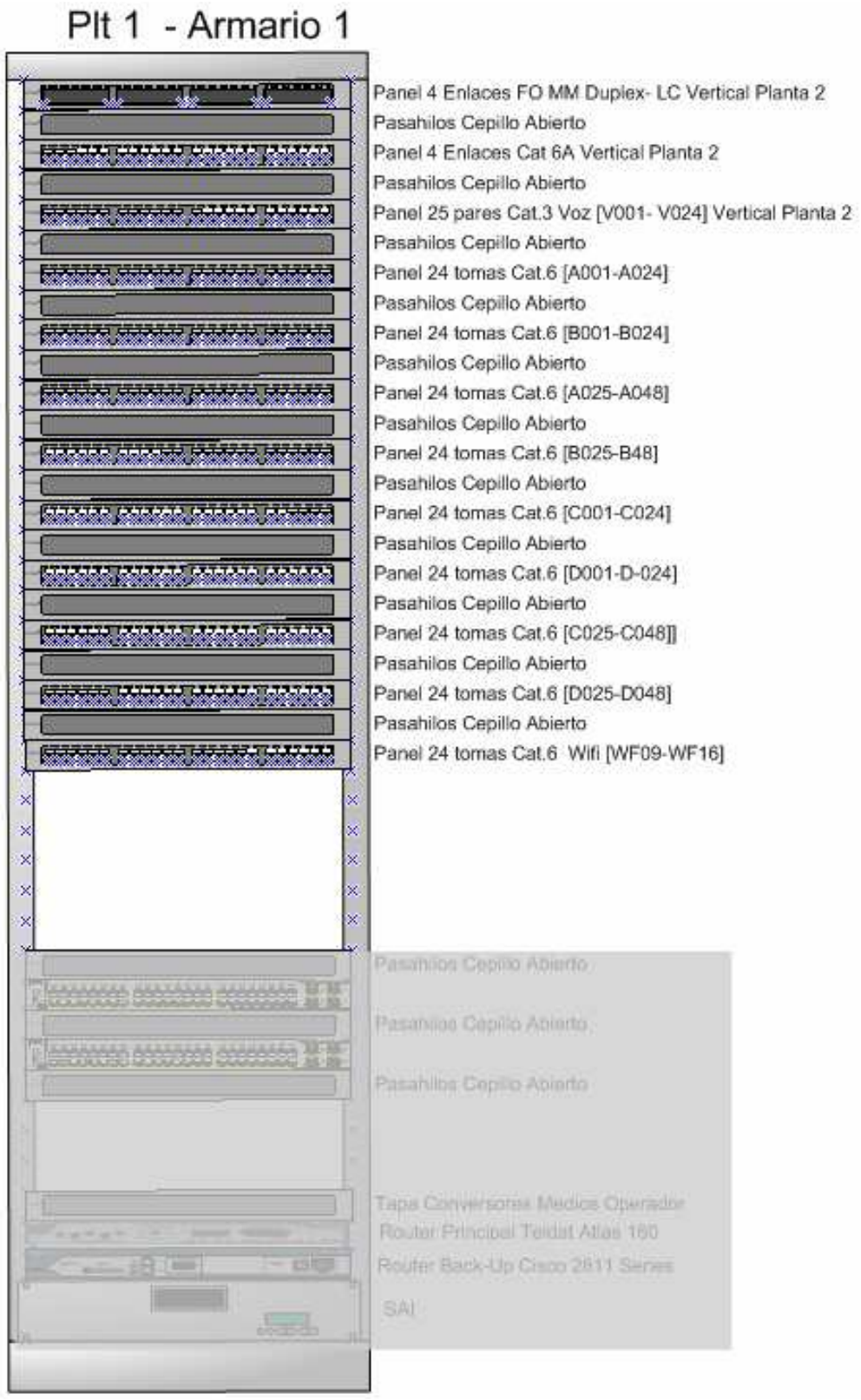


Figura 42- Layout Frontal Armario Planta 1

Layout Frontal Armarios Planta 2

Figura 43 - Layout Frontal Armarios Planta 2

Layout Distribución Subsistema cableado Vertical

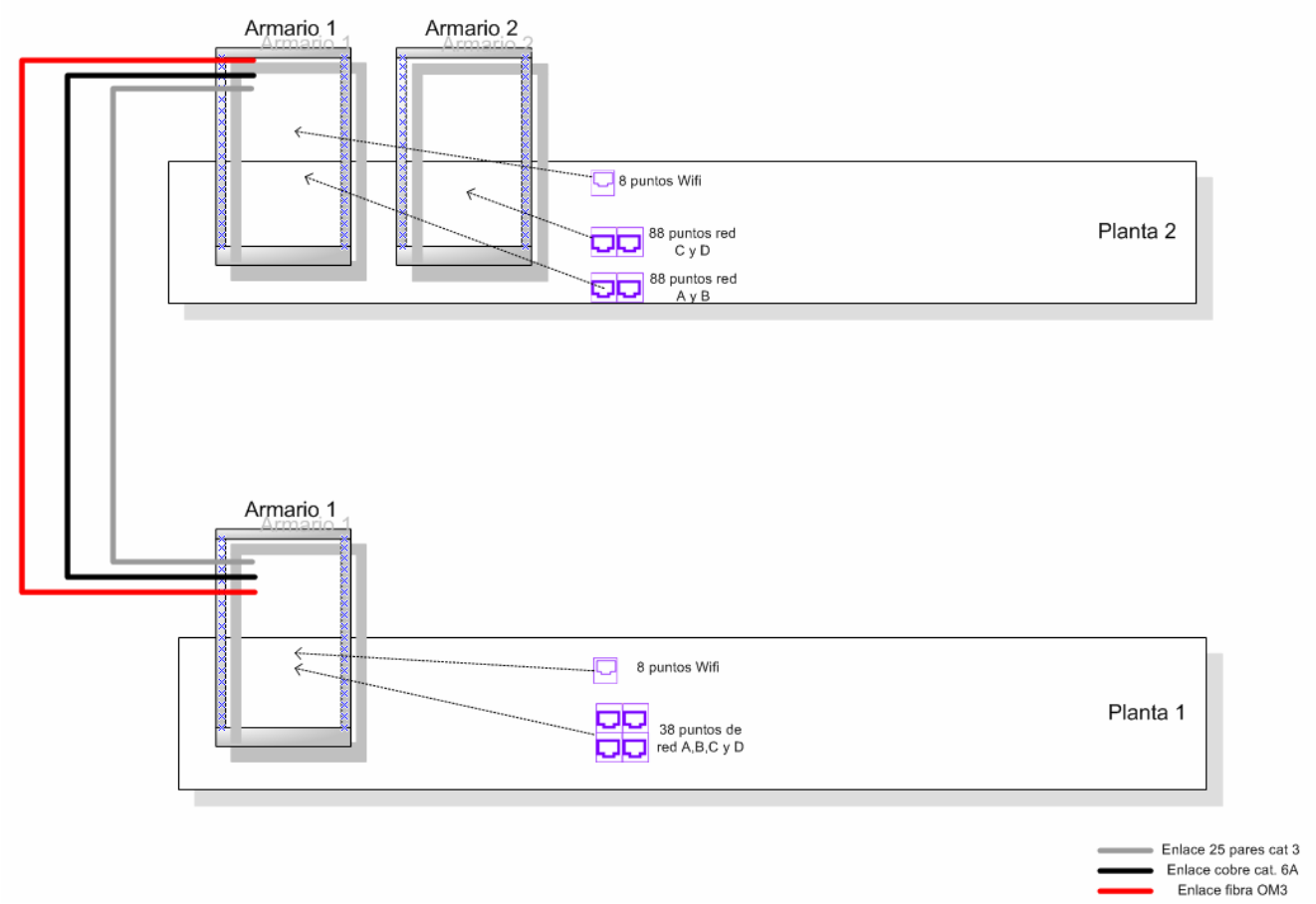


Figura 44- Layout Distribución Subsistema cableado Vertical

1.2.3.4. Certificación instalación

Una de las partes más importantes de cara a verificar la correcta instalación del cableado estructurado es la certificación del mismo. Mediante el proceso de certificación del cableado se comprueban parámetros como:

1. Parámetros primarios (Enlaces):
   - Longitudes (ecometría)
   - Atenuación
   - Atenuación de paradiafonía (NEXT)
   - Relación de Atenuación/Paradiafonía (ACR)
2. Parámetros secundarios
   - Pérdidas de retorno
   - Impedancia característica
   - Resistencia óhmica en continua del enlace
   - Nivel de ruido en el cable
   - Continuidad
   - Continuidad de masa
3. Otros parámetros
   - Capacidad por unidad de longitud (pf/m)
   - Retardo de propagación

Las medidas de certificación se realizan colocando el elemento certificador, uno a uno, en cada uno de los puntos de cableado motivo del estudio de certificación. El certificador tiene dos partes. Una se coloca conectada al panel en el armario repartidor de planta y la otra en la toma de usuario, y se realiza el chequeo de la instalación.

Figura 45 – Certificación Instalación- Colocación certificador

Tras la certificación se obtiene reporte de la misma semejante el mostrado en la siguiente figura:

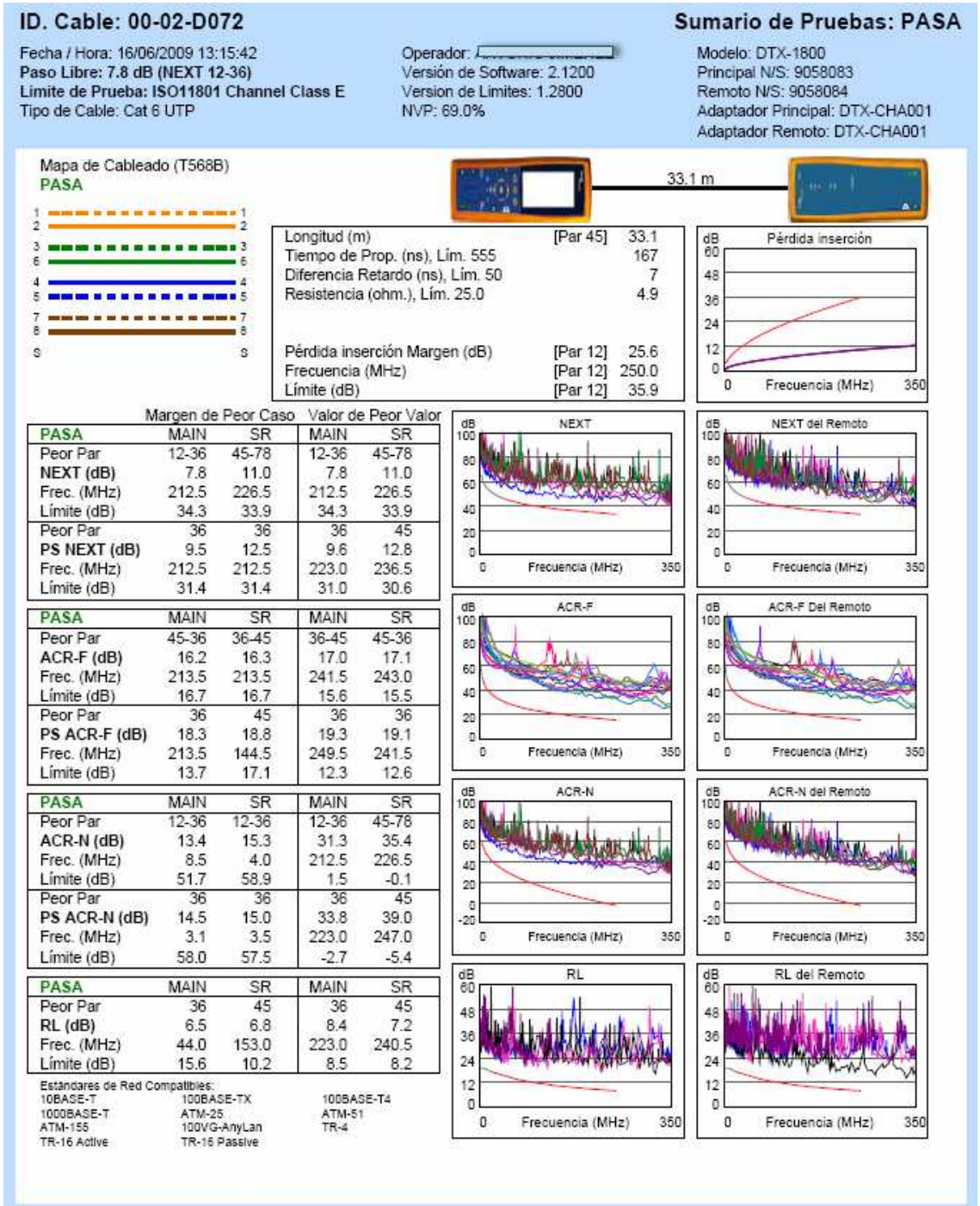


Figura 46 – Reporte de Certificación Punto Cableado

1.3. Infraestructura Capa Acceso

1.3.1. Acercamiento teórico diseño capa 2

Una vez completado el nivel 1 de la arquitectura TCP/IP, es decir, todo lo relacionado con la infraestructura de comunicaciones, vamos a abordar el diseño y configuración del nivel 2, capa de acceso.

El tratamiento de esta parte teórica seguirá el siguiente esquema.

- **Acceso al medio físico**
- **Estándares**
- **Ethernet**
  - Dominios de colisión
  - Segmentación
  - Hub vs Switch
  - Dominio de Broadcast
  - Switch: Spanning-Tree, VLAN, QoS

Acceso al medio Físico

Una de los aspectos destacados para realizar el diseño de la capa de nivel es definir como se va a realiza el acceso al medio físico. Consideraremos una serie de dispositivos conectados (ya se definirá como) al medio físico único (cableado estructurado) y es necesario definir que dispositivo va a acceder al medio físico para transmitir información. Es así como llegamos al concepto de control de acceso al medio, donde se definen básicamente dos categorías:

- Determinísticas (por turnos)
- No determinísticas (el que primero llega transmite)

Figura 47 – Control de acceso al medio [Deterministica , No deterministica]

Los controles determinísticos básicamente se basan en el **denominado paso de testigo**. Este método se emplea cuando la topología de la red es en anillo. Mientras ninguna de las estaciones de la red tenga ningún mensaje que transmitir, circula por el anillo un testigo que es recibido y retransmitido por las estaciones. Con frecuencia el testigo suele ser un byte formado, por ejemplo, por ocho unos (11111111), utilizándose técnicas de relleno de bit para evitar que esta secuencia aparezca en un mensaje.

Cuando una estación quiere transmitir espera recibir el testigo y no lo vuelve a retransmitir, tomando así el control del canal. Puede entonces enviar sus paquetes pendientes de transmisión. Finalizada la transmisión envía nuevamente el testigo. Es, pues, una técnica de transmisión secuencial, impuesta por el orden de conexión física de las estaciones al anillo.

Para reducir el retardo local origen-destino que el proceso de retransmisión del testigo impone en cada estación, se suele efectuar la retransmisión inmediata de cada bit. Cuando una estación quiere transmitir, su módulo de comunicaciones debe retransmitir los 7 primeros bits del testigo e invertir el último, generando así un byte 11111110 que suele denominarse conector o testigo ocupado, e inicia inmediatamente la retransmisión del paquete. De esta forma se consigue que el retardo introducido por cada estación sea de un solo bit, en lugar de los 8 bits de longitud del testigo.

Conforme los bits efectúan una vuelta completa a la red y vuelven a la estación transmisora, ésta puede recibirlos y utilizarlos para comprobar que la transmisión a lo largo de todo el canal ha sido correcta, o descartarlos sin analizarlos (transmisión

sorda). La transmisión se finaliza mandando el testigo a la estación siguiente en el anillo y pasando la estación a modo escucha.

Este método tiene muy buen rendimiento cuando existe un número elevado de estaciones que quieren transmitir.

Los controles **no determinísticos se basan en métodos de contienda**. Existen 3 protocolos de contienda:

- CSMA 1-persistente
- CSMA No persistente
- CSMA/CD ➔ Ethernet

Para mejorar el rendimiento de las redes y evitar en la medida de lo posible las colisiones de tramas, surgen los protocolos de acceso al medio por contienda, más diplomáticos", que antes de transmitir miran si alguien ya lo está haciendo. Esto permite hacer un uso más eficiente del canal y llegar a mayores grados de ocupación, ya que no se interrumpe la transmisión en curso. Estos protocolos se denominan de acceso múltiple con detección de portadora o CSMA (Carrier Sense Multiple Access); la denominación 'detección de portadora' hace referencia a esa consulta previa sobre la ocupación del canal.

En las redes que utilizan estos métodos no se presupone la existencia de estaciones maestras ni esclavas, sino que todas ellas pueden tener el mismo derecho a transmitir.

CSMA 1-persistente

En su forma más simple el protocolo CSMA tiene el siguiente comportamiento: cuando tiene una trama que enviar primero escucha el canal para saber si está libre; si lo está, envía la trama, y en caso contrario espera a que se libere y en ese momento la envía. Este protocolo se denomina CSMA 1-persistente porque hay una probabilidad 1 (es decir certeza) de que la trama se transmita cuando el canal esté libre.

En una situación real con tráfico intenso es muy posible que cuando un ordenador termine de transmitir haya varios esperando para enviar su trama: con CSMA 1- persistente todas esas tramas serán emitidas a la vez y colisionarán. Este proceso puede repetirse varias veces con la consiguiente degradación del rendimiento.

A pesar de este inconveniente el CSMA 1-persistente supone un avance respecto al ALOHA ranurado, ya que toma la precaución de averiguar antes si el canal está disponible, con lo que se evitan un buen número de colisiones.

CSMA no persistente

En un intento por resolver el problema de colisiones de CSMA 1-persistente se puede adoptar la estrategia siguiente: si el canal está ocupado la estación, en vez de permanecer a la escucha pendiente de usarlo en cuanto se libere, espera un tiempo aleatorio después del cual repite el proceso de escucha. A este protocolo se le denomina CSMA no persistente.

Este protocolo tiene una menor eficiencia que CSMA 1-persistente para tráficos moderados, pues introduce una mayor latencia; sin embargo se comporta mejor

en situaciones de tráfico intenso ya que se evita la concentración de demandas-colisiones cuando el canal pasa de ocupado a libre.

CSMA con detección de colisión (CSMA/CD)

En los protocolos que hemos descrito hasta ahora una vez se había empezado a transmitir una trama el ordenador sigue transmitiendo aun cuando se detecte una colisión. En ese caso sería lógico y más eficiente parar de transmitir, ya que la trama será errónea e inútil. Esta mejora es la que incorporan los protocolos conocidos como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, acceso multiple por detección de portadora con detección de colisiones) que se utiliza en la red local IEEE 802.3, también conocida como Ethernet.

El funcionamiento de CSMA/CD es el siguiente:

- Cuando un nodo tiene un mensaje a transmitir escucha previamente el canal, y si está libre procede a su transmisión.
- Dado que dos o más nodos pueden haber comenzado a transmitir a la vez, o con una diferencia de tiempo lo bastante pequeña como para que la señal de uno no haya podido llegar al otro antes de que éste empiece a transmitir, existe riesgo de que se produzca colisión. Para resolver el conflicto todo nodo que transmite continúa escuchando la red mientras transmite. Cuando detecta una colisión por un cambio en el nivel de energía del canal, interrumpe la transmisión y espera un tiempo aleatorio de pocos microsegundos para intentar de nuevo el acceso.

Dado que en estas redes el tamaño de la trama es variable, para que CSMA/CD funcione correctamente es necesario que se detecte la colisión antes de que se complete la emisión de la trama mínima, cuyo tamaño es de 64 bytes. Este hecho comporta, pues, una limitación en la longitud que puede tener el medio compartido, que se ilustra en el ejemplo siguiente.

Suponiendo dos ordenadores A y B situados en extremos opuestos de la red y que la señal tarda un tiempo τ en propagarse de uno a otro extremo a otro. En el caso más desfavorable, B podría haber empezado a transmitir justo en el instante $\tau-\varepsilon$, o sea inmediatamente antes de que le haya llegado la trama de A; por lo que sólo después de un tiempo 2τ puede A estar seguro de que no ha colisionado con ninguna otra estación, y que por tanto se ha "apoderado" del canal de transmisión.

Dado que el emisor debe estar escuchando de manera continua el canal para detectar las posibles colisiones, la comunicación en redes basadas en CSMA/CD es necesariamente semi-dúplex. Esta limitación desaparece con la microsegmentación en redes Ethernet, en las que cada estación tiene el medio de transmisión para su uso exclusivo y por tanto pueden abandonar el esquema CSMA/CD y realizar comunicaciones full-dúplex (esto se ve en mayor detalle en el tema dedicado a la interconexión de redes de área local).

La siguiente figura ilustra el funcionamiento del CSMA/CD

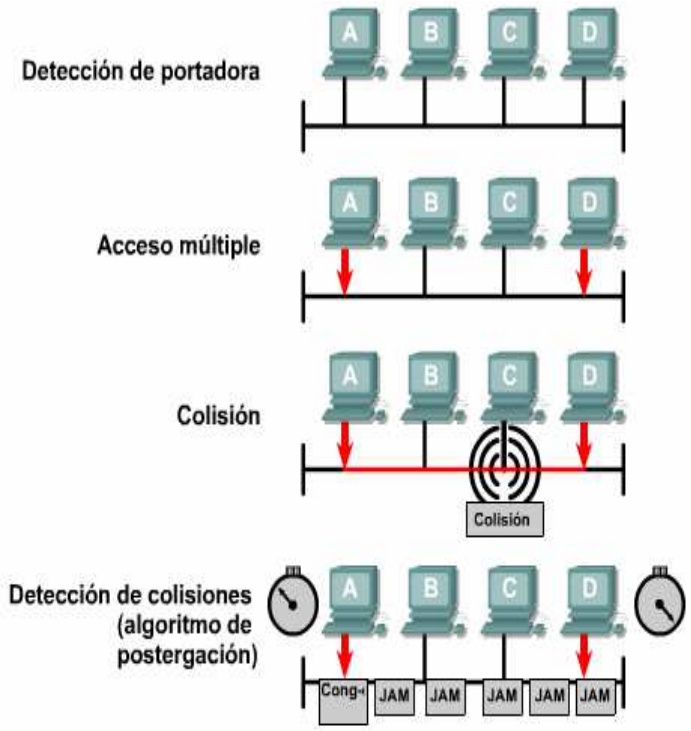


Figura 48- Control de acceso al medio – CSMA/CD

Estándares

Los estándares de referencia relativos al funcionamiento de la capa de acceso están recogidos por el IEEE dentro de la familia de estándares 802.xx

Los más destacados son los siguientes:

- 802.1: protocolos LAN de nivel superior
- 802.3: Ethernet
- 802.5: Token ring
- 802.11: WLAN

- 802.1D: STP
- 802.1P/Q: VLANs/QoS

- 802.3ae: agregación de enlaces
- 802.3af: alimentación sobre Ethernet
- 802.3x: full duplex y control de flujo
- 802.3z: 1 Gbit/s sobre fibra óptica.
- 802.3ab: 1 Gbit/s sobre par trenzado no blindado
- 802.3an: 10 Gbit/s sobre par trenzado no blindado (UTP)

Los estándares 802.3, 802.1D y 802.1P/Q será tratados con detalle en posteriores capítulos.

Ethernet

Desde su comienzo en la década de 1970, Ethernet ha evolucionado para satisfacer la creciente demanda de LAN de alta velocidad. En el momento en que aparece un nuevo medio, como la fibra óptica, Ethernet se adapta para sacar ventaja de un ancho de banda superior y de un menor índice de errores que la fibra ofrece.

El éxito de Ethernet se debe a los siguientes factores:

- Sencillez y facilidad de mantenimiento.
- Capacidad para incorporar nuevas tecnologías.
- Confiabilidad
- Bajo costo de instalación y de actualización.

Es la tecnología de capa 2 mas extendida, está basada en el protocolo de contención CSMA/CD.

A partir de este momento se asimilará el concepto LAN al de Ethernet, al ser Ethernet la tecnología de capa 2 mas extendida para el diseño de Redes de Area Local (LAN).

La representación por tanto de una red Ethernet se realiza de la siguiente forma:

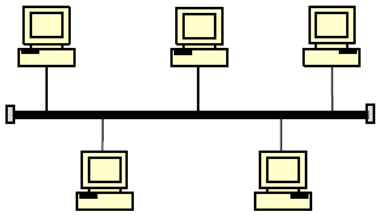


Figura 49- Ethernet – Topología Lógica

Pero en realidad, ¿una red Ethernet es un cable?, es decir, la topología física de la red es un cable a modo de bus. La respuesta es no.

La topología física de una red Ethernet es una estrella donde existen una serie de dispositivos donde se concentran las conexiones de todos los elementos que se conecten a ella.

La topología física real de una red Ethernet se representa en la siguiente figura:

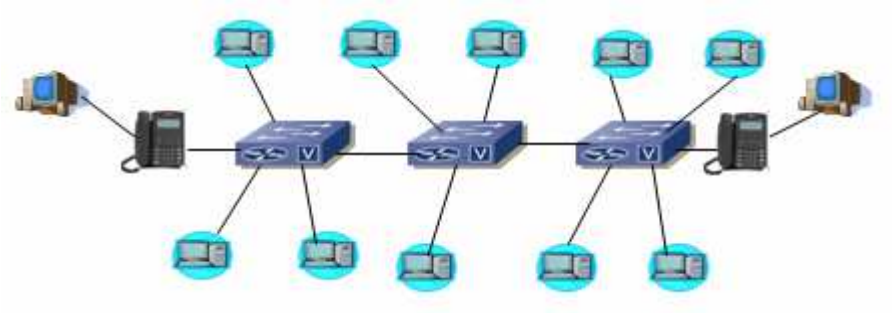


Figura 50- Ethernet – Topología Física

Los dispositivos de nivel 2 que se utilizan habitualmente son los siguientes:

- HUB: El pasado (aun se utilizan)
- Switch: El presente

Dominio de Colisión

Los nodos Ethernet utilizan CSMA/CD acceso múltiple con detección de portadora y detección de colisiones (carrier sense multiple access with collision detection). (Escuchar antes de Transmitir). Cada nodo debe disputar con otros nodos para acceder al medio compartido o al dominio de colisión. Si dos nodos transmiten al mismo tiempo, se produce una colisión. Cuando se produce una colisión la trama transmitida se elimina y se envía una señal de embotellamiento a todos los nodos del segmento. Los nodos esperan un período de tiempo al azar y luego vuelven a enviar los datos. Las colisiones excesivas pueden reducir el ancho de banda disponible de un segmento de red a treinta y cinco o cuarenta por ciento del ancho de banda disponible

Por tanto es necesario intentar que los dominios de colisión sean lo más pequeños posibles.

Figura 51- Dominios de Colisión

HUB: es un dispositivo de red que permite la interconexión de los distintos terminales que se comunican en una red Ethernet. Tiene una serie de puertos de interconexión, y básicamente lo que haces es repetir eléctricamente la señal que recibe en un puerto por todos los puertos que tiene conectado. Es decir, la comunicación entre todos los dispositivos está basada en la inundación. Las velocidades de transmisión son bajas (10Mbps) y operan en modo half-duplex.

Este modo de funcionamiento hace que cada HUB sea un dominio de colisión único, es decir, todos los dispositivos *compiten* por el acceso al medio, lo que provoca continuas colisiones.

En la siguiente figura se aprecia el funcionamiento de un HUB con 4 terminales conectados.

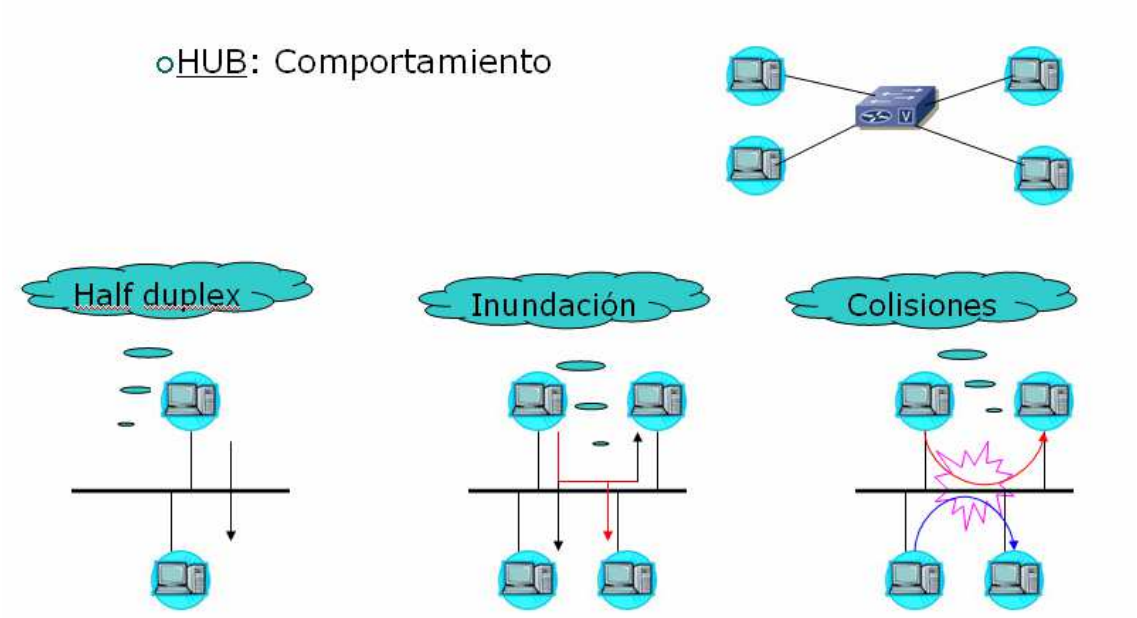


Figura 52- Colisiones en un HUB

Por tanto, derivado del echo de que los dominios de colisión deben de ser lo más pequeños posibles, surge el concepto de segmentación. La segmentación se realiza cuando un sólo dominio de colisión se divide en dominios de colisión más pequeños.

Segmentación

La segmentación se realiza cuando un sólo dominio de colisión se divide en dominios de colisión más pequeños. Los dominios de colisión más pequeños reducen la cantidad de colisiones en un segmento LAN y permiten una mayor utilización del ancho de banda.

Los dispositivos de la Capa 2 como por ejemplo switches se pueden utilizar para segmentar una LAN.

Switch: es un dispositivo de red que permite la interconexión de los distintos terminales que se comunican en una red Ethernet. Las características mas destacadas de estos dispositivos son:

- Los switches proporcionan conexiones a estaciones individuales, servidores, segmentos de red, troncales u otros conmutadores
- Proporciona mayor densidad de puertos a menor coste que los tradicionales hubs
- Proporcionan puertos de alta velocidad (10/100/1000-Mbps Ethernet / Fast Ethernet, Gb)
- Proporcionan ancho de banda dedicado por puerto (10/100/1000-Mbps)
- Proporcionan Segmentación. Cada uno de los puertos de un switch se convierte en un dominio de colisión único.
- Cada usuario recibe acceso instantáneo al ancho de banda asignado y no tiene que competir por el ancho de banda disponible con otros usuarios- Por tanto no se producen colisiones
- La comunicación full-duplex (enviar y recibir al mismo tiempo) dobla el ancho de banda permitido
- Las comunicaciones dedicadas entre dispositivos de red, libres de colisiones, incrementan la rapidez de operaciones tediosas como las transferencias de ficheros
- Admiten nuevas funcionalidades: gestión remota del dispositivo, creación y gestión de vlan, aplicación de QoS [Calidad de Servicio], algunos implementan funcionalidades incluso de capa 3.

En la siguiente figura se aprecia el funcionamiento de un Switch.

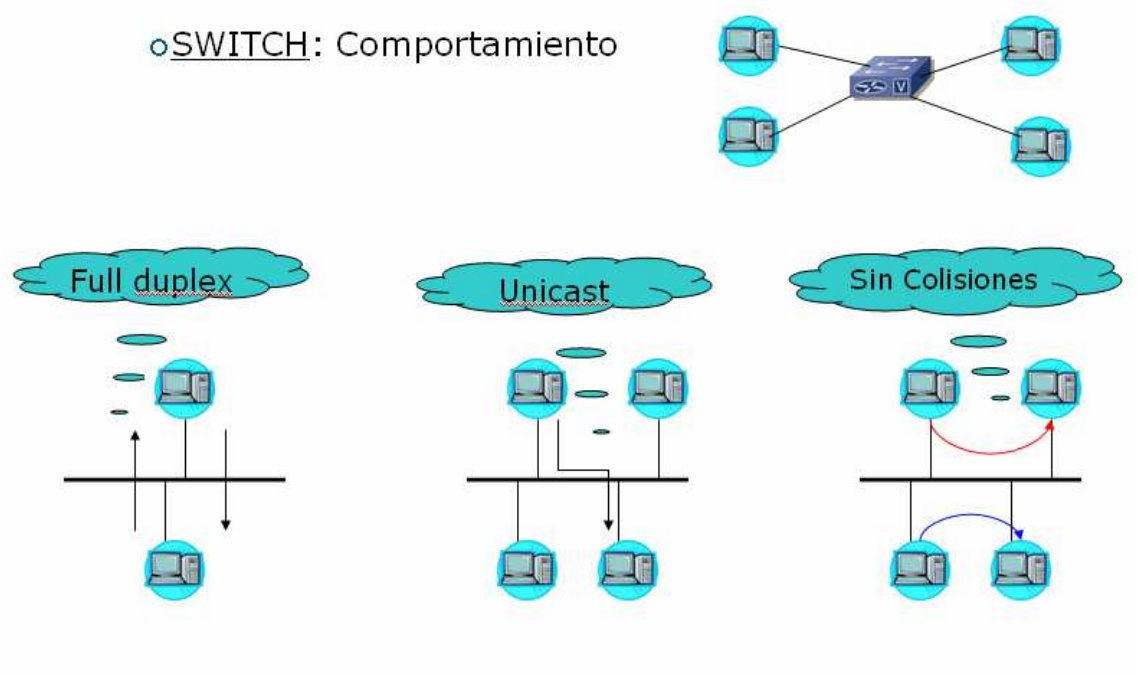


Figura 53 - Funcionamiento Switch sin colisiones

HUB vs Switch

Por todo lo expuesto anteriormente, es evidente que la utilización de switches en la redes Ethernet hace que desaparezcan las colisiones, y por tanto se incremente el ancho de banda efectivo.

Además permite la utilización del modo de transmisión full-duplex, lo que nos permite duplicar el ancho de banda efectivo, y añade funcionalidades adicionales.

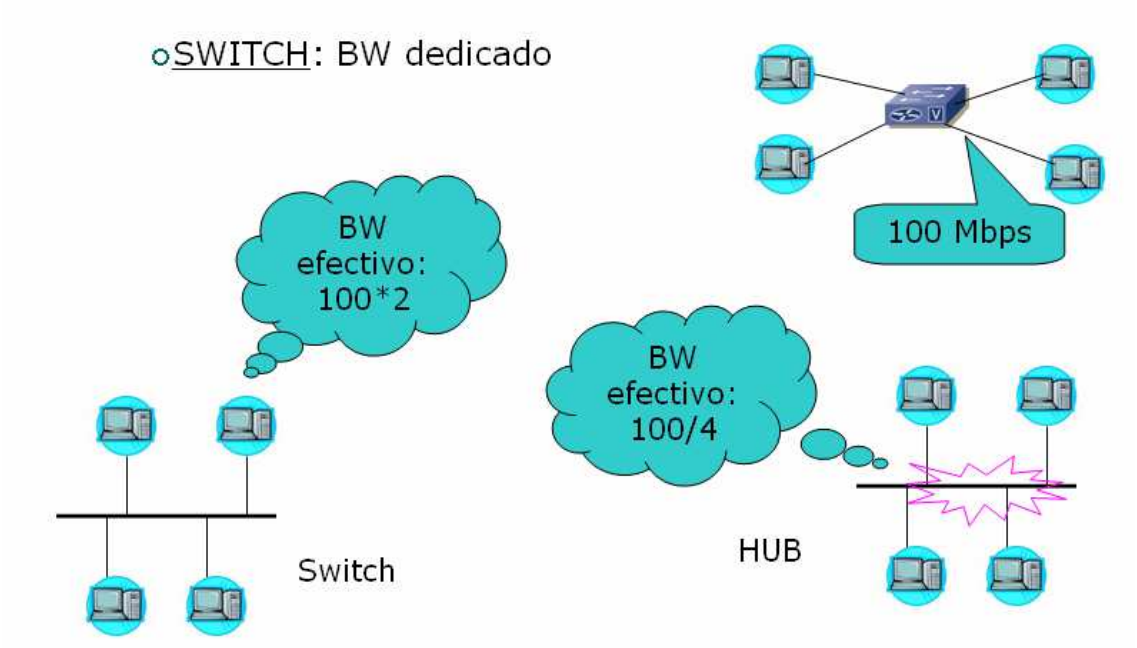


Figura 54- Hub vs Switch

Dominio de Broadcast

Se produce un broadcast cuando el control de acceso al medio destino (MAC) se configura en FF-FF-FF-FF-FF-FF. Un dominio de broadcast se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. Todos los hosts que reciben una trama de datos de broadcast deben procesarla. Este proceso consume los recursos y el ancho de banda disponible del host. Los dispositivos de Capa 2 como los switches reducen el tamaño de un dominio de colisión. Estos dispositivos no reducen el tamaño del dominio de broadcast. Los routers reducen el tamaño del dominio de colisión y el tamaño del dominio de broadcast en la Capa 3.

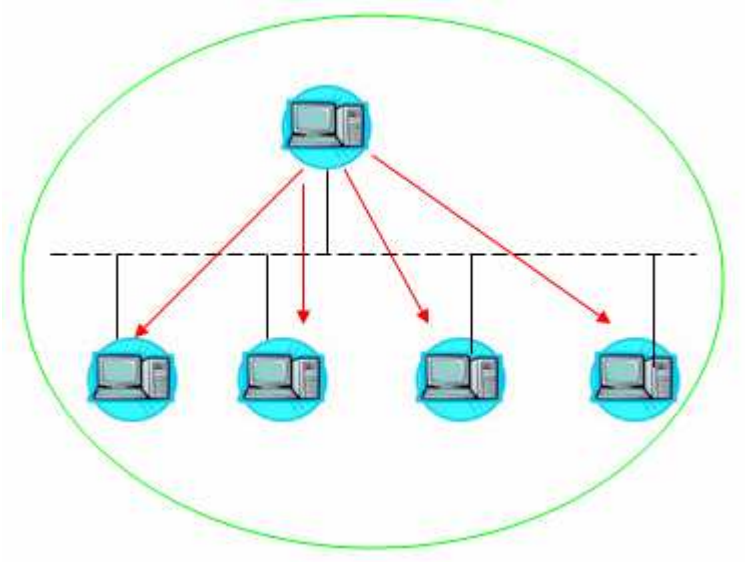


Figura 55 – Dominio de Broadcast Ethernet

Es decir, los switches no reducen el tamaño de un dominio de broadcast, a priori. Los únicos dispositivos que reducen los dominios de broadcast, a priori, son los dispositivos de nivel 3, básicamente los routers.

Comentamos que, a priori, los switches no reducen el dominio de broadcast, pero realmente esta afirmación no es del todo cierta. Se verá más adelante cuando se trate el tema de las LANs virtuales (VLANs), cuando veamos que realmente un dominio de broadcast está confinado en cada vlan.

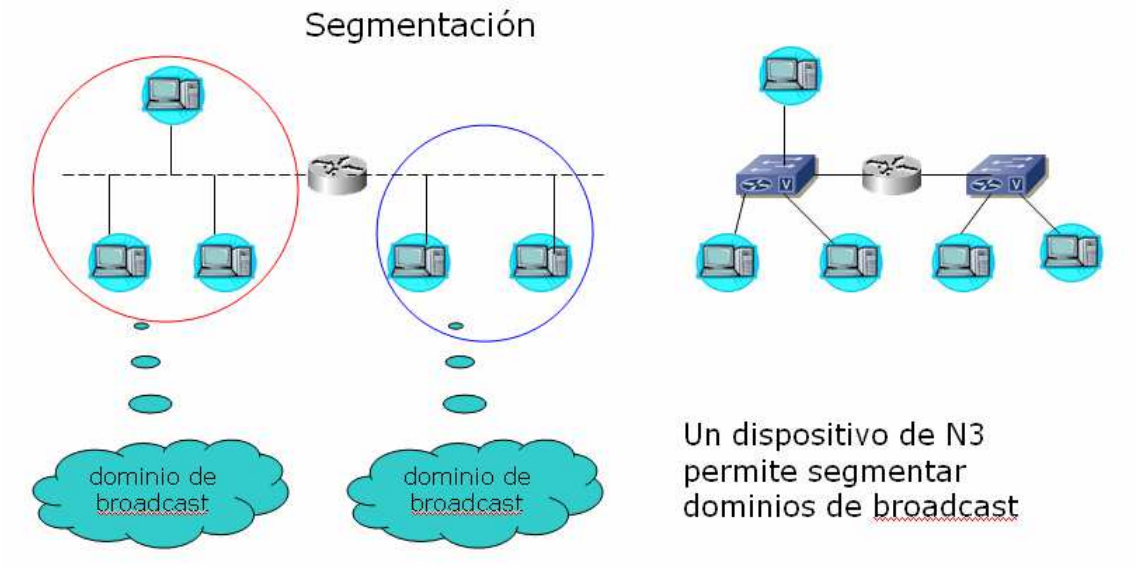


Figura 56- Segmentación de un dominio de Broadcast

Pero, ¿cómo funciona un switch?. Realmente el switch escucha en modo promiscuo por todos los puertos, de forma que va aprendiendo que MACs tiene "visibles" en cada puerto. A medida que va identificando MACs y puertos va guardando esta información en las denominadas tablas de MACs, de forma que los envíos dejan de ser a todos los puertos para pasar a ser al puerto donde se encuentra la dirección MAC en concreto

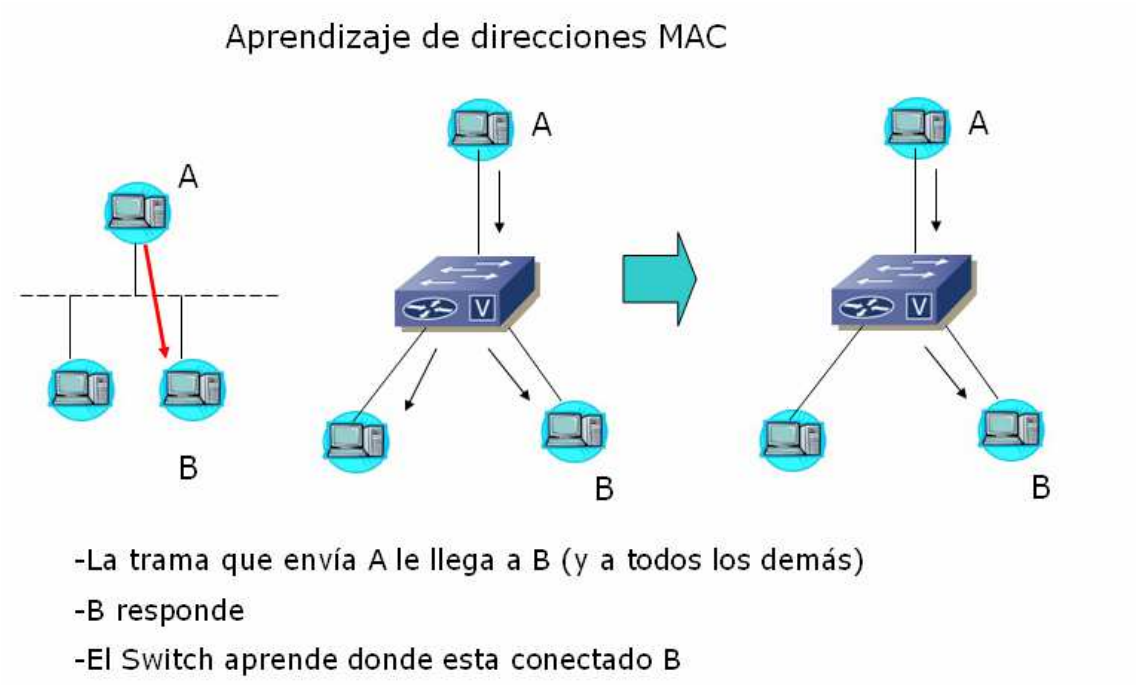


Figura 57 – Modo funcionamiento switch

Este mecanismo se denomina Conmutación de tramas, y los switches tienen distinta forma de realizarlos:

A diferencia de los puentes, un conmutador no requiere leer la trama completa, basta con la dirección destino, logrando así una baja latencia. Según la manera en que procese las tramas, entonces, podemos distinguir las siguientes formas de conmutación de tramas:

• **Almacenamiento y reenvío**: El conmutador recibe la trama en su totalidad, comprueba el CRC y la retransmite si es correcta (si no la descarta). La ventaja de este sistema es que previene del uso ineficiente de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa la latencia del conmutador. En el caso de tramas grandes el requerimiento de comprobación del CRC introduce un retardo notable en la propagación de la trama, a menudo superior al que introduce el propio proceso de conmutación; además si la trama ha de atravesar varios conmutadores el almacenamiento y reenvío se ha de realizar en cada uno de ellos.

• **Cut-through** (Cortar-Continuar): El conmutador empieza retransmitir la trama tan pronto ha leído la dirección de destino (6 primeros bytes). De esta forma se consigue una menor latencia que en el caso anterior. El efecto negativo es que, aunque el CRC sea erróneo, la trama se retransmite. En este caso las tramas erróneas serán descartadas por el host de destino, por lo que no hay riesgo de que se interpreten como correctos datos erróneos, pero aun así la situación es perjudicial para la red puesto que se esta ocupando ancho de banda con tráfico inútil. Así, este modo de funcionamiento es indicado para redes con poca latencia de errores.

• **Cut-through libre de fragmentos**: su modo de funcionamiento es similar al de Cut-through, con la salvedad de que espera a haber recibido 64 bytes antes de comenzar a retransmitir la trama. Así se asegura que no es un fragmento de colisión.

• **Híbrido**: Este conmutador normalmente opera como cut-through, pero siguen comprobando el CRC, y monitoriza constantemente la frecuencia a la que una estación envía tramas inválidas o dañadas. Si este valor supera un umbral prefijado el conmutador pasa a modo almacenamiento/reenvío para las tramas que vienen de esa dirección MAC. Si desciende este nivel se pasa al modo inicial.

Esta forma de proceder se basa en la hipótesis de que una estación que genera tramas correctas tiene una alta probabilidad de seguir generando tramas correctas, mientras que una que genera tramas erróneas, normalmente por algún problema de tipo físico, tendrá una probabilidad mayor de seguir generando tramas erróneas.

Switch – Otras Funcionalidades

Repasaremos ahora algunas funcionalidades adicionales que nos aporta la utilización de switches como mecanismo de conmutación de tramas de nivel 2. Son las siguientes:

- Full duplex
- Control de flujo
- Auto negociación
- Agregación de enlaces
- Topologías redundantes - STP
- VLANs

Full-Duplex

Se refiere al modo de conexión entre el switch y los distintos dispositivos de red que se conectan a cada uno de sus puertos. Mediante el modo de conexión Full-Duplex se permite que por el puerto se pueda enviar y recibir información a la vez, sin riesgo de colisión de la misma.

Asociado al modo de conexión se encuentra la velocidad de conexión. Actualmente los switches de acceso varían en velocidades de 100 Mbps, 1000 Mbps, 10Gbps.

Control de Flujo

Junto con el funcionamiento full dúplex, el grupo de trabajo IEEE 802.3x incluyó además una nueva funcionalidad, el **control de flujo**, para evitar que se produjeran desbordamientos de los buffers del receptor debido a que múltiples estaciones intenten comunicar con él durante un espacio de tiempo significativo. Este control de flujo se implementa mediante el comando PAUSE, en el cual el receptor le indica al emisor por cuánto tiempo debe dejar de enviarle datos. Durante ese tiempo el receptor puede enviar nuevos comandos PAUSE prolongando, reduciendo o suprimiendo la pausa inicialmente anunciada.

Auto negociación

Cuando un equipo de conecta a uno de los puertos del switch envía unas señales anunciando sus posibilidades, de acuerdo con un protocolo especial.

Esto les permite 'negociar' y funcionar de la forma compatible más eficiente posible.

A veces, es necesario realizar acciones manuales para "forzar" los parámetros de la transmisión (modo y velocidad de conexión) para evitar incoherencias. Una mala autonegociación puede producir multitud de errores de transmisión

Agregación de enlaces

La agregación de enlaces, también llamada trunking o multiplexado inverso, consiste en la utilización de varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, realizando reparto del tráfico entre ellos. Hoy en día esta funcionalidad es ofrecida por multitud de fabricantes para todas las velocidades de Ethernet.

La agregación de enlaces requiere deshabilitar el Spanning Tree entre los enlaces que se agregan, para así poder repartir el tráfico entre ellos. Los enlaces han de ser todos de la misma velocidad.

Además de permitir acceder a capacidades superiores cuando no es posible cambiar de velocidad por algún motivo, la agregación de enlaces permite un crecimiento gradual a medida que se requiere, sin necesidad de cambios traumáticos en las interfaces de red o en la infraestructura. Aunque existen en el mercado productos que permiten agregar hasta 32 enlaces full dúplex, parece que cuatro es un límite razonable, ya que al aumentar el número de enlaces la eficiencia disminuye, y por otro lado el coste de las interfaces aconseja entonces pasar a la velocidad superior en vez de agregar enlaces.

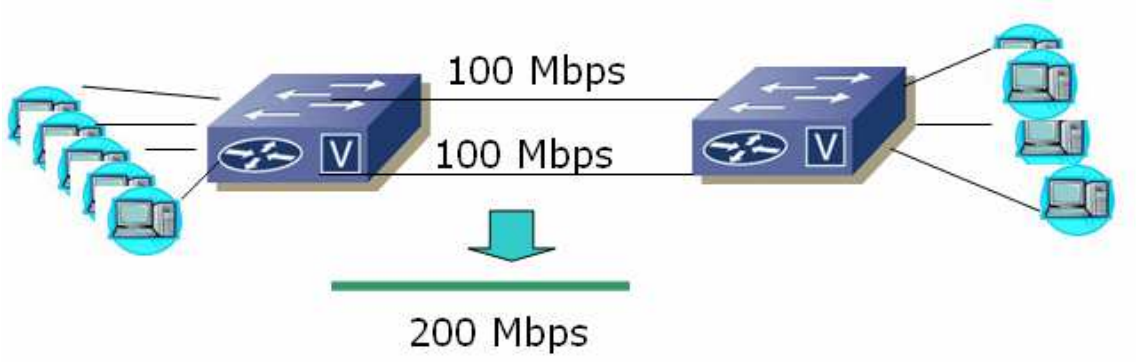


Figura 58 – Agregación enlaces switch

Topologías Redundantes – STP

La fiabilidad es una característica fundamental de una red. A medida que las redes crecen y se hacen más complejas por medio de interconexiones cada vez más extendidas, resulta imprescindible introducir redundancia para aumentar la fiabilidad y minimizar los tiempos de indisponibilidad.

El problema de las topologías redundantes basadas en puentes o en conmutadores que son vulnerables a las tormentas de broadcast, retransmisiones innecesarias de tramas y problemas de estabilidad en el aprendizaje de direcciones físicas por parte de los dispositivos de red.

Así pues, añadir redundancia requiere de una cuidadosa planificación y una posterior monitorización para garantizar su adecuado funcionamiento.

Esto es especialmente importante cuando las redes crecen por medio de interconexiones de redes más pequeñas. Un pequeño bucle en una red aislada puede provocar la caída de la red entera si no se controla adecuadamente.

Para resolver el problema de los bucles físicos, los fabricantes de dispositivos de red introdujeron en sus dispositivos el uso del Spanning Tree Protocol (STP). Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes. El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión de forma transparente a las estaciones de usuario, de forma que se garantice que la topología está libre de lazos.

STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle. Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva.

El intercambio entre dispositivos de la información necesaria para crear los árboles de expansión se realiza mediante tramas de datos especiales denominadas BPDUs (Bridge Protocol Data Units).

Este protocolo fue estandarizado por el IEEE dentro de las especificaciones 802.1D, aunque en la revisión de 2004 se declaró obsoleto y ha sido sustituido por el Rapid Spanning Tree Protocol (RSTP). La diferencia fundamental frente al anterior estriba en que RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología. Además, aumenta drásticamente el número de puertos interconectados que permite (2048 conexiones o 4096 puertos interconectados en comparación con 256 puertos conectados en STP), al tiempo que mantiene compatibilidad con STP.

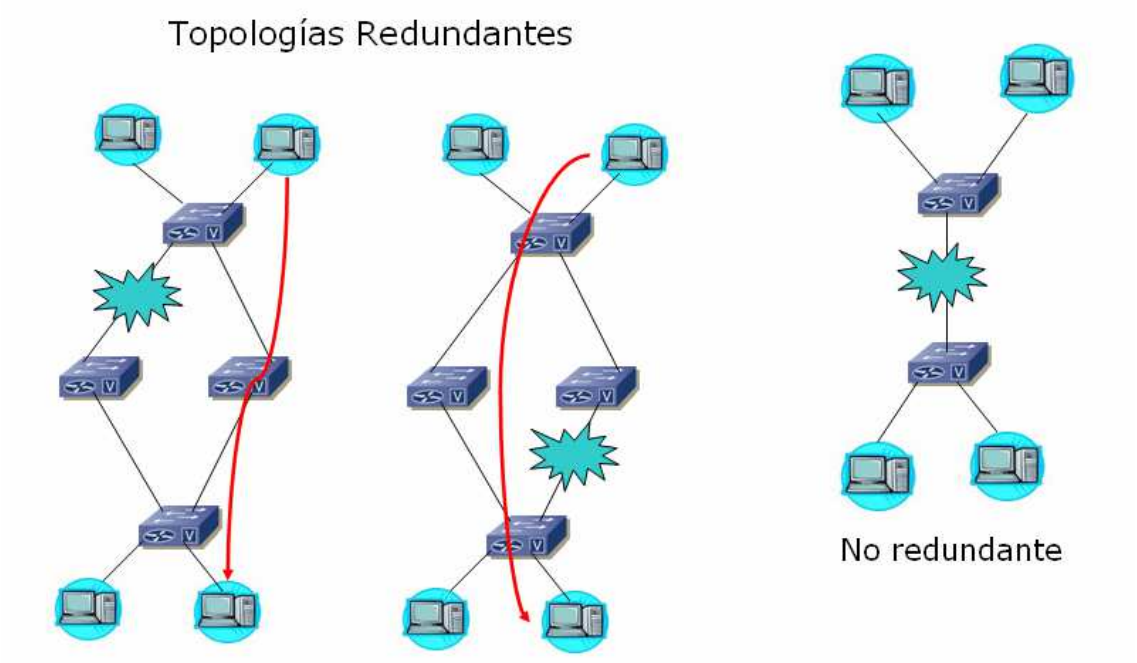


Figura 59- Topologías Redundantes STP

Virtual LAN (VLAN)

Una VLAN es una agrupación lógica, definida dentro de uno o más conmutadores interconectados, de un conjunto de dispositivos y estaciones de la red. Estas estaciones pueden agruparse por cualquier criterio que se requiera: función, departamento de pertenencia, etc. a pesar de que las estaciones puedan estar físicamente separadas en segmentos de red distintos.

Los dispositivos que forman una VLAN sólo pueden comunicarse en el sentido de una LAN con ellos mismos.

Existen dos modos fundamentales de definir VLANs:

• VLAN estática: También conocida como VLAN basada en puertos. La red local virtual se define en el conmutador mediante la asociación de varios puertos del mismo a dicha VLAN, de forma que no permite la conmutación de tramas directa entre puertos que no pertenezcan a la misma VLAN. La ventaja de este tipo de VLAN es que, mediante la utilización de tecnología ASIC (Application Specific Integrated Circuits), la conmutación se realiza de manera muy rápida. El mayor inconveniente es la necesidad de gestionar estas VLANs directamente sobre el conmutador físico.

• VLAN dinámica: en este caso el conmutador reconoce automáticamente a qué VLAN pertenecen las estaciones conectadas a cada uno de sus puertos. Las redes locales virtuales se asignan desde una aplicación gestora, normalmente en función de la dirección MAC, aunque también puede realizarse a través de la dirección IP o incluso el

tipo de protocolo empleado. En el caso de que no se emplee microsegmentación, podría darse la situación de que a un mismo puerto estuvieran conectadas estaciones pertenecientes a dos VLANs distintas, con lo que se pierde la ventaja de la separación de dominios de colisión.

Para comunicar distintas VLAN entre sí o con el mundo exterior se requiere la utilización de dispositivos que actúen en el nivel 3 ó superior (normalmente encaminadores).

La conexión con dicho dispositivo se realiza mediante el uso de de enlaces "trunk" del conmutador, de mayor capacidad que los puertos normales, de forma que un mismo cable se comparta para diferentes VLANs.

Los enlaces trunk suponen un cambio importante en el funcionamiento de los conmutadores, ya que al mezclar tramas de diferentes VLANs por el mismo cable es preciso etiquetarlas de alguna manera a fin de poder entregarlas a la VLAN adecuada en el otro extremo. El marcado se hace añadiendo un campo nuevo en la cabecera de la trama MAC, lo cual hace que el tamaño de la trama Ethernet pueda superar ligeramente la longitud máxima de 1518 bytes en algunos casos, ya que un conmutador puede recibir una trama de 1500 bytes y si la ha de enviar por un enlace trunk tendrá que incorporarle la etiqueta correspondiente (ya que en ningún caso está permitido fragmentar la trama original). Los primeros sistemas de etiquetado de tramas eran propietarios, por lo que los enlaces trunk solo podían interoperar entre equipos del mismo fabricante. Hoy en día el protocolo utilizado prácticamente por todos los equipos es el definido por el IEEE en su especificación 802.1Q. Este protocolo introduce una etiqueta de 4 bytes, con lo que la trama Ethernet pasa a tener un tamaño máximo de 1522 bytes.

Las tramas se marcan únicamente para su tránsito por el enlace trunk. Una vez se conmutan o encaminan fuera de dicho enlace, se elimina la etiqueta con lo que se recupera la trama original.

El enlace trunk se utiliza también para comunicar dos conmutadores entre sí, de manera que se pueda definir VLANs utilizando los puertos de más de un conmutador.

El estándar 802.1Q incorpora además el protocolo MSTP (Multiple Spanning Tree Protocol), que define una extensión del protocolo RSTP para su utilización en instalaciones donde hay definidas más de una VLAN. Este protocolo configura un Spanning Tree por cada VLAN y bloquea los enlaces redundantes dentro de cada Spanning Tree.

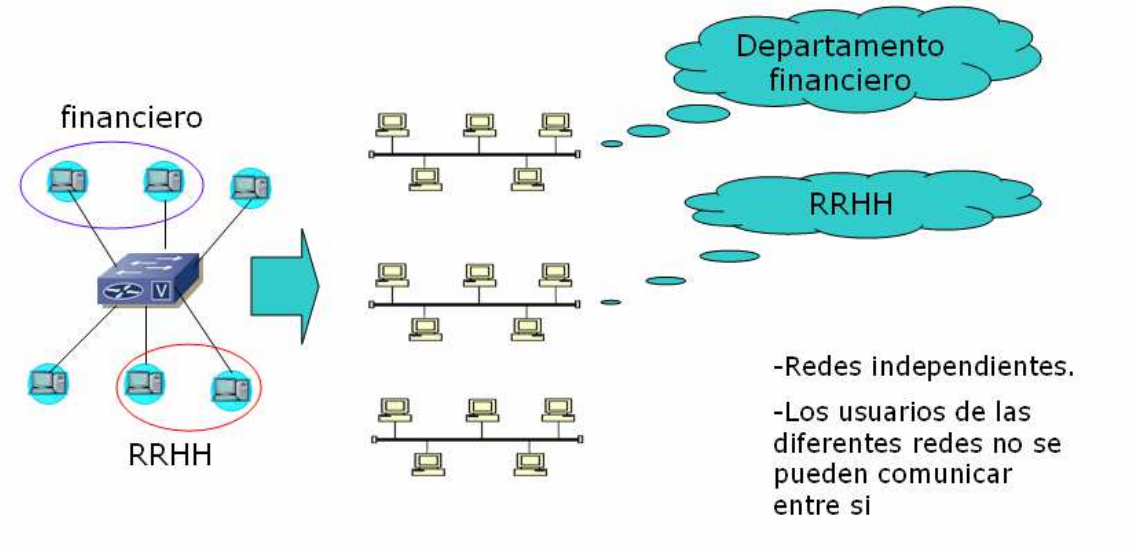


Figura 60 – Segmentación en VLANs

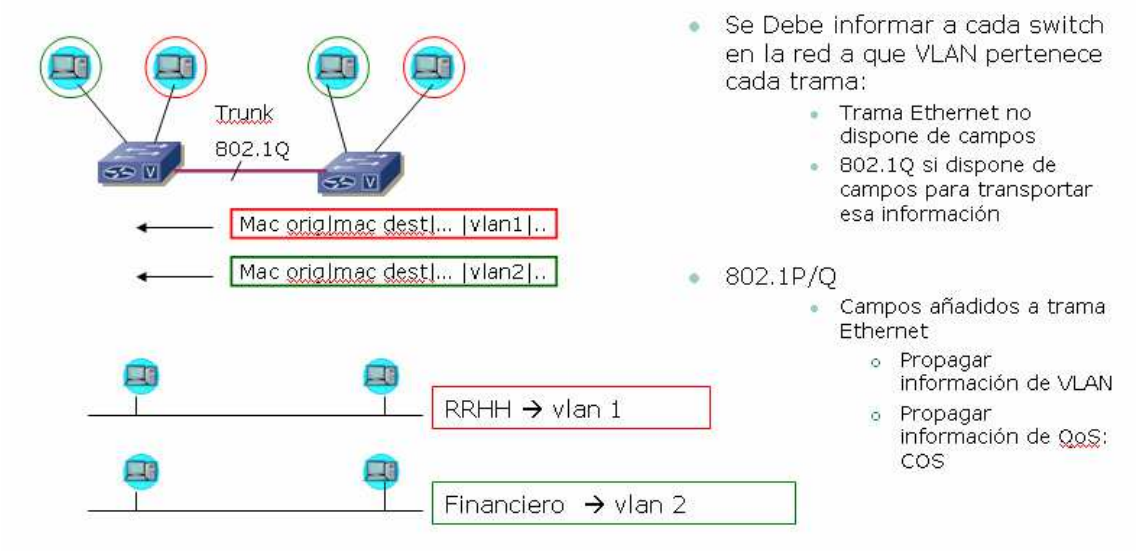


Figura 61 – Enlaces Trunk – Segmentación vlans

1.3.2. Tendencias de Diseño

A la hora de diseñar el subsistema de nivel 2, en función de la distribución del cableado estructurado, tendremos que acometer la distribución de switches de distintas formas. Así pues, veíamos, dentro de las tendencias de diseño de cableado estructurado que existían dos grandes tendencias:

- Cableado Centralizado: En este caso todo el cableado estructurado que dará cobertura a la red de datos y/o voz se encuentra centralizado, concentrado en un solo cuarto técnico. Por tanto será necesario que todos los switches se concentren en el mismo cuarto técnico.

- Cableado repartido por plantas: En este caso se dispondrá de armarios repartidores, ubicados en cada una de las plantas e interconectados mediante verticales entre ellos. Se hace necesario, por tanto, disponer de al menos un switch en cada de estos armarios. Tiene la desventaja, que en plantas con pocos usuarios, es posible que se desperdicien muchos puertos de switch.

1.3.2.1. Conexionado Switches

En el mercado actual existen multitud de fabricantes de electrónica de nivel 2 [switches], pero la gran mayoría realizan equipos con similares características y similitud de puertos. A saber, todos los equipos tiene una zona para la interconexión masiva de los dispositivos [pc/teléfonos] con velocidades de 100/1000 Mbps, y algunos puertos "especiales" que permiten la interconexión de dispositivos con requerimientos de ancho de banda mayor [servidor departamental, equipo videoconferencia, cascadas entre switches...] con velocidades de 1/10 Gbps. Un ejemplo de frontal de un switch lo podemos ver en la siguiente figura

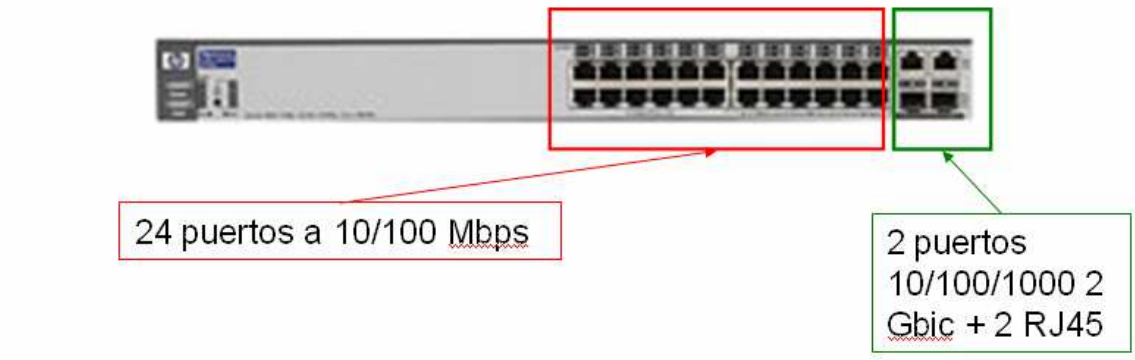


Figura 62 – Frontal Switch Procurve HP

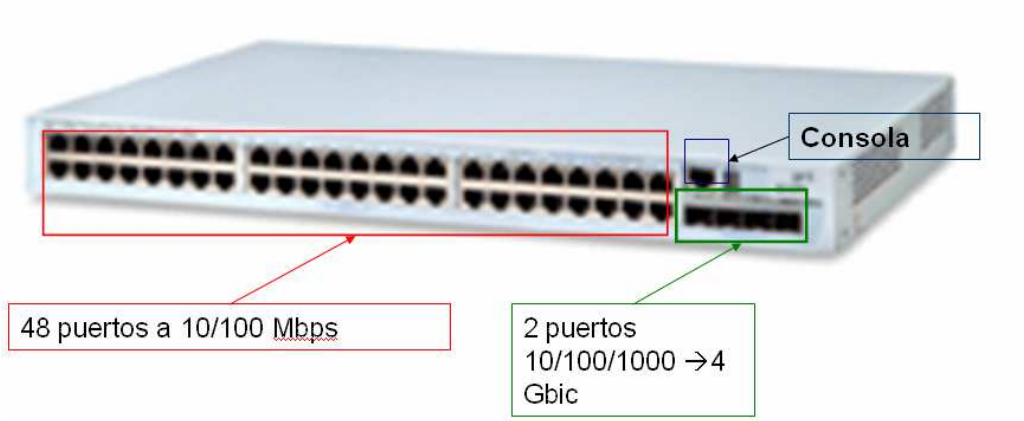


Figura 63 – Frontal Switch 3COM

Un aspecto importante a la hora de diseñar una infraestructura de switches es definir de forma correcta la interconexión de los mismos, y la interconexión con el resto de dispositivos que conformarán nuestra red LAN.

Por un lado se definirán de forma correcta los puertos importantes de LAN, es decir, aquellos donde se encuentran conectados los dispositivos mas importantes de la red local: routers, servidor, equipo videoconferencia, resto de switches. En la siguiente figura se muestran los puertos más importantes en cualquier instalación LAN. [la nomenclatura puede variar en función de la instalación pero el significado se mantiene]

PUERTO	DESCRIPCIÓN
Puerto 1	Router Principal
Puerto 2	Router Back Up
Puerto 3	Servidor, si Giga no libre
Puerto 4	Videoconferencia
Puertos Giga	Servidor,cascadas switches

Figura 64 – Puertos importantes conexión switch [LAN]

Así, el esquema de una red LAN básica con un solo switch, y los servicios más importantes sería:

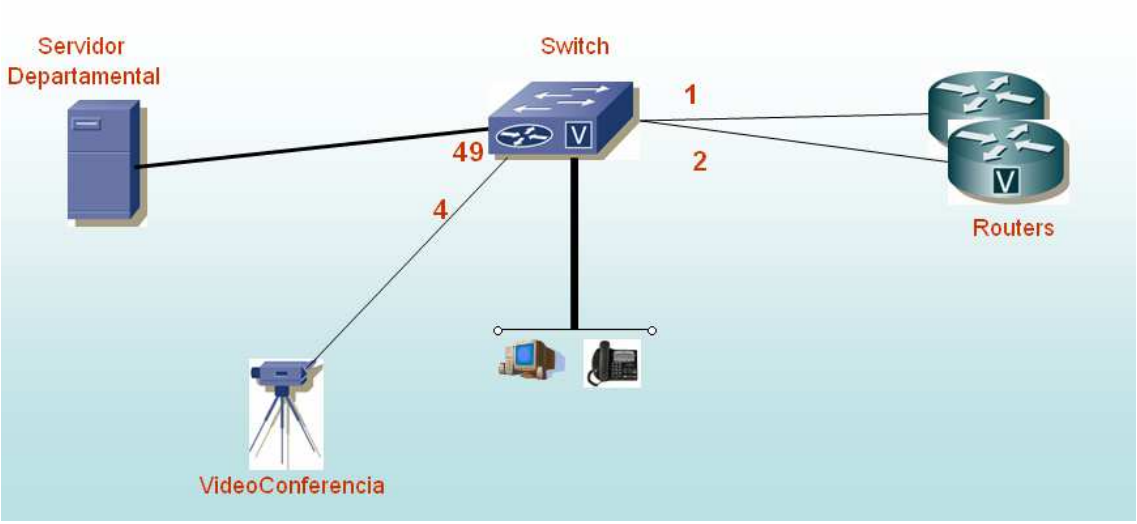


Figura 65- Esquema básico interconexión Red LAN

Lo habitual es utilizar los puertos a 1Gbps, para realizar las cascadas entre varios switches, pero teniendo en cuenta que los equipos comerciales tienen entre 2 y 4 puertos a 1Gbps se plantean distintas opciones de interconexión.

La problemática a solucionar es que si se pierde la conectividad en un de los puertos de la cascada todos los switches que haya detrás de la misma también perderán conectividad. Es necesario sopesar dos aspectos: la disponibilidad de la red LAN y velocidad de la red LAN.

Por disponibilidad entendemos la cantidad de puertos que mantienen conectividad en caso de desconectarse una vertical de interconexión entre switches. Interesa por tanto disponibilidades altas de la red LAN, es decir, que ante caída de alguno de los enlaces verticales pierdan conexión el número mínimo de puertos.

Por velocidad entendemos que los enlaces troncales de nuestra red LAN, que son los que aglutinan todas las conexiones hacia el router, servidor o equipo de videoconferencia, tienen que tener la máxima capacidad, idealmente nos interesa una red LAN a 1Gbps.

Así se plantean distintas opciones [suponiendo que solo tenemos dos puertos a 1Gbps para realizar las cascadas entre switches].

- Aceptable relación Velocidad-Tasa de Fallos

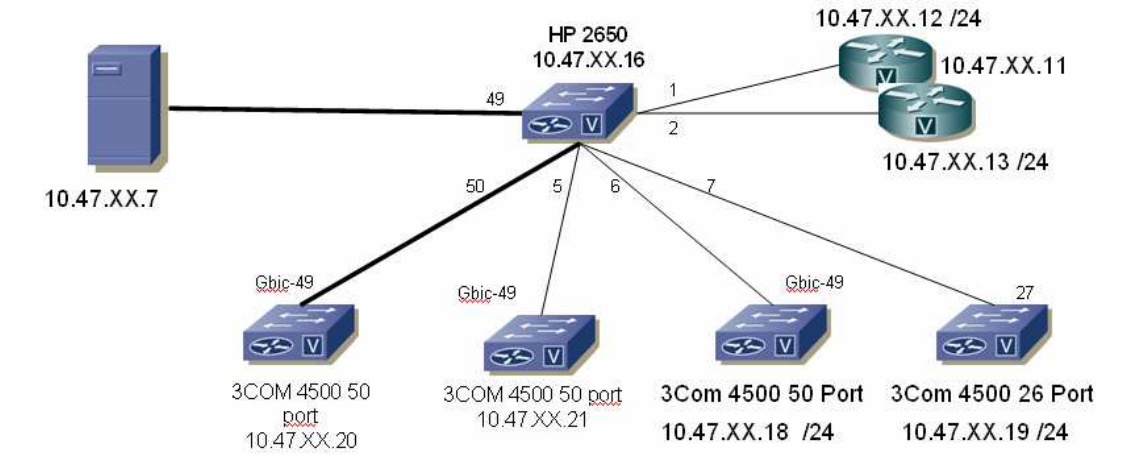


Figura 66 – Interconexión LAN – velocidad tasa de fallos 1

Es necesario interconectar 5 switches, uno de ellos será el switch principal de la sede, el que aglutine todo el tráfico LAN. A el se conectarán mediante uno de los puertos a 1Gbps, por un lado el servidor, y por otro uno de los switches. El resto de switches [3] se conectarán mediante puertos de 100Mbps.

Tenemos un solo punto de fallos central, el switch principal, pero la velocidad de gran parte de la LAN queda restringida a 100Mbps.

- Velocidad vs Disponibilidad

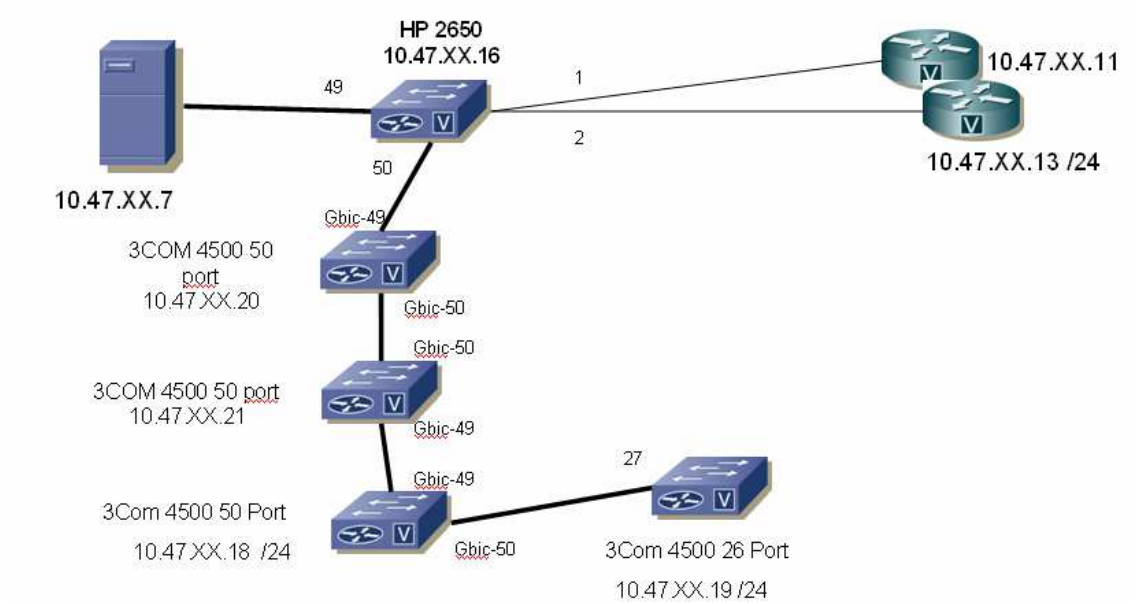


Figura 67- Interconexión LAN – velocidad tasa de fallos 2

Se ha conseguido una red LAN con velocidad en su core de 1Gbps, al aprovechar las conexión a 1Gbps de cada uno de los switches, pero sin embargo se tienen 4 puntos críticos de fallo, ya que un error en el segundo switch de la cascada deja incomunicados a todos los usuarios de los switches 2º, 3º, 4º y 5º, y así sucesivamente con el resto de switches.

- Relación Optima

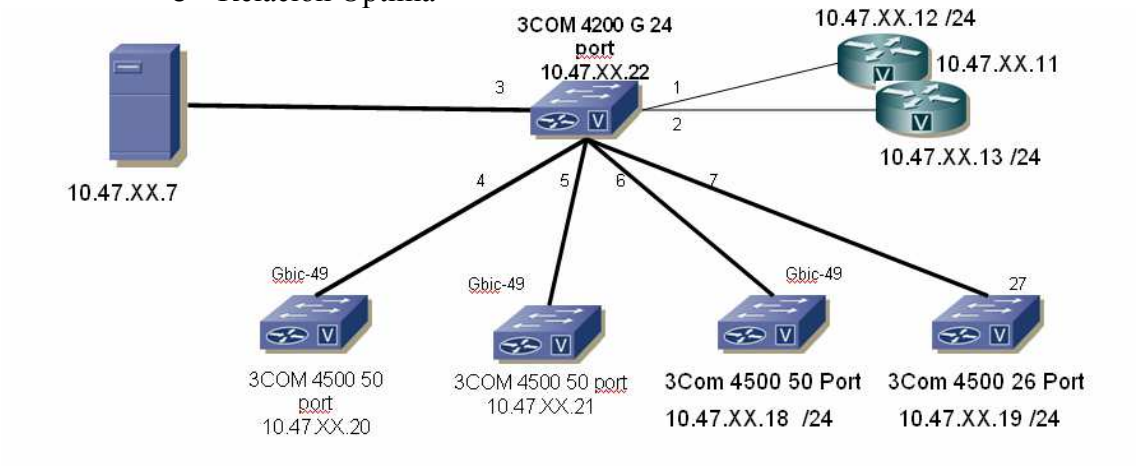


Figura 68 - Interconexión LAN – velocidad tasa de fallos 3

Lo idea es disponer de un equipo capaz de aglutinar mas de dos conexiones a 1Gbps de tal forma que se pueda montar una especie de Core de red LAN. Existen distintos fabricantes que proporcionan este tipo de equipamiento. Un ejemplo puede ser el equipo 4200G de 3COM.

1.3.2.2. Diseño ToIP

Uno de los aspectos claves en la actuales redes LAN es la convivencia sobre la red de datos de todo la arquitectura de voz, es decir, es muy habitual que toda la infraestructura de voz, sea IP, es decir, que se implemente un sistema de telefonía IP extremo a extremo para dotar a la oficina del servicio de voz.

A la hora de diseñar la red LAN para soportar el servicio de voz es necesario tener cuenta varios aspectos:

- Disponer de electrónica de nivel 2 con **Power Over Ethernet**, PoE **IEEE 802.3af-2003**, es decir, la posibilidad de alimentar un dispositivo conectado a la red a través del propio cableado de red Ethernet, sin necesidad de transformadores de corriente accesorios. Esto nos permitirá, controlar la alimentación de los terminales. El estándar PoE es capaz de suministrar hasta 15.4 W, mas que suficiente para alimentar cualquier modelo de teléfono IP del mercado En las distribuciones actuales y con el control exhaustivo de la alimentación Poe a los teléfonos se puede conseguir realizar un control de ahorro energético, simplemente controlado la energía que se suministra a los terminales: Se pueden definir tramos horarios en los que se apaguen los dispositivos, se puede recudir su velocidad (bajar los puertos a 10Mbps), todo encaminado a un ahorro energético considerable.

- Poe Plus. Existe una tendencia de mercado, en alimentar mediante PoE, no solo los teléfonos IP; aparecen también puntos de acceso wifi, y dispositivos que empiezan a reemplazar a los actuales PCs de escritorio. Se trata de terminales "tontos", que lo único que necesitan es una conexión a la red para poder conectarse con los servicios que se le proporcionen [acceso BBDD, herramientas ofimáticas, Internet]. Estos dispositivos no tienen fuente de alimentación y también se alimentan vía PoE desde la electrónica a la que están conectadas. En este caso se ha desarrollado la tecnología PoE Plus, amparada para el standard **IEEE 802.3at-2009,** que es capaz de suministrar hasta 25W.

- Vlan. Uno de los aspectos clave en la transmisión de la voz por una red de "datos" es la separación lógica de ambos flujos de información. El tráfico de voz es un tráfico muy sensible a los retardos, a las congestiones y al jitter (variación del retardo), es por ello que se necesario asegurar que el tráfico de voz no se ve comprometido por el tráfico [masivo] de datos. La mejor forma de asegurar esto es encapsulando el tráfico de voz en una vlan distinta a la vlan de los datos, de forma que se tratada con una prioridad superior por todos los elementos de la red por la que pasen: switches, routers,..

- Reducción cableado. Utilización Mini-switch: Uno de los aspectos importantes que potencia la instalación de soluciones de nivel 2 con posibilidad de Telefonía IP es la posibilidad de reducir el número de tomas de cableado. Así, en una instalación tradicional lo más habitual era cablear físicamente 1 o 2 tomas para datos y una toma para voz (tradicional). En la siguiente figura se aprecia el conexionado tradicional de la infraestructura de voz

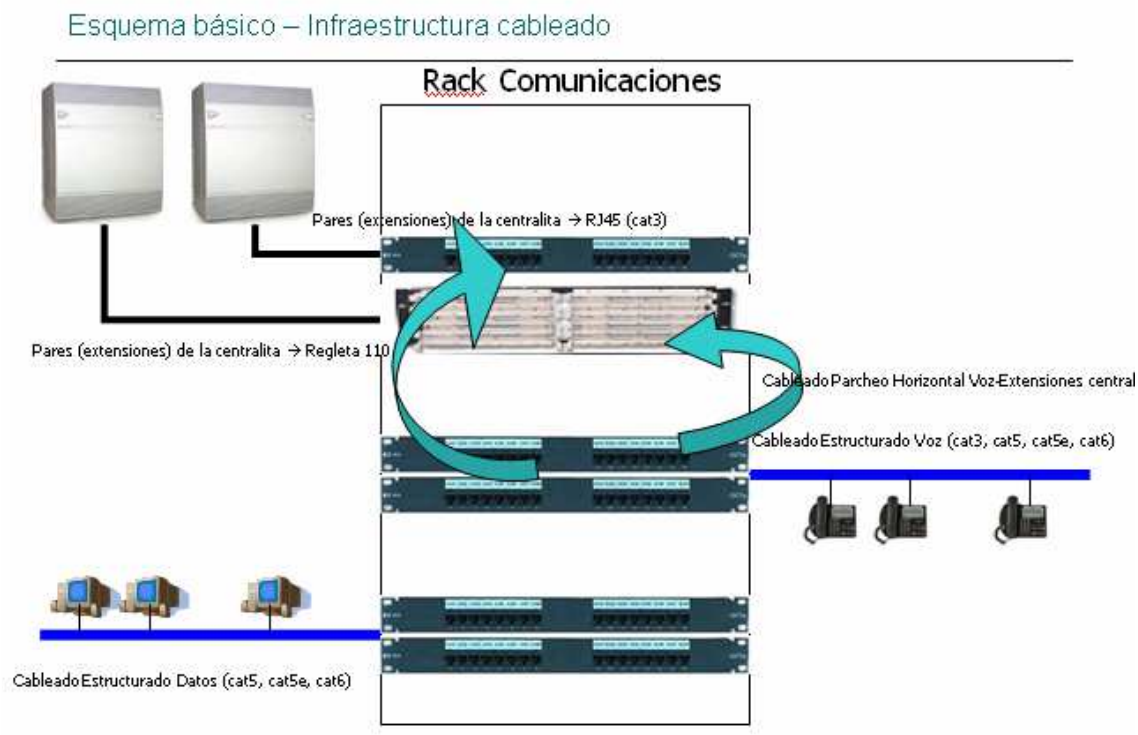


Figura 69 – Conexionado tradicional Voz

Ahora con los nuevos terminales IP, y con una única toma de datos se pueden prestar tanto el servicio de datos como el servicio de voz. Esto se consigue utilizando terminales IP con mini-switch integrado. Es necesario marcar la vlan de voz en el propio terminal IP. La conexión se realiza, desde la toma del usuario al teléfono y utilizando el mini-switch se conecta el teléfono al ordenador, como indica la figura.

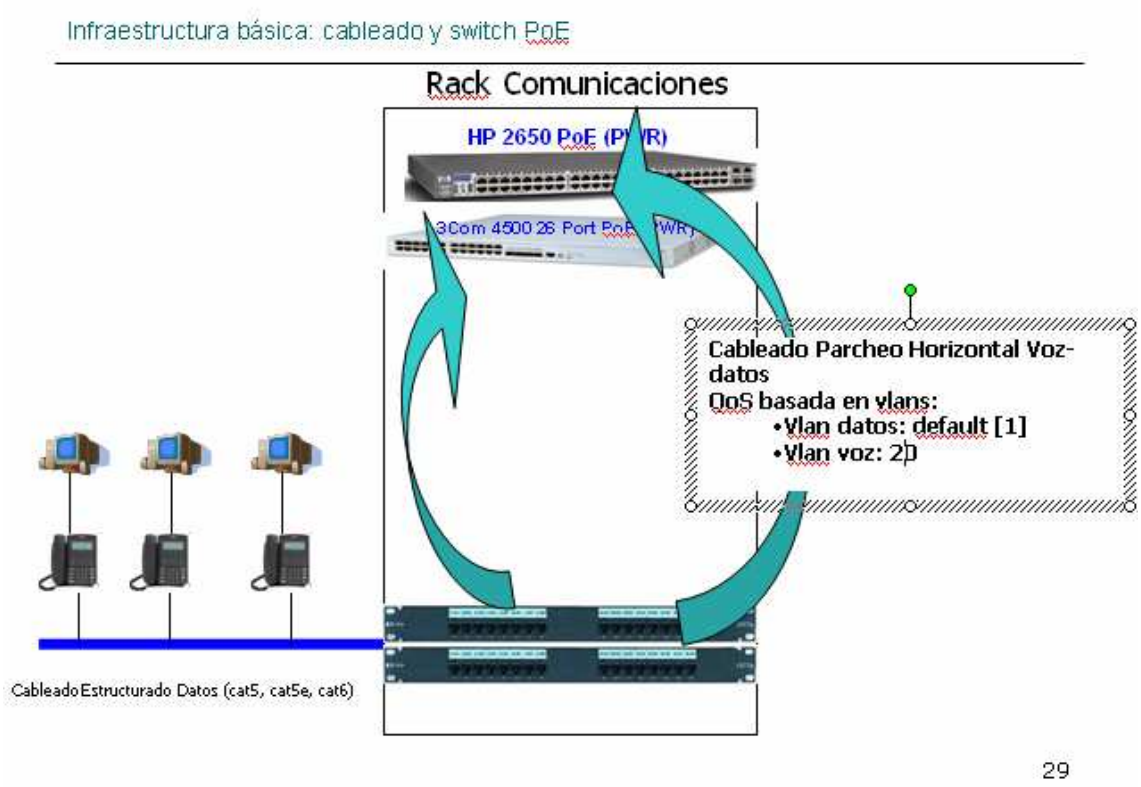


Figura 70 – Conexiona Terminal IP con Miniswitch

- SAI. Uno de los aspectos a tener en cuenta en la instalación de un subsistema de nivel 2 que proporcione soporte a una plataforma de telefonía IP es la necesidad de contar con un sistema, aunque sea básico, de alimentación ininterrumpida. La telefonía tradicional funciona, en general, aunque se pierda el suministro eléctrico. Los teléfonos IP no. Para ello, para dotar de cierta redundancia en caso de caída del suministro eléctrico a los switches PoE se hace necesario alimentarlos a través de un equipo de alimentación ininterrumpida, bien sea propio del edificio que albergue la electrónica [grupos electrógenos], bien locales a cada uno de los switches.

- QoS Voz: Además de la vlan de voz, que nos diferenciará el tráfico de voz, del tráfico de datos, muchos switches proporcionan funcionalidades en lo que a la aplicación de calidad de servicio en el nivel se refiere, esto es, marcado de paquetes de voz, priorización de los mismos en la red.. Dadas las características intrínsecas al tráfico de voz [bajo retardo, bajo jitter, bajo ancho de banda], la utilización de este tipo de funcionalidades se hacen necesaria.

- SW control nivel2/3: Hasta ahora los switches se comportaban como elementos que realizaban tareas propias del nivel 2 de la pila TCP/IP [macs, vlans, arp, parámetros puertos…]. Desde hace unos años la frontera entre los dispositivos de nivel 2 [switches] y los dispositivos

de nivel 3 [routers] es cada vez más difusa. Los switches incorporan cada vez mas funcionalidades propias del nivel 3, por ejemplo:

- SNMP
- VRRP - Virtual Router Redundancy Protocol
- OSPF
- Control QoS por puerto basada en datos de nivel 3 [IP] y nivel 4 [puerto]
- Gestión IP del dispositivo. Mediante esta gestión se ha obtenido un grado de control absoluto sobre lo que pasa en el subsistema de nivel 2, con control absoluto del tráfico que cursa un puerto, del modo y la velocidad de conexión. Algunas imágenes de gestión web de un dispositivo de nivel 2 las podemos ver a continuación

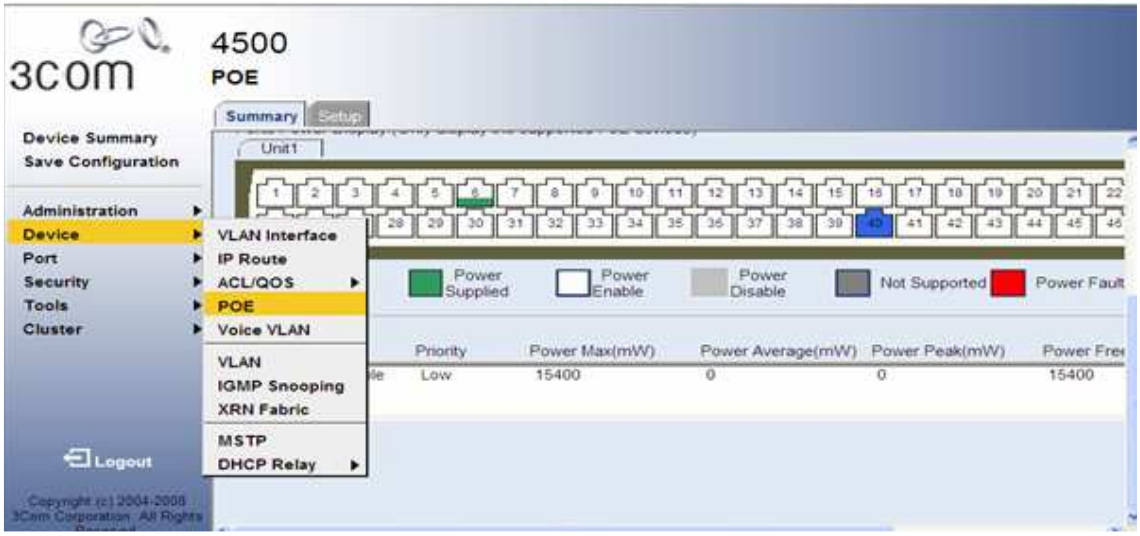


Figura 71- Gestión IP web switch 3COM

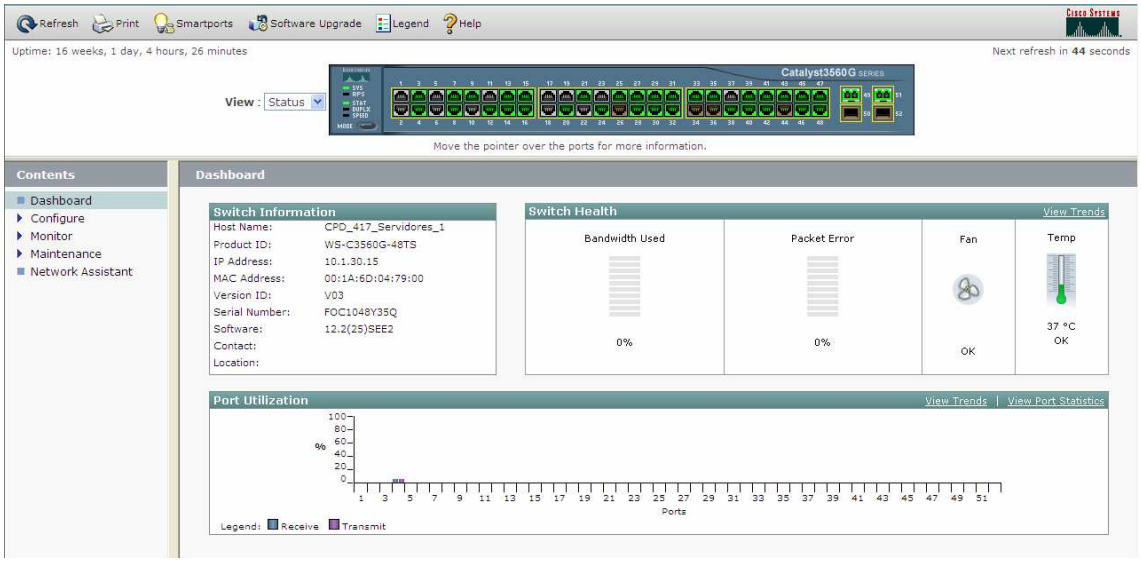
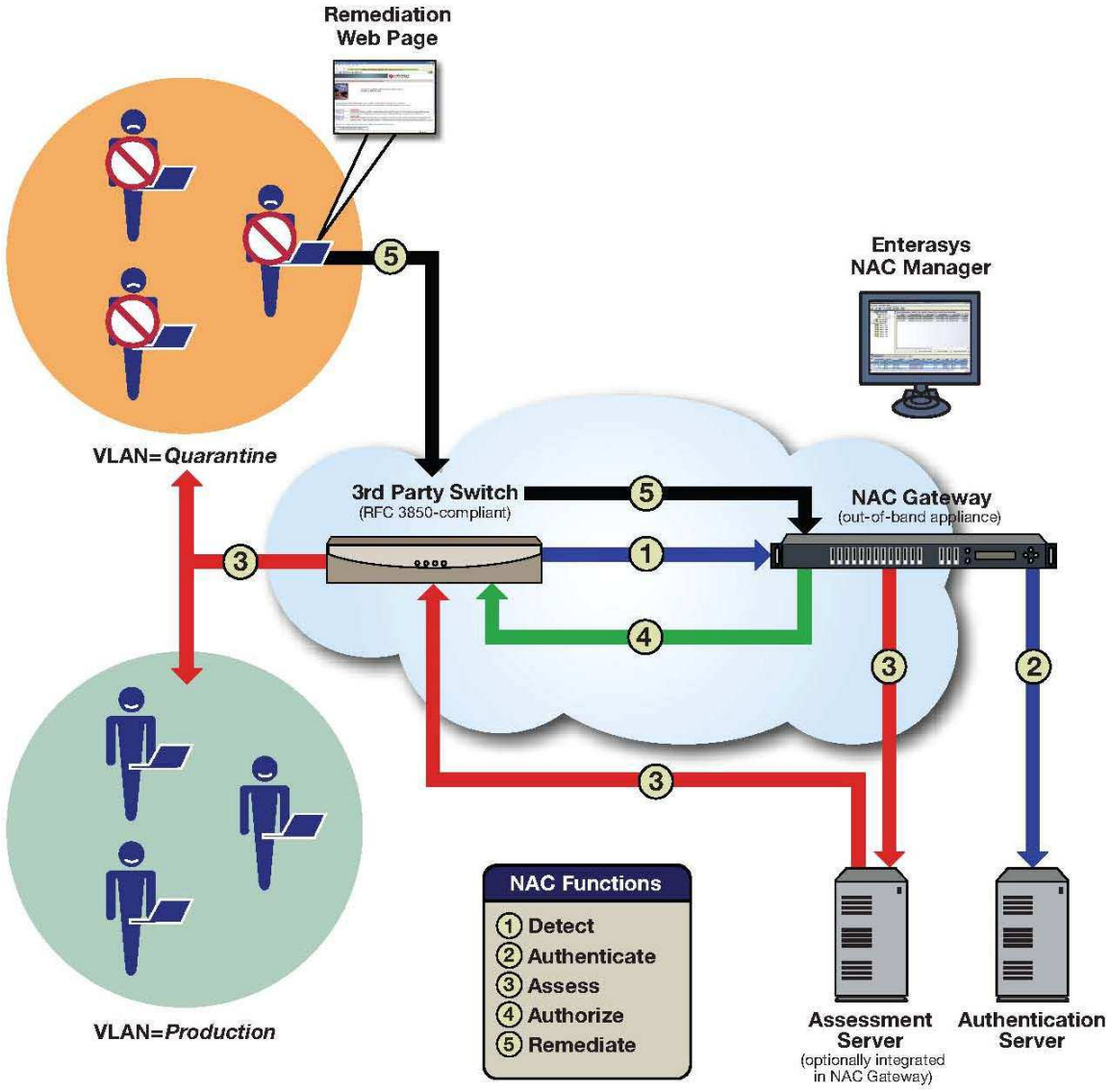


Figura 72 - Gestión IP web switch Cisco

1.3.2.3. NAC

Uno de los paradigmas que mas desarrollo está experimentando en el sector de las comunicaciones, es el control de acceso al medio, conocido como NAC. Básicamente consiste en, basándonos en la potencia de segmentación que nos dan las vlans en los dispositivos de nivel 2, poder decidir en función de parámetros muy variados si a un usuario [pc, tablet, smartphone…] se le dota de conectividad [con distintos niveles de privilegios] o no.

Un esquema genérico de cómo integrar un proyecto de NAC dentro de nuestro subsistema de nivel 2 se a aprecia en la siguiente figura.



En primer lugar identificamos las partes que componen el esquema:

- Switch: mínimo con dos vlans configuradas, y con cumplimiento de la RFC-3850. Vlan producción y vlan cuarentena
- Servidores de Autenticación: básicamente basados en protocolo Radius
- Servidores de Evaluación (Assesment)
- NAC Gateway: Interconexión entre elementos
- Plataforma de Remediación
- Plataforma de Gestión Centralizada

El funcionamiento se bastante sencillo:

- Un dispositivo se conecta a la red y tiene que ser detectado e identificado.
- Habitualmente se realizará un primer chequeo de usuario y contraseña basada en un servidor de autenticación radius.
- Se realiza un proceso de evolución del estado de salud [parches, antivirus, políticas generales seguridad, y se determina si el dispositivo se asignado a la zona de cuarentena [vlan de cuarentena] o por el contrario se considera un dispositivo "sano" y es asignado a la zona de producción [vlan de producción]
- En caso necesario, se le proporciona posible remediación de su estado de salud [mediante portal cautivo, links para descargas de parches obligatorios, actualizaciones del antivirus..]
- Continuamente se realiza un proceso de monitorización post-conexión

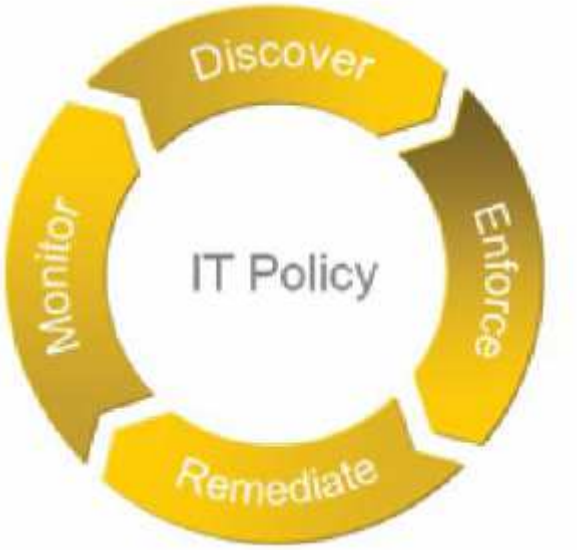


Figura 73- Fases NAC

Que datos nos interesa considerar en la implantación de este tipo de soluciones

- Arquitectura Centralizada / Distribuida.
- Modo de funcionamiento en línea / fuera de línea.
- Soporte Radius, VPN, 802.1x
- Comunicaciones.
- Escalabilidad.
- Alta disponibilidad.
- Electrónica de red existente.
- Acceso basado en roles & perfiles.
- Single Sign On (SSO) & Integración con LDAP X.500.
- Remediación incorporada & integración con terceros.
- Inventario de dispositivos (S.Operativo, Aplicaciones…).
- Tratamiento Pre-admisión y Pos-admisión.
- Gestión de vulnerabilidades (escaneo & integración).
- Monitorización.
- Políticas de seguridad corporativas.
- Cumplimiento de normativas.

A continuación algunas recomendaciones y tendencias a tener en cuenta en un proyecto NAC

- Sin Agente / Agente Ligero.
- Solución fuera de banda (OOB).
- Funcionamiento con / sin 802.1x
- Arquitectura física & virtual.
- Usuarios corporativos / no corporativos (Portal de Autoenrollment).
- Gestión amigable en definición y aplicación de políticas.
- Integración con tecnologías existentes de Anti-Malware.
- Bloqueo a los puertos de los Switches de acceso y acceso por redes inalámbricas.
- Soportar nuevos entornos de movilidad (IOS, Android, etc.).
- Integración con FW / IPS.
- Integración con normativas y estándares (PCI, SOX, LOPD…).
- Visibilidad hasta la capa de aplicación (Nivel 7).
- Informes potentes y comprensibles.
- Reducir costes de explotación.

La siguiente imagen nos ilustras sobre distintos fabricantes actuales de soluciones NAC. Están divididos en tres grandes grupos:

- Fabricantes de Nicho de Mercado. Muy ligados a la fabricación de dispositivos de red. Recomendables para entornos con una gran homogeneidad de dispositivos.
- Endpoints: Empresas principalmente lideres en el mercado de la seguridad, que tienen líneas potentes de producto NAC, integrado en mayor o menor medida con su solución de seguridad
- Nativos o agnósticos: Compañías que nacen, sin estar ligados a una marca en concreto de dispositivos de red, y que en principio se adaptan en mayor o menor medida a las necesidades con arquitecturas de red muy heterogéneas.

Figura 74- Fabricantes soluciones NAC

En las siguientes figuras se ve el posicionamiento de estas compañías en los cuadrantes de Gartner y Forrester.

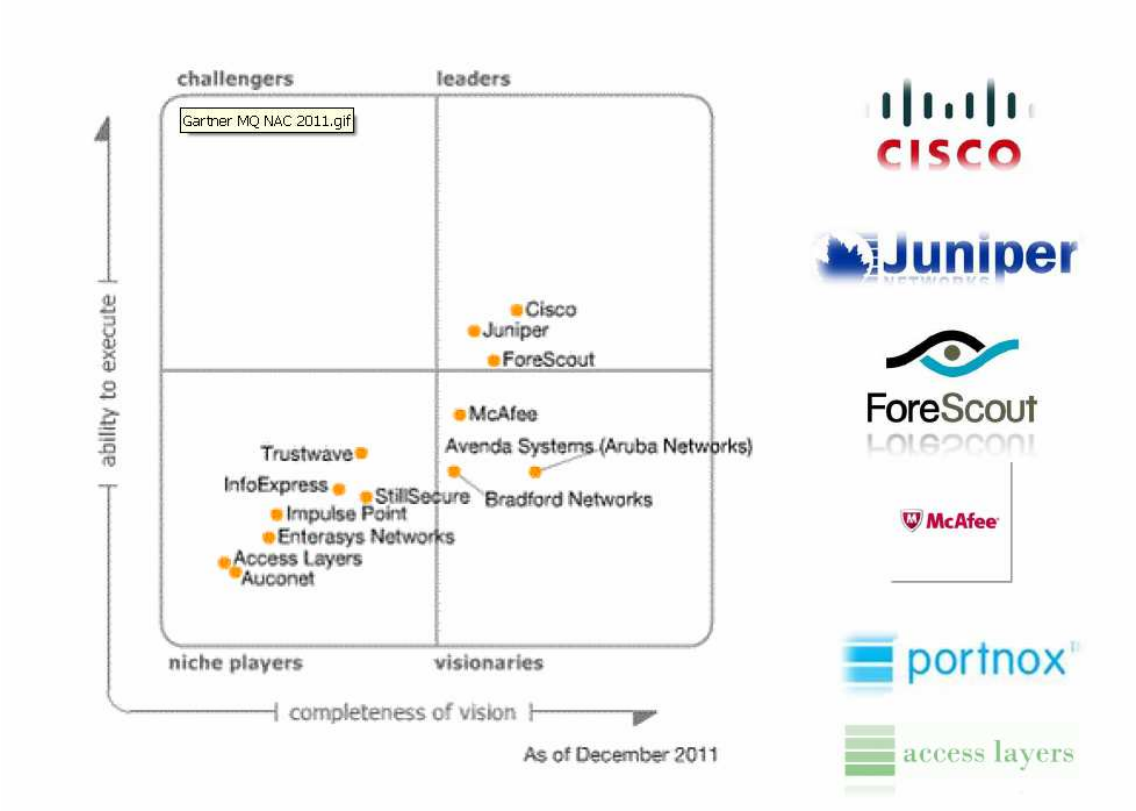


Figura 75- Posicionamiento compañías NAC - Gartner

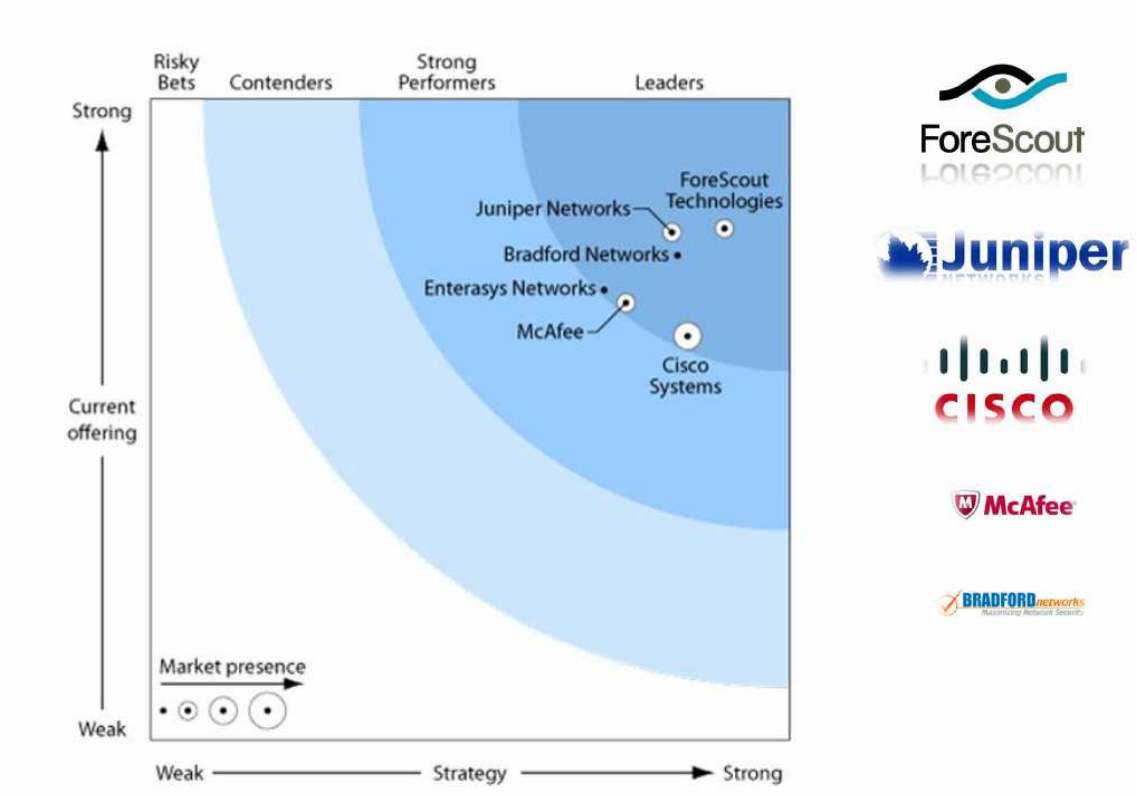


Figura 76- Posicionamiento compañías NAC Forrester

1.3.3. Aplicación Práctica

Siguiendo con el ejemplo de cableado estructura presentado para el subsistema de nivel 1, vamos a completar la parte correspondiente al subsistema del nivel 2. A modo de recordatorio, el proyecto consistía en la dotación de un sistemas comunicaciones en un edificio de dos plantas, con la siguiente distribución:

La distribución de puntos de cableado por plantas es la siguiente:

- **Planta 1:**

Se pretende dotar la zona con una densidad alta de puestos de trabajo, incluyendo puestos cableados para usuarios finales y puntos de cableado para la conexión de puntos de acceso wifi.

El número total de puntos es el siguiente:
- Puntos de cableado usuario: 38
- Puntos de cableado para conexión APs wifi: 8

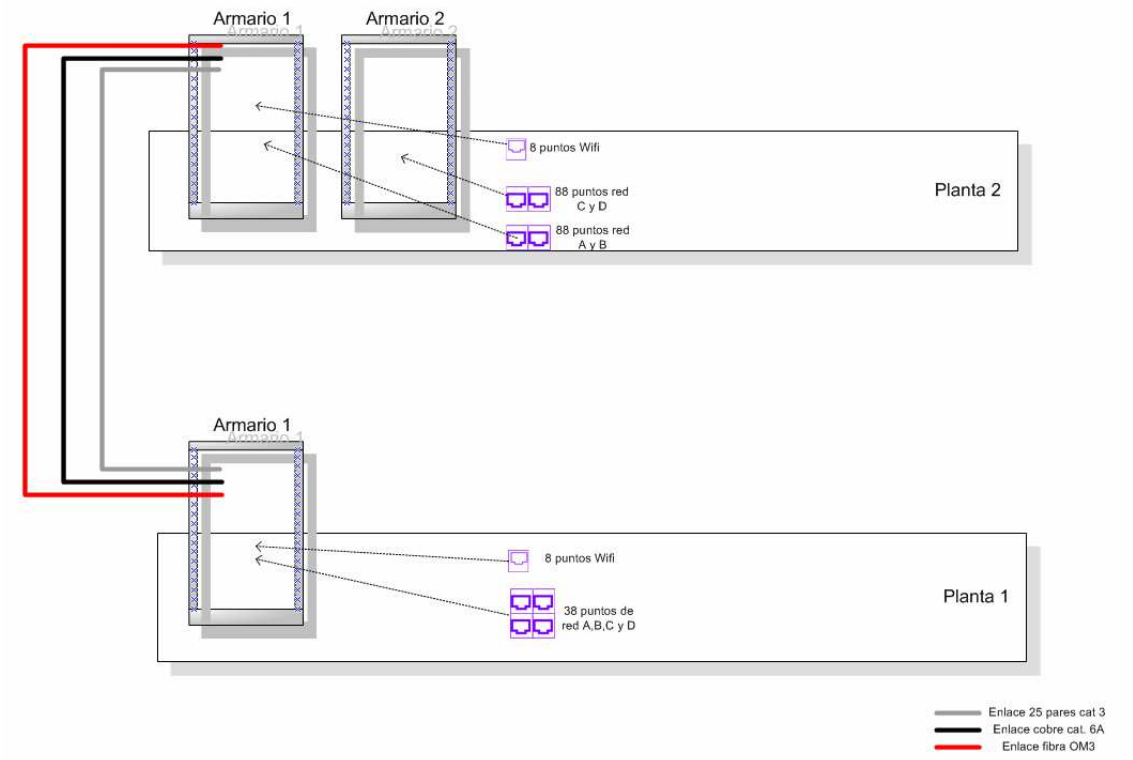
- **Planta 2:**

Se pretende dotar la zona con una densidad alta de puestos de trabajo, incluyendo puestos cableados para usuarios finales y puntos de cableado para la conexión de puntos de acceso wifi.

El número total de puntos es el siguiente:
- Puntos de cableado usuario: 88
- Puntos de cableado para conexión APs wifi: 8

1.3.3.1. Distribución switches

La distribución física de los switches en la sede vendrá determinada por la distribución del cableado realizado, ya que será necesario dotar de electrónica de nivel dos a todos los armarios de comunicaciones susceptibles de tener conectados usuarios o dispositivos de comunicaciones [en nuestro caso puntos de acceso wifi]. La distribución de armarios por plantas queda como se aprecia en la figura siguiente:



De la siguiente distribución se desprende que tendremos que dotar de switches a todos los armarios de la figura, es decir, a los armarios 1 y 2 de la planta 2 y al armario 1 de la planta 1.

Los equipos a instalar serán **Avaya Ethernet Routing Switch 4500T PWR,** equipos que cuentan con todas las características que destacamos en el apartado 1.3.2.2

Teniendo en cuenta la distribución de puntos en los armarios, se ha decidido montar la siguiente electrónica de nivel 2:

Planta	Armario	Switch
Primera	1	Avaya 4550 T PWR
Segunda	1	Avaya 4550 T PWR
		Avaya 4550 T PWR
	2	Avaya 4550 T PWR
		Avaya 4550 T PWR

En definitiva para dar cobertura de red a toda la sede se van a instalar 5 switches Avaya 4550 T PWR. Las características de estos dispositivos son:

Puertos:

48 x 10/100BASE-TX PoE plus 2 x Combo 10/100/1000BASE-T or 100/1000BASE-SFP

Características generales

• Switch Fabric performance: 48.8 to 184Gbps
• Frame forwarding rate: 6.6 to 72Mpps
• Latency: 9µsec
• Jitter: 12-14µsec
• Frame length: 64 to 1518 Bytes (802.1Q Untagged), 64 to 1522 Bytes (802.1Q Tagged)
• Jumbo Frame support: up to 9,000 Bytes (802.1Q Tagged)
• Multi-Link Trunks: up to 32 Groups, with 8 Links per Group
• VLANs: up to 256 Port/Protocol/802.1Q-based
• Multiple Spanning Tree Groups: 8
• MAC Address: up to 8k
• DHCP Snooping: up to 1,024 table entries
• ARP Entries: up to 1,792
• IP Interfaces: up to 64
• IPv4 Routes: up to 512
• OSPF Instances: up to 4
• OSPF Adjacencies: up to 16

Compatibilidad de estandares

• IEEE 802.1D Spanning Tree Protocol
• IEEE 802.1p Prioritizing
• IEEE 802.1Q VLAN Tagging
• IEEE 802.1X EAPoL
• IEEE 802.1ab Link Layer Discovery Protocol
• IEEE 802.3 Ethernet
• IEEE 802.3u Fast Ethernet
• IEEE 802.3x Flow Control

- *IEEE 802.3z Gigabit Ethernet*
- *IEEE 802.3ab Gigabit Ethernet over Copper*
- *IEEE 802.3ad Link Aggregation*
- *RFC 768 UDP*
- *RFC 791 IP*
- *RFC 792 ICMP*
- *RFC 793 TCP*
- *RFC 826 ARP*
- *RFC 854 Telnet*
- *RFC 894 IP over Ethernet*
- *RFC 951 BootP*
- *RFC 1058 RIP v1*
- *RFC 1112 IGMPv1*
- *RFC 1157 SNMP*
- *RFC 1213 MIB-II*
- *RFC 1271 RMON*
- *RFC 1350 TFTP*
- *RFC 1493 Bridge MIB*
- *RFC 1583 OSPF v2*
- *RFC 1757 RMON*
- *RFC 1850 OSPF v2 MIB*
- *RFC 1945 HTTP v1.0*
- *RFC 2131 BootP/DHCP Relay Agent*
- *RFC 2236 IGMPv2*
- *RFC 2328 OSPF v2*
- *RFC 2453 RIP v2*
- *RFC 2474 DiffServ*
- *RFC 2475 DiffServ*
- *RFC 2665 Ethernet MIB*
- *RFC 2674 Q-BRIDGE-MIB*
- *RFC 2737 Entity MIBv2*
- *RFC 2819 RMON MIB*
- *RFC 2863 Interfaces Group MIB*
- *RFC 2865 RADIUS*
- *RFC 2866 RADIUS Accounting*
- *RFC 3046 DHCP Relay Agent Information Option*
- *RFC 3410 SNMPv3*
- *RFC 3411 SNMP Frameworks*
- *RFC 3412 SNMP Message Processing*
- *RFC 3413 SNMPv3 Applications*
- *RFC 3414 SNMPv3 USM*
- *RFC 3415 SNMPv3 VACM*
- *RFC 3576 RADIUS*
- *RFC 3768 Virtual Router Redundancy Protocol (VRRP)*
- *RFC 3917 IP Flow Information Export*
- *RFC 3993 DHCP Subscriber-ID sub-option*
- *RFC 3954 NetFlow Services Export v9*
- *RFC 4022 TCP MIB*
- *RFC 4113 UDP MIB*

• *RFC 4293 IPv6*
• *RFC 4673 RADIUS Dynamic Authorization Server MIB*
• *RFC 5101 – Specification of the IP Flow Information Export (IPFIX)*

Dimensiones del dispositivo:

• *Altura: 4.45cm (1.75in) – 1RU*
• *Ancho: 43.82cm (17.25in)*
• *Profundo: 36.9cm (14.53in)*
• *Peso: 5.0 to 6.4kg (11 to 14lb)*

Especificaciones Potencia

Input Voltage: 100-240VAC
• *Input Current*
– 3 to 6.5A @ 100-120VAC
– 1.5 to 3.3A @ 200-240VAC
• *Power Consumption: 150 to 470W*
• *Thermal Rating: 188 to 788Btu/h*

En la siguiente figura se aprecia el aspecto físico de los switches a instalar

Figura 77- Switches a Instalar

El layout final de cara armario con los switches enracados se aprecia en las siguientes figuras:

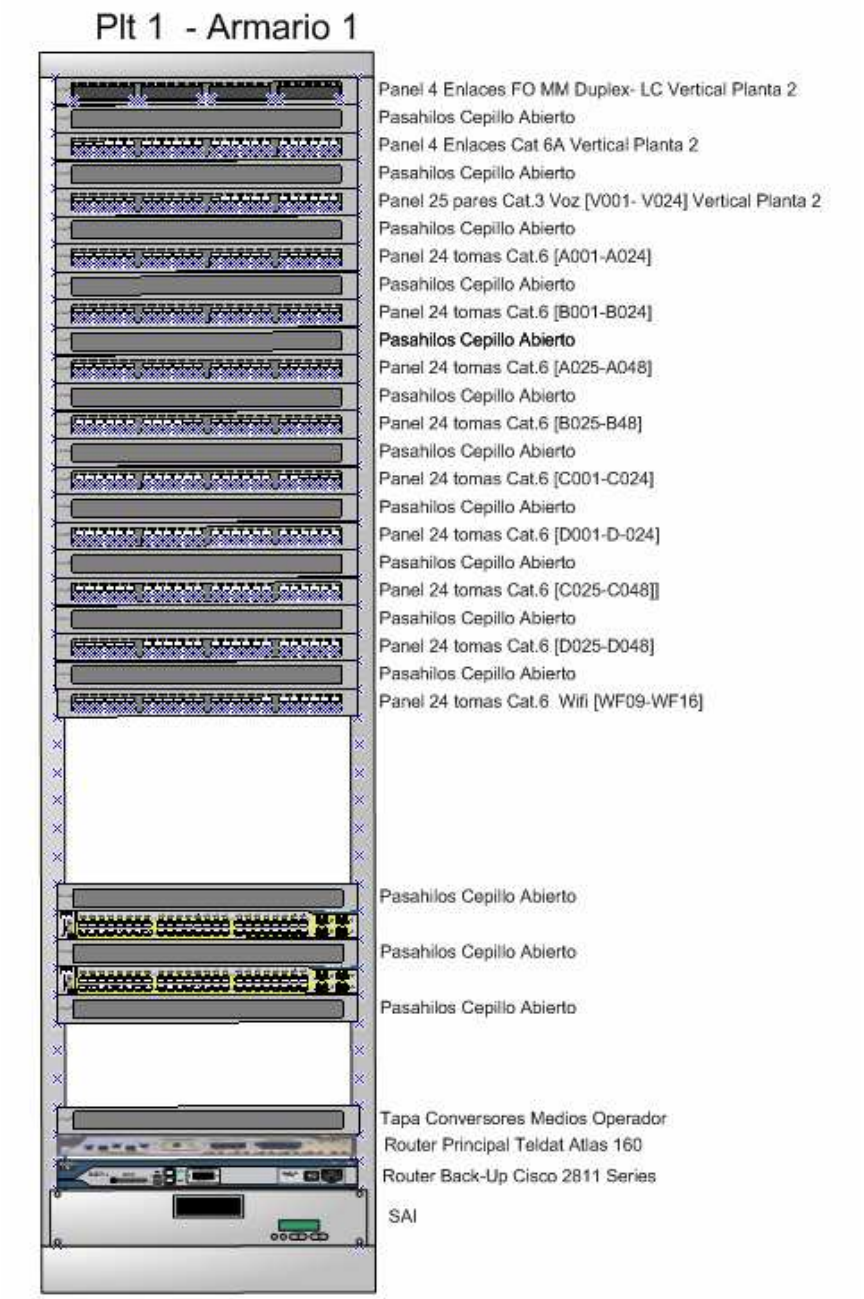


Figura 78- Layout Armario 1 Planta 1 con switches

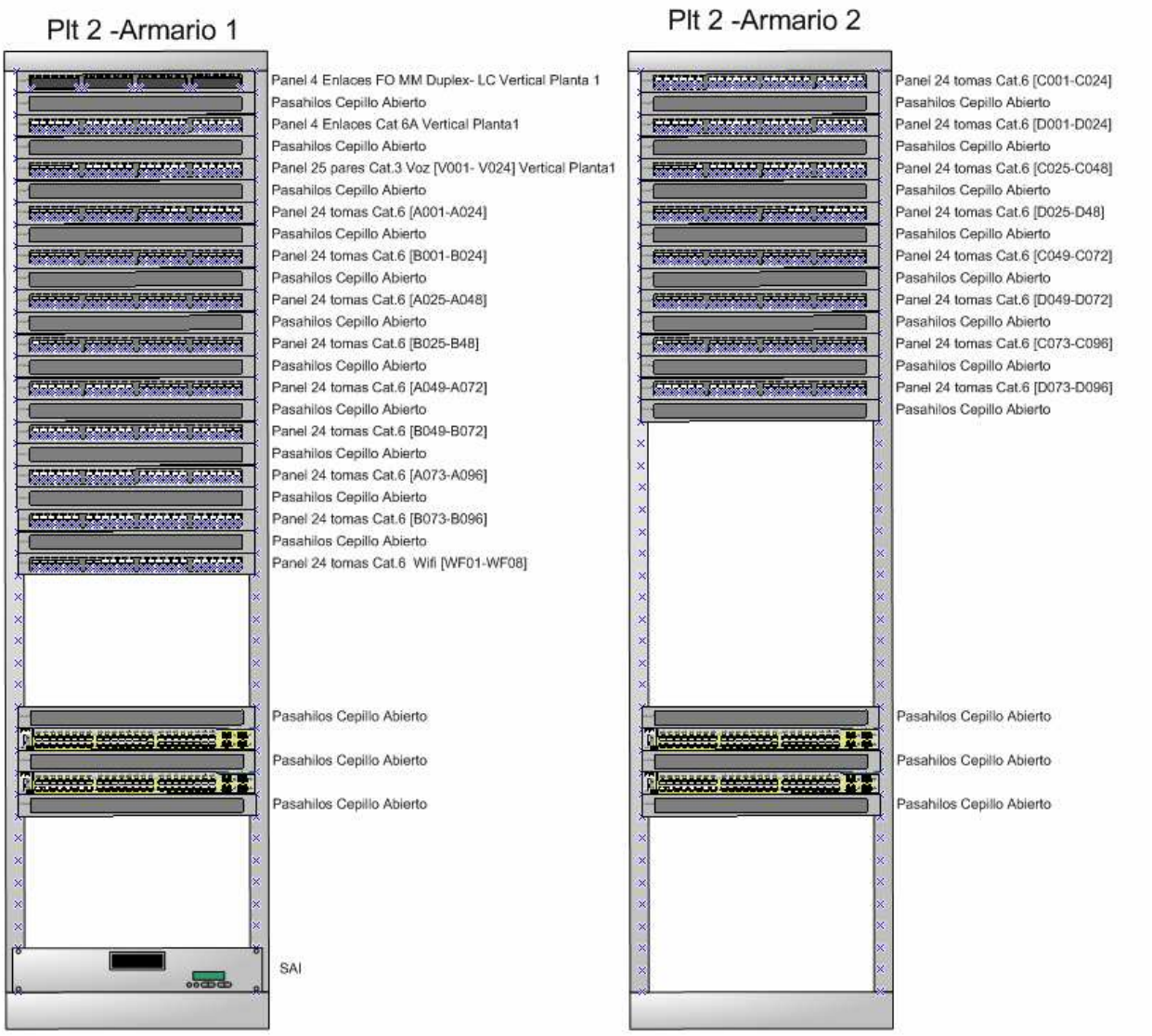


Figura 79- Layout Planta 2 – Armario 1 y 2 – con switches

1.3.3.2. Interconexión switches

En esta apartado se detallará como se va a realizar la interconexión física de:

- Los switches dentro de cada armario

Los enlaces de cascada de switches dentro de cada armario se van a realizar, en la medida de lo posible, utilizando los enlaces Gi (Gigabit Ethernet 1000 Mbps), prefiriblemente en cobre, utilizando latiguillos con terminación RJ45 Cat 6ª. Se da la consideración especial que, al estar dotados solamente de dos enlaces Gi, en el armario 1 de la planta 2 no se disponen de tantos puertos, por lo que la cascada interna se realiza con un puerto Fe (Fast Ethernet 100 Mbps), garantizando la conexión a 1Gbps con el armario 2 de esa misma planta

Interconexión Planta 1 – Armario 1

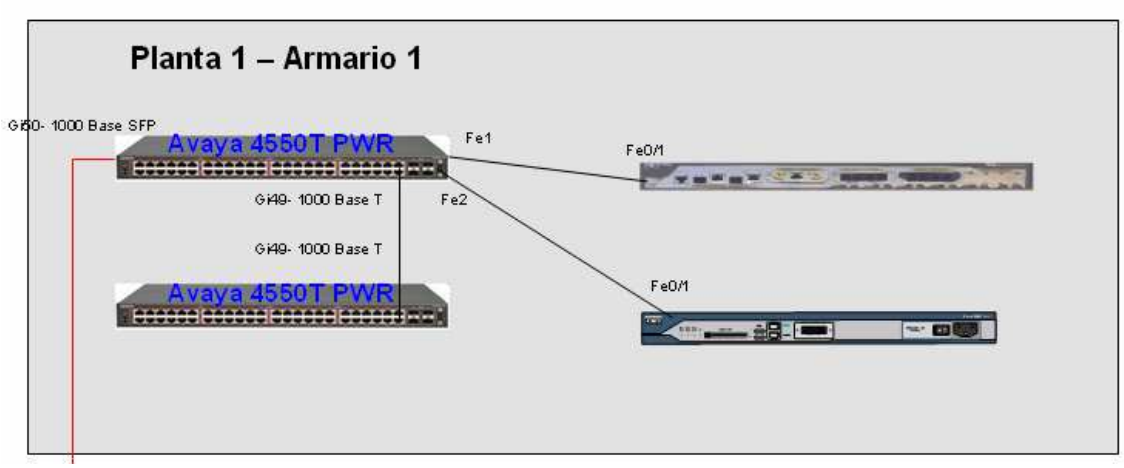


Figura 80- Interconexión switches Planta 1 – Armario 1

Interconexión Planta 2- Armario 1

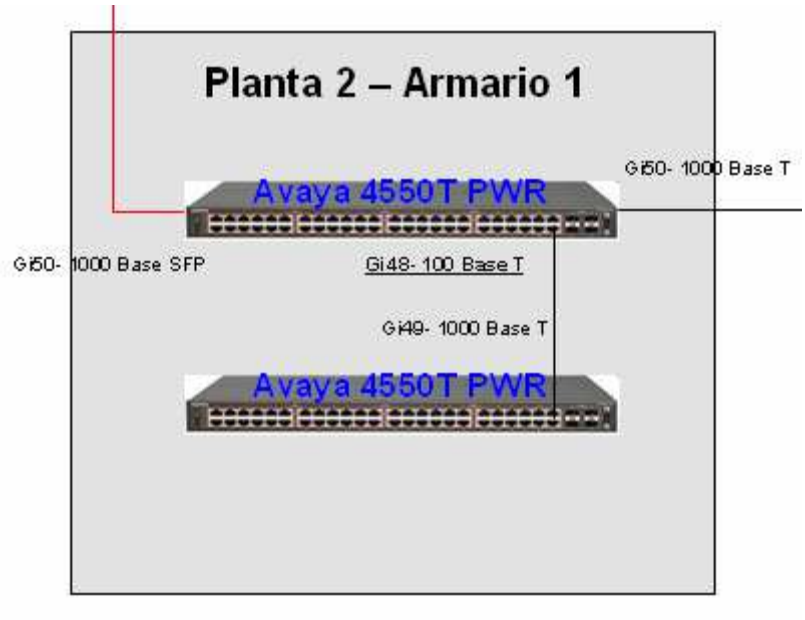


Figura 81- Interconexión switches Planta 2 – Armario 1

Interconexión Planta 2- Armario 2

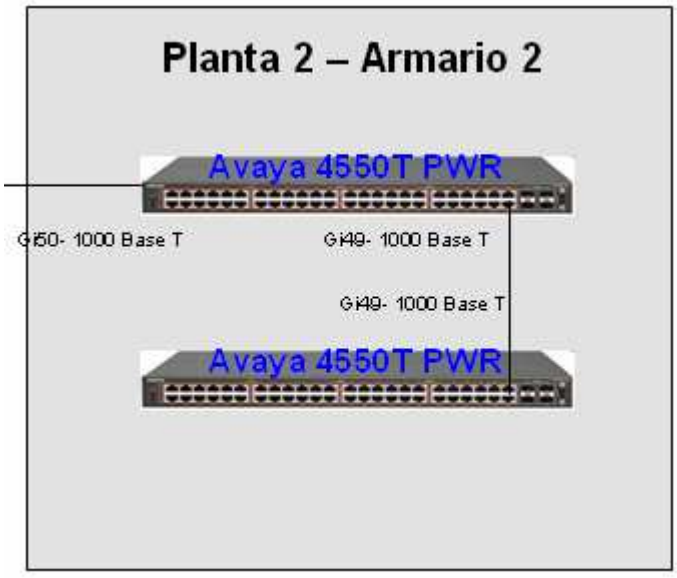


Figura 82- Interconexión switches Planta 2 – Armario 2

- Los armarios dentro de cada planta

En el caso de la planta2 es necesario conectar los dos armarios de planta. Para mantener la conectividad utilizando puertos Gi se realiza la interconexión entre los puertos Gi50 de cada uno de los switches principales del armario. No existen paneles de cableado entre armarios de la planta, por lo que la conexión se realizará con un latiguillos RJ45 directo entre los puertos indicados.

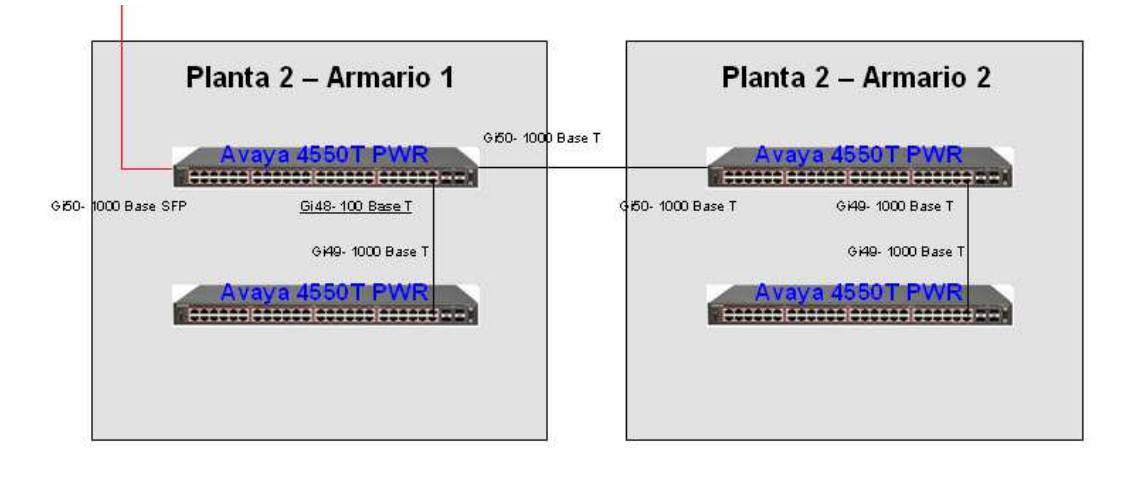


Figura 83-Interconexión armarios planta 2

- Los armarios entre plantas

Es necesario comunicar los armarios 1 de las plantas 1 y 2. Para ello se utilizará el panel de fibra óptica Multimodo OM3 Duplex cableado entre ellos. La conexión se realizará utilizando los puertos 1000 BASE SFP, es decir, utilizando las bahías para colocación de SFP que nos permita introducir latiguillos con terminación LC, de hasta 10 Gbps [por el momento la electrónica no lo soporta, en la versión seleccionada, pero ya se tendrá preparada la vertical entre plantas para un aumento del ancho de banda. En el esquema este enlace está interconectado entre los puertos Gi50 de ambos switches y está marcado en rojo [para identificar conexionado con F.O]

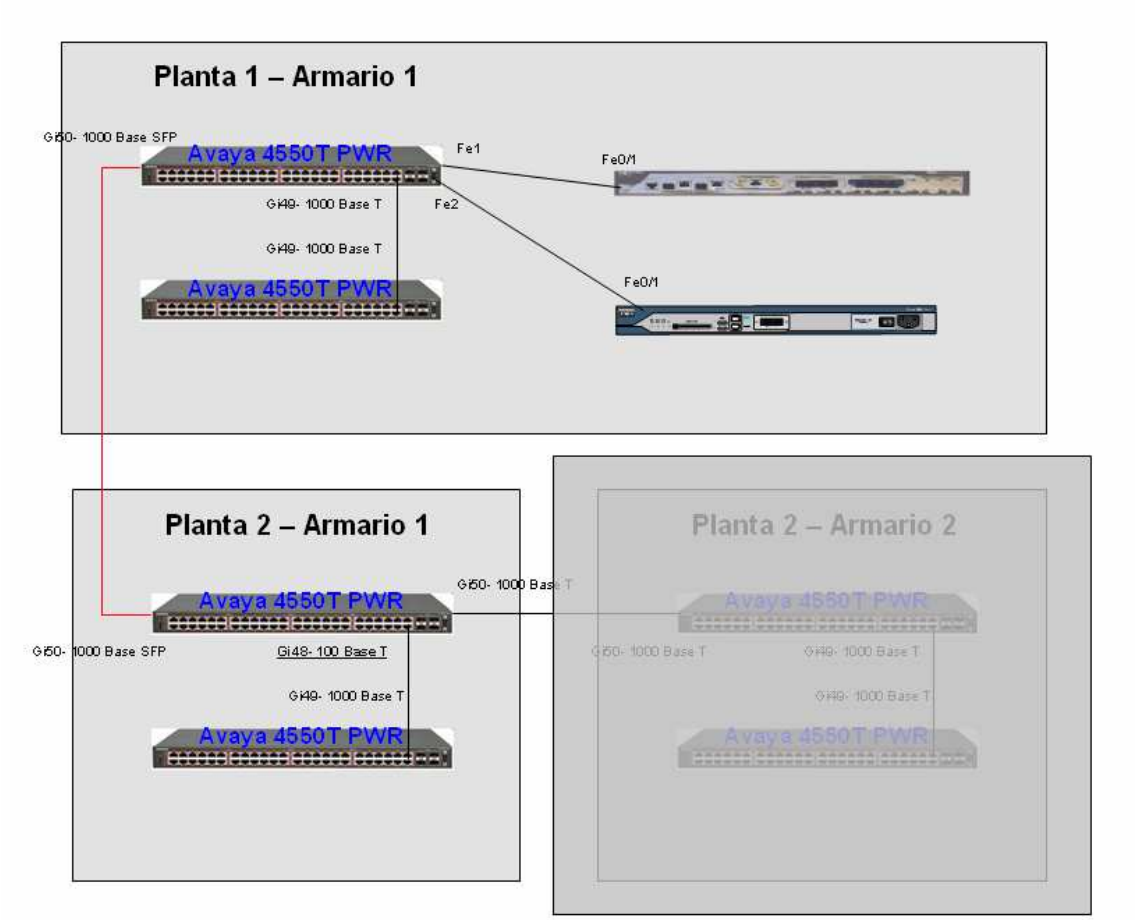


Figura 84 – Interconexión Armarios entre plantas

- Los switches con los equipos del subsistema de nivel 3 [routers] en el armario de la planta 1

En el armario de la planta 1, además de los switches que darán servicio de LAN a los usuarios se encuentran también los equipos del subsistema de nivel 3, que veremos en detalle en el capítulo 1.4. La interconexión con estos dispositivos merece especial atención, al ser el punto final de la línea de comunicaciones.

Así, conectaremos el switch principal del armario con ambos routers, utilizando los puertos Fe1 y Fe2 [Fast Ethernet 100 Mbps].

-Puerto 1 Router principal

-Puerto2: Router de Backup

Es importante hacer notar que estos puertos tendrán forzado tanto la velocidad de funcionamiento [100 Mbps], como el modo de funcionamiento [Full-Duplex], y que este forzado de puertos también deberá darse en el extremo de los routers. Así un problema en la conexión [especialmente de cableado], hará que los puertos se pongan en down. Es preferible una caída total del puerto, que una autonegociación a 10 Half-Duplex, que puede llegar a tardarse en ser descubierta.

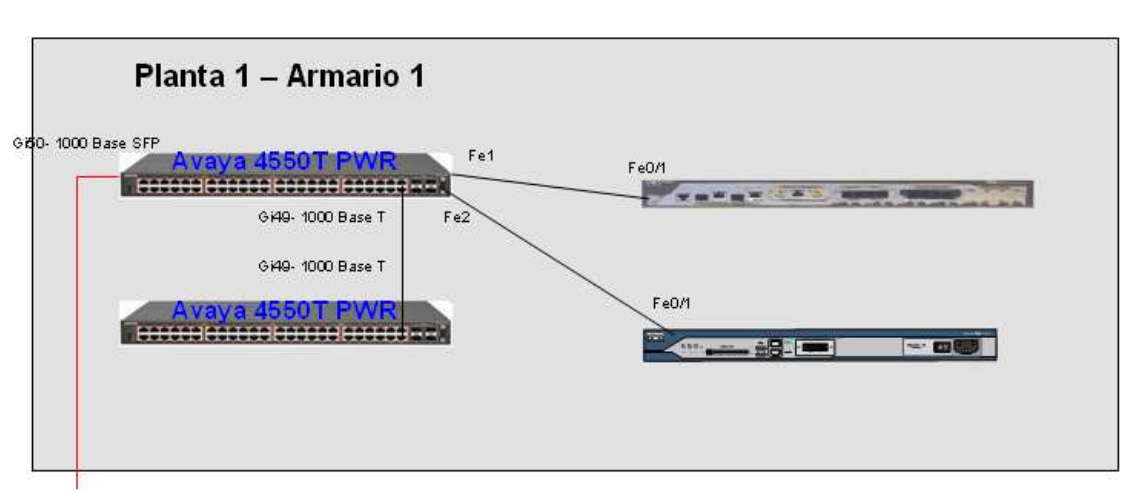


Figura 85 – Interconexión switches routers

La siguiente figura muestra la interconexión total de los elementos de comunicaciones de la sede:

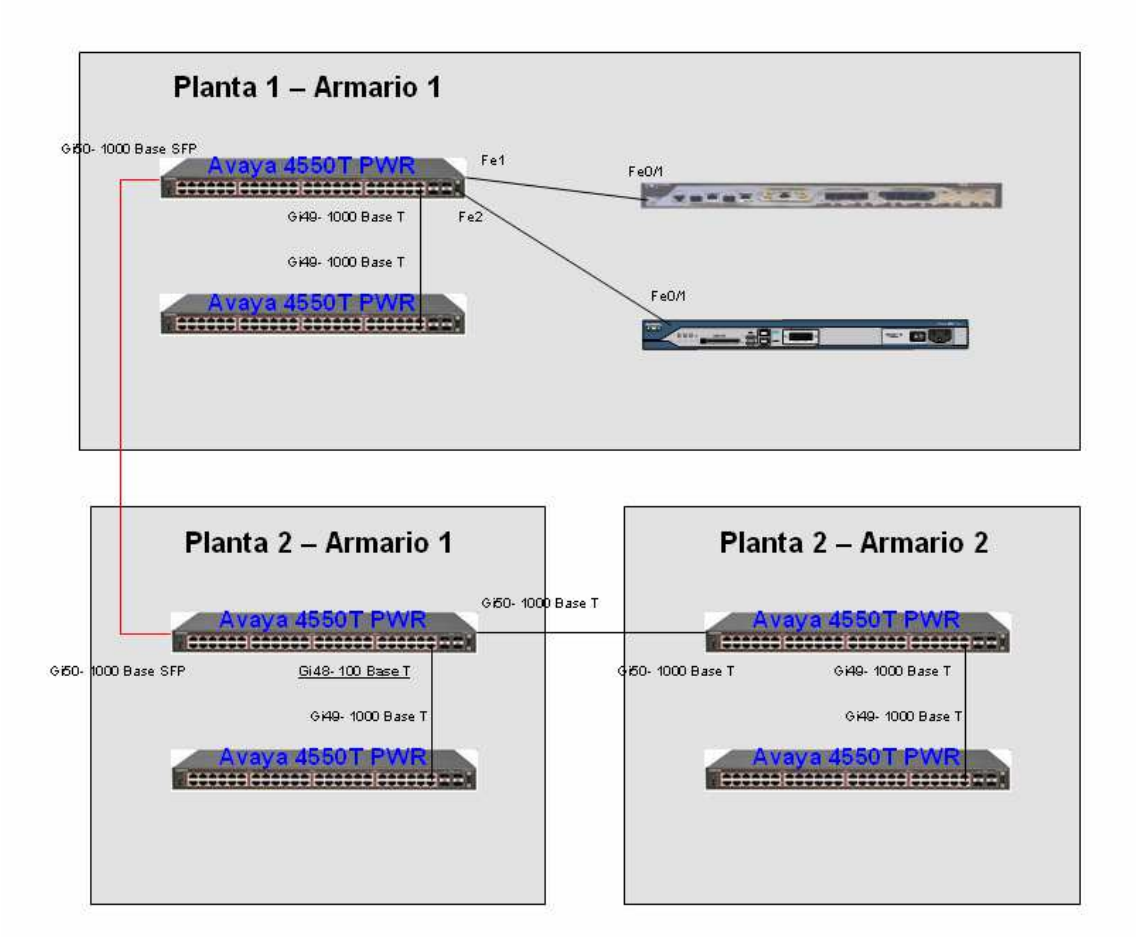


Figura 86-Interconexión elementos comunicaciones Total

Especial atención merece la utilización de una SAI (Sistema de Alimentación Interrumpida) en cada una de las plantas, para la conexión de todos los dispositivos de comunicaciones, ante la posibilidad de caídas en el voltaje, picos de tensión..

Figura 87- SAI

1.3.3.3. Configuración switches.

Se pretende mostrar en este punto las configuraciones reales [puertos, vlans, gestión, snmp..] de los switches que forman parte del proyecto, con especial atención a los puertos que conectan las troncales

La siguiente figura muestra los puertos de interconexión de los switches, y las ips de gestión asignadas a los mismos.

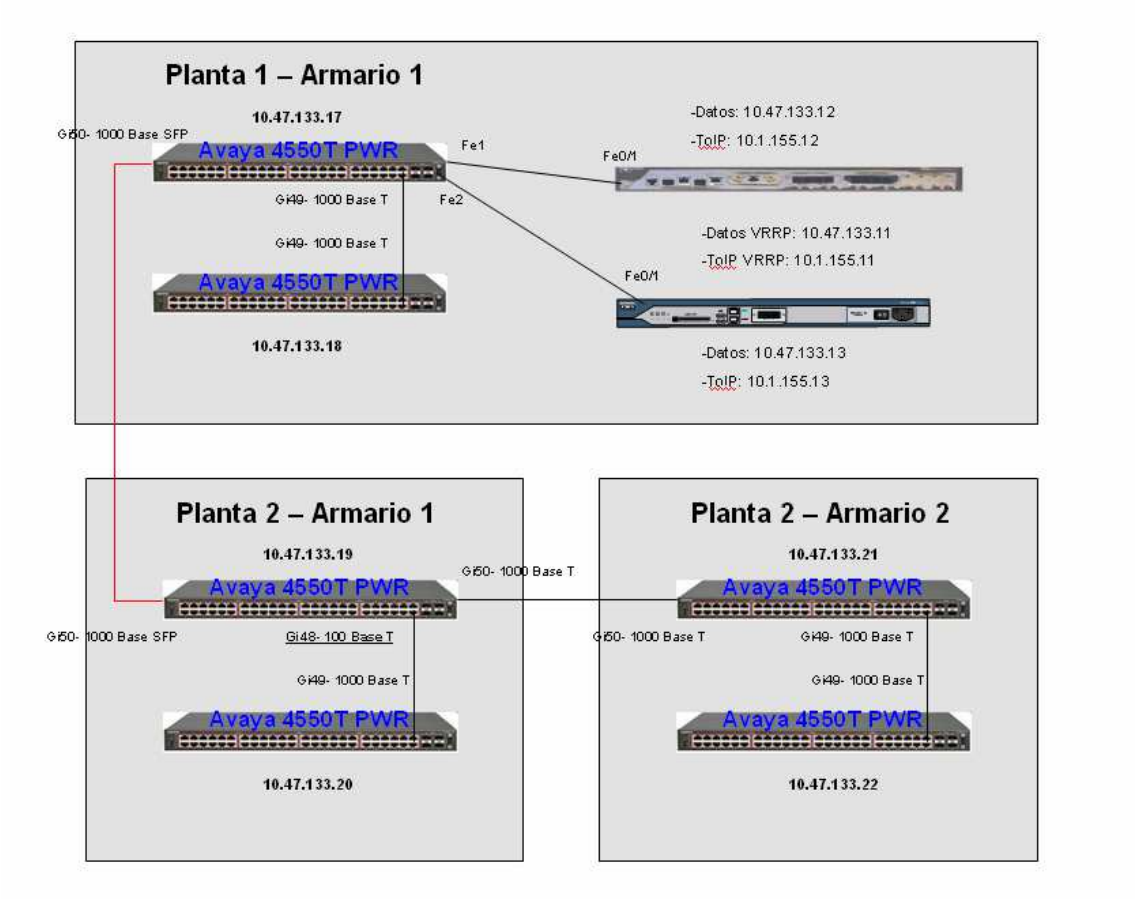


Figura 88 – Topología Subsistema Nivel 2 – LAN

La configuración de todos los switches será exactamente igual, ya que al realizar la conexión de los terminales IP y los PCs utilizando todos los puertos del switch tienen que estar configurados en trunk de la vlan de datos [1], como de la vlan de voz[20]. La única diferencia que encontraremos será las descripciones asociadas a los puertos de interconexión entre switches o con los routers que, evidentemente indicarán contra que equipo se conectan.

Vemos la configuración del switch identificado en el esquema con IP 10.47.133.17.

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 4550T-PWR
! Software version = v5.4.0.008
!
! Displaying only parameters different to default
!================================================
enable
configure terminal
!
! *** CORE ***

! No guardar la configuracion continuamente

no autosave enable
! Servidor NTP - Hora
sntp server primary address 10.1.29.5
sntp enable

! accesos de telnet que los introduzca en el log

telnet-access logging all
! contraseña verificación en local
cli password switch telnet loca
l
! creacion de usuarios

username "operador" "operador" ro
username "comunicaciones" "comunicaciones" rw

!
! *** SNMP ***
! Nombre del equipo
snmp-server name "PFG-Plt1-Rack1"

!
! *** IP  ***
! Ip de gestión y la mascara
ip address switch 10.47.133.17
ip address netmask 255.255.255.0
!


! *** IP Manager ***
! Ips autorizadas para el acceso telnet
ipmgr source-ip 1 10.1.74.182 mask 255.255.255.255
ipmgr source-ip 2 10.1.74.237
ipmgr source-ip 3 10.1.74.198
ipmgr source-ip 4 10.1.74.119
ipmgr source-ip 5 10.1.73.126
ipmgr source-ip 6 10.1.74.138
ipmgr source-ip 7 10.1.73.137
ipmgr source-ip 8 10.1.72.128
ipmgr source-ip 9 10.1.24.208
ipmgr source-ip 10 10.47.133.9
!
```

```
! *** ASSET ID ***
!
!
! *** EAP ***
!
!
! *** IPFIX ***
!
!
! *** System Logging ***
!
!
! *** STACK ***
!
!
! *** Custom Banner ***
!
!
! *** MSTP (Phase 1) ***
!
!The Spanning tree operation mode cannot be changed without rebooting.
!The Spanning tree operation mode is required to be set to MSTP before
!loading this ASCII configuration file.
! Definición de STP : Modo Multispanning-tree
spanning-tree op-mode mstp
! nombre región STP
spanning-tree mstp region region-name "PFG"
! version region STP
spanning-tree mstp region region-version 1

!
! *** VLAN ***
!Definición vlan 20 para ToIP
vlan create 20 type port cist
vlan name 20 "ToIP"
! todos los puertos en trunk para la conexión mediante mini-switch
vlan ports ALL tagging unTagPvidOnly
vlan configcontrol flexible
vlan members 20 ALL
!
! *** EAP Guest VLAN ***
!
!
! *** EAP Fail Open VLAN ***
!
!
! *** EAP Voip VLAN ***
!
!
! *** Port Mirroring ***
!
!
! *** QOS ***
!
! Definición QoS [autoQoS] puro --> El terminal IP que conectamos es un terminal Avaya que entiende la configuración de Qos
qos agent aq-mode pure
!
! *** RMON ***
```

```
!
!
! *** Interface ***
! Denominación de los interfaces mas importantes

interface FastEthernet ALL
name port 1 "conexion-router-ppal-10.47.133.12"
name port 2 "conexion-router-backup-10.47.133.13"
name port 49 "conexion-sw2-PFG-Pl1-Rack1-10.47.133.18"
name port 50 "conexion-sw3-PFG-Pl2-Rack1-10.47.133.19"

exit

! Limitación del tráfico broadcast. Se aplica en todos los puertos una limitación hasta el 80 % de tráfico broadcast

interface FastEthernet ALL
rate-limit port ALL broadcast 8
exit
!
! *** MLT (Phase 1) ***
!
!
! *** MAC-Based Security ***
!
!
! *** LACP ***
!
!
! *** ADAC ***
!
!
! *** MSTP (Phase 2) ***
!
!
! *** VLAN Phase 2***
!
!
! *** MLT (Phase 2) ***
!
!
! *** PoE ***
!
!
! *** RTC ***
!
!
! *** Avaya Energy Saver ***
!
!
! *** AUR ***
!
!
! *** AAUR ***
!
!
! *** L3 ***
!
```

```
! Routing entre las vlans de datos y voz
! IP de gestión adicional al switch dentro de la vlan 20 y del direccionamiento de voz
ip routing
interface vlan 20
ip address 10.1.155.18 255.255.255.0 2
exit

! Ruta estática hacia el gateway [dirección HSRP router virtual]

ip route 0.0.0.0 0.0.0.0 10.47.133.11 1
!
! *** IPV6 ***
!
!
! *** VLACP ***
!
!
! *** DHCP Relay ***
!
!
! *** 802.1ab ***
!

!
! *** 802.1AB MED Voice Network Policies ***
!
!
! *** L3 Protocols ***
!

! --- Proxy ARP ---


! --- UDP Broadcast Forwarding ---


! --- Route Policies ---


! --- OSPF ---


! --- RIP ---

!
! *** DHCP SNOOPING ***
!
!
! *** ARP INSPECTION ***
!
!
! *** IP SOURCE GUARD ***
!
!
! *** STACK MONITOR ***
!
```

Figura 89 – Configuración Switch Nivel 2

1.1.1.1.1. Implantación ToIP

La solución de telefonía de la sede objeto del estudio, será la implantación de un sistema de ToIP puro, es decir, con la instalación de terminales IP conectados directamente a la red IP de la sede.

Para ello se han seleccionado terminales IP del fabricante Avaya, por compatibilidad con los switches de acceso de la sede. Los terminales seleccionados son los siguientes.

- Avaya IP Phone 1210: Terminal básico.
- Avaya IP Phone 1230: Terminal avanzando, permite disponer de varias líneas sobre un mismo terminal físico, captura y transferencia de llamadas, posibilidad de añadir bases de expansión.
- Avaya IP Phone 1140E: Modelo alta gama, pensado para los cargos más importantes de la sede.

Figura 90 – Modelos Terminales IP a instalar

Con la siguiente figura se pretende ilustrar el conexionado entre los terminales IP, los ordenadores y los switches de acceso.

Figura 91- Interconexión Terminal IP y Ordenador

Todos los terminales seleccionados van equipados con un mini-switch interno que nos permite por un lado realizar la conexión del terminal IP con el switch de acceso PoE, y por otro lado se conecta el ordenador/portátil del usuario. De este modo se consigue reducir el número de puntos de cableado ocupados y por tanto el coste de la instalación de infraestructura, al no tener que realizar cableados con tanta densidad de puntos.

Mediante la conexión directa del terminal IP con el switch de planta conseguimos utilizar la opción del PoE, de forma que el terminal sea alimentado directamente por el switch, sin necesidad de conexiones eléctricas adicionales.

Además es interesante hacer mención especial a dos comandos de visualización en el switch que nos da información básica de los teléfonos conectados en cada puerto, de su dirección ip, así como datos básicos como MAC, modelo, versión de firmware. Este descubrimiento se basa en la localización de vecinos [neigbor] con el siguiente comando:

```
!
! Para verificar los telefonos conectados, información basica, se puede ejecutar
sh lldp neighbor detail
! Resultado

Port: 12    Index: 23              Time: 0 days, 00:01:22
      ChassisId: Network address    IPv4  10.1.155.107
      PortId:    MAC address       fc:a8:41:f3:0e:1f
      SysCap:    TB / TB           (Supported/Enabled)
      PortDesc:  Avaya IP Deskphone
      SysDescr:  Avaya 1210 IP Deskphone, Firmware:062AC8L


PVID: 0                       PPVID Supported: not supported(0)
VLAN Name List: 20            PPVID Enabled: none

Dot3-MAC/PHY Auto-neg: supported/enabled      OperMAUtype:  100BaseTXFD
PSE MDI power:         not supported/disabled  Port class:   PD
PSE power pair:        signal/not controllable Power class:  2
LinkAggr: not aggregatable/not aggregated     AggrPortID:   0
                                MaxFrameSize: 1522
PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD)

MED-Capabilities: CNLDI / CNDI       (Supported/Current)
MED-Device type:  Endpoint Class 3
MED-Application Type: Voice                VLAN ID: 20
L2 Priority: 6        DSCP Value: 40       Tagged Vlan, Policy unknown
```

MED-Application Type: Voice Signaling VLAN ID: 20
L2 Priority: 6 DSCP Value: 40 Tagged Vlan, Policy unknown
Med-Power Type: PD Device Power Source: Unknown
Power Priority: High Power Value: 6.0 Watt
HWRev: FWRev: 062AC8L
SWRev: SerialNumber:
ManufName: Avaya-05 ModelName: 1210 IP Deskphone
AssetID:

Port: 18 *Index: 29 Time: 0 days, 00:01:25*
ChassisId: Network address IPv4 10.1.155.99
PortId: MAC address cc:f9:54:93:c3:26
SysCap: TB / TB (Supported/Enabled)
PortDesc: Avaya IP Deskphone
SysDescr: Avaya 1210 IP Deskphone, Firmware:062AC8L

PVID: 0 PPVID Supported: not supported(0)
VLAN Name List: 20 PPVID Enabled: none

Dot3-MAC/PHY Auto-neg: supported/enabled OperMAUtype: 100BaseTXFD
PSE MDI power: not supported/disabled Port class: PD
PSE power pair: signal/not controllable Power class: 2
LinkAggr: not aggregatable/not aggregated AggrPortID: 0
MaxFrameSize: 1522
PMD auto-neg: 10Base(T, TFD), 100Base(TX, TXFD)

MED-Capabilities: CNLDI / CNDI (Supported/Current)
MED-Device type: Endpoint Class 3
MED-Application Type: Voice VLAN ID: 20
L2 Priority: 6 DSCP Value: 40 Tagged Vlan, Policy unknown
MED-Application Type: Voice Signaling VLAN ID: 20
L2 Priority: 6 DSCP Value: 40 Tagged Vlan, Policy unknown
Med-Power Type: PD Device Power Source: Unknown
Power Priority: High Power Value: 6.0 Watt
HWRev: FWRev: 062AC8L
SWRev: SerialNumber:
ManufName: Avaya-05 ModelName: 1210 IP Deskphone
AssetID:

Port: 6 *Index: 30 Time: 0 days, 00:01:50*
ChassisId: Network address IPv4 10.1.155.115
PortId: MAC address 58:16:26:bf:f5:a9
SysCap: TB / TB (Supported/Enabled)
PortDesc: Avaya IP Deskphone
SysDescr: Avaya 1210 IP Deskphone, Firmware:062AC8L

PVID: 0 PPVID Supported: not supported(0)
VLAN Name List: 20 PPVID Enabled: none

Dot3-MAC/PHY Auto-neg: supported/enabled OperMAUtype: 100BaseTXFD
PSE MDI power: not supported/disabled Port class: PD
PSE power pair: signal/not controllable Power class: 2
LinkAggr: not aggregatable/not aggregated AggrPortID: 0
MaxFrameSize: 1522
PMD auto-neg: 10Base(T, TFD), 100Base(TX, TXFD)

MED-Capabilities: CNLDI / CNDI (Supported/Current)

```
MED-Device type:  Endpoint Class 3
MED-Application Type: Voice                VLAN ID: 20
L2 Priority: 6       DSCP Value: 40        Tagged Vlan, Policy unknown
MED-Application Type: Voice Signaling      VLAN ID: 20
L2 Priority: 6       DSCP Value: 40        Tagged Vlan, Policy unknown
Med-Power Type: PD Device          Power Source: Unknown
Power Priority: High             Power Value:    6.0 Watt
HWRev:                          FWRev: 062AC8L
SWRev:                          SerialNumber:
ManufName: Avaya-05              ModelName: 1210 IP Deskphone
AssetID:
```

Figura 92 – Switch nivel 2: Información de los terminales IP conectados

Otro de los aspectos claves, es la gestión del consumo de los terminales IP; mediante el control del consumo del PoE realizado en el switch. Para ello existen básicamente tres comandos

- sh poe-main-status: visión general del estado del PoE, con consumo general
- sh poe-port-status: estado del parámetro PoE en cada puerto del switch
- sh poe-power-measurement: consume particulas de tension y corriente en cada Puerto

```
! Consumo del PoE
PFG-Plt1-Rack1#sh poe-main-status
PoE Main Status - Stand-alone
-------------------------------------------------
Available DTE Power       : 370 Watts
DTE Power Status          : Normal
DTE Power Consumption     : 84 Watts
DTE Power Usage Threshold  : 80 %
Traps Control Status      : Enable
PD Detect Type            : 802.3af and Legacy
Power Source Present      : AC Only
AC Power Status           : Present
DC Power Status           : Not Present


#sh poe-port-status
     Admin      Current                        Limit
Port  Status     Status           Classification   (Watts)  Priority
----  -------    -----------------   --------------   -------  --------

44    Enable     Detecting              0        16       Low
45    Enable     Detecting              0        16       Low
46    Enable     Delivering Power       2        16       Low
47    Enable     Delivering Power       2        16       Low
48    Enable     Detecting              0        16       Low

#sh poe-power-measurement
Port  Volt(V)  Current(mA)   Power(Watt)
----  -------  -----------   ---------------
44    0.0      0             0.000
45    0.0      0             0.000
46    47.8     58            2.772
```

```
47   47.9    59          2.826
48   0.0     0           0.000
```

Figura 93 – Switch Nivel 2 – Información estado PoE. Consumo

Para una correcta implementación de la QoS en una instalación de ToIP es necesario que los switches prioricen el tráfico de voz sobre el tráfico de datos, de forma que nos aseguremos que las tramas de datos que contengan voz, sean priorizadas, tengan menos retrasos, tenga menos jitter [variación del retardo], en definitiva sean tratadas de forma prioritaria sobre las tramas de datos que contienen información de datos.

Al tratarse de equipamiento del mismo fabricante, terminales IP y switches son capaces de "dialogar" utilizando un protoloco propietario que nos permite de forma muy sencilla aplicar QoS en la LAN. En concreto en la configuración del switch, vemos que activamos una auto-qos puro, es decir, terminal IP y switch son del mismo fabricante. Si no fuera así, habría que activar un auto-qos parcial, y verificar los tags de marca que realizar el teléfono, para indicar al switch que tramas, con que tag tiene que priorizar.

```
! *** QOS ***
!
! Definición QoS [autoQoS] puro --> El terminal IP que conectamos es un terminal Avaya que entiende la configuración de Qos
qos agent aq-mode pure
```

Figura 94- Switch Nivel 2 – Configuración QoS

Debido a que se va a utilizar un direccionamiento distinto para la subred de voz que para la subred de datos, de cara a poder obtener arp de los puertos, ips y macs asociadas en el switch, es necesario que el switch tenga configurada una ip de gestión en ambos rangos de direccionamiento. Por tanto, para el switch de ejemplo, tendremos:

- IP gestión rango datos: 10.47.133.17
- IP gestión rango voz: 10.1.155.18

```
! *** IP  ***
! Ip de gestión y la mascara
ip address switch 10.47.133.17
ip address netmask 255.255.255.0
!


! Routing entre las vlans de datos y voz
! IP de gestión adicional al switch dentro de la vlan 20 y del direccionamiento de voz
ip routing
interface vlan 20
ip address 10.1.155.18 255.255.255.0 2
exit
```

Figura 95- Switch Nivel 2 – Direccionamiento Gestión

De esta forma seremos capaces de ver las entradas arp para ambas vlans.

```
PFG-Plt1-Rack1#sh arp vlan 1
================================================
IP ARP
        ============================================================
P Address     Age (min) MAC Address      VLAN-Unit/Port/Trunk Flags

        ------------------------------------------------------------------------
        10.47.133.255   0       ff:ff:ff:ff:ff:ff VLAN#1            LB
        10.47.133.15    265     00:24:73:8c:f2:41 VLAN#1-50         D
        10.47.133.183   139     d0:27:88:07:52:8b VLAN#1-50         D
        10.47.133.14    266     00:1e:c1:c0:c2:01 VLAN#1-50         D
        10.47.133.230   164     00:19:21:be:c7:f6 VLAN#1-50         D
        10.47.133.166   132     90:e6:ba:e8:81:88 VLAN#1-50         D
        10.47.133.38    113     90:fb:a6:4a:af:50 VLAN#1-50         D
        10.47.133.110   82      00:19:21:bd:cd:cf VLAN#1-50         D
        10.47.133.229   141     00:00:74:ac:bf:53 VLAN#1-50         D
        10.47.133.173   138     00:23:7d:1c:f0:48 VLAN#1-50         D
        10.47.133.93    82      00:1b:b9:94:1f:50 VLAN#1-50         D
        10.47.133.77    51      d0:27:88:07:50:42 VLAN#1-50         D
        10.47.133.36    209     e0:cb:4e:35:13:53 VLAN#1-50         D
        10.47.133.188   201     00:00:74:ca:22:5c VLAN#1-50         D
        10.47.133.156   194     d0:27:88:07:50:91 VLAN#1-50         D
        10.47.133.180   170     d0:27:88:07:50:2f VLAN#1-50         D
        PFG-Plt1-Rack1#sh arp vlan 20
        ============================================================
                                IP ARP
        ============================================================I
P Address     Age (min) MAC Address      VLAN-Unit/Port/Trunk Flags

        ------------------------------------------------------------------------
        10.1.155.255    0       ff:ff:ff:ff:ff:ff VLAN#20           LB
        10.1.155.15     266     00:1e:c1:c0:c2:01 VLAN#20-50        D
        10.1.155.12     34      00:1e:7a:60:3e:68 VLAN#20-50        D
        10.1.155.17     0       70:38:ee:43:c0:41 VLAN#20           L
        10.1.155.0      0       ff:ff:ff:ff:ff:ff VLAN#20           LB
        Total ARP entries : 5
        ------------------------------------------------------------------------
        Flags Legend:
        S=Static, D=Dynamic, L=Local, B=Broadcast
```

1.1.1.1.2. Segmentación vlans

Como se ha comentado anteriormente es necesario una segmentación de vlans para dotar a la red LAN de los servicios de datos y voz, y que sobre todo un posible problema en el servicio de datos [tormentas de broadcast, problemas de ancho de banda]

Como hemos visto en la configuración de los puertos del switch, para que esta arquitectura funcione, será necesario que todos los puertos de usuario del switch estén configurados en trunk de las vlans de datos [1] y de la vlan de voz [20]

```
! *** VLAN ***
!Definición vlan 20 para ToIP
vlan create 20 type port cist
vlan name 20 "ToIP"
! todos los puertos en trunk para la conexión mediante mini-switch
vlan ports ALL tagging unTagPvidOnly
vlan configcontrol flexible
vlan members 20 ALL
```

Figura 96- Switch Nivel 2 – Configuración vlans

```
! Limitación del tráfico broadcast. Se aplica en todos los puertos una limitación hasta el 80 % de tráfico broadcast
interface FastEthernet ALL
rate-limit port ALL broadcast 8
exit
```

Figura 97- Switches Nivel 2 – Limitación Broadcast

1.1.1.1.3. Gestión de los dispositivos

Para poder realizar un buen control y diagnostico de los dispositivos de nivel 2 es necesario contar con herramientas que nos ayuden en la gestión de los mismos. En general, la gestión de los dispositivos de nivel 2 está basada en el protocolo SMNP, **Simple Network Management Protocol, RFC 1157,** pensado para facilitar el intercambio de información en la administración de dispositivos en red.

La configuración es relativamente sencilla, es necesario básicamente habilitar una comunidad, al menos de lectura, en el dispositivo a gestionar, para que un software de gestión pueda consultar las variables que se estimen oportunas. La configuración SNMP en nuestros switches es la siguiente:

```
!
! *** SNMP ***
! Nombre del equipo
snmp-server name "PFG-Plt1-Rack1"
snmp-server community "compfg" ro
```

Se le dota al dispositivo de un nombre único dentro de la red a gestionar y se habilita una comunidad de solo lectura "read-only – ro" denominada ***compfg.***

Veamos a continuación las distintas formas que se tienen para gestionar el dispositivo:

- Gestión Dispositivo via interfaz **Telnet o ssh**

Utilizando El software putty iniciamos una sesión telnet contra la ip de gestión del dispositivo.

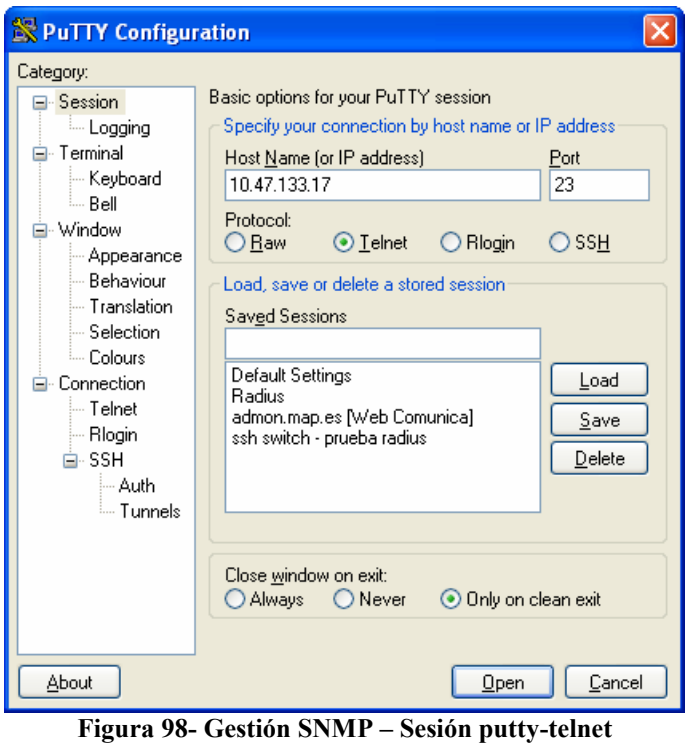


Figura 98- Gestión SNMP – Sesión putty-telnet

Se obtiene el siguiente prompt del fabricante Avaya. Pulsando Ctrl+Y nos presenta la pantalla de usuario y contraseña

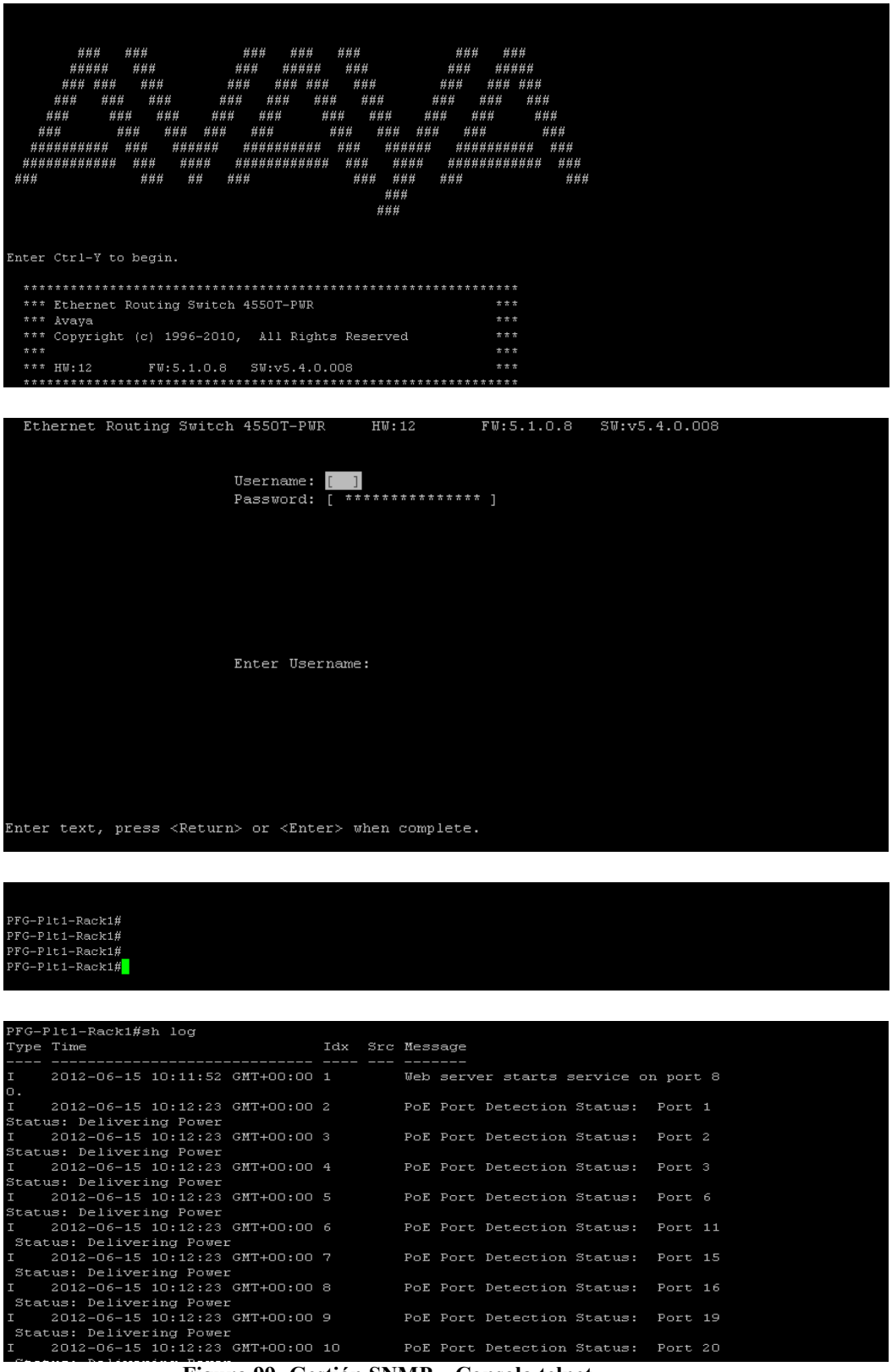


Figura 99- Gestión SNMP – Consola telnet

- Gestión de dispositivo con interfaz WEB

Una gestión más amigable, aunque en ocasiones restringidas en lo que a configuraciones se refiere es la interfaz WEB que incorporan la gran parte de los dispositivos. El acceso se realiza a través de un navegador de Internet, utilizando la dirección ip de gestión del switch a gestionar.

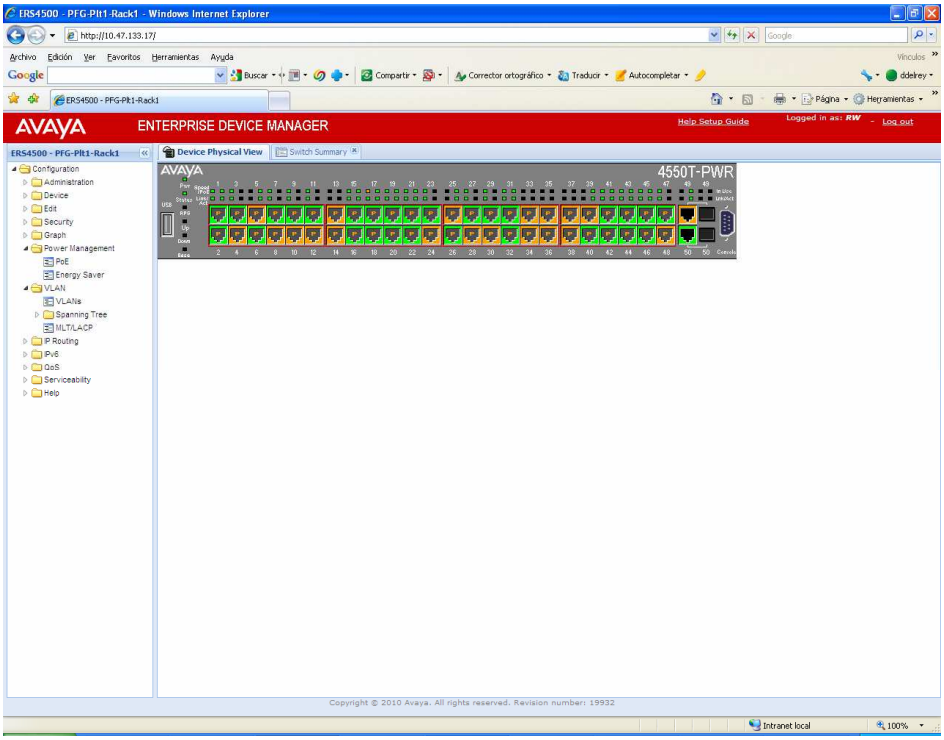


Figura 100- Switches Nivel 2 – Visión general

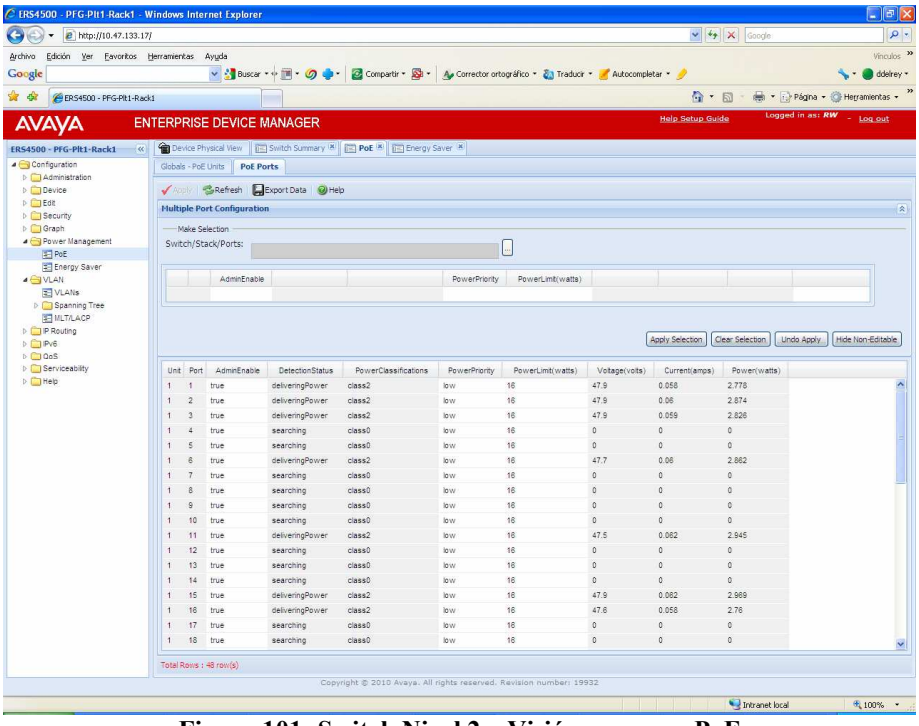


Figura 101- Switch Nivel 2 – Visión consumo PoE

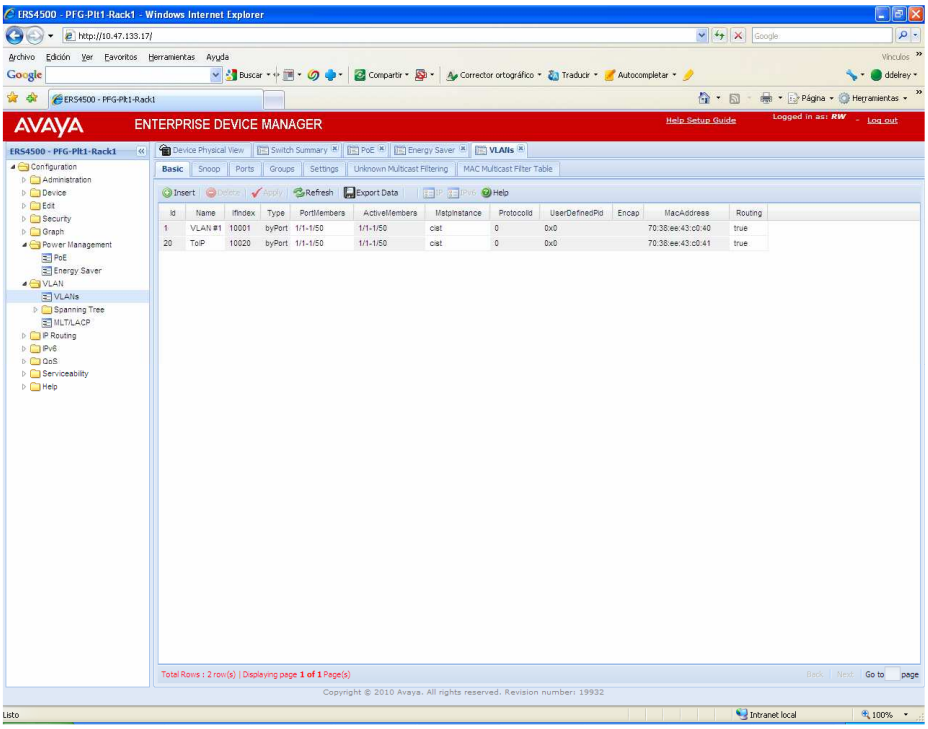


Figura 102- Switch Nivel 2 – Configuración vlan

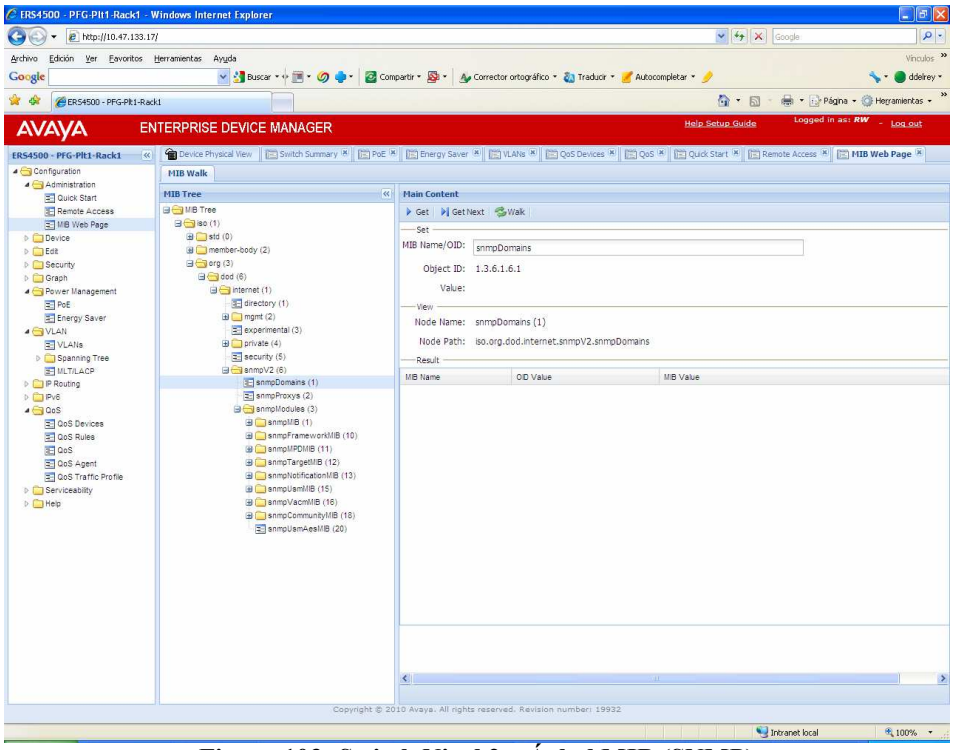


Figura 103- Switch Nivel 2 – Árbol MIB (SNMP)

- Gestión eventos, traps, tráfico por puertos mediante herramienta específica: WhatsUP de IpSwitch

Existen en el mercado multitud de herramientas de gestión de dispositivos de comunicaciones, basados en información SNMP. Se ha seleccionado el producto WhatsUp de IpSwitch, por su facilidad de puesta en marcha y su competitivo precio.

Es un producto basado únicamente en el estándar SNMP, no es propietario de ningún fabricante, por lo que se puede indicar que es multiplataforma.

En palabras del propio fabricante:

''Diseñada sobre una arquitectura central escalable y ampliable, WhatsUp Gold Distributed es una solución completa de monitoreo de aplicaciones, servidor y redes diseñada para gestionar redes complejas, con sitios múltiples. Compatible con instalaciones centrales y remotas, WhatsUp Gold Distributed Edition proporciona gestión y monitoreo de redes de manera local, así como también, un resumen de todos los datos críticos para el sitio central para realizar análisis y acciones de manera coordinada."

Algunas imágenes del producto.

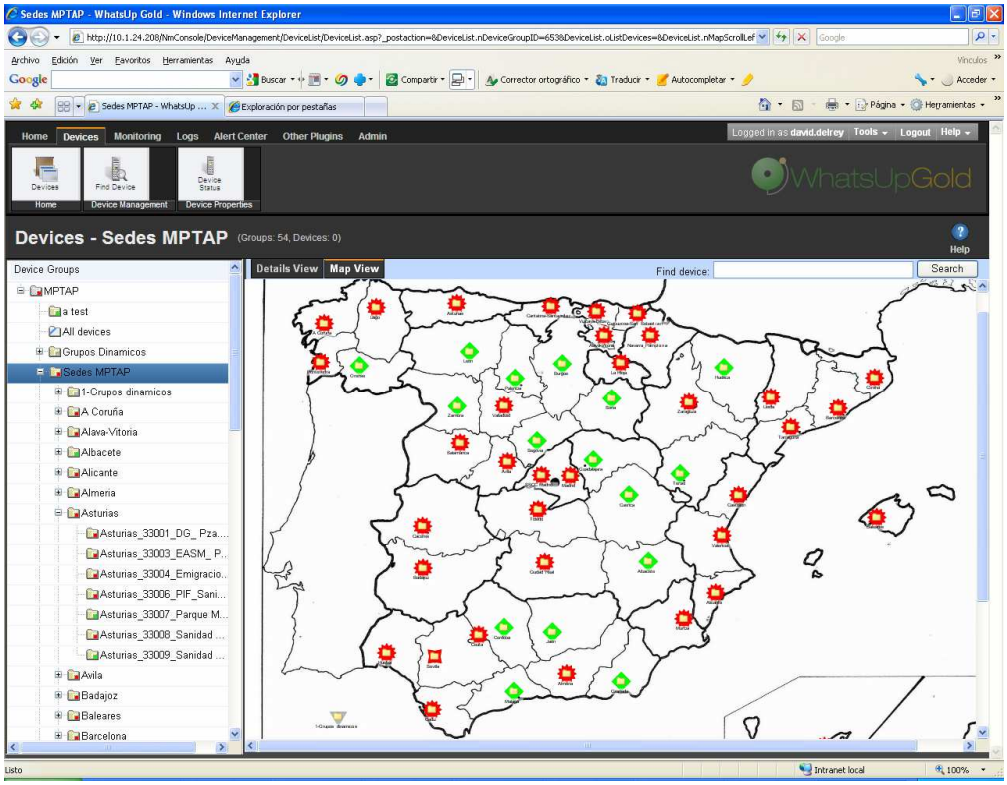


Figura 104 Gestión Switch Nivel 2- WhatsUp – Imagen 1

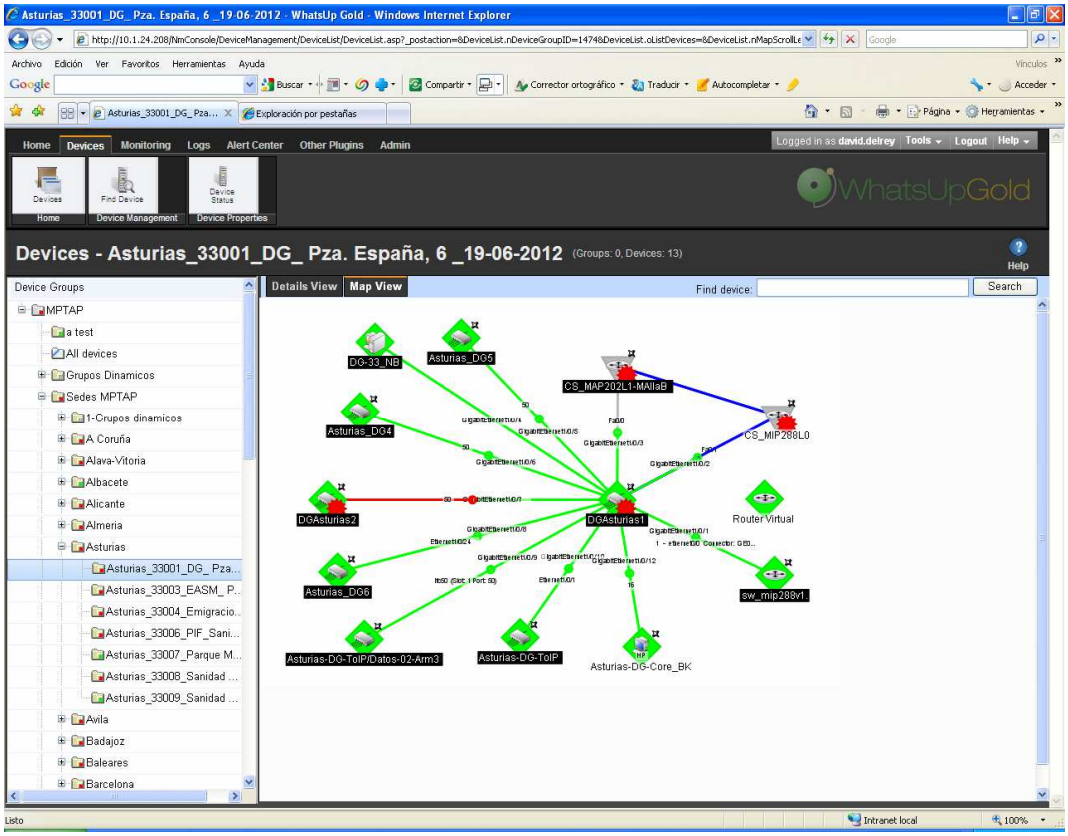


Figura 105 - Gestión Switch Nivel 2- WhatsUp – Imagen 2

1.3.3.4. Configuración Puntos de Acceso Wifi

Se ha seleccionado un sistema Wifi basado en gestión centralizada del fabricante AeroHive, en concreto el Hive AP 330, que tiene las siguientes características

El HiveAP 330 es un Punto de Acceso 802.11n de alto rendimiento y fiabilidad. Proporciona alto rendimiento dual simultaneo (2,4 GHz y 5 GHz) 802.11n 3x3 con tres flujos espaciales MIMO (450Mbps por radio), así como puertos duales 10/100/1000.

El HiveAP 330 es una solución 3x3 MIMO diseñada para entornos empresariales que demandan alto ancho de banda. Con radios múltiples y capacidad de proporcionar servicios en las bandas de 2,4 GHZ y 5 GHZ al mismo tiempo, puede proporcionar hasta una tasa de datos de 450 Mbps.

Proporciona MESH y compatibilidad con el 802.11a, b y clientes g, es el único con arquitectura sin controlador.

Los Puntos de Acceso (AP) de la serie 100 proporcionan un alto rendimiento concurrente doble de (2,4 y 5 GHz) 802.11n (2x2) MIMO, así como un puerto Ethernet 10/100/1000.

Figura 106 – HiveAP 330 – Punto de Acceo Wifi

En lo que respecta a la alimentación de los equipos la conexión se realizará utilizando el switch PoE y por tanto tendremos asegurada la alimentación de los mismos.

Los dispositivos soportan 802.11i, WPA, WPA2, WEP, 802.1X, PSK, Wi-Fi Certificado Alliance.

La gran potencia de este tipo de soluciones centralizadas consisten en que precisamente se utiliza un solo contenedor para la gestión de todos los APs, contenedor que en el caso de AeroHive es accesible desde Internet. Este contenedor se denomina HiveManager y tiene las siguientes características.

El **HiveManager** es un sistema de gestión de la infraestructura de red Wireless que proporciona la configuración centralizada, la monitorización, informes y la resolución de problemas. Este appliance-virtual de gestión no es esencial para la operación normal de la infraestructura de red Wireless.

- Gestión Simple Centralizada

Una sola instancia de gestión central para miles de HiveAPs.

La función de la políticas basada en perfiles permite cambios a la totalidad de grupos de HiveAPs con unos pocos clics .

Actualización Simple y centralizada de firmware .

Mapas de red, que permiten una fácil visualización de la topología y el estado de la fiabilidad.

El servicio es supervisado 24x7 con copias de seguridad diarias fuera de la ubicación e instalaciones de recuperación de desastres

Situado en un centro de SAS 70 Tipo 2, Nivel 4 de datos

- Seguridad y Privacidad

Atención al cliente y red de datos privada y segura.

El tráfico de clientes no atraviesa la red de Aerohive.

- Sin configuración inicial en el despliegue de HiveAP.

Aprovisionamiento automático de enlace en el HiveManager - todo lo que hay que hacer es conectar e iniciar sesión

- Seguimiento e Informes

Capacidades de auditoría de configuración para asegurar que todas las configuraciones están al día.

Recopilación centralizada de alertas ante ataques, puntos de acceso ajenos y de clientes.

Monitorización en tiempo real de alarmas y eventos de los HiveAPs

El HiveManager permite una gestión sofisticada basada en la política de identidad así como una configuración sencilla de dispositivos, actualizaciones de firmware HiveOS™, monitorización de los HiveAP™ dentro de una arquitectura WLAN de Control Cooperativo y troubleshooting simplificado.

Dentro de la arquitectura de Control Cooperativo, los HiveAPs se ocupan de su propio control y de las funciones de reenvío de datos. Esto deja al HiveManager con la única responsabilidad de gestionar y monitorizar a los HiveAPs. Aunque se elimine de la red el HiveManager, los HiveAPs continúan funcionando y proporcionando todas sus funcionalidades. Sin toda la sobrecarga de control y reenvío de datos que existe en soluciones de gestión WLAN basadas en controladores, la arquitectura de HiveManager

escala para permitir la gestión y monitorización de miles de HiveAPs desde una única consola.

En la siguiente figura se puede ver el interfaz Web centralizado para el control de los puntos de accesos dados de alta.

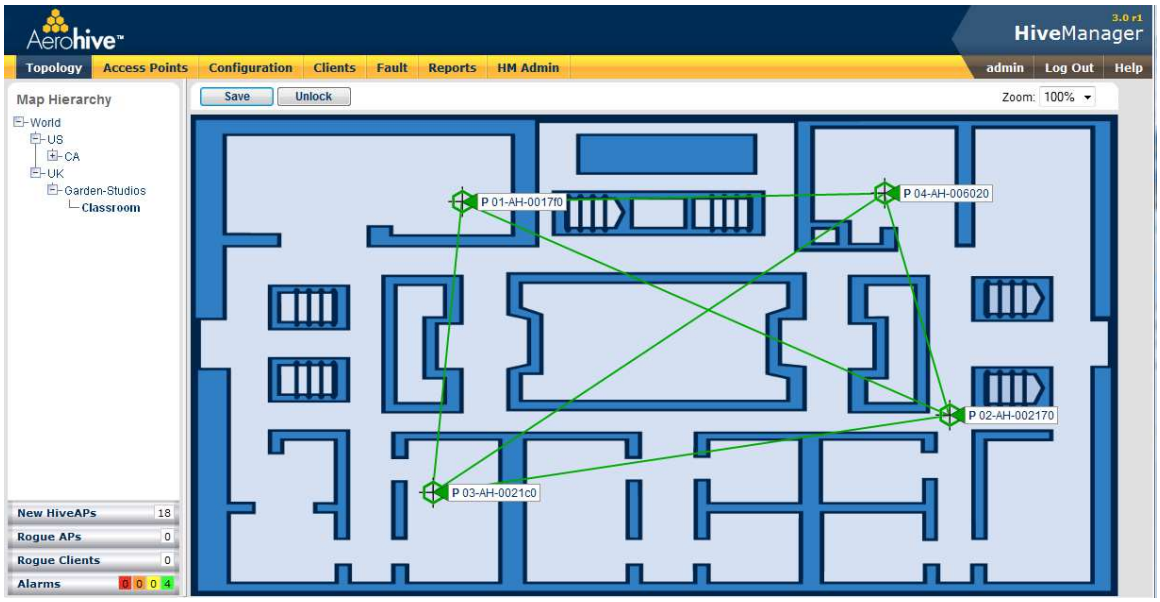


Figura 107- Acceso WEB Centralizado HiveManager- Control APs

Los HiveAPs y el HiveManager se comunican entre sí usando el protocolo borrador del IETF (Internet Engineering Task Force) para el estándar CAPWAP (Control and Provisioning Wireless Access Points), así como un conjunto de aplicaciones estándares incluyendo SSHv2, SCP, y SNMP. Con estos protocolos y aplicaciones, el HiveManager puede gestionar de forma segura y efectiva las configuraciones y registros de monitorización, y actualizar los sistemas de operación de los HiveAPs.

Aunque se puede configurar cada HiveAP usando un interfaz de línea de comandos robusto, se recomienda utilizar el HiveManager. El HiveManager simplifica la gestión y monitorización de los HiveAPs usando una combinación de vistas de topologías y planos de planta, perfiles de configuración y políticas, grupos y plantillas, así como una sencilla configuración masiva de propiedades de los elementos.

El interfaz gráfico de gestión para el Hive Manager se ha diseñado para que miles de HiveAPs se puedan gestionar y monitorizar utilizando perfiles de configuración. Los perfiles de configuración en el HiveManager se utilizan para categorizar opciones de configuración como Hives, SSIDs, RADIUS, radios, clasificación y marcado QoS, servicios de gestión, y perfiles de usuario. Una vez los perfiles de configuración están definidos, se asignan a uno o más perfiles de HiveAP para atarlos todos juntos.

Los perfiles de HiveAP son un mecanismo muy potente utilizado para organizar y aplicar una configuración a un gran número de HiveAPs. Basado en la ubicación o en un tipo de despliegue lógico, los perfiles de HiveAP asignan perfiles de

configuración y definen asociaciones desde SSIDs a perfiles de usuario e identificadores de VLAN.

Asociando SSIDs, perfiles de usuario e identificadores de VLAN dentro de un perfil de HiveAP, la configuración de la red se abstrae de la política de usuario de QoS y firewall, permitiendo utilizar los mismos perfiles de usuario a lo largo de toda la organización, a pesar de las diferencias en la topología de la red o la configuración del interfaz (por ejemplo Mallada vs. Acceso). Además, si se requieren diferentes políticas de firewall o QoS en ubicaciones diferentes, pueden crearse nuevos perfiles HiveAP que asignen los SSIDs a un nuevo conjunto de perfiles de usuario y VLANs en estas ubicaciones.

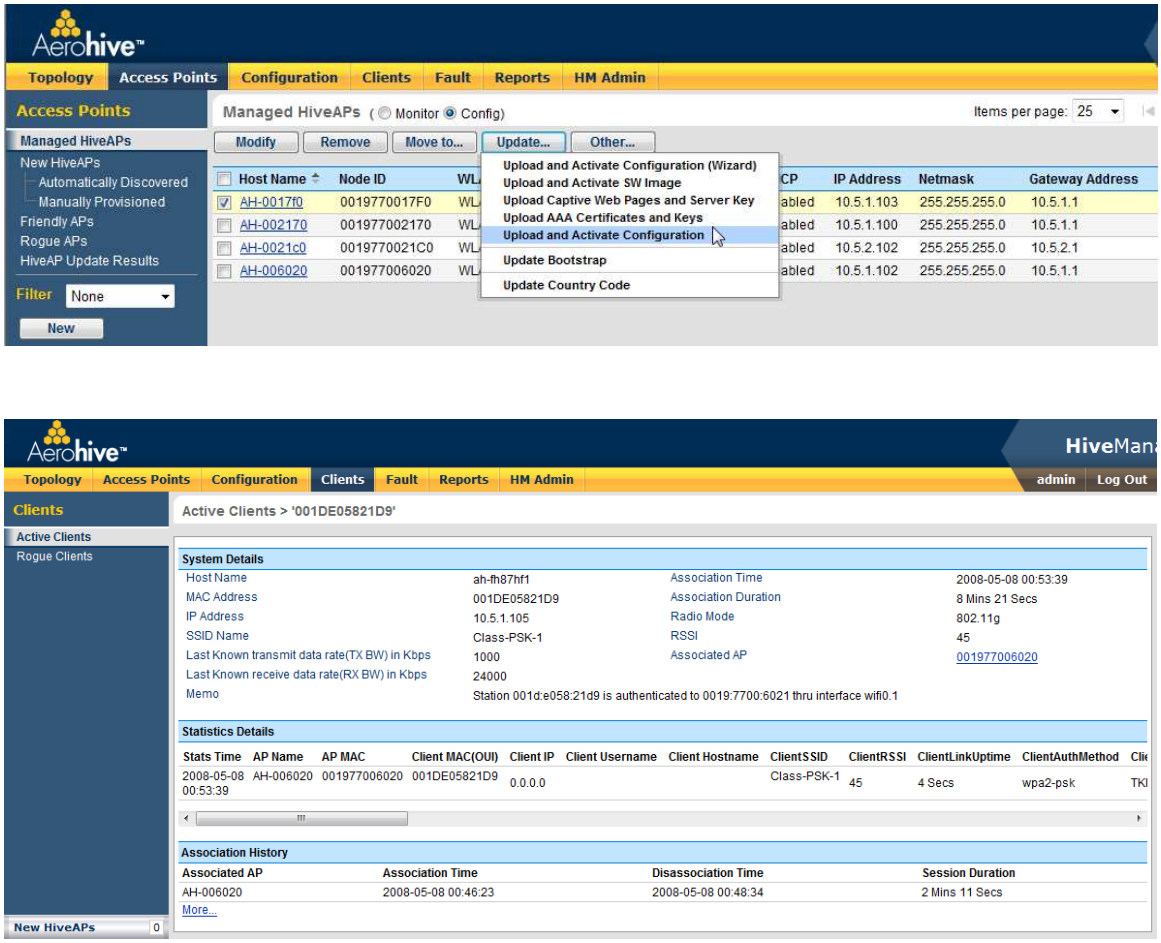


Figura 108- Gestión de un AP utilizando HiveManager

Los perfiles de usuario en diferentes grupos de dispositivos pueden contener diferentes políticas de firewall y QoS, pero pueden definirse con el mismo conjunto de identificadores de grupos de perfiles de usuario como definidos en otros grupos de dispositivo. De esta forma, según un usuario cambia a una nueva ubicación, su identificador de grupo de perfil de usuario los asocia al perfil de usuario correspondiente en cada ubicación. Esto permite una configuración de usuario de firewall, QoS y VLAN que puede cambiarse dinámicamente y seguir a los usuarios donde quiera que vayan en la WLAN.

Monitorización, Informes y Resolución de problemas

Junto con una configuración y gestión de sistema operativo simplificada, el HiveManager hace sencillo monitorizar y resolver problemas de los HiveAPs en una infraestructura de red inalámbrica. Utilizando vistas de mapas jerárquicos, un completo conjunto de mapas desde una vista del mundo, hasta niveles de planta, se pueden importar para organizar los HiveAPs basados en su ubicación física. Pueden añadirse iconos para representar ubicaciones, edificios, plantas y HiveAPs, y el color de los iconos cambia según la propagación de las alarmas de los HiveAPs.

Desde cualquier mapa de topología o desde una lista filtrable y ordenable de HiveAPs gestionados, los administradores pueden, haciendo clic con el botón derecho en la entrada del HiveAP, ver información en tiempo real como un listado de clientes inalámbricos asociados, logs, información de roaming, configuraciones y estadísticas.

Desde el HiveManager, los administradores pueden también utilizar herramientas como ping o traceroute, o pulsar un botón para lanzar una conexión SSH directamente contra los HiveAPs para tareas más avanzadas de resolución de problemas. El HiveManager también permite ver todos los clientes activos en la WLAN, mostrando su dirección IP, dirección MAC, hostname, nombre de usuario (si utiliza 802.1X), SSIDs, tiempos de inicio de sesión, valores de fuerza de la señal, y los HiveAPs a los que están conectados los clientes. Esta información se almacena en el HiveManager y puede exportarse en un archivo CSV para análisis forense de la red o una resolución avanzada de problemas.

Otra información que se puede exportar para realizar informes incluye un informe de inventario de todos los HiveAPs y los principales ajustes de configuración, informe de HiveAP contiguo e información de AP/cliente no autorizado. Para ser más proactivo, los administradores pueden también configurar notificaciones por correo electrónico de forma que pueden informarse inmediatamente de alarmas en la WLAN.

1.4. *Infraestructura Capa Red*

1.4.1. Acercamiento teórico diseño capa 3

El primer gran concepto que nos aparece a la hora de definir la infraestructura de capa de red es el tipo de conmutación que se va a realizar, es decir, la tecnología que se va a utilizar para el transporte de la información desde nuestra sede al resto de las sedes de nuestra compañía. Por tanto en función que exista un camino dedicado o no para nuestras conexiones, tendremos:

- Conmutación de circuitos:
  - Camino físico dedicado durante la llamada
  - Ejemplos: RTB, RDSI

- Conmutación de paquetes:
  - No hay un Camino físico dedicado durante la llamada Concepto
  - Ejemplos: FR, ATM, IP, MPLS (VPLS)

Cuando se definen la arquitectura de capa de red, es necesario tener en cuenta el nivel en la torre OSI o TCP que ocupa esta tecnología. En concreto nos estamos refiriendo al nivel de Red (Osi) o capa de Internet (IP) en el modelo TCP.

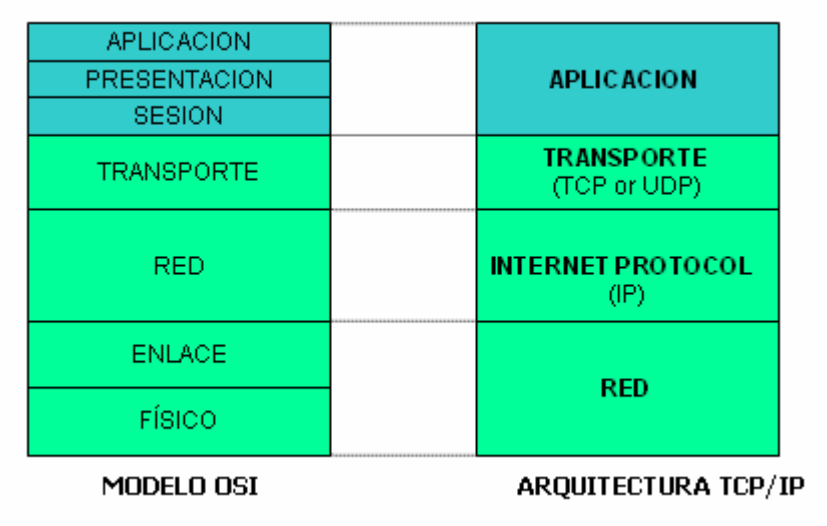


Figura 109- Nivel 3 TCP/IP

El modelo es el siguiente:

- Una trama Ethernet que ha sido conducida por los switches a través de la red LAN llega al dispositivo de nivel de red (router), que básicamente lo que hace es validar la cabecera IP, y verificar si hacer acceder a la IP destino es necesario realizar un proceso de enrutado

Protocolos Encaminamiento

Una de las decisiones importantes a la hora de preparar la infraestructura de la capa de red es la de decidir el protocolo de routing que se va a implementar en los routers. Básicamente será necesario decidir sobre la conveniencia de implementar un protocolo de encaminamiento dinámico o estático. Vemos las diferencias.

Un protocolo de enrutamiento es un software complejo que se ejecuta de manera simultánea en un conjunto de routers, con el objetivo de completar y actualizar su tabla de enrutamiento con los mejores caminos para intercambiar información con otras redes. Así, podríamos resumir que un protocolo de enrutamiento tiene como objetivos los siguientes:

- Descubrir redes lejanas con las que intercambiar información
- Mantener la información de enrutamiento actualizada de manera fiable
- Elegir el mejor camino posible en cada momento hacia las redes de destino
- Encontrar un nuevas rutas para sustituir a aquellas que dejen de estar disponibles en los términos necesarios.

Frente al enrutamiento estático, el enrutamiento dinámico ofrece nuevas posibilidades, se adapta mejor a nuevas circunstancias pero requiere una mayor complejidad en los sistemas y en la gestión de estos.

La siguiente figura intenta resumir las características de ambos:

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Por lo general es independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos del administrador	Se requiere de un conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere la intervención del administrador
Escalamiento	Adecuado para las topologías simples y complejas	Adecuada para topologías simples
Seguridad	Es menos seguro	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma

Figura 110 -*Enrutamiento estático vs enrutamiento dinámico (Fuente: Cisco System, Inc.)*

Los protocolos de enrutamiento dinámico se clasifican (en una primera instancia) según sean de aplicación a sistemas de Gateway interior o exterior, y los primeros se agrupan según consideren como variable el vector distancia o el estado del enlace.

A continuación se muestra un esquema de clasificación.

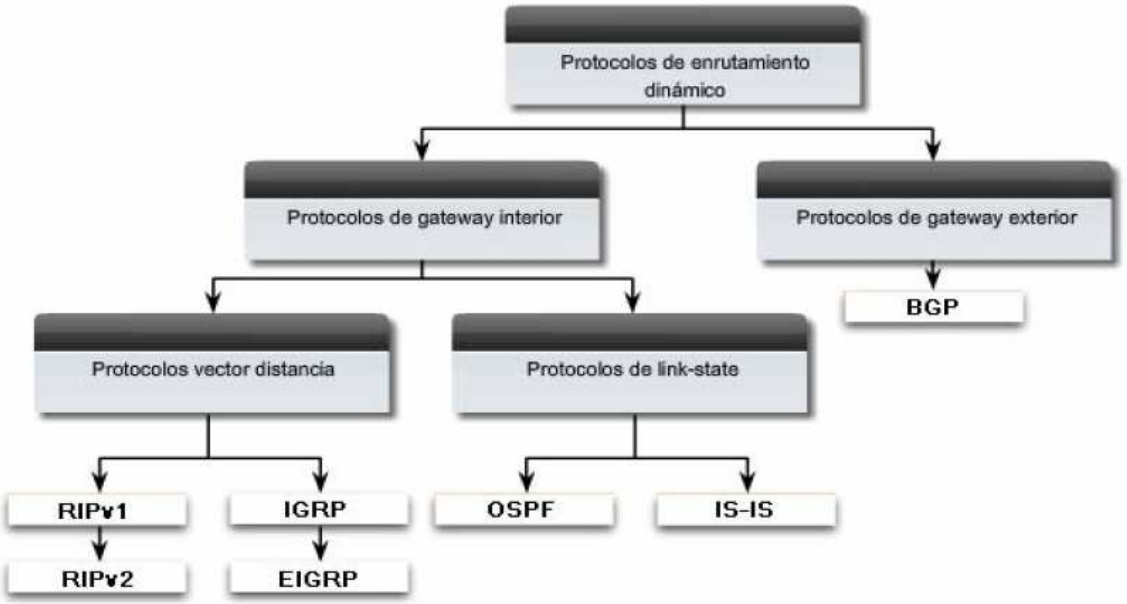


Figura 111 -*Clasificación de los protocolos de enrutamiento dinámico (Fuente Cisco System, Inc)*

Los protocolos de Gateway interior se utilizan para tareas de enrutamiento en los

llamados sistemas autónomos, que son aquellos en gestionados por un solo administrador. El protocolo BGP (*Border Gateway Protocol*) de Gateway exterior se utiliza para interconectar los sistemas autónomos.

Los protocolos que consideran el estado y capacidad del enlace hasta la red de destino son IS-IS (*Intermediate System To Intermediate System*) y OSPF (*Open Shortest Path First*).

Nuestro estudio se centrará en los dos protocolos que actualmente se implementan en las instalaciones de red WAN, y que serán los que implementemos en los routers de nuestro subsistema de nivel de red. Son los protocolos OSPF y BGP

Consideraciones sobre OSPF

OSPF es un protocolo de enrutamiento sin clase y de estado del enlace, cuya versión actual para IPv4 es la OSPFv2 descrita en la RFC 2328. Entre sus características básicas habría que destacar las siguientes:

• Sus mensajes se encapsulan en un paquete IP con indicador de protocolo 89.
• La dirección de destino se establece para una de dos direcciones multicast: 224.0.0.5 ó 224.0.0.6. Si el paquete OSPF se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-05 o 01-00-5E-00-00-06.
Tiene asignada una distancia administrativa de 110

OSPF es un protocolo de routing dinámico de link state (modificaciones de estado) que detecta y aprende las mejores rutas a destinos (accesibles). OSPF puede percibir rápidamente cambios en la topología de un Sistema Autónomo (SA), y después de un pequeño periodo de convergencia, calcular nuevas rutas. OSPF no encapsula los paquetes IP, sino que los hace progresar basándose solamente en la dirección de destino.

OSPF está diseñado para proporcionar servicios no disponibles con el protocolo RIP. Sus características avanzadas incluyen:

· *Routing menos costoso*. Permite configurar los costes de camino (path) basándose en cualquier combinación de parámetros de la red. Por ejemplo ancho de banda, retraso, y coste.
· *Sin limitaciones en la métrica de routing*. Mientras que RIP restringía la métrica de routing a 16 saltos, OSPF no tiene restricción alguna a este respecto.
· *Routing multicamino*. Permite la utilización de múltiples caminos de igual coste que conectan a los mismos puntos. Se pueden utilizar estos caminos para conseguir un equilibrio (balancear la carga) lo que resulta en un uso más eficiente del ancho de banda de la red.

· *Routing de área*. Disminuye los recursos (memoria y ancho de banda de la red) consumidos por el protocolo y proporciona un nivel adicional de protección al routing.

· *Máscaras de subred de longitud variable*. Permiten fraccionar una dirección IP en subredes de tamaño variable, conservando el espacio de dirección IP.

· *Autenticación de routing*. Proporciona seguridad adicional al routing.

Existen cinco tipos de paquetes OSPF:

- **Paquete Hello**. Se utiliza para mantener activa la conexión OSPF con otros routers adyacentes
- **Paquete DBD (*DataBase Description*)**. Contiene información de la base de datos del router que lo emite acerca del estado de los enlaces locales a este.
- **Paquete LSR (*Link-State Request*)**. Es una solicitud de información sobre cualquier entrada de la base de datos de estado del enlace.
- **Paquete LSU (*Link-State Update*)**. Es una respuesta a las peticiones LSR y contiene diferentes tipos de notificaciones sobre el estado del enlace, LSA (*Link-State Advertisement*).
- **Paquete LSAck (*Link-State acknowledgment*)**. Es un acuse de recibo de un paquete LSU.

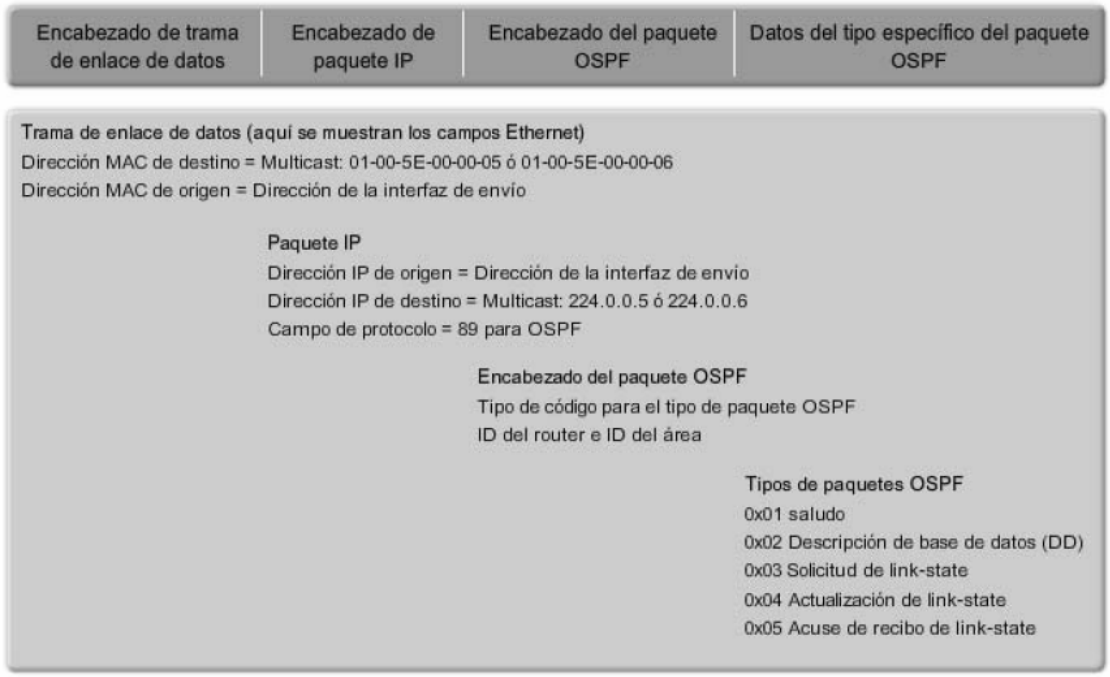


Figura 112 -*Formato del mensaje OSPF*

Cada router OSPF mantiene una base de datos de link-state que contiene las LSA recibidas por parte de todos los demás routers. Una vez que un router recibió todas las LSA y creó su base de datos de link-state local, OSPF utiliza el algoritmo SPF (primero el camino más corto, *Shortest Path First*) de Dijkstra para crear un árbol SPF.

El árbol SPF luego se utiliza para completar la tabla de enrutamiento IP con las mejores rutas para cada red. Esto implica que cada router mantiene un árbol propio y que no tiene porqué ser similar al de los routers del mismo dominio de enrutamiento.

El proceso de activación y configuración de OSPF requiere los siguientes pasos en cada router:

1. Activación del proceso asignándole un identificador propio que sólo tiene significado local al router
2. Enumeración de las redes conectadas que formarán parte en el proceso de enrutamiento, indicando para cada una de ellas.

    a. La dirección de red
    b. La máscara, en formato complementado a las máscaras de subred
    c. Un identificador de área OSPD. Número entero que coincidirá en todos los routers del área de enrutamiento que compartan información sobre el estado de los enlaces.

En OSPF cada router tiene que tener una identificación propia e inequívoca que coincide, en el caso de los routers de Cisco, con el siguiente orden de precedencia:

1. La dirección IP configurada expresamente con tal fin (comando `routerid`).
2. Si no se configura expresamente, la dirección IP más alta de cualquier de sus *interfaces de loopbak* (son interfaces software activadas en cada router con el propósito de simular otras redes no existentes físicamente).
3. Si no se ha configurado ninguna interfaz de loopbak, la dirección IP más alta de cualquiera de sus interfaces físicas activas.

El coste OSPF de una ruta es un valor entero que se obtiene sumando los costes individuales de cada uno de los enlaces que forman parte de la ruta. El coste individual de un enlace en los routers de Cisco tiene un valor de referencia de 10^8 por defecto

Tipo de interfaz	10^8/bps = Costo
Fast Ethernet y más rápida	10^8/100 000 000 bps = 1
Ethernet	10^8/10 000 000 bps = 10
E1	10^8/2 048 000 bps = 48
T1	10^8/1 544 000 bps = 64
128 kbps	10^8/128 000 bps = 781
64 kbps	10^8/64 000 bps = 1562
56 kbps	10^8/56 000 bps = 1785

Figura 113 -*Valores del costo de los distintos tipos de enlace en los routers Cisco*

El protocolo OSPF soporta los siguientes tipos de redes físicas:

- *Punto a Punto*. Son las redes que usan una línea de comunicación para unir un único par de routers. Un ejemplo de red punto a punto puede ser una línea serie a 56 Kbps que conecte dos routers.
- *Broadcast*. Son redes que soportan más de dos routers conectados y que son capaces de direccionar un único mensaje físico a todos los routers conectados. Un ejemplo de red broadcast puede ser una red Token Ring.
- *No Broadcast*. Son redes que soportan más de dos routers conectados pero no tienen capacidad de broadcast. Una red de datos pública X.25 es un ejemplo de red no broadcast. Para que OSPF funcione correctamente esta red necesita información de configuración adicional sobre otros routers OSPF conectados a la red no broadcast.

Consideraciones BGP

El protocolo BGP (Border Gateway Protocol) se estableció como un estándar de Internet en 1989 y fue definido originalmente en la RFC 1105, adoptándose como un protocolo para la comunicación entre dominios dentro de la comunicación EGP. La versión actual es la BGP-4, que se adoptó en 1995 y ha sido definida en la RFC 1771. BGP-4 soporta CIDR (Classles Inter Domain Routing) y es el protocolo de enrutamiento que actualmente se usa de forma mayoritaria para encaminar las información entre sistemas autónomos, ya que ha demostrado ser fácilmente escalable, estable y dotado de los mecanismos necesarios para soportar políticas de encaminamiento complicadas. A partir de ahora cuando se nombre al protocolo BGP, se está haciendo mención de la versión BGP-4.

BGP continúa desarrollándose a través del trabajo del proceso de los estándares de Internet en el IETF.

Como los requisitos del encaminamiento de Internet cambian, el protocolo BGP se extiende para continuar proporcionando mecanismos que controlen la información de encaminamiento y soporten los nuevos requisitos. Por eso, la RFC básica ha sido extendida por varias RFCs posteriores.

El protocolo BGP utiliza el protocolo TCP para establecer una conexión segura entre dos extremos BGP en el puerto 179. Una sesión TCP se establece exactamente entre cada par para cada sesión del BGP. Ninguna información de encaminamiento puede ser intercambiada hasta que se ha establecido la sesión TCP. Esto implica la existencia previa de conectividad IP para cada par de extremos BGP. Para dotarlo de mayor seguridad, se pueden usar firmas MD5 para verificar cada segmento TCP.

Se dice que BGP es un protocolo de encaminamiento vectorial, porque almacena la información de encaminamiento como combinación entre el destino y las características de la ruta para alcanzar ese destino. El protocolo utiliza un proceso de selección determinista de la ruta para seleccionar la mejor dentro de las rutas factibles múltiples, usando las cualidades de la ruta como criterios. Las características como por ejemplo el retardo, la utilización del enlace o el número de saltos no se consideran dentro de este proceso. El proceso de selección de la ruta es la clave para comprender y establecer las políticas del protocolo BGP y se analizarán más adelante.

Al igual que la mayoría de los protocolos del tipo IGP, BGP envía solamente una actualización completa del encaminamiento una vez que se establece una sesión BGP, enviando posteriormente sólo cambios incrementales. BGP únicamente recalcula la información de encaminamiento concerniente a estas actualizaciones, no existiendo proceso que actualice toda su información de encaminamiento como los cálculos del SPF en el OSPF o el IS-IS. Aunque la convergencia IGP puede ser más rápida, un IGP no está preparado para soportar el número de las rutas empleadas en el encaminamiento inter - dominio. Un IGP también carece de las cualidades de ruta que el BGP lleva, y que son esenciales para seleccionar la mejor ruta y construir políticas de encaminamiento. BGP es el único protocolo adecuado para el uso entre sistemas autónomos, debido a la ayuda inherente que las políticas sobre rutas proporcionan para el encaminamiento. Estas políticas permiten que se acepte o rechace la información de cambio de encaminamiento antes de que se utilice para tomar decisiones de envío. Esta capacidad da a los operadores de red un alto grado de protección contra información de encaminamiento que puede ser no deseada, y así controlar la información de encaminamiento según sus necesidades particulares.

BGP opera en dos modos: EBGP e IBGP. EBGP (BGP exterior) se utiliza entre distintos sistemas autónomos, e IBGP (BGP interior) se utiliza entre routers BGP dentro del mismo sistema autónomo.

Criterios de selección de rutas

El protocolo BGP trabaja con una tabla privada de rutas que incluye tanto las rutas de la tabla de rutas activas del equipo, como las rutas aprendidas por BGP de todos los vecinos.

En la tabla de rutas de BGP puede haber varias rutas para ir al mismo destino, de las que se seleccionan sólo las más prioritarias para instalarlas en la tabla de rutas activas del equipo. Para ello el protocolo BGP maneja diversos parámetros que determinan la prioridad de cada ruta.

Existen distintas formas de selección de rutas:

- Preferencia (distancia Administrativa)
- Preferencia2 (tie-breaker)
- Metrica (Multi_exit_disc)
- Metrica2 (Local_Pref)
- As-path

¿Cómo realiza el router la elección de ruta?

El protocolo BGP utiliza las siguientes reglas para elegir la mejor ruta o salto a un determinado destino:

· La ruta con la menor Preferencia (Distancia Administrativa) es la elegida.

· Si dos rutas tienen la misma Preferencia, se elige la ruta con la menor Preferencia2 (tie -breaker).

· Si las dos rutas se han aprendido por BGP se aplican los siguientes criterios:

  o Se prefiere la ruta con mayor Métrica2 (LOCAL_PREF). Si no se ha asignado valor de Métrica2 (aparece –1) se considera el valor máximo.

  o Una ruta con información de AS-path es preferida frente a otra sin AS-path.

  o Entre dos rutas con AS-path, provenientes del mismo AS, y con información de Métrica, se prefiere aquella que tiene menor valor de Métrica (MULTI_EXIT_DISC).

  o Entre dos rutas con AS-path distintos, se prefiere la de origen IGP, y si no la de origen EGP.

  o Entre dos rutas con AS-path distintos y con mismo origen, se prefiere la de AS-path de menor longitud.

· Una ruta aprendida desde IGP es preferida a una aprendida desde EGP. La ruta menos preferida es la que se obtiene indirectamente de un IGP que la ha obtenido de un EGP.

· Si ambas rutas se aprendieron del mismo protocolo y el mismo AS, se usa la que tenga la menor Métrica.

· Se prefieren las rutas instalables en la tabla de rutas activas del equipo frente a las rutas no instalables.

· Se prefiere la ruta que tenga siguiente salto con el valor de dirección IP más bajo.

Para la elección del protocolo de routing también es importante tener claro de que tipo de conexión WAN se dispondrá en la sede [RDSI, Frame Relay, ATM, MPLS].

En el entorno actual de las comunicaciones de datos, hablar de conexiones RDSI y Frame Relay deja de tener sentido, son redes antiguas, con anchos de banda muy limitados, y sobre todo muy limitadas para el transporte de los distintos servicios que actualmente son demandados para el transporte por las redes de datos [datos, voz, videoconferencia, multimedia..]

Por tanto parece que tiene sentido pensar en dotar a cualquier sede remota de una conexión MPLS para su enlace principal de datos, y de una, al menos, una conexión ATM de menor capacidad, para su enlace de respaldo.

Veamos algunas consideraciones básicas de ambas tecnologías de infraestructura WAN, que nos permitirán entender mejor los parámetros de configuración en los routers.

Consideraciones ATM

La tecnología ATM empezó a desarrollarse en los primeros años de la década de los 80, y es alrededor de 1992 cuando comienza su despegue industrial. ATM ha sido una de las tecnologías predilectas por los visionarios de turno, considerada como la única capaz de ofrecer un transporte multiservicio integrando las redes corporativas con las de los operadores y proveedores de servicio. Las redes de acceso fijo a Internet de banda ancha ADSL y las redes de telefonía móvil UMTS de tercera generación favorecieron su despliegue en el entorno WAN de las redes de operadores, debido a la inmadurez de Ethernet/IP para proporcionar una red convergente.

ATM nunca llegó a cuajar en el entorno LAN (ATM LANE), debido a su complejidad, coste y rendimiento. La madurez y economías de escala de Ethernet, junto a flexibilidad y adaptabilidad, ha permitido desde hace años entrar en el mercado WAN, retirando definitivamente a ATM de la guerra por la convergencia. Sin embargo, ATM sigue instalado en las redes de muchos operadores conviviendo con Ethernet/IP.

El modo de transferencia asíncrono o ATM (Asyncronous Transfer Mode) es un estándar adoptado por la ITU-T (International Telecommunication Union-Telecommunication Standardization Sector) en 1985 para soportar la red digital de servicios integrados de banda ancha o B-ISDN (Broadband Integrated Services Digital Network). La tecnología ATM permite la integración de los servicios orientados y no orientados a conexión. La integración de estos servicios en una única red, reduce enormemente los costes en infraestructura y en personal de operación y mantenimiento en las operadoras de telecomunicaciones.

La tecnología ATM se basa en la multiplexación y conmutación de celdas o pequeños paquetes de longitud fija, combinando los beneficios de la conmutación de circuitos (capacidad garantizada y retardo de transmisión constante), con los de la conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente).

Proporciona ancho de banda escalable, que va desde los 2 Mbps a los 10 Gbps; velocidades muy superiores a los 64 Kbps como máximo que ofrece X.25 o a los 2

Mbps de Frame Relay. Además, ATM es más eficiente que las tecnologías síncronas, tales como la multiplexación por división en el tiempo o TDM (Time Division Multiplexing) en la que se basan PDH y SDH. Puesto que ATM es asíncrono, las ranuras temporales están disponibles bajo demanda con información identificando la fuente de la transmisión contenida en la cabecera de cada celda ATM.

Las principales características de ATM son: no hay control de flujo ni recuperación de errores extremo, opera en modo orientado a conexión, tiene una baja sobrecarga de información en la cabecera -que permite altas velocidades de conmutación-, tiene un campo de información relativamente pequeño –que reduce el tamaño de las colas y el retardo en las mismas- y utiliza paquetes de longitud fija –que simplifica la conmutación de datos a alta velocidad-.

Una red ATM está formada por conmutadores ATM y puntos finales ATM. El conmutador ATM es responsable del tránsito de celdas a través de la red ATM: acepta las celdas que le llegan de un punto final ATM o un conmutador ATM, lee y actualiza la información en la cabecera de la celda, y rápidamente conmuta la celda a una interfaz de salida hacia su destino. Un punto final ATM o sistema final, contiene un adaptador de interfaz a la red ATM, el cual sí lee los bytes de datos de la celda. Ejemplos de puntos finales son: las estaciones de trabajo, routers, unidades de servicio digitales, conmutadores LAN, y codificadores y decodificadores de vídeo.

Los conmutadores ATM soportan dos tipos primarios de interfaces:

- UNI (User to Network Interface). La interfaz UNI conecta sistemas finales ATM (tales como servidores y routers) a un conmutador ATM.
- NNI (Network to Network Interface). Conecta dos conmutadores ATM.
-

Los dispositivos ATM utilizan un formato de direcciones NSAP (Network Service Access Point) del modelo OSI de 20 bytes, en el caso de redes ATM privadas; y un formato de direcciones E.164 del ITU-T, semejante a números telefónicos, para las redes públicas B-ISDN. Cada sistema ATM necesita de una dirección ATM, independiente de los protocolos de nivel superior como IP o IPX.

La funcionalidad de ATM se corresponde con la capa física y parte de la capa de enlace del modelo de referencia OSI (Open Systems Interconnection) de la ISO (International Organization for Standardization). En la Figura 97 se ilustra el modelo de referencia ATM.

El **modelo de referencia ATM** está compuesto por los siguientes **planos**:

- **Control**. Este plano es responsable de generar y de manejar las peticiones de señalización.
- **Usuario**. Este plano es responsable de manejar la transferencia de datos.
- **Gestión**. Este plano contiene una componente denominada gestión de la capa que maneja funciones específicas del nivel ATM, tales como la detección de fallos y los problemas de protocolo, y otra capa denotada gestión de plano que maneja y coordina funciones relacionadas con el sistema completo.

El **modelo de referencia ATM** se compone de los siguientes **niveles**:

- **Nivel físico**. Semejante al nivel físico del modelo de referencia OSI, el nivel físico ATM maneja la transmisión dependiente del medio físico. Define las características eléctricas y las interfaces de red.
- **Nivel ATM**. El nivel ATM, en combinación con el nivel de adaptación ATM, es análogo al nivel de enlace de datos del modelo de referencia OSI. El nivel ATM es responsable del establecimiento de conexiones y del paso de celdas a través de la red ATM. Para ello toma los datos que van a ser enviados y añade la información de la cabecera de 5 bytes que asegura que la celda es enviada por la conexión correcta.
- **Nivel de adaptación ATM**. La AAL (*ATM Adaptation Layer*), combinada con el nivel ATM, es semejante al nivel de enlace de datos del modelo de referencia OSI. La AAL es responsable de aislar los detalles de los procesos ATM a los protocolos de niveles superior. Se encarga de asegurar las características de servicio apropiadas y de segmentar cualquier tipo de tráfico en una carga de 48 bytes que será transmitida en las celdas ATM. Para implementar los distintos tipos de servicio ATM se han especificado varias capas AAL que adapten el flujo de celdas ATM a un flujo con las características requeridas por cada uno de ellos.
- **Niveles superiores**. Son los niveles que residen sobre la AAL, los cuales aceptan los datos de usuario, los clasifican en paquetes, y los pasan a la AAL.

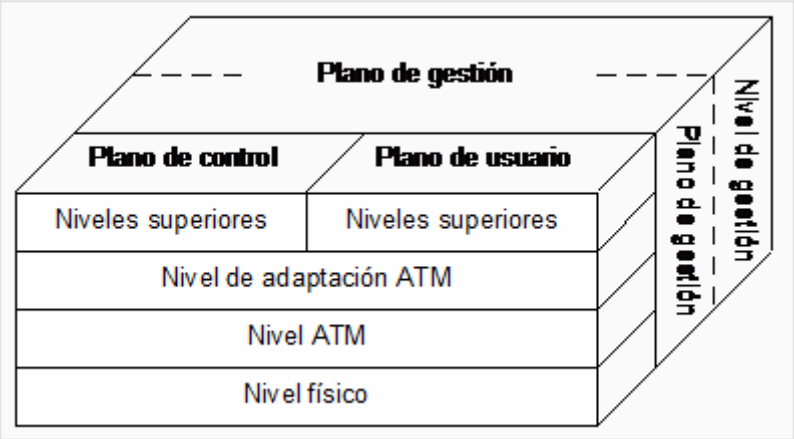


Figura 114-Modelo de referencia ATM.

Las redes ATM están fundamentalmente orientadas a conexión (funcionamiento similar al sistema de conmutación telefónico estándar), donde las llamadas son establecidas basándose en los extremos finales antes de que se produzca el intercambio de información.

Cuando se establece un circuito a través de un sistema ATM, todas las celdas relacionadas con ese flujo de datos, viajan por la misma ruta durante toda la sesión. Por lo tanto, las celdas llegan en orden, simplificando su procesamiento. En cambio, en la conmutación de paquetes, los paquetes se encaminan dinámicamente en cada nodo.

Los sistemas de señalización y de gestión reservan un canal virtual consistente en una cantidad apropiada de ancho de banda dentro de un camino con un mayor ancho de banda. En una **conexión permanente o PVC (*Permanent Virtual Connection*)**, el ancho de banda se establece de forma permanente –similar a una línea alquilada-, mientras que en una **conexión conmutada o SVC (*Switched Virtual Connection*)**, el ancho de banda se reserva al iniciar la sesión mediante el sistema de señalización y dicha reserva es liberada por el sistema de señalización cuando se finaliza la llamada –similar a una llamada telefónica por la red telefónica básica-.

Las conexiones en ATM pueden ser punto a punto o bien punto a multipunto. Las conexiones punto a punto conectan dos sistemas finales ATM y pueden ser unidireccionales o bidireccionales. Las conexiones punto a multipunto conectan un único sistema final origen con múltiples sistemas finales destino y sólo pueden ser unidireccionales.

Una PVC garantiza la disponibilidad de la conexión y no requiere de establecimientos de llamada entre los conmutadores. Entre sus desventajas, están el carácter estático de la conexión y la necesidad de un establecimiento manual. Entre las ventajas del SVC, están la flexibilidad de la conexión y que el establecimiento de la llamada puede ser manejado automáticamente por el dispositivo de red. Entre sus desventajas, están el tiempo extra y la sobrecarga requerida para establecer la conexión.

En cada conmutador ATM, para cada una de sus interfaces, se tiene una tabla de conmutación introducida manualmente mediante los procesos de gestión (en PVCs) o creada dinámicamente por los mecanismos de señalización (en SVCs). La tabla hace una correspondencia entre los valores VPI/VCI de la celda entrante y los nuevos valores para el trayecto siguiente de la celda, además de indicarse la interfaz de salida del conmutador.

Consideraciones MPLS

El enorme crecimiento de la red Internet ha convertido al protocolo IP (*Internet Protocol*) en la base de las actuales redes de telecomunicaciones, contando con más del 80% del tráfico cursado. La versión actual de IP, conocida por IPv4 y recogida en la RFC 791, lleva operativa desde 1980. Este protocolo de capa de red (Nivel 3 OSI), define los mecanismos de la distribución o encaminamiento de paquetes, de una manera no fiable y sin conexión, en redes heterogéneas; es decir, únicamente está orientado a servicios no orientados a conexión y a la transferencia de datos, por lo que se suele utilizar junto con TCP (*Transmission Control Protocol*) (Nivel 4 de OSI) para garantizar la entrega de los paquetes.

A mediados de la década de los 90, la demanda por parte de los clientes de los ISP (*Internet Service Providers*) de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS (*Quality of Service*) garantizada, propiciaron la introducción de ATM (*Asyncronous Transfer Mode*) en la capa de enlace (Nivel 2 de OSI) de sus redes. En esos momentos, el modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, utilizando el encaminamiento inteligente de nivel 3 de los routers IP en la red de acceso, e incrementando el ancho de banda y rendimiento basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los switches ATM en la red troncal. Esta arquitectura,

no obstante, presenta ciertas limitaciones, debido a: la dificultad de operar e integrar una red basándose en dos tecnologías muy distintas, la aparición de switches ATM e IP de alto rendimiento en las redes troncales, y la mayor capacidad de transmisión ofrecida por SDH/SONET (*Synchronous Digital Hierarchy / Syncronous Optical NETwork*) y DWDM (*Dense Wavelength Division Multiplexing*) respecto a ATM.

Durante 1996, empezaron a aparecer soluciones de conmutación de nivel 2 propietarias diseñadas para el núcleo de Internet que integraban la conmutación ATM con el encaminamiento IP; como por ejemplo, Tag Switching de Cisco o Aggregate Route-Based IP Switching de IBM. La base común de todas estas tecnologías, era tomar el software de control de un router IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un switch ATM y crear un router extremadamente rápido y eficiente en cuanto a coste. La integración en esta arquitectura era mayor, porque se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; pero los protocolos no eran compatibles entre sí y requerían aún de infraestructura ATM.

Finalmente en 1997, el IETF (*Internet Engineering Task Force*) establece el grupo de trabajo **MPLS (*MultiProtocol Label Switching*)** para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. El resultado fue la definición en 1998 del estándar conocido por MPLS, recogido en la RFC 3031. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad. Por otro lado, a diferencia de las soluciones de conmutación de nivel 2 propietarias, está diseñado para operar sobre cualquier tecnología en el nivel de enlace, no únicamente ATM, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM.

Concepto de MPLS

MPLS es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un router. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un router, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (*Forward Equivalence Class*), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes. La etiqueta es un identificador de conexión que sólo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio. Cuando MPLS está implementado como una solución IP pura o de nivel 3, que es la

más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete. Los campos de la cabecera MPLS de 4 bytes, son los siguientes:

Label (20 bits). Es el valor actual, con sentido únicamente local, de la etiqueta MPLS. Esta etiqueta es la que determinará el próximo salto del paquete.

CoS (3 bits). Este campo afecta a los algoritmos de descarte de paquetes y de mantenimiento de colas en los nodos intermedios, es decir, indica la QoS del paquete. Mediante este campo es posible diferenciar distintos tipos de tráficos y mejorar el rendimiento de un tipo de tráfico respecto a otros.

Stack (1 bit). Mediante este bit se soporta una pila de etiquetas jerárquicas, es decir, indica si existen más etiquetas MPLS. Las cabeceras MPLS se comportan como si estuvieran apiladas una sobre otra, de modo que el nodo MPLS tratará siempre la que esté más alto en la pila. La posibilidad de encapsular una cabecera MPLS en otras, tiene sentido, por ejemplo, cuando se tiene una red MPLS que tiene que atravesar otra red MPLS perteneciente a un ISP u organismo administrativo externo distinto; de modo que al terminar de atravesar esa red, se continúe trabajando con MPLS como si no existiera dicha red externa.

Elementos de una red MPLS

En MPLS un concepto muy importante es el de LSP (*Label Switch Path*), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (*Label Distribution Protocols*), tales como RSVP-TE (*ReSerVation Protocol – Traffic Engineering*) o CR-LDP (*Constraint-based Routing – Label Distribution Protocol*); siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos.

Una red MPLS está compuesta por dos tipos principales de nodos, los **LER (*Label Edge Routers*)** y los **LSR (*Label Switching Routers*)**, tal y como se muestra en el ejemplo de la Figura 1. Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los routers IP normales, intercambian información sobre la topología de la red mediante los protocolos de encaminamiento estándar, tales como OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*) y BGP (*Border Gateway Protocol*), a partir de los cuales construyen tablas de encaminamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. Teniendo en cuenta dichas tablas de encaminamiento, que indican la dirección IP del siguiente nodo al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS y, por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de encaminamiento.

Los LERs están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino

y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un router IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar encaminamiento de alto rendimiento basado en la conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias.

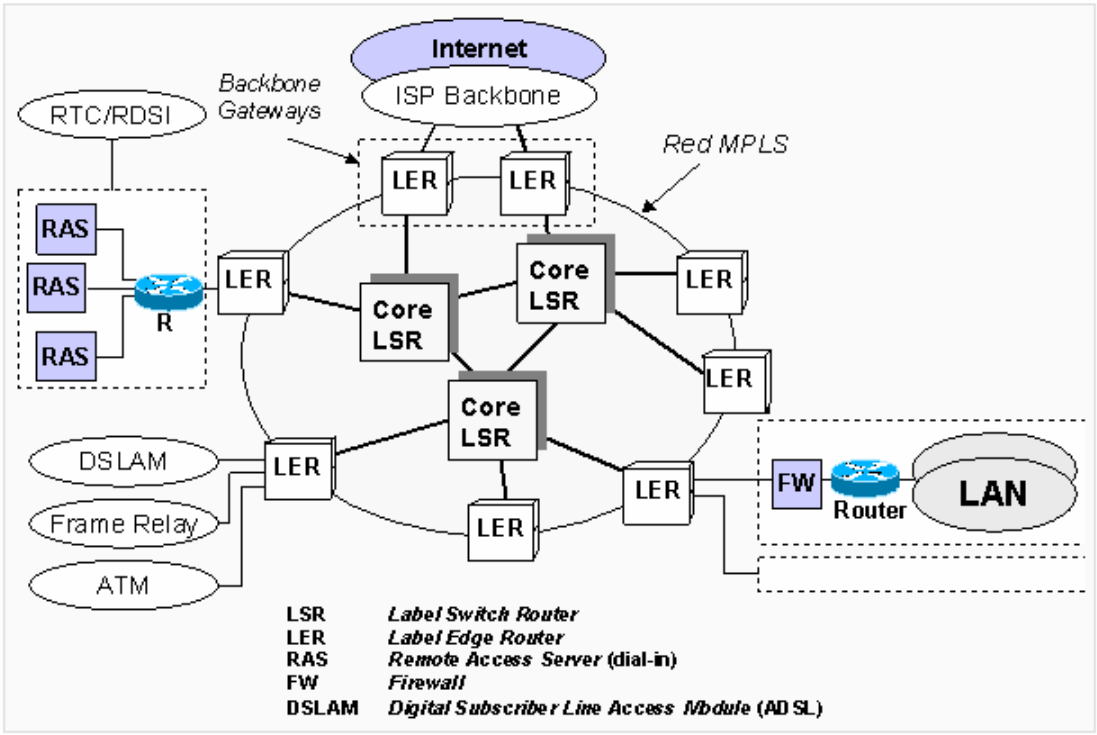


Figura 115 -Ejemplo de una red MPLS.

Una vez visto el concepto de MPLS, veamos los distintos tipos de implementaciones actuales, en concreto: MPLS como una solución IP sobre Ethernet, IP sobre ATM, e IP sobre Frame Relay. No se contempla la aplicación de MPLS a las redes ópticas de próxima generación, conocida como GMPLS (*Generalized MPLS*), por encontrarse aún en proceso de estudio y estandarización por parte del IETF. GMPLS es una extensión natural de MPLS para ampliar el uso de MPLS como un mecanismo de control y provisión, no únicamente de caminos en dispositivos basados en paquetes, sino también de caminos en dispositivos no basados en paquetes; como los conmutadores ópticos de señales multiplexadas por división en longitud de onda, los conmutadores de fibras ópticas, y los conmutadores de señales digitales multiplexadas por división en el tiempo. Es decir, GMPLS busca una integración total en la parte de control de las redes de conmutación de paquetes IP y las redes ópticas SONET/SDH y DWDM; dando lugar a las redes ópticas inteligentes de próxima generación, cuya

evolución final será la integración de IP directamente sobre DWDM utilizando algún mecanismo de encapsulamiento como los "digital wrappers".

La implementación de MPLS como una solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, en este caso, la etiqueta MPLS está ubicada después de la cabecera de nivel 2 y antes de la cabecera IP. Los LSR saben como conmutar utilizando la etiqueta MPLS en vez de utilizar la cabecera IP. El funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad. Estas limitaciones propiciaron el desarrollo de la siguiente generación del protocolo Internet o IPv6, definido en la RFC 1883. La versión IPv6 puede ser instalada como una actualización del software en los dispositivos de red de Internet e interoperar con la versión actual IPv4, produciéndose esta migración progresivamente durante los próximos años. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6, estando su uso descrito en la RFC 1809.

La implementación de MPLS como una solución IP sobre ATM también está muy extendida. Primeramente indicar, que MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de switches ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (*Private Network to Network Interface*). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM, puesto que LDP entiende y utiliza direcciones IP y los protocolos de encaminamiento utilizados en las redes MPLS son los mismos que los utilizados en las redes IP. En este caso, descrito en la RFC 3035, la etiqueta es el valor del VPI/VCI (*Virtual Path Identifier/Virtual Channel Identifier*) de la cabecera de la celda ATM.

Finalmente, MPLS también se ha desarrollado como una solución IP sobre Frame Relay. En este caso, descrito en la RFC 3034, la etiqueta es el DLCI (*Data Link Control Identifier*) de la cabecera Frame Relay.

Beneficios de MPLS

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (*Traffic Engineering*),

cursar tráfico con diferentes calidades de clases de servicio o CoS (*Class of Service*) o grados de calidad de servicio o QoS (*Quality of Service*), y crear redes privadas virtuales o VPN (*Virtual Private Networks*) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, descrita en la RFC 2702, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red.

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (*Wide Area Network*) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPNs mediante MPLS, pero la mayoría se basan en la RFC 2547.

1.4.2. Configuración routers

Una vez definidos una serie de conceptos teóricos necesarios, pasamos a mostrar la solución final para el subsistema de nivel de red, que nos permitirá interconectar la sede objeto del trabajo con una red mallada multiservicio.

La solución final para este subsistema estará basado en el siguiente equipamiento:

- Router Principal Teldat Atlas 160
  - Tecnología: MPLS
  - Routing: BGP
  - Ancho de banda Contratado: 51 Mbps

Figura 116-Router Principal Teldat Atlas 160

- Características básicas equipamiento

	Atlas 60	Atlas 60A8	Atlas 60A16	Atlas 160	Atlas 260	Atlas 360
Ethernet WAN	2 x GE	2 x GE	2 x GE	2 x GE	2 x GE	2 x GE
Ethernet LAN (PoE opc.)	8 x FE	8 x FE	16 x FE	0	0	0
ADSL2+ en placa base	No	Si	Si	No	No	No
Slots PMC	0	0	0	2	3	4
Slot WiFi	Si	Si	Si	Si	Si	Si
Slot 3G	Si	Si	Si	No	No	No
Slot para Switch (PoE opc.)	No	No	No	No	No	16 x FE
USB 2.0	Si	Si	Si	No	No	No
Cifrado hardware	Si	Si	Si	Si	Si	Si
Soporte ToIP	Opc.	Opc.	Opc.	Opc.	Opc.	Opc.

Figura 117 – Características Familia x6x Teldat

- Router Backup Cisco 2811
  - Tecnología: ATM
  - Routing: OSPF
  - Ancho de Banda contratado: 34 Mbps

Figura 118- Router Back-Up Cisco 2811

- Características básicas del equipamiento

Feature	Benefit
Enhanced Network-Module (NME) Slots	• The NME slots support existing network modules (Note: NM and NME support on Cisco 2811, 2821, and 2851 only) • NME Slots offer high data throughput capability (up to 1.6Gbps) and support for Power over Ethernet (POE). • NME slots are highly flexible with support for extended NMEs (NME-X on Cisco 2821 and 2851 only) and enhanced double-wide NMEs (NME-XDs) (Note: Cisco 2851 only).
High-Performance WIC (HWIC) Slots with Enhanced Functionality	• Four integrated HWIC slots on Cisco 2811, 2821, and 2851 and two integrated HWIC slots on Cisco 2801 allow for more flexible and dense configurations. • HWICs slots can also support WICs, VICs, and VWICs • HWIC slots offer high data throughput capability (up to 400 Mbps half duplex or 800 Mbps aggregate throughput) and Power over Ethernet (POE) support. • A flexible form factor supports up to two double-wide HWIC (HWIC-D) modules.
Dual AIM Slots	• Dual AIM slots support concurrent services such as hardware-accelerated security, ATM segmentation and reassembly (SAR), compression, and voice mail (Refer to Table 7 for more details on specific platform support).
Packet Voice DSP Module (PVDM) Slots on Motherboard	• Slots for Cisco PVDM2 Modules (DSP Modules) are integrated on the motherboard, freeing slots on the router for other services.
Extension-Voice-Module (EVM) Slot	• The EVM supports additional voice services and density without consuming the network-module slot (Note: available only on Cisco 2821 and 2851).
USB Support	• Up to two USB ports are available per Cisco 2800 series router. The routers' Universal Serial Bus (USB) ports enable important security and storage capabilities.

Figura 119- Características Básicas Familia 2800 Cisco

Todo el equipamiento anteriormente descrito será montado en el armario 1 de la planta 1.

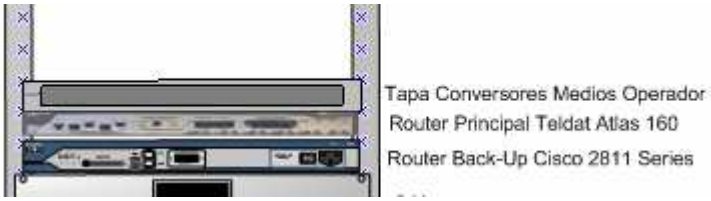


Figura 120- Elementos subsistema nivel 3

1.4.2.1. Protocolos routing

Enlace Principal

Se ha seleccionado el protocolo de routing BGP sobre tecnología MPLS por ser el requerido para la formación de una malla de interconexión todos con todos. Mediante este protocolo, por cierto el utilizado para la conexión al mundo Internet, se puede crear una estructura mallada donde exista visibilidad de todas las sedes que forman la organización, de forma que no existe un punto común, por el que tengan que pasar todas las comunicaciones.

Además, mediante MPLS conseguimos una red:

- Flexible: Los enlaces puede ser ampliados (siempre que se tenga capacidad física), simplemente realiza configuración en los routers finales. No es necesaria la provisión de enlaces adicionales
- Multiservicio: Como veremos en el apartado de clase de servicio, la red nos permite incluir todos los tipos actuales de tráfico: voz, datos, multimedia, video…
- Basada en etiquetas: A las tramas IP se les anexan unas etiquetas, mediante las cuales se realiza la conmutación de tramas en la red MPLS. Esta conmutación es muy rápida, permitiendo unos retardos en red muy bajos

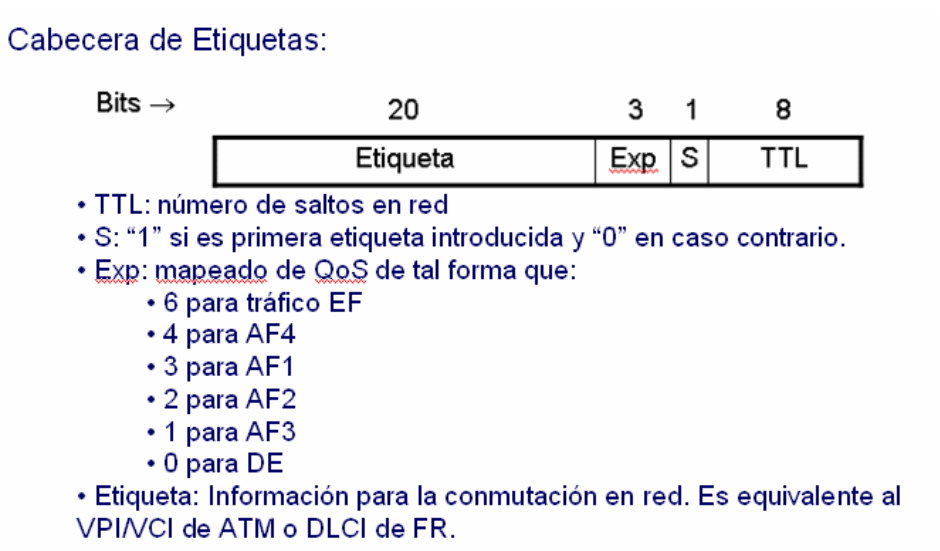


Figura 121- Etiquetado Red MPLS

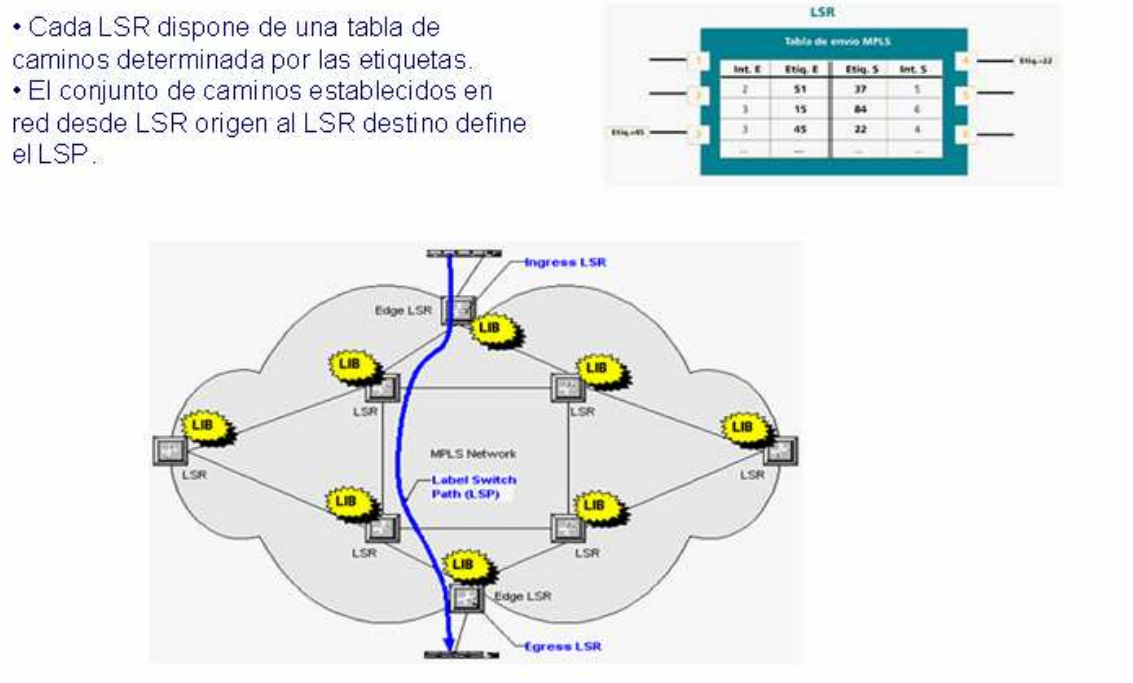


Figura 122- Creación del camino en destino- Red MPLS

- Al tratarse de de una red WAN Ethernet de nivel 2, la conmutación de tramas es muy rápida, sobre todo en el ámbito provincial, donde todos las sedes se conectan a equipos de conmutación de red de operador [pej. Alcatel 7750], que nos permite tiempos de respuesta "parecidos" a los obtenidos en entornos LAN

Figura 123- Equipamiento WAN Operador – Red MPLS

- Anchos de banda superiores a los que se conseguían con tecnologías ATM. Lo habitual es estar en el orden de magnitud de los 10Mb, 50 Mb o 100Mb.

A continuación se muestran las configuraciones BGP en el router principal

```
  protocol bgp
; -- Border Gateway Protocol user configuration --
    enable
;
; Sistema autonomo 65535
    as 65535
    export as 65535 prot direct 10.47.133.0 mask 255.255.255.0 exact
    export as 65535 prot direct 10.1.155.0 mask 255.255.255.0 exact
;
    group type internal peer-as 65535
; -- BGP group configuration --
; Direccionamiento de los root-reflector [equipos core de central]
      peer 172.29.250.3
      peer 172.29.250.3 local-as 65535
      peer 172.29.250.4
      peer 172.29.250.4 local-as 65535
```

Enlace Backup

Se ha seleccionado OSPF para el enlace de back-up con tecnología ATM. La tecnología ATM nos permite configurar caminos pre-establecidos con los destinos mas habituales. Así por ejemplo, se definirá un camino [pvc] contra la sede central, donde se concentran los servicios típicos de acceso para la sede objeto del estudio. Este PVC tendrá una capacidad de 7 Mb.

Además se estima necesario que esta sede también tenga comunicación directa con otra de las sedes más importantes de la provincia donde se encuentra. Se definirá por tanto otro PVC de capacidad 3 Mb contra esa otra sede.

La siguiente figura ilustra las conexiones sobre la red ATM

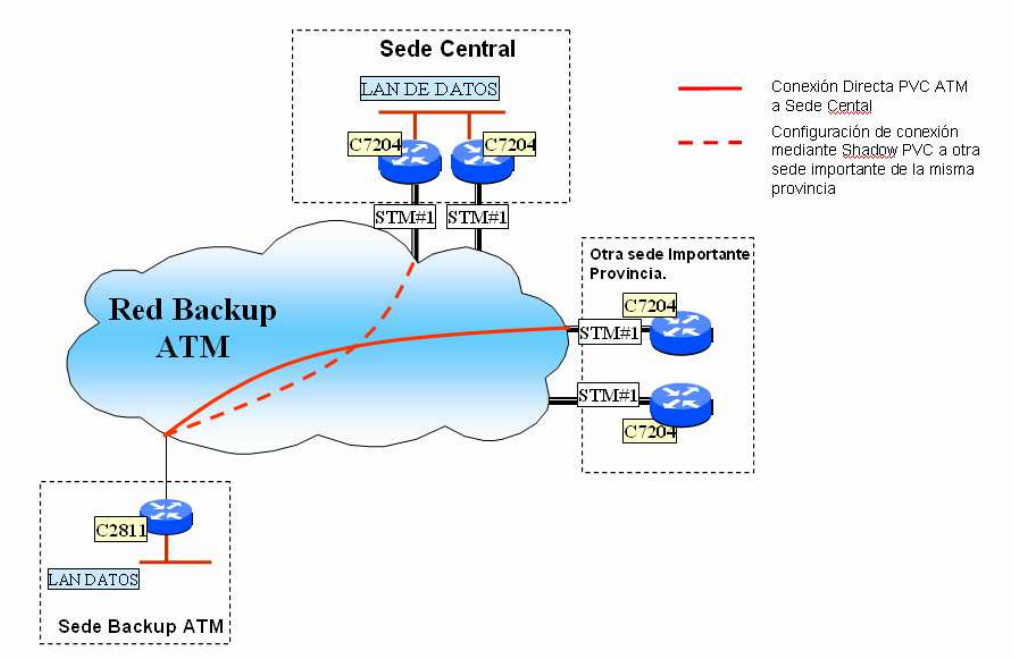


Figura 124- Router Backup – Conexión ATM

A continuación se muestras las configuraciones OSPF y dimensionado de los PVCs rt y nrt en el router de back-up

```
! Confituración OSPF
router ospf 132
router-id 10.251.33.25
log-adjacency-changes
area 31 nssa

network 10.1.155.0 0.0.0.255 area 31
network 10.47.133.0 0.0.0.255 area 31
network 10.251.33.0 0.0.0.3 area 31
bundle VOZDAT
  class-bundle pvc-bundle
  pvc-bundle DAT_MAP001L1 0/32
   class-vc pvc-vc
! Ancho de Banda del PVC nrt
   vbr-nrt 9000 9000 1
  pvc-bundle VID_MAP001L1 0/40
```

```
    class-vc pvc-vc

  ! Ancho de Banda del PVC rt

    vbr-rt 768 768 1
```

1.4.2.2. Aplicación calidad de servicio

Uno de los aspectos más importantes a la hora del diseño de un enlace WAN es la necesidad de dotar a los mismos de funcionalidades que nos permitan clasificar los distintos tipos de tráfico que se generen en nuestra redes LAN, de cara a un optimo transporte de los mismos. No es lo mismo una sede en la que simplemente se trate de tráfico de datos hacia/desde Internet, que una sede con necesidades de telefonía IP, o una sede con grandes necesidades de tráfico multimedia.

Es por ello que los distintos operadores de comunicaciones, desde hace ya unos años, son capaces de soportar distintas clasificaciones de tráfico en los enlaces WAN. A cada una de estas clasificaciones las denominaremos Clases de Servicio.

Lo más básico consiste en tener, como mínimo 3 clases de servicio:

- Clase de Servicio para Voz (ToIP)
- Clase de Servicio tráfico corporativo
- Clase de Servicio por defecto (resto tráfico e Internet)

En concreto para la realización de este proyecto se han demandado mas clases de servicio a nuestro operador de comunicaciones, consiguiendo hasta 6 clases de servicio que definen de la siguiente forma en el enlace principal:

- Clase de Servicio para Voz [ToIP] → EF: Clase de servicio con la más alta prioridad. El ancho de banda asignado a esta clase de servicio no podrá se ocupado por ningún otro tipo de tráfico. Los paquetes marcados con esta clase de servicio además tendrán prioridad en lo que a retardo y jitter se refiere, muy problemático en este tipo de tráfico
- 4 clases de servicio marcadas como AFx [4,1,2,3], para el transporte de distintos tipos de tráfico.
    - AF4: Se reserva para tráfico multimedia, principalmente video o videoconferencia. Es el más prioritario de los AF
    - AFx [1,2,3]: se reserva para el resto de necesiades de tráfico de datos [correo electrónico, acceso servidores criticos…]
    - DE: Default: Tráfico por defecto, el de menos prioridad, habitualmente reservado para el tráfico de navegación de Internet pública

En la siguiente figura se aprecia una posible división del tráfico

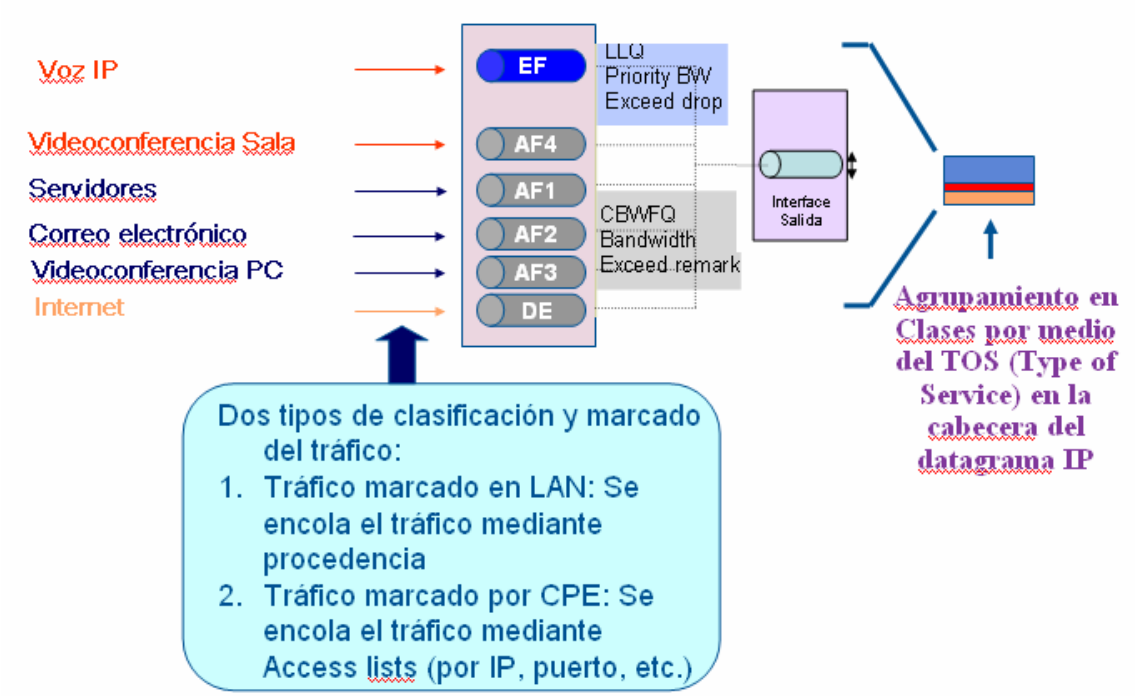


Figura 125- Calidad de Servicio enlace MPLS

Uno de los aspectos importantes es determinar cuanto porcentaje del ancho de banda contratado se asigna a cada clase de servicio. En el caso que nos ocupa, los porcentajes, y por tanto el ancho de banda mínimo asignado será.

Calidad de Servicio	Servicio
EF	Voz
AF4	Videoconferencia sala y despacho
AF1	Acceso Servicios Corporativos
AF2	Correo Electrónico
AF3	Videoconferencia de puesto usuario
DE	Internet y resto tráfico

CALIDAD DE SERVICIO	PORCENTAJE BW	BW TOTAL(Mbps)
EF	5%	50
AF4	5%	50
AF1	40%	400
AF2	20%	200
AF3	5%	50
DE	25%	250

Figura 126- Asignación Calidad de Servicio enlace principal

Es importante tener en cuenta que la gestión de QoS no es estática, es decir, el ancho de banda asignado a una clase de servicio en concreto se deberá entender como el mínimo ancho de banda que tendrá asignado este tipo de tráfico en caso de congestión del enlace.

Si no se produce congestión del enlace, las clases de servicio pueden aumentar o disminuir su ancho de banda asignado en función de sus necesidades, "tomando prestado" el ancho de banda necesario de cualquier otra clase de servicio, mientras ésta última no lo necesite. La siguiente figura ilustra este funcionamiento.

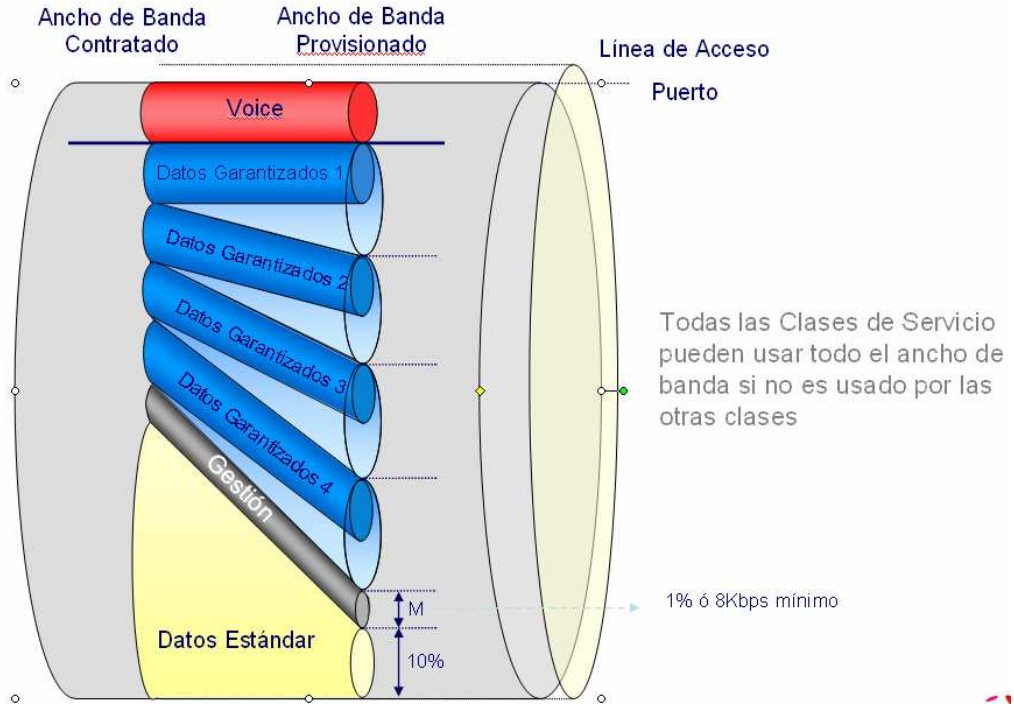


Figura 127- Funcionamiento QoS enlace principal

A continuación se muestra la configuración de QoS en el rouer principal.

```
; Calidad de Servicio

feature bandwidth-reservation
; -- Bandwidth Reservation user configuration --
     network ethernet1/0.100


      class ef_out 100 real-time
        class ef_out set dscp 46
        class ef_out rate-limit 16500
;
        class af41_out 10
```

```
        class af41_out set dscp 34
        class af41_out rate-limit 5600
        class af41_out exceed classify af42_out
;
        class af31_out 5
        class af31_out set dscp 26
        class af31_out rate-limit 2800
        class af31_out exceed classify af32_out
;
        class af21_out 20
        class af21_out set dscp 18
        class af21_out rate-limit 8400
        class af21_out exceed classify af22_out
;
        class af11_out 40
        class af11_out set dscp 10
        class af11_out rate-limit 11200
        class af11_out exceed classify af12_out
```

El enlace de respaldo basado en tecnología ATM, en lo que a QoS se refiere, se configura utilizando los distintos tipos de PVC que dispone el estándar [real time, no real time].

Se configura un PVC Real Time [rt] para incluir todo el tráfico de voz y video, el cual habitualmente está centralizado contra la sede principal.

Se configura un PVC No Real Tme [nrt] para incluir todo el resto de tráfico.

El mapeo entre los PVCs ATM y las clases de servicio MPLS se puede observar en la siguiente figura.

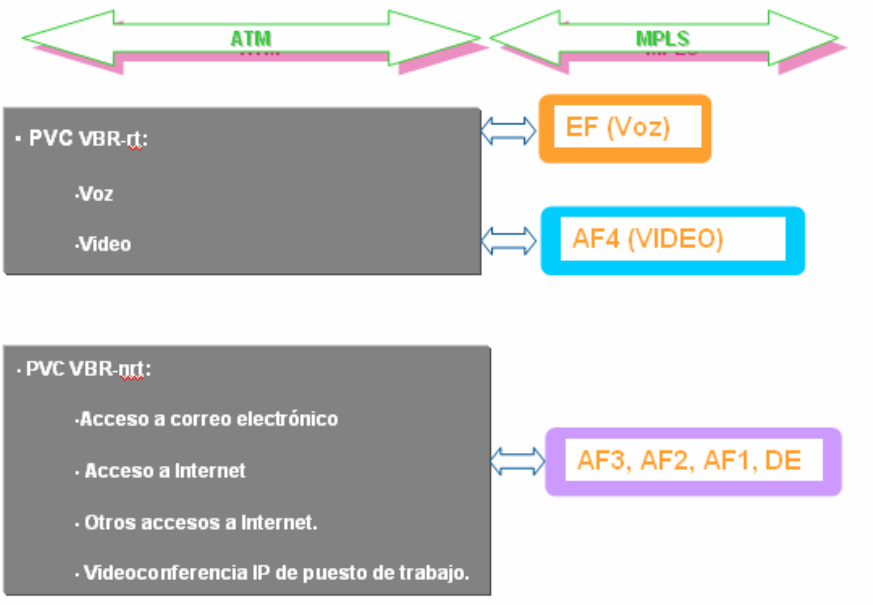


Figura 128- Mapeo PVCs ATM con QoS MPLS

A continuación se muestra la calidad de servicio en el router de backup basada en PVCs.

```
- QoS basada en PVcs NRT
vc-class atm prec-vbrnrt
 precedence 0-2, 4, 6-7
 no bump traffic
 protect vc
!
vc-class atm prec-vbrrt
 precedence 3, 5
 no bump traffic
 protect vc
```

1.4.2.3. Configuración enlaces LAN/WAN – Direccionamiento

La sede objeto de este proyecto formará parte de una red de sedes todas ellas conectadas entre si, para las cuales se ha especificado un plan de direccionamiento tanto para los enlaces LAN [con los switches], como con los enlaces WAN [red MPLS y ATM].

El direccionamiento WAN, será relativamente sencillo, y estará formado por subredes típicamente /27 o /28 con la configuración IP de los routers en sus interfaces WAN.

El direccionamiento LAN tiene algunas implicaciones adicionales, principalmente el número de usuarios de los que dispondrá la sede. Hay que tener en cuenta que la sede cuenta con un servicio de ToIP, servicio que también necesita su propio espacio de direccionamiento. Al utilizar el mini-switch en los terminales IP, y por tanto compartir los servicios de voz y datos puerto en el switch, será necesario montar subinterfaces en los interfaces físicos de los routers, par dar cabida a las dos subredes.

El direccionamiento seleccionado para la sede objeto de nuestro proyecto es el siguiente.

- Red Datos: 10.47.133.0 /24
- Red ToIP: 10.1.155.0 /24

Por tanto el direccionamiento asignado a las distintas subinterfaces (ToIP y datos) en los interfaces LAN son:

- Router Principal:
  - Datos: 10.47.133.12
  - ToIP: 10.1.155.12
- Router Backup:
  - Datos: 10.47.133.13
  - ToIP: 10.1.155.13
- VRRP:
  - Datos: 10.47.133.11
  - Voz: 10.1.155.11

Figura 129- Direccionamiento LAN Routers

A continuación se muestra el direccionamiento LAN en el router principal, así como la configuración de TVRP, para el montaje final de VRRP entre ambos routers.

Uno de los problemas que se presentan al disponer de dos conexiones WAN (MPLS y ATM) y dos routers, es que ante la caída del router principal, es decir, de la dirección IP gateway [puerta de enlace], si esta es la dirección IP física del router, los equipos conectados en la red ethernet no tendrán conectividad, ya que éstos no serán capaces de forma automática de cambiar la dirección IP Gateway en su pila de protocolo TCP/IP.

Por tanto se hace necesario implementar algún tipo de mecanismo que permita realizar esta conmutación de forma automática.

En nuestro caso tenemos equipos de subsistema de nivel 3 [routers] de distintos fabricantes, Teldat para el router principal y Cisco para el router de Back-up.

El protocolo propietario de Cisco para solucionar esta problemática es HSRP. El protocolo propietario de Teldat para solucionas esta problemática es TVRP, pero no se podrá implementar uno u otro ya que son incompatibles entre si.

La solución a esta problemática consiste en implementar VRRP que es un protocolo de redundancia no propietario definido en el RFC 3768.

El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico. Los dos routers físicos se configuran representando al router virtual, con sólo uno de ellos realizando realmente el enrutamiento. Si el router físico actual que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

Un router virtual tiene que utilizar la siguiente dirección MAC: 00-00-5E-00-01-XX. El último byte de la dirección es el identificador de router virtual (*Virtual Router IDentifier* o VRID), que es diferente para cada router virtual en la red. Esta dirección sólo la utiliza un único router físico a la vez, y es la única forma de que otros routers físicos puedan identificar el router maestro en un router virtual. Los routers físicos que actúan como router virtuales deben comunicarse entre ellos utilizando paquetes con dirección IP multicast 224.0.0.18 y número de protocolo IP 112.

Los routers maestros tienen una prioridad de 255 y los de respaldo entre 1 y 254. Cuando se realiza un cambio planificado de router maestro se cambia su prioridad a 0 lo que fuerza a que alguno de los routers de respaldo se convierta en maestro más rápidamente. De esta forma se reduce el periodo de desconexión en un cambio rol VRRP.

```
   network ethernet0/0

; -- Ethernet Interface User Configuration --

   description " conexion LAN DATOS "
;
   ip address 10.47.133.12 255.255.255.0
;
   ip dhcp-relay server 10.47.48.7

   ip tvrp 10 ip 10.47.133.11
   ip tvrp 10 priority 110
   ip tvrp 10 authentication-data "cisco"
   ip tvrp 10 destination-ip 20.20.20.20

;- subinterface del puerto fisico ethernet 0/0, para subred voz, vlan 20

   network ethernet0/0.20

; -- Ethernet Subinterface Configuration --
   description " conexion LAN Voz"

   ip address 10.1.155.12 255.255.255.0

   ip tvrp 30 ip 10.1.155.11
   ip tvrp 30 priority 110
   ip tvrp 30 authentication-data "cisco"
   ip tvrp 30 destination-ip 20.20.20.20
;    encapsulation dot1q 20
```

A continuación se muestra el direccionamiento LAN en el router de backup, así como la configuración de HSRP, para el montaje final de VRRP entre ambos routers.

```
- Direccionaminet LAN
interface FastEthernet0/0

description LAN DATOS PFG-Sede1

no ip address

speed 100

full-duplex

end

! Direccionamiento LAN Datos

interface FastEthernet0/0.1

encapsulation dot1Q 1 native

ip address 10.47.133.13 255.255.255.0

ip helper-address 10.47.48.7

no cdp enable

-- HSRP Datos
standby 10 ip 10.47.133.11

standby 10 preempt delay minimum 5

end


! Direcciona LAN Voz

interface FastEthernet0/0.20

! vlan 20 voz

encapsulation dot1Q 20

ip address 10.1.155.13 255.255.255.0

no cdp enable

- HSRP LAN Voz

standby 30 ip 10.1.155.11

standby 30 preempt delay minimum 5
end
```

1.4.2.4. Gestión equipo y gestión usuarios

Uno de los aspectos a tener en cuenta en la configuración de los equipos es la utilización de una IP de gestión de los mismos, distinta a las IPs de tráfico, preferiblemente asociadas incluso a una vlan distinta, para que en caso de algun tipo de problema con la red [vlan] de tráfico de datos, al menos se puede conseguir alcanzar el router por la IP de gestión, y poder diagnosticar el problema.

En nuestro caso se realiza una configuración adicional de una vlan para la gestión de los equipos y se les asigna un direccionamiento "ad-hoc" para la gestión del dispositivo.

A continuación se muestra la configuración del enlace WAN del router principal, donde existe configurada una subinterface vlan 3000 para la gestión del dispositivo.

```
;
  feature vlan
; -- VLAN configuration --

    enable
;
    vlan 100 ethernet1/0 port 1
    vlan 100 ethernet1/0 port internal
    vlan 200 ethernet1/0 port 2
    vlan 200 ethernet1/0 port internal
    vlan 300 ethernet1/0 port 3
    vlan 300 ethernet1/0 port internal
    vlan 3000 ethernet1/0 port 1
    vlan 3000 ethernet1/0 port internal

- Gestión WAN

  network ethernet1/0.3000
; -- Ethernet Subinterface Configuration --
    ip address 10.150.24.169 255.255.254.0
;
    encapsulation dot1q 3000

  exit
```

A continuación se muestra la configuración del enlace WAN del router de backup

```
- Interfaz WAN

interface ATM1/0.32 point-to-point

description CONEXION BACKUP DATOS A SSCC MIP001L1 ATM4/0.448 /

ip address 10.251.33.2 255.255.255.252
```

Otro de los aspectos importantes es la gestión de usuarios, perfiles y formas de acceso al router. Es indispensable tener un usuario con todos los privilegios [lectura-escritura] para poder realizar las configuraciones de los equipos. Al ser fabricantes distintos los privilegios se obtienen de forma distinta:

- Router Teldat
    - Es necesario crear un usuario con privilegios para el menú P4 y P5, donde se realizan las tareas de configuración
    - Se creará un usuario con acceso de solo lectura , es decir, acceso al menú P3
    -
- Router Cisco
    - Es necesario crear un usuario con privilegios "enable"
    - Se creará un usuario con acceso de solo lectura "show".

A continuación se muestra la creación de usuarios en el router principal.

```
; -- Gestión usuarios, acceso lectura access-level monitor (solo lectura) P3

  user map hash-password 26B54246C65C4D7FFABE5720F73C5B53

  user map access-level monitor
```

A Continuación se muestra la creación de usuarios en el router de back-up

```
! - Gestion de usuarios

username map privilege 2 secret
```

1.4.2.5. Gestión Ancho de Banda Consumido

Uno de los aspectos claves en la gestión de los dispositivos del subsistema del nivel 3 es la capacidad para determinar el ancho de banda consumido por su enlace WAN, de forma que se puedan obtener estadísticas del tráfico cursado de cara a la toma de decisiones como el aumento o dismunición de la capacidad de ancho de banda del enlace [recordad que una de las características básicas del los enlaces MPLS era su capacidad de crecimiento o disminución de ancho de banda, siempre que no se sobrepase la capacidad física del enlace, simplemente reconfigurando el parámetro ancho de banda.

Para la realización de esta tarea se ha seleccionado la herramienta Cacti, distribuida bajo licencia GPL.

Cacti ofrece un interfaz web ágil, intuitivo y sencillo de utilizar que, basándose en el protocolo SNMP, permite obtener de forma gráfica el consumo de ancho de banda [entre otras cosas] de un enlace de un router.

Lo primero será dar de alta el dispositivo en la BBDD de dispositivos [devices] de Cacti.

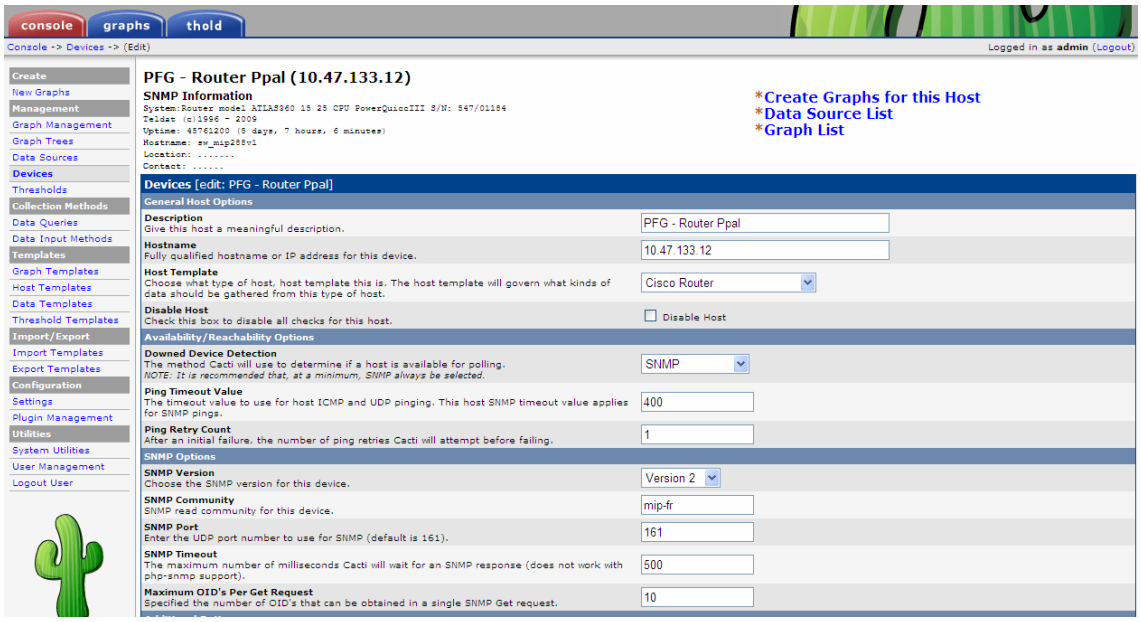


Figura 130- Cacti – Creación dispositivo a monitorizar

Los parámetros básicos que hay que proporcionar son:

- Descripción: que se le quiere dar el dispositivo
- Hostname: dirección IP de gestión del dispositivo
- Opciones SNMP: Versión SNMP, comunidad y puerto

A continuación se crará un gráfico para este dispositivo, pulsado la opción correspondiente. Cacti nos mostrará una lista con todos los interfaces del dispositivo, para que se seleccione del que se quieren obtener datos de estadísticas.

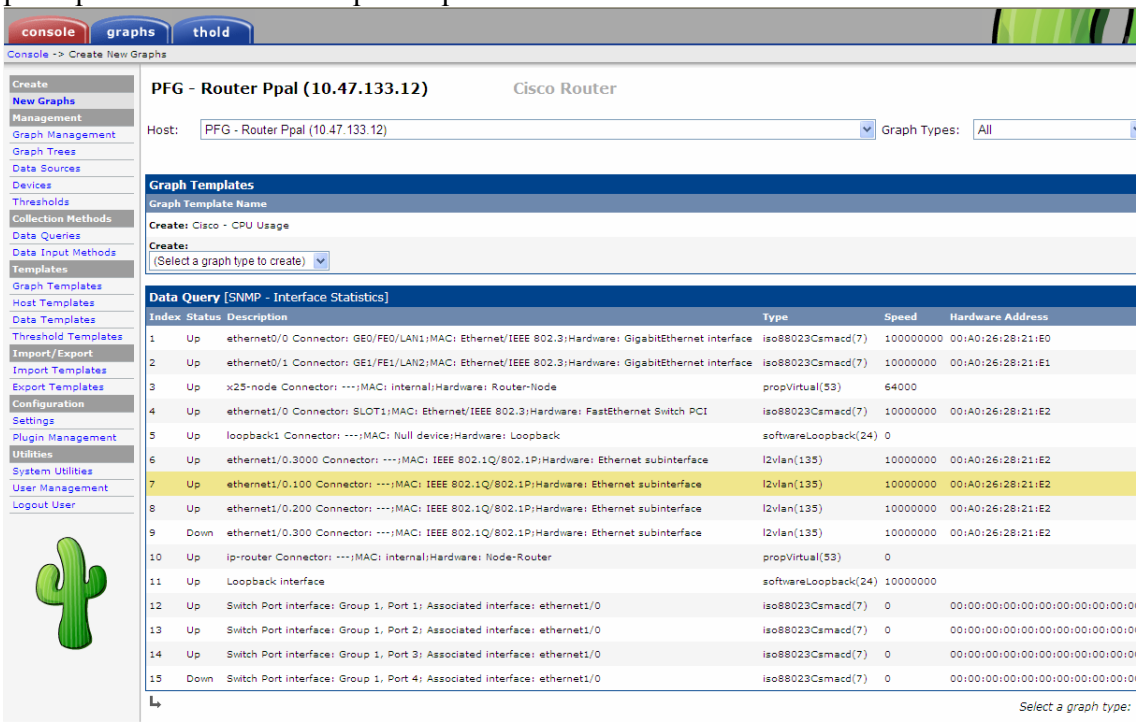


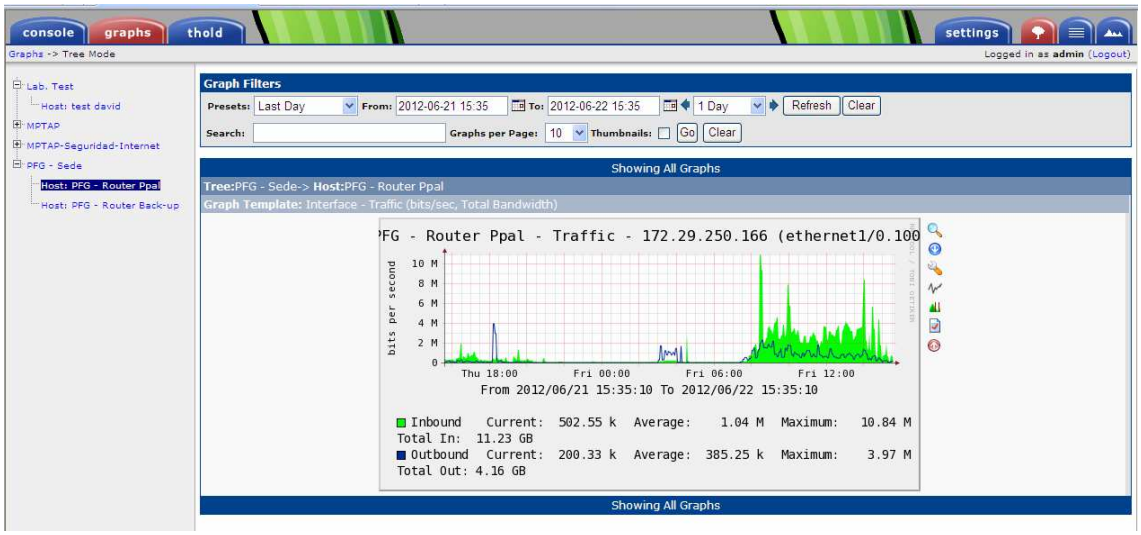
Figura 131- Cacti creación gráfico asociado a router

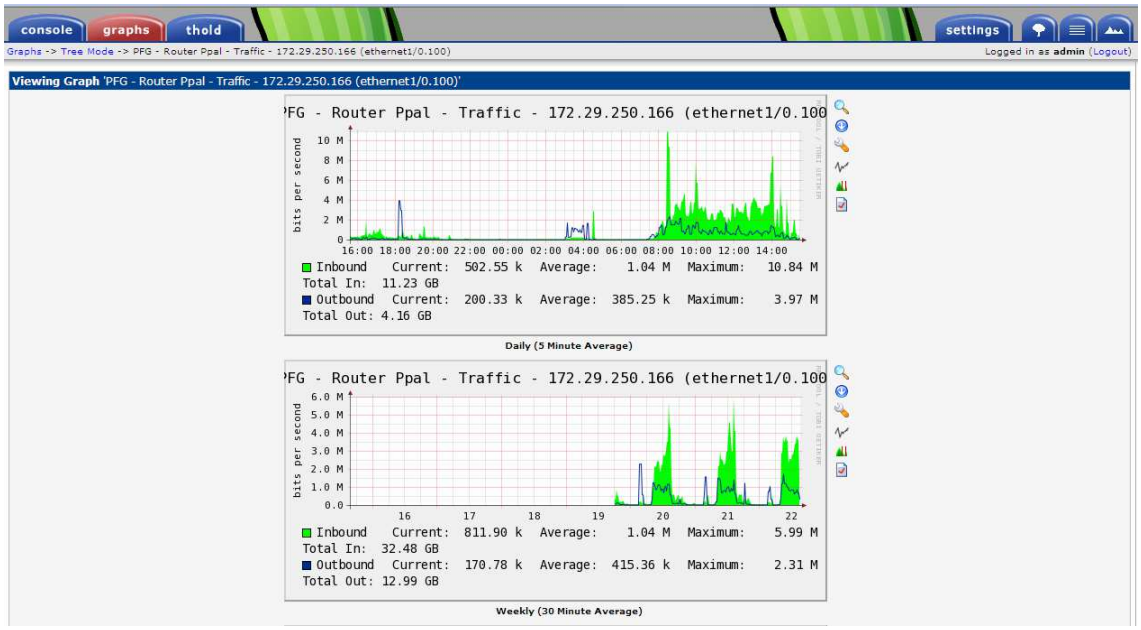
Una vez creado el gráfico es necesario crear un arbol de gráficos para contenerlos. Para ello se pulsa sobre la opción Graph Trees y procedemos a crear un nuevo arbol de gráficos. Se añaden los routers al árbol.

Figura 132 – Creación árbol con hosts [routers] asociados

Una vez creada toda la estructura, cada 5 minutos se realizará un pooling por parte de Cacti, al interfaz indicado, para obtener la ocupación del mismo. Este dato será representado en los gráficos correspondientes.

Las gráficas correspondientes al router principal de la sede son:





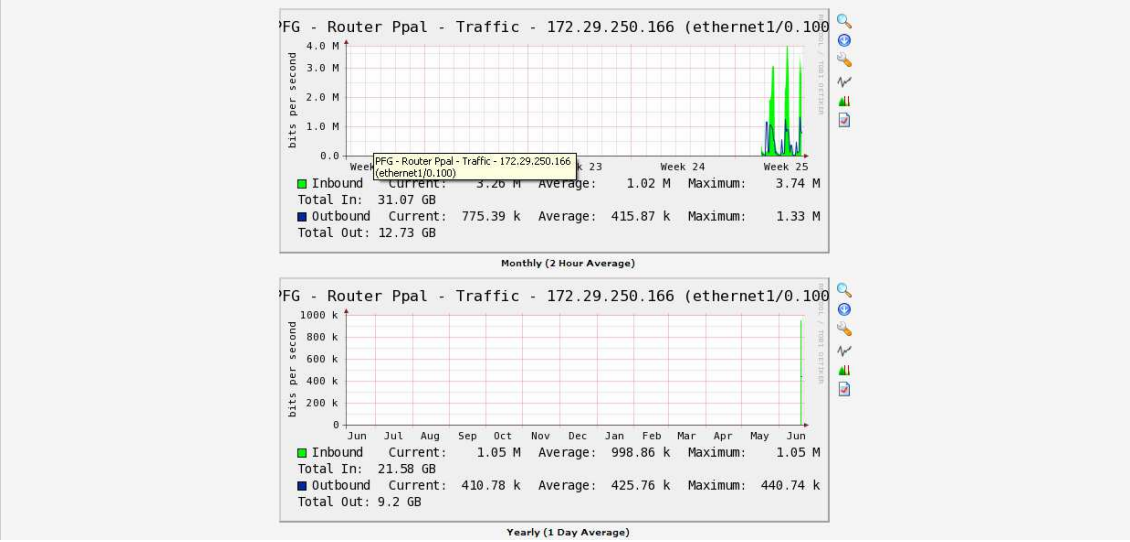


Figura 133- Nivel 3- Graficas Cacti Router Principal

Las gráficas correspondientes al router de backup son las siguientes [lo lógico es obtener gráficas de muy pocos kbps, al no transitar tráfico por estos enlaces]

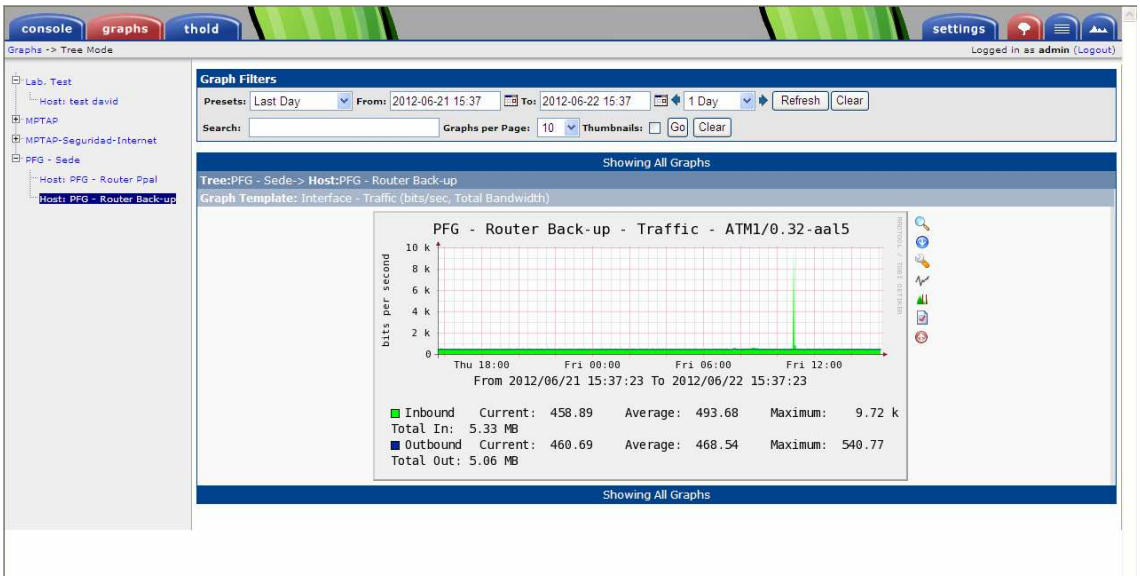


Figura 134- Nivel 3 – Gráficas Cacti Router Back-up

1.4.2.6. Cronograma

A continuación se presenta un cronograma de alto nivel donde aparecen detalladas para cada subsistema a implantar, las distintas tareas y los tiempos de implementación de las mismas.

El proyecto global se ha estimado en unos 16 dias laborables.

Se ha conseguido acortar plazos realizando tareas en paralelo tareas independientes de los distintos subsitemas, teniendo en cuenta que se contará con personal dedicado y especializado para cada subsistema.

Evidentemente lo primero será el inicio de las labores de cableado estructurado, infraestructura básica para poder dotar a la oficina de las necesidades de comunicación dentro de cada planta y entre plantas.

Los trabajos de definición del diseño de nivel 2 y del nivel 3, así como la provisión de switches y routers se lanzan además prácticamente en paralelo con el inicio del proyecto, al tener perfectamente definido el mismo, en lo que a equipamiento se refiere.

WBS	Tasks	Task Lead	Start	End	Duration (Days)	% Complete	Working Days	Days Complete	Days Remaining
1	**Subsistema Cableado Estructurado**	[Name]	30-may-12	14-jun-12	16	0%	12	0	16
1.1	Reunión Inicial Proyecto - Definición del proyecto		30-may-12	30-may-12	1	0%	1	0	1
1.2	Recepción Planos Arquitectura - Revisión		31-may-12	1-jun-12	2	0%	2	0	2
1.2.1	Revisión Canalización Definida		31-may-12	31-may-12	1	0%	1	0	1
1.2.2	Revisión Distribución Cajas Cableado		1-jun-12	1-jun-12	1	0%	1	0	1
1.3	Provisión Material necesario y personal		2-jun-12	4-jun-12	3	0%	1	0	3
1.4	Realización de los trabajos de cableado estructurado		5-jun-12	14-jun-12	10	0%	8	0	10
1.4.1	Cableado Planta 1		5-jun-12	8-jun-12	4	0%	4	0	4
1.4.2	Cableado Planta 2		9-jun-12	11-jun-12	3	0%	1	0	3
1.4.3	Impactado en Rack Principal		12-jun-12	13-jun-12	2	0%	2	0	2
1.4.4	Certificación Instalación		14-jun-12	14-jun-12	1	0%	1	0	1
2	**Subsistema Nivel Acceso**	[Name]	2-jun-12	14-jun-12	13	0%	9	0	13
2.1	Definición Diseño Nivel 2		2-jun-12	3-jun-12	2	0%	0	0	2
2.2	Provisión Switches, Terminales IP y Personal		4-jun-12	8-jun-12	5	0%	5	0	5
2.3	Creación de las plantillas basicas Configuración: gestion, vlans, qos...		4-jun-12	8-jun-12	5	0%	5	0	5
2.4	Enracado e implementación de la configuración		9-jun-12	10-jun-12	2	0%	0	0	2
2.5	Parcheo de las tomas a los switches		14-jun-12	14-jun-12	1	0%	1	0	1
3	**Subsistema Nivel Enrutamiento**	[Name]	2-jun-12	11-jun-12	10	0%	6	0	10
3.1	Definición Diseño Nivel 3		2-jun-12	3-jun-12	2	0%	0	0	2
3.2	Provisión routers y Personal		4-jun-12	8-jun-12	5	0%	5	0	5
3.3	Creación de las plantillas basicas Configuración: gestion, direccionamiento, qos...		4-jun-12	8-jun-12	5	0%	5	0	5
3.4	Enracado e implementación de la configuración		9-jun-12	10-jun-12	2	0%	0	0	2
3.5	Conexionado con los switches		11-jun-12	11-jun-12	1	0%	1	0	1
4	**Documentación**		12-jun-12	16-jun-12	5	0%	4	0	5
4.1	Documentación Cableado Estructurado		15-jun-12	16-jun-12	2	0%	1	0	2
4.2	Documentación Subsistema Nivel 2		15-jun-12	16-jun-12	2	0%	1	0	2
4.3	Documentación Subsistema Nivel 3		12-jun-12	13-jun-12	2	0%	2	0	2

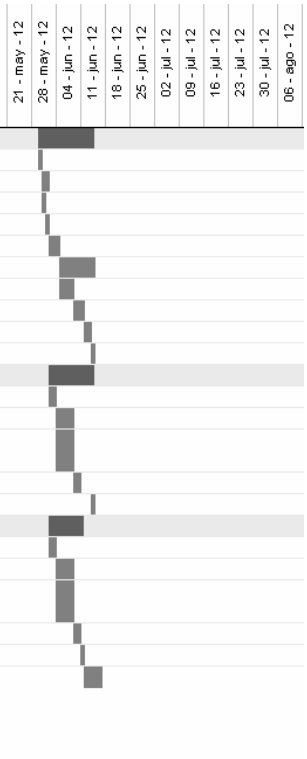


Figura 135- Cronograma Proyecto

Bibliografía

International Organization of Standardization [http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40636]

Tyco Electronics Ltd. / Network Solutions / AMP NETCONNECT - 568-C.0: La Nueva Generación de Estándares de Cableado
[http://www.ampnetconnect.com/documents/lan_standards_update_2009_aug_espan.pdf]

CommsCope – Componentes para cableado
[http://awapps.commscope.com/catalog/systimax/catalog.aspx]

Poe + Poe Plus – Información sobre Power over Ethernet
[http://standards.ieee.org/news/]

RFC- 3850 - Secure/Multipurpose Internet Mail Extensions
[http://www.ietf.org/rfc/rfc3850.txt]

Avaya Router Switch 4500 Series – Documentación
[http://www.avaya.com]

Teldat routers. Configuracion y Protocolos
[http://www.teldat.com/es/index.php?home=routers-gateways-inicio]

Cisco Systems, Inc. Routers y switches
[http://www.cisco.com/]

Artículos Tecnología: ATM y MPLS. Ramón Millan
[http://www.ramonmillan.com]

IpSwitch-WhatsUp
[http://www.whatsupgold.com/es/]