



POLITÉCNICA

"Ingeniamos el futuro"

CAMPUS
DE EXCELENCIA
INTERNACIONAL



Graduado en Ingeniería Informática

Universidad Politécnica de Madrid

Escuela Técnica Superior de
Ingenieros Informáticos

TRABAJO FIN DE GRADO

Diseño de una Red Corporativa para un Edificio Empresarial

Memoria Final

Autor: Pablo Trujillo Díez

Tutor: D.^a Sonia Frutos Cid

MADRID, enero 2019

Resumen

Este proyecto consistirá en el estudio y el diseño de una red empresarial que constará de cuatro sedes distribuidas geográficamente en Madrid. Una de las sedes se contemplará como la principal de todas y las otras tres recibirán el servicio de la primera. El diseño constará de cuatro partes diferenciadas, las cuales son, la arquitectura de red de telefonía IP, la arquitectura de la red de datos donde se contemplará la parte inalámbrica y la parte cableada, la arquitectura de la seguridad de la propia red y un direccionamiento de la red principal para el tráfico de conexiones a ellos. Para la realización de la red se establecerá un estudio sobre los dispositivos adecuados para el proyecto, para ello se realizará un dimensionado de cada una de las partes para poder adaptar los diferentes dispositivos a los requisitos de la red empresarial.

Finalmente se evaluarán las condiciones finales de la red, así como los costes finales y distribuciones finales de los diferentes elementos para poder estimar los gastos finales de la red, con la finalidad de poder incorporar el proyecto final a un caso real para cualquier empresa recién incorporada al sector.

Abstract

This project will consist of the study and design of a business network that will consist of four sites distributed geographically in Madrid. One of the venues will be considered as the main one of all and the other three will receive the service of the first one. The design will consist of four distinct parts, which are the IP telephony network architecture, the data network architecture where the wireless part and the wired part will be contemplated, the security architecture of the network itself and an address of the main network for traffic connections to them. To carry out the network, a study will be established on the appropriate devices for the project, for which a dimensioning of each of the parts will be carried out to adapt the different devices to the requirements of the business network.

Finally, the final conditions of the network will be evaluated, as well as the final costs and final distributions of the different elements to be able to estimate the final expenses of the network, with the purpose of being able to incorporate the final project to a real case for any newly incorporated company into the sector.

Índice de Contenidos

Capítulo 1: Introducción	1
1.1. Descripción del Proyecto	2
1.2. Objetivos del Proyecto	3
1.3. Estructura de la Memoria	4
Capítulo 2: Planteamiento del Problema	5
Capítulo 3: State of Art	7
3.1. Telefonía IP	8
3.1.1. Concepto de VoIP	9
3.1.1.1. VENTAJAS	9
3.1.1.2. DESVENTAJAS	9
3.1.2. Protocolos	10
3.1.2.1. PROTOCOLO SIP	10
3.1.2.2. PROTOCOLO SCCP	11
3.1.2.3. PROTOCOLO H.323	12
3.1.2.4. PROTOCOLO IAX	12
3.1.3. Elementos fundamentales	12
3.1.3.1. CÓDEC	12
3.1.3.2. QoS	13
3.1.4. Cisco Call Manager	13
3.2. Redes de Datos	16
3.2.1. Red de Área Local (LAN)	16
3.2.1.1. REDES DE CABLEADO	17
3.2.1.1.1. Estructura del Cableado	17
3.2.1.1.2. Estándares del Cableado	17
3.2.1.1.3. Tipos de Cables	18
3.2.1.1.4. Arquitectura Cableado	21
3.2.1.2. REDES INALÁMBRICAS	22
3.2.1.2.1. Tipos de Redes Inalámbricas	23
3.2.1.2.2. Estándares IEEE	23
3.2.1.2.3. Arquitectura de las redes WiFi	24
3.2.2. Red de Área Extensa (WAN)	25
3.2.2.1. TIPOS DE REDES WAN	26
3.2.2.2. RED PRIVADA VIRTUAL (VPN)	26
3.2.2.2.1. Tipos de redes VPN	27
Capítulo 4: Solución Propuesta	28
4.1. Requisitos Iniciales	29
4.1.1. Número de Usuarios	29
4.1.2. Servicios	30
4.1.2.1. SERVICIO DE COMUNICACIONES DE VOZ	30
4.1.2.2. SERVICIO DE COMUNICACIONES DE DATOS	30
4.1.2.3. SERVICIOS DE COMUNICACIONES UNIFICADAS (UC)	30
4.1.3. Calidad de Servicio. QoS	31
4.1.3.1. TRÁFICO ELÁSTICO	31
4.1.3.2. TRÁFICO INELÁSTICO	31
4.1.4. Oficinas de la empresa	32
4.1.4.1. HENARES (CPD)	32

4.1.4.2. RESTO DE OFICINAS	33
4.2. Diseño de la Red	35
4.2.1. Diseño de la Red de Voz	35
4.2.1.1. ELEMENTOS PARA LA RED DE VOZ	36
4.2.1.1.1. Servidores UC	36
4.2.1.1.2. Gateway de Voz	37
4.2.1.1.3. Terminales para los Usuarios	42
4.2.1.1.4. Desglose Final	46
3.3.2. Diseño de la Red de Datos	47
3.3.2.1. DISEÑO DE RED WAN	47
4.2.2.1.1. Arquitectura de red WAN	47
4.2.2.1.2. Dimensionado de Red WAN	49
4.2.2.1.3. Tabla Resumen Red WAN	56
4.2.2.2. DISEÑO DE RED LAN	57
4.2.2.2.1. Arquitectura de Red LAN	57
4.2.2.2.2. Dimensionado Red LAN	58
4.2.2.2.3. Tabla Resumen Red LAN	61
4.2.2.3. DISEÑO DE RED WiFi	62
4.2.2.3.1. Arquitectura de Red WiFi	62
4.2.2.3.2. Dimensionado de la Red Wifi	63
4.2.2.3.3. Tabla Resumen red WiFi	65
4.2.3. Desglose de Presupuesto Final	65
4.3. Plan de Direccionamiento	66
4.4. Simulación	69
Capítulo 5: Conclusión	86
Capítulo 6: Futuras Líneas	88
Referencias	90

Índice de Tablas

TABLA 3.1: Pautas del escalamiento Clúster Cisco Call Manager	14
TABLA 3.2: Número máximo de dispositivos por Plataforma.....	15
TABLA 3.3: Clasificación de cables por Categorías	20
TABLA 3.4: Estándares IEEE 802.11	23
TABLA 4.1: Servicios de los usuarios	31
TABLA 4.2: Número de Usuarios de la empresa.....	32
TABLA 4.3: Especificaciones del Servidor	36
TABLA 4.4: Ocupación de los canales de 1 servidor	37
TABLA 4.5: Tipos de Gateways	39
TABLA 4.6: Componentes Gateway de una oficina de 500 usuarios.....	40
TABLA 4.7: Componentes Gateway de una oficina de 50 usuarios.....	41
TABLA 4.8: Distribución de perfiles de usuarios	45
TABLA 4.9: Desglose Final de Voz	46
TABLA 4.10: Caudal y velocidad de la MPLS.....	51
TABLA 4.11: Caudal y velocidad de la salida a Internet.....	51
TABLA 4.12: Especificaciones Juniper SRX1500	54
TABLA 4.13: Especificaciones PA-5060	55
TABLA 4.14: Desglose final Red WAN.....	56
TABLA 4.15: Desglose final Red LAN	61
TABLA 4.16: Prestaciones Wireless Controller	64
TABLA 4.17: Desglose final Red WiFi	65
TABLA 4.18: Desglose Final.....	65
TABLA 4.19: Redes para oficina Boadilla	66
TABLA 4.20: Redes para oficina Villaverde	67
TABLA 4.21: Redes para oficina Castilla.....	67
TABLA 4.21: Redes para oficina Henares.....	68

Índice de Figuras

FIGURA 3.1: Llamada protocolo SIP	11
FIGURA 3.2: Clúster de un Call Manager	14
FIGURA 3.3: Cable coaxial	18
FIGURA 3.4: Cable coaxial fino y grueso	19
FIGURA 3.5: Cable UTP	20
FIGURA 3.6: Cable STP	20
FIGURA 3.7: Cable de Fibra Óptica	21
FIGURA 3.8: Arquitectura de red Centralizada	21
FIGURA 3.9: Arquitectura de red Distribuida	21
FIGURA 3.10: Punto de Acceso	24
FIGURA 3.11: Controladora WiFi	24
FIGURA 3.12: Herramienta AirWave	25
FIGURA 4.1: Oficina Boadilla	34
FIGURA 4.2: Arquitectura de Voz	35
FIGURA 4.3: Componentes de los servidores	36
FIGURA 4.4: Calculadora Erlang B 500 usuarios	38
FIGURA 4.5: Calculadora Erlang B 50 usuarios	38
FIGURA 4.6: Cisco ISR 4351	40
FIGURA 4.7: Cisco ISR 4331	41
FIGURA 4.8: Cisco IP Phone 7911G	42
FIGURA 4.9: Cisco IP Phone 7941G	43
FIGURA 4.10: Cisco IP Phone 7962G y módulo 7915	44
FIGURA 4.11: Módulo 7915	44
FIGURA 4.12: Samsung Galaxy S8	45
FIGURA 4.13: Arquitectura Red WAN	47
FIGURA 4.14: Diagrama CPD	48
FIGURA 4.15: Cisco ASR 1001-HX	52
FIGURA 4.16: Módulo para ASR 1001-HX	52
FIGURA 4.17: SFP para 10 Gbps y 1 Gbps	52
FIGURA 4.18: Fuentes de alimentación ASR 10001-HX	52
FIGURA 4.19: Cisco Catalyst 4900M	53
FIGURA 4.20: Módulo WS-X4920-GB-RJ45	53
FIGURA 4.21: Módulo WS-X4908-10GE (=)	53
FIGURA 4.22: Adaptador CVR-X"-SFP10G	53
FIGURA 4.23: Módulo WS-X4904-10GE (=)	54
FIGURA 4.24: Juniper SRX1500	54
FIGURA 4.25: Palo Alto PA-5060	55

FIGURA 4.26: Arquitectura de Red LAN	57
FIGURA 4.27: Cisco C9500-40X-A	59
FIGURA 4.28: Cisco Catalyst C9407R.....	60
FIGURA 4.29: Cisco C9400-LC-48T	60
FIGURA 4.30: Cisco C9400-SUP-1XL/2	61
FIGURA 4.31: Diagrama de Red WiFi	62
FIGURA 4.32: Aruba AirWave AW-HW630-ENT.....	63
FIGURA 4.33: Aruba AP 335	64
FIGURA 4.34: Aruba Controller 7030.....	64
FIGURA 4.35: Aruba Controller 7024.....	64

Glosario

ANSI: American National Standard Institute

AP: Access Point

ATM: Asynchronous Transfer Mode

BNC: Bayonet Neill-Concelman

CME: Communications Manager Express.

CODEC: CODificador DECodificador.

CPD: Centro de Procesamiento de Datos.

CPU: Central Processing Unit.

CS-ACELP: Conjugate Structure-Algebraic Code Excited Linear Prediction.

CSS7: Chanel Signaling System 7.

DNS: Domain Name System.

DSP: Digital Signal Processor.

ECD: Equipo de Circuito de Datos

EIA: Electronic Industrial Alliance

ETD: Equipo Terminal de Datos

FSS: Foreign System Services

FTTH: Fiber To The Home

Gbps: GigaBit Per Second

GE: Gigabit Ethernet

GHz: GigaHerzios

HTTP: HyperText Transfer Protocol.

HWIC: High-Speed Wan Interface Card.

IAX: Inter-Asterisk eXchange.

IEEE: Institute Electrical and Electronic Engineering

IETF: Internet Engineering Task Force.

IM: Instant Messaging.

IP: Internet Protocol.

ISO: International Standard Organization

ISP: Internet Service Provider

ISR: Integrated Service Router.

ITU-T: International Telecommunication Union.

Kbps: KiloBit Per Second

LAN: Local Area Network.

LOPD: Ley Orgánica de Protección de Datos.

MAC: Media Access Control.

MAN: Metropolitan Area Network

Mbps: MegaBit Per Second

Megaco: Media Gateway Control

MGCP: Mega Gateway Control Protocol.

MGF: Multi Gigabit Fabric.

MINET: Mutual Information NETwork.

MPLS: MultiProtocol Label Switching.

MTP: Media Transfer Protocol.

PAN: Personal Area Network

PBX: Private Branch eXchange.

PDA: Personal Digital Assistant

PDU: Protocol Data Unit

PSTN: Public Switched Telephone Network

PVDM: Packet Voice Digital Module.

QoS: Quality of Service.

RDSI: Red Digital de Servicios Integrados.
RF: RadioFrecuencia
RTC: Real-Time Communications.
RTP: Real-time Transport Protocol.
S2S: Site to Site
SAN: Stored Area Network
SCCP: Skinny Client Control Protocol.
SEC: SouthEastern Conference.
SEP: Stable Election Protocol.
SFP: Small Form-factor Pluggable
SIP: Sesion Initiation Protocol.
SMTP: Simple Mail Transfer Protocol.
SNMP: Simple Network Management Protocol
SRST: Survivable Remote Site Telephony.
STP: Spanning-Tree Protocol
TCP: Transmission Control Protocol.
TDM: Time Division Multiplexing
TFTP: Trivial File Transfer Protocol.
TIA: Electronic Industrial Alliance
TV: TeleVision
UC: Unified Communications.
UCCX: Unified Contact Center eXpress.
UDP: User Datagram Protocol.
UNIStim: Unified Networks IP Stimulus.
UPS: Uninterruptible Power Supply.
UTP: Unshielded Twisted Pair
VLAN: Virtual Local Area Network.
VoIP: Voice Over Internet Protocol.
VPN: Virtual Private Network

WAN: Wide Area Network.
WiFi: Wireless Fidelity
WLAN: Wireless Local Area Network
WPAN: Wireless Personal Area Network
WWAN: Wireless Wide Area Network
XMPP: eXtensible Messaging and Presence Protocol.

Capítulo 1: Introducción

1.1. Descripción del Proyecto

La importancia del tráfico interno de las empresas es, hoy en día, cada vez mayor debido a las aplicaciones y servidores que se emplean para el trabajo diario y los procesos internos. La ubicación donde se concentran los recursos necesarios para el procesamiento de la información en una empresa se denomina Centro de procesamiento de datos (CPD).

En sedes tipo CPD, el tráfico interno es muy grande. Y eso conlleva la necesidad de disponer de una infraestructura de LAN escalable y flexible, de forma, que sea fácilmente configurable para separar los distintos servicios y atender a sus requerimientos de calidad y con interfaces cada vez de mayor velocidad.

También cobra mucha importancia la necesidad de una red Wireless Fidelity (WiFi) adecuada dentro del edificio, para que los trabajadores puedan trabajar en movilidad, pues se tiende en las empresas actuales a definir espacios colaborativos de trabajo, salas de reuniones, tener a personal externo subcontratado, además de un mayor número de trabajadores en puestos fijos y tomas de red LAN fija, etc.

Otro punto a tener en cuenta dentro de las empresas es la criticidad de los servicios de acceso a Internet en cuanto a disponibilidad y seguridad. Una sede central de una empresa pública muchos servicios al exterior que deben estar adecuadamente protegidos. Además, hoy en día en España, se obliga al cumplimiento de determinadas directivas de seguridad tipo LOPD y Esquema Nacional de Seguridad, que implica que tengas que tener una red interna con los mecanismos de seguridad adecuados: DNS, sistemas de protección del correo y antispam, proxis, firewalls, etc.

En cuanto al tema de la comunicación, actualmente, la tendencia es la sustitución de las soluciones de telefonía empresariales tradicionales, basadas en centralitas TDM conectadas a la Red Telefónica Pública mediante accesos digitales (accesos primarios o básicos RDSI) por soluciones basadas en centralitas IP, en las que la lógica de llamadas es una aplicación software que puede ubicarse virtualmente en servidores de la empresa donde los teléfonos son teléfonos IP conectados a la propia LAN del edificio. Esto facilita la movilidad de los usuarios, que no quedan asociados a un puesto fijo, y el ahorro en comunicaciones de telefonía entre sedes remotas de la misma organización, ya que se pueden llevar las comunicaciones de voz por la red de datos, mediante Voz sobre IP.

Todo esto hace que sea necesario disponer de una LAN adecuada para las comunicaciones, con switches que implementen adecuadamente la separación de los servicios, en VLAN's diferenciadas, que apliquen calidad de servicio diferenciada a cada servicio, etc. Teniendo todo esto en cuenta, voy a diseñar las comunicaciones corporativas de la sede central de una empresa, considerando:

- La LAN, el cableado y la Red WiFi.
- Las comunicaciones con Internet y su arquitectura de seguridad.
- La solución de telefonía IP del Edificio.

1.2. Objetivos del Proyecto

El presente proyecto se basa en el diseño de una red de área local para un edificio empresarial, llevando a cabo tanto la implementación de la arquitectura del acceso inalámbrico, como toda la conectividad del edificio a nivel de cableado y dispositivos.

El proyecto constará de dos partes claramente diferenciadas. La primera parte conllevará todo el estudio y la adquisición del conocimiento de herramientas que posteriormente utilizaremos en la segunda parte que será el diseño propio de la red. Una vez finalizado el proyecto, se pretenden conseguir los siguientes objetivos:

- Profundizar en el conocimiento de herramientas y métodos para la medición de cobertura WIFI evaluando la distribución y el tipo de materiales de los que está hecho el edificio.
- Familiarizarse con los dispositivos que componen una red LAN y su utilización. Junto con esto se revisará todo lo relacionado con sistema de seguridad para proteger a la red interna.
- Buscar las soluciones de telefonía IP permitiendo integrar en una misma red, basada en protocolo IP, las comunicaciones de voz y datos.
- Diseñar la red corporativa basándose en todos los conceptos estudiados en los objetivos anteriores. Se realiza la distribución, compra y despliegue de los dispositivos, así como la interconexión y la tira del cableado pertinente. Por último, se establecerá un presupuesto con todos los dispositivos elegidos.
- Aprender el manejo de direcciones IP en los diferentes dispositivos para establecer un plan de direccionamiento adecuado para todos los servidores y usuarios de toda la red corporativa.
- Evaluación del diseño y de la conectividad de manera que los usuarios puedan trabajar dentro de esa red.

1.3. Estructura de la Memoria

La memoria del Proyecto va a estar dividida en diferentes capítulos en los que se tratarán los diferentes temas del trabajo completo. A continuación, se detallará el contenido de los capítulos de la memoria:

- **CAPÍTULO 1:** consiste en una introducción sobre el proyecto final para dar a conocer una primera visión general, como los objetivos y la estructura general.
- **CAPÍTULO 2:** consiste en el planteamiento del problema que se va a tratar en el proyecto, el cual será el motivo por el que se desarrollará el mismo.
- **CAPÍTULO 3:** consiste en mostrar las diferentes tecnologías que se emplearán en el desarrollo del proyecto, así como en la documentación teórica del mismo.
- **CAPÍTULO 4:** consiste en la aplicación de las tecnologías del capítulo anterior para aportar una solución final a nuestro problema, así como la arquitectura de la empresa.
- **CAPÍTULO 5:** consiste en la finalización del proyecto realizando un análisis de conclusiones.
- **CAPÍTULO 6:** consiste en un espacio reservado a futuros trabajos y ampliaciones sobre el proyecto final con la finalidad de poder mejorarlo.

Capítulo 2: Planteamiento del Problema

Actualmente nos encontramos con una empresa totalmente nueva en el sector, que nos ofrece un total de cuatro oficinas en la localidad de Madrid. Se desea diseñar una red corporativa para la empresa donde se pretende interconectar las distintas oficinas entre sí, teniendo en cuenta que una de ellas será principal y las otras tres serán sucursales de la primera.

Al comienzo de todo, la empresa no dispone de ningún dispositivo por lo que hay que partir de cero y establecer un estudio de todos los dispositivos adecuados para nuestra red. Únicamente contamos con los planos de infraestructura de las diferentes oficinas y las ubicaciones de estas, lo cual tendremos en cuenta para la instalación WAN entre ellas.

La solución que propondremos será detallada en los diferentes apartados de nuestro proyecto. De este modo, el objetivo consistirá en dar el mejor servicio posible para cubrir todas las necesidades de nuestra empresa y poder conseguir una mayor conexión entre las diferentes oficinas para poder dar servicio a los diferentes clientes que pueda tener nuestra empresa en un futuro.

Ésta será una consultora multinacional que ofrece un amplio servicio a los diferentes clientes, así como soluciones en estrategia, consultoría, digital, tecnología y operaciones.

La ubicación de las diferentes oficinas de nuestra empresa, se encuentran distribuidas por las siguientes localidades de Madrid:

- San Fernando de Henares (CPD).
- Villaverde Edificio Empresarial.
- Boadilla del Monte Edificio Empresarial.
- Plaza Castilla Edificio Empresarial.

Capítulo 3: State of Art

Una red corporativa permite conectar todas las localizaciones de la empresa de una forma permanente, privada, segura y fiable a través de una fibra óptica y mediante la tecnología MPLS que permite a la empresa cursar todas sus comunicaciones, ya sean de datos, de voz, vídeo o imágenes, de un modo rápido, seguro y gestionado por la red IP/MPLS preparada para dar “calidad de servicio”. Una red corporativa típica tiene las siguientes características:

- Muchos segmentos de LAN con una red troncal.
- Más de un protocolo de red.
- Áreas configuradas con “Abrir” la ruta de acceso más corta primero.
- Conexiones de acceso telefónico para usuarios que establezcan una conexión desde su casa o mientras viajan.
- Conexiones de línea concedida con sucursales.
- Conexiones de mercado a petición con sucursales.
- Conexiones con Internet.

La solución diseñada en el proyecto irá enfocada a las necesidades de nuestro cliente, dotando al mismo de una comunicación completa creando una red estable que optimice los tiempos de respuesta.

Por lo tanto, las áreas que se van a incluir en el diseño de una red corporativa que vamos a tratar en este proyecto son las siguientes:

- Red de Telefonía IP.
- Red de Datos.
- Seguridad.

3.1. Telefonía IP

La Telefonía IP es una tecnología que permite integrar en una misma red, basada en protocolo IP, las comunicaciones de voz y datos. En algunas ocasiones se emplean términos de redes convergentes o convergencia IP, donde se referencia a un concepto más amplio en la integración en la red de todos los elementos de comunicación ^[1].

Siempre que nos dirigimos a un sistema de Telefonía IP, nos referimos a un conjunto de elementos que debidamente integrados permiten suministrar un servicio de telefonía, basado en VoIP a la empresa. En este servicio de telefonía existen una serie de elementos básicos que forman parte de él: la centralita IP, el Gateway IP y los diferentes teléfonos IP. ^[1]

3.1.1. Concepto de VoIP

VoIP proviene del inglés Voice Over Internet Protocol que significa “voz sobre un protocolo de internet”. Consiste en un método por el cual tomando señales de audio analógicas del tipo de las que se escuchan cuando uno habla por teléfono se las transforma en datos digitales que pueden ser transmitidos a través de internet hacia una dirección IP determinada ^[2].

3.1.1.1. VENTAJAS

- **Menor coste:** una llamada mediante VoIP es mucho más barata que su equivalente en telefonía convencional, esto es debido a que se utiliza la misma red para la transmisión de datos y voz. La telefonía convencional tiene costes fijos que la telefonía IP no tiene. Una llamada entre dos teléfonos IP es gratuita, sin embargo, entre un teléfono IP y un teléfono convencional, los gastos corren a cargo del teléfono IP ^[3].
- **Portátil:** Con VoIP se pueden realizar llamadas desde cualquier punto que exista una conectividad a Internet. Esto es debido a que las transmisiones de internet se realizan a través de Internet, estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión ^[3].
- **Sin características adicionales:** VoIP viene con características que los teléfonos regulares tienen también. Si se está utilizando un teléfono regular, y se quiere actualizar a fin de que haya transferencia de llamadas, correo de voz y llamada en espera entonces se tiene que pagar cargos adicionales para su instalación. Con VoIP, estas características ya vienen con el sistema sin costo alguno ^[3].

3.1.1.2. DESVENTAJAS

- **Banda ancha:** VoIP requiere de una conexión de ancho de banda. La constante expansión que están sufriendo las conexiones de banda ancha todavía hay hogares que tienen conexiones por modem, este tipo de conectividad no es suficiente para mantener una conversación fluida con VoIP. Sin embargo, este problema se verá solucionado a la brevedad por el sostenido crecimiento de las conexiones de banda ancha ^[4].
- **Conexión eléctrica:** VoIP requiere de una conexión eléctrica. En caso de un corte eléctrico a diferencia de los teléfonos VoIP los teléfonos de la telefonía convencional siguen funcionando. Esto es así porque el cable telefónico es todo lo que un teléfono convencional necesita para funcionar ^[4].
- **Ataques:** VoIP es susceptible a virus, gusanos y hacking, a pesar de que esto es muy raro que ocurra y los desarrolladores de VoIP están trabajando en la encriptación para solucionar este tipo de problemas ^[4].

3.1.2. Protocolos

Los protocolos son los lenguajes que utilizaran los distintos dispositivos VoIP para su conexión. El objetivo principal de un protocolo de VoIP consiste en dividir en paquetes los distintos flujos de audio para poder transportarlos sobre las redes basadas en IP. Para la VoIP existen varios protocolos, de los cuales vamos a desarrollar los 4 primeros ya que son los más extendidos en la telefonía IP ^[5].

- Protocolo SIP.
- Protocolo SCCP.
- Protocolo H.323.
- Protocolo IAX.
- Protocolo Megaco (también conocido como H.248).
- Protocolo MGCP: protocolo de control. Propiedad de Cisco
- Protocolo UNISTim: Protocolo propiedad de Nortel.
- Protocolo MiNet: Protocolo propiedad Mitel.
- Protocolo CorNet: Protocolo propiedad de Siemens.
- Protocolo Skype: Protocolo peer-to-peer utilizado en la aplicación Skype.
- Protocolo Jingle: Protocolo abierto utilizado en tecnología XMPP.
- Protocolo weSIP: Protocolo con licencia gratuita de VozTelecom.

3.1.2.1. PROTOCOLO SIP

El protocolo SIP (Session Initiation Protocol) es un protocolo de control y señalización usado mayoritariamente en los sistemas de Telefonía IP, que fue desarrollado por el IETF. Dicho protocolo permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia ^[6]. Las principales funciones son:

- Localización de usuarios.
- Capacidades de usuarios.
- Disponibilidad del usuario.
- Establecimiento y mantenimiento de una sesión.

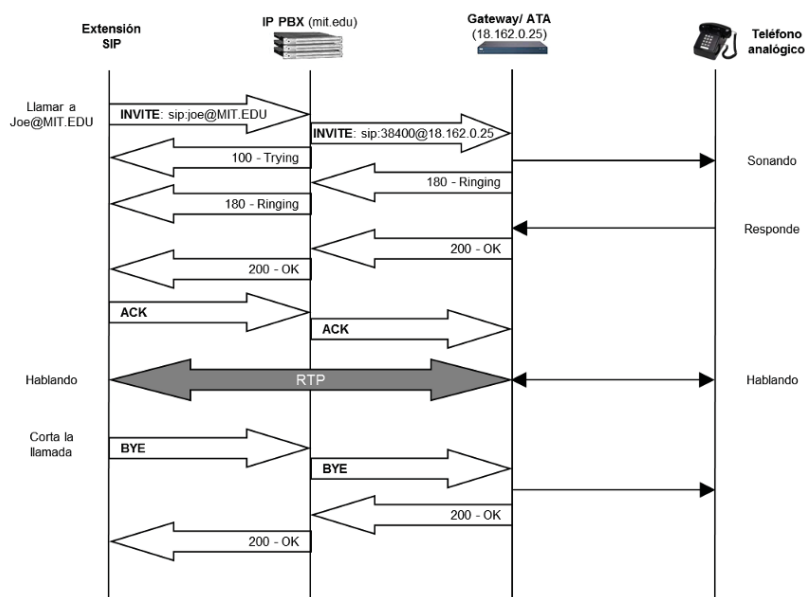


FIGURA 3.1: Llamada protocolo SIP

Según se observa en la imagen, el primer paso consiste en enviar una petición INVITE, por lo que se da por hecho que ambos usuarios han pasado la fase en la que se tienen que registrar. Por tanto, una vez lanzada dicha petición se responde con un TRYING para parar las retransmisiones y reenvían la petición al usuario. Dicho usuario envía un RINGING cuando el teléfono comienza a sonar y también es reenviado por el servidor hacia el emisor de la llamada. Por último, se recibe un OK en el momento en el que se acepta la llamada y el usuario receptor descuelga el teléfono.

3.1.2.2. PROTOCOLO SCCP

El protocolo SCCP (Skinny Client Control Protocol) es un protocolo propietario de Cisco, el cual realiza la señalización entre el Call Manager y los teléfonos IP. Un cliente skinny utiliza TCP/IP para conectarse a los Call Managers y así poder transmitir las llamadas. Para transportar el audio utiliza RTP, UDP e IP ^[7].

Cisco adquirió la tecnología SCCP cuando compró la empresa Selsius a finales de los años 1990. Como una reminiscencia del origen de los actuales teléfonos IP Cisco, el nombre por defecto de los teléfonos Cisco registrados en un Call Manager es SEP (Selsius Ethernet Phone) seguido de su MAC address ^[7].

SCCP es también usado en CSS7 (señalización de red) como complemento al conjunto de protocolos de transporte fiable MTP. Ofrece funciones adicionales a este último, ya sea a servicios orientados a conexión o no ^[7].

3.1.2.3. PROTOCOLO H.323

El protocolo H.323 es parecido al protocolo SIP, ya que es un protocolo para la configuración, administración y terminación de una sesión de comunicación. Es una recomendación del ITU-T (International Telecommunication Union), que defiende los protocolos para proveer sesiones de comunicación audiovisual sobre paquetes de red^[8].

Es un protocolo relativamente viejo y por eso ha sido reemplazado en gran medida por el protocolo SIP. Una de las ventajas de SIP es que es más sencillo y es más parecido a los protocolos HTTP y SMTP.

3.1.2.4. PROTOCOLO IAX

El protocolo IAX (Inter-Asterisk eXchange protocol) fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk, aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo. El protocolo ha quedado obsoleto, por lo que actualmente se utiliza IAX2, una nueva versión dentro del protocolo original^[9].

Es un protocolo robusto, lleno de novedades y muy simple en comparación con otros. Permite manejar una gran cantidad de códecs y un gran número de streams, lo que significa que puede ser utilizado para transportar cualquier tipo de dato. Esto hace que sea muy útil para realizar videoconferencias o realizar prestaciones remotas. En definitiva, está diseñado para darle prioridad a los paquetes de voz sobre una red IP^[9].

3.1.3. Elementos fundamentales

3.1.3.1. CÓDEC

Un Códec convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo. Esta es la esencia del VoIP, la conversión de señales entre analógico-digital^[10].

Los códecs operan usando algoritmos avanzados que les permiten tomar las muestras, ordenarlas, comprimir y empaquetar los datos. El algoritmo CS-ACELP (conjugate-structure algebraic-code-excited linear prediction) es uno de los algoritmos más comunes en VoIP. CS-ACELP ayuda a organizar el ancho de banda disponible^[10].

Entre los códecs más utilizados en VoIP encontramos:

- G.711: bit-rate de 56 o 64 Kbps.
- G.723: bit-rate de 5,3 o 6,4 Kbps.
- G.729: bit-rate de 8 o 13 Kbps.

3.1.3.2. QoS

QoS o calidad de servicio (quality of service) es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente mide la calidad de los servicios que son considerados en varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión, disponibilidad, jitter, etc ^[11].

Calidad de servicio es particularmente importante para el transporte de tráfico con requerimientos especiales. En particular, muchas tecnologías han sido desarrolladas para permitir a las redes de computadoras ser tan útiles como las redes de teléfono para conversaciones de audio, así como el soporte de nuevas aplicaciones con demanda de servicios más estrictos. ^[11]

3.1.4. Cisco Call Manager

El software Cisco Call Manager se basa en un Sistema de tratamiento de llamadas y telefonía sobre IP, el cual está desarrollado por Cisco Systems. El funcionamiento consiste en rastrear las componentes de la VoIP que se encuentra activos en la red, ya sean teléfonos, Gateways, puentes para conferencia, entre otros.

Call Manager utiliza SCCP (Skinny Client Control Protocol) como protocolo de comunicaciones para señalización de teléfonos IP. Para señalización entre gateways usa H.323, MGCP (Media Gateway Control Protocol) o SIP (Session Initiation Protocol). El Cisco Call Manager incluye las siguientes características:

- Altamente escalable ya que soporta hasta 30.000 líneas por clúster de servidor.
- Tiene capacidad para soportar un gran número de comunicaciones y aplicaciones, en ello incluimos las que se basan en el protocolo SIP.
- Altamente disponible para la continuidad del negocio, ya que soporta múltiples niveles de redundancia del servidor.
- Soporta una amplia variedad de teléfonos en función de las necesidades de los usuarios.
- Se puede elegir el Sistema operativo sobre el que irá instalado, puede ser un servidor basado en Windows o Linux.

Los dispositivos de Cisco Call Manager que forman parte de un clúster proporcionan un mecanismo para la distribución de llamadas que son procesadas a través de una red convergente que soporta la telefonía IP, redundancia y provee de funciones de transparencia y escalabilidad.

Para ello se establece una solución con dos servidores Call Manager con licencias necesarias para dar servicio a todas las extensiones del cliente. Los servidores implicados serán: Publisher, Subscriber y servidor TFTP el cual activa el Publisher.

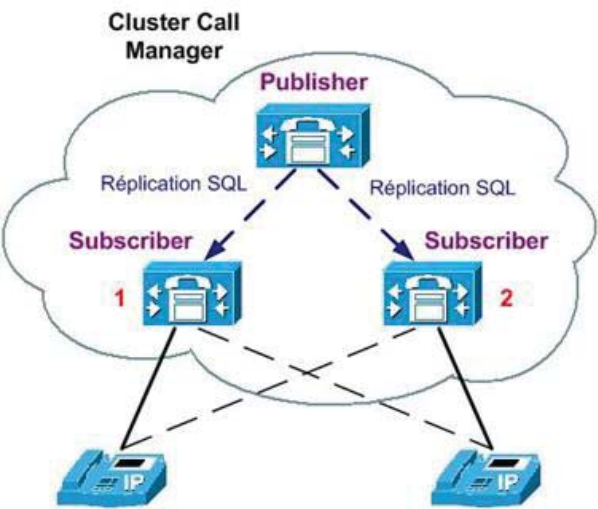


FIGURA 3.2: Clúster de un Call Manager

Según se observa en la página principal de Cisco, podemos encontrar las pautas de escalamiento de los clústeres de Cisco Call Manager para desempeñar las funciones.

Required Number of IP Phones within a Cluster	Recommended Number of Cisco CallManagers	Maximum Number of IP Phones per Cisco CallManager
2,500	Three servers total: <ul style="list-style-type: none">• Combined publisher / TFTP• One primary Cisco CallManager• One backup Cisco CallManager	2,500
5,000	Four servers total: <ul style="list-style-type: none">• Combined publisher / TFTP• Two primary Cisco CallManagers• One Backup Cisco CallManager	2,500
10,000	Eight servers total: <ul style="list-style-type: none">• Database publisher• TFTP server• Four primary Cisco CallManagers• Two backup Cisco CallManagers	2,500

TABLA 3.1: Pautas del escalamiento Clúster Cisco Call Manager

Estas recomendaciones de la tabla anterior proporcionan una solución óptima, pero es posible también reducir la cantidad de redundancia, y por lo tanto utilizar pocos servidores. Para un sistema pequeño bastaría con tener un clúster de dos servidores donde la Base de Datos y el servidor TFTP estén en el servidor Publisher y las funciones de backup se instalan sobre el otro servidor.

El número total de dispositivos que un servidor Cisco Call Manager puede controlar depende directamente del propio servidor. Para ello, la propia página de Cisco nos proporciona una tabla donde se detalla el número máximo de dispositivos en una plataforma.

Server Platform Characteristics	Maximum Device Units per Server	Maximum IP Phones per Server
MCS-7835-1000 ¹ PIII 1000MHz, 1G RAM	5000	2500
MCS-7835 PIII 733MHz, 1G RAM	5000	2500
MCS-7830 PIII 500MHz, 1G RAM	3000	1500
MCS-7830 PIII 500MHz, 512M RAM	1000	500
MCS-7825-800 ¹ PIII 800MHz, 512M RAM	1000	500
MCS-7822 PIII 550MHz, 512M RAM	1000	500
MCS-7820 PIII 500MHz, 512M RAM	1000	500

1. This server platform will not be available until first quarter of 2001.

TABLA 3.2: Número máximo de dispositivos por Plataforma

Además, cada teléfono IP que se encuentre dentro del clúster se le puede registrar como lista de prioridad de hasta tres Cisco Call Manager de tal forma que se establece una redundancia por si alguno de ellos falla, no tener una pérdida total, puesto que se activaría el siguiente en la lista de prioridades.

3.2. *Redes de Datos*

Se entiende por red de datos a una infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes, es diseñada específicamente para satisfacer los diferentes objetivos que pueda solicitar, con una arquitectura determinada para facilitar el intercambio de contenidos. ^[12]

Además, debemos considerar que una red de datos pone en funcionamiento el poder compartir el software y hardware de los dispositivos, otorgándole un soporte y centralización a la administración. ^[12]

Existen varios tipos de redes de datos en función de las necesidades, las cuales detallaremos a continuación.

- **Personal Area Network (PAN):** Es una red que interconecta computadoras situadas cerca de una persona. ^[13]
- **Local Area Network (LAN):** Es una red que favorece el intercambio de datos en una zona pequeña como un edificio o una oficina. ^[13]
- **Storage Area Network (SAN):** Es una red especial que se despliega en centros de datos y se utiliza para el funcionamiento de máquinas virtuales. ^[13]
- **Metropolitan Area Network (MAN):** Es una red de tamaño regional, cuyo objetivo es ofrecer una infraestructura entre redes de menor tamaño. ^[13]
- **Wide Area Network (WAN):** Es una red que brinda un servicio de infraestructura en un área geográfica más extensa. ^[13]

En nuestro proyecto nos centraremos en las redes LAN para las diferentes oficinas de nuestra empresa y en las redes WAN para la interconexión entre ellas.

3.2.1. Red de Área Local (LAN)

Una red de área local (LAN) es una red que conecta diferentes equipos de una compañía o de una organización. Con este tipo de red, se consigue que los empleados de la compañía sean capaces de intercambiar información, comunicarse entre sí y acceder a diversos servicios. ^[14]

Por lo general, este tipo de red se emplea para conectar equipos como impresoras o recursos a través de un medio de transmisión de cableados o dentro de un perímetro geográfico pequeño. ^[14]

Para este tipo de conexión se emplean dos medios de conexión, una red por cableado llamada conexión Ethernet, en el cual se interconectan los dispositivos entre sí mediante un dispositivo llamado router y una red inalámbrica que nos permite prescindir de cables, ya que se realiza a través de ondas de radio. ^[14]

3.2.1.1. REDES DE CABLEADO

El cableado estructurado de una red consiste en un tendido de cables localizados en el interior de un edificio con la intención de implantar la propia red de área local. Estos cables suelen ser de par trenzado de cobre con protección (STP) o sin ella (UTP) para las redes de tipo IEEE 802.3, aunque puede tratarse de fibras ópticas o cables coaxiales también. ^[15]

El objetivo fundamental de las redes de cableado es cubrir las necesidades de los usuarios durante la vida útil del edificio sin necesidad de realizar más tendido de cables.

3.2.1.1.1. Estructura del Cableado

Existen diferentes tipos de cableados en función de las necesidades adecuadas de cada uno de ellos y de la disposición que se propondrá en cada escenario de la oficina:

- **Cableado de Campus:** Se suele utilizar como cableado de interconexión entre las distintas oficinas de los diferentes edificios con los distribuidores de la zona empresarial. ^[16]
- **Cableado Vertical:** Se suele utilizar como cableado de interconexión de las distintas plantas que haya en el edificio. ^[16]
- **Cableado Horizontal:** Se suele utilizar como cableado de interconexión de los dispositivos que se encuentran en una misma planta. ^[16]
- **Cableado de Usuario:** Se suele utilizar como cableado de interconexión desde los dispositivos hasta los puestos donde se encontrarán los usuarios de la empresa.

3.2.1.1.2. Estándares del Cableado

Existen tres organismos fundamentales, los cuales se utilizarán para las normas a cumplimentar en las estructuras del cableado de la oficina. Estas son las siguientes:

- **Telecommunications Industry Association (TIA):** Desarrolla en normas de cableado industrial voluntario en los productos de las telecomunicaciones. ^[16]
- **International Standards Organization (ISO):** Es una organización no gubernamental a nivel mundial que contiene cuerpos de normas nacionales. ^[16]
- **Institute Electrical and Electronical Engineers (IEEE):** Es el responsable de los estándares de las especificaciones de las redes de área local como 802.3 Ethernet, 802.5 Token Ring, ATM y las normas de GigabitEthernet. ^[16]

Teniendo en cuenta los organismos, las normas que se tendrán en cuenta para el cableado son combinaciones de estos organismos. Las cuales vamos a destacar son:

- | | |
|--------------------|--------------------|
| • ANSI/TIA/EIA-568 | • ANSI/TIA/EIA-606 |
| • ANSI/TIA/EIA-569 | • ANSI/TIA/EIA-607 |
| • ANSI/TIA/EIA-570 | • ANSI/TIA/EIA-758 |

3.2.1.1.3. Tipos de Cables

Las principales diferencias de rendimiento entre los distintos tipos de cables radican en la anchura de banda permitida (y consecuentemente en el rendimiento máximo de transmisión), su grado de inmunidad frente a interferencias electromagnéticas y la relación entre la pérdida de la señal y la distancia recorrida (atenuación). En la actualidad existen básicamente tres tipos de cables factibles de ser utilizados para el cableado en el interior de edificios o entre edificios:

- Coaxial (No se recomienda para instalaciones nuevas, excepto redes de TV).
- Par Trenzado.
- Fibra Óptica.

Cable coaxial

El cable coaxial está formado por un núcleo de cobre que se encuentra rodeado por un material aislante, el cual, a su vez, está cubierto por una pantalla de material conductor, que según el tipo de cable o calidad está formada por una o dos mallas de cobre, un papel de aluminio o ambos. ^[17]

El apantallamiento del material se encarga de la protección de los datos transmitidos absorbiendo las señales electrónicas espurias, es decir, el ruido. La lámina aislante y una de las capas del apantallamiento de metal se conoce como el apantallamiento doble. ^[17]

El núcleo de cobre del cable coaxial, conocido por vivo, se encarga de transportar las señales electrónicas que forman los datos. Puede ser sólido y, por tanto, suele ser de cobre, o de hilos. La capa aislante que lo rodea se denomina dieléctrica que se encarga de separar la malla del hilo. ^[17]

Antiguamente, el cable coaxial era no de los más utilizados debido a que tenía dos características que fomentaban su utilización: ^[17]

- Era barato.
- Era ligero, flexible y sencillo de manejar.

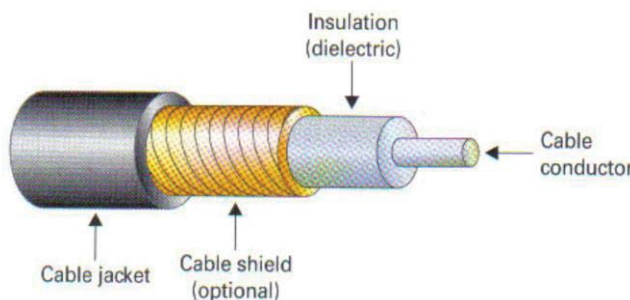


FIGURA 3.3: Cable coaxial

Existen dos tipos de cables coaxiales aplicados para las redes:

- **Grueso (Coaxial amarillo de 50 Ω).** Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Utilizado en la norma Ethernet 10Base-5.
- **Fino (Coaxial RG58 de 50 Ω).** con terminaciones BNC. Es más barato y fino y, por tanto, solventa algunas de las desventajas del cable grueso; aunque obtiene peores rendimientos que el cable amarillo. Utilizado en la norma Ethernet 10Base-2.



FIGURA 3.4: Cable coaxial fino y grueso

Para los cables coaxiales existen varios tipos de conectores en función de las necesidades de conectividad de cada uno de ellos.

Cable Par Trenzado

Es actualmente el tipo de cable más común en redes de área local (LAN) y se originó como solución para conectar redes de comunicaciones reutilizando el cableado existente de redes telefónicas.^[17]

Este cable necesita unos conectores y otro hardware para asegurar su correcta instalación. Los elementos de la conexión son los siguientes:

- **Conector RJ-45** contiene ocho conexiones de cables.
- **Conector RJ-11** contiene cuatro conexiones de cables.

El cable de Par trenzado se utiliza si la LAN pudiera tener una limitación de presupuesto y si se desea una instalación que pueda ser sencilla. Por el contrario, no se debería utilizar si se requiere una LAN con un gran nivel de seguridad y si los datos se deben transmitir a largas distancias y a altas velocidades.^[17]

Existen dos tipos de cables:

- **Par trenzado no apantallado (UTP):**



FIGURA 3.5: Cable UTP

- **Par trenzado apantallado (STP):**

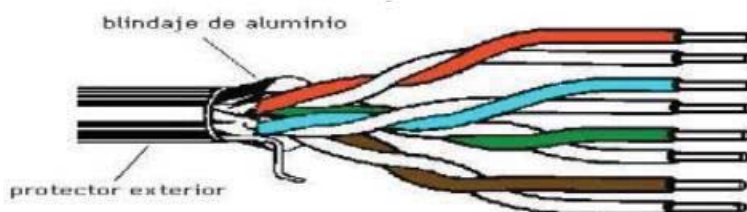


FIGURA 3.6: Cable STP

Y si clasificamos por categorías, podemos encontrar varios tipos de cables.

Categoría	Frecuencia Máxima	Tipo de cable	Conectores	Usos (Mbps)
Categoría 3	16MHz	UTP	RJ-11 / RJ-45	Voz analógica
Categoría 4	20MHz	UTP	RJ-45	Token Ring (16)
Categoría 5,5e	100MHz	UTP/STP	RJ-45 / RJ-49	Eth (100/1.000)
Categoría 6	250MHz	UTP/STP	RJ-45 / RJ-49	Eth (1000)
Categoría 6a	500MHz	UTP/STP	RJ-45 / RJ-49	Eth (10.000)
Categoría 7	600MHz	STP	GG-45 (RJ-45)	Eth (10.000)

TABLA 3.3: Clasificación de cables por Categorías

Fibra Óptica

Consiste en un cable con dos conjuntos de hilos de vidrios en envolturas separadas, ya que cada uno de ellos permiten el paso de las señales en una única dirección, por tanto, uno transmite y el otro recibe. Estos cables se encierran en un revestimiento de plástico para obtener una protección adecuada al cable. ^[17]

Estos cables no están sujetos a intermodulaciones eléctricas, por lo que son extremadamente rápidos, llegando a transmitir velocidades de 1GBps, aunque normalmente lo hacen a unos 100Mbps, por distancias de varios kilómetros. ^[17]

Los usos de este cable suelen ser para transmitir datos a velocidades muy altas y a grandes distancias en medios seguros. Por el contrario, el presupuesto es limitado y no tiene el conocimiento para interconectar varios dispositivos de forma apropiada. ^[17]



FIGURA 3.7: Cable de Fibra Óptica

3.2.1.1.4. Arquitectura Cableado

Existen dos tipos de arquitectura en función de la distribución que se quiera disponer en la conectividad y en función de la electrónica.

- **Arquitectura de red Centralizada:**

Consiste en dejar pasar la información desde un único punto, es decir, todo el sistema se concentra en un punto desde el que se transmite la información al resto de puntos requeridos. ^[18]

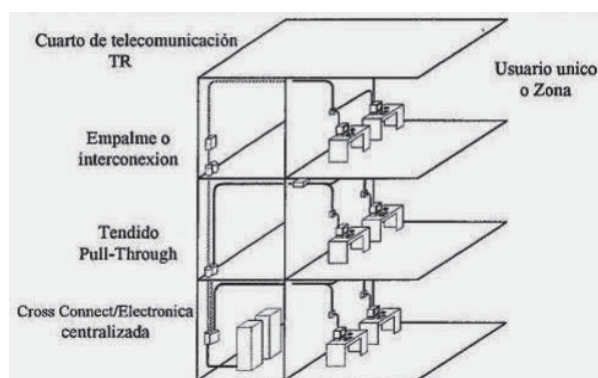


FIGURA 3.8: Arquitectura de red Centralizada

- **Arquitectura de red Distribuida:**

Consiste en tener una estructura de nodos donde la información se transmite tipo árbol, es decir, desde cada planta del edificio. Existe un centro donde se emite la información y pasa por unos nodos intermedios, los cuales distribuyen la información, o no, a los receptores finales. ^[18]

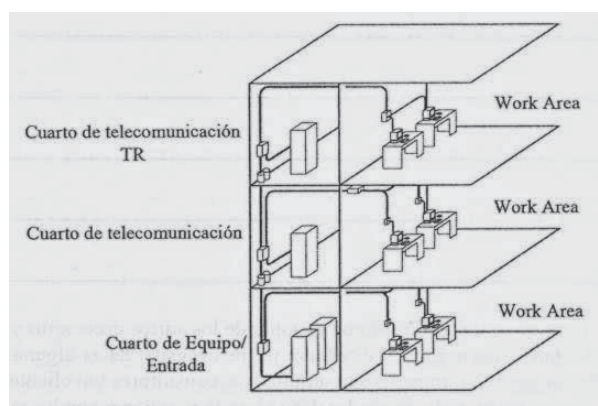


FIGURA 3.9: Arquitectura de red Distribuida

Elementos Principales

Para el cableado estructurado se necesitan una serie de elementos que deben estar en toda instalación de cualquier arquitectura.

- **Cableado Horizontal:** Es aquel que se extiende desde la salida del puesto de trabajo del usuario final hasta el cuarto de telecomunicaciones. ^[19]
- **Cableado Backbone o vertical:** Es aquel que proporciona varias interconexiones entre los cuartos de entrada y los servicios del edificio, cuartos de equipos y de telecomunicaciones. Además, incluye la conexión vertical entre los distintos pisos del edificio. ^[20]
- **Cuarto de Telecomunicaciones:** Es una habitación utilizada exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones. ^[21]
- **Cuarto de Equipos:** Es un espacio centralizado para los equipos de telecomunicaciones que sirven a los ocupantes del edificio. Sólo sirve para guardar los equipos relacionados con los sistemas de telecomunicaciones. ^[22]
- **Cuarto de Entrada de Servicios:** Consiste en una entrada de servicios de telecomunicaciones al edificio, la cual tiene un punto de entrada en la pared del edificio y continua hasta el cuarto del área de entrada ^[23].
- **Sistema de Puesta a Tierra y Puenteado:** Es un componente importante en cualquier sistema de cableado estructurado moderno. Se deberá de disponer de una toma de tierra conectada a la tierra general de la instalación eléctrica para poder efectuar las conexiones de todo equipamiento. ^[20]

3.2.1.2. REDES INALÁMBRICAS

El término de la tecnología inalámbrica se refiere al uso de la propia tecnología sin cables, la cual permite la conexión entre varios equipos entre sí ^[24].

De este modo, este tipo de tecnología se ha ido convirtiendo en el foco de estudio para los temas de transmisión de datos, adquiriendo mayor interés en lugares donde, por ciertas circunstancias, no es posible la instalación de cables o redes alámbricas ^[24].

El uso de esta tecnología inalámbrica permite dejar en el olvido los cables sin la necesidad de dejar de establecer una conexión, desapareciendo las limitaciones de espacio y tiempo, dando la impresión de que puede ubicarse una oficina en cualquier lugar del mundo ^[24].

Las redes inalámbricas son de carácter libre, están diseñadas para operar en bandas de frecuencia para las que no se necesita licencia de uso. Éste es el caso de la banda de 2.4 GHz y de 5GHz. Esto ha favorecido enormemente la implantación de la tecnología inalámbrica, ya que da lugar a unos costos de uso mucho menores que las redes basadas en sistemas celulares. Además, permiten crear redes en áreas complicadas donde se pueden conectar gran cantidad de dispositivos, en lugares donde resulta dificultoso o muy cara la conexión de cables.

3.2.1.2.1. Tipos de Redes Inalámbricas

- **Las redes inalámbricas de área global o WWAN (Wireless Wide Area Network):** La revolución más grande de la comunicación sin cables se inició con los teléfonos móviles, los cuales han sido el producto electrónico con mayor éxito de todos los tiempos. Se trata de un sistema para mantener la comunicación independientemente del lugar donde nos encontremos. Las tecnologías WWAN se conocen también como sistemas de segunda generación (2G), de tercera generación (3G) o los actuales sistemas (4G) ^[24].
- **Las redes inalámbricas de área local o WLAN (Wireless Local Area Network):** Proporciona más libertad en el ambiente de trabajo. A través de una red sin cables los trabajadores pueden acceder a la información desde cualquier lugar de la compañía, no están limitados a puntos de acceso a través de cables fijos para acceder a la red. Estas redes están pensadas para crear un entorno de red local entre ordenadores o terminales situados en un mismo edificio o grupo de edificios ^[24].
- **Las redes inalámbricas de área personal o WPAN (Wireless Personal Area Network):** Existe dentro de un área relativamente pequeña, que conecta dispositivos electrónicos con ordenadores, impresoras, escáner, aparatos de fax, PDA's y ordenadores notebook, sin la necesidad de cables ni conectores para que sea efectivo el flujo de información. La finalidad de estas redes es la comunicación entre cualquier dispositivo personal ^[24].

En nuestro caso, nos vamos a centrar en la tecnología inalámbrica WLAN, para la conexión de los edificios.

3.2.1.2.2. Estándares IEEE

Dentro de la tecnología para los sistemas de red existe el estándar 802 llevado a cabo por el Institute of Electrical and Electronic Engineers (IEEE), donde el modelo 802.11 se relaciona con las tecnologías inalámbricas mientras que el modelo 802.3 se corresponde a las tecnologías alámbricas. Dentro del modelo 802.11 existen varios tipos en función de la tecnología inalámbrica que se obtenga, en nuestro caso, emplearemos el modelo 802.11b ^[25].

Estándar	Velocidad máxima	Frecuencia	Compatible con modelos anteriores
802.11a	54Mb/s	5 GHz	No
802.11b	11 Mb/s	2,4 GHz	No
802.11g	54Mb/s	2,4 GHz	802.11b
802.11n	600 Mb/s	2,4GHz o 5GHz	802.11a/b/g
802.11ac	1,3 Gb/s (1300 Mb/s)	2,4GHz y 5GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2,4GHz, 5GHz y 60 GHz	802.11a/b/g/n/ac

TABLA 3.4: Estándares IEEE 802.11

3.2.1.2.3. Arquitectura de las redes WiFi

Para poder montar una tecnología inalámbrica y, por tanto, una arquitectura WiFi, se necesitan una serie de componentes que son partícipes en todo el diseño. Cada uno de ellos tiene su propio cometido, de tal forma que la unión de todos establece la conexión de manera exitosa, siempre y cuando se haya diseñado y montado correctamente.

Punto de Acceso

Consiste en un dispositivo WLAN que puede actuar como punto central de una red inalámbrica autónoma. A su vez, se puede utilizar también como un punto de conexión entre una red inalámbrica y otra cableada ^[26].

Un uso típico corporativo involucra unir varios puntos de acceso a una red cableada y luego brindar acceso inalámbrico a la LAN de la oficina. Los puntos de acceso inalámbricos son gestionados por un controlador de WLAN que se ocupa de los ajustes automáticos a la potencia de RF, los canales, la autenticación y seguridad ^[27].



FIGURA 3.10: Punto de Acceso

Controladores

Estos dispositivos están diseñados para poder conectar dos o más redes que se encuentren ubicadas en distintos edificios ^[27].

Los controladores tienen una gran importancia en las redes WIFI, ya que, son los responsables de facilitar la gestión de la red inalámbrica y el acceso de los usuarios a ella. Mediante su funcionalidad y la de los puntos de acceso, la cobertura completa está garantizada ^[28].

Sin embargo, hay factores negativos, como la pérdida de eficiencia en las conexiones. La razón es que normalmente tienen un punto único por el que se conectan todos los dispositivos y, por tanto, es por donde pasa toda la información ^[28].



FIGURA 3.11: Controladora WiFi

Herramienta AirWave

“Aruba AirWave es un sistema de operaciones de redes, poderoso y sencillo de utilizar, que no tan sólo administra infraestructura alámbrica e inalámbrica de Aruba y de una amplia gama de otros fabricantes, sino que también proporciona visibilidad granular de dispositivos, usuarios y aplicaciones en la red” [29].

Airwave utiliza el protocolo estándar SNMP para comunicarse con las redes de acceso, por tanto, es capaz de gestionar no sólo redes Aruba, sino también de otros fabricantes, tanto LAN como WLAN. Esta característica lo hace idóneo para poder ser utilizado como consola única de la red de acceso.

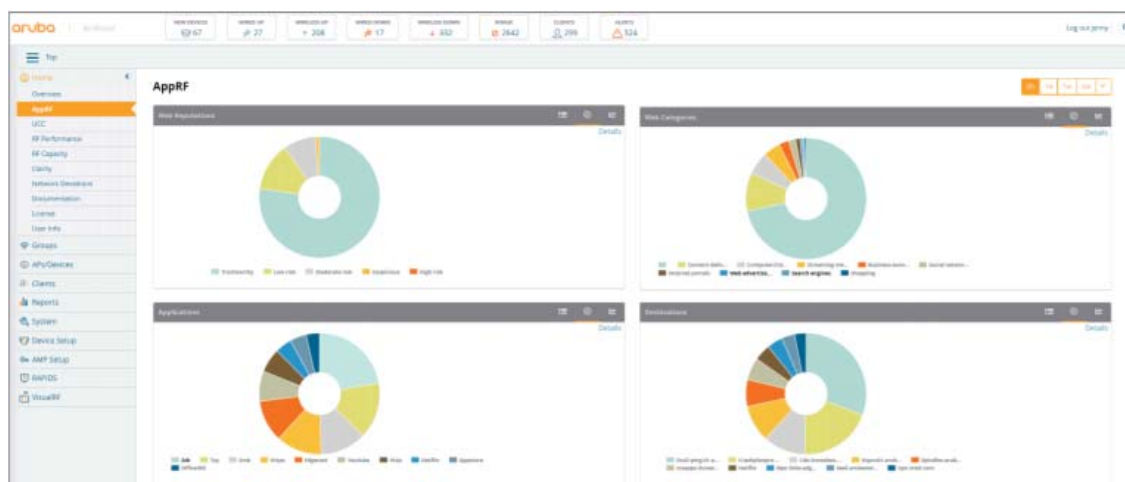


FIGURA 3.12: Herramienta AirWave

3.2.2. Red de Área Extensa (WAN)

Una red de Área Extensa consiste en redes de comunicaciones que conectan varios equipos destinados a la ejecución de programas de usuarios en áreas de cientos o incluso miles de kilómetros de distancias desde el origen al destino. Lo normal es que los dispositivos hosts, se conecten a esta red WAN a través de una red LAN, pero también puede haber ciertos terminales que estén conectados directamente al router sin la necesidad de que estén integrados en la propia red WAN [30].

La red consiste en computadores de conmutación (ECD) que están conectados entre sí alquilando los canales de alta velocidad. Cada uno de ellos emplea protocolos responsables de encaminar los datos correctamente y proporcionar los datos a los terminales finales (ETD) [30].

Para estos ETDs, el ETC es el dispositivo encargado de aislar la red con el objetivo de que cada uno de los hosts que pertenezcan a una red concreta, solo puedan disponer de esa red hasta llegar al router, el cual se encarga de distribuir el tráfico entre el resto de las redes hasta llegar a la red requerida [30].

3.2.2.1. TIPOS DE REDES WAN

En función del tipo de red que se quiera implantar en la infraestructura, existen varios tipos de redes:

- **Conmutadas por Circuitos:** Son redes que, para establecer la comunicación, se debe efectuar una llamada y cuando se establece la conexión, los usuarios obtienen un enlace directo desde los diferentes segmentos que hay en la red ^[30].
- **Conmutadas por mensaje:** Son redes que, tienen conmutadores que suelen ser ordenadores que cumplen la tarea de aceptar el tráfico de cada uno de los terminales conectados a ellas ^[30].
- **Conmutados por paquetes:** Son redes que, los datos de los distintos usuarios están divididos en paquetes. Estos paquetes están insertados dentro de informaciones del protocolo y recorren la red como si fueran entidades diferenciadas e independientes ^[30].
- **Redes Orientadas a Conexión:** Son redes que, existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios ^[30].
- **Redes no orientadas a conexión:** Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace ^[30].
- **Red Pública de Conmutación Telefónica (PSTN):** Son redes que, fueron diseñadas originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino ^[30].

3.2.2.2. RED PRIVADA VIRTUAL (VPN)

Es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos. En realidad, una red VPN consiste en la unión WAN entre varios sitios, pero al usuario le aparece como una conexión privada ^[31].

Para poder establecer una conexión de red VPN, es necesario que el usuario se encuentre identificado, que los datos que se vayan a transmitir estén correctamente cifrados con los algoritmos adecuados y que los usuarios mantengan actualizadas sus claves ^[31].

3.2.2.2.1. Tipos de redes VPN

Existen cuatro tipos de conexiones VPN.

VPN de acceso remoto

Se considera el modelo más utilizado por los usuarios y consiste en que los usuarios se conectan a las redes de las empresas o de recintos privados desde lugares remotos utilizando Internet como vínculo de acceso ^[31].

VPN punto a punto

Este tipo de conexión consiste en conectar oficinas remotas con sede central de la organización. El propio servidor dispone de un vínculo permanente hacia Internet, acepta las conexiones y establece el túnel. Gracias a que los servidores se conectan a Internet usando su propio servicio local, pueden eliminar los vínculos punto a punto tradicionales, sobre todo en conexiones internacionales ^[31].

Tunneling

Esta técnica de red privada consiste en encapsular un protocolo de red sobre otro para crear un túnel dentro de una red de equipos. Este túnel se establece incluyendo una PDU dentro de otra PDU con el objetivo de transmitirla desde un extremo sin que sea necesaria la interpretación intermedia de la PDU encapsulada. De este modo, el túnel queda definido por los puntos extremos y el protocolo de comunicación del usuario. El uso de esta técnica tiene diferentes objetivos dependiendo del problema tratado ^[31].

VPN sobre LAN

Consiste en una variante del acceso remoto, por lo que las empresas lo utilizan bastante. La diferencia es que, en vez de emplear Internet, emplea la misma red de área local de la empresa como modo de conexión. Sirve para poder aislar zonas y servicios dentro de la red local ^[31].

Capítulo 4: Solución Propuesta

4.1. Requisitos Iniciales

La empresa recibirá el nombre de Foreign System Services (FSS) y es una consultora multinacional encargada de las diferentes funciones indicadas, por lo que hay que establecer un servicio donde se cubran todas las de la empresa.

Consta de cuatro oficinas en la localidad de Madrid distribuidas por la provincia a las cuales nos referiremos con el nombre de Castilla, Villaverde, Boadilla y Henares. En esta última ubicaremos el CPD principal. Estas oficinas se van a clasificar en S1 la cual se nombrará al CPD, S2 en la que incluiremos la de Castilla y S3 donde se agrupará Villaverde y Boadilla. Esta agrupación viene dada por capacidad total de la oficina correspondiente.

4.1.1. Número de Usuarios

Para poder definir la red que se va a utilizar, debemos tener en cuenta en el número total de usuarios y de empleados que van a trabajar en las diferentes oficinas, así como los puestos asignados a cada uno de ellos. Para determinar los permisos y las necesidades de cada uno, voy a agrupar a los usuarios en diferentes perfiles y cada uno de ellos dispondrá de sus propias necesidades. Los perfiles serán:

- **Usuario de planta:** Este usuario va a tener una ubicación fija dentro de la oficina, por lo que realizará continuos usos de los servicios de ésta. Debido a su localización, únicamente dispondrán de un terminal fijo de gama media para realizar llamadas internas sin necesidad de un terminal móvil. Para poder realizar su trabajo dispondrán de un ordenador portátil por si tuviera que realizar alguna intervención fuera de su puesto de trabajo, aunque no suelen desempeñar estas funciones. Dentro de este perfil incluiremos a todos los empleados de distintos departamentos, así como los de soporte técnico.
- **Usuario móvil:** Este usuario se va a desplazar continuamente por motivo de trabajo ya que tendrán un contacto directo con los distintos clientes de la entidad por lo que realizarán numerosos viajes para realizar reuniones, meetings, etc. Debido a ello, necesitarán un terminal móvil que puedan tener en su poder todo el tiempo para que estén localizables en todo momento. Para realizar su trabajo necesitan un ordenador portátil que puedan llevar consigo a todos los lugares que su trabajo lo requiera. Dentro de este perfil incluiremos a todos los empleados de soporte de servicios con desplazamiento a clientes y a los consultores de la empresa.
- **Usuario directivo:** Este usuario va a tener, por lo general, una ubicación fija, lo cual no implica que tenga que realizar algún desplazamiento por algún motivo en concreto. Debido a ello, necesitarán un terminal fijo de gama media-alta, así como un terminal móvil que pueda llevar consigo en esos viajes puntuales. Para realizar su trabajo necesitarán un portátil por lo mismo que los anteriores perfiles. Dentro de este perfil incluiremos a todos los supervisores, managers y directivos de los distintos departamentos de la empresa.

- **Usuario de planta especializado:** Este usuario realiza las mismas funciones de un usuario de planta, sin embargo, poseen un cargo especializado en telefonía, por lo que incluiremos a las secretarías y operadoras. Debido a ello necesitarán un terminal fijo de gama alta, así como un portátil como los usuarios de planta.

4.1.2. Servicios

Las diferentes oficinas de nuestra empresa contarán con varios servicios que los cuales serán necesarios para el funcionamiento de la empresa, aunque los usuarios solo podrán utilizar los servicios acordes al perfil que pertenezcan. Se detallarán a continuación, los diferentes servicios con los que contaremos para el diseño de la red.

4.1.2.1. SERVICIO DE COMUNICACIONES DE VOZ

Incluye el conjunto completo de servicios habilitados por VoIP, como la interconexión de teléfonos para comunicaciones; servicios relacionados como facturación y planes de marcación; y funciones básicas que pueden incluir conferencias, transferencia de llamadas, reenvío de llamadas y llamada en espera.

4.1.2.2. SERVICIO DE COMUNICACIONES DE DATOS

Este grupo hace referencia a los servicios que necesitan los usuarios de la empresa disponibles a través de la red de datos. Distinguimos tres tipos de acceso diferentes utilizados por los usuarios:

- **Acceso Internet:** Navegación a través de cualquier Web que necesite el usuario para su trabajo.
- **Acceso interno Intranet:** Navegación a través de las páginas corporativas de la empresa o cualquier herramienta interna propia de la empresa desde cualquier sede y de forma segura, para lo que se conectan las distintas sedes a través de la red de datos privada virtual constituida sobre infraestructura de un operador de telecomunicaciones.
- **Acceso remoto:** Conexión a la red de datos de la empresa desde cualquier ubicación que esté fuera de cualquiera de las sedes. Los usuarios con teletrabajo utilizan este acceso para trabajar con las herramientas de la empresa como si estuvieran en la propia sede.

4.1.2.3. SERVICIOS DE COMUNICACIONES UNIFICADAS (UC)

Se entiende por Comunicaciones Unificadas a la integración de los diferentes medios de comunicación que posee una organización. Esto es; voz, mensajería de texto y video tanto en tiempo real como diferido. El objetivo es canalizar las comunicaciones de acuerdo con la disponibilidad y preferencias de los usuarios, dando independencia en medios y terminales. Dentro de este tipo de servicio encontramos:

- Mensajería instantánea (IM) y Gestión de Presencia.
- Compartición de escritorio.
- Video Conferencias.
- Mensajería Unificada.

Los servicios asignados a los diferentes perfiles son los siguientes:

SERVICIOS	PLANTA	MÓVIL	DIRECTIVO	ESPECIALIZADO
Gama Media	SÍ	NO	NO	NO
Gama Media-Alta	NO	NO	SÍ	NO
Gama Alta	NO	NO	NO	SÍ
Teléfono móvil	NO	SÍ	SÍ	NO
Ordenador Portátil	SÍ	SÍ	SÍ	SÍ

TABLA 4.1: Servicios de los usuarios

4.1.3. Calidad de Servicio. QoS

Es importante para la empresa tener en cuenta la necesidad que tiene la red en dar un servicio óptimo a nuestros usuarios. Para ello, es necesario incluir el concepto de Calidad de Servicio, el cual hace referencia a las diversas tecnologías que garantizan una cierta calidad para los distintos servicios de red. Podemos distinguir dos tipos de tráfico:

4.1.3.1. TRÁFICO ELÁSTICO

Este tipo de tráfico soportado por redes basadas en TCP/IP. Los routers gestionan a ciegas los paquetes IP entrantes, sin importarles el tipo de aplicaciones ni si un paquete forma parte de una transferencia grande o pequeña. ^[32]

- Transferencia de archivos.
- Correo electrónico.
- Conexión remota.
- Gestión de Red.
- Acceso Web.

4.1.3.2. TRÁFICO INELÁSTICO

No se adapta fácilmente a variaciones de retardo y rendimiento de una red, necesitando algún mecanismo para otorgar un tratamiento preferente a las aplicaciones que tengan los requisitos de mayor exigencia. ^[32]

Las aplicaciones no elásticas, normalmente no reducen su demanda para enfrentarse a la congestión. En momentos de congestión el tráfico no elástico seguirá proporcionando alta carga y el elástico será expulsado. ^[32]

Se considera tráfico no elástico el cursado en tiempo real como voz y datos (Aplicaciones Multimedia). ^[32]

En conclusión, al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. ^[32]

QoS promete un uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red, priorizándolo según su importancia, y utilizando métodos de control y evasión de congestión para darles un tratamiento preferencial. ^[32]

Implementando QoS en una red, hace al rendimiento de la red más predecible, y a la utilización de ancho de banda más eficiente. ^[32]

4.1.4. Oficinas de la empresa

En la tabla de a continuación, se detallarán los distintos usuarios de nuestra empresa repartidos por las diferentes oficinas para saber la cantidad total de puestos en cada una de ellas, así como las diferentes plantas con las que contamos en las oficinas.

OFICINA	USUARIOS	PLANTAS
Castilla	400	2
Villaverde	500	3
Boadilla	500	3
Henares (CPD)	5	1

TABLA 4.2: Número de Usuarios de la empresa

4.1.4.1. HENARES (CPD)

La oficina está localizada en San Fernando de Henares en la provincia de Madrid y consiste en el Centro de Procesamiento de Datos principal de nuestra empresa. En él podemos encontrar una gran sala o nave la cual estará adaptada para poder integrar el mayor número posible de dispositivos electrónicos que darán servicio al resto de oficinas.

Será el principal punto generador de tráfico de la red, sobre todo en sentido CPD-oficinas remotas, al hacer uso los usuarios empresariales cada vez más de aplicaciones en la nube, distribuidas, que se albergan en este centro por lo que tendrá que tenerse en cuenta a la hora de dimensionar sus necesidades de comunicaciones en el diseño, así como la redundancia de estas debido a su criticidad.

Las funciones principales del CPD son garantizar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, así como servidores de bases de datos que puedan contener información crítica. Además, hay que incluir las siguientes funciones para los puestos de trabajo del CPD.

- Gestión y administración del propio CPD.
- Soporte a los usuarios de la empresa.
- Desarrollo de los sistemas informáticos empleados en la empresa.
- Servicio a clientes.

La sala donde se instalarán los equipos debe estar accesible en todo momento para que se pueda solventar cualquier problema en todo momento. A su vez los diferentes equipos estarán protegidos en cabinas de racks para que no se puedan manipular con facilidad, ya que puede tener una gran repercusión en la vulnerabilidad del sistema. El acceso a la sala deberá tener un sistema de seguridad con tarjetas de banda magnética por seguridad de la sala. Los requisitos con los que contaremos serán los siguientes:

- Aire acondicionado para el refrigerio de la sala.
- Doble contratación de sistema eléctrico con dos compañías diferentes.
- Redundancia en los cables que conectarán con el exterior.
- Montacargas adecuado para las máquinas introducidas en el CPD.
- Seguridad a nivel de vigilancia y nivel de averías o incendios.
- Controles de temperatura y humedad.
- Falsos suelos y techos.
- UPS y generadores de corriente eléctrico.

4.1.4.2. RESTO DE OFICINAS

En el proyecto realizaremos el diseño de una de las tres oficinas restantes y las demás tendrán una estructura similar a ella. A continuación, se detallará un plano de infraestructura de las plantas de esa oficina. La oficina establecida es Boadilla, por tanto, dicha oficina tiene 3 plantas, tal y como se indicó en la tabla 4.2.

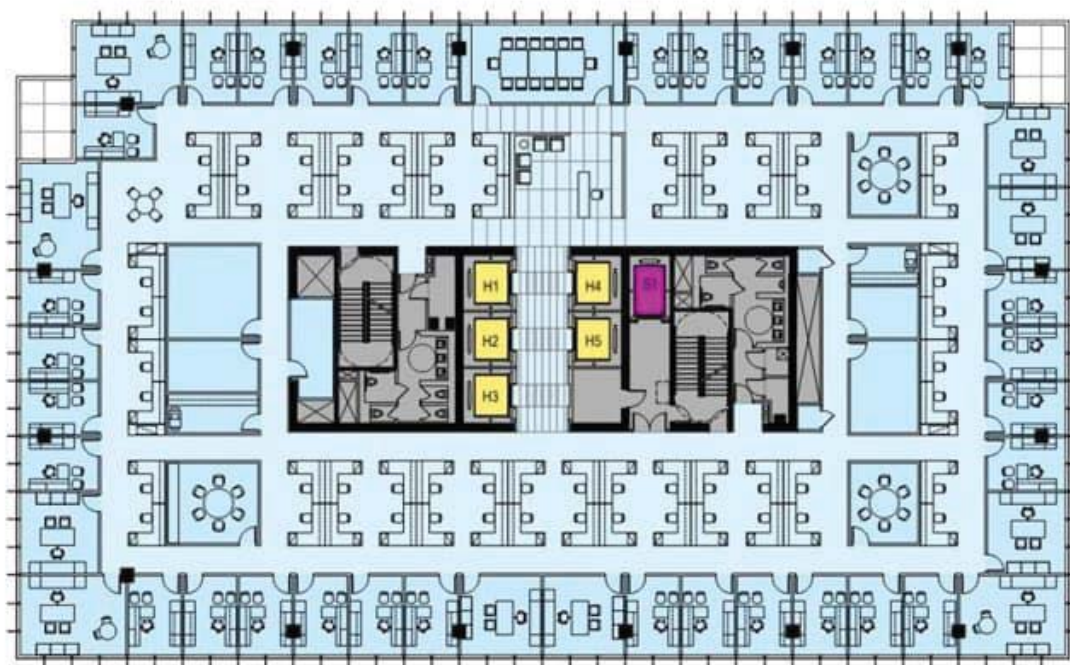


FIGURA 4.1: Oficina Boadilla

4.2. Diseño de la Red

4.2.1. Diseño de la Red de Voz

Después de revisar todos los requisitos necesarios y del número de empleados por oficina, vamos a establecer la arquitectura sobre la red de voz de nuestra empresa.

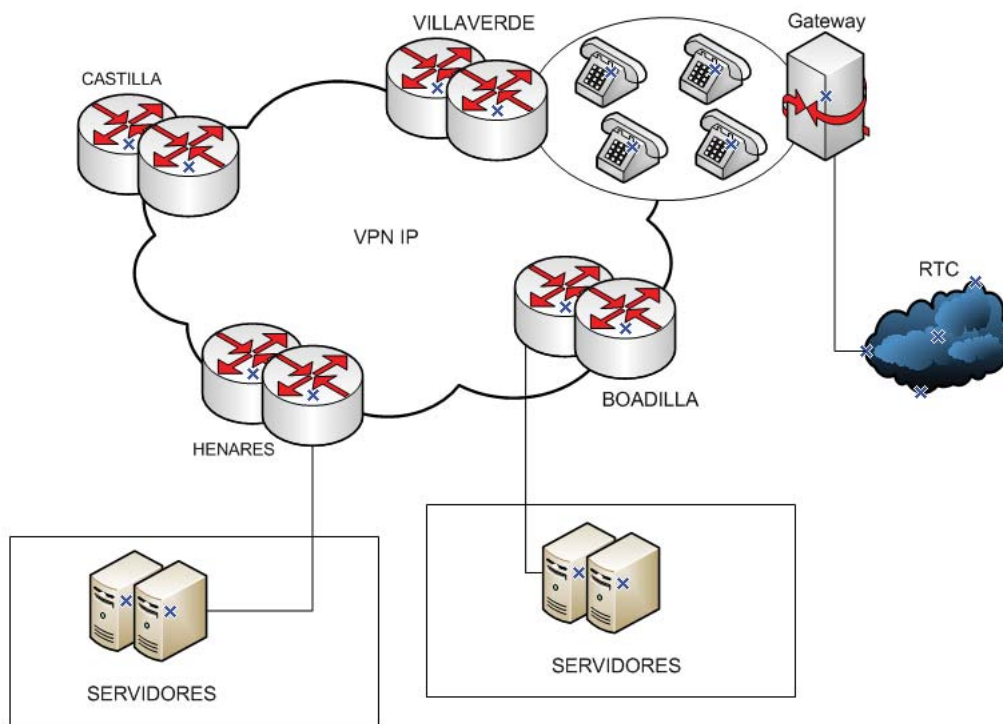


FIGURA 4.2: Arquitectura de Voz

Tal y como se puede ver en el diagrama, cada oficina compondrá de dos routers en el que incluiremos un Gateway de voz por si los dos se caen, poder tener redundancia de voz por éste. El Gateway irá conectado a la RTC que es la red del operador contratado.

Para la comunicación por voz se establecerán dos servidores físicos donde se virtualizarán las componentes necesarias para la VoIP que son; Publisher, Subscriber, UCCX, Unity, servidor TFTP e Hipervisor. Un servidor se encuentra en la oficina de Boadilla y el otro en el CPD de Henares. Este servidor estará redundado también

Además, en cada sede dispondremos de terminales IPs de diferentes gamas para que los distintos perfiles de usuarios puedan comunicarse tanto con usuarios de la empresa como con personas externas.

4.2.1.1. ELEMENTOS PARA LA RED DE VOZ

4.2.1.1.1. Servidores UC

En nuestro caso, debido al número de usuarios a atender, las máquinas virtuales a desplegar para proporcionar servicios y la necesidad de recursos estimada de los servidores, hemos optado por el modelo C240 M3 TRC perteneciente a la familia BE7000 que como se puede ver en las especificaciones de la página de Cisco se compone de 2 CPUs de 6 Cores de 300GB cada uno.

Item	Specification
Chassis	Two rack-unit (2RU) server
Processors	Either 1 or 2 Intel® Xeon® processor E5-2600 v3 or v4 product family CPUs
Chipset	Intel C610 series
Memory	Up to 24 double-data-rate 4 (DDR4) dual in-line memory (DIMMs) of up to 2400 MHz speeds
PCIe slots	Up to 6 PCI Express (PCIe) Generation 3 slots (four full-height and full-length; four NCSI-capable and VIC-ready; two GPU-ready)
Hard drives	Up to 24 small-form factor (SFF) drives or 12 large form-factor (LFF) drives, plus two optional internal SATA boot drives, and NVMe drive support
Embedded NIC	Two 1-Gbps Intel i350-based Gigabit Ethernet ports
mLOM	mLOM slot can flexibly accommodate 1-Gbps, 10-Gbps, or 40-Gbps adapters
RAID controller	Cisco 12 Gb SAS modular RAID controller for internal drives Cisco 9300-8E 12 Gb SAS HBA for external drives Embedded software RAID (entry RAID solution) for up to four SATA drives

TABLA 4.3: Especificaciones del Servidor

Debido a lo explicado anteriormente, se distribuirán las componentes virtualizadas dentro del servidor del modo que se indicará en la figura 4.5 de las dos oficinas que incluirán estos servidores.

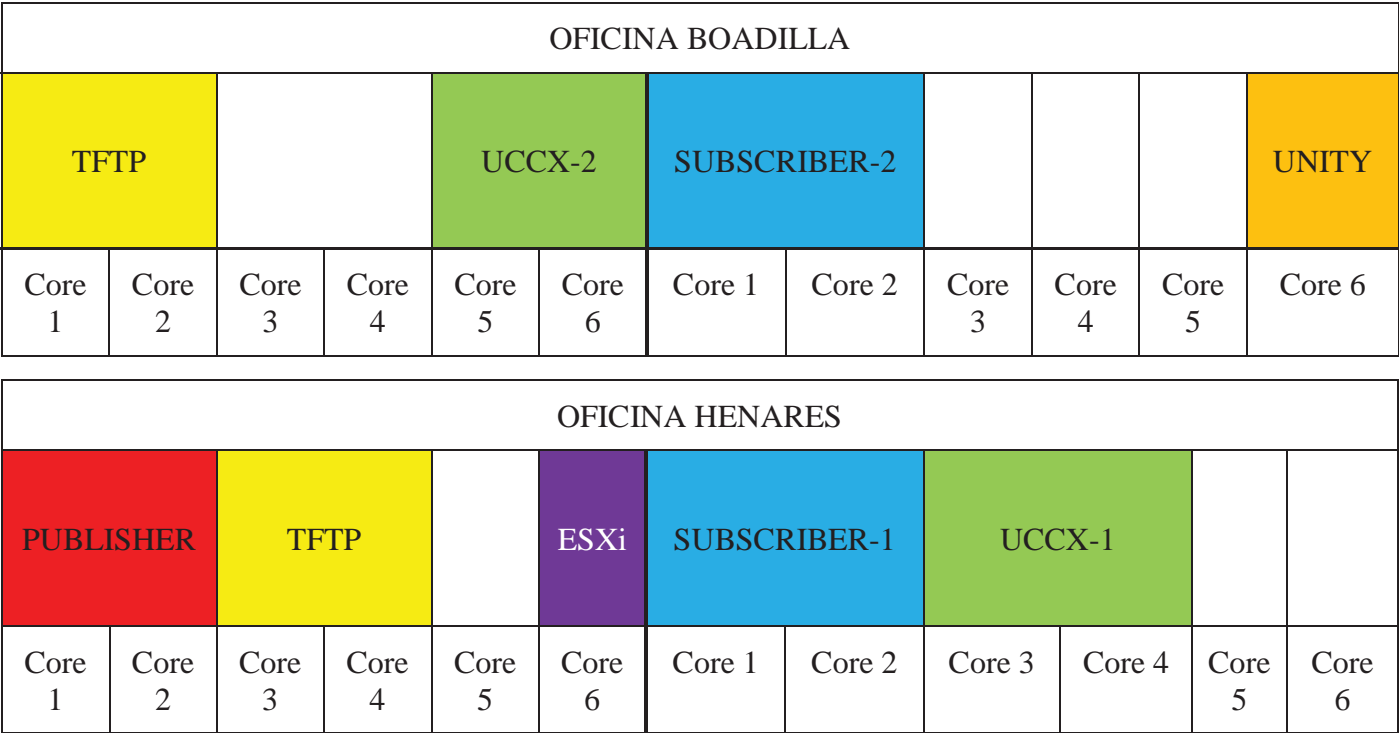


FIGURA 4.3: Componentes de los servidores

4.2.1.1.2. Gateway de Voz

Los Gateways de voz son unos dispositivos encargados del backup de los routers principales en caso de que ambos se caigan, con el fin de que cada una de las oficinas siga teniendo salida de Voz a través de la RTC. Otra de sus funciones del Gateway consiste en actuar como centralita con funciones básicas de voz cuando exista pérdida de conectividad con los terminales IP con los servidores principales a través de la red de datos. Esto puede ser debido a que exista una caída de los routers o acceso de datos de la sede u otros posibles fallos.^[33]

A continuación, se dimensionará el Gateway que se asignará a las oficinas teniendo en cuenta las necesidades de cada una de ellas, eligiendo los modelos y las componentes necesarias para dar un servicio óptimo al cliente.

Lo primero a tener en cuenta, es saber el número de canales que necesitará cada una de las oficinas, lo cual nos proporcionará el número de primarios (E1) que hay en la conexión con la Red Telefónica Conmutada (RTC). Para poder realizar este cálculo utilizaremos la calculadora Erlang B introduciendo las siguientes hipótesis como parámetro en los valores de ocupación

Según la teoría de colas, hay que calcular el tráfico medio de ocupación de canal de un usuario en su jornada laboral y tener en cuenta los siguientes puntos.

Valores de Ocupación de los canales	
Tráfico de 1 usuario	0,16 Erlangs/usuario
Tasa de pérdida	1%
Ocupación externa	66%
Ocupación en la misma oficina	17%
Ocupación entre oficinas	17%

TABLA 4.4: Ocupación de los canales de 1 servidor

En la ocupación externa es la ocupación que más nos interesa debido a que las ocupaciones de las oficinas van a través de nuestra red interna. Por parte de los móviles, las cargas van a través del proveedor que seleccionemos para contratar el servicio y, por tanto, no lo tendremos demasiado en cuenta.

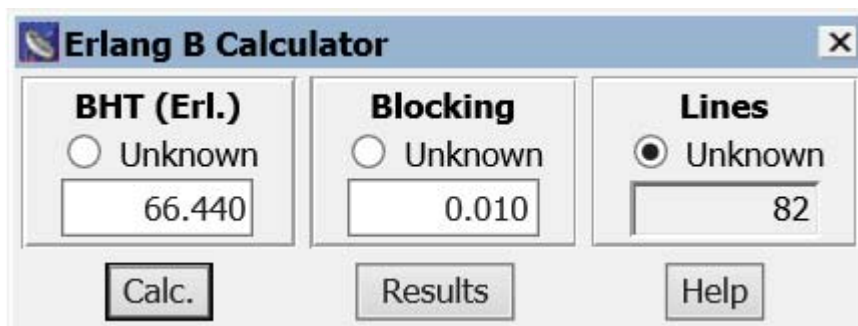
En función a nuestras oficinas, vamos a agrupar las de Boadilla, Villaverde y Castilla debido a que tienen 500 usuarios las dos primeras y 400 usuarios la última, por lo que contaremos como una oficina de 500 usuarios. En cuanto a Henares, contaremos como una oficina de 50 usuarios, aunque haya 5, debido a que el tráfico de estos usuarios puede ser mayor y siempre tener canales de sobra y asegurar que no haya colapso en ellos.

Oficina 500 Usuarios:

$\text{Tráfico/oficina} = \text{Usuarios/oficina} * \text{Tráfico/usuario} \rightarrow 500 * 0,16 = \mathbf{80 \text{ Erlangs}}$

$\text{Tráfico/usuarioExt} = \text{Tráfico/oficina} * (\text{OcupaciónExt} + \text{OcupacionOtrasOfi})$

$\rightarrow 80 * (0,66 + 0,17) = \mathbf{66,44 \text{ Erlangs}}^{[34]}$



The screenshot shows the 'Erlang B Calculator' window. It has three main input sections: 'BHT (Erl.)' with a radio button for 'Unknown' and a text box containing '66.440'; 'Blocking' with a radio button for 'Unknown' and a text box containing '0.010'; and 'Lines' with a radio button for 'Unknown' and a text box containing '82'. At the bottom, there are three buttons: 'Calc.', 'Results', and 'Help'.

FIGURA 4.4: Calculadora Erlang B 500 usuarios

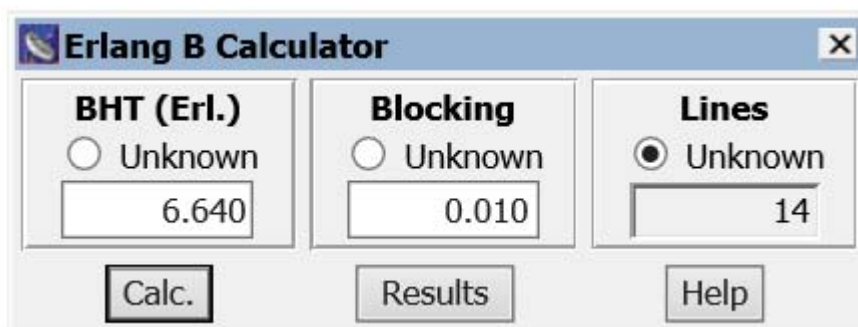
Como Podemos observar, se establecen 82 canales en las oficinas de 500 usuarios para el tráfico necesario. Esto equivale a 3 canales primarios de 30 canales cada uno (E1) para conectar con el RTC.

Oficina 50 Usuarios:

$\text{Tráfico/oficina} = \text{Usuarios/oficina} * \text{Tráfico/usuario} \rightarrow 50 * 0,16 = \mathbf{8 \text{ Erlangs}}$

$\text{Tráfico/usuarioExt} = \text{Tráfico/oficina} * (\text{OcupaciónExt} + \text{OcupacionOtrasOfi})$

$\rightarrow 8 * (0,66 + 0,17) = \mathbf{6,64 \text{ Erlangs}}^{[34]}$



The screenshot shows the 'Erlang B Calculator' window. It has three main input sections: 'BHT (Erl.)' with a radio button for 'Unknown' and a text box containing '6.640'; 'Blocking' with a radio button for 'Unknown' and a text box containing '0.010'; and 'Lines' with a radio button for 'Unknown' and a text box containing '14'. At the bottom, there are three buttons: 'Calc.', 'Results', and 'Help'.

FIGURA 4.5: Calculadora Erlang B 50 usuarios

Como Podemos observar, se establecen 14 canales en las oficinas de 50 usuarios para el tráfico necesario. Esto equivale a 1 canal primario de 30 canales (E1) para conectar con el RTC.

Platform	Number of Phones Supported ¹	Part Number (Spare)
Cisco 800 Integrated Services Router	Up to 5 phones	FL-CME-SRST-5=
Cisco 2901 Integrated Services Router	Up to 35 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 2911 Integrated Services Router	Up to 50 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 2921 Integrated Services Router	Up to 100 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 2951 Integrated Services Router	Up to 250 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 3925 Integrated Services Router	Up to 730 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 3945 Integrated Services Router	Up to 1200 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 3925E Integrated Services Router	Up to 1350 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 3945E Integrated Services Router	Up to 1500 phones	FL-CME-SRST-5=, FL-CME-SqRST-25=, FL-CME-SRST-100=
Cisco 4321 Integrated Services Router	Up to 50 phones	FL-CME-SRST-5=, FL-CME-SRST-25=
Cisco 4331 Integrated Services Router	Up to 100 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 4351 Integrated Services Router	Up to 750 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 4431 Integrated Services Router	Up to 1200 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=
Cisco 4451-X Integrated Services Router	Up to 2000 phones	FL-CME-SRST-5=, FL-CME-SRST-25=, FL-CME-SRST-100=

TABLA 4.5: Tipos de Gateways

Según Podemos observar en la tabla 4.5, existen varios modelos de routers Cisco según el número de teléfonos soportados. A continuación, detallaré en función de la oficina y del número de canales que necesitamos para cada una de ellas, el modelo elegido, sí como las distintas licencias y módulos a añadir al propio router.

En primer lugar, necesitamos un módulo PVDM en versión 4 (última versión) el cual nos va a soportar la densidad de los distintos canales para el procesamiento digital de la señal (DSP). Además de ello, necesitaremos la opción de software que disponen la serie Cisco de Cisco Survivable Remote Site Telephony (SRST) que nos ayuda a garantizar que los empleados de las oficinas dispongan de servicios y funciones de telefonía de manera ininterrumpida, aunque la conexión con el servidor falle. También podemos optar por la licencia dentro del software de Cisco IOS de Cisco Unified Communications Manager Express (CME) que ofrece una amplia gama de funciones para centralitas privadas (PBX) IP y sistemas clave integradas en el router para sucursales medianas y pequeñas.

Otro módulo a tener en cuenta para incluir a nuestro Gateway es una tarjeta de interfaz WAN de alta velocidad HWIC. Los Gateways deberán disponer de ranuras para estas tarjetas las cuales deben de ofrecer la capacidad para transmisión de datos de alta velocidad.

- Velocidad total de hasta 1,6 Gbps hacia el procesador del router.
- Velocidad total de hasta 2 Gbps hacia otras ranuras de módulos por la estructura multigigabit (MGF).

Finalmente, para los modelos de Gateway es necesario incorporar una fuente de alimentación redundante externa para protegernos de posibles fallos de la fuente de alimentación principal.

Oficina 500 Usuarios:

Para la oficina de 500 usuarios, he seleccionado el Gateway de *Cisco ISR 4351* con licencia SEC para mayor seguridad, ya que soporta un total de 750 teléfonos, suficiente para todos los usuarios de la oficina. La serie 4000 de Cisco es la más actual y es la que se está poniendo en las diferentes empresas.



FIGURA 4.6: Cisco ISR 4351 [35]

El módulo seleccionado para el procesamiento digital de la señal es un *PVDM4-128 (=)* debido a que necesitamos un total de 82 canales y de esta forma estableceremos 128. El anterior a éste obtendría 64 canales lo cual queda insuficiente para nuestra oficina.

Las dos licencias mencionadas antes se pueden unificar en una sola de la forma *FL-CME-SRST (=)* y, tal y como vemos en la tabla 4.4, existen para 5, 25 o 100 usuarios. En nuestro caso seleccionamos un total de 6 de 100 usuarios ya que, en las oficinas de 500, con 5 de ellas quedaríamos un poco justos.

Para las tarjetas HWIC, tenemos en cuenta que en esta oficina necesitaremos un total de 3 primarios, por lo que elegimos la tarjeta *HWIC-2CE1T1-PRI (=)* la cual dispone de dos primarios en cada una. Al necesitar un total de tres, elegimos dos tarjetas en total lo que supondrá un total de 4 primarios de los que usaremos 3 en principio, ya que puede haber futuras ampliaciones.

Finalmente, he seleccionado una fuente de alimentación adicional para el propio Gateway por motivos de seguridad y poder mantener la corriente del dispositivo en caso de fallo eléctrico del servidor. La fuente de alimentación es *PWR-4450-POE-AC (=)*.

CÓDIGO	DESCRIPCIÓN	CANTIDAD	PRECIO
Cisco ISR 4351-SEC/K9	Modelo Gateway	1	8.091€
FL-CME-SRST-100=	Licencia 100 usuarios	6	1.861€
HWIC-2CE1T1-PRI=	Tarjetas de alta velocidad	2	3.915€
PWR-4450-POE-AC=	Fuente de alimentación	1	1.861€
PVDM4-128=	Módulo DSP con 128 canales	1	6.327€

TABLA 4.6: Componentes Gateway de una oficina de 500 usuarios

Oficina 50 Usuarios:

Para la oficina de 50 usuarios, he seleccionado el Gateway de *Cisco ISR 4331* con licencia SEC para mayor seguridad, ya que soporta un total de 100 teléfonos, suficiente para todos los usuarios de la oficina. La serie 4000 de Cisco es la más actual y es la que se está poniendo en las diferentes empresas.



FIGURA 4.7: Cisco ISR 4331 ^[36]

El módulo seleccionado para el procesamiento digital de la señal es un *PVDM4-32* debido a que necesitamos un total de 14 canales y de esta forma estableceremos 32. El anterior a éste obtendría 16 canales lo cual queda bastante justo para nuestra oficina y limitado en el caso de futuras ampliaciones.

Las dos licencias mencionadas antes se pueden unificar en una sola de la forma *FL-CME-SRST* y, tal y como vemos en la tabla 4.4, existen para 5, 25 o 100 usuarios. En nuestro caso seleccionamos una de 100 usuarios ya que, en las oficinas de 50, cubre de sobra las necesidades.

Para las tarjetas HWIC, tenemos en cuenta que en esta oficina necesitaremos un total de 1 primario, por lo que elegimos la tarjeta *HWIC-2CE1T1-PRI* la cual dispone de dos primarios en cada una. Al necesitar una, elegimos una tarjeta por lo que supondrá un total de 2 primarios de los que usaremos 1 en principio, ya que puede haber futuras ampliaciones.

Finalmente, he seleccionado una fuente de alimentación adicional para el propio Gateway por motivos de seguridad y poder mantener la corriente del dispositivo en caso de fallo eléctrico del servidor. La fuente de alimentación es *PWR-4330-POE-AC (=)*.

CÓDIGO	DESCRIPCIÓN	CANTIDAD	PRECIO
Cisco ISR 4331-SEC/K9	Modelo Gateway	1	3.641€
FL-CME-SRST-100=	Licencia 100 usuarios	1	1.861€
HWIC-2CE1T1-PRI=	Tarjetas de alta velocidad	1	3.915€
PWR-4330-POE-AC=	Fuente de alimentación	1	465€
PVDM4-32=	Módulo DSP con 32 canales	1	1.582€


TABLA 4.7: Componentes Gateway de una oficina de 50 usuarios

4.2.1.1.3. Terminales para los Usuarios

A continuación, se va a establecer los diferentes terminales asociados en función de los perfiles que diferenciamos anteriormente (planta, móvil, directivo, especializado).


Gama Media:

Para los usuarios que dispondrán teléfonos de gama media, se utilizará el modelo de teléfono *Cisco IP Phone 7911G*, el cual dispone de las siguientes características.



Cisco IP Phone 7911G - VoIP phone

Part Number: CP-7911G

3 Related Models 

MISCELLANEOUS /	
Color	dark gray
Color Category	gray
IP TELEPHONY /	
VoIP Protocols	SCCP
Voice Codecs	G.711a, G.711u, G.729a, G.729ab
Quality of Service	IEEE 802.1Q (VLAN), IEEE 802.1p
IP Address Assignment	DHCP
VoIP	Yes
Security	128-bit AES
HEADER /	
Brand	Cisco
Product Line	Cisco IP Phone
Model	7911G
Packaged Quantity	1
GENERAL /	
Manufacturer	Cisco

FIGURA 4.8: Cisco IP Phone 7911G ^[18]

Esta gama de terminales será utilizada por los usuarios básicos que no necesitan muchas funcionalidades en su teléfono para desempeñar su trabajo.

Gama Medio-Alta:

Para esta gama elegimos el modelo *Cisco IP Phone 7941G* que es un teléfono IP de segunda generación para usuarios con unos volúmenes de tráfico medio. Proporciona dos botones programables de líneas/prestaciones y cuatro teclas programables que orientan al usuario a través de las prestaciones y funciones de llamada. Sus características son las siguientes:



MISCELLANEOUS /

Color	dark gray
Color Category	gray

IP TELEPHONY /

VoIP Protocols	SCCP
Voice Codecs	G.711u, G.729a
Quality of Service	IEEE 802.1Q (VLAN), IEEE 802.1p
IP Address Assignment	DHCP
VoIP	Yes
Network Protocols	TFTP

HEADER /

Brand	Cisco
Product Line	Cisco Unified IP Phone
Model	7941G
Packaged Quantity	1

GENERAL /

Manufacturer	Cisco
--------------	-------

FIGURA 4.9: Cisco IP Phone 7941G

Esta gama de terminales la utilizarán los perfiles de usuario avanzado y representativo que necesitan de teléfonos con más funcionalidades que los de gama baja.

Gama Alta:

Estos son los terminales que utilizaran las operadoras y las secretarias. Se ha elegido el teléfono *Cisco IP Phone 7962G* con dos módulos de expansión de *Cisco 7915*. Sus características son las siguientes:


<div></div> <div>Cisco Unified IP Phone 7962G - VoIP phone Part Number: CP-7962G 3 Related Models ▾</div>	
MISCELLANEOUS /	
Color	dark gray, silver
Color Category	gray, silver
Placing / Mounting	table-top, wall-mountable
IP TELEPHONY /	
VoIP Protocols	SCCP, SIP
Voice Codecs	G.711a, G.711u, G.722, G.729a, G.729ab, iLBC
Quality of Service	IEEE 802.1Q (VLAN), IEEE 802.1p
IP Address Assignment	DHCP, static
VoIP	Yes
Security	128-bit AES
Network Protocols	TFTP
HEADER /	
Brand	Cisco
Product Line	Cisco Unified IP Phone
Model	7962G
Packaged Quantity	1
GENERAL /	
Manufacturer	Cisco

FIGURA 4.10: Cisco IP Phone 7962G y módulo 7915

El módulo de expansión 7915 permite la visualización del estado y marcación directa de hasta 24 usuarios, recomendable para la realización de las labores de operadora.



FIGURA 4.11: Módulo 7915

Además de la elección de los terminales para cada usuario dependiendo de los perfiles en los que pertenece, se va a asignar un terminal móvil para los perfiles que correspondan. Estos terminales móviles serán los mismos para todos los usuarios independientemente del puesto a desempeñar. El teléfono móvil seleccionado para todos los perfiles será el *Samsung Galaxy S8*, un teléfono de alta gama capaz de mantener una buena calidad de servicio para cada momento. Este teléfono tendrá acceso a todas las aplicaciones requeridas para mantener una comunicación al instante.



FIGURA 4.12: Samsung Galaxy S8

Para determinar el número total de usuarios perteneciente a cada perfil se va a desarrollar un estudio en porcentaje de las diferentes oficinas, de este modo, se hará una estimación del número total de terminales a distribuir.

Las oficinas de Boadilla y Villaverde contarán con un 40% de usuarios planta, 30% usuarios móviles, 15% usuarios directivos y 15% usuarios especializados. En estas dos oficinas contarán con el mayor número de usuarios normales sin ningún tipo de cargo.

La oficina de Castilla contará con un 20% usuarios planta, 20% usuarios móviles, 30% usuarios directivos y 30% usuarios especializados. En esta oficina está oficina localizaremos el mayor parte de los usuarios directivos.

En la oficina Henares, no se ubicará ningún terminal debido a que los 5 usuarios son de perfil móvil.

De este modo, las distribuciones de los perfiles en las distintas oficinas quedan distribuidas del siguiente modo.

OFICINA	TOTAL	PLANTA	MÓVIL	DIRECTIVO	ESPECIALIZADO
Boadilla	500	200	150	75	75
Villaverde	500	200	150	75	75
Henares	400	80	80	120	120
Castilla	5	0	4	1	0
TOTAL	1405	480	384	271	270

TABLA 4.8: Distribución de perfiles de usuarios

4.2.1.1.4. Desglose Final

Si tenemos en cuenta la tabla 4.8 donde se indican los perfiles, y la tabla 4.1 donde se indican los terminales asociados a los distintos usuarios podremos establecer el número total de terminales a asignar.

Del mismo modo, contemplando la tabla 4.6 y la tabla 4.7 donde indicamos el número de dispositivos en una oficina y sabiendo que tenemos 3 oficinas de 500 usuarios y 1 oficina de 50 usuarios, podemos desglosar el número total de dispositivos necesarios.

SERVICIO	CANTIDAD	PRECIO UNIT	PRECIO FINAL
Cisco ISR 4351-SEC/K9	3	8.091€	24.273€
FL-CME-SRST-100=	19	1.861€	35.359€
HWIC-2CE1T1-PRI=	7	3.915€	27.405€
PWR-4450-POE-AC=	3	1.861€	5.583€
PVDM4-128=	3	6.327€	18.981€
Cisco ISR 4331-SEC/K9	1	3.641€	3.641€
PWR-4330-POE-AC=	1	465€	465€
PVDM4-32=	1	1.582€	1.582€
CISCO IP PHONE 7911G	480	136€	65.280€
CISCO IP PHONE 7941G	271	208€	56.160€
CISCO IP PHONE 7962G	270	575€	155.250€
SAMSUNG GALAXY S8	655	699€	457.845€
			TOTAL = 851.824€

TABLA 4.9: Desglose Final de Voz

3.3.2. Diseño de la Red de Datos

Para la realización del diseño de la red de datos vamos a tener en cuenta los conceptos explicados en el apartado anterior.

En nuestro sistema vamos a componer una red WAN que conectarán las oficinas entre ellas, diferentes redes LAN en cada una de las oficinas y una red WiFi para no tener conectividad única por medio de cableado.

3.3.2.1. DISEÑO DE RED WAN

El diseño de la red WAN consistirá en definir la interconexión con las distintas oficinas junto con la salida a Internet de toda la red corporativa.

4.2.2.1.1. Arquitectura de red WAN

Para la arquitectura WAN he contemplado una solución de diagrama como se puede ver a continuación.

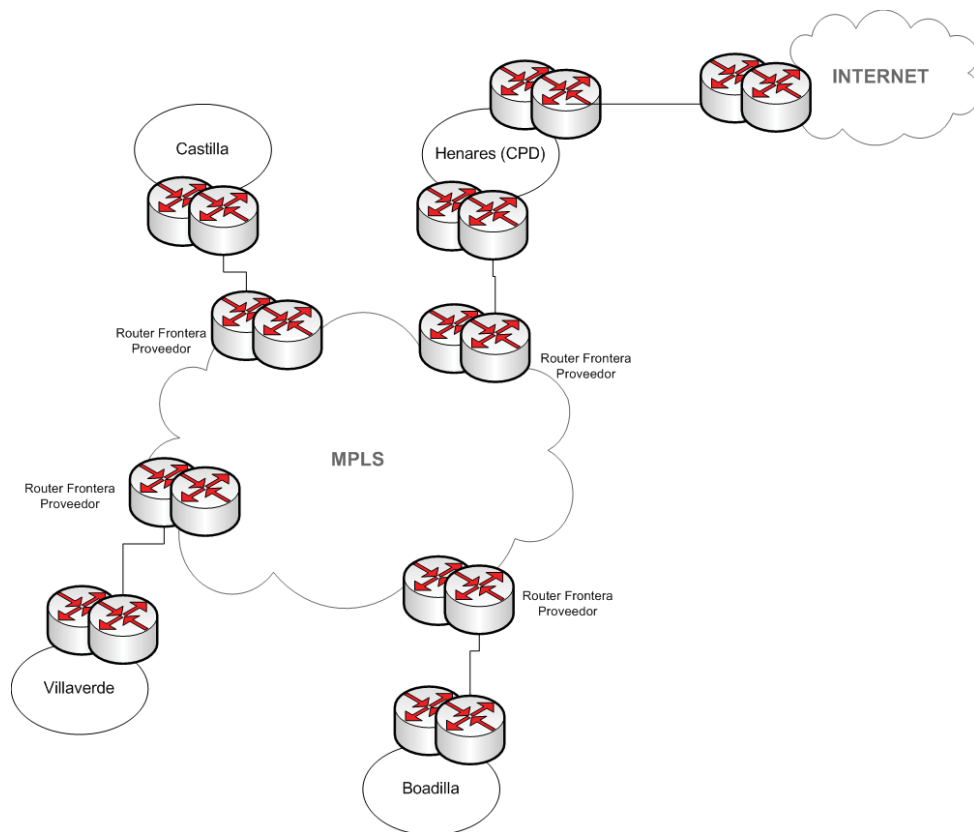


FIGURA 4.13: Arquitectura Red WAN

Una solución planteada consiste en la unión de las diferentes oficinas a través de un circuito de MPLS contratado con un proveedor. Tal y como se pudo ver en el state of art, la MPLS consiste en un sistema de interconexión por una línea contratada con un proveedor, el cual dispone de unos routers frontera donde conectaremos los routers de

cada una de las oficinas y, mediante la conexión del proveedor se establecerá la conexión con el otro extremo en la otra oficina. A continuación, detallaré la comunicación por parte de nuestro extremo conectado al primer router de la línea MPLS.

Este tipo de tecnología despliega un mayor control sobre la calidad del servicio, la ingeniería del tráfico y la utilización del ancho de banda, a la vez que reduce los requisitos de nuestros dispositivos de comunicación.

Para la disposición de los dispositivos de nuestro extremo, contaremos en cada oficina con dos routers en la frontera de cada oficina que irán conectados con los routers frontera del proveedor. En nuestro caso utilizaremos dos switches Core en lugar de routers como tal, ya que nos sirven como conector con los distintos dispositivos de planta (explicado en el apartado de la Red LAN).

Estos routers irán conectados mediante fibra óptica a dos routers frontera del proveedor de forma que se establecerá redundancia por tema de caídas. Estos routers frontera se encontrarán ubicados en cada una de las diferentes sedes para ya conectarse a la red interna del proveedor y establecer la interconexión entre oficinas.

Además, debemos tener en cuenta la salida hacia Internet, la cual se realizará desde el CPD de la oficina de Henares tal y como se indicó en el diagrama. Allí se realizará la conexión con los routers del proveedor que se contraten de Internet.

Por último, utilizaremos una conexión S2S (Site to Site) en el CPD para la conexión con los posibles clientes de la propia empresa para tener una conexión directa y privada.

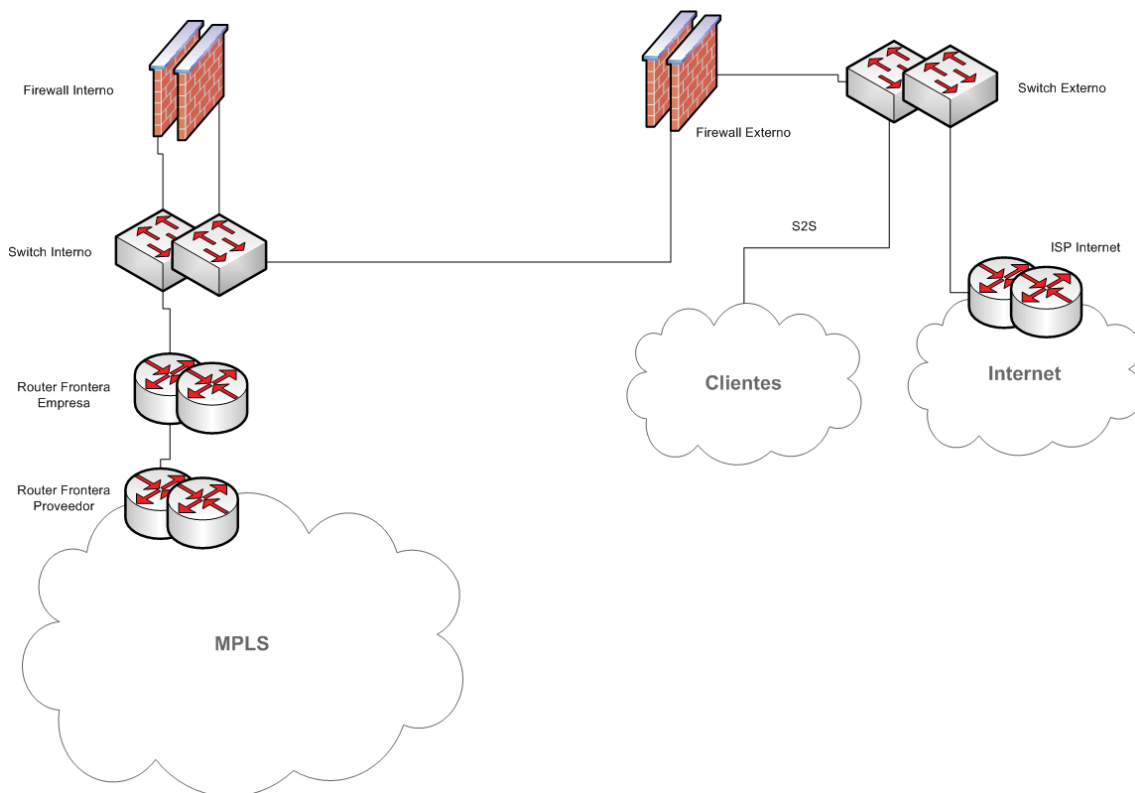


FIGURA 4.14: Diagrama CPD

Observando el diagrama, detallaré cada una de las funciones de los distintos dispositivos, así como los distintos aspectos a tener en cuenta en todos ellos.

- **Router Frontera Proveedor:** Consiste en el router del proveedor de la MPLS que conectará con el resto de routers frontera del proveedor de las distintas oficinas que se encuentran conectadas a la MPLS.
- **Router Frontera Empresa:** Consiste en el router de la empresa que se encuentra en la frontera de ésta que conectará mediante fibra óptica directamente con los routers frontera del proveedor de la MPLS. Por el otro lado, estos routers conectarán con un Switch interno de nivel 2 por una interfaz para llegar al firewall.
- **Switch Interno:** Consiste en un switch de nivel 2 que servirá de conexión entre el router frontera de la empresa al firewall interno, debido a que para establecer esta conexión es necesario que exista este switch como intermediario. Además, en este switch conectaremos los distintos servidores que utilizaremos en nuestra infraestructura, los cuales estarán protegidos por nuestro firewall ante posibles ataques. Por último, servirá también como switch externo de este firewall para aprovechar al máximo el número de puertos.
- **Firewall Interno:** Consiste en el firewall interno de nuestra infraestructura, el cual protegerá los distintos servidores y se encargará del filtrado de las conexiones que irán desde nuestras oficinas hacia internet como desde las oficinas hacia los distintos clientes.
- **Firewall Externo:** Consiste en el firewall externo que tendrá salida directa de toda nuestra infraestructura de red, es decir, el último dispositivo antes de salir de ella. Por tanto, este firewall tendrá la función de analizar y filtrar todo el tráfico que pueda atacar a nuestra infraestructura y permitir todos los accesos tanto a Internet como a los distintos clientes.
- **Switch Externo:** Consiste en el switch externo para dar la salida final debido a que el firewall necesita este dispositivo para conectar con los demás dispositivos. Tendrá dos funciones principales:
 - Primera: Dar salida a internet, por lo que establecerá la conexión con el ISP de internet.
 - Segunda: Conectar un Site to Site (S2S) con los distintos clientes.

Todos los dispositivos que tienen funciones en esta oficina deberán estar redundados para prevenir posibles caídas de toda la infraestructura.

4.2.2.1.2. Dimensionado de Red WAN

A continuación, detallaremos los puntos que hay que tener en cuenta a la hora de dimensionar la infraestructura y los puntos que hay que tener en cuenta para poder elegir los dispositivos adecuados para realizar las funciones detalladas anteriormente.

Caudales:

En nuestra arquitectura de red, disponemos de dos tipos de acceso por parte de los distintos usuarios de cada oficina.

1. De cada oficina con la red MPLS del Operador para la Red Privada.
2. Desde la oficina del CPD con la red MPLS del Operador para el acceso a Internet.

Para todos ellos, hay que indicar la velocidad de los accesos (10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps) y el caudal para el tráfico elástico y para el tráfico inelástico.

- TRÁFICO ELÁSTICO:

Para poder realizar una estimación del tráfico que se va a usar en cada una de las sedes, vamos a tomar como referencia el dato del consumo medio de un usuario.

Como se puede observar en la estimación de tráfico para un usuario FTTH para el año 2018 es de 748Kbps. En base a este dato, calculamos la cantidad de tráfico elástico que consumirá cada una de las oficinas. ^[37]

- Para la oficina de 500 usuarios:

$$500 \text{ usuarios} \times 748 \text{ Kbps} = 374.000 \text{ Kbps} = \mathbf{374 \text{ Mbps}}$$

Para el CPD hay que tener en cuenta que el peor de los casos ocurre cuando llega el máximo tráfico elástico de todas las oficinas a la vez, por lo que hay que tenerlo en cuenta para el dimensionado, debido a que tiene que soportar todo el tráfico.

- Para el CPD de 50 usuarios:

$$(50 \text{ usuarios} \times 748 \text{ Kbps}) + (3 \text{ oficinas} \times 374 \text{ Mbps}) = \mathbf{1.159,4 \text{ Mbps}}$$

- TRÁFICO INELÁSTICO:

Para este tráfico hay que tener en cuenta que cada uno de los canales de voz ocupan 32 Kbps. Por tanto, para las distintas oficinas hay que tener en cuenta lo siguiente:

- Para la oficina de 500 usuarios:

$$82 \text{ canales} \times 32 \text{ Kbps} = \mathbf{2.624 \text{ Kbps}}$$

Tanto en el CPD como en la oficina de Boadilla recibirán todo el tráfico debido a que tienen los servidores UCS en su oficina. En el CPD, a pesar de ser pocos usuarios, se va a tener en cuenta ya que es conveniente tener una línea por tema de cobertura.

- Para oficina Boadilla y CPD:

$$(14 \text{ canales} \times 32 \text{ Kbps}) + (3 \text{ oficinas} \times 2.624 \text{ Kbps}) = 8.320 \text{ Kbps} = \mathbf{8,32 \text{ Mbps}}$$

- VELOCIDAD TOTAL:

Después de determinar todos los tráficos y las caudales necesarios en las distintas oficinas, queda una tabla resumen de los distintos tráficos totales a tener en cuenta para elegir los distintos dispositivos que vamos a utilizar en nuestra arquitectura.

Para la conexión entre las oficinas por la MPLS.

Oficinas	Caudal inelástico	Caudal elástico	Caudal total	Acceso
Castilla	2.624 kbps	374 Mbps	376,624 Mbps	1 GE
Villaverde	2.624 kbps	374 Mbps	376,624 Mbps	1 GE
Boadilla	8.320 kbps	374 Mbps	382,32 Mbps	1 GE
Henares (CPD)	8.320 kbps	1.159,4 Mbps	1.167,72 Mbps	10 GE

TABLA 4.10: Caudal y velocidad de la MPLS

Para la conexión del CPD con la salida de internet.

Oficinas	Caudal inelástico	Caudal elástico	Caudal total	Acceso
Henares (CPD)	8.320 kbps	1.159,4 Mbps	1.167,72 Mbps	10 GE

TABLA 4.11: Caudal y velocidad de la salida a Internet

Dispositivos:

Teniendo en cuenta todos los requisitos que hemos indicado anteriormente para cumplir con todas las necesidades, detallaremos los dispositivos apropiados para cumplir cada una de sus funciones.

- ROUTER FRONTERA EMPRESA

Este router se localizará tanto en el CPD como en todas las demás oficinas para cumplir la función de ser la frontera de cada oficina con la MPLS que contrataremos con el proveedor ^[38]. Para los dispositivos de las oficinas, se detallarán los requisitos necesarios en el apartado de Dimensionado de Red LAN, por lo que ahora nos centraremos en los routers del CPD.

Necesitamos un dispositivo que disponga de:

- 4 puertos de 10 GE para establecer la conexión con los 2 Routers Frontera del Proveedor y los 2 Switches Internos para tener redundancia.
- 1 puertos de 1 GE para establecer la comunicación entre los dos dispositivos.

Por tanto, si tenemos en cuenta la serie de dispositivos más adecuados para nuestra arquitectura, emplearemos el *Cisco ASR 1001-HX*, el cual cumple con esos requisitos ^[39].



FIGURA 4.15: Cisco ASR 1001-HX

Este dispositivo necesita los siguientes componentes ^[40]:

- Módulo con 8 puertos de 1 GE y 8 puertos de 10 GE.



FIGURA 4.16: Módulo para ASR 1001-HX

- Para hacer las conexiones de 10 GE usaremos el modelo *SFP-10G-SR* y para las conexiones de 1 GE usaremos el modelo *GLC-T1000Base-T*



FIGURA 4.17: SFP para 10 Gbps y 1 Gbps

- 2 Fuentes de alimentación AC para tener redundancia en cortes.



FIGURA 4.18: Fuentes de alimentación ASR 10001-HX

• SWITCH INTERNO Y EXTERNO

Estos switches son los encargados de propagar las diferentes Vlan de servidores o de conexiones entre los firewalls antes de dar salida a Internet o las redes privadas de los clientes ^[41]. Por ello necesitamos un switch de capa 2 con bastantes puertos que soporten todo el tráfico de toda la arquitectura de red ^[42].

Los requisitos para el Switch Interno son:

- 7 puertos de 10 GE para establecer las conexiones con el Router Frontera y con los 2 Firewalls, tanto externo como interno. Estas conexiones son duplicadas por la redundancia. Además, se conectará una plataforma de virtualización donde irán conectados los servidores. El modelo será *VMware ESXi*.
- Puertos de 1 GE para futuras conexiones con futuros servidores ya que el ESX solo dispondrá de los servidores básicos.

Los requisitos para el Switch Externo son:

- 2 puertos de 10 GE para establecer la conexión con el Firewall Externo.
- Puertos de 1 GE para establecer la conexión con Internet y con los clientes.

El dispositivo que cumple con las características y requisitos necesarios para la parte interna como para la parte externa es el *Cisco Catalyst 4900M* ^[43].



FIGURA 4.19: Cisco Catalyst 4900M

Para este dispositivo como Switch Interno usaremos los siguientes módulos para adaptarlo a nuestras necesidades:

- Un módulo *WS-X4920-GB-RJ45* (=) que dispone de 20 puertos 10/100/1000 Base-T con entrada de *RJ-45* que se emplearán para las conexiones de los servidores ubicados en el CPD ^[43].



FIGURA 4.20: Módulo WS-X4920-GB-RJ45

- Un módulo *WS-X4908-10GE* (=) que dispone de 8 puertos de 10 GE donde se conectarán los 7 puertos que necesitamos dejando uno para futuras ampliaciones.



FIGURA 4.21: Módulo WS-X4908-10GE (=)

Como se puede observar las conexiones necesitan un convertor a SFP del modelo que vimos en la Figura 4.19 del modelo *CVR-X2-SFP10G*.



FIGURA 4.22: Adaptador CVR-X"-SFP10G

Para el Switch Externo se usarán un módulo de *WS-X49020-GB-RJ45* (=) y otro módulo de *WS-X4904-10GE* (=) ya que dispone de 4 puertos de 10 GE suficiente para cubrir nuestras necesidades. También se añadiría su correspondiente adaptador

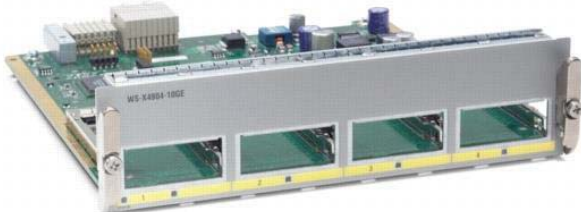


FIGURA 4.23: Módulo WS-X4904-10GE (=)

• FIREWALL INTERNO

Este Firewall se encarga únicamente del filtrado de reglas para redirigir el tráfico a los servidores internos o bien al Firewall Externo donde se realizará el análisis exhaustivo del tráfico ya que es donde se realizará la salida de toda la infraestructura, ya sea a los distintos clientes como a Internet ^[44]. Necesitaremos los siguientes puertos:

- 2 puertos de 10 GE donde se conectará con el Switch Interno. Ese mismo enlace servirá como entrada desde el Switch al Firewall como de salida del Firewall al Switch, ya que se configurará el puerto en modo “trunk”.
- 1 puerto de 1 GE donde se conectará el enlace de comunicación entre los dos firewalls para formar el clúster entre ellos.

El dispositivo que cumple con todos los requisitos y las necesidades que abarca este firewall es el *Juniper SRX1500* ya que es un cortafuegos de baja latencia y alto rendimiento para campus empresariales distribuidos y centros de datos pequeños y medianos. Ideal para nuestra arquitectura ^[44].



FIGURA 4.24: Juniper SRX1500

Este firewall dispone de las siguientes especificaciones y cumple con las necesidades que indicamos al principio ^[45].

Hardware Specifications	
Specification	SRX1500
Connectivity	
Total onboard ports	16x1GbE and 4x10GbE
Onboard RJ-45 ports	12x1GbE
Onboard small form-factor pluggable (SFP) transceiver ports	4x1GbE
Onboard SFP+ ports	4x10GbE
Out-of-Band (OOB) management ports	1x1GbE
Dedicated high availability (HA) ports	1x1GbE (SFP)
PIM slots	2
Console (RJ-45 + miniUSB)	1
USB 2.0 ports (type A)	1
Memory and Storage	
System memory (RAM)	16 GB
Primary boot storage (mSATA)	16 GB
Secondary storage (SSD)	100 GB

TABLA 4.12: Especificaciones Juniper SRX1500

- FIREWALL EXTERNO

Este firewall será el encargado de dar salida al exterior a todo el tráfico que requiera conectarse tanto a Internet como a redes privadas con los clientes. Por este motivo, este firewall tendrá que ser de alta gama para tener una gran protección y seguridad ante cualquier ataque o cualquier intento de penetrar a nuestra infraestructura. Necesitaremos una serie de requisitos a la hora de seleccionar el dispositivo ^[46].

- 4 puertos de 10 GE donde se conectará el Switch Interno y el Switch externo.
- 1 puerto de 1 GE donde se conectará el enlace de comunicación entre los dos firewalls para formar el clúster entre ellos.

Por tanto, para desempeñar el papel de Firewall Externo, he elegido el *Palo Alto PA-5060*, ya que la serie *PA-5000* permite de forma segura aplicaciones, usuarios y contenido a velocidades de hasta 20 Gbps. Los recursos de procesamiento dedicados asignados a redes, seguridad, coincidencia de firmas y funciones de gestión garantizan un rendimiento predecible.



FIGURA 4.25: Palo Alto PA-5060

Este firewall cumple con los requisitos ya que dispone de las siguientes especificaciones ^[47].

PA-5060
<ul style="list-style-type: none"> • 20 Gbps firewall throughput (App-ID enabled¹) • 10 Gbps threat prevention throughput • 4 Gbps IPSec VPN throughput • 4,000,000 max sessions • 120,000 new sessions per second • 8,000 IPSec VPN tunnels/tunnel interfaces • 20,000 SSL VPN Users • 225 virtual routers • 25/225 virtual systems (base/max²) • 900 security zones • 40,000 max number of policies

TABLA 4.13: Especificaciones PA-5060

4.2.2.1.3. Tabla Resumen Red WAN

Este es el presupuesto de la parte de Red WAN del CPD. No he contemplado los dispositivos de las distintas oficinas que forman parte de nuestra red WAN debido a que los tendré en cuenta en la red LAN. Por otro lado, no he tenido en cuenta la contratación de la MPLS ya que únicamente he añadido los dispositivos con sus adaptadores ^[48].

SERVICIO	CANTIDAD	PRECIO UNIT	PRECIO TOTAL
Cisco ASR 1001-HX	2	82.630,53€	165.261,06€
SFP-10G-SR	38	865.45€	32.887,1€
GLC-T1000Base-T	2	382.71€	765,42€
Cisco Catalyst 4900M	4	19.288,64€	77.154,56€
WS-X4920-GB-RJ45	4	3.444,40€	13.777,6€
WS-X4908-10GE (=)	2	7.405,46€	14.810,92€
CVR-X2-SFP10G	18	172,22€	3.099,96€
WS-X4904-10GE (=)	2	4.994,38€	9.988,76€
VMware ESXi	2	939,50€	1.879€
Juniper SRX1500	2	12.921,21€	25.842,42€
Palo Alto PA-5060	2	113.275,70€	226.551,4€
			TOTAL: 572.018,2€

TABLA 4.14: Desglose final Red WAN

4.2.2.2. DISEÑO DE RED LAN

El diseño de la red LAN consistirá en establecer los accesos y conexiones de los distintos usuarios en cada una de las oficinas. Para la realización de este apartado, voy a establecer como modelo la oficina de Boadilla, ya que en ella se encuentra la mayor concentración de usuarios y de dispositivos, por lo que el resto de las oficinas serán similares a esta (exceptuando el CPD).

4.2.2.2.1. Arquitectura de Red LAN

Como he indicado, voy a tener como referencia la oficina de Boadilla para realizar la arquitectura de red LAN ya que cuenta con los mismos dispositivos que en las otras oficinas añadiéndole uno de los servidores UCS que ya introduje en el apartado de Red de Voz.

Lo primero que hay que tener en cuenta es el tipo de arquitectura que vamos a usar, en nuestro caso será Arquitectura distribuida ya que se adapta de la mejor forma a la arquitectura de nuestra oficina. Cada una de las plantas de la oficina dispondrá de un cuarto de dispositivos llamado IDF que se parecerá a un pequeño CPD donde situaremos todos los dispositivos de esa oficina. En esta sala encontraremos una distribución de la siguiente manera:

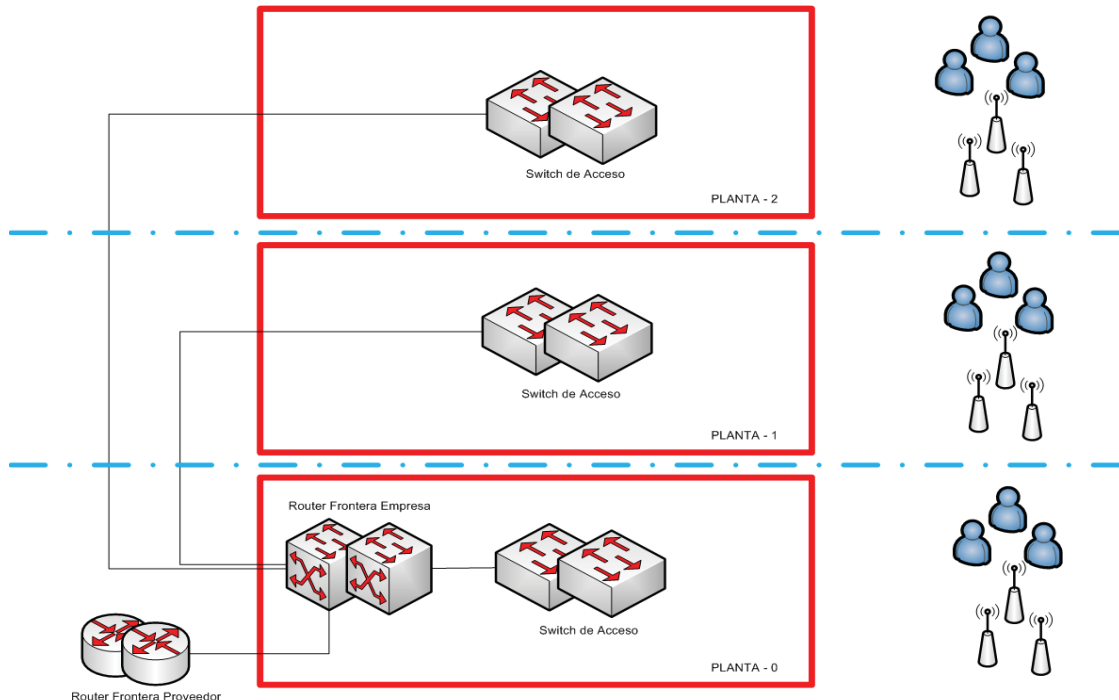


FIGURA 4.26: Arquitectura de Red LAN

Según observamos en el diagrama, en nuestra oficina diferenciaremos dos tipos de dispositivos en función de su utilidad, uno son los Router Frontera de Empresa y otro

es el Switch de Acceso. También hay que mencionar los Puntos de Acceso para la red WIFI (Explicado en el apartado de Red WIFI).

- **Router Frontera Empresa:** En nuestro caso vamos a usar un Switch Core multinivel que se encargará de la distribución de la red por las diferentes plantas de nuestra oficina, así como dar salida hacia la MPLS que realizará la interconexión entre las distintas oficinas hasta llegar al CPD donde se produce la salida al exterior. Además, se conectará el Gateway de voz de cada una de las oficinas por lo que se necesitará un dispositivo de mayor potencia y que pueda establecer el nivel 3 de las vlnes que propagaremos hasta las áreas de trabajo.
- **Switches de Acceso:** En estos switches se conectarán los distintos usuarios y teléfonos para dar servicio a todos los empleados de las oficinas de nuestra empresa. A su vez se conectarán todos los puntos de acceso para dar servicio por WiFi en el caso de no querer realizar la conexión por cable. Por tanto, necesitaremos tantos puertos como usuarios tengamos en cada una de las plantas.

Según observamos en el diagrama, la distribución de estos dispositivos indica que el CPD de la oficina se encuentra en la planta baja, ya que es donde se encontrará el Router Frontera Empresa, el Switch de Acceso de esa plana, el Gateway de Voz, los Routers Frontera Proveedor, las controladoras WiFi y el servidor UCS (en el caso de esta oficina únicamente), mientras que las otras plantas únicamente tendrán los Switches de Acceso.

Cableado:

Debido a que vamos a establecer una arquitectura distribuida, el cableado de la oficina consistirá en dos tipos de cableados, tal y como vimos en el apartado de state of art:

- **Cableado Horizontal:** encargado de comunicar los puertos de los Switches de Acceso junto con las tomas finales de los patch pannels de los usuarios. Esta conexión se realiza con cables de cobre del tipo RJ-45.
- **Cableado Vertical:** encargado de unir las conexiones entre las plantas para poder conectar los Switches de Acceso de las otras plantas al Router Frontera Empresa. Esta conexión se realiza con cables de Fibra Óptica.

4.2.2.2.2. Dimensionado Red LAN

Una vez establecidas las necesidades de las oficinas en cuanto a red LAN se refiere, hay que ver los distintos dispositivos que se puedan ajustar a ellas para tener una óptima arquitectura de todos los equipos necesarios. Para todos estos dispositivos vamos a utilizar la marca CISCO en todos ellos ya que es una de las marcas punteras en el sector y la mayoría de sus dispositivos son de gran calidad y cumplirán con las necesidades adoptadas en cada oficina.

Dispositivos:

- ROUTER FRONTERA EMPRESA

Este router va a ser diferente al Router Frontera Empresa localizado en el CPD ya que, en cada una de las oficinas utilizaremos un Switch Multinivel que pueda realizar la función de distribuidor de Switch Core de la oficina, así como de poder gestionar el nivel 3 de la misma. Establezco los puertos necesarios para poder dimensionar el número total de puertos disponibles a la hora de seleccionar nuestro dispositivo ^[49].

- 3 puertos de 1 GE para fibra para cada una de las 3 plantas de nuestra oficina.
- 2 puertos de 1GE para la conexión entre los 2 Routers Frontera Empresa para establecer la redundancia entre ambos.
- 2 puertos de 1 GE para la conexión con los 2 Routers Frontera Proveedor, para establecer la comunicación con la red WAN.
- 1 puerto de 1 GE para la conexión con el Gateway de voz.
- 1 puerto de 1 GE para la conexión con el servidor UCS.
- 1 puerto de 1 GE para la conexión con la controladora de WiFi.

Por tanto, cumpliendo los requisitos indicados donde necesitaremos un total de 9 puertos de 1 GE, excepto en la oficina de Boadilla que necesitaremos 10 puertos de 1 GE, debido a que es la única de las 3 oficinas que dispone de servidor UCS. Por tanto, el Switch que vamos a seleccionar se corresponde a la serie de C9500, ya que son switches de última generación con capacidad para soportar interfaces de hasta 100 Gbps ^[50].

Dentro de esta serie, he seleccionado el *Cisco C9500-40X-A* que dispone de un total de 40 puertos adaptados para conectar SFPs tanto de fibra como de RJ-45, los cuales pueden servir para 1GE o 10 GE ^[50].



FIGURA 4.27: Cisco C9500-40X-A

A este dispositivo se le pueden añadir módulos de 8x1/10GE o de 2x40GE, sin embargo, no se necesitan actualmente por lo que se dejará la tapa vacía para posible ampliación.

Al seleccionar este modelo de Switch, hay que tener en cuenta que necesitaremos la fuente de alimentación *PWR-C4-950WAC-R*, ya que es la indicada para él y necesitaremos los SFP de *SFP-10G-SR* para los puertos de fibra óptica y los *GLC-T1000Base-T* para los puertos a usar los cables de RJ-45.

- SWITCHES DE ACCESO

Para poder seleccionar el switch adecuado para dar acceso a nuestra oficina, tenemos que tener en cuenta las distintas áreas de trabajo y antenas por planta, ya que esto determinará cuantos puertos serán necesarios en total por oficina.

Tomamos como referencia la oficina de Boadilla para poder replicar los requisitos en el resto de las oficinas.

- Disponemos de 170 áreas de trabajo debido a que hay un total de 500 usuarios en la oficina completa, por lo que, si dividimos 500 usuarios en tres plantas, nos quedan aproximadamente 170 puestos.
- En cada planta dispondremos de un total de 20 antenas, que necesitarán un total de 40 puertos debido a que cada antena necesita 2 puertos para establecer la redundancia (explicado en el apartado 4.2.2.3 Diseño de red WiFi).

Por tanto, nos queda un total de 210 puertos mínimo por planta de cada una de las oficinas y serán puertos de 1 GE para tener una capacidad más que suficiente para el servicio de cada usuario como el de cada antena.

El Switch que cumple con todos los requisitos es el *Cisco Catalyst C9407R*, ya que dispone de un total de 7 slots de los cuales son 2 para las supervisoras y 5 slots para puertos ^[51].



FIGURA 4.28: Cisco Catalyst C9407R

De acuerdo con el número de puertos, vamos a necesitar 5 módulos del tipo *Cisco C9400-LC-48T* ya que dispone de un total de 48 puertos cada uno de ellos, lo que nos resulta un total de 240 puertos, por lo que nos sobrarían 30 puertos para ampliaciones ^[52].



FIGURA 4.29: Cisco C9400-LC-48T

En este módulo irán conectadas las antenas y los usuarios finales desde sus tomas. Para la conexión entre el Switch de acceso y el Switch Core usaremos la supervisora *Cisco C9400-SUP-1XL/2* ^[53].



FIGURA 4.30: Cisco C9400-SUP-1XL/2

Este modelo dispone de puertos a los que añadir los SFPs de fibra para realizar las conexiones entre los Switches de acceso con el Switch Core.

Por último, en este modelo de Switch se pueden añadir hasta un máximo de 8 fuentes de alimentación del modelo *3200W AC*.

4.2.2.2.3. Tabla Resumen Red LAN

En la siguiente tabla podemos contemplar el presupuesto en función de los dispositivos que necesitamos en las distintas oficinas incluyendo los dispositivos frontera que forman la unión con el resto de las oficinas a través de la MPLS ^[48].

SERVICIO	CANTIDAD	PRECIO UNIT	PRECIO TOTAL
Cisco C9500-40X-A	6	23.675,52€	142.053,12€
PWR-C4-950WAC-R	6	1.814,55€	10.887,30€
SFP-10G-SR	48	865,45€	41.541,60€
GLC-T1000Base-T	20	382,71€	7.654,20€
Cisco Catalyst C9407R	8	4.406,76€	35.254,08€
Cisco C9400-LC-48T	40	6.169,46€	246.778,40€
Cisco C9400-SUP-1XL/2	16	16.745,68€	267.930,88€
			TOTAL: 752.099,58€

TABLA 4.15: Desglose final Red LAN

4.2.2.3.2. Dimensionado de la Red Wifi

Para la realización del dimensionado de nuestra arquitectura de red WiFi hay que establecer una serie de requisitos iniciales que necesitamos para poder seleccionar el número total de dispositivos, así como el tipo y modelo de ellos. Este paso es muy importante debido a que, si se cometen errores en la toma de datos, se irán incrementando a medida que se van realizando los pasos correspondientes en el dimensionado. En la toma de datos debemos tener en cuenta tres puntos importantes:

- **Tipo de Servicio:** consiste en determinar los servicios que puede soportar nuestra arquitectura. Existen dos tipos de servicio:
 - Diseño basado en cobertura: se centra en maximizar los niveles de cobertura intentando cubrir el máximo área posible.
 - Diseño basado en capacidad: se centra en llevar a cabo un diseño en capacidad. Para ello se debe hacer un uso de mayor densidad de puntos de acceso para cubrir el mayor espacio posible.

Para nuestra red, tenemos que tener en cuenta que necesitamos una red que soporte aplicaciones, vídeos y VoIP por lo que, es recomendable emplear el segundo diseño para dar soporte a todo tipo de tráfico. Gracias a nuestra herramienta de Aruba, conseguiremos determinar el número de puntos de accesos para cubrir todo el espacio de cada planta.

- **Ubicación electrónica de Red:** consiste en determinar la posición de los diferentes puntos de acceso y distribuirlos por toda la planta de la mejor manera posible. Una vez colocados, se ubicarán en el techo de la oficina y se conectarán a los switches de acceso para que los controladores puedan gestionar la información transmitida por los puntos de acceso.
- **Planos y diagramas de la superficie:** consiste en integrar los puntos de acceso en el plano de las plantas de cada una de las oficinas. En nuestro caso, se usará la oficina de Boadilla ya que será aplicado del mismo modo en el resto de ellas.

Dispositivos:

- SERVIDOR ARUBA AIRWAVE

Para la administración de las antenas se emplea el servidor *Aruba AW-HW630-ENT* el cual emplea una interface bastante intuitiva a la hora de establecer la configuración del resto de dispositivos.



FIGURA 4.32: Aruba AirWave AW-HW630-ENT

- ANTENAS (ACCESS POINT)

Una vez establecido el dimensionado de cada una de las oficinas a través del servidor de AirWave, calculamos que se necesitan un total de 12 antenas por planta en cada oficina. Las antenas seleccionadas son *Aruba AP 335* las cuales son de última generación y dan soporte para cubrir todas nuestras necesidades ^[54].



FIGURA 4.33: Aruba AP 335

- CONTROLADOR (WIRELESS CONTROLLER)

Este dispositivo se encarga de recibir la información transmitida por los puntos de accesos para poder enviarla al servidor donde se gestiona toda la información. En las oficinas de Boadilla y Villaverde, al disponer de 3 plantas, necesitaremos un total de 36 antenas, mientras que en la oficina de Castilla necesitaremos 24. En el CPD, al ser una oficina con muy pocos usuarios, nos sirve una única antena ^[55].

Para las dos oficinas de 36 antenas usaremos el *Aruba 7030 Mobility Controller* ya que permite un total de 64 AP, mientras que el anterior modelo se queda en 32. Por ello, ese modelo anterior nos sirve para la oficina de Castilla de 24 antenas en total. El modelo sería *Aruba 7024 Mobility Controller* ^[56].

PERFORMANCE AND CAPACITY		
Features	7024	7030
Maximum campus AP licenses	32	64
Maximum remote AP licenses	32	64
Maximum concurrent users/devices	2,048	4,096
Maximum VLANs	4,094	4,094
Active firewall sessions	32,768	65,536
Concurrent GRE tunnels	512	1,024
Concurrent IPsec sessions	1,024	2,048
Mobility Access Switch tunneled-node ports	1,024	2,048
Firewall throughput	4 Gbps	8 Gbps
Encrypted throughput (3DES, AES-CBC)	2.4 Gbps	2.4 Gbps
Encrypted throughput (AES-CCM)	3.4 Gbps	4.0 Gbps

TABLA 4.16: Prestaciones Wireless Controller



FIGURA 4.34: Aruba Controller 7030



FIGURA 4.35: Aruba Controller 7024

4.2.2.3.3. Tabla Resumen red WiFi

En la siguiente tabla podemos contemplar el presupuesto en función de los dispositivos que necesitamos en las distintas oficinas para la gestión y administración de la red WiFi de cada una de ellas ^[48].

SERVICIO	CANTIDAD	PRECIO UNIT	PRECIO TOTAL
Aruba AW-HW630-ENT	1	56.953,86€	56.953,86€
Aruba AP 335	97	1.478,81€	143.444,57€
Aruba 7030 Mobility Controller	2	9.592,64€	19.185,28€
Aruba 7024 Mobility Controller	1	6.539,05€	6.539,05€
			TOTAL: 226.122,76€

TABLA 4.17: Desglose final Red WiFi

4.2.3. Desglose de Presupuesto Final

El presupuesto final para todas las partes implicadas en la infraestructura de red de la empresa sería la siguiente:

TIPO DE ARQUITECTURA	PRESUPUESTO FINAL
RED DE VOZ	851.824€
RED WAN	572.018,2€
RED LAN	752.099,58€
RED WiFi	226.122,76€
TOTAL: 2.402.064,54€	

TABLA 4.18: Desglose Final

4.3. Plan de Direccionamiento

Nuestro Proyecto va a estar dividido en dos partes diferenciadas, una de ellas irá encargadas para proyectos y clientes, para las que utilizaremos redes privadas de clase B (**172.16.0.0/12**) y otra parte dedicada para todos los temas corporativos dentro de nuestra empresa como sean los propios usuarios, los servidores, la WiFi, etc. Para estos últimos, se emplearán redes de clase A (**10.0.0.0/8**).

Para la conexión para salir a internet, emplearemos redes públicas. Ya que se debería de tener contacto con el proveedor para esa asignación de redes públicas, nosotros emplearemos redes de públicas de clase B (**215.27.140.0/24**) y para las conexiones con el proveedor para la MPLS utilizaremos redes privadas de clase C (**192.168.0.0/16**).

Debido a que cada una de las oficinas, dispondrán de nivel 3 propio, se podrán utilizar los mismos id's de VLAN's para cada oficina. Esto servirá para identificar a que pertenece cada una de ellas. Todas las oficinas dispondrán de:

- VLAN de usuarios – (VLAN 10).
- VLAN de gestión de dispositivos de equipos (VLAN 11).
- VLAN de servidores (VLAN 12).
- VLAN de impresoras (VLAN 13).
- VLAN de seguridad (VLAN 14).
- VLAN de red WiFi (VLAN 20).
- VLAN de gestión de dispositivos WiFi (VLAN 21).
- VLAN de voz (VLAN 30).

NOMBRE	ID	RED	MÁSCARA
Vlan de Usuarios	10	10.10.0.0	255.255.252.0
Vlan de gestión de equipos	11	10.10.4.0	255.255.255.240
Vlan de servidores	12	10.10.4.16	255.255.255.240
Vlan de impresoras	13	10.10.4.32	255.255.255.224
Vlan de seguridad	14	10.10.4.64	255.255.255.224
Vlan de red WiFi	20	10.10.20.0	255.255.252.0
Vlan de gestión de WiFi	21	10.10.24.0	255.255.255.192
Vlan de voz	30	10.10.30.0	255.255.254.0

TABLA 4.19: Redes para oficina Boadilla

NOMBRE	ID	RED	MÁSCARA
Vlan de Usuarios	10	10.20.0.0	255.255.252.0
Vlan de gestión de equipos	11	10.20.4.0	255.255.255.240
Vlan de servidores	12	10.20.4.16	255.255.255.240
Vlan de impresoras	13	10.20.4.32	255.255.255.224
Vlan de seguridad	14	10.20.4.64	255.255.255.224
Vlan de red WiFi	20	10.20.20.0	255.255.252.0
Vlan de gestión de WiFi	21	10.20.24.0	255.255.255.192
Vlan de voz	30	10.20.30.0	255.255.254.0
Vlan ejemplo Cliente	200	172.16.0.0	255.255.255.0

TABLA 4.20: Redes para oficina Villaverde

NOMBRE	ID	RED	MÁSCARA
Vlan de Usuarios	10	10.30.0.0	255.255.254.0
Vlan de gestión de equipos	11	10.30.2.0	255.255.255.240
Vlan de servidores	12	10.30.2.16	255.255.255.240
Vlan de impresoras	13	10.30.2.32	255.255.255.224
Vlan de seguridad	14	10.30.2.64	255.255.255.224
Vlan de red WiFi	20	10.30.20.0	255.255.254.0
Vlan de gestión de WiFi	21	10.30.22.0	255.255.255.192
Vlan de voz	30	10.30.30.0	255.255.254.0

TABLA 4.21: Redes para oficina Castilla

NOMBRE	ID	RED	MÁSCARA
Vlan de Usuarios	10	10.40.0.0	255.255.255.240
Vlan de gestión de equipos	11	10.40.0.16	255.255.255.240
Vlan de servidores	12	10.40.1.0	255.255.255.0
Vlan de impresoras	13	10.40.0.32	255.255.255.248
Vlan de seguridad	14	10.40.0.40	255.255.255.248
Vlan de red WiFi	20	10.40.20.0	255.255.255.128
Vlan de gestión de WiFi	21	10.40.20.128	255.255.255.192
Vlan de voz	30	10.40.30.0	255.255.255.240

TABLA 4.21: Redes para oficina Henares

4.4. Simulación

Para representar la solución propuesta, voy a realizar una simulación en el programa Packet Tracer con equipos virtuales. Debido a que el programa no dispone de los modelos seleccionados, se intentará realizar las pruebas con equipos similares. Para ello se establece el siguiente diagrama con la siguiente tabla de direccionamiento acorde al plan propuesto en el punto anterior.

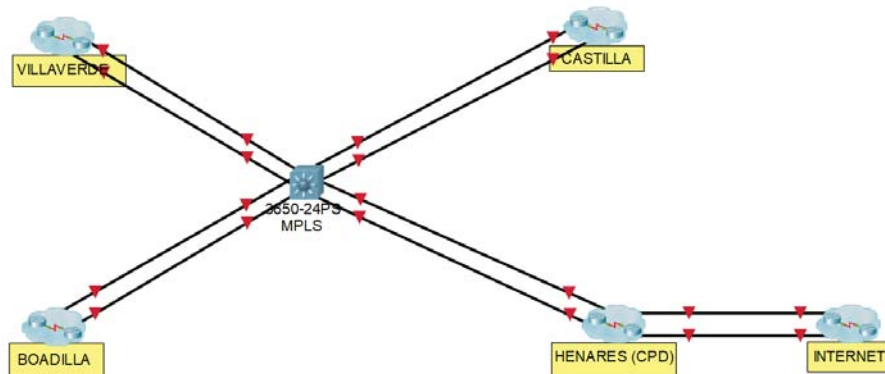


FIGURA 4.36: Diagrama de la empresa

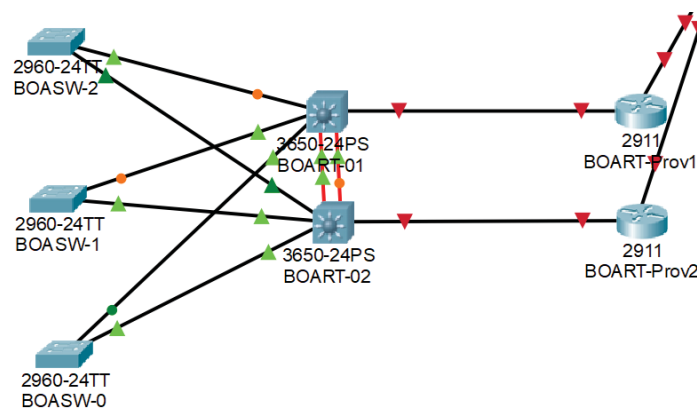


FIGURA 4.37: Diagrama de cualquier oficina

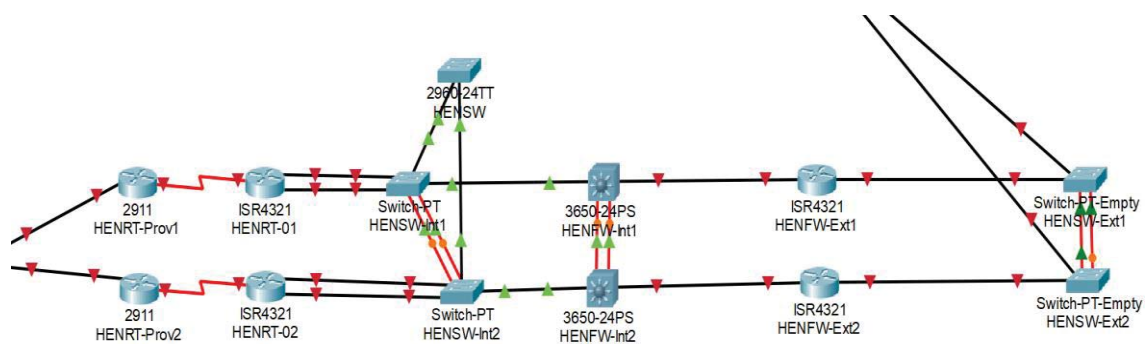


FIGURA 4.38: Diagrama del CPD

Como se puede observar, los firewalls son empleados por routers dentro de la simulación debido a que no voy a contemplar ningún método de seguridad.

TABLA DE DIRECCIONAMIENTO

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
BOART-01	Vlan 10	10.10.0.1	255.255.252.0	
	Vlan 11	10.10.4.1	255.255.255.240	
	Vlan 12	10.10.4.17	255.255.255.240	
	Vlan 13	10.10.4.33	255.255.255.224	
	Vlan 14	10.10.4.65	255.255.255.224	
	Vlan 20	10.10.20.1	255.255.252.0	
	Vlan 21	10.10.24.1	255.255.255.192	
	Vlan 30	10.10.30.1	255.255.254.0	
	Vlan 99	192.168.10.1	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/0/3	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		
BOART-02	Vlan 10	10.10.0.2	255.255.252.0	
	Vlan 11	10.10.4.2	255.255.255.240	
	Vlan 12	10.10.4.18	255.255.255.240	
	Vlan 13	10.10.4.34	255.255.255.224	
	Vlan 14	10.10.4.66	255.255.255.224	
	Vlan 20	10.10.20.2	255.255.252.0	
	Vlan 21	10.10.24.2	255.255.255.192	

	Vlan 30	10.10.30.2	255.255.254.0	
	Vlan 99	192.168.10.2	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/0/3	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		
BOASW-0	Gi0/1	Trunk		
	Gi0/2	Trunk		
BOASW-1	Gi0/1	Trunk		
	Gi0/2	Trunk		
BOASW-2	Gi0/1	Trunk		
	Gi0/2	Trunk		
BOART-Prov1	Gi0/0/0	192.168.10.4	255.255.255.248	
BOART-Prov2	Gi0/0/0	192.168.10.5	255.255.255.248	

TABLA 4.22: Tabla Direccionamiento Boadilla

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
VILRT-01	Vlan 10	10.20.0.1	255.255.252.0	
	Vlan 11	10.20.4.1	255.255.255.240	
	Vlan 12	10.20.4.17	255.255.255.240	
	Vlan 13	10.20.4.33	255.255.255.224	
	Vlan 14	10.20.4.65	255.255.255.224	
	Vlan 20	10.20.20.1	255.255.252.0	

	Vlan 21	10.20.24.1	255.255.255.192	
	Vlan 30	10.20.30.1	255.255.254.0	
	Vlan 99	192.168.20.1	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/0/3	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		
VILRT-02	Vlan 10	10.20.0.2	255.255.252.0	
	Vlan 11	10.20.4.2	255.255.255.240	
	Vlan 12	10.20.4.18	255.255.255.240	
	Vlan 13	10.20.4.34	255.255.255.224	
	Vlan 14	10.20.4.66	255.255.255.224	
	Vlan 20	10.20.20.2	255.255.252.0	
	Vlan 21	10.20.24.2	255.255.255.192	
	Vlan 30	10.20.30.2	255.255.254.0	
	Vlan 99	192.168.20.2	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/0/3	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		

VILSW-0	Gi0/1	Trunk		
	Gi0/2	Trunk		
VILSW-1	Gi0/1	Trunk		
	Gi0/2	Trunk		
VILSW-2	Gi0/1	Trunk		
	Gi0/2	Trunk		
VILRT-Prov1	Gi0/0/0	192.168.20.4	255.255.255.248	
VILRT-Prov2	Gi0/0/0	192.168.20.5	255.255.255.248	

TABLA 4.23: Tabla Direccionamiento Villaverde

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
CASRT-01	Vlan 10	10.30.0.1	255.255.254.0	
	Vlan 11	10.30.2.1	255.255.255.240	
	Vlan 12	10.30.2.17	255.255.255.240	
	Vlan 13	10.30.2.33	255.255.255.224	
	Vlan 14	10.30.2.65	255.255.255.224	
	Vlan 20	10.30.20.1	255.255.254.0	
	Vlan 21	10.30.22.1	255.255.255.192	
	Vlan 30	10.30.30.1	255.255.254.0	
	Vlan 99	192.168.30.1	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		

CASRT-02	Vlan 10	10.30.0.2	255.255.254.0	
	Vlan 11	10.30.2.2	255.255.255.240	
	Vlan 12	10.30.2.18	255.255.255.240	
	Vlan 13	10.30.2.34	255.255.255.224	
	Vlan 14	10.30.2.66	255.255.255.224	
	Vlan 20	10.30.20.2	255.255.254.0	
	Vlan 21	10.30.22.2	255.255.255.192	
	Vlan 30	10.30.30.2	255.255.254.0	
	Vlan 99	192.168.30.2	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/0/2	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Acceso		
CASSW-0	Gi0/1	Trunk		
	Gi0/2	Trunk		
CASSW-1	Gi0/1	Trunk		
	Gi0/2	Trunk		
CASSW-2	Gi0/1	Trunk		
	Gi0/2	Trunk		
CASRT-Prov1	Gi0/0/0	192.168.30.4	255.255.255.248	
CASRT-Prov2	Gi0/0/0	192.168.30.5	255.255.255.248	

TABLA 4.23: Tabla Direccionamiento Castilla

Dispositivo	Interfaz	Dirección IP	Máscara	Gateway
HENRT-01	Gi0/0/0.10	10.40.0.1	255.255.255.240	
	Gi0/0/0.11	10.40.0.17	255.255.255.240	
	Gi0/0/1.12	10.40.1.1	255.255.255.0	
	Gi0/0/0.13	10.40.0.33	255.255.255.248	
	Gi0/0/0.14	10.40.0.41	255.255.255.248	
	Gi0/0/0.20	10.40.20.1	255.255.255.128	
	Gi0/0/0.21	10.40.20.129	255.255.255.192	
	Gi0/0/0.30	10.40.30.1	255.255.255.240	
	Gi0/1/0	192.168.40.1	255.255.255.248	
	Gi0/0/1.98	192.168.40.9	255.255.255.248	
HENRT-02	Gi0/0/0.10	10.40.0.2	255.255.255.240	
	Gi0/0/0.11	10.40.0.18	255.255.255.240	
	Gi0/0/1.12	10.40.1.2	255.255.255.0	
	Gi0/0/0.13	10.40.0.34	255.255.255.248	
	Gi0/0/0.14	10.40.0.42	255.255.255.248	
	Gi0/0/0.20	10.40.20.2	255.255.255.128	
	Gi0/0/0.21	10.40.20.130	255.255.255.192	
	Gi0/0/0.30	10.40.30.2	255.255.255.240	
	Gi0/1/0	192.168.40.2	255.255.255.248	
	Gi0/0/1.98	192.168.40.10	255.255.255.248	
HENSW-Int1	Gi0/1	Trunk		
	Gi1/1	Trunk		
	Gi2/1	Trunk		

	Gi3/1	Trunk		
	Gi8/1	Trunk		
	Gi9/1	Trunk		
HENSW-Int2	Gi0/1	Trunk		
	Gi1/1	Trunk		
	Gi2/1	Trunk		
	Gi3/1	Trunk		
	Gi8/1	Trunk		
	Gi9/1	Trunk		
HENSW	Gi0/1	Trunk		
	Gi0/2	Trunk		
HENSW-Ext1	Gi0/1	Trunk		
	Gi7/1	Trunk		
	Gi8/1	Trunk		
	Gi9/1	Trunk		
HENSW-Ext2	Gi0/1	Trunk		
	Gi7/1	Trunk		
	Gi8/1	Trunk		
	Gi9/1	Trunk		
HENFW-Ext1	Gi0/0/0	215.27.140.4	255.255.255.248	
	Gi0/0/1	215.27.140.9	255.255.255.248	
HENFW-Ext2	Gi0/0/0	215.27.140.5	255.255.255.248	
	Gi0/0/1	215.27.140.10	255.255.255.248	
HENFW-Int1	Vlan 97	192.168.40.13	255.255.255.248	

	Vlan 96	215.27.140.1	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Trunk		
HENFW-Int2	Vlan 97	192.168.40.14	255.255.255.248	
	Vlan 96	215.27.140.2	255.255.255.248	
	Gi1/0/1	Trunk		
	Gi1/1/1	Trunk		
	Gi1/1/2	Trunk		
	Gi1/0/24	Trunk		
HENRT-Prov1	Gi0/0/0	192.168.40.4	255.255.255.248	
HENRT-Prov2	Gi0/0/0	192.168.40.5	255.255.255.248	

TABLA 4.23: Tabla Direccionamiento Castilla

A continuación, se conectarán varios equipos a la simulación empleando un escenario ficticio de los usuarios conectados en cada puesto de la oficina y unos cuantos servidores tanto por el lado de una oficina como en el lado del centro de datos.

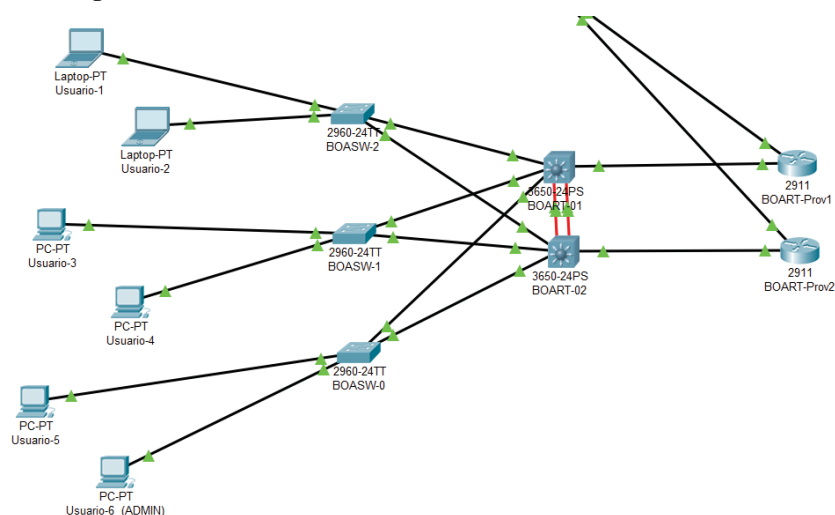


FIGURA 4.39: Diagrama Oficina Boadilla

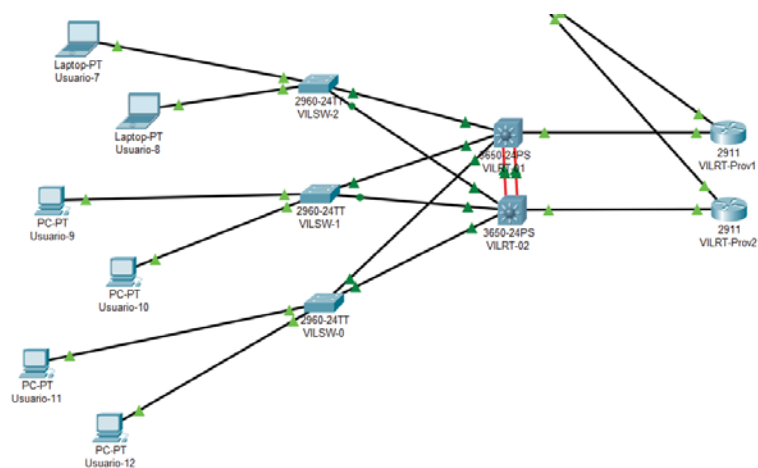


FIGURA 4.40: Diagrama Oficina Villaverde

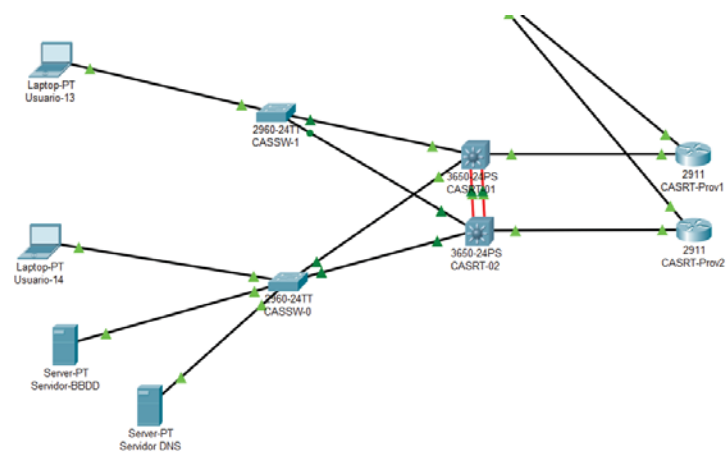


FIGURA 4.41: Diagrama Oficina Castilla

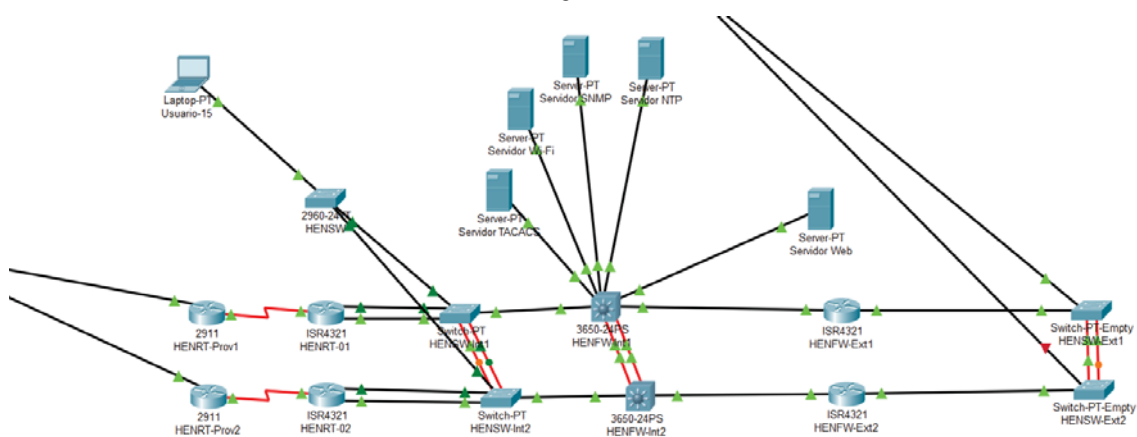
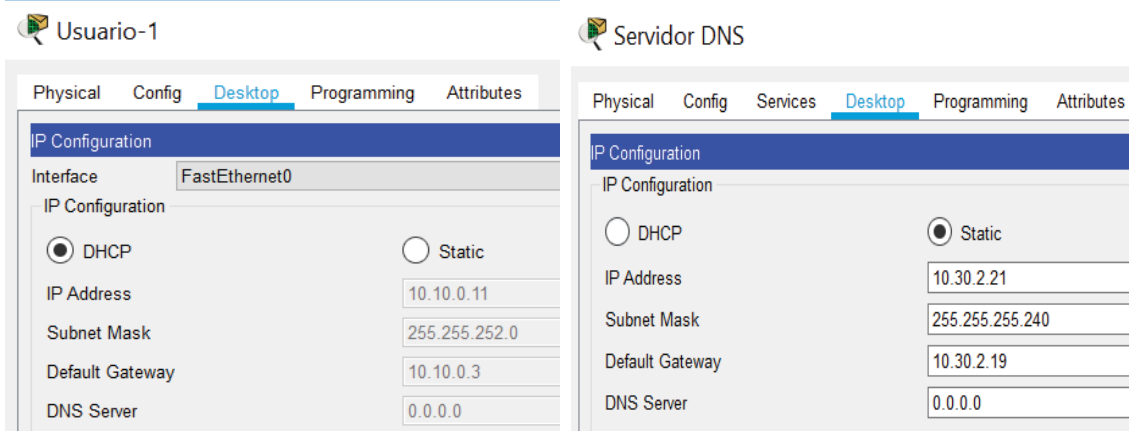


FIGURA 4.42: Diagrama Oficina Henares

Una vez conectados varios equipos en las diferentes oficinas, se van a realizar unas series de pruebas para comprobar que existe conectividad entre las distintas oficinas, así como varias pruebas especificando los dispositivos que tengan permisos y los que no para probar la propia seguridad de la empresa.

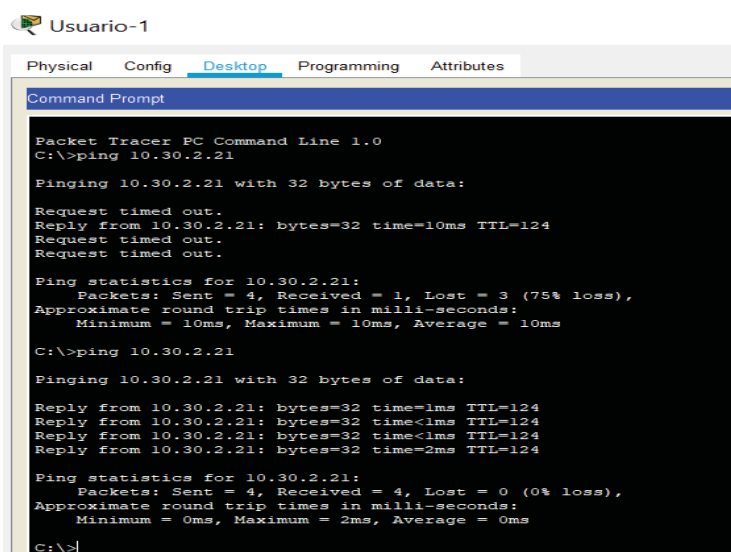
Las pruebas realizadas para la comprobación son las siguientes:

- **ACCESO DE UN USUARIO A UN SERVIDOR DE OTRA OFICINA**



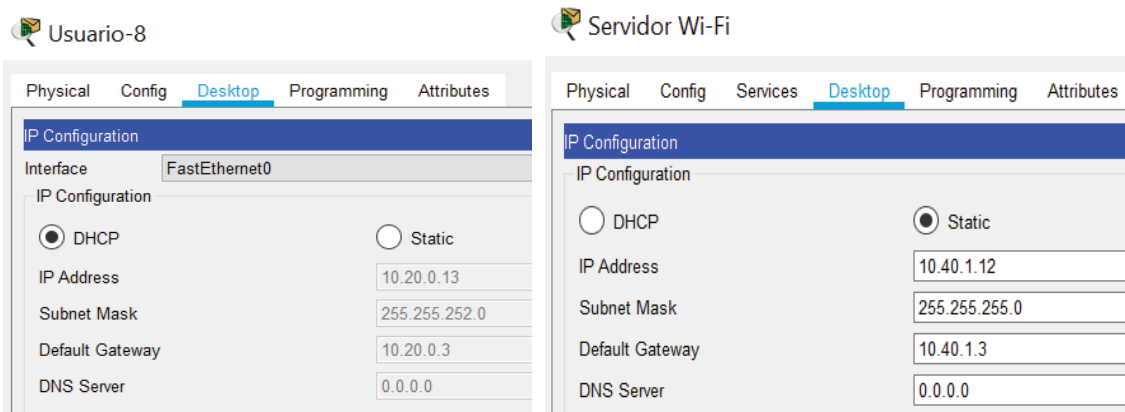
Para esta prueba, escogemos un usuario que se encuentra en la oficina de Boadilla, que recibe a través del DHCP una ip de la vlan de usuarios indicada en la tabla de direccionamiento (10.10.0.11) y se desea conectar a un servidor que se localiza en la oficina de Castilla, por lo que asignamos una ip estática al servidor de la vlan de servidores (10.30.2.21) correspondiente a esa oficina. Al servidor se la indicamos de manera estática debido a que no puede cambiar dicha ip, siempre debe tener la misma.

Para realizar la prueba, haremos un ping desde dicho usuario hasta el servidor.



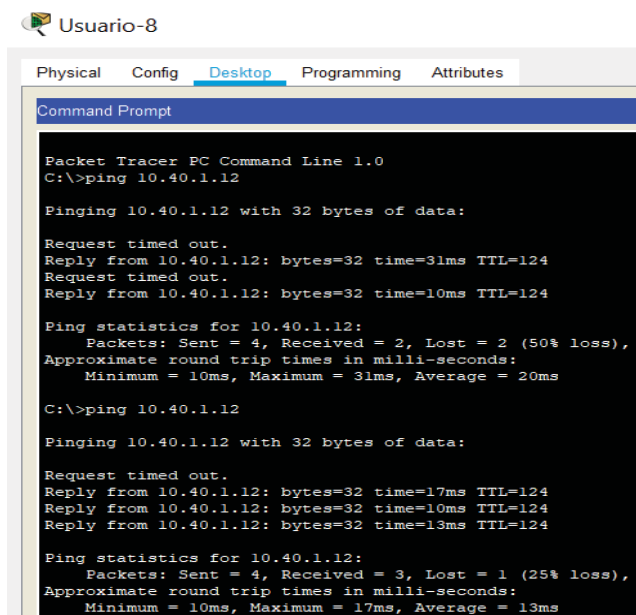
Realizamos la prueba dos veces, debido que la primera nos da un resultado de 3 timeout, con 1 sola respuesta positiva, debido a que las primeras peticiones son de establecer la conexión. Sin embargo, observamos que en la segunda prueba se consigue un 100% de éxito en las 4 peticiones que se realizan

- **ACCESO DE UN USUARIO A UN SERVIDOR DEL CENTRO DE DATOS**



Para esta prueba, escogemos un usuario que se encuentra en la oficina de Villaverde, que recibe a través del DHCP una ip de la vlan de usuarios indicada en la tabla de direccionamiento (10.20.0.13) y se desea conectar a un servidor que se localiza en la oficina de Castilla, por lo que asignamos una ip estática al servidor de la vlan de servidores (10.40.1.12) correspondiente a esa oficina. Al servidor se la indicamos de manera estática debido a que no puede cambiar dicha ip, siempre debe tener la misma.

Para realizar la prueba, haremos un ping desde dicho usuario hasta el servidor.



Realizamos la prueba dos veces, debido que la primera nos da un resultado de 2 timeout, con 2 respuestas positivas, debido a que las primeras peticiones son de establecer la conexión. Sin embargo, observamos que en la segunda prueba se consigue un 75% de éxito en las 4 peticiones que se realizan por lo que se garantiza el acceso al servidor.

- **ACCESO DE UN USUARIO A INTERNET**

Usuario-3

ISPPC

Para esta prueba, escogemos un usuario que se encuentra en la oficina de Boadilla, que recibe a través del DHCP una ip de la vlan de usuarios indicada en la tabla de direccionamiento (10.10.0.15) y se desea conectar a internet. Como internet he seleccionado un equipo que tiene la ip (215.27.140.20) para poder simular la conectividad.

Para realizar la prueba, haremos un ping desde dicho usuario hasta el servidor.

Usuario-3

```
C:\>ping 215.27.140.20

Pinging 215.27.140.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 215.27.140.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 215.27.140.20

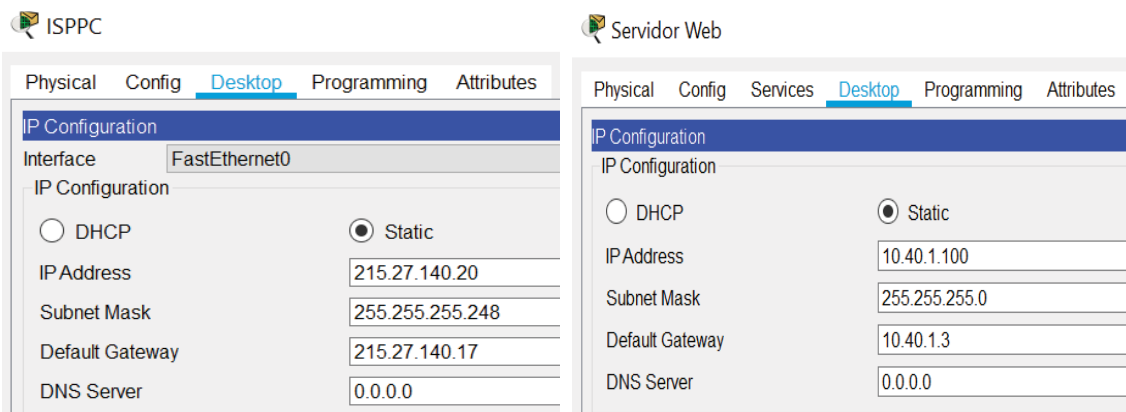
Pinging 215.27.140.20 with 32 bytes of data:

Reply from 215.27.140.20: bytes=32 time=2ms TTL=121
Request timed out.
Reply from 215.27.140.20: bytes=32 time=22ms TTL=121
Reply from 215.27.140.20: bytes=32 time=24ms TTL=121

Ping statistics for 215.27.140.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 24ms, Average = 16ms
```

Realizamos la prueba dos veces, debido que la primera nos da un resultado de 2 timeout, con 0 respuestas positivas, debido a que las primeras peticiones son de establecer la conexión. Sin embargo, observamos que en la segunda prueba se consigue un 75% de éxito en las 4 peticiones que se realizan por lo que se garantiza el acceso a internet.

- **ACCESO DESDE INTERNET A UN SERVIDOR DE PRODUCCIÓN**



Para la realización de esta prueba escogemos un usuario que se encuentra en internet por lo que dispone de una ip pública (215.27.140.20) y se quiere conectar a un servidor web de producción. Este servidor tiene una ip privada, sin embargo, el usuario no podrá conectarse a dicho servidor a través de su ip privada, por lo que realizamos un NAT (network address translation) para poder establecer una ip pública, la cual será accesible desde internet para evitar ataques a nuestra red. La ip será (215.27.140.129).

Para realizar la prueba, haremos un ping desde dicho usuario hasta el servidor.

```

Packet Tracer PC Command Line 1.0
C:\>ping 10.40.1.100

Pinging 10.40.1.100 with 32 bytes of data:
Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.

Ping statistics for 10.40.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 215.27.140.129

Pinging 215.27.140.129 with 32 bytes of data:
Request timed out.
Reply from 215.27.140.129: bytes=32 time=11ms TTL=124
Reply from 215.27.140.129: bytes=32 time=20ms TTL=124
Reply from 215.27.140.129: bytes=32 time=12ms TTL=124

Ping statistics for 215.27.140.129:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 20ms, Average = 14ms
  
```

Como podemos ver, si lanzamos el ping al servidor con la ip privada (primer comando) el resultado es “Destination host unreachable” debido a que no se puede acceder a dicho servidor por esa dirección. Sin embargo, si se lanza el ping a la ip pública indicada, podemos acceder sin problema (perdemos el primero debido a que hay que establecer la conexión).

- **CONECTARSE A UN EQUIPO POR SSH**

Usuario-10

Para esta prueba elegimos un usuario que está conectado en la oficina de Villaverde a la vlan de usuarios con la ip (10.20.0.16). Probamos a establecer la conexión por ssh a cualquier dispositivo siempre y cuando esté gestionado por nuestra empresa, es decir, los routers de los proveedores no son gestionados por nosotros. Seleccionamos el router de la oficina de Castilla (CASRT-01) para acceder a él. Para ello escogemos cualquiera de sus ips, en nuestro caso la de gestión que pertenece a su vlan de gestión (10.30.2.1)

Usuario-10

Usuario-10

Como Podemos observar, establece correctamente la conexión

- **ACCESO POR SSH A UN EQUIPO NO PERMITIDO**

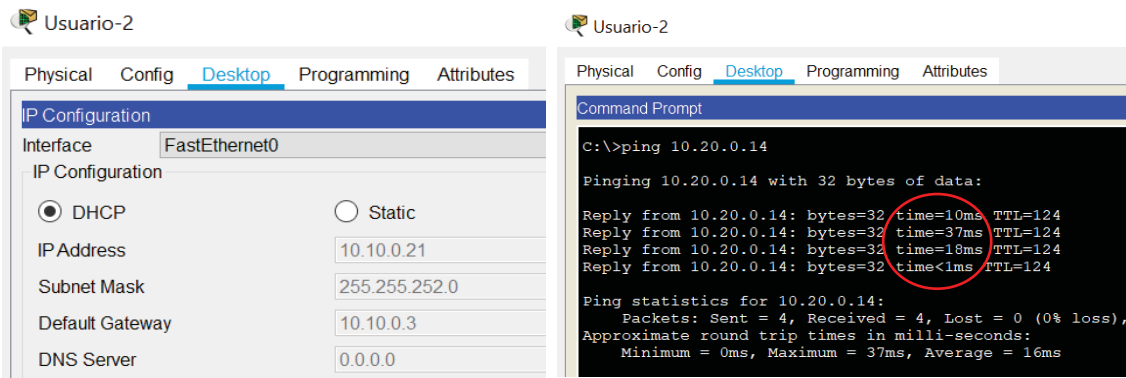
Sin embargo si realizamos la misma prueba a un equipo que no tenemos acceso por ssh, ya que pertenecen a los proveedores, no podemos conectarnos a ninguno de ellos. Si tomamos como ejemplo el CASRT-Prov1, como router del proveedor de la misma oficina con la ip de gestión (192.168.130.3) obtenemos lo siguiente:

Usuario-10

Usuario-10

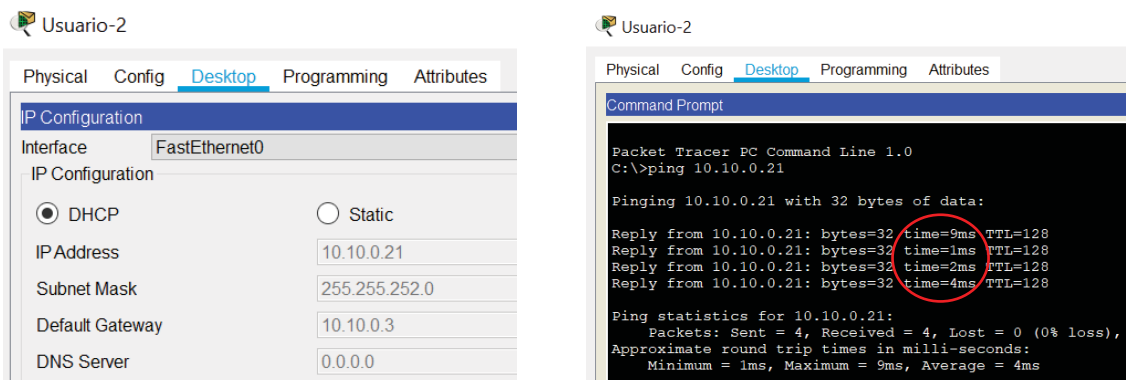
Por lo que se deniega el acceso

- **TIEMPO EN REALIZAR UN PING A UN EQUIPO ENTRE 2 OFICINAS**



Para la realización de esta prueba, usaremos a un usuario de la oficina de Boadilla con la ip (10.10.0.21) de la vlan de usuarios y queremos conectarnos a un usuario de la ip de la vlan de usuarios de la oficina de Villaverde (10.20.0.14). Vemos que la conectividad se hace sin problema, pero son tiempos un poco altos dentro de la normalidad debida a la distancia que existe entre ellas.

- **TIEMPO EN REALIZAR UN PING A UN EQUIPO MISMA OFICINA**



Si realizamos un ping desde este usuario de la oficina de Boadilla a un dispositivo que se localiza en su misma oficina, obtenemos que los tiempos de acceso son bastante inferiores a los de un acceso a un usuario de otra oficina, debido a que las distancias son menores.

- **ACCESO A UN SERVIDOR NO PERMITIDO**

Finalmente, elegimos un servidor de los que consideramos internos al cual nos queremos conectar desde el usuario de internet (215.27.140.20).

ISPPC

Physical	Config	Desktop	Programming	Attributes
IP Configuration				
Interface: FastEthernet0				
IP Configuration				
<input type="radio"/> DHCP <input checked="" type="radio"/> Static				
IP Address: 215.27.140.20				
Subnet Mask: 255.255.255.248				
Default Gateway: 215.27.140.17				
DNS Server: 0.0.0.0				

Servidor Wi-Fi

Physical	Config	Services	Desktop	Programming	Attributes
IP Configuration					
IP Configuration					
<input type="radio"/> DHCP <input checked="" type="radio"/> Static					
IP Address: 10.40.1.12					
Subnet Mask: 255.255.255.0					
Default Gateway: 10.40.1.3					
DNS Server: 0.0.0.0					

Para ello realizamos un ping a la ip privada del servidor, debido a que no se realiza ningún NAT a esa ip, ya que no tiene que estar accesible desde internet, que sólo sea accesible desde las redes internas de la empresa.

ISPPC

```

C:\>ping 10.40.1.12

Pinging 10.40.1.12 with 32 bytes of data:

Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.
Reply from 192.168.40.10: Destination host unreachable.

Ping statistics for 10.40.1.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
  
```

Como observamos en el resultado, obtenemos el mensaje “Destination host unreachable”, lo cual indica que el acceso está denegado.

Capítulo 5: Conclusión

El proyecto se ha basado fundamentalmente en la experiencia laboral adquirida durante un año en una empresa de servicios que diseña, implementa y da soporte a soluciones reales de comunicaciones, en escenarios reales de empresa.

Su objetivo principal ha sido la elaboración de una arquitectura de red empresarial actual. Para ello hemos realizado el diseño de la red de telefonía y de la red de datos en cada una de las sedes con las que cuenta nuestra empresa distribuidas en distintos puntos geográficos.

Uno de los puntos más interesantes que se pueden comentar en la realización de este proyecto ha sido cómo mediante un determinado diseño de red se puede diferenciar el perfil de cada uno de los usuarios dando más capacidad a unos que a otros según el trabajo que desempeñen dentro de la empresa.

En cuanto a las aportaciones este proyecto explica paso a paso como podemos realizar el diseño de una red empresarial y que criterios he ido siguiendo en cada una de las partes que lo componen.

Los requisitos de entrada para llevarlo a cabo también están incluidos dentro de él lo que hace que pueda utilizarse de base para cualquier tipo de diseño que se quiera implementar.

Tras la finalización del proyecto, me he dado cuenta de los numerosos campos que hay que tener en cuenta a la hora de dimensionar una empresa para que todo quede de la forma más segura posible. He cumplido cada uno de los objetivos, ya que he recopilado bastante información de todos los campos para finalizar el proyecto.

He disfrutado durante la realización por el hecho de que es un concepto al que me dedico profesionalmente y al que quiero seguir ligado en un futuro aumentando mis conocimientos.

Siento que me he quedado con las ganas en la carrera de haber tenido más asignaturas enfocadas a este campo ya que es la rama de la informática que más me ha llamado la atención, sin embargo, solo he dispuesto de la asignatura de Redes de Computadores y de Cisco CCNA: Routing and Switching para irme introduciendo en el temario.

Gracias a mis compañeros de trabajo que me han ayudado a enfocar el trabajo, he podido aumentar dicho conocimiento con las búsquedas de documentación para el proyecto.

Capítulo 6: Futuras Líneas

Este apartado consiste en las posibles ampliaciones que puedan surgir para el proyecto para mejorar el diseño planteado. Evidentemente, siempre se puede mejorar, ya sea para optimizar, para sustitución de dispositivos con mejor rendimiento o para abaratar el diseño en el caso de no disponer un presupuesto tan elevado.

A medida que vayan sacando nuevos equipos, los propuestos quedarán obsoletos, por lo que, en esta sección se podrá añadir los nuevos equipos en un futuro. De esta manera no queda el proyecto con un punto final con solución única, sino que queda abierto a nuevas ideas de mejoras.

Además de los cambios de equipos para seguir renovando la infraestructura, se pueden realizar nuevas tecnologías que puedan dar soporte a nuestra empresa. Esto conlleva realizar un nuevo estudio sobre cómo poder adaptar a las necesidades de la empresa, estas tecnologías.

Una de las nuevas tecnologías que están surgiendo actualmente en el mercado, se trata de la llamada CISCO ACI, que consiste en acoplar los equipos en una plataforma desde la que se gestiona de todo. De este modo la empresa tendrá únicamente los equipos que se encuentren en esta plataforma y allí, se distribuye todo el tráfico por las diferentes oficinas de la empresa.

En cuanto a los posibles cambios dentro de nuestro mismo modelo de infraestructura, se podían incluir nuevos tipos de conexiones como las VPN, las cuales son bastante útiles a la hora de poder trabajar desde cualquier punto sin necesidad de asistir físicamente a la oficina.

Por últimos, si no se desea cambiar nada de la tecnología, ya sea por equipos, por nuevas tecnologías o por nuevas técnicas de comunicación, este proyecto se debe ampliar siempre y cuando nuestra empresa aumentase en número de oficinas, ya que podemos tener en cuenta las oficinas que existen actualmente para tenerlas como referencia para las otras. En el caso de necesitar oficinas que se encuentren fuera de la misma ciudad (MADRID), se puede incluir una nueva MPLS como WAN externa entre las distintas ciudades que dispongan de oficina, y dejar esta MPLS de nuestro proyecto como la encargada de unificar lo que llamaríamos como MAN, ya que sería inferior en extensión que la WAN.

Referencias

- [1] "¿Qué es la telefonía IP? | Quarea.com", Quarea.com, 2018. [Online]. Available: <http://www.quarea.com/es/que-es-telefonía-ip>. [Accessed: 20- Sept- 2018].
- [2] "¿Cuál es la definición del término VoIP (Voice over IP)?", 3CX.es, 2018. [Online]. Available: <https://www.3cx.es/voip-sip/voip-definicion/>. [Accessed: 20- Sept- 2018].
- [3] "Ventajas de la Telefonía IP, ¿Porque utilizar VoIP?", Telefonivozip.com, 2018. [Online]. Available: <http://www.telefonivozip.com/voip/ventajas-de-la-telefonía-ip.htm>. [Accessed: 20- Sept- 2018].
- [4] "Desventajas de la Telefonía IP", Telefonivozip.com, 2018. [Online]. Available: <http://www.telefonivozip.com/voip/desventajas-de-la-telefonía-ip.htm>. [Accessed: 20- Sept- 2018].
- [5] "Protocolos en la Telefonía IP, Protocolos VoIP", Telefonivozip.com, 2018. [Online]. Available: <http://www.telefonivozip.com/voip/protocolos-en-la-telefonía-ip.htm>. [Accessed: 20- Sept- 2018].
- [6] "Protocolo de iniciación de sesión", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Protocolo_de_iniciaci%C3%B3n_de_sesi%C3%B3n. [Accessed: 20- Sept- 2018].
- [7] "Skinny Client Control Protocol", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Skinny_Client_Control_Protocol. [Accessed: 20- Sept- 2018].
- [8] "H.323", Es.wikipedia.org, 2018. [Online]. Available: <https://es.wikipedia.org/wiki/H.323>. [Accessed: 20- Sept- 2018].
- [9] "IAX2", Es.wikipedia.org, 2018. [Online]. Available: <https://es.wikipedia.org/wiki/IAX2>. [Accessed: 20- Sept- 2018].
- [10] "Codecs en la Telefonía IP, Codecs VoIP", Telefonivozip.com, 2018. [Online]. Available: <http://www.telefonivozip.com/voip/codecs-voip.htm>. [Accessed: 27- Sept- 2018].
- [11] "Calidad de servicio", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Calidad_de_servicio. [Accessed: 27- Sept- 2018].
- [12] P. Support, C. Endpoints and C. Series, "Cisco Unified IP Phone 7911G", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7911g/model.html>. [Accessed: 04- Oct- 2018].
- [13] "Definición de red de datos — Definicion.de", Definición.de, 2018. [Online]. Available: <https://definicion.de/red-de-datos/>. [Accessed: 04- Oct- 2018].
- [14] "Redes de área local", CCM, 2018. [Online]. Available: <https://es.ccm.net/contents/295-redes-de-area-local>. [Accessed: 04- Oct- 2018].

- [15] "Cableado estructurado", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Cableado_estructurado. [Accessed: 04- Oct- 2018].
- [16] 2018. [Online]. Available: http://materias.fi.uba.ar/6679/apuntes/CABLEADO_ESTRUC.pdf. [Accessed: 04- Oct- 2018].
- [17] "ACTIVIDAD 5. CABLEADO DE LAS REDES LAN Y WAN 5.1.- CABLEADO LAN 5.2.- CABLEADO WAN", prezi.com, 2018. [Online]. Available: <https://prezi.com/kgts7ndvxyas/actividad-5-cableado-de-las-redes-lan-y-wan-51-cableado-lan-52-cableado-wan/>. [Accessed: 11- Oct- 2018].
- [18] "REDES: CENTRALIZADAS, DESCENTRALIZADAS Y DISTRIBUIDAS", Lapautaqueconecta.blogspot.com, 2018. [Online]. Available: <http://lapautaqueconecta.blogspot.com/2009/08/redes-centralizadas-descentralizadas-y.html>. [Accessed: 11- Oct- 2018].
- [19] 2018. [Online]. Available: http://www.axioma.co.cr/cableado_horizontal.html. [Accessed: 11- Oct- 2018].
- [20] "Cableado estructurado", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Cableado_estructurado. [Accessed: 11- Oct- 2018].
- [21] "Cuartos de Telecomunicaciones", Axioma.co.cr, 2018. [Online]. Available: http://www.axioma.co.cr/cuartos_telecomunicaciones.html. [Accessed: 11- Oct- 2018].
- [22] Garfio Garcia, "Cuarto de equipos", Es.slideshare.net, 2018. [Online]. Available: <https://es.slideshare.net/garfio Garcia/cuarto-de-equipos>. [Accessed: 11- Oct- 2018].
- [23] V. perfil, "cuarto de entrada de servicios", Estructuradorogers.blogspot.com, 2018. [Online]. Available: <http://estructuradorogers.blogspot.com/p/cuarto-de-entrada-de-servicios.html>. [Accessed: 11- Oct- 2018].
- [24] M. Johnatan Zavaleta Milla, "Tecnología inalámbrica - Monografias.com", Monografias.com, 2018. [Online]. Available: <https://www.monografias.com/trabajos37/tecnologia-inalambrica/tecnologia-inalambrica.shtml>. [Accessed: 18- Oct- 2018].
- [25] "Estándares Inalámbricos - EcuRed", Ecured.cu, 2018. [Online]. Available: https://www.ecured.cu/Est%C3%A1ndares_Inal%C3%A1mbricos. [Accessed: 18- Oct- 2018].
- [26] "COMPONENTES DE UNA RED INALAMBRICA", prezi.com, 2018. [Online]. Available: <https://prezi.com/nlvzgl4nmx7/componentes-de-una-red-inalambrica/>. [Accessed: 18- Oct- 2018].
- [27] "Punto de acceso inalámbrico", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico#Funciones. [Accessed: 18- Oct- 2018].

- [28] "Controladores Wifi, su efectividad en la balanza | eConectia", eConectia, 2018. [Online]. Available: <https://www.econectia.com/blog/controladores-wifi-efectividad>. [Accessed: 18- Oct- 2018].
- [29] Arubanetworks.com, 2018. [Online]. Available: https://www.arubanetworks.com/assets/_es/ds/DS_AW.pdf. [Accessed: 18- Oct- 2018].
- [30] "Red de área extensa (WAN) - EcuRed", Ecured.cu, 2018. [Online]. Available: [https://www.ecured.cu/Red_de_%C3%A1rea_extensa_\(WAN\)](https://www.ecured.cu/Red_de_%C3%A1rea_extensa_(WAN)). [Accessed: 24- Oct- 2018].
- [31] "Red privada virtual", Es.wikipedia.org, 2018. [Online]. Available: https://es.wikipedia.org/wiki/Red_privada_virtual. [Accessed: 24- Oct- 2018].
- [32] Cic.puj.edu.co, 2018. [Online]. Available: http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_-_calidad_de_servicio_qos_.pdf. [Accessed: 31- Oct- 2018].
- [33] "¿Qué es un Gateway VoIP? | Quarea.com", Quarea.com, 2018. [Online]. Available: <http://www.quarea.com/es/que-es-un-gateway-voip>. [Accessed: 31- Oct- 2018].
- [34] 2018. [Online]. Available: <http://www.erlang.com/calculator/erlb/>. [Accessed: 31- Oct- 2018].
- [35] P. Support and C. Routers, "Cisco 4351 Integrated Services Router", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/support/routers/4351-integrated-services-router/model.html>. [Accessed: 31- Oct- 2018].
- [36] P. Support and C. Routers, "Cisco 4331 Integrated Services Router", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/support/routers/4331-integrated-services-router-isr/model.html>. [Accessed: 31- Oct- 2018].
- [37] Cnmc.es, 2018. [Online]. Available: https://www.cnmc.es/sites/default/files/1313161_41.pdf. [Accessed: 09- Nov- 2018].
- [38] "Todos los productos de router - Cisco", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/es_mx/products/routers/product-listing.html. [Accessed: 09- Nov- 2018].
- [39] P. Services and C. Routers, "Compare Models ASR 1000 Series Aggregation Services Routers", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/products/routers/asr-1000-series-aggregation-services-routers/models-comparison.html>. [Accessed: 09- Nov- 2018].
- [40] P. Services and C. Routers, "Cisco ASR 1001-HX Router", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/products/routers/asr-1001-hx-router/index.html>. [Accessed: 09- Nov- 2018].

- [41] "Todos los productos de switching", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/es_es/products/switches/product-listing.html. [Accessed: 15- Nov- 2018].
- [42] P. Services, C. Distribution and C. Switches, "Cisco Catalyst 4900M Switch", Cisco, 2018. [Online]. Available: <https://www.cisco.com/c/en/us/products/switches/catalyst-4900m-switch/index.html>. [Accessed: 15- Nov- 2018].
- [43] P. Services, C. Distribution and C. Switches, "Cisco Catalyst 4900M Series", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4900-series-switches/Prod_Bulletin_447737_Cat_4900M-Ex.html. [Accessed: 15- Nov- 2018].
- [44] "SRX Series Networking Firewalls | Juniper Networks", Juniper.net, 2018. [Online]. Available: <https://www.juniper.net/us/en/products-services/security/srx-series/>. [Accessed: 15- Nov- 2018].
- [45] Juniper.net, 2018. [Online]. Available: <https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000551-en.pdf>. [Accessed: 15- Nov- 2018].
- [46] "Next-Generation Firewall - Palo Alto Networks", Paloaltonetworks.com, 2018. [Online]. Available: <https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall>. [Accessed: 26- Nov- 2018].
- [47] "PA-5000 Series - Palo Alto Networks", Paloaltonetworks.com, 2018. [Online]. Available: <https://www.paloaltonetworks.com/products/secure-the-network/next-generation-firewall/pa-5000-series>. [Accessed: 26- Nov- 2018].
- [48] R. Limited, "IT Price | Cisco Global Price List 2018 | HP HPE Price List Tool", Itprice.com, 2018. [Online]. Available: <http://itprice.com/cisco-gpl>. [Accessed: 26- Nov- 2018].
- [49] "Switches de red, switches para LAN y empresariales", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/es_mx/products/switches/index.html#~stickynav=2. [Accessed: 26- Nov- 2018].
- [50] P. Services, C. Distribution, C. Switches and D. Sheets, "Cisco Catalyst 9500 Series Switches Data Sheet", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/data_sheet-c78-738978.html. [Accessed: 26- Nov- 2018].
- [51] P. Services, C. Access, C. Switches and D. Sheets, "Cisco Catalyst 9400 Series Switch Data Sheet", Cisco, 2018. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/data_sheet-c78-739053.html. [Accessed: 26- Nov- 2018].
- [52] P. Services, C. Access, C. Switches and D. Sheets, "Cisco Catalyst 9400 Series Switch Line Cards Data Sheet", Cisco, 2018. [Online]. Available:

- <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-739054.html>. [Accessed: 26- Nov- 2018].
- [53] 2018. [Online]. Available:
<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/datasheet-c78-740209.html>. [Accessed: 06- Dec- 2018].
- [54] Arubanetworks.com, 2018. [Online]. Available:
https://www.arubanetworks.com/assets/ds/DS_AP330Series.pdf. [Accessed: 31- Dec- 2018].
- [55] "Mobility Controllers", Aruba, 2018. [Online]. Available:
<https://www.arubanetworks.com/es/productos/productos-de-red/controladores/>. [Accessed: 06- Dec- 2018].
- [56] Arubanetworks.com, 2018. [Online]. Available:
https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf. [Accessed: 06- Dec- 2018].

Este documento esta firmado por



Firmante	CN=tfgm.fi.upm.es, OU=CCFI, O=Facultad de Informatica - UPM, C=ES
Fecha/Hora	Sun Jan 13 23:41:31 CET 2019
Emisor del Certificado	EMAILADDRESS=camanager@fi.upm.es, CN=CA Facultad de Informatica, O=Facultad de Informatica - UPM, C=ES
Numero de Serie	630
Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)