Universidad del País Vasco Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

GRADO EN INGENIERÍA EN TECNOLOGÍA DE TELECOMUNICACIÓN

# TRABAJO FIN DE GRADO

# *ESTUDIO Y ANÁLISIS DE LOS SERVICIOS PARA LA MEJORA DE UNA RED CORPORATIVA*

**Alumno/Alumna**: CAMPOS GARCÍA, ERIK

**Director/Directora:** IBARROLA ARMENDARIZ, ANA EVA

**Curso:** 2018-2019

**Fecha: Bilbao, 20 de julio de 2019**

# Índice

# Resumen trilingüe

[ES]

Ante la necesidad de rediseñar la infraestructura de la red corporativa de la empresa SATEC, este proyecto persigue establecer los requerimientos para mejorar el rendimiento de las aplicaciones y servicios soportados por la red. Para ello, se desarrolla un estudio de la situación actual para analizar las problemáticas de rendimiento más importantes que hacen que los servicios actuales de la oficina de Bilbao no se den con la calidad suficiente. En base a los resultados de este análisis, se desarrolla un dictamen de las necesidades y requerimientos de las aplicaciones y servicios, que servirá de base para la definición de las especificaciones para el rediseño de la infraestructura de la red.

*Análisis, servicios, aplicaciones, red, corporativa*

[EUS]

SATEC enpresaren sare korporatiboaren azpiegitura berriro diseinatu beharra kontuan hartuta, proiektu honek aplikazioen eta zerbitzuen errendimendua hobetzeko errekerimenduak ezarri nahi ditu. Horretarako, gaur egungo egoeraren inguruko ikasketa bat garatu da, Bilboko bulegoetako egungo zerbitzuen kalitate gabeziaren ondorioz, funtzionamendu-arazo garrantzitsuenak aztertzeko. Analisi honen emaitzen arabera, aplikazioen eta zerbitzuen beharren eta errekerimenduen inguruko irizpena garatzen da, sareko azpiegituraren diseinua zehazteko oinarria.

*Analisia, zerbitzuak, aplikazioak, sarea, korporatibo*

[EN]

Given the need to redesign the infrastructure of SATEC's branch office, this project aims to establish the requirements to improve the performance of the applications and services supported by the network. In order to do this, a study of the current situation is developed to analyze the most important performance problems caused by the insufficient quality of the current services of the office. Based on the results of this analysis, an opinion is developed on the needs and requirements of the applications and services, which will serve as the basis for the definition of the specifications for the redesign of the network infrastructure.

*Analysis, services, applications, network, branch office*

# Lista de ilustraciones



# Lista de tablas

# Acrónimos

| | |
|---|---|
| **AAA** | Authentication, authorization and accounting |
| **CCNA** | Cisco Certified Network Associate |
| **CLI** | Command Line Interface |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DiffServ** | Differentiated services |
| **DNS** | Domain Name System |
| **DSCP** | Differentiated Services Code Point |
| **ESI** | Escuela Superior de Ingeniería |
| **IETF** | Internet Engineering Task Force |
| **IntServ** | Integrated services |
| **IP** | Internet Protocol |
| **IPsec** | Internet Protocol security |
| **ITU-T** | International Telecommunication Union |
| **MIB** | Management Information Base |
| **NAS** | Network Access Server |
| **NAT** | Network Address Translation |
| **NETCONF** | Network Configuration Protocol |
| **NMS** | Network Management Station |
| **OAM** | Operation, administration and management |
| **OSPF** | Open Shortest Path First |
| **PHB** | Per Hop Behavior |
| **PoE** | Power over Ethernet |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **RFC** | Request For Comments |
| **RSVP** | Resource Reservation Protocol |
| **SAI** | Sistema de Alimentación Ininterrumpida |
| **SATEC** | Sistemas Avanzados de Tecnología, S.A. |
| **SCTP** | Stream Control Transmission Protocol |
| **SDN** | Software Defined Network |
| **SNMP** | Simple Network Management Protocol |
| **SSH** | Secure Shell |
| **STP** | Spanning Tree Protocol |
| **TACACS+** | Terminal Access Controller Access Control System + |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **UDP** | User Datagram Protocol |
| **VLAN** | Virtual Local Area Network |
| **VoIP** | Voice over Internet Protocol |
| **VPN** | Virtual Private Network |
| **XML** | eXtensible Markup Language |
| **YANG** | Yet Another Next Generation |

# 1. Introducción

Las redes corporativas tienen un papel muy importante en la empresa para permitir la conectividad de sus usuarios. Estas redes deben adaptarse a las necesidades corporativas y ser capaces de ofrecer los servicios que soliciten tanto los clientes de la empresa como los propios usuarios. Por eso, es fundamental comprender qué requerimientos existen para la red en cuanto a aplicaciones y servicios para conseguir una red completa que permita a sus usuarios disponer de todas las funcionalidades necesarias para desempeñar su labor en la empresa.

Las necesidades de una red corporativa no cesan de crecer con el tiempo, aumentando los servicios y creando nuevas necesidades para sus usuarios. Los recursos de la red resultan limitados y quedan obsoletos si la red no se renueva con frecuencia y el mantenimiento es insuficiente. Para evitar un funcionamiento limitado de la red, es fundamental realizar un análisis de su rendimiento para verificar que cumple con los requerimientos de sus usuarios.

En caso de que la red no disponga de las capacidades suficientes para dar cobertura a los servicios demandados, se debe plantear un posible análisis para adecuar la red a las necesidades y soportar el crecimiento de las redes con la incorporación de todos los servicios requeridos.

Con la llegada de nuevas aplicaciones y servicios a las redes corporativas, es necesario asignar recursos a cada uno de ellos considerando las necesidades de los mismos y ajustándose a las características propias de su naturaleza. Teniendo en cuenta las capacidades que posea la red corporativa, se debe cuidar la asignación de los recursos de manera que sea posible la convivencia de los diferentes servicios y se asegure la posibilidad de que los servicios se utilicen de forma concurrente. En general, la diferenciación de servicio tiene que buscar una solución equilibrada y realista que asigne los recursos disponibles de la red equitativamente entre los servicios incorporados, adecuándose a los recursos requeridos por cada servicio.

Conociendo la multitud de aplicaciones que tiene que soportar una red corporativa hoy en día, es imprescindible considerar la introducción de calidad de servicio. Para una gestión óptima de los recursos de una red, es conveniente aplicar reglas de calidad de servicio, sobre todo si se trata de un entorno empresarial, donde una buena gestión de los servicios es fundamental para el correcto desempeño de los servicios de la empresa. La calidad de servicio permite establecer una prioridad en aquel tráfico que tiene una necesidad concreta para la empresa. Además, la gestión de la calidad de servicio ofrece una visión amplia de la circulación del tráfico en la red corporativa y facilita la administración de los flujos de tráfico, evitando posibles congestiones en el equipamiento de la red.

La creciente virtualización del hardware en el mundo de las redes ha traído nuevas tecnologías que permiten construir redes definidas por software. A medida que los recursos hardware se vuelven más asequibles y los terminales son cada vez más

potentes, existe la posibilidad de virtualizar sistemas completos en equipos grandes. SDN es una tecnología que permite construir arquitecturas de red definidas por software.

Estas tecnologías definidas por software son soluciones innovadoras que permiten redefinir las redes corporativas en función de sus requerimientos. Es un nuevo paradigma en el entorno de las redes que permite que sean altamente flexibles posibilitando la virtualización y administración central de hardware, software de control y aplicaciones. Todo esto nos lleva a un nuevo escenario en el mundo de las redes corporativas, donde las aplicaciones y servicios cobran una importancia mayor. De hecho, el diseño y la topología de red junto con el equipamiento dependen directamente de los requerimientos de estos servicios a soportar por la red.

En general, es importante adaptar las redes corporativas a las necesidades que surjan con la incorporación de nuevos servicios y entender que un análisis de estos es esencial para el posterior diseño y análisis de la topología y el equipamiento de la red.

# 2. Contexto

Este trabajo se desarrolla en el marco de una cooperación educativa en la empresa SATEC (Sistemas Avanzados de Tecnología, S.A.). El alumno se encuentra en un contrato con una duración aproximada de 5 meses en la empresa en cuestión, donde desempeña, a grandes rasgos, labores de networking.

El proyecto global comprende el estudio, análisis y mejora de la red corporativa de esta empresa. Debido a la envergadura del proyecto, el trabajo se ha subdividido en dos subproyectos diferenciados:

- Un proyecto inicial que estudia y analiza, tanto el estado actual de los servicios actualmente soportados y sus requerimientos de mejora, como la necesidad de introducir nuevos servicios.
- Un segundo proyecto que, en base a los resultados del análisis anterior, estudia las mejoras a implementar en la infraestructura de la red y desarrolla una propuesta para el rediseño de la misma.

Este trabajo fin de grado comprende el primero de los proyectos antes mencionados. El segundo de ellos se ha desarrollado también en el marco de una cooperación educativa de otro alumno de la ESI de Bilbao. Ha sido imprescindible, por tanto, un trabajo colaborativo para la consecución del objetivo global de mejorar la red de la empresa SATEC. Se trata, por tanto, de un proyecto cooperativo relacionado, además, con la especialidad de telemática, y más concretamente con la ingeniería de redes.

SATEC (SATEC, 2019) es una multinacional española con más de 30 años de experiencia en la integración de soluciones tecnológicas, especializada en servicios avanzados asociados a las nuevas tecnologías de la información. SATEC es hoy un grupo empresarial internacional con presencia activa en múltiples países. Aunque la sede principal de la empresa se encuentra ubicada en Madrid, tiene una sede en Bilbao, concretamente, en el Parque Tecnológico de Zamudio. Allí se encuentra trabajando el alumno, donde desarrolla este trabajo en cooperación con la empresa y la universidad.

El proyecto nace de la necesidad de analizar la situación actual de la red corporativa ubicada en la sede de Bilbao. Debido a un cambio de localización de la sede en 2017, se migró el equipamiento de red a la localización actual. Durante esta migración no se analizó con suficiente profundidad la evolución de la red y la incorporación de nuevos servicios con requerimientos específicos. Esto dio lugar a un diseño de red poco eficiente, difícilmente escalable y con configuraciones residuales debidas a la migración de servicios obsoletos.

Más de dos años después de la migración, la red de la oficina continúa añadiendo nuevos servicios a clientes de manera provisional en la red. Además, debido al aumento de plantilla, la red ha sufrido extensiones presuntamente provisionales que han permanecido hasta ahora.

El rendimiento actual de la red en la oficina puede mejorarse en ciertos aspectos como la robustez, la escalabilidad, la seguridad y las tasas de velocidad. En estos momentos, la situación es preocupante. Las tasas de velocidad para los usuarios que se conectan a las tomas de las mesas son muy bajas y se produce alta latencia en las conexiones debido a la compleja configuración heredada de la migración.

Estas problemáticas de rendimiento hacen que los servicios actuales de la oficina no se den con la calidad suficiente debido, en gran parte, a un diseño de red que no tiene en cuenta las necesidades de los servicios que surgen de los usuarios, tanto corporativos como a clientes y hasta la propia navegación de datos. En conclusión, existen grandes problemáticas en la red corporativa de la oficina que han surgido tras años de una gestión pobre del diseño y el equipamiento de la red desde que se migró a la nueva localización de la sede de Bilbao. Esto ha llevado a la oficina a una situación en la que no se han contemplado los servicios requeridos. Con configuraciones residuales y discordantes, la red ofrece recursos muy limitados a sus usuarios con dificultades sustanciales para proporcionar sus servicios tanto corporativos como a clientes.

En el marco de este contexto, se plante el siguiente proyecto que pretende mejorar el rendimiento de la red corporativa de la sede de Bilbao mediante el análisis de las necesidades y requerimientos de las aplicaciones y servicios para el posterior rediseño de la estructura de la red a todos los niveles.

Este proyecto, además, pretende establecer un diseño de los servicios homologado para todas las delegaciones. Desde la sede principal de Madrid han decidido que el proyecto sirva como referencia para la restructuración de otras delegaciones. El objetivo es obtener una solución de diseño de servicios común para todas las sedes. De esta forma, podrían soportarse, de forma adecuada, las nuevas aplicaciones y servicios de los que dispone la empresa.

# 3. Objetivos y alcance

Conociendo la situación de partida descrita en el apartado anterior, la empresa plantea una actualización del diseño de la red corporativa. Tras conocer las evidentes problemáticas surgidas del pobre mantenimiento después de una migración residual, surge la necesidad de llevar a cabo una restructuración de la red para lo que es imprescindible, previamente, **un análisis de las aplicaciones y servicios soportados (o a soportar en un futuro) por la red corporativa de la oficina, así como sus requerimientos. Este estudio constituye el objetivo principal de este proyecto.**

En cuanto a objetivos parciales, previo a comenzar con el análisis, es necesario identificar la situación actual de la red y documentar las problemáticas existentes en las configuraciones del equipamiento de la red corporativa. Se analizará el equipamiento existente para conocer sus funcionalidades y capacidades. Un análisis exhaustivo del funcionamiento de cada equipo de la red conducirá a un rediseño que mejor se adapte a las necesidades de la oficina. Será necesario conocer las capacidades de los enlaces de la red, las latencias que se produzcan y la posibilidad de priorizar y clasificar tráfico.

Tras la fase inicial de documentación y conocida la situación de partida, se comenzará con el análisis de las aplicaciones y servicios demandados en la actualidad por la oficina, sus usuarios y los clientes de la empresa. Se diferenciará entre los servicios corporativos y aquellos orientados a clientes. También se tendrán en cuenta las necesidades que puedan surgir del entorno de la oficina, relacionadas con la disposición y la organización del espacio de la oficina.

Para comprender cuáles son los servicios más relevantes y qué requerimientos pueden tener, se procederá a completar un análisis de rendimiento que identifique los cuellos de botella y las problemáticas existentes en los servicios que se están soportando actualmente con datos significativos. Este análisis servirá de ayuda para entender las causas de los problemas surgidos en la red corporativa y además realizar una comparativa con el rendimiento posterior de la red tras su reestructuración.

Tras el correspondiente análisis de rendimiento, se comenzarán a contemplar las nuevas aplicaciones y servicios que se deseen añadir a las prestaciones actuales de la red. Esto requerirá un estudio de los posibles requerimientos que puedan tener estos nuevos servicios para poder realizar un rediseño que se ajuste a las necesidades de los mismos y sea capaz de soportar conjuntamente todas las nuevas funcionalidades. Este estudio irá acompañado de una investigación en la que se observarán las diferentes recomendaciones y normativas relativas a calidad de servicios y sus requerimientos de los organismos más relevantes del sector.

Después de completar el estudio de las recomendaciones más relevantes, se comenzarán a describir los nuevos servicios que se van a soportar en el escenario

de la mejora de la red corporativa. Se establecerán los requerimientos de éstos en función de lo estudiado en las recomendaciones referentes a calidad de servicio de los organismos del sector. Es importante definir las características de los servicios de la red y realizar una clasificación en función de si se trata de un servicio a usuarios (ya sean clientes de la empresa o usuarios corporativos) o de un servicio propio de la red corporativa (gestión, mantenimiento, tráfico de datos...). Este análisis nos permitirá obtener unos requerimientos que servirán para establecer las especificaciones que debe tener el nuevo diseño de la infraestructura de la red corporativa.

Tras la descripción de los requerimientos, se plantearán unas alternativas de diseño para las que se escogerán criterios de selecciones que se ajusten a las características del proyecto. Las alternativas seleccionadas formarán la solución final que se llevará a cabo para la implantación de los nuevos servicios en la infraestructura de red corporativa de la oficina.

Resumiendo, **se analizará la red corporativa de la oficina actual identificando las problemáticas existentes y se procederá a desarrollar el análisis y estudio de los requerimientos de las aplicaciones y servicios soportados por la red** para ser ofrecidos con garantías de óptimo rendimiento. Se persigue que los resultados de este estudio puedan servir de base para el establecimiento de las especificaciones requeridas para el rediseño de la red.

# 4. Beneficios

Partiendo de que el objetivo principal del proyecto es el estudio de los requerimientos de los servicios para mejorar el diseño de la red corporativa, el desarrollo de este proyecto pretende obtener beneficios directos en el ámbito técnico, social y económico. A continuación, se analizan los beneficios del proyecto desde la perspectiva de los distintos ámbitos.

## 4.1. Beneficios técnicos

Desde el punto de vista técnico, el proyecto supone un beneficio técnico en la propia red corporativa de la empresa. Los resultados del estudio servirán de base para la mejora del equipamiento de red y la adaptación de la red que garantice proporcionar los servicios con un rendimiento óptimo y una calidad adecuada. En este sentido, el análisis desarrollado permitirá el rediseño de la red para mejorar el rendimiento por medio de una asignación de recursos más eficiente.

Así mismo, las propuestas para mejorar la robustez y seguridad que se plantean con el estudio supondrán unas garantías de mejora técnica sustanciales en las infraestructuras. Las mejoras de seguridad propuestas servirán de base para una configuración correcta y sencilla adaptada a los servicios que se proporcionan para el acceso al soporte de clientes.

Por otro lado, las tasas de velocidad de la red van a aumentar sustancialmente debido a la restructuración de la red con el estudio de los requerimientos de los servicios. La nueva gestión de la red presentará latencias más bajas al solventar las problemáticas que suponen la deficiente gestión de los servicios actuales. Deshacerse de las configuraciones residuales y la implantación de tecnologías más recientes supone también un avance tecnológico para la red de la empresa.

Finalmente, la implantación de diferenciación de servicios y calidad de servicio en la red permite tener mayor control y capacidad de gestión sobre la red para detectar y evitar problemáticas en el equipamiento y posibles congestiones de tráfico.

## 4.2. Beneficios sociales

Desde una perspectiva social, este proyecto supone un mejor rendimiento de la red de la oficina, lo que se traduce en un aumento de la calidad de la experiencia de los usuarios de la misma. Esto deriva también en un mejor servicio de la oficina para los clientes de la empresa. En general, una mejora del servicio, en términos sociales, es un beneficio para todas las personas involucradas en los trámites de la sede de Bilbao. En otras palabras, las personas a las que se les proporcione un servicio derivado de la red tendrán un servicio de mayor calidad.

El planteamiento de realizar un rediseño de la situación actual de la red es una propuesta de renovación y de actualización para la empresa. Esto implica que la

red de la oficina se actualizará para adoptar las últimas tecnologías del mercado. Además, la red se prepara para manejar la incorporación de nuevos servicios. De esta forma, la red corporativa evoluciona con la implantación de nuevas tecnologías y servicios, proporcionando a la sociedad de los mejores servicios y fomentando la investigación y el desarrollo de las últimas tecnologías.

Durante la fase de adecuación de la red a diferenciación de servicios e incorporación de calidad de servicio, los usuarios de la red verán un aumento de calidad en los servicios proporcionados en la red. Asegurar la calidad de servicio se traduce en un beneficio para las personas que den uso a ese servicio.

## 4.3. Beneficios económicos

Desde un punto de vista financiero, este proyecto plantea una mejora en el rendimiento de la red, lo que deriva en un aumento de la productividad de los usuarios de la misma. Estos usuarios verán una mejora sustancial en el servicio proporcionado por la red. Con tasas de velocidad más altas y latencias inferiores, serán capaces de ofrecer mejor servicio a sus clientes: más eficiente, más rápido y de mayor calidad.

Con la implantación de diferenciación de servicios y calidad de servicio en la red, los trabajadores de la oficina se encontrarán en un entorno de calidad con una red robusta y eficiente que les permita ser lo más productivos y dar lo mejor de ellos mismos. Teniendo en cuenta esto, las mejoras derivadas del rediseño de la red se traducirán en un beneficio económico para la empresa, que se verá reflejado a través de la productividad de los usuarios de la sede de Bilbao.

Por otro lado, se plantea mejorar la asignación de los recursos de los que dispone la red. Esta mejora se traduce en una gestión eficiente de recursos que deriva en un mejor funcionamiento de la red de la empresa. En otras palabras, la empresa mantendrá los mismos recursos de red, pero tendrá un mejor servicio para los usuarios. Esto es un beneficio económico para la empresa, que no tendrá que invertir en un aumento de los recursos disponibles.

En conclusión, este proyecto garantiza una situación final de la red en la que sea posible asegurar la calidad de servicios corporativos y los ofrecidos a los clientes de la sede de Bilbao.

# 5. Análisis de la situación actual

Antes de definir cuáles serán los nuevos servicios y aplicaciones que se soportarán en la red, es conveniente describir y analizar el estado actual de la red para comprender cómo se pueden introducir mejoras significativas que impliquen un aumento del rendimiento. Para ello, se van a describir los servicios que se están soportando en el entorno de la oficina y cómo se están manejando actualmente a través de la red corporativa. Además, se van detallar las problemáticas derivadas de la gestión perjudicial de los servicios y posibles soluciones para corregir y modernizar la manera de mantenerlos. Para describir estos servicios, se van a clasificar en servicios destinados a usuarios y aquellos propios de la red.

## 5.1. Servicios a usuarios

### 5.1.1. Servicios a corporativos

La oficina de Bilbao de SATEC tiene actualmente alrededor de 25 trabajadores, entre los que se diferencian perfiles técnicos, comerciales y directivos. Estos empleados requieren de telefonía y conectividad de datos, que se proporcionan mediante telefonía IP y un servicio de datos cableados. De este modo, los trabajadores pueden contactar con sus clientes y realizar sus labores con propiedad. Adicionalmente, existen dos puntos de acceso en la extensión de la oficina que dan conectividad inalámbrica. Por otro lado, debido a la gran escala de la empresa, existe una conexión túnel que comunica la sede de Bizkaia con Madrid. Este túnel permite a los trabajadores de la oficina acceder a los recursos corporativos como almacenamiento compartido o acceso a bases de datos.

Respecto a la disposición física de la oficina, hay tomas de usuario en cada puesto de trabajo que dan la conectividad a los usuarios. También existen dos salas de reuniones con sus correspondientes tomas preparadas para conferencias telefónicas. Los usuarios tienen disponible una impresora y un sistema de almacenamiento conectado en red para compartir archivos. Asimismo, hay disponible un servidor de virtualización para uso de la oficina.

Para el desempeño de las labores técnicas, los trabajadores tienen a su disposición un laboratorio donde poner en marcha proyectos con su correspondiente equipamiento. Para ello, se proporciona un espacio con conectividad a la oficina. Es en este lugar donde los técnicos realizan pruebas a equipamiento de clientes y preparan sus servicios.

En cuanto a seguridad, hay dos cámaras de videovigilancia y un sistema de control de acceso con lector de huella y tarjeta magnética que tiene conectividad con Madrid a través del túnel. Este servicio es requerido desde Madrid para realizar el control de horarios de sus trabajadores.

Sumado a todo esto, el equipo técnico de SATEC de otras sedes requiere de acceso al equipamiento de red para la convergencia y homogeneidad de las sedes. Es por

eso que existe la posibilidad de acceso remoto al equipamiento con servicio de autenticación. También se realiza una monitorización del equipamiento para corroborar el estado de los equipos y detectar fallos en la red.

### 5.1.2. Soporte a clientes

SATEC es una empresa integradora que proporciona servicios de soporte de networking a múltiples clientes. Entre ellos, aquellos que necesitan un servicio de monitorización a través de la red corporativa se encuentran el Parque Tecnológico de Zamudio y sus Sistemas de Alimentación Ininterrumpida (SAI). Estos servicios al parque se proporcionan desde la sede principal de la empresa en Madrid. Existen equipos de monitorización en Madrid que controlan el funcionamiento del equipamiento de red existente en la red que compone toda la extensión del parque tecnológico. Se trata de una red que interconecta los distintos edificios del lugar con cableado de fibra. Las características de esta red requieren una constante gestión de la red con alarmas y avisos para asegurar la conectividad en el parque.

Por otro lado, se da también un servicio de soporte a Itelazpi desde la sede de Bilbao, concretamente, un amplio servicio de networking que incluye monitorización, gestión y mantenimiento del equipamiento que tienen ubicado en el Parque Tecnológico. El acceso a este servicio de cliente se proporciona a través de la red corporativa.

## 5.2. Servicios de red

Para proporcionar todos los servicios a usuarios mencionados, existe una segmentación lógica de la red con VLAN. Esta tecnología muy extendida en entornos corporativos pretende administrar la red separando en redes lógicas independientes la red de área local de la oficina. En base a los usuarios y sus necesidades, la segmentación actualmente instaurada en la oficina es la siguiente en función de sus servicios.

**Tabla 1 Segmentación VLAN en la actualidad**

| ID VLAN | SERVICIO | DIRECCIONAMIENTO |
|---|---|---|
| 1 | Soporte cliente PTZ | 192.168.100.0/24 |
| 6 | Soporte cliente PTZ SAIs | 192.168.113.0/24 |
| 7 | Soporte cliente Itelazpi | 10.101.103.252/30 |
| 10 | Telefonía IP | 172.18.12.0/24 |
| 13 | Laboratorio | X.X.51.160/28 |
| 15 | Direccionamiento público para recursos | X.X.51.0/26 |
| 16 | Datos y navegación | 172.19.16.0/24 |
| 20 | Control de accesos y videoseguridad | 10.0.40.0/24 |
| 100 | Gestión y mantenimiento | 10.15.4.0/24 |

Para proporcionar a los usuarios de una dirección, se utiliza el extendido protocolo DHCP para la asignación dinámica de direccionamiento IP para las VLANs de telefonía IP (10) y datos y navegación (16). Una solución muy práctica para que los usuarios se conecten a las tomas y puedan navegar sin necesidad de configuración.

Siguiendo con el direccionamiento, para evitar el uso de direccionamiento público, se establece una traducción dinámica de direccionamiento de red (NAT). Esta tecnología se utiliza para utilizar un direccionamiento privado para aquellos servicios que no requieran ser accesibles desde el exterior. Esta traducción también se está utilizando para el acceso al equipamiento del parque desde Madrid tanto en origen como en destino, ya que el parque tecnológico utiliza direccionamiento privado para su red. De este modo, el equipo de monitorización de SATEC ataca a un direccionamiento público que se traduce al direccionamiento privado del parque.

Para el servicio de monitorización, se utiliza el protocolo SNMP tanto para el equipamiento de interconexión del parque como para el equipamiento propio de la oficina. Además, para el acceso remoto a los equipos, se utiliza el protocolo de autenticación TACACS que permite a verificar si el usuario tiene acceso a la red.

En cuanto a servicios de rutado, la conexión túnel establecida entre las sedes se utiliza para el anuncio de rutas del protocolo OSPF. A través de esta conexión, SATEC Madrid anuncia el direccionamiento corporativo para llegar a las demás sedes. Esta conexión túnel utilizan el protocolo GRE para encapsulado de tráfico y IPSec para proteger y asegurar el tráfico que viaja por la red.

Por último, mencionar que la empresa tiene contratados dos proveedores de Internet: Sarenet y Movistar. Por un lado, Sarenet ofrece una salida a Internet con una velocidad de 100 Mbps, que se utiliza para dar servicio a los puestos de trabajo y a los trabajadores. Este servicio se da a través de una conexión directa desde la oficina a la red del parque tecnológico, que después llega a Internet. Por el otro lado, Movistar ofrece una salida a Internet de 300 Mbps, que se utiliza exclusivamente para el servicio de videovigilancia y control de acceso a la oficina, que después se envía a la sede de Madrid a través de un túnel.

## 5.3. Dimensión de la oficina

Para comprender la capacidad de la oficina para soportar a usuarios, es conveniente tener en cuenta las dimensiones de la oficina. Esto ayuda a después elaborar un dimensionamiento de red que permita soportar los nuevos servicios que se demanden. Es por eso que, a continuación, se muestran las capacidades de la oficina.

La oficina tiene disponibles hasta 40 puestos de trabajo. Por otro lado, se pueden habilitar hasta cinco salas de reuniones. En cuanto a accesos, hay una única entrada oficial en la que se deben situar dos sistemas de control de accesos

(entrada y salida). Para dar cobertura a la videoseguridad, es conveniente situar por lo menos cuatro cámaras distribuidas por la oficina.

En cuanto a equipamiento de red, hay una sala de comunicaciones climatizada donde se pueden situar hasta 20 equipos de red. Hay disponible un laboratorio en el que probar equipamiento. Este espacio puede albergar hasta 20 equipos de laboratorio.

En general, la oficina tiene tamaño suficiente para más trabajadores de los que soporta actualmente. A continuación, se resume en una tabla las capacidades de dimensión de la oficina.

**Tabla 2 Dimensiones de la oficina**

| DIMENSIONES DE LA OFICINA | Cantidad |
|---|---|
| Puestos de trabajo | 40 |
| Salas de reuniones | 5 |
| Sistemas de control de accesos | 2 |
| Videoseguridad | 4 |
| Equipamiento de red | 20 |
| Laboratorio | 20 |

## 5.4. Análisis de rendimiento y problemáticas actuales

Para comprender la situación actual, es conveniente realizar un análisis de rendimiento que nos permita descubrir cómo se están ofreciendo los servicios, cuál es la calidad de los mismos y dónde se encuentran las posibles problemáticas existentes. Este análisis sirve para continuar con una descripción de los requerimientos que pueden tener los nuevos servicios y establecer un punto de partida para la mejora del rendimiento de éstos.

### 5.4.1. Procedimiento y herramientas utilizadas

Las recomendaciones y estándares de referencia para indicadores de calidad en rendimiento de transferencia de paquetes IP en redes y servicios de datos son las recogidas en los estándares Y.1540 y Y.1541 del organismo ITU-T. Atendiendo a los indicadores de estas normativas, se miden las siguientes métricas para el análisis de rendimiento:

- Ancho de banda disponible
  - Tasa de bajada
  - Tasa de subida
- Latencia (ping)
- Jitter (fluctuación de retardo)
- Pérdida de paquetes (packet loss)

En cuanto a herramientas para la medición y obtención de las métricas, se utilizan tres herramientas principales que son: Iperf3, Speedtest by Ookla y Bandwidth Place. Éstas permiten medir las métricas mencionadas mediante metodologías diferentes que se puede consultar en la bibliografía.

Iperf3 es una herramienta que envía flujos de datos (con transporte TCP o UDP) para medir el rendimiento de la red. El funcionamiento se basa en una arquitectura cliente-servidor en la que los equipos intercambian flujos de datos con características diferentes. Iperf pone a disposición de los usuarios servidores públicos para ejecutar las pruebas. Para este análisis, se usa el servidor de bouygues.iperf.fr para el test TCP y el servidor ping.online.net para el test UDP, ambos ubicados en Francia. La herramienta permite medir las siguientes métricas:

- Transporte TCP
    - Ancho de banda disponible
        - Tasa de bajada
        - Tasa de subida
- Transporte UDP
    - Latencia
    - Pérdida de paquetes
    - Jitter

Speedtest Ookla es una popular herramienta para probar la velocidad y el rendimiento de la conectividad a Internet. La versión más conocida es la de navegador, que permite escoger el servidor de destino entre una gran variedad de localizaciones hacía el que se realizarán las pruebas y lanzarlas mediante un solo clic. Para las pruebas, se utiliza el servidor por defecto, que se detecta automáticamente. Esta versión nos ofrece datos de ancho de banda disponible y latencia. Sin embargo, hay disponible una versión de escritorio que, siguiendo el mismo funcionamiento, posee funcionalidades añadidas. El test se divide en cuatros fases: un test de retardo, un test previo, un test de bajada y finalmente un test de subida. Utilizando una serie de peticiones HTTP, el servidor es capaz de obtener las métricas relacionadas con retardos (latencia, pérdidas y jitter). En la fase del test previo, se calcula el tamaño óptimo del archivo a enviar en las próximas conexiones en base a sus resultados. Finalmente, se realizan envíos de ficheros binarios mediante TCP para estimar el ancho de banda disponible. En general, la aplicación de escritorio facilita las siguientes métricas:

- Ancho de banda disponible
    - Tasa de bajada
    - Tasa de subida
- Latencia
- Pérdida de paquetes
- Jitter

Bandwidth Place es una herramienta muy similar a Speedtest Ookla para calcular la velocidad de acceso a Internet basada en HTML5. A diferencia de Speedtest, solamente hay disponible una versión de navegador. Al igual que el test de Ookla, se puede seleccionar el servidor hacía el que lanzar las pruebas. El servidor por defecto que se ajusta y que se utiliza en las pruebas está ubicado en Paris, Francia. El funcionamiento del test es por medio de conexiones HTTP y TCP. También se lanzan pings del protocolo ICMP para retardos. Las métricas facilitadas por esta herramienta son las siguientes:

- Ancho de banda disponible
  - Tasa de bajada
  - Tasa de subida
- Latencia

### 5.4.2. Resultados obtenidos

Para el análisis de rendimiento que se plantea, se realiza una serie de cuatro iteraciones del test para cada una de las herramientas mencionadas en diferentes instantes de tiempo. Concretamente, se prueban estas series para la conexión cableada para datos y navegación de la oficina y para la conexión inalámbrica de los puntos de acceso corporativos. En esta sección, se presentan estos resultados desglosados y se obtienen conclusiones de los mismos.

#### 5.4.2.1. Conexión cableada

La conexión cableada de la oficina llega desde la sala de comunicaciones hasta las tomas de usuario a través de un parcheo. Estos usuarios salen a través de la conexión de Sarenet de 100 Mbps. Para el test, se ha conectado el equipo a una de las tomas de usuario de uno de los puestos de trabajo. Como servidor del test Ookla, se autoconfigura Sarenet, en Zamudio. Para el test de Bandwidth Place, se configuran servidores en Londres y París. A continuación, se presentan los resultados de la ejecución de las pruebas.

**Tabla 3 Resultado de prueba Iperf3 en cx. cableada**

| IPERF3 | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de bajada **(Mbps)** | 35,0 | 31,1 | 34,0 | 34,2 |
| Tasa de subida **(Mbps)** | 34,4 | 36,3 | 34,9 | 36,5 |
| Latencia **(ms)** | 22 | 24 | 25 | 22 |
| Pérdida de paquetes **(%)** | 21 | 21 | 16 | 13 |
| Jitter **(ms)** | 7,436 | 9,006 | 5,744 | 9,768 |

**Tabla 4 Resultado de prueba Speedtest Ookla en cx. cableada**

| SPEEDTEST OOKLA | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de bajada **(Mbps)** | 46,25 | 46,18 | 45,50 | 45,19 |
| Tasa de subida **(Mbps)** | 41,84 | 43,15 | 37,16 | 40,78 |
| Latencia **(ms)** | 0 | 0 | 0 | 0 |
| Pérdida de paquetes **(%)** | 19 | 21 | 18 | 19 |
| Jitter **(ms)** | 0,89 | 0,78 | 3,22 | 2,56 |

**Tabla 5 Resultado de prueba Bandwidth Place en cx. cableada**

| BANDWIDTH PLACE | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de bajada **(Mbps)** | 46,24 | 45,71 | 51,61 | 52,98 |
| Tasa de subida **(Mbps)** | 19,79 | 19,19 | 19,66 | 19,34 |
| Latencia **(ms)** | 31 | 31 | 34 | 30 |

#### 5.4.2.2. Conexión inalámbrica

La oficina tiene dos puntos de acceso distribuidos para dar cobertura a todos los lugares. Estos equipos se manejan desde la sede de Madrid y utilizan la conexión túnel habilitada a través de Sarenet para dar conectividad a los usuarios. Para el test, se ha conectado el equipo a la red inalámbrica, asegurando una proximidad que ofrezca cobertura y asegure la conectividad. Como servidor del test de Ookla se utiliza Vodafone, en Madrid. Los resultados de ejecutar las pruebas planteadas son los siguientes.

**Tabla 6 Resultado de prueba Iperf3 en cx. inalámbrica**

| IPERF3 | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de bajada **(Mbps)** | 5,11 | 4,98 | 4,18 | 5,24 |
| Tasa de subida **(Mbps)** | 1,63 | 0,88 | 0,85 | 0,97 |

| | | | | |
|---|---|---|---|---|
| Latencia **(ms)** | 38 | 37 | 37 | 37 |
| Pérdida de paquetes **(%)** | 0,55 | 4,3 | 2,7 | 4,7 |
| Jitter **(ms)** | 7,421 | 8,791 | 8,174 | 5,054 |

**Tabla 7 Resultado de prueba Speedtest Ookla en cx. inalámbrica**

| SPEEDTEST OOKLA | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de **bajada (Mbps)** | 3,23 | 2,72 | 2,82 | 2,50 |
| Tasa de **subida (Mbps)** | 9,84 | 7,42 | 7,92 | 7,20 |
| **Latencia (ms)** | 14 | 15 | 15 | 15 |
| **Pérdida de paquetes (%)** | 2 | 0 | 0 | 0 |
| **Jitter (ms)** | 0,78 | 2,11 | 4,89 | 0,78 |

**Tabla 8 Resultado de prueba Bandwidth Place en cx. inalámbrica**

| BANDWIDTH PLACE | Prueba 1 | Prueba 2 | Prueba 3 | Prueba 4 |
|---|---|---|---|---|
| Tasa de bajada **(Mbps)** | 0,87 | 0,50 | 0,63 | 0,10 |
| Tasa de subida **(Mbps)** | 2,26 | 1,95 | 2,43 | 1,96 |
| Latencia **(ms)** | 55 | 48 | 83 | 53 |

### 5.4.3. Conclusiones y análisis de resultados

En base a los resultados presentados en *Anexo I: Gráficas y análisis de rendimiento*, se obtienen las siguientes conclusiones.

Empezando por la conexión cableada, destaca entre los resultados y gráficas obtenidas una alta pérdida de paquetes de alrededor del 20% que obtenemos de las herramienta Iperf3 y Speedtest Ookla. Esto se debe a la complicada infraestructura y diseño actual de la red que hace que el encaminamiento de los paquetes se balancee resultando en una pérdida de paquetes. Las tasas de velocidad tanto de subida como de bajada son bastante altas teniendo en cuenta que se ha ejecutado el test en horario de oficina. Sin embargo, la herramienta Bandwidth Place, que utilizan servidores del test ubicado en Londres y París, se

puede apreciar una bajada en la velocidad de subida. Aun así, las pruebas en Iperf3 y Speedtest ofrecen buenos resultados con servidores más próximos. En cuanto a latencia y jitter, los resultados son aceptables teniendo en cuenta la ubicación de los servidores.

En lo que se refiere a la conexión inalámbrica, los resultados son más dispares. Las tasas de velocidad son bastante bajas en comparación con la conexión cableada, nada extraordinario. Esto se puede deber a las limitaciones del hardware de los puntos de acceso, que no soportan grandes velocidades. Además, la conexión inalámbrica funciona a través del túnel establecido con la sede principal de Madrid, lo que deriva en latencias algo superiores, pero nada realmente significativo o que pueda suponer un problema. En cuanto a pérdidas de paquetes, existen ciertos porcentajes eventuales de pérdidas que probablemente se deban a la naturaleza inalámbrica del medio. Es conveniente revisar el funcionamiento del equipamiento para buscar soluciones a estas problemáticas. El jitter, en cambio, se mantiene relativamente bajo y se puede considerar aceptable.

En conclusión, a nivel de usuario, el rendimiento de la red actual permite a los usuarios conectados a las tomas de usuario navegar a velocidades relativamente altas con latencias bajas. Sin embargo, presentan altas pérdidas de paquetes que pueden suponer un problema.

Los usuarios que utilizan la alternativa inalámbrica, sin embargo, tiene tasas de velocidad muy inferiores que rondan los 5 Mbps de bajada y no llegan a 1 Mbps de subida con latencias más altas. Con algunas pérdidas espontaneas, los usuarios pueden navegar con más dificultades debido a las tasas tan inferiores de velocidad que pueden llegar a resultar problemáticas para aplicaciones que requieran anchos de banda más exigentes.

### 5.4.4. Problemáticas identificadas

Respecto a los servicios de proveedor contratados, la empresa tiene 400 Mbps de ancho de banda disponibles totales a través de dos proveedores. Sin embargo, como ya se ha mencionado, 300 Mbps de ese ancho de banda se emplean para videovigilancia y control de acceso y los 100 Mbps restantes para los demás servicios de la oficina. Esto da lugar a una gran problemática en el rendimiento de la red debido al ineficiente reparto de los servicios contratados. Esta configuración desperdicia gran parte del ancho de banda contratado por la oficina de Bizkaia, lo que da lugar a bajas tasas de velocidad para los usuarios, que están utilizando solamente un 25% de las velocidades contratadas. Una correcta configuración que sepa aprovechar las dos salidas a Internet permitirá mejorar el rendimiento notablemente. La idea es que los servicios críticos puedan salir a través de Sarenet, conocido proveedor de acceso a Internet en entornos empresariales, que asegura una disponibilidad mayor que la que ofrecen otros proveedores. Para los servicios que no requieran tanta disponibilidad, se puede utilizar la salida de Movistar, que

además dispone de un ancho de banda superior para proveer a los usuarios de tasas altas de velocidad.

Por otro lado, la estructura centralizada de la empresa hace que ciertos servicios se realicen de manera remota desde la sede principal en Madrid, como, por ejemplo, la monitorización del equipamiento de la red del parque tecnológico de Zamudio. Además, existe una conexión túnel a Madrid desde la oficina, principalmente pensada para tráfico corporativo, pero empleada para el acceso a Internet, lo que es la principal causa de las altas latencias de los usuarios a la hora del acceder a Internet.

En cuanto a cuellos de botella, el equipamiento de red que se está utilizando en la oficina tiene ciertas limitaciones de velocidad, con puertos de acceso a usuarios de tipo FastEthernet que permiten llegar a los 100 Mbps. Esto supone un cuello de botella en términos de ancho de banda. Es conveniente que este equipamiento sea renovado por soluciones de tipo Gigabit Ethernet o superiores, que ascenderían la velocidad hasta 1 Gbps. Además, para que Sarenet provea a la oficina de acceso a Internet, utiliza un acceso a la red del parque a través de la propia oficina mediante un conversor de fibra limitado a velocidades de 100Mbps, lo que supone un punto crítico en la oficina. Es importante renovar este equipamiento para evitar cuellos de botella si, en un futuro próximo, se desea ampliar el ancho de banda en la oficina.

Otra problemática relevante derivada de malas prácticas es el uso actual de red de gestión. Planteada principalmente para el acceso remoto al equipamiento tanto desde Madrid como desde la propia oficina, es un direccionamiento inutilizado. En su lugar, se utiliza el direccionamiento público reservado para recursos corporativos. Lo apropiado es utilizar el direccionamiento propuesto para la gestión para esos accesos por parte de los técnicos.

A nivel más bajo, existen varias VLANs para equipamiento y servicios distintos que, al migrar la localización de la sede, algunas se renombraron y cambiaron de identificador, lo que provoca configuraciones discordantes en algunos de los equipos. De la migración, hay varios equipos de red que están destinados a unas pocas funcionalidades que podrían unificarse en un solo equipo. Además, estos equipos mantienen algunas configuraciones antiguas de la antigua localización. Por ejemplo, como se ha mencionado anteriormente, la sede de Madrid tiene servicios de monitorización de la red del parque tecnológico a través de SNMP. Para proporcionar este servicio, existe una configuración de NAT para traducir IPs conocidas en Madrid a IPs locales de la red del parque. Este proceso está distribuido en dos equipos de rutado con reglas de NAT ambiguas y excesivamente complejas.

En cuanto a equipamiento, la red tiene en uso varios routers corporativos para servicios distintos con configuraciones incompatibles. De hecho, la red se encuentra segmentada en dos: por un lado, el acceso de Sarenet, que tiene dos routers en falsa redundancia debido a configuraciones erróneas (el router

secundario está prácticamente obsoleto y se mantiene por la migración con gran cantidad de configuración residual). Por otro lado, el acceso a Movistar, que consta de un router corporativo conectado a un switch donde se sitúa el equipamiento de control de acceso y cámaras.

Otra gran problemática relacionada con el equipamiento, es la ausencia de diversificación de la red. Las dos salidas disponibles de proveedores distintos no se están aprovechando para establecer redundancia ni la topología actual de la red está preparada para posibles caídas de enlaces. No existe diversificación de caminos en caso de fallos en la red, es decir, si uno de los enlaces se cae todo el tráfico que va por él se vería afectado sin posibilidad de restauración hasta que se reponga el enlace correspondiente. Es conveniente plantear un diseño con una topología que tenga presente la diversificación, de manera que el equipamiento pueda adaptarse a cambios y errores en el servicio. Para proveer a la red de esta característica, es importante ofrecer redundancia de caminos, stack de equipamiento y habilitar vías de recuperación.

En cuanto a seguridad y protección, los servicios críticos a clientes y los servicios corporativos se encuentran en la misma infraestructura de red, lo que supone un peligro ante posibles ataques que podrían acabar con la estabilidad de los servicios críticos. Separar y diferenciar estos servicios en equipamiento de red independiente sería una solución que permitiría evitar ciertos riesgos y otras problemáticas de seguridad.

En conclusión, existen muchas problemáticas y cuellos de botella derivados de un conjunto de malas prácticas, una migración no razonada y la obsolescencia del equipamiento de red. Por eso, es importante plantear el rediseño de la infraestructura de esta red para la mejora general de su rendimiento a través del estudio y análisis de los servicios. Atendiendo a las recientes necesidades surgidas y con la incorporación de nuevas aplicaciones y servicios, la red corporativa de la oficina de SATEC en Bizkaia debe solventar estos problemas a través el rediseño planteado.

# 6. Descripción de requerimientos

A continuación, se realiza un análisis para describir los requerimientos de los nuevos servicios considerados en el nuevo escenario de infraestructura de la red corporativa. Para ello, tienen en cuenta las características de los servicios, las recomendaciones de grandes fabricantes como Cisco y las normativas y recomendaciones de los organismos internacionales más relevantes del sector de las telecomunicaciones como ITU-T o IETF. En base a los requerimientos mínimos establecidos por estas recomendaciones, se marcan unos requisitos para los servicios que los superen para asegurar una calidad suficiente, ya que estamos en un entorno corporativo, donde se busca ofrecer un servicio de calidad superior.

Entre los servicios que se van a describir, se encuentras aquellos que se han soportado hasta ahora junto con algunas novedades. Estas nuevas aplicaciones y servicios obedecen a las últimas tendencias en entornos corporativos, donde surgen nuevas necesidades y ampliaciones del servicio.

En cuanto a la estructura del análisis, se comienza describiendo los servicios de usuarios tanto corporativos como los relacionados con clientes. Después, se estudian y detallan las características de los servicios de red que se necesitan en la red corporativa. Para terminar, se definen los requerimientos generales a modo resumen en una serie de tablas explicativas.

## 6.1. Servicios de usuarios

### 6.1.1. Telefonía IP

El servicio de telefonía IP es fundamental en entornos corporativos y es uno de los más extendidos en empresas. Este servicio concreto tiene requerimientos muy específicos por su carácter en tiempo real, que necesita muy bajo jitter y latencia. La telefonía es sensible a retardos y se considera un servicio de alta prioridad.

Los retardos en trasmisión de voz tienen un impacto enorme en los servicios de voz en conversación. Una latencia alta puede suponer la creación de eco en las conversaciones e incluso el acoplamiento acústico. Esto causa degradaciones importantes en la calidad de la voz, por lo que es necesario tomar medidas de control de eco. Además, cuando el retardo aumenta excesivamente, puede afectar a la dinámica de la conversación hasta el punto en que se percibe un retardo en la respuesta de la otra parte de la conversación. Para que se de este efecto, los niveles de latencia deben superar los cientos de milisegundos. Aun así, el oído humano no tolera apenas la variación de retardos con fluctuación de fase. Para evitar este efecto indeseable, los servicios de voz eliminan el jitter mediante una memoria de eliminación de la fluctuación de fase. En lo que se refiere a pérdidas de información, el oído humano es capaz de soportar cierto grado de distorsión en la señal de voz y comprender al oyente.

Consultando la recomendación G.1010 de la ITU-T (ITU-T, 2001) en cuanto a objetivos de calidad para aplicaciones de audio y video, se puede resumir su contenido en la siguiente tabla.

**Tabla 9 Objetivos de calidad para aplicaciones audio y vídeo. G.1010 (ITU-T)**

| Aplicaciones audio y vídeo | | Velocidades de datos | Latencia | Jitter | Pérdida paquetes |
|---|---|---|---|---|---|
| Audio | Voz en conversación (doble sentido) | 4-64 kbps | ‹150 ms | ‹1 ms | ‹3% |
| | Mensajería vocal | 4-32 kbps | ‹150 ms | ‹1 ms | ‹3% |
| | Audio en tiempo real de gran calidad | 16-128 kbps | ‹10 s | ‹1 ms | ‹1% |
| Vídeo | Videoconferencia (doble sentido) | 16-384 kbps | ‹150 ms | - | ‹1% |
| | Un sentido | 16-384 kbps | ‹ 10 s | - | ‹1% |

Según la recomendación de la ITU-T, los servicios de voz en conversación han de tener una latencia no superior a 150 ms, una jitter máximo de 1 ms y una pérdida de paquetes que no supere el 3%. En cuanto a velocidad de datos, establece que debe ser de 4-64 kbps por llamada.

La recomendación RFC 4594 del IETF (IETF, 2006) establece que las características de la telefonía son pequeños paquetes de longitud fija, tasa de emisión constante y flujos inelásticos de baja velocidad. Además, marca que este servicio tiene muy baja tolerancia a latencia, jitter y pérdidas de paquetes.

**Tabla 10 Características de los servicios de audio y vídeo. RFC 4594 (IETF)**

| Servicio | Características | Pérdida paq. | Latencia | Jitter |
|---|---|---|---|---|
| Telefonía | Paquetes pequeños de longitud fija, emisión constante de flujos inelásticos | Muy bajo | Muy bajo | Muy bajo |
| Videoconferencia | Paquetes de tamaño variable, intervalos de transmisión constante, velocidad adaptativa | Bajo - Medio | Muy bajo | Bajo |

En cuanto a recomendaciones de fabricantes, Cisco (Szigeti, 2004) fija unos requerimientos para los servicios VoIP. Concretamente, manifiesta que la pérdida de paquetes no debe superar el 1%, que la latencia máxima debe ser 150 ms, que el jitter no debe estar por debajo de los 30 ms y que debe asegurarse un ancho de

banda por llamada del rango de 21-320 kbps, dependiendo del códec, frecuencia de muestreo y otros factores.

En cuanto a requisitos de equipamiento de red, para dar alimentación a los teléfonos, es necesario que los puertos soporten la tecnología PoE. De esta manera, se puede prescindir de la alimentación externa y los teléfonos se alimentan directamente a través de estos puertos.

En base a estas recomendaciones, se definen los requerimientos para soportar telefonía IP en la red corporativa.

**Requerimientos del servicio de telefonía IP**

- Ancho de banda: 384 kbps por llamada
- Latencia: ‹100 ms
- Jitter: ‹1 ms
- Pérdidas de paquetes: ‹1%

### 6.1.2. Transferencia de datos y navegación

Uno de los servicios más básicos para cualquier entorno de red es el de datos genéricos y navegación. Éste engloba múltiples tipos de tráfico y supone una gran cantidad del uso del ancho de banda de la red. Por ello, se establece una diferenciación entre el tráfico de datos para servicios corporativos y para los demás servicios.

La recomendación G.1010 (ITU-T, 2001) marca ciertos objetivos de calidad para datos clasificados por tipos de aplicaciones, entre los que encontramos navegación web, transferencia de archivos, correo electrónico, transacciones de alta prioridad, etc. En general, desde el punto de vista del usuario, el requisito principal para las aplicaciones de transferencia de datos es garantizar que no hay pérdida de paquetes. A continuación, se muestra una tabla resumen de las clasificaciones más relevantes de la recomendación para aplicaciones de datos.

**Tabla 11 Objetivos de calidad para aplicaciones de datos. G.1010 (ITU-T)**

| Aplicaciones de datos | Velocidades de datos | Latencia | Pérdida paquetes |
|---|---|---|---|
| Navegación web | 10 KB | ‹2 s | Nula |
| Transferencia de gran volumen de datos | 10 KB – 10MB | ‹15 s | Nula |
| Transacciones de alta prioridad | ‹10 KB | ‹2 s | Nula |
| Juegos interactivos | ‹1 KB | ‹200 ms | Nula |
| Correo electrónico | ‹10 KB | ‹2 s | Nula |
| Transacción de baja prioridad | ‹10 KB | ‹ 30 s | Nula |

En la clasificación de la recomendación G.1010, no se incluye ninguna aplicación que encaje en la transferencia de datos para servicios corporativos y no corporativos. Es por ello que se toman los valores más restrictivos de la clasificación para marcar los requerimientos tanto servicio de datos corporativos como no corporativos. Por lo tanto, los valores de referencia que se adquieren de esta norma son 200 ms de latencia máxima, pérdidas de información nula y una velocidad de datos superior a 10 KB.

En relación a transmisión de datos, la recomendación RFC 4594 del IETF (IETF, 2006) marca varios tipos de servicios para datos con características distintas. A continuación, se muestran los datos más relevantes de las aplicaciones de datos.

**Tabla 12 Características de los servicios de datos. RFC 4594 (IETF)**

| Servicio | Características | Pérdida paq. | Latencia | Jitter |
|---|---|---|---|---|
| **Datos de baja latencia** | Velocidad variable, flujos elásticos a ráfagas | Bajo | Bajo - Medio | Alto |
| **Datos de alto throughput** | Velocidad variable, flujos elásticos a ráfagas | Bajo | Medio - Alto | Alto |

Dentro de estos, se encuentran los datos de baja latencia, que se caracterizan por tener una tasa de velocidad variable con flujos de datos elásticos a ráfagas. La norma específica que estos datos deben tener bajas pérdidas, una latencia media-baja y ser tolerante al jitter. Se puede considerar que este tipo de servicio encaja en la diferenciación que se establece para el servicio de datos corporativos. Por otro lado, la norma establece unas características para datos de alto throuhput. Se puede utilizar esta descripción para definir los requisitos que pueda tener el servicio de datos no corporativos.

Respecto a las indicaciones del fabricante Cisco (Szigeti, 2004) para datos, enuncia que las características del tráfico de datos varían de una aplicación a otra, e incluso dentro de la misma aplicación. Esto da lugar a muchas problemáticas a la hora de establecer un modelo de calidad de servicio para la transferencia de datos. Sin embargo, considerando algunas características generales y comunes en las distintas aplicaciones, se puede clasificar en cuatro tipos de servicios de datos: datos best-effort, datos de gran volumen, datos transaccionales y datos críticos empresariales.

Dentro de esta clasificación, la clase que mejor se adapta al servicio de datos corporativos es el servicio de datos transaccionales, ya que recoge los servicios más comunes en entornos corporativos como bases de datos, recursos compartidos, y autenticación. El fabricante especifica que este servicio debe tener un ancho de banda adecuado garantizado para soportar las operaciones en cuestión.

Para el servicio de datos no corporativos, en cambio, la clase de datos best-effort es la que mejor define sus características, ya que es la clase por defecto para el tráfico de datos restante. Cisco establece que este servicio debe tener un ancho de banda recomendado de al menos el 25% de la capacidad del enlace, ya que ha de soportar el tráfico de la mayoría de las aplicaciones.

Teniendo en cuenta las aportaciones de las recomendaciones más relevantes mencionadas, se fijan los siguientes requerimientos para los servicios de transferencia de datos.

**Requerimientos de los servicios de datos y navegación**

| Servicios de datos | Ancho de banda | Latencia | Pérdida de paquetes |
|---|---|---|---|
| Datos corporativos | 10% del enlace | ‹100 ms | ‹0,5% |
| Datos no corporativos | 25% del enlace | ‹100 ms | ‹2% |

### 6.1.3. Acceso inalámbrico

Otro servicio fundamental para los usuarios de la oficina es el acceso vía WiFi, que facilita a los trabajadores desplazarse por la oficina sin perder conectividad, dando lugar a un entorno de trabajo versátil y cooperativo. Además, se contempla dar un servicio de acceso a Internet a los usuarios invitados, de manera que puedan tener conectividad mientras permanezcan en la oficina.

Para proporcionar este servicio, basta con disponer de puntos de acceso distribuidos por la oficina, de manera que den cobertura a todas las localizaciones donde puedan situarse los usuarios.

Adicionalmente, para que los usuarios invitados puedan utilizar este servicio, se habilita un portal cautivo con autenticación que proporciona acceso temporal a la red.

En cuanto a requerimientos para este servicio, se soporta mediante el servicio de transferencia de datos ya establecido anteriormente.

### 6.1.4. Seguridad

Los servicios de seguridad son importantes para regular el flujo de personas en la oficina y detectar posibles intrusiones que puedan poner en riesgo la integridad de la empresa.

Respecto a recomendaciones, no existe ninguna referencia a este tipo de servicios, por lo que se ajustarán los requerimientos en función de las características propias del servicio y los criterios de la empresa.

#### 6.1.4.1. Control de accesos

Este servicio funciona mediante sistemas de control de acceso vía huella digital y tarjeta magnética colocados en los puntos de entrada y salida a la oficina. Los

sistemas de control de acceso no tienen grandes requerimientos en cuanto a ancho de banda, tan solo con una latencia baja y pocas pérdidas de paquetes es suficiente para soportar este servicio. Respecto a requisitos del equipamiento de red, es necesario que soporten la tecnología PoE para alimentarse.

Estos son los requerimientos de los sistemas basados en los requisitos del hardware.

**Requerimientos del servicio de control de acceso**

- Ancho de banda: 100 kbps por sistema
- Latencia: ‹100 ms
- Pérdidas de paquetes: ‹2%
- Tecnologías: PoE

#### 6.1.4.2. Videoseguridad

El servicio de videoseguridad se maneja con una serie de cámaras distribuidas por la localización de la oficina. Estas cámaras necesitan un ancho de banda de alrededor de 1 Mbps cada una para la transmisión del vídeo, con un jitter y pérdidas bajas. En cuanto a requisitos del equipamiento de red, es indispensable que soporten la tecnología PoE para alimentar a las cámaras de videoseguridad.

Por lo tanto, teniendo en cuenta los requerimientos del sistema, se definen los siguientes requerimientos para este servicio.

**Requerimientos del servicio de videoseguridad**

- Ancho de banda: 1,5 Mbps por cámara
- Latencia: ‹200 ms
- Jitter: ‹50 ms
- Pérdidas de paquetes: ‹2%
- Tecnologías: PoE

### 6.1.5. Videoconferencia

El servicio de videoconferencia en entornos corporativos es un pilar fundamental para la comunicación de la empresa. Teniendo en cuenta que SATEC es una empresa multinacional con varias delegaciones distribuidas por distintas localizaciones, la videoconferencia es necesaria para mantener reuniones entre las sedes.

La recomendación G.1010 de la ITU-T (ITU-T, 2001) define que el servicio de videoteléfono tiene los siguientes requerimientos mínimos: ancho de banda de 16-384 kbps por sesión, latencia no superior a 150 ms y pérdidas de menos del 1%.

En cuanto a la recomendación RFC 4594 del IETF (IETF, 2006), se define una clase de servicio de conferencias multimedia con las siguientes características: paquetes de tamaño variable, intervalos de transmisión constantes y tasa de velocidad

adaptativa. Los requerimientos que marca para este servicio son una pérdidas de paquetes baja, una latencia muy baja y un jitter bajo.

El fabricante Cisco (Szigeti, 2004) recomienda las siguientes directrices para el servicio de videoconferencia: pérdidas que no superen el 1%, latencia máxima de 150 ms y jitter no superior a 30 ms. En cuanto a la reserva de ancho de banda, Cisco recomienda proporcionar un ancho de banda del tamaño de cada sesión más un 20 por ciento adicional para soportar el servicio.

Para el caso concreto de este proyecto, conocidas las recomendaciones más relevantes, se establecen los siguientes requerimientos para el servicio de videoconferencia.

**Requerimientos del servicio de videoconferencia**

- Velocidad de datos: 460 kbps por sesión
- Latencia: ‹100 ms
- Jitter: ‹10 ms
- Pérdidas de paquetes: ‹1%

### 6.1.6. Gestión y mantenimiento de red

El servicio de gestión es fundamental para el tráfico asociado a la gestión, monitorización, administración y mantenimiento de la propia red corporativa. La estructura centralizada de la empresa necesita este servicio para la administración de las redes de las distintas delegaciones.

La recomendación RFC 4594 (IETF, 2006) define una clase de servicio denominada OAM, sigla de operaciones, administración y gestión (management), que soporta las funciones de configuración y administración de la red. Las características que describen a este servicio son flujos de paquetes de tamaño variable elásticos o inelásticos. En cuanto a requerimientos, la recomendación establece que este servicio debe tener una pérdida de paquetes baja y una latencia media.

El fabricante Cisco (Szigeti, 2004) define que las aplicaciones de gestión de red deben de asegurarse con un ancho de banda mínimo garantizado. Concretamente, recomienda reservar al menos un 2% del ancho de banda del enlace para este tipo de tráfico, ya que es indispensable para el funcionamiento de la red y tiene un papel crucial en situaciones críticas.

**Requerimientos del servicio de gestión y mantenimiento de red**

- Ancho de banda: 2% del enlace
- Latencia: ‹100 ms
- Pérdidas de paquetes: ‹1%

### 6.1.7. Almacenamiento en red

La oficina necesita que los usuarios de la red puedan compartir y gestionar sus recursos de manera remota. Para ello, hay disponible un servicio de almacenamiento en red para que los trabajadores puedan almacenar toda la información relevante que deseen conservar y poder gestionar eficientemente los recursos de los clientes.

Sabiendo que la oficina puede llegar a albergar hasta 40 trabajadores, se establecen los siguientes requerimientos para el almacenamiento de red.

**Requerimientos del servicio de almacenamiento en red**

- Capacidad por trabajador: 100 GB/trabajador
- Capacidad total: 4TB

### 6.1.8. Soporte a clientes

Los servicios a clientes no deben situarse en la misma infraestructura que los servicios corporativos. Hasta ahora, los servicios de soporte a clientes se manejaban a través de la red corporativa. Con la reestructuración de los servicios, se pretende separar estos servicios de la infraestructura de la red corporativa.

## 6.2. Servicios de red

### 6.2.1. Independencia de red: diferenciación VLAN

Para proporcionar todos los servicios a los usuarios, se utiliza la tecnología VLAN para realizar una segmentación lógica de la red. Teniendo en cuenta los servicios de usuarios y sus requerimientos, la diferenciación de la delegación es la mostrada en la siguiente tabla, con un direccionamiento aconsejado para la uniformidad de las delegaciones.

**Tabla 13 Diferenciación VLAN**

| ID VLAN | SERVICIO | DIRECCIONAMIENTO |
|---|---|---|
| 10 | Telefonía IP | 172.16.10.0/24 |
| 20 | Videoconferencia | 172.16.20.0/24 |
| 30 | Datos y navegación | 172.17.30.0/24 |
| 40 | Seguridad | 172.17.40.0/24 |
| 50 | Laboratorio | 172.17.50.0/24 |
| 60 | Servidores y direccionamiento accesible | 172.17.60.0/24 |
| 100 | Gestión y mantenimiento de red | 10.X.100.0/24 |

### 6.2.2. Asignación dinámica de direccionamiento

Para proporcionar a los usuarios de una dirección, se continúa utilizando el protocolo DHCP para la asignación dinámica de direccionamiento IP. En concreto,

se utiliza para los servicios de telefonía IP, videoconferencia y transferencia de datos. Para los demás servicios, se asignan las direcciones de manera estática.

### 6.2.3. Traducción de direccionamiento de red (NAT)

Continuando con lo soportado hasta ahora, se sigue utilizando la tecnología NAT para evitar el uso de direccionamiento público. De este modo, los usuarios utilizan direccionamiento privado en el entorno de la oficina, como hasta ahora. En cuanto a la traducción que se empleaba para el acceso desde la sede de Madrid al equipamiento de red del parque, los servicios a clientes quedan fuera de la infraestructura de la red, por lo que se suprime este servicio de red. Para el acceso a los servicios corporativos, se utiliza la traducción de puertos, de manera que sean accesibles desde el exterior.

### 6.2.4. Extensión de red de área local

La estructura centralizada de la empresa con delegaciones desplegadas por distintas localizaciones hace necesario establecer una comunicación entre todas las sedes. Para ello, se plantea implantar un sistema de túneles que interconecte las sedes entre sí. Así, se consigue una interconexión completa que permite comunicar de un extremo a otro a todos los trabajadores de la empresa. En la siguiente ilustración (*Ilustración 1 Sistema de túneles para interconexión de la empresa*) se puede ver este sistema aplicado a la empresa SATEC.

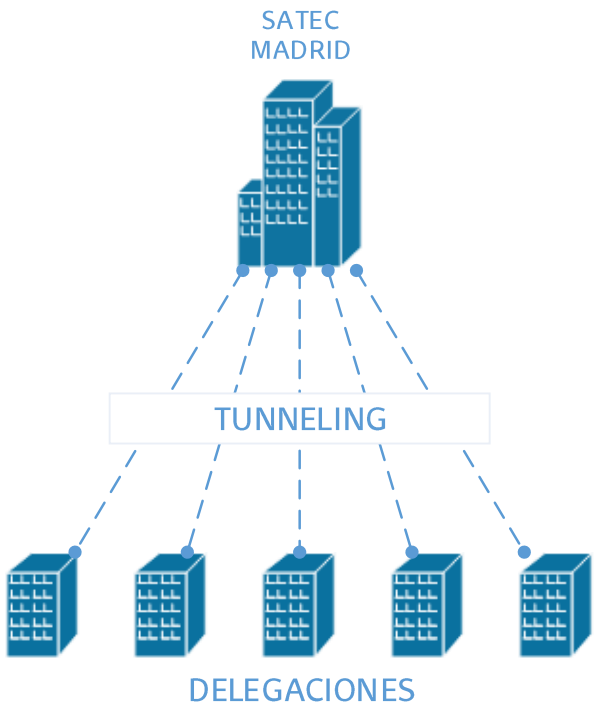



**Ilustración 1 Sistema de túneles para interconexión de la empresa**

Para llevar a cabo esto, se plantea utilizar la tecnología de extensión de área local VPN, que permite a las delegaciones establecer ese túnel hacía la sede principal.

### 6.2.5. Resolución de nombres de dominio

Otro servicio de red muy común en entornos corporativos es el servidor de resolución de nombres de dominio (DNS). Este servicio permite a los usuarios navegar utilizando nombres de dominio consultando la resolución IP a un servidor. Siguiendo con la estructura centralizada de la empresa, el servidor de este servicio se ubica en la sede principal de Madrid, a la que acceden los trabajadores de la oficina para consultar la resolución de los nombres.

### 6.2.6. Autenticación, autorización y contabilidad (AAA)

Para evitar intrusos en la red, se pone en funcionamiento un sistema de autenticación que se decidirá entre una selección de alternativas. Este sistema permitirá a los usuarios pasar por una fase de autenticación y autorización antes de acceder a sus recursos y a la gestión de red.

Este proceso de autenticación se gestionará de manera centralizada, con un servidor alojado en la sede principal de Madrid a la que acceden los usuarios de las delegaciones.

### 6.2.7. Administración y monitorización

Para la gestión del equipamiento de red de manera remota, es importante definir un servicio de monitorización. Para seleccionar la mejor alternativa para proporcionar este servicio, se realiza un análisis de alternativas en el que se contemplan varías tecnologías.

En línea con la estructura empresarial, la monitorización se realizará desde la sede principal de la corporación. Desde allí, se accederá al equipamiento de red para consultar y gestionar las correspondientes alarmas que puedan surgir.

### 6.2.8. Gestión

Aprovechando el servicio de gestión de red y siguiendo con lo instaurado hasta ahora, se habilita la gestión del equipamiento de la red corporativa. Para ello, debe existir la posibilidad de acceder este equipamiento remotamente mediante SSH.

### 6.2.9. Rutado y encaminamiento

Para proporcionar acceso entre las sedes, es necesario establecer unas directrices de rutado. Para ello, se utiliza el protocolo OSPF como hasta ahora para anunciar las rutas a las demás sedes. Se anuncian solo aquellas redes que son necesarias para la comunicación entre sedes y se evita compartir redes que sean de uso local restringido a la propia oficina.

Para el anuncio de las rutas de encaminamiento, se emplea el sistema de túneles habilitado para la interconexión de la sedes. El tráfico correspondiente al rutado ha de ser correctamente securizado y se recomienda implantarlo con el protocolo de seguridad IPsec.

### 6.2.10. Punto de acceso inalámbrico

Aunque ya se contempla este servicio de usuarios, es conveniente mencionarlo como servicio de red, ya que se necesita equipamiento de red específico para este servicio. Para dar cobertura a este servicio, es necesario ubicar puntos de acceso a lo largo de la oficina para cubrir todas las localizaciones de los usuarios.

### 6.2.11. Redundancia de caminos

Teniendo en cuenta los nuevos servicios y la reestructuración de la red, se va a aumentar la diversificación de caminos, lo que puede llevar a bucles. Para evitar estas problemáticas, se puede considerar implantar el protocolo de red STP que gestiona la presencia de bucles ante enlaces redundantes.

## 6.3. Dimensionamiento de red

Teniendo en cuenta las dimensiones y capacidades de la oficina analizadas en el apartado 5.3, ahora se ajustan los requerimientos de red que han de cumplirse para soportar los nuevos servicios demandados. Teniendo en cuenta los servicios requeridos hasta ahora, en la siguiente tabla se muestran los requerimientos de dimensionamiento de la red.

**Tabla 14 Requerimientos de dimensionamiento de la oficina**

| Servicio | Ctd | Puertos/ unidad | PoE | Puerto PoE | Puertos totales |
|---|---|---|---|---|---|
| Puestos de trabajo | 40 | 2 | 50% | 40 | 80 |
| Salas de reuniones (videoconferencia) | 5 | 4 | 50% | 10 | 20 |
| Equipos seguridad | 10 | 1 | 100% | 10 | 10 |
| Virtualización | 15 | 2 | 0% | 0 | 30 |
| Equipamiento de red | 30 | 1 | 0% | 0 | 30 |
| Laboratorio | 20 | 1 | 50% | 10 | 20 |
| TOTALES | **120** | | | **70** | **190** |

# 7. Análisis de alternativas

A continuación, partiendo de lo enunciado hasta ahora, se analizan las posibles alternativas en los diferentes aspectos relevantes del proyecto. Para el análisis, se identifican los servicios más relevantes del proyecto y se presentan una serie de alternativas a analizar por cada uno de ellas. Después, se realiza una comparativa entre las alternativas presentadas, evaluándolas según los criterios establecidos que mejor se ajusten a las características del proyecto. La evaluación se recoge en una tabla al final del análisis de cada problemática, con una puntuación obtenida en función de la importancia que se aplica a los criterios seleccionados. La alternativa con mayor puntuación será la mejor de las soluciones y la que mejor se adapte a la naturaleza del proyecto.

Para este proyecto, se van a someter a análisis de alternativas los siguientes aspectos: la arquitectura de calidad de servicio, el servicio de autenticación, autorización y contabilidad (AAA) y el servicio de administración y monitorización.

## 7.1. Arquitectura de calidad de servicio

Con la llegada de las nuevas aplicaciones y servicios a la red corporativa, es importante considerar la implantación de mecanismos de calidad de servicio para que éstos puedan soportarse asegurando un mínimo de calidad a los usuarios. Escoger una arquitectura de calidad de servicio que se adapte a las características de los servicios permite a los usuarios aprovechar las capacidades de la red para ofrecer el mejor servicio posible. Para ello, se van a someter al análisis las dos arquitecturas más relevantes para soportar calidad de servicio en redes corporativas: Diffserv y IntServ.

### 7.1.1. DiffServ

La arquitectura de servicios diferenciados (DiffServ) permite establecer un modelo de calidad de servicio sobre redes IP basado en clasificación de tráfico. Este mecanismo de clasificación permite priorizar cierto tráfico frente a otro marcando los paquetes con un nivel de prioridad. De este modo, cada clase de tráfico tiene un tratamiento diferenciado aplicando políticas de manera que se asegure la calidad para determinadas clases respecto a otras.

Este tratamiento basado en clases se denomina Per Hop Behavior (PHB) y se hace en cada salto por los nodos que atraviesa el paquete a través de la red corporativa. Aunque este tratamiento se aplica de manera independiente a cada red, las recomendaciones (IETF, 2006) establecen una arquitectura a seguir para conseguir una interoperabilidad entre redes. El marcado de clases de los paquetes para la priorización se hace en el campo DSCP de la cabecera IP. Este marcado se realiza en cada paquete dentro del dominio de calidad establecido, que se limita a la red corporativa.

### 7.1.2. IntServ

La arquitectura de servicios integrados (IntServ) define un modelo de calidad de servicio para garantizar y reservar los recursos necesarios para el servicio extremo a extremo. En este modelo, los servicios reservan una cantidad de recursos para determinados flujos de datos a lo largo del camino de la red.

Para ello, el equipamiento de red debe llevar un registro de los flujos que los atraviesan comprobando si existen los recursos necesarios para asegurar la calidad del servicio. Esto se realiza mediante el protocolo de reserva de recursos como RSVP. Este protocolo permite reservar recursos para asegurar la calidad del servicio extremo a extremo. El tráfico se clasifica en flujos asociados a servicios distintos, cada uno con sus características propias.

Sin embargo, la necesidad de procesar los flujos de tráfico para la reserva de recursos provoca un consumo de procesamiento alto en el equipamiento de red si la red aumenta su tamaño. Es por ello que este modelo tiene problemas de escalabilidad.

### 7.1.3. Comparativa

Las dos arquitectura presentadas permiten asegurar una calidad de servicio, pero existen grandes diferencias entre ellas. La arquitectura DiffServ tiene un enfoque más escalable con un modelo distribuido entre el equipamiento de red. Esto ofrece mayor flexibilidad y eficiencia a la hora de procesar el tráfico. IntServ, en cambio, plantea una solución más apropiada en redes pequeñas, donde mantener el estado de la reserva de recursos por flujos en el equipamiento de red no supone un peligro para la estabilidad de la red. Esa problemática de escalabilidad limita el diseño de la red, lo que puede suponer un riesgo teniendo en cuenta lo acontecido hasta ahora en la delegación, que ha tenido muchas dificultades para manejar este aspecto en la red.

Por otro lado, la gestión de los recursos es distinta para cada arquitectura. IntServ plantea una reserva extremo a extremo, lo que implica que los recursos ya reservados para determinados servicios no pueden emplearse para otros. En la arquitectura DiffServ, en cambio, los recursos se comparten entre las diferentes clases de tráfico. Sin embargo, la arquitectura IntServ da la posibilidad de garantizar un ancho de banda a cada servicio. Esto es más complejo de conseguir en arquitectura de servicios diferenciados.

Teniendo en cuenta que se define una arquitectura de servicios homologada para todas las delegaciones, hay que tener en cuenta la compatibilidad e interoperabilidad de la tecnología con otras redes. Con IntServ, la reserva se realiza extremo a extremo, lo que facilita esa compatibilidad. DiffServ, sin embargo, presenta ciertos problemas para funcionar si el clasificado no es homogéneo en otras redes. Tratándose de una solución homologada y siguiendo las

recomendaciones, se puede garantizar, hasta cierto punto, el mismo tratamiento de clases en otras redes.

En base a los servicios definidos para la red corporativa, se comparan las dos alternativas presentadas seleccionando los criterios de valoración que mejor se ajusten a las características de los servicios. A continuación, es muestran los criterios establecidos para la valoración:

- Gestión de los recursos. 30%
- Escalabilidad. 30%
- Compatibilidad. 20%
- Garantía de ancho de banda. 20%

**Tabla 15 Análisis de alternativas para arquitectura de calidad de servicio**

| | DiffServ | IntServ |
|---|---|---|
| **Gestión de los recursos** | 4 | 2 |
| **Escalabilidad** | 4 | 1 |
| **Compatibilidad** | 3 | 5 |
| **Garantía de ancho de banda** | 2 | 5 |
| **TOTALES** | **3,4** | **2,9** |

Teniendo en cuenta los resultados del análisis, la arquitectura que mejor se adapta a las necesidades de la red corporativa es la de servicios diferenciados DiffServ.

## 7.2. Autenticación, autorización y contabilidad (AAA)

La autenticación, autorización y contabilidad (AAA) son algunos de los servicios que se someten a análisis de alternativas. Estos servicios son importantes de cara a llegar a una solución homologada para todas las delegaciones, ya que marca las vías de acceso que tendrán los usuarios. Además, servirá para la gestión y administración del equipamiento de manera remota, por lo que es fundamental para que conseguir una homologación uniforme en todas las sedes. Por ello, se va a instaurar el servicio AAA seleccionando una de las siguientes tecnologías: TACACS+, RADIUS y DIAMETER.

Antes de comenzar con el análisis de las alternativas para este servicio, conviene conocer como es una arquitectura básica de un servicio AAA (*Ilustración 2 Arquitectura AAA*). Se trata de una arquitectura cliente/servidor en la que el usuario accede a un cliente AAA para autenticarse. Este cliente se sitúa en el servidor de acceso a la red (NAS), que establece el punto de entrada a la red corporativa. El cliente pide acceso al usuario al servidor AAA, que contiene una base de datos con las configuraciones relacionadas con la autenticación. En base a el contenido de la base de datos, el servidor toma la decisión de permitir (o no) el acceso al usuario.

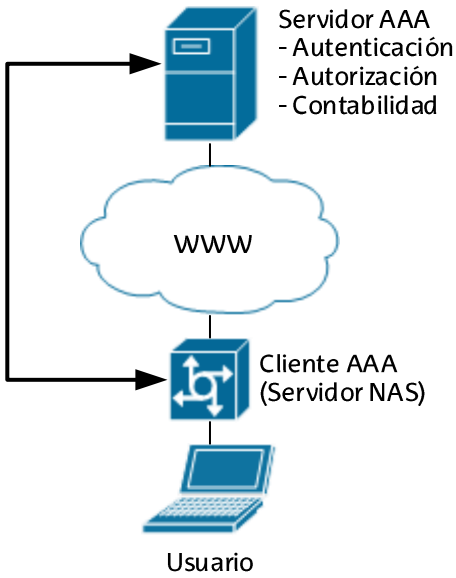



**Ilustración 2 Arquitectura AAA**

### 7.2.1. TACACS+

TACACS+ es una familia de protocolos de autenticación, autorización y contabilidad propietaria de Cisco para el acceso remoto a la administración de red. El funcionamiento se basa en uno o varios servidores centralizados hacia el que los clientes se conectan.

Una de las ventajas más relevantes de este protocolo es que las tres funcionalidades AAA se pueden separar en componentes independientes. Esta flexibilidad permite distribuir los servicios en servidores distintos. Esta característica encaja en la estructura centralizada de la empresa.

TACACS+ utiliza el protocolo TCP para el transporte, que es orientado a conexión. Además, permite encriptar el contenido del paquete pero deja una cabecera estándar sin encriptar. Hay un campo en esta cabecera que indica si el mensaje está encriptado. Esto lo hace uno de los protocolos de AAA más seguros.

Las características de este protocolo se resumen a continuación:

- Separa los tres elementos AAA, construyendo un protocolo más flexible.
- Encripta el contenido del mensaje, incluyendo usuarios, contraseñas y atributos.
- Permite una gestión centralizada para el servicio AAA.
- Utiliza el protocolo TCP de transmisión fiable y orientada a conexión.

### 7.2.2. RADIUS

RADIUS es un protocolo de AAA definido en el RFC 2965 (IETF, 2000). El funcionamiento se fundamenta en una arquitectura cliente-servidor (*Ilustración 3 Funcionamiento del protocolo RADIUS*). Se sitúa un cliente RADIUS en la delegación,

concretamente en el servidor de acceso a la red (NAS), encargado de gestionar quién accede a la red corporativa. El cliente es el responsable de enviar la información a los usuarios a los servidores RADIUS, que se encuentran en la sede principal de la empresa.

Los servidores RADIUS reciben las peticiones del cliente y se encargan de autenticar y autorizar a los usuarios a partir de los datos recibidos. Durante este proceso, se verifica la validez usuario y los recursos a los que tiene acceso. De manera complementaria, se registran los datos relevantes de la sesión para la posterior contabilidad.


**Ilustración 3 Funcionamiento del protocolo RADIUS**

A diferencia de TACACS+, utiliza el protocolo de transporte UDP, que no ofrece trasporte orientado a conexión, lo que hace que la aplicación tenga que implementarlo. Esto implica que RADIUS caree el nivel de soporte incorporado que ofrece el protocolo TCP.

En cuanto a seguridad, RADIUS solo encripta las contraseñas en los paquetes de solicitud de acceso, desde el cliente al servidor. El resto del paquete permanece sin encriptar, por lo que datos como el nombre de usuario, servicios autorizados y accounting puedan ser capturados por terceros.

En general, RADIUS es un protocolo más inseguro, pero también tiene una implementación más sencilla y ligera que genera un tráfico muy inferior al que genera el protocolo TACACS+.

### 7.2.3. Diameter

Diameter es un protocolo AAA que surgió como una extensión de RADIUS con características y funcionalidades añadidas. Es muy similar a RADIUS en cuestiones de servicios proporcionados. Sin embargo, existen ciertas diferencias entre ellos:

- Arquitectura peer to peer que aporta flexibilidad y mayor escalabilidad.
- Mecanismos de recuperación de errores para garantizar el envío de mensajes.
- Incluye una implementación básica de sesiones y control de usuarios
- Soporte para agentes proxy que permiten redirección, retransmisión y traducción.
- Trasmisión confiable con TCP y SCTP para el transporte.
- Ofrece protección con IPsec y TLS en cliente y servidor.

La arquitectura que propone Diameter añade un nuevo actor intermedio: el agente. Estos agentes pueden realizar funcionalidades distintas como retransmisión, redirección, traducción o actuar como proxy. Esto permite crear una arquitectura distribuida peer to peer en la que todos los nodos pueden ser clientes, servidores o agentes Diameter (*Ilustración 4 Arquitectura AAA de Diameter*).

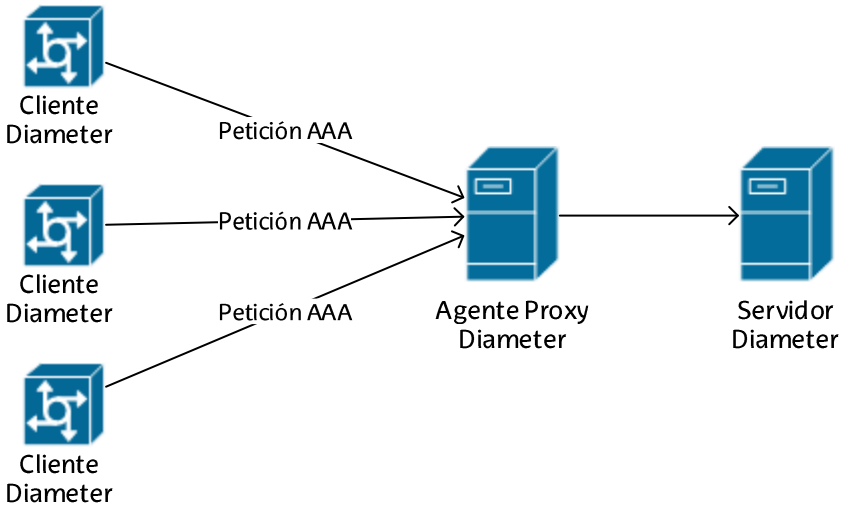



**Ilustración 4 Arquitectura AAA de Diameter**

En resumen, el protocolo Diameter proporciona un mejor transporte, un mejor servicio de proxy, un mejor control de la sesión y una mejor seguridad en comparación con el protocolo RADIUS. Además, ofrece una arquitectura más flexible y escalable para servicios AAA. Sin embargo, tiene una implementación más pesada que genera mayor cantidad de tráfico.

### 7.2.4. Comparativa

SATEC estructura su empresa de manera centralizada: una sede principal ubicada en Madrid y las correspondientes delegaciones distribuidas en localizaciones diferentes como Bilbao. Los tres protocolos propuestos para los servicios de autenticación, autorización y contabilidad encajan correctamente en esta estructura, ya que sus arquitecturas AAA están basadas en modelos cliente/servidor. Sin embargo, Diameter amplía su arquitectura sumando un agente a la ecuación, dando resultado a un modelo peer to peer que aporta más flexibilidad y escalabilidad, sumando complejidad al sistema. TACACS+ y RADIUS, en cambio, no presentan muchas diferencias en lo que se refiere a modelos de arquitectura.

En cuanto al transporte, TACACS+ utiliza el protocolo TCP, lo que hace que el transporte sea fiable y orientado a conexión. RADIUS, por su parte, funciona mediante el protocolo UDP, que no aporta fiabilidad ni es orientado a conexión. Esto puede suponer un problema a la hora de transportar la información, aunque los paquetes serán más ligeros, generando menos sobrecarga en la red. Por último, Diameter ofrece la posibilidad de usar TCP o SCTP, ambos protocolo fiables y

orientado a conexión. Esta flexibilidad es interesante, sobretodo porque SCTP implementa algunas características adicionales de fiabilidad como multihoming.

Respecto a la seguridad, TACACS+ ofrece una encriptación del contenido de los paquetes mientras que RADIUS solo encripta las contraseñas. En este aspecto, RADIUS supone un peligro ante posibles ataques de seguridad que puedan comprometer la integridad de las comunicaciones de la empresa. Diameter, en cambio, ofrece seguridad mediante IPsec y TLS, lo que lo hace el más seguro de los tres protocolos.

A continuación, se comparan las tres alternativas de protocolos para el servicio de autenticación, autorización y contabilidad. Para la valoración, se fijan unos criterios de selección basados en los intereses y características de la empresa a los que se les asigna un peso en función de su relevancia en el proyecto. La alternativa se escoge puntuando sobre cinco estos criterios para cada una de las alternativas presentadas. Los criterios de valoración son los siguientes:

- Seguridad. 30%
- Arquitectura. 20%
- Facilidad de implementación. 20%
- Flexibilidad. 20%
- Escalabilidad. 10%

**Tabla 16 Análisis de alternativas para el servicio AAA**

| | TACACS+ | RADIUS | Diameter |
|---|---|---|---|
| **Seguridad** | 4 | 1 | 5 |
| **Arquitectura** | 4 | 4 | 5 |
| **Implementación** | 5 | 4 | 3 |
| **Flexibilidad** | 2 | 1 | 3 |
| **Escalabilidad** | 3 | 2 | 4 |
| **TOTALES** | **3,7** | **2,3** | **4,1** |

En conclusión, la alternativa que mejor encaja para el servicio de autenticación, autorización y contabilidad es el protocolo Diameter.

## 7.3. Administración y monitorización

La administración y monitorización del equipamiento de red de las delegaciones es uno de los servicios más importantes para la empresa. Realizar una buena gestión de los recursos de las distintas sedes es muy importante para marcar una diferencia a la hora de administrar las delegaciones. Además, para definir un diseño de los servicios homologado y poder proporcionar un mantenimiento, es indispensable administrar todas las redes de las delegaciones corporativas. Con el protocolo de administración y monitorización adecuado, se puede conseguir un buen funcionamiento de todos los demás servicios que se den en las oficinas de SATEC.

Las alternativas a valorar para este servicio son las siguientes: SNMP, NETCONF y una solución combinada que implemente los dos anteriores.

### 7.3.1. SNMP

SNMP es un protocolo de administración y monitorización de red que facilita el intercambio de información entre equipamiento de red. Permite a los administradores de la red supervisar el funcionamiento de los equipos que conforman la red, como por ejemplo, consultar información del dispositivo, monitorizar su estado, modificar parámetro del dispositivo, habilitar alarmas, generar informes, etcétera.

El funcionamiento de este protocolo se fundamenta en dos agentes: la estación de gestión de red (NMS) y los agentes SNMP. La NMS es un servidor centralizado que se emplea para la monitorización y administración remota de dispositivos. Los agentes SNMP son clientes que residen en los dispositivos de red a administrar. Estos recogen la información a administrar del dispositivo y se coordinan con la NMS para comunicarse. Tiene la capacidad para atender las consultas y es responsable del envío de alertas a la NMS. La información que manejan los agentes se denominan Management Information Base (MIB), que son bases de datos en estructura de árbol almacenadas en los agentes que contienen los datos a administrar del dispositivo.

El protocolo SNMP tiene dos modos de funcionamiento diferenciados: polling y traps. En el modo polling, el servidor NMS inicia una consulta acerca de una variable del MIB hacia el agente SNMP correspondiente y éste le responde con su valor. En el modo trap, en cambio, los agentes se configuran para enviar mensajes de notificación al servidor NMS cuando ciertos valores de las variables del MIB superar los umbrales marcados.

Aunque el protocolo tiene algunas capacidades para administración y cambios en la configuración de dispositivos, está muy limitado en cuanto a las operaciones que se pueden hacer. Es un protocolo muy extendido para la monitorización, pero no para tareas administración.

Algunas de las ventajas de este protocolo se mencionan a continuación:

- Interoperabilidad. SNMP ofrece una interfaz común no propietaria para la administración de equipamiento de red de múltiples fabricantes.
- Automatización. Permite establecer alarmas para el envío automático de alertas cuando los dispositivos presenten funcionamientos indebidos.
- Monitorización. SNMP permite a los administradores de la red monitorizar parámetros clave de los dispositivos para identificar posibles problemáticas en el funcionamiento de la red.
- Flexibilidad. Las tareas de administración son independientes de las características y tecnologías de red del equipamiento administrado.

### 7.3.2. NETCONF

NETCONF es un protocolo de administración y monitorización de red que permite instalar, manipular y eliminar configuraciones en equipamiento de red. Emplea el lenguaje de marcado XML (junto a YANG) para enviar mensajes de configuración a los equipos. Funciona mediante una arquitectura cliente/servidor donde el cliente es típicamente un script o una aplicación, que actúa como administrador de la red. El servidor es, normalmente, un dispositivo de red (router o switch), al que se conecta mediante SSH.

NETCONF se ideó para suplir esa faceta de administración que SNMP no tiene. Es una herramienta que permite a los operadores de la red reemplazar el sistema de comandos a través de CLI para realizar configuraciones en equipos de manera remota.

Las MIB estándar de la industria generalmente no admiten el cambio de los datos de configuración; los proveedores proporcionan una interfaz de configuración que no es SNMP o extienden las MIB estándar de la industria con extensiones propietarias. La falta de una interfaz estándar de la industria para configurar los elementos de la red ha afectado gravemente la administración de dispositivos de diferentes proveedores y la capacidad de automatizar eficazmente muchos procesos de administración. NETCONF abre nuevas puertas para el mundo de la administración y configuración, aportando las siguientes ventajas:

- YANG ha sido ampliamente adoptado por los organismos de estándares clave (como IETF y ONF) para producir una amplia gama de modelos ricos de YANG. Modela tanto la configuración como el estado de las capas clave de la red.
- Las extensiones adecuadas se requieren con menos frecuencia, lo que facilita la interoperabilidad de múltiples proveedores.
- Permite operaciones y políticas automatizadas.
- Proporciona una base sólida para la automatización y SDN.

Teniendo en cuenta el nuevo paradigma de las redes definidas por software, este protocolo de administración abre la posibilidad de realizar y automatizar el proceso de administración y monitorización del equipamiento de red de una manera sencilla. Además, NETCONF ofrece interoperabilidad y facilita la implementación en algunos de los fabricantes más importante del mercado como Cisco y Juniper.

### 7.3.3. Solución combinada

Conocidos los dos protocolos y sabiendo que se complementan, una solución que combine NETCONF y SNMP puede ser interesante. NETCONF ofrece esa faceta de administración y configuración automatizada del equipamiento de red que SNMP no es capaz de ofrecer por sus limitaciones con la estructura de datos mediante MIBs. Sin embargo, SNMP proporciona esa interfaz de monitorización del equipamiento que continúa muy extendida e instaurada en las redes.

El nuevo paradigma de las redes definidas por software plantea ese escenario donde los dos protocolos coexisten en la misma red pero realizando diferentes funcionalidades. Esta solución ofrece las ventajas de los protocolos teniendo un resultado final con una fuerte monitorización mediante SNMP con polling y traps que alerten a los operadores de la red y con una interfaz para la administración y configuración del equipamiento de red con scripts automatizados de NETCONF.

### 7.3.4. Comparativa

SATEC ya tiene implantado un sistema de monitorización de la red mediante SNMP. Se utiliza para monitorizar de manera centralizada las delegaciones de la empresa desde la sede principal en Madrid. El planteamiento de sustituir el sistema instaurado actual por NETCONF supondría perder esa interfaz de monitorización. Sin embargo, continuar utilizando solo SNMP dejaría la parte administrativa de la red más débil. La solución combinada, en cambio, ofrece una alternativa equilibrada en la que los aspectos tanto de monitorización como de administración tienen un peso importante en el servicio.

Teniendo en cuenta lo mencionado hasta ahora, se comparan las tres alternativas presentadas para el servicio de administración y monitorización de la red. Para la valoración, se fijan los siguientes criterios de selección:

- Monitorización. 30%
- Administración. 20%
- Facilidad de implementación. 20%
- Coste. 20%
- Escalabilidad. 10%

**Tabla 17 Análisis de alternativas para administración y monitorización**

| | SNMP | NETCONF | Solución combinada |
|---|---|---|---|
| **Monitorización** | 5 | 3 | 5 |
| **Administración** | 2 | 5 | 5 |
| **Implementación** | 3 | 2 | 1 |
| **Coste** | 4 | 3 | 2 |
| **Escalabilidad** | 2 | 3 | 5 |
| **TOTALES** | **3,5** | **3,2** | **3,6** |

Concluyendo, la alternativa que mejor se adapta a las necesidades de la empresa es la solución combinada que implemente los dos protocolos: SNMP y NETCONF.

# 8. Descripción de la solución

Tras analizar las alternativas propuestas y seleccionar las mejores soluciones para el proyecto, a continuación, se describe la solución final de aplicaciones y servicios para la mejora de una red corporativa.

Primero, se describen los servicios de usuarios que se van a soportar en la red corporativa. Después, se detallan los servicios de red junto con las alternativas escogidas. Posteriormente, se describe el dimensionamiento presentado para la oficina. Para terminar, se explica la arquitectura de calidad de servicio propuesta para asegurar la calidad de los servicios en la red.

## 8.1. Servicios de usuarios

Entre los servicios de usuarios, aquellos relacionados con aplicaciones de audio y vídeo que se van a manejar en la red son el servicio de telefonía IP y la videoconferencia. Éstos son fundamentales para asegurar la comunicación entre todas las sedes que conforman la empresa. La telefonía es la herramienta principal de los trabajadores para la comunicación con los clientes, por lo que tiene requerimientos exigentes para asegurar su funcionamiento. En cuanto a la videoconferencia, es muy importante para establecer líneas de comunicaciones entre delegaciones y la sede principal y necesita requerimientos suficientes para soportarlo.

Los servicios relacionados con aplicaciones de transferencia de datos que se van a instaurar en la red se diferencian en dos: servicios de datos corporativos y no corporativos. Esta diferenciación sirve para asegurar una calidad al tráfico de datos corporativo, que necesita priorización para el funcionamiento de las delegaciones de la empresa. La estructura centralizada de la empresa hace que los servicios principales se encuentren ubicados en la sede principal, por lo que gran parte del tráfico de las delegaciones se dirige a la sede principal con fines corporativos. Para el resto de tráfico de datos, que sigue teniendo un gran peso en la red, se reservan también altos requerimientos.

En cuanto a servicios de seguridad de la oficina, se instaura videoseguridad y control de accesos. Estos servicios se manejan también de manera centralizada, por lo que necesitan requerimientos adecuado para asegurar la calidad. La videoseguridad y el control de accesos permiten a la oficina identificar posibles intrusiones y llevar una contabilidad del horario de los trabajadores. Además, deben comunicar a la sede principal de esta contabilidad para llevar un control de los trabajadores.

Respecto a servicios de administración, se pone en marcha un servicio de gestión y mantenimiento para los usuarios de manera que puedan encargarse de la gestión de la red. Este servicio se lleva a cabo localmente y remotamente, ya que se debe acceder al equipamiento de red tanto desde la oficina como desde la sede principal

para conseguir una solución homologada. El mantenimiento de red se realiza a través de este servicio para asegurar el correcto funcionamiento de la red con una solución escalable y a largo plazo.

Otro servicio para usuarios de la red es el almacenamiento en red. Éste da la oportunidad a los trabajadores de la oficina de mantener sus ficheros almacenados en una ubicación compartida y accesible para los usuarios. Es fundamental asegurar a cada usuario una capacidad de almacenamiento suficiente para sus necesidades.

Para terminar con los servicios de usuarios, mencionar que los servicios críticos de soporte a clientes se separan de la infraestructura de la red para la oficina, ya que no es conveniente por razones de seguridad mantener los servicios críticos de clientes en la misma infraestructura.

## 8.2. Requerimientos de servicios de usuarios

Teniendo en cuenta todos los servicios descritos y sus requerimientos en el apartado 6, se detallan los requerimientos de los servicios de usuarios en la siguiente tabla.

**Tabla 18 Requerimientos de los servicios de usuarios**

| | Velocidad de datos | Latencia | Jitter | Pérdida paquetes | Otros |
|---|---|---|---|---|---|
| **Telefonía IP** | 384 kbps/llamada | ‹100 ms | ‹1 ms | ‹1% | PoE |
| **Datos corporativos** | 10% del enlace | ‹100 ms | - | ‹0,5% | - |
| **Datos no corporativos** | 25% del enlace | ‹100 ms | - | ‹2% | - |
| **Videoseguridad** | 1,5 Mbps/cámara | ‹200 ms | ‹50 ms | ‹1% | PoE |
| **Control de accesos** | 100 kbps/sistema | ‹100 ms | - | ‹2% | PoE |
| **Videoconferencia** | 460 kbps/sesión | ‹100 ms | ‹10 ms | ‹1% | - |
| **Gestión de red** | 5% del enlace | ‹100 ms | - | ‹1% | - |

## 8.3. Servicios de red

Para asegurar la independencia de red entre los diferentes servicios, se establece una diferenciación mediante VLAN que permita separar en segmentos los servicios que se soportan en la red. Para ello, se sigue sugiere la siguiente segmentación mostrada en la tabla.

**Tabla 19 Segmentación VLAN propuesta**

| ID VLAN | SERVICIO |
|---|---|
| 10 | Telefonía IP |
| 20 | Videoconferencia |
| 30 | Datos y navegación |
| 40 | Seguridad |
| 50 | Laboratorio |
| 60 | Servidores y direccionamiento accesible |
| 100 | Gestión y mantenimiento de red |

Continuando con los servicios de red, se plantea el uso de DHCP para la asignación dinámica de direccionamiento de red. Esto permite a los usuarios obtener direccionamiento dinámico en los servicios de telefonía IP, videoconferencia y transferencia de datos. Para los demás servicios, se utiliza direccionamiento estático.

Para evitar el uso masivo de direccionamiento público, se propone utilizar la extendida tecnología NAT para que los usuarios utilicen direccionamiento privado en el entorno de la oficina, como hasta ahora. Esto permite a la empresa optimizar el uso del direccionamiento público provisto y limitar el uso para aquellos servicios que necesiten ser accesibles desde el exterior.

Para asegurar la comunicación entre las sedes de la empresa, se plantea implantar un sistema de túneles que interconecte las sedes entre sí. Así, se consigue una interconexión completa que permite comunicar a todos los trabajadores, permitiendo además el acceso a todos los recursos centralizados de la empresa. Para ello, se propone utilizar la tecnología VPN para la extensión de la red de área local.

Se plantea también el uso de un servidor para resolución de nombres de dominio con el protocolo DNS, de manera que los usuarios puedan navegar utilizando nombres de dominio que se traduzcan a direcciones IP. Siguiendo la estructura centralizada, el servidor se encuentra en la sede principal y las delegaciones acceden a él por medio de los túneles provistos.

Uno de los servicios de red que se ha sometido a análisis de alternativas es el servicio AAA. El protocolo seleccionado para dar este servicio es Diameter, que es una de las soluciones más completas para manejar el servicio AAA en entornos empresariales.

El servicio de administración y monitorización de la red también ha sido analizado en el estudio de alternativas. La solución seleccionada para este servicio ha sido una combinación de los protocolo SNMP y NETCONF. Utilizando SNMP para la monitorización del equipamiento de red y NETCONF para desplegar configuración de manera remota y administrar los equipos, esta solución es muy apropiada para

las necesidades de la empresa. Adicionalmente, para la gestión remota del equipamiento será necesario el protocolo SSH en el equipamiento.

Para el acceso y la comunicación entre las sedes, es necesario implantar un servicio de rutado y encaminamiento. Para ello, se propone utilizar el protocolo OSPF para el anuncio de rutas a través de túneles securizados con IPsec.

Otro servicio relacionada con la red es el acceso inalámbrico. Para ello, se necesita instalar puntos de acceso a lo largo de la oficina para asegurar una cobertura completa para los usuarios. Esto permite a los trabajadores moverse con flexibilidad en la oficina, dando la posibilidad de crear un entorno de trabajo cooperativo y comunicativo.

Para acabar con los servicios de red, es conveniente mencionar que, con la nueva arquitectura de la red y la diversificación de caminos, existe la posibilidad de que se creen bucles. Por ello, se plantea el uso del protocolo STP para evitar problemáticas derivadas de bucles de encaminamiento.

Otro aspecto a tener en cuenta a la hora de manejar los servicios es el dimensionamiento de la red. Para ello, se propone una estimación para poder soportar los servicios que se encuentra en el apartado 6.3.Este dimensionamiento se plantea para la delegación concreta de Bilbao y es de utilidad para el posterior desarrollo del proyecto complementario de rediseño de la infraestructura de red.

De todos estos servicios mencionados, surgen ciertos requerimientos para el equipamiento de red, por lo que es necesario que soporte las siguientes tecnologías y protocolos:

- Telefonía IP
  - VoIP
  - PoE
- Extensión de área local
  - VPN
- Independencia de red
  - VLAN
- Traducción de direccionamiento de red
  - NAT
- Administración y gestión de red
  - SNMP
  - NETCONF
  - SSH
- Rutado y encaminamiento
  - OSPF
  - STP
- Resolución de nombres de dominio
  - DNS

- Autenticación, autorización y contabilidad
  - Diameter
- Arquitectura de calidad de servicio
  - DiffServ (DSCP)

## 8.4. Arquitectura de calidad de servicio

Para asegurar la calidad de servicio en la red, se ha sometido a análisis de alternativas las posibles arquitecturas de calidad de servicio. La arquitectura propuesta finalmente ha sido DiffServ, también denominada arquitectura de servicios diferenciados.

Esta arquitectura permite establecer un marcado para clasificar el tráfico mediante el campo DSCP de la cabecera IP de manera que se clasifique en función del servicio al que pertenece. Así, con una buena gestión del tráfico, se puede conseguir asegurar la calidad del servicio en la red corporativa ajustándolo a las necesidades y requerimientos establecidos para todos los servicios.

Para el caso concreto de los servicios de usuarios propuestos, se puede establecer un modelo de clases como el de la siguiente ilustración (*Ilustración 5 Modelo de clases para calidad de servicio*). Teniendo en cuenta los requerimientos marcados, se puede construir una arquitectura de calidad de servicios diferenciados basada en el modelo propuesto.


**Ilustración 5 Modelo de clases para calidad de servicio**

## 8.5. Estructura homologada de los servicios

El proyecto nace con la ambición de conseguir una solución homologada para los servicios en todas las delegaciones. Es por ello que se han estudiado diversas alternativas para aquellos servicios más relevantes a la hora de conseguir una administración homologada. Como ya se ha mencionado, la empresa tiene una estructura centralizada, por lo que la administración de las delegaciones se encuentra en la sede principal de Madrid. Desde allí se realizan los servicios de gestión, monitorización, autenticación y autorización de las delegaciones de la corporación, por lo que es importante tener una homogeneidad en estos servicios.

En la siguiente ilustración (*Ilustración 6 Estructura homologada de los servicios*), se muestra un esquema donde puede verse de manera visual la estructura centralizada de los servicios que se lleva a cabo para conseguir una homologación de las delegaciones.

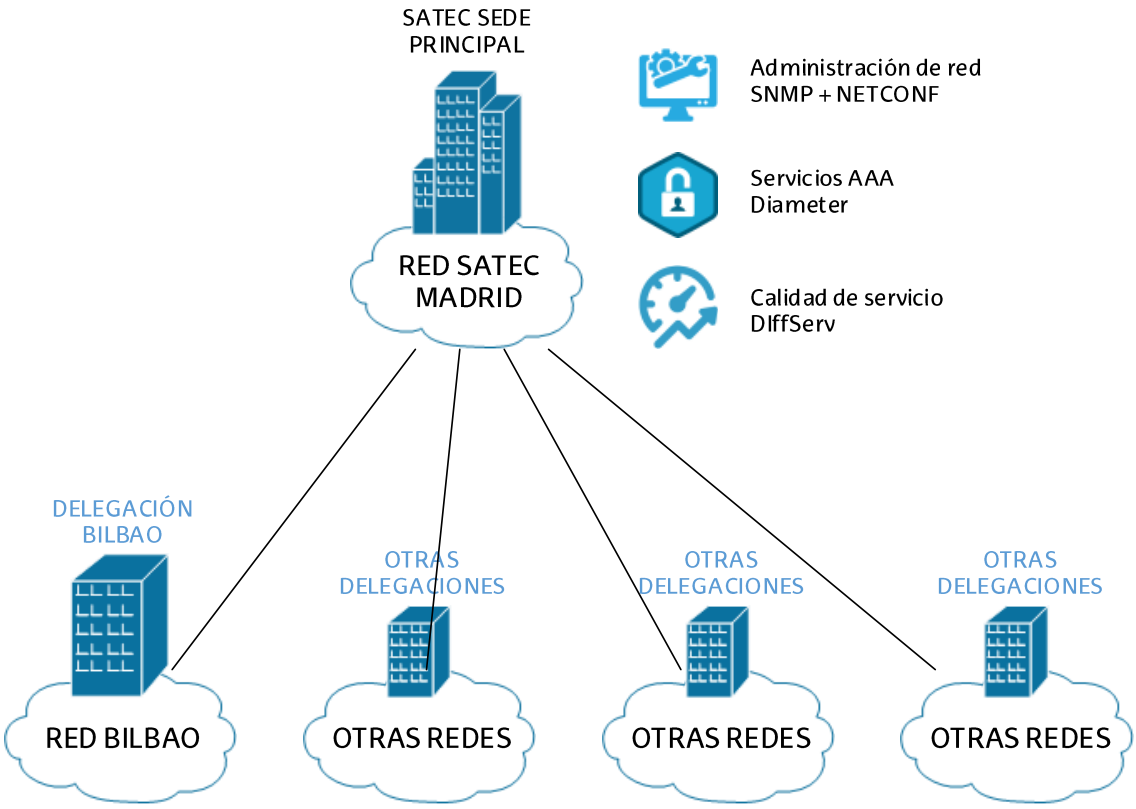



**Ilustración 6 Estructura homologada de los servicios**

Esta estructura ayuda a la empresa a llevar un control de cómo se encuentra las delegaciones desde la sede central. Con una arquitectura de calidad de servicio homogénea en las delegaciones se puede conseguir asegurar calidad para todos los servicios propuestos. De este modo, mediante el marcado y clasificado siguiendo el modelo de clases propuesto, se puede conseguir la calidad deseada entre delegaciones en todos los tipos de servicios.

## 8.6. Infraestructura de red

La solución descrita es una propuesta para la homologación de una arquitectura de servicios para las delegaciones de la empresa SATEC. Sin embargo, este proyecto comprende la primera parte de un proyecto global para la mejora de la infraestructura de la red corporativa de la delegación de Bilbao. Este estudio y análisis de los servicios sirve de base para el posterior rediseño de la infraestructura de red por parte de otro alumno (Martin, 2019).

La labor conjunta de los dos trabajos logra completar el objetivo final del proyecto, que es la reestructuración de la red para la mejora del rendimiento de la red corporativa.

# 9. Descripción de tareas

A continuación, se presenta la planificación del proyecto junto con la descripción de las tareas realizadas para la consecución del mismo. Para ello, las tareas se han agrupado en distintos paquetes de trabajo de manera estructurada. El proyecto se ha divido en seis paquetes de trabajo diferenciados, los cuales se describen brevemente en este apartado.

- Formación y familiarización con el proyecto. Fase de formación del personal del proyecto junto con la fijación de los objetivos del proyecto.
- Análisis de la situación actual. Estudio de la situación de la red y el equipamiento correspondiente, análisis de las capacidades de la misma y análisis de rendimiento de los servicios.
- Estudio de aplicaciones y servicios soportados en la actualidad. Investigación sobre los servicios que se dan en la red y cómo se está manejando, clasificándolos en servicios corporativos, críticos y propios de la red.
- Descripción de requerimientos de nuevas aplicaciones y servicios. Definición de los nuevos servicios a soportar por la red, descripción de las características de los mismos y exposición de los requerimientos de cada uno de ellos.
- Análisis de alternativas. Estudio de las tecnologías en tendencia y análisis de las alternativas para los servicios establecidos.
- Documentación y gestión del proyecto. Proceso paralelo de documentación de las tareas del proyecto junto con la entrega final del mismo.

En los siguientes subapartados, se presenta una tabla de descripción de los paquetes de trabajo junto a sus tareas e hitos correspondientes y el diagrama de Gantt del proyecto (*Ilustración 7 Diagrama de Gantt del proyecto*).

**Tabla 20 Descripción de tareas del proyecto**

| Nombre de tarea | Duración | Comienzo | Fin |
|---|---|---|---|
| **Formación y familiarización con el proyecto** | **43 días** | **lun 06/05/19** | **mié 03/07/19** |
| Definición del proyecto | 5 días | lun 06/05/19 | vie 10/05/19 |
| Curso CCNA | 9 días | mié 08/05/19 | mié 03/07/19 |
| **Análisis de la situación actual** | **10 días** | **lun 13/05/19** | **vie 24/05/19** |
| Descripción del diseño de red | 5 días | lun 13/05/19 | vie 17/05/19 |
| Análisis del equipamiento actual | 3 días | lun 20/05/19 | mié 22/05/19 |
| Estudio de capacidades actuales | 2 días | jue 23/05/19 | vie 24/05/19 |
| Análisis de rendimiento | 5 días | lun 20/05/19 | vie 24/05/19 |
| Entrega de informe de situación actual | Hito | vie 24/05/19 | vie 24/05/19 |
| **Estudio de aplicaciones y servicios soportados en la actualidad** | **10 días** | **lun 27/05/19** | **vie 07/06/19** |
| Estudio de servicios corporativos | 3 días | lun 27/05/19 | mié 29/05/19 |
| Estudio de servicios críticos y a clientes | 2 días | jue 30/05/19 | vie 31/05/19 |
| Estudio de servicios de red | 5 días | lun 03/06/19 | vie 07/06/19 |
| Entrega de estudio de servicios soportados | Hito | vie 07/06/19 | vie 07/06/19 |
| **Descripción de requerimientos de nuevas aplicaciones y servicios** | **10 días** | **lun 10/06/19** | **vie 21/06/19** |
| Definición de nuevas aplicaciones y servicios | 3 días | lun 10/06/19 | mié 12/06/19 |
| Estudio de normativas y recomendaciones | 2 días | jue 13/06/19 | vie 14/06/19 |
| Descripción detallada de los servicios | 5 días | lun 17/06/19 | vie 21/06/19 |
| Definición de requerimientos | 5 días | lun 17/06/19 | vie 21/06/19 |
| Entrega de descripción de requerimientos | Hito | vie 21/06/19 | vie 21/06/19 |
| **Análisis de alternativas** | **15 días** | **lun 24/06/19** | **vie 12/07/19** |
| Identificación de aspectos a analizar | 2 días | lun 24/06/19 | mar 25/06/19 |
| Estudio de nuevas tecnologías | 3 días | mié 26/06/19 | vie 28/06/19 |
| Estudio de alternativas para servicios AAA | 5 días | lun 01/07/19 | vie 05/07/19 |
| Estudio de alternativas para servicios de administración y monitorización | 5 días | lun 01/07/19 | vie 05/07/19 |
| Descripción de la solución | 5 días | lun 08/07/19 | vie 12/07/19 |
| Entrega de análisis de alternativas y descripción de la solución | Hito | vie 12/07/19 | vie 12/07/19 |
| **Documentación y gestión del proyecto** | **55 días** | **lun 06/05/19** | **vie 19/07/19** |
| Fase de documentación | 50 días | lun 06/05/19 | vie 12/07/19 |
| Entrega del proyecto | 5 días | lun 15/07/19 | vie 19/07/19 |

## 9.1. Diagrama de Gantt

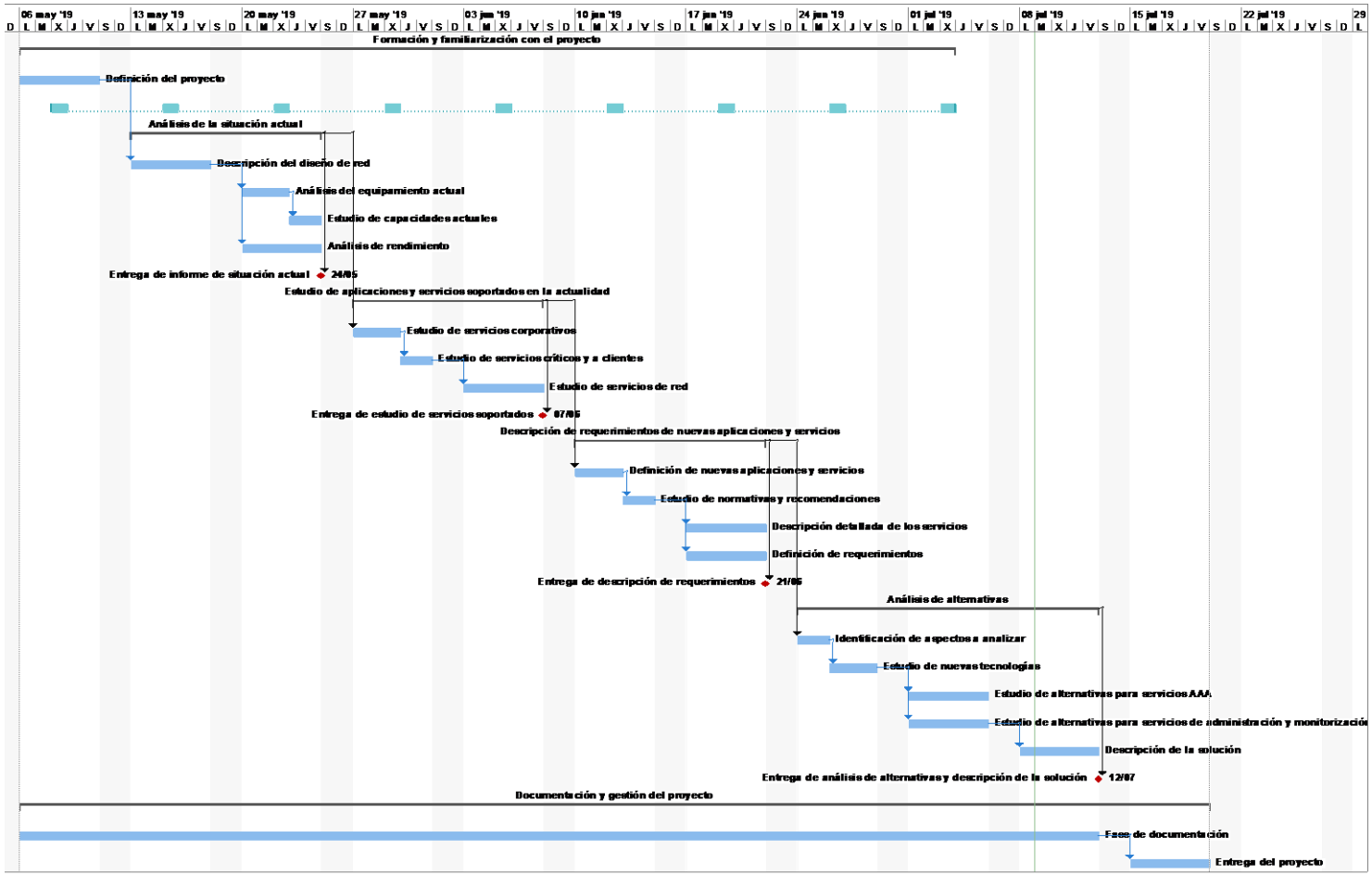



**Ilustración 7 Diagrama de Gantt del proyecto**

# 10. Presupuesto

Este apartado presenta el presupuesto de proyección. Este presupuesto comprende la realización del estudio y análisis de los servicios que se recogen en el documento.

El presupuesto contempla, por un lado, el coste de las horas internas de la dirección del proyecto, la labor de un ingeniero senior y un ingeniero junior. Por otro lado, se detallan los costes derivados de la amortización del equipamiento utilizado para la realización del proyecto. Además, el presupuesto contiene los gastos del material fungible de oficina. Para finalizar, se recogen los costes mencionados en una tabla resumen en la que se tienen en consideración los costes indirectos (como el 5% de los costes directos) y los imprevistos (10% del total).

**Tabla 21 Presupuesto - horas internas**

| Horas internas | Coste por hora | Carga de trabajo | Coste |
|---|---|---|---|
| Directora del proyecto | 60 €/hora | 30 horas | 1.800,00 € |
| Ingeniero senior | 50 €/hora | 20 horas | 1.000,00 € |
| Ingeniero junior | 15 €/hora | 300 horas | 4.500,00 € |
| TOTAL | | | **7.300,00 €** |

**Tabla 22 Presupuesto - amortizaciones**

| Amortizaciones | Coste | Vida útil | Uso | Coste |
|---|---|---|---|---|
| Lenovo L440 | 849 € | 5 años | 4 meses | 56,60 € |
| Windows 10 Pro | 259 € | 5 años | 4 meses | 17,27 € |
| Microsoft Office 365 | 69 € | 1 años | 3 meses | 17,25 € |
| TOTAL | | | | **91,12 €** |

**Tabla 23 Presupuesto - gastos**

| Gastos | Coste |
|---|---|
| Material de oficina | 100,00 € |
| TOTAL | **100,00 €** |

**Tabla 24 Presupuesto - coste total**

| Concepto | Coste |
|---|---|
| Horas internas | 7.300,00 € |
| Amortizaciones | 91,12 € |
| Gastos | 100,00 € |
| Subtotal | 7.491,12 € |
| Costes indirectos (5%) | 374,56 € |
| Subtotal | 7.865,67 € |
| Imprevistos (10%) | 786,57 € |
| TOTAL | **8.652,24 €** |

# 11. Conclusiones

Este proyecto estudia y analiza una solución para la mejora del rendimiento y la calidad de las aplicaciones y servicios en el entorno de una red corporativa. Concretamente, se presentan una serie de requerimientos para garantizar mejoras esenciales en el funcionamiento de la red de una delegación de la empresa de estructura centralizada

Los requerimientos establecidos están fundamentados en el análisis de las problemáticas de rendimiento y calidad que presenta actualmente la red corporativa en la sede de Bilbao.

Así mismo, el estudio ha tomado como punto de partida las recomendaciones y estándares más relevantes del sector. En base a todo ello, se ha desarrollado un análisis de alternativas para llegar a una solución adecuada de establecimiento de requerimientos de los servicios que permita ofrecer los mismos con garantías óptimas de funcionamiento.

El desarrollo del proyecto ha permitido a la oficina de SATEC en Bilbao marcar y establecer una solución homologada para los servicios que se pueda extender a todas las delegaciones. El trabajo forma parte de un proyecto global que pretende la mejora de la red corporativa de Bilbao mediante el rediseño de la infraestructura de red.

El proyecto global permite a la red corporativa funcionar y soportar los servicios demandados. Junto con los nuevos servicios que se plantean, la red dispone de las tecnologías más adecuadas para los servicios AAA y de administración y monitorización, ya que se han seleccionado las alternativas que mejor se ajustan a las necesidades de la empresa. Esto da lugar a un escenario en el que la sede principal de SATEC tiene las prestaciones necesarias para dar estos servicios de la mejor manera posible.

Por otro lado, se ha propuesto una arquitectura de servicios diferenciados para asegurar la calidad de servicio en la red. Acompañado de un modelo de clases adaptado a las nuevas aplicaciones y servicios, la red tiene las capacidades para clasificar y marcar el tráfico en función de los requerimientos propuestos para los servicios asegurando a los usuarios un nivel de calidad suficiente.

En conclusión, los resultados del estudio de los servicios llevado a cabo en el proyecto han sido el punto de partida para dotar a la red de una nueva infraestructura en la que se puedan soportar las nuevas aplicaciones y servicios asegurando la calidad del servicio, habilitando la mejora del rendimiento de la red corporativa de la delegación de Bilbao. Además, se ha establecido una solución homologada aplicable a todas las delegaciones de la empresa SATEC, siguiendo su estructura centralizada con sede principal en Madrid.

# 12. Bibliografía

Cisco. (2015). *Bandwidth Management.*

Eror, D. (17 de Junio de 2015). *Benefits of Implementing NETCONF*. Recuperado el 2019, de https://learning.nil.com/assets/Tips-/Benefits-of-implementing-NETCONF.pdf

ETSI. (2009). *TR 102 805-1: End-to-end QoS management at the Network Interfaces.*

IETF. (1993). *RFC 1492: An Access Control Protocol, Sometimes Called TACACS.*

IETF. (1994). *RFC 1633: Integrated Services in the Internet Architecture: an Overview.*

IETF. (1998). *RFC 2475: An Architecture for Differentiated Services.*

IETF. (2000). *RFC 2865: Remote Authentication Dial In User Service (RADIUS).*

IETF. (2002). *RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.*

IETF. (2006). *RFC 4594: Configuration Guidelines for DiffServ Service Classes.*

IETF. (2011). *RFC 6241: Network Configuration Protocol (NETCONF).*

IETF. (2012). *RFC 6733: Diameter Base Protocol.*

ITU-T. (2001). *G.1010 : End-user multimedia QoS categories.*

ITU-T. (2011). *Y.1541: Network performance objectives for IP-based services.*

Lopez, A. (5 de Febrero de 2015). *Protocolos AAA y control de acceso a red: Radius.* Recuperado el 2019, de https://www.incibe-cert.es/blog/protocolos-aaa-radius

Martin, M. (2019). Análisis y rediseño de la red de telecomunicaiones de una sucursal corporativa remota. UPV/EHU.

Moreno, J. I., & González, F. J. (sin fecha). *QoS Requirements for Multimedia Services.*

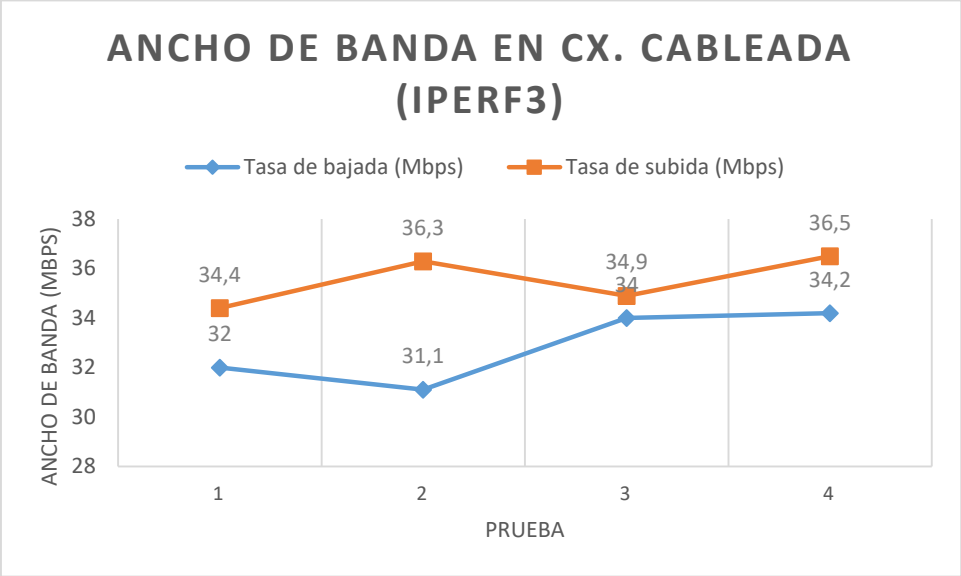
Ookla. (21 de Mayo de 2017). *How Does Speedtest Custom Work?* Recuperado el 2019, de https://support.ookla.com/hc/en-us/articles/115000234391-How-Does-Speedtest-Custom-Work-

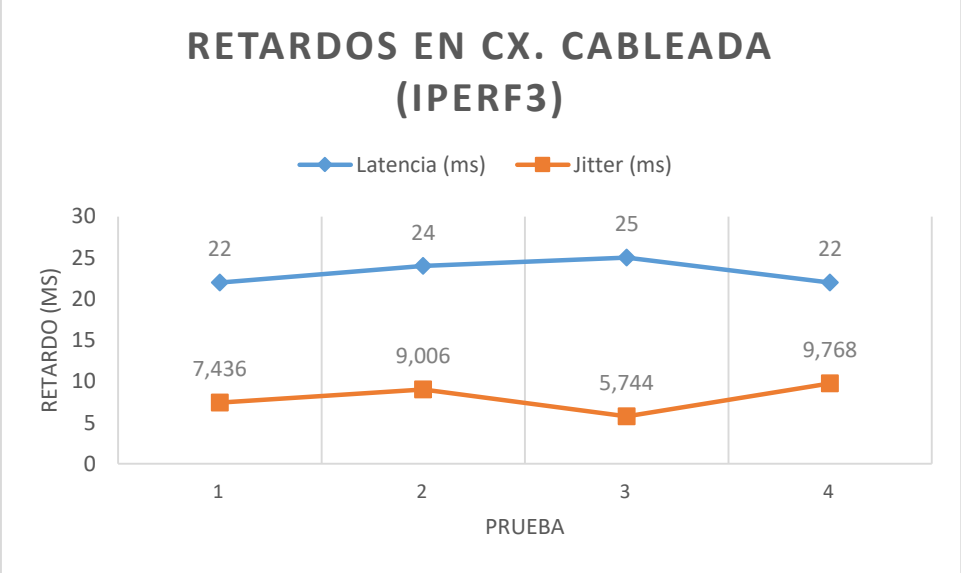
SATEC. (2019). *Página web de SATEC.* Recuperado el 2019, de https://www.satec.es/

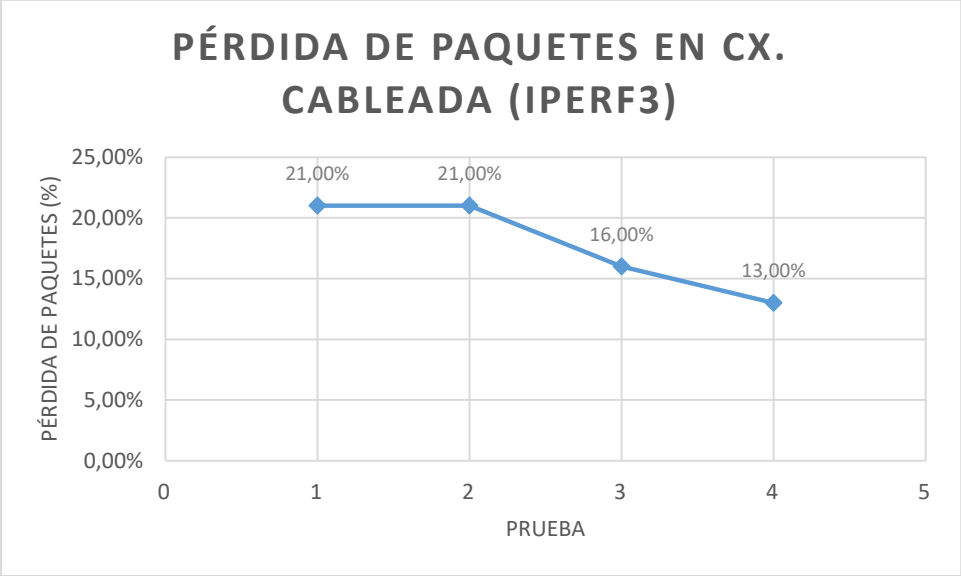
Szigeti, T. (2004). *End-to-End QoS Network Design.* Cisco Press.

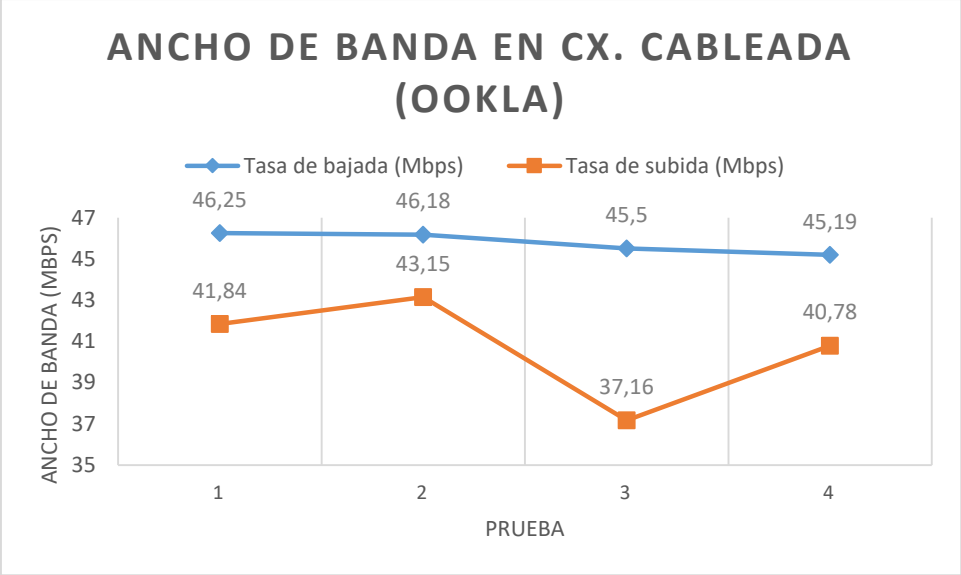
# Anexo I: Gráficas y análisis de rendimiento

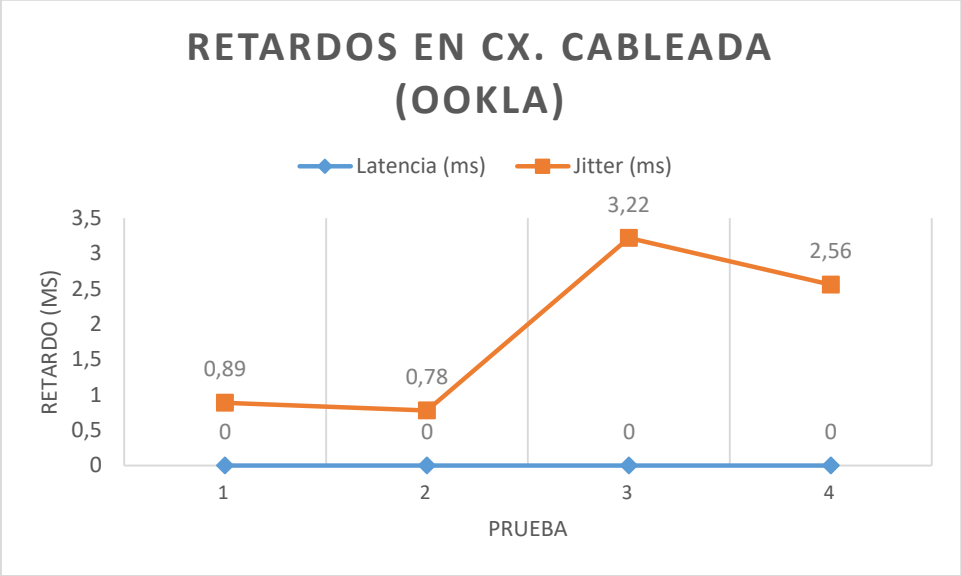
A continuación, se muestran las gráficas resultantes del análisis de rendimiento realizado en el apartado 5.4.

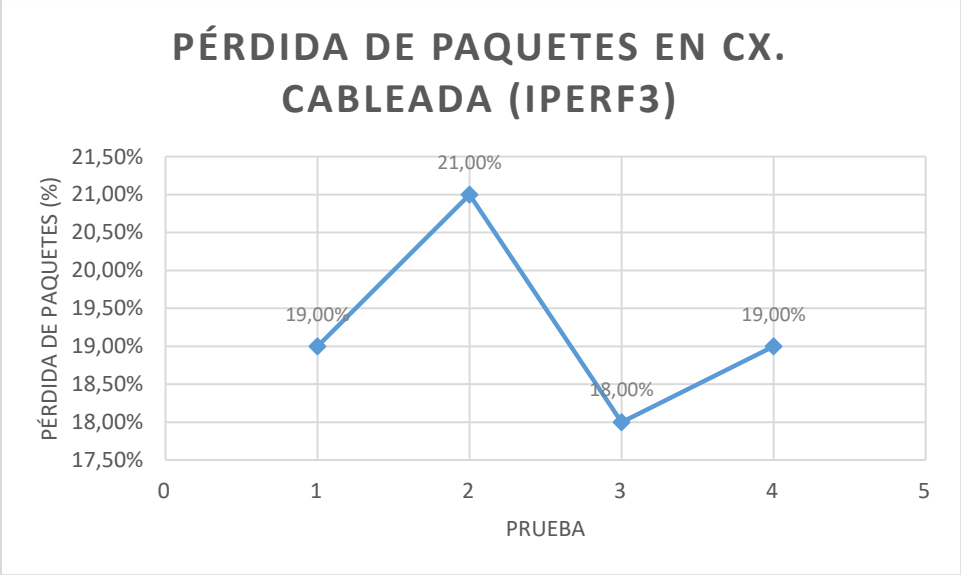


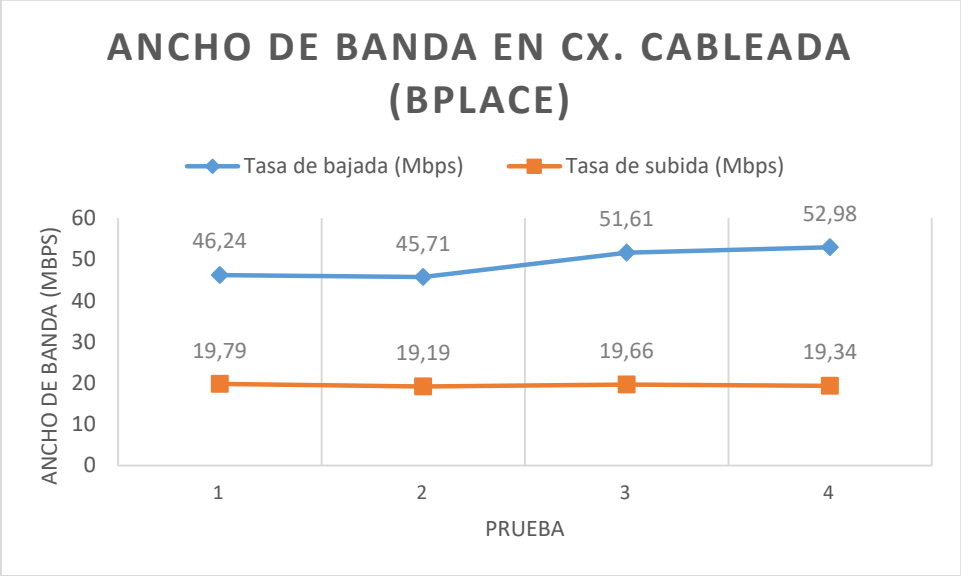



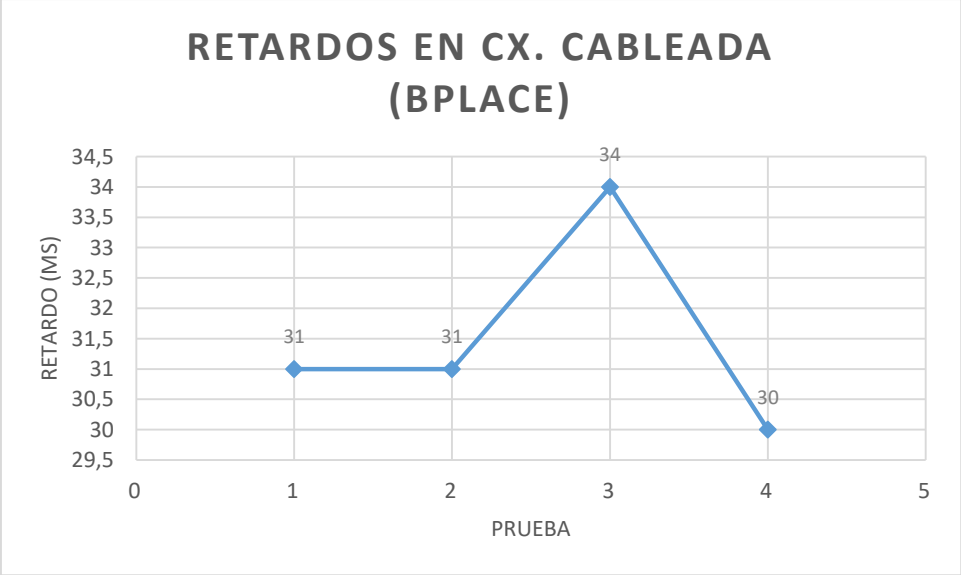

PÉRDIDA DE PAQUETES EN CX. CABLEADA (IPERF3)
PÉRDIDA DE PAQUETES (%)
25,00%
20,00%
15,00%
10,00%
5,00%
0,00%
21,00%
21,00%
16,00%
13,00%
0
1
2
3
4
5
PRUEBA

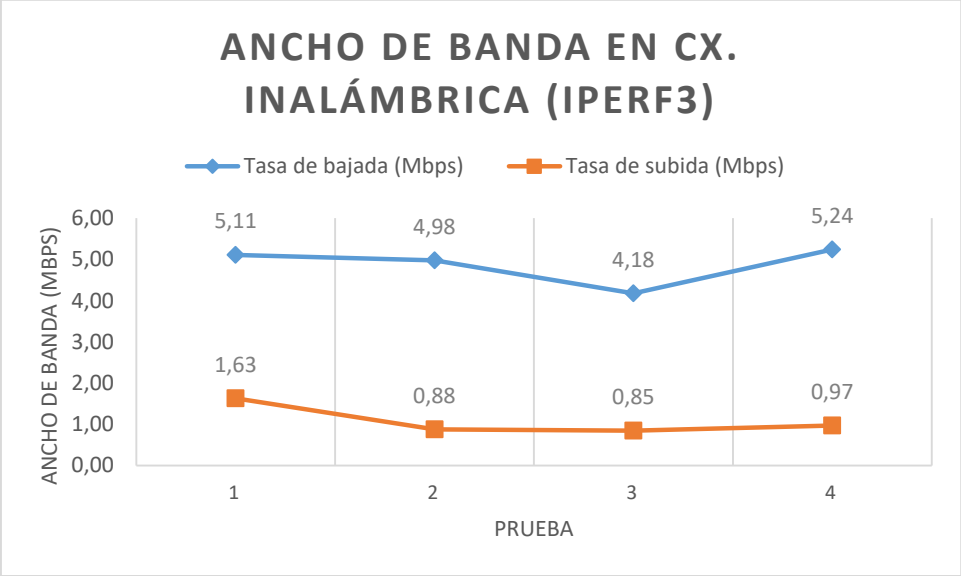

ANCHO DE BANDA EN CX. CABLEADA (OOKLA)
Tasa de bajada (Mbps)
Tasa de subida (Mbps)
ANCHO DE BANDA (MBPS)
47
45
43
41
39
37
35
46,25
46,18
45,5
45,19
41,84
43,15
37,16
40,78
1
2
3
4
PRUEBA

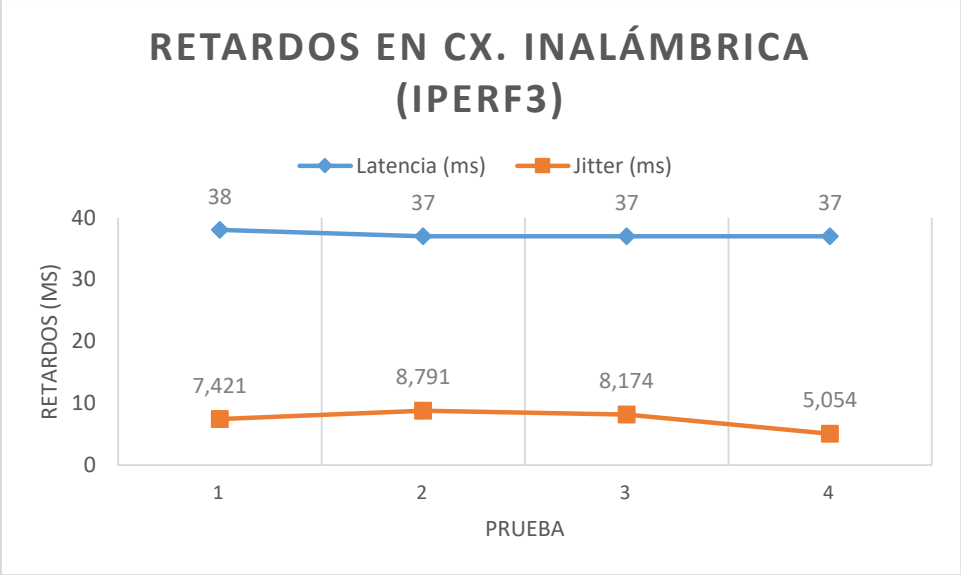

RETARDOS EN CX. CABLEADA (OOKLA)
Latencia (ms)
Jitter (ms)
RETARDO (MS)
3,5
3
2,5
2
1,5
1
0,5
0
0,89
0,78
3,22
2,56
0
0
0
0
1
2
3
4
PRUEBA

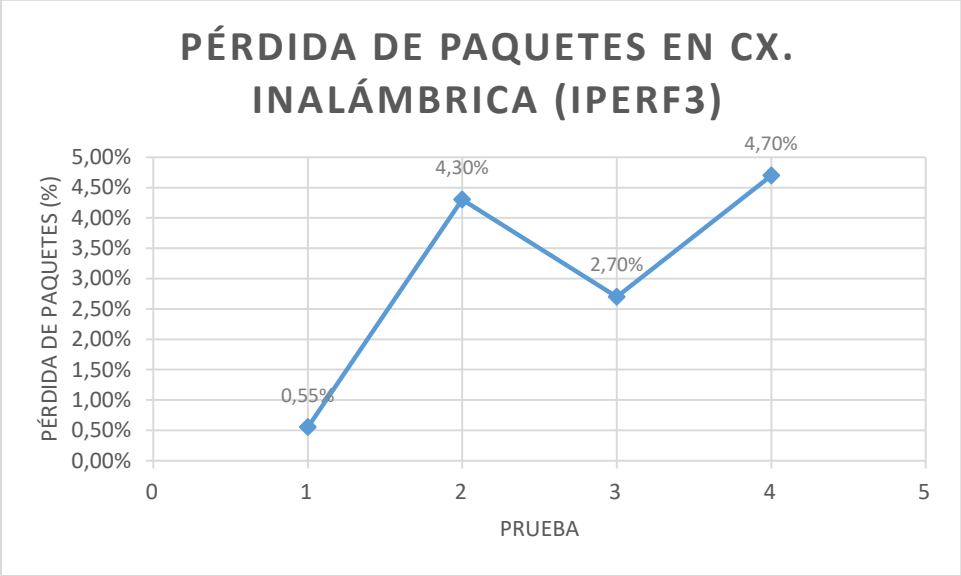

PÉRDIDA DE PAQUETES EN CX. CABLEADA (IPERF3)
PÉRDIDA DE PAQUETES (%)
21,50%
21,00%
20,50%
20,00%
19,50%
19,00%
18,50%
18,00%
17,50%
19,00%
21,00%
18,00%
19,00%
0
1
2
3
4
5
PRUEBA

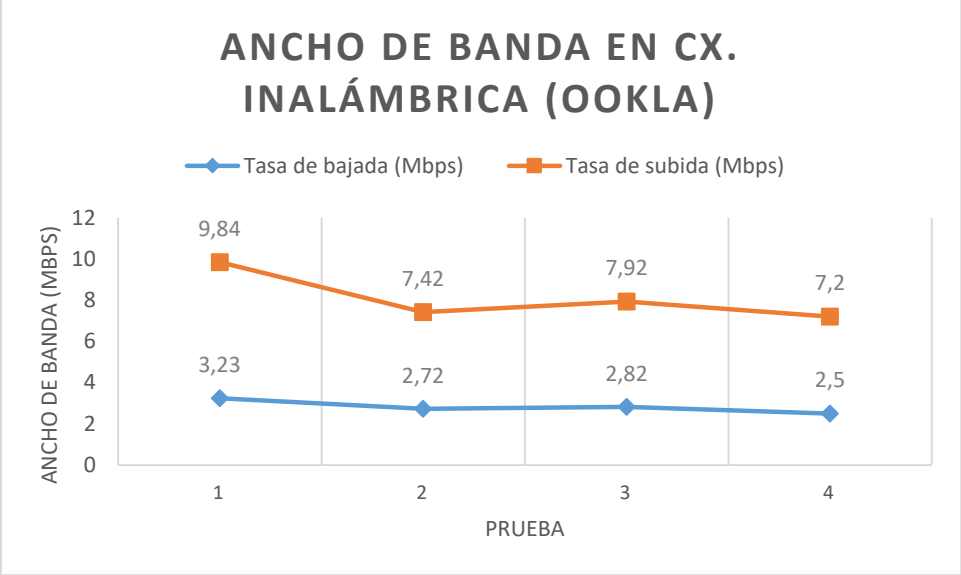

ANCHO DE BANDA EN CX. CABLEADA (BPLACE)
Tasa de bajada (Mbps)
Tasa de subida (Mbps)
ANCHO DE BANDA (MBPS)
60
50
40
30
20
10
0
46,24
45,71
51,61
52,98
19,79
19,19
19,66
19,34
1
2
3
4
PRUEBA

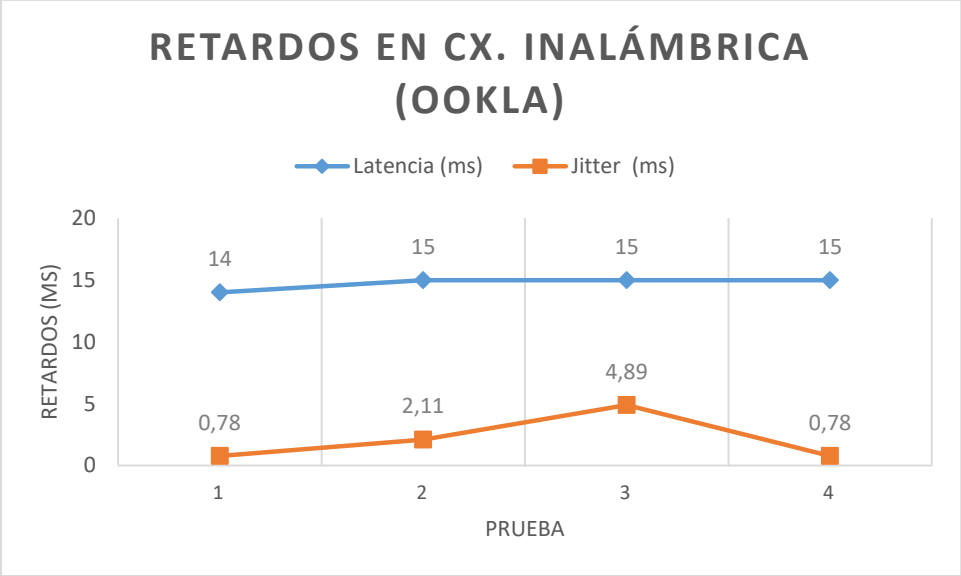

RETARDOS EN CX. CABLEADA (BPLACE)
RETARDO (MS)
34,5
34
33,5
33
32,5
32
31,5
31
30,5
30
29,5
31
31
34
30
0
1
2
3
4
5
PRUEBA

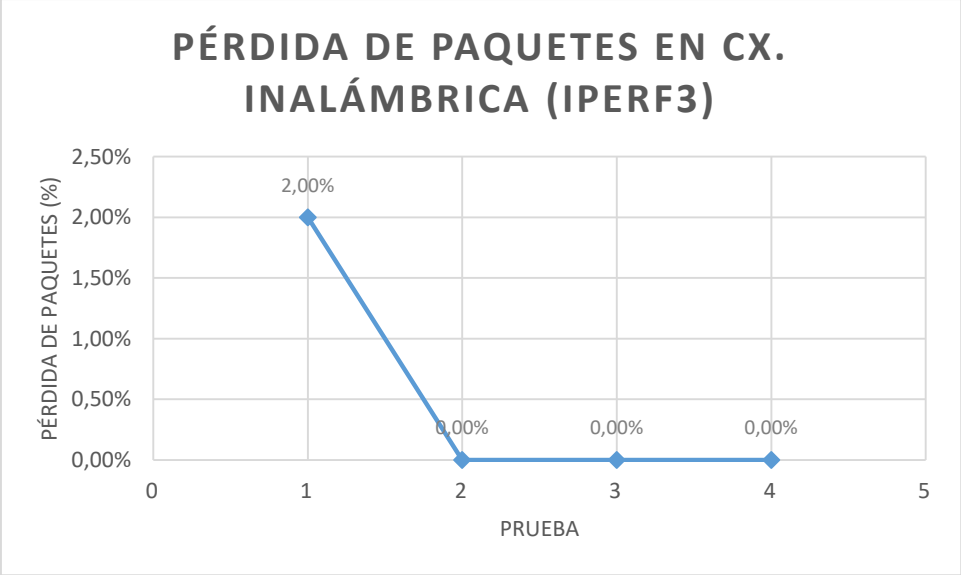

ANCHO DE BANDA EN CX. INALÁMBRICA (IPERF3)
Tasa de bajada (Mbps)
Tasa de subida (Mbps)
ANCHO DE BANDA (MBPS)
6,00
5,00
4,00
3,00
2,00
1,00
0,00
5,11
4,98
4,18
5,24
1,63
0,88
0,85
0,97
1
2
3
4
PRUEBA

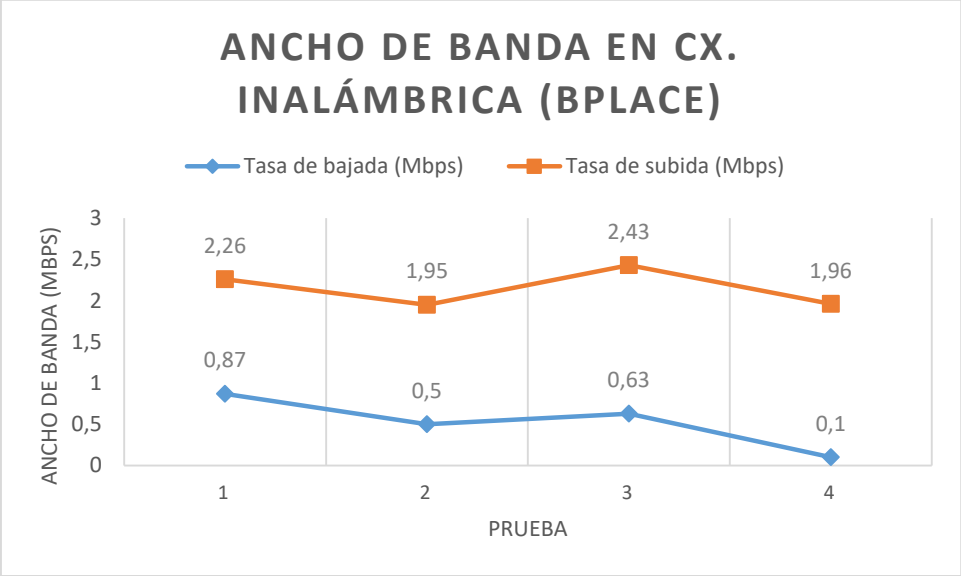

RETARDOS EN CX. INALÁMBRICA (IPERF3)
Latencia (ms)
Jitter (ms)
RETARDOS (MS)
40
30
20
10
0
38
37
37
37
7,421
8,791
8,174
5,054
1
2
3
4
PRUEBA

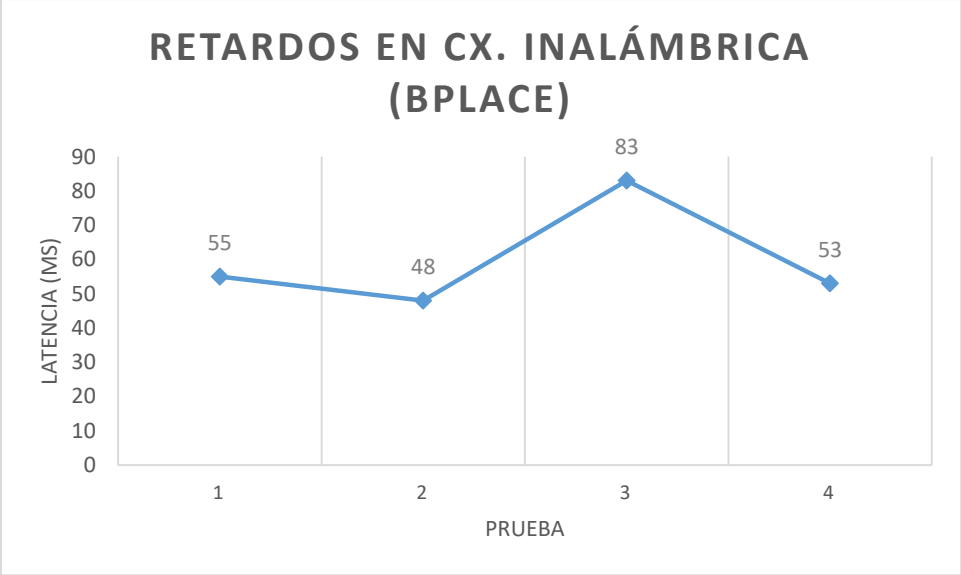

PÉRDIDA DE PAQUETES EN CX. INALÁMBRICA (IPERF3)
PÉRDIDA DE PAQUETES (%)
5,00%
4,50%
4,00%
3,50%
3,00%
2,50%
2,00%
1,50%
1,00%
0,50%
0,00%
0,55%
4,30%
2,70%
4,70%
0
1
2
3
4
5
PRUEBA


ANCHO DE BANDA EN CX. INALÁMBRICA (OOKLA)
Tasa de bajada (Mbps)
Tasa de subida (Mbps)
ANCHO DE BANDA (MBPS)
12
10
8
6
4
2
0
9,84
7,42
7,92
7,2
3,23
2,72
2,82
2,5
1
2
3
4
PRUEBA


RETARDOS EN CX. INALÁMBRICA (OOKLA)
Latencia (ms)
Jitter (ms)
RETARDOS (MS)
20
15
10
5
0
14
15
15
15
0,78
2,11
4,89
0,78
1
2
3
4
PRUEBA


PÉRDIDA DE PAQUETES EN CX. INALÁMBRICA (IPERF3)
PÉRDIDA DE PAQUETES (%)
2,50%
2,00%
1,50%
1,00%
0,50%
0,00%
2,00%
0,00%
0,00%
0,00%
0
1
2
3
4
5
PRUEBA


ANCHO DE BANDA EN CX. INALÁMBRICA (BPLACE)
Tasa de bajada (Mbps)
Tasa de subida (Mbps)
ANCHO DE BANDA (MBPS)
3
2,5
2
1,5
1
0,5
0
2,26
1,95
2,43
1,96
0,87
0,5
0,63
0,1
1
2
3
4
PRUEBA


RETARDOS EN CX. INALÁMBRICA (BPLACE)
LATENCIA (MS)
90
80
70
60
50
40
30
20
10
0
55
48
83
53
1
2
3
4
PRUEBA