

**DISEÑO DE UNA RED LAN PARA LA EMPRESA BITS AMERICAS
S.A.S**

CRISTIAN DAVID HENAO PINTO

JAIRO HERNAN GARCIA
DIRECTOR DE PROYECTO

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA
MAYO, 2019

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTRÓNICA

AREA DE ENFASIS: TELECOMUNICACIONES

**DISEÑO DE UNA RED LAN PARA LA EMPRESA BITS AMERICAS
S.A.S**

CRISTIAN DAVID HENAO PINTO

JAIRO HERNAN GARCIA
DIRECTOR DE PROYECTO

NOTA DE SALVEDAD

Según el artículo 37 del 14 de diciembre de 1989 del acuerdo 017, "La Universidad El Bosque, no se hace responsable de los conceptos emitidos por los investigadores en su trabajo, solo velará por el rigor científico, metodológico y ético del mismo en aras de la búsqueda de la verdad y la justicia".

AGRADECIMIENTOS

Agradezco primera mente a Dios, por permitirme vida y salud, oportunidades de tener un hogar, una familia, un trabajo y estudio ya que sin dicha ayuda nada de esto seria posible hoy en dia.

Quiero agradecer a mis padres por apoyarme durante estos 5 años con la carrera de ingenieria electronica tanto en la parte economica como en la parte motivacional.

Agradezco a mis amigos y compañeros de la universidad por hacer parte de este proceso en el que ellos hicieron parte e hicieron del tiempo allí un espacio de risas y experiencias que siempre tendre en el corazón.

Por ultimo agradezco a mi director Jairo Garcia y el jurado Carlos Castillo que me guiaron en el desarrollo de la tesis e hicieron que este documento fuese escrito lo mejor posible.

RESUMEN

Este proyecto plantea una propuesta de diseño a la infraestructura de red de datos de la empresa BITS AMERICAS SAS que a lo largo de los 10 años que se lleva consolidando como empresa no ha dedicado el tiempo necesario para diseñar su red LAN.

El planteamiento se hace sobre los usuarios que la empresa tendrá a 3 años y los servicios requeridos por la misma como lo son servicios de voz, datos y video en una sola infraestructura para hacer del diseño una solución que cumpla con las expectativas del cliente y pueda ejercer sus actividades como la creación de software a la medida de la mejor manera.

Por último, se entregará este documento para que sirva de base de planeación e implementación de la propuesta que aquí se presenta, contando con toda la información necesaria para poder implementar la solución y posiblemente si es de ayuda para cualquier otra entidad que este dentro de las PYMES.

Palabras Clave: LAN, redes, infraestructura, voz, datos, videos, IP, cableado estructurado, jerarquía, arquitectura.

ABSTRACT

This project proposes a design proposal to the data network infrastructure of the company BITS AMERICAS SAS, which over the 10 years that it has been consolidating as a company has not dedicated the time necessary to design its LAN network.

The approach is made about the users that the company will have for 3 years and the services required by it, such as voice, data and video services in a single infrastructure to make the design a solution that meets the client's expectations and can exercise your main activity like creating custom software in the best way.

Finally, this document will be delivered to serve as a basis for planning and implementation of the proposal presented here, with all the necessary information to implement the solution and possibly if it is helpful for any other entity that is within PYMES.

Keywords: network, infrastructure, voice, data, video, IP, structured wiring, hierarchy, architecture.

Tabla de Contenidos

1	Introducción	15
2	Definición del problema	15
2.1	Contexto	15
2.2	Manifestación	17
2.3	Causas	17
2.4	Efectos	17
2.5	Aspectos por solucionar	18
2.6	Justificación del proyecto	18
2.7	Propuesta de solución	19
3	Estado del arte	19
3.1	Bases teóricas.....	19
3.2	Tecnología.....	29
4	GLOSARIO DE TEMRINOS.....	31
5	Objetivos.....	32
5.1	General	32
5.2	Específicos.....	32
6	Requerimientos.....	32
6.1	Funcionales	32
6.2	De calidad	32
6.3	Restrictivos.....	33
7	Diseño Funcional.....	33
7.1	Caja con entradas y salidas.....	33
7.2	Propuestas de solución	34
7.2.1	Propuesta de solución 1	34
7.2.2	Propuesta de solución 2	34
7.3	Funciones de cada caja	35
7.3.1	Propuesta de solución 1	35
7.3.2	Propuesta de solución 2	35
7.4	Sumatoria de funciones vs función del sistema.....	36
7.4.1	Propuesta de solución 1	36
7.4.2	Propuesta de solución 2	36
7.5	Selección de propuesta.....	37

8	Diseño detallado	37
8.1	Diseño de la red alámbrica e inalámbrica	38
8.1.1	Calcular el número de clientes, servidores y dispositivos	38
8.1.2	Planear el diseño de la red	40
8.1.3	Selección del cableado estructurado de la red	49
8.1.4	Seleccionar el hardware de la red	53
8.1.5	Configuración Básica de los dispositivos	68
8.1.6	Configuración de enlaces troncales	70
8.1.7	Configuración protocolo troncal virtual	71
8.1.8	Definición y configuración de redes virtuales (VLANs).....	72
8.1.9	Direccionamiento IP.....	73
9	Plan de Pruebas del Sistema	76
9.1	Plan de pruebas IP Estáticas	76
9.2	Plan de pruebas DHCP.....	77
9.3	Plan de pruebas de VLSM	78
9.4	Plan de pruebas VTP	79
9.5	Plan de pruebas VLAN	80
9.6	Plan de pruebas de Ping	81
9.7	Plan de pruebas de disponibilidad y protocolo STP.....	81
10	IMPLEMENTACIÓN	82
11	Diseño industrial	88
11.1	Análisis de la actividad y el contexto	88
11.1.1	Análisis del contexto	88
11.1.2	Casos de uso	90
11.2	Requerimientos industriales.....	91
11.2.1	Requerimientos de uso	91
11.2.2	Requerimientos de función.....	92
11.2.3	Requerimientos de estructura.....	92
11.2.4	Requerimientos Legales y normativos	92
11.2.5	Requerimientos de identificación	93
11.3	Materiales, procesos y normativas	93
11.3.1	Materiales de Protección	93

11.3.2	Cableado	94
11.3.3	Procesos.....	96
11.3.4	Normativas	96
11.4	Planificación de la producción	98
11.4.1	Primera alternativa	98
11.4.2	Segunda alternativa.....	98
11.5	Diseño detallado.....	101
11.5.1	Definición de componentes principales.....	101
12	Resultados.....	103
13	Discusión.....	103
14	Conclusiones.....	104
15	Referencias Documentales	105
16	Anexos	106
16.1	Anexo A: Especificaciones técnicas dispositivos actuales	106
16.1.1	Sede Principal	106
16.1.2	Segunda sede	109
16.2	Anexo B: Especificaciones técnicas de los dispositivos a utilizar	113
16.3	Anexo C: Configuración de dispositivos	119
16.4	Anexo D: Documentación diseño industrial	125

Lista de Figuras

Figura 1, Bosquejo topología física actual	16
Figura 2, Red LAN (5)	20
Figura 3, Símbolos comunes de las redes de datos [5].....	22
Figura 4, Algunos protocolos vinculados a los servicios más usados. [5].....	22
Figura 5, Topología Punto a Punto. [5].....	25
Figura 6, Topología lógica punto a punto. [5]	25
Figura 7, Topología en Estrella.....	26
Figura 8, Topología Multiacceso. [5].....	27
Figura 9, Topología en anillo. [7]	27
Figura 10, Agregación de ancho de banda. [8].....	28
Figura 11, Diámetro de Red. [8]	28
Figura 12, Redundancia. [8]	29
Figura 13, Diseño jerárquico LAN [9].....	30
Figura 14, Sistema representado en bloques.....	33
Figura 15 Propuesta de solución 1.....	34
Figura 16, Propuesta de solución 2.....	35
Figura 17, Descripción de dispositivos necesarios en una red LAN	38
Figura 18, Crecimiento estimado a 3 años en el personal de BITS AMERICAS SAS ...	39
Figura 19, Numero de usuarios pico por tipo de actividad en una semana.....	41
Figura 20, Tabla de ancho de banda requerido por Microsoft teams y Skype	44
Figura 21, Tabla de ancho de banda en KBps consumido por RDC.....	46
Figura 22, Primer piso	50
Figura 23, Segundo piso.....	50
Figura 24, Boceto de topología de red	52
Figura 25, Topología red actual sede principal.....	53
Figura 26, Cisco RV082	62
Figura 27, Familia Switch 3COM 4800G	63
Figura 28, TP-LINK TL-SL3452.....	67

Figura 29, Máquina virtual para GNS3	83
Figura 30, GNS3 VM Información	83
Figura 31, Agregando los switches capa 2 y capa 3 con IOU	84
Figura 32, Topología de red diseñada.....	85
Figura 33, Capa de acceso topología red LAN BITS AMERICAS	85
Figura 34, Vlan y configuración de enlaces	86
Figura 35, Capa de Core/dist topología red LAN BITS AMERICAS.....	87
Figura 36, Consola de los dispositivos.....	88
Figura 37, Piso 1.....	89
Figura 38, Piso 2.....	89
Figura 39, Rack a utilizar	94
Figura 40, Cableado por regata.....	94
Figura 41, Cableado por techo falso	95
Figura 42, Especificaciones categoría cable UTP	95
Figura 43, Cable UTP categoria 5E	96
Figura 44, Primera alternativa de cableado	98
Figura 45, Segunda alternativa de cableado.....	99

Lista de Tablas

Tabla 1, Calculo de numero de clientes, servidores y dispositivos	40
Tabla 2, Estudio de simultaneidad de usuarios	42
Tabla 3, Ancho de banda total necesario para internet	47
Tabla 4, Ancho de banda total necesario para intranet	48
Tabla 5, Caracteristicas router/firewall elegido	63
Tabla 6, Caracteristicas Switch 3COM 4800G.....	64
Tabla 7, Precios del switch 3COM 4800G 48port.....	65
Tabla 8, Comparación switch capa 2	66
Tabla 9, Caracteristicas TP-LINK TL-SL3452.....	67
Tabla 10, nombre de los dispositivos.....	69
Tabla 11, banner de presentación	70
Tabla 12, configuración de contraseñas de modo privilegiado	70
Tabla 13, Configuración de enlaces troncales	71
Tabla 14, Configuración VTP.....	72
Tabla 15, direccionamiento IP.....	74
Tabla 16, Asignación de VLANS.....	75
Tabla 17, Plan de pruebas IP Estaticas	76
Tabla 18, Plan de pruebas DHCP.....	77
Tabla 19, Plan de pruebas VLSM.....	78
Tabla 20, Plan de pruebas VTP	79
Tabla 21, Plan de pruebas VLANS.....	80
Tabla 22, Plan de pruebas PING.....	81
Tabla 23, Plan de pruebas STP y disponibilidad	82
Tabla 24, Caracteristicas cable UTP Cat 5E	96
Tabla 25, Evaluación de las alternativas	99
Tabla 26, Componentes a utilizar	101

1 INTRODUCCIÓN

Los desafíos que las tecnologías de la información (TI) han traído consigo, han hecho que la manera en la que se comunican las empresas en la actualidad evolucione a pasos agigantados, basta con conocer las tendencias top como BYOD (Bring Your Own Device) lo que hace pensar que las redes de datos actuales y su infraestructura deben diseñarse para estar preparadas para los millones de millones de equipos que se pueden conectar a la red. Es por eso por lo que el diseño debe tener en cuenta las comunicaciones online como documentos compartidos, comunicaciones de video o en la nube, debido a que las redes cada vez están más orientadas a los servicios y aplicaciones.

BITSAMERICAS S.A.S es una empresa que está en ese constante cambio y aprovecha esa orientación de las redes a los servicios y aplicaciones para llevar a cabo su actividad principal que es desarrollar software a la medida. Es por eso por lo que una empresa que depende tanto de su infraestructura de red no puede quedarse atrás en esta área de la tecnología. Cuando se decidió trabajar con esta empresa, se tuvo en cuenta que sus procesos y proyectos se están viendo alterados por constantes caídas del sistema y tiempo perdido al resolver fallas repetitivas, esto por no contar con una documentación del funcionamiento y estructura de su red y las lecciones aprendidas del historial de fallos que han venido teniendo.

Por lo anterior el proyecto presente propondrá los aspectos necesarios para aplicar los conceptos que se han venido aprendiendo a lo largo de la carrera en el área de la telemática y aplicar los conocimientos al servicio de entidades como BITSAMERICAS S.A.S.

2 DEFINICIÓN DEL PROBLEMA

2.1 Contexto

Durante los últimos cuatro años la empresa diseñadora de software a la medida Bits Américas S.A.S presentó un crecimiento exponencial debido a el contacto con clientes multinacionales como Carvajal y Millicom, Además de la fusión con una empresa llamada INNANA que contaba con un producto prestador de servicios a las entidades de salud llamado

IMedical. Desde entonces, el recurso humano ha venido creciendo, llegando hoy en día a 90 personas, generando una separación en dos sedes en la ciudad de Bogotá. Debido a esto el área de TI fue reforzando la infraestructura de red de una forma plana y sin las características básicas que la arquitectura necesita para cumplir con las expectativas de los usuarios como tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.

Además, el uso indiscriminado del ancho de banda por parte de los empleados genera que la red se caiga de 3 a 5 veces por semana, repercutiendo en los indicadores de los usuarios y su rendimiento al ejecutar proyectos. Esto se puede evidenciar debido a que últimamente se estima que los proyectos se están demorando un 5% más del tiempo planificado por solicitudes de soporte de parte de los usuarios quejándose de la red. [1]

La infraestructura actual no cuenta con políticas de seguridad que se encargue de controlar el tráfico entrante y saliente de datos, por esta razón, los servidores locales que almacenan la información contable, administrativa, telefonía IP y pruebas están expuestos a cualquier tipo de hackeo. Además, los switches de acceso simplemente están multiplicando la densidad de puertos que el router no tiene para abastecer la cantidad de empleados, y no existe una segmentación en la red que permitan la confidencialidad de información según el rol del empleado que puede ser Administrativos, Comerciales, TI o Servicios TI. Ver [Figura 1](#).

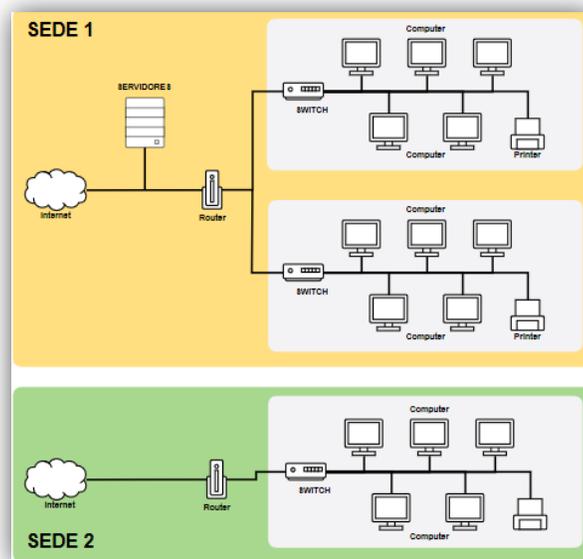


Figura 1, Bosquejo topología física actual

Por último y no menos importante, no existe documentación de la información que define la infraestructura y funcionamiento de la red, como direccionamiento, topología física y lógica, haciendo tediosa la administración y control.

2.2 Manifestación

La empresa BITS AMERICAS S.A.S manifiesta que aprovechará la oportunidad de traslado y unificación de sede para replantear el diseño de red LAN con el que cuentan, debido a que durante los últimos 8 meses se ha presentado un incremento en los reclamos y quejas referentes a fallas o lentitud en la red porque la misma no fue pensada para el personal que lo conforman actualmente.

2.3 Causas

Las causas del problema son:

1. La infraestructura de red de datos se ha venido consolidando con soluciones paliativas, no se tuvo previsto el crecimiento, por lo tanto, no es escalable, es decir cuenta con un diseño plano y no con un correcto diseño jerárquico.
2. No se tienen en cuenta los diversos tipos de tráfico, ni se clasifica según su prioridad ocasionando que las aplicaciones de la red se hagan lentas y esta misma inestable.
3. No existe una segmentación en la red para dividir el tráfico que circula por en la parte de servicios y aplicaciones según el rol del usuario, es decir no cuenta con procesos de control y seguridad.
4. inexistencia de la documentación de la estructura y funcionamiento de la red la hace tediosa de controlar y administrar.

2.4 Efectos

Los efectos que conlleva este problema son:

1. la empresa ha tenido que incurrir en costos adicionales innecesarios de ancho de banda en su canal dedicado, llegando actualmente a las 40Megas, incrementando su presupuesto mensual para ISP, pasando de 1.8 millones a 4 millones mensuales.

2. La empresa está invirtiendo 10 millones de pesos aproximadamente en soluciones circunstanciales para mantener la calidad de servicio a sus clientes por culpa de la infraestructura de red.
3. Actualmente las solicitudes de soporte dentro de la empresa son un 80% la degradación de los aplicativo utilizados y un 20% están relacionados con la indisponibilidad de la red.
4. La empresa tuvo que contratar 2 ingenieros de soporte adicionales asignados a cada sede para contrarrestar el problema de la red. Esto representa gastos adicionales.
5. La red se cae entre 3 a 5 veces por semana. Ocasionando tiempos muertos de los empleados de la empresa al no tener medios de conexión a la red. Esto representa incumplimiento en los compromisos adquiridos con los clientes.
6. Las teleconferencias con los clientes potenciales se ven afectadas debido a la intermitencia de la propia red. Dejando una imagen corporativa de bajo nivel.
7. El control de la infraestructura de red de datos actual es ineficiente porque no se tiene documentada la misma.

2.5 Aspectos por solucionar

Los aspectos por solucionar dentro del proyecto son:

1. La infraestructura de red de datos se ha venido consolidando con soluciones paliativas, no se tuvo previsto el crecimiento, por lo tanto, no es escalable, es decir cuenta con un diseño plano y no con un correcto diseño jerárquico.
2. No existe una segmentación en la red para dividir el tráfico que circula por en la parte de servicios y aplicaciones según el rol del usuario, es decir no cuenta con procesos de control y seguridad.
3. No se tienen en cuenta los diversos tipos de tráfico, ni se clasifica según su prioridad ocasionando que las aplicaciones de la red se hagan lentas y esta misma inestable.
4. La inexistencia de la documentación de la estructura y funcionamiento de la red la hace tediosa de controlar y administrar.

2.6 Justificación del proyecto

Se evidencia la necesidad de realizar este proyecto debido a que plantear un nuevo diseño a la red de la empresa permitirá tener una administración organizada y preparada para controlar las operaciones que mantiene la empresa a diario y de ofrecer una alta calidad de servicio para los recursos humanos de la compañía.

Además, la información estará protegida bajo un dispositivo de seguridad de la red que monitorea el tráfico y decide si permite o bloquea algún tráfico en específico y debido a la segmentación de la red, evitando así la infiltración de entes maliciosos a la red local y controlando todos los datos de entrada y salida que se manejan entre las sedes y que viajan por internet.

Al contar con una red apta para posibles contingencias permite tener la capacidad de detectar un fallo de la manera más rápida posible y que, a la vez, sea capaz de recuperarse del problema de forma eficiente, afectando lo menos posible al servicio que es la herramienta de trabajo principal de todo el personal y además para responder a tiempo a sus clientes.

2.7 Propuesta de solución

Estudio de diseño para la red LAN de la empresa en su nueva sede para garantizar la calidad de servicio a sus empleados y la seguridad de su propia información.

3 ESTADO DEL ARTE

3.1 Bases teóricas

Las redes de área local **LAN** son redes de datos que cubre un área geográfica relativamente pequeña. Por lo general, conecta estaciones de trabajo, computadoras personales, impresoras, servidores y otros dispositivos. Las LAN ofrecen a los usuarios de computadoras muchas ventajas, incluido el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos entre usuarios conectados y la comunicación entre usuarios a través del correo electrónico y otras aplicaciones.[3]

En definitiva, permite una conexión entre dos puntos o más equipos permitiéndoles el intercambio de información para compartir recursos. el termino red engloba tanto la parte de

hardware como software necesario para la interconexión de los distintos dispositivos y la manipulación de información.[4]

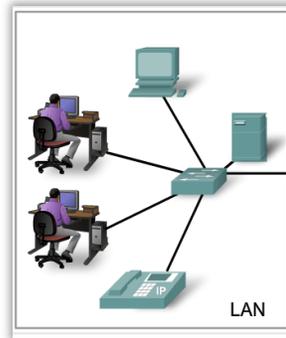


Figura 2, Red LAN (5)

En principio, las empresas utilizaban redes de datos para registrar y administrar internamente la información financiera, la información del cliente y los sistemas de nómina de empleados. Las redes comerciales evolucionaron para permitir la transmisión de diferentes tipos de servicios de información, como e-mail, video, mensajería y telefonía. Las intranets, redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales. Las compañías desarrollan extranet o internetwork extendidas para brindarles a los proveedores, fabricantes y clientes acceso limitado a datos corporativos para verificar estados, inventario y listas de partes.[5]

Poder comunicarse en forma confiable con todos en todas partes es de vital importancia para nuestra vida personal y comercial. Para respaldar el envío inmediato de los millones de mensajes que se intercambian entre las personas de todo el mundo, confiamos en una Web de redes interconectadas. Estas redes de información o datos varían en tamaño y capacidad, pero todas las redes tienen cuatro elementos básicos en común:

- Reglas y acuerdos para regular cómo se envían, redireccionan, reciben e interpretan los mensajes,
- Los mensajes o unidades de información que viajan de un dispositivo a otro,
- Una forma de interconectar esos dispositivos, un medio que puede transportar los mensajes de un dispositivo a otro.[5]
- Los dispositivos de la red que cambian mensajes entre sí.

La estandarización de los distintos elementos de la red permite el funcionamiento conjunto de equipos y dispositivos creados por diferentes compañías. Los expertos en diversas tecnologías pueden contribuir con las mejores ideas para desarrollar una red eficiente sin tener en cuenta la marca o el fabricante del equipo.[5]

La interconexión de redes es un tema orientado gráficamente y los íconos se utilizan comúnmente para representar sus dispositivos. En la parte izquierda del diagrama se muestran algunos dispositivos comunes que generalmente originan mensajes que constituyen nuestra comunicación. Esto incluye diversos tipos de equipos (se muestran íconos de una computadora de escritorio y de una portátil), servidores y teléfonos IP. En las redes de área local, estos dispositivos generalmente se conectan a través de medios LAN (con cables o inalámbricos). El lado derecho de la figura muestra algunos de los dispositivos intermedios más comunes, utilizados para direccionar y administrar los mensajes en la red, como así también otros símbolos comunes de interconexión de redes. Los símbolos genéricos se muestran para:

- Switch: el dispositivo más utilizado para interconectar redes de área local,
- Firewall: proporciona seguridad a las redes,
- Router: ayuda a direccionar mensajes mientras viajan a través de una red,
- Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas,
- Nube: se utiliza para resumir un grupo de dispositivos de red, sus detalles pueden no ser importantes en este análisis,
- Enlace serial: una forma de interconexión WAN (Red de área extensa), representada por la línea en forma de rayo.(5)

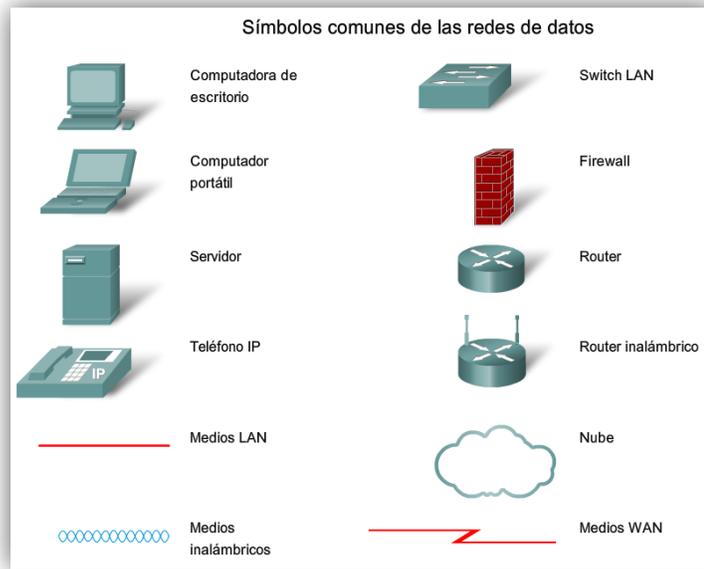


Figura 3, Símbolos comunes de las redes de datos [5]

Las personas generalmente buscan enviar y recibir distintos tipos de mensajes a través de aplicaciones informáticas; estas aplicaciones necesitan servicios para funcionar en la red. Algunos de estos servicios incluyen World Wide Web, e-mail, mensajería instantánea y telefonía IP. Los dispositivos interconectados a través de medios para proporcionar servicios deben estar gobernados por reglas o protocolos. En el cuadro se enumeran algunos servicios y un protocolo vinculado en forma más directa con ese servicio.[5]

Servicio	Protocolo ("Regla")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Mensaje instantáneo (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Sistema abierto para la comunicación en tiempo real)
Telefonía IP	SIP (Session Initiation Protocol)

Figura 4, Algunos protocolos vinculados a los servicios más usados. [5]

Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí. Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado

TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.[5]

Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad.[5]

- **Tolerancia a fallas**

Una red tolerante a fallas es la que limita el impacto de una falla del software o hardware y puede recuperarse rápidamente cuando se produce dicha falla. Estas redes normalmente tienen enlaces o rutas redundantes entre el origen y el destino del mensaje. Tanto las infraestructuras físicas como los procesos lógicos que direccionan los mensajes a través de la red están diseñados para adaptarse a esta redundancia.[5]

- **Escalabilidad**

Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. La capacidad de la red de admitir estas nuevas interconexiones depende de un diseño jerárquico en capas para la infraestructura física subyacente y la arquitectura lógica. El funcionamiento de cada capa permite a los usuarios y proveedores de servicios insertarse sin causar interrupción en toda la red.[5]

- **Calidad de servicio (QoS)**

Los nuevos requerimientos para admitir una buena calidad de servicio en una red convergente cambian la manera en que se diseñan e implementan las arquitecturas

de red. Las transmisiones de voz y video en vivo requieren un nivel de calidad consistente y un envío ininterrumpido que no era necesario para las aplicaciones informáticas tradicionales. La calidad de estos servicios se mide con la calidad de experimentar la misma presentación de audio y video en persona. Las redes de voz y video tradicionales están diseñadas para admitir un único tipo de transmisión y, por lo tanto, pueden producir un nivel aceptable de calidad.[5]

- **Seguridad**

Debido a la cantidad de información crítica y confidencial que se transmite entre los distintos usuarios de una red empresarial, las necesidades de seguridad y privacidad han sido incluidas en el diseño de la arquitectura de redes.[5] [6]

Los problemas que normalmente presentan las redes y que son consecuencia de los ataques a las mismas son:

- Interrupciones de red que evitan la realización de las comunicaciones.
- Direccionamiento enfocado a destinos no deseados obteniendo así información confidencial de la empresa.
- Hurto de la información.
- Pérdida de confianza dentro del mercado.

Cuando se tienen los elementos que pertenecen a una red, ya sean routers, switches, ordenadores, servidores, etc. La configuración o la relación que existe entre los elementos y la interconexión de los mismo se le llama topología. Estas se pueden definir en un nivel físico o en un nivel lógico.[5]

- **Topología Física**

Hace referencia a la manera como se usan los medios para interconectar con los dispositivos, se especifican la configuración de los nodos y las conexiones físicas entre ellos.[5]

- **Topología Lógica**

Hace referencia a las conexiones virtuales entre los nodos de una red independiente de su distribución física, es decir, especifica la forma en que una red transmite tramas de un nodo al otro.[5]

Las topologías más usadas generalmente en el diseño de redes son:

- **Punto a Punto**

Una topología punto a punto conecta dos nodos directamente entre sí, es decir que todas las tramas que se coloquen en el medio solo pueden viajar entre los dos nodos (desde y hacia). [5]

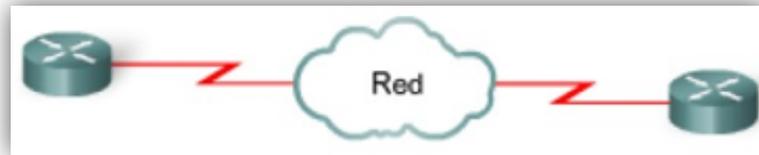


Figura 5, Topología Punto a Punto. [5]

Esto no necesariamente indica que los nodos están conectados directos físicamente, es decir conectados por medio de un cable, entre los nodos se pueden presentar una cantidad N de dispositivos, sin embargo, la topología lógica no se afecta, en donde a pesar de tener varios dispositivos entre los nodos la topología continúa siendo Punto a Punto:[5]



Figura 6, Topología lógica punto a punto. [5]

Estrella.

En este tipo de topología, cada estación de trabajo está conectada directamente a un dispositivo central, el cual es el encargado de realizar el reenvío de las tramas que reciba. [7]

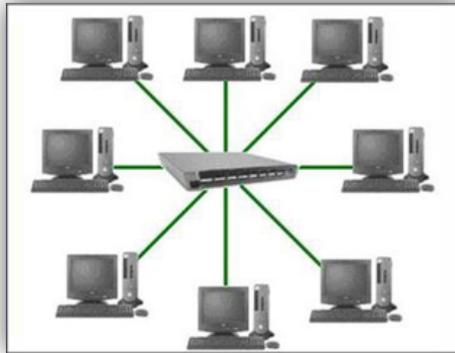


Figura 7, Topología en Estrella.

Como dispositivo central se puede utilizar un *Hub* (Repetidor), el cual se encarga de recibir las tramas y reenviarlas a todas las estaciones conectadas a él. Este tipo de dispositivos no son ya comúnmente utilizados, dado que permite que se generen colisiones que terminan deteriorando el funcionamiento de la red. [5]

Por lo anterior, como dispositivo central se recomienda utilizar una *Switch* el cual realiza la conmutación de tramas, es decir, recibe una trama y esta es solo enviada por la interfaz en donde se encuentra conectada la estación de trabajo destino.[5]

- **Multi-acceso**

Este tipo de topología permite a una cantidad de nodos comunicarse entre a través de un mismo medio de transmisión. Todos los nodos de la red pueden ver las tramas que se colocan en el medio y analizan si ellos son el destinatario. Solo el destinatario procesa los contenidos de la trama. [5]

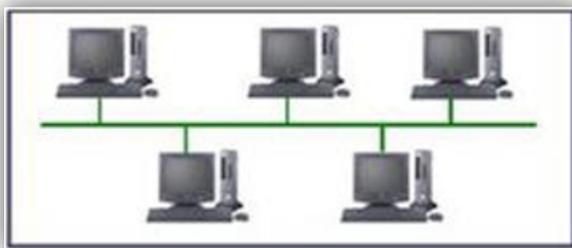


Figura 8, Topología Multiacceso. [5]

Debido a que todas las estaciones de trabajo comparten el mismo medio para transmitir, se presenta una competencia por acceder y utilizar el medio.[7]

- **Anillo**

Esta topología se compone de un solo anillo cerrado formado por nodos y enlaces, es decir que cada nodo sólo está conectado con sus dos nodos adyacentes.[7]

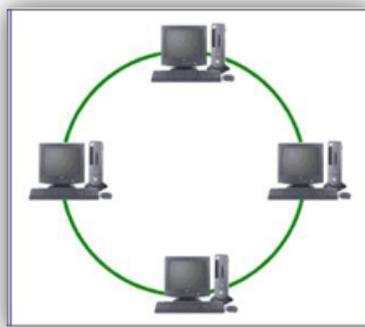


Figura 9, Topología en anillo. [7]

En esta topología cada estación de trabajo recibe una trama por turno y si la trama no está direccionada al nodo, entonces el nodo pasa la trama a la siguiente estación de trabajo. Esto permite que se utilice la técnica *Token* para acceder y utilizar el medio.[7]

En la actualidad se ha establecido que un buen diseño de red es aquel que utiliza una arquitectura jerárquica, sin embargo, no es el único criterio que evaluar debido a que se deben tener en cuenta muchos factores adicionales al momento de realizar el diseño para cumplir de la mejor manera con las necesidades del cliente.

A continuación, se explican algunos de los principios básicos de diseño que se deben

considerar:

- **Ancho de banda agregado.**

Este principio considera preciso las necesidades del cliente para optimizar el ancho de banda posible en la red, para esto se agregan dos o más puertos de enlaces entre determinados Switch con lo que se logra un rendimiento superior entre dichos *switchs*. [8]

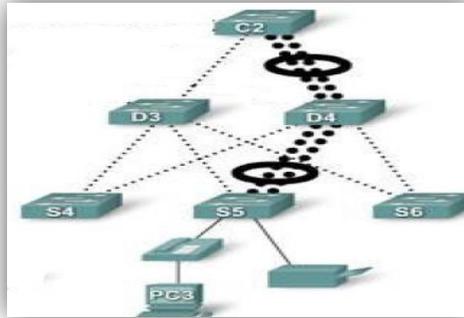


Figura 10, Agregación de ancho de banda. [8]

- **Diámetro de Red**

Se entiende por diámetro en telemática como la cantidad de dispositivos que un paquete de información debe cursar antes de alcanzar su destino. Si este diámetro durante el diseño de la red se mantiene en niveles bajos, se asegura que la red tendrá una latencia baja y predecible entre los dispositivos, es decir el tiempo en que se demora en procesar la información uno de los dispositivos de la red. [8]

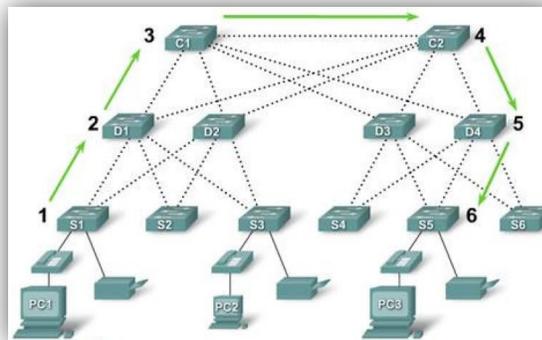


Figura 11, Diámetro de Red. [8]

- **Redundancia**

Con este principio se busca darle alta disponibilidad a la red que se está diseñando, esto se puede lograr de tres maneras, una con duplicidad de conexiones entre los equipos, la segunda con duplicidad de dispositivos y la tercera con una combinación de las dos maneras anteriores.[8]

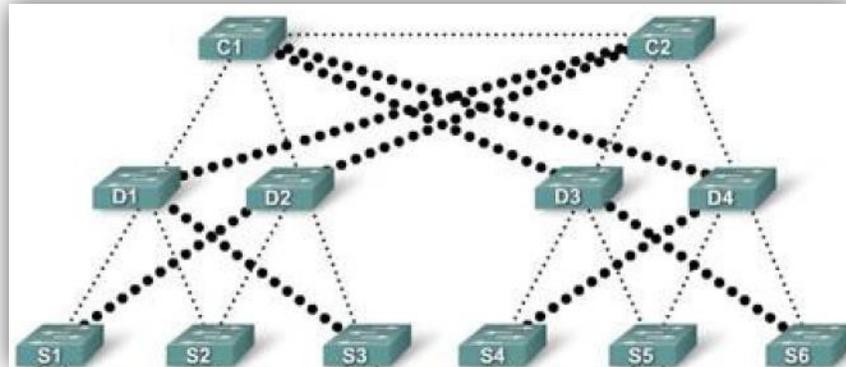


Figura 12, Redundancia. [8]

3.2 Tecnología

Actualmente la tecnología LAN cableada en campus usa un modelo de diseño jerárquico para desglosarlo en grupos modulares o capas. Este desglose del diseño en capas permite a cada capa implementar funciones específicas, lo que simplifica el diseño de red y, por lo tanto, la implementación y administración de la red. El modularidad en el diseño de red permite crear elementos de diseño que pueden replicarse en toda la red. La replicación ofrece una manera sencilla de ampliar la red, así como también un método de implementación homogéneo. En arquitecturas de red mallada o plana, los cambios tienden a afectar a una gran cantidad de sistemas. Un diseño de red LAN jerárquico incluye las siguientes tres capas:[9]

- **Capa de acceso:** ofrece a los terminales y usuarios acceso directo a la red.[9]
- **Capa de distribución:** une las capas de acceso y ofrece conectividad a los servicios.(9)

- **Capa central:** ofrece conectividad entre las capas de distribución para entornos de LAN grandes.[9]

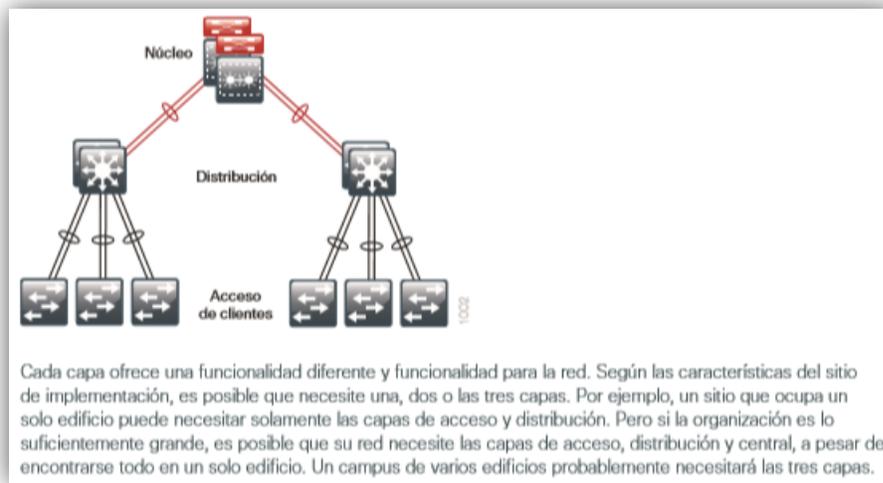


Figura 13, Diseño jerárquico LAN [9]

Hay una tendencia a deducir la red como una simple plomería, pensar que todo lo que tiene que considerar es el tamaño y la longitud de las tuberías o las velocidades y avances de los enlaces, y descartar el resto como no importante. Así como las tuberías en un estadio grande o en una gran altura tienen que diseñarse para su escala, propósito, redundancia, protección contra manipulación o denegación de operación y la capacidad para manejar cargas máximas, la red requiere una consideración similar. Dado que los usuarios dependen de la red para acceder a la mayoría de la información que necesitan para realizar su trabajo y para transportar su voz o video con confiabilidad, la red debe ser capaz de proporcionar transporte flexible e inteligente. El diseño de red confiable también necesita incorporar versatilidad para abordar las necesidades cambiantes de una organización. Estos son algunos conceptos clave que debe abordar al crear un diseño de red confiable y versátil.

La red debe ser:[10]

- **Auto curación:** continua y disponible.[10]
- **Auto defensa:** proteger a la organización y sus usuarios.[10]

- **Auto optimizado:** se adapta a las necesidades cambiantes, más allá de los límites de los estándares básicos.[10]
- **Auto consciente:** impulsa el cambio a través de la percepción de la actividad de la red.[10]

4 GLOSARIO DE TEMRINOS

- IP: Numero único que identifica de manera lógica un dispositivo. Existen las versiones IPv4 y IPv6.
- TCP/IP: Es una denominación para identificar a la pila de protocolos de red que respaldan a internet y que hacen posible la transferencia de datos entre redes y ordenadores.
- TRÁFICO: Es la cantidad de datos enviados y recibidos por los usuarios de la red.
- LATENCIA: Es el tiempo exacto que tarda en transmitirse un paquete dentro de la red, el tiempo que tarda en establecerse una conexión.
- JITTER: Es las variaciones que se presentan en la latencia y sucede cuando los paquetes de un origen llegan a sus destinos con diferente tiempo de retardo.
- PERDIDAS DE PAQUETES: Cantidad de paquetes que se pueden perder en el trascurso de la transmisión de datos, que puede ocurrir por sobrepasar el tiempo de encolamiento en el buffer.
- PROTOCOLOS: Reglas que denominan la sintaxis, semántica y sincronización de la comunicación. Estos pueden ser implementados por hardware, software o ambas.
- JERARQUÍA DE RED: Es una técnica que consiste en dividir la red en niveles o capas con funcionamientos específicos que permiten dividir la red en secciones de fácil crecimiento y mantenimiento.
- TOPOLOGÍA: Hace referencia a la forma como va conectada la red tanto física como lógica.
- DMZ: Zona desmilitarizada que funciona como técnica para almacenar servidores que trabajan con tráfico de datos externo y están ubicados físicamente dentro de la LAN, pero no tienen acceso a la red local.

5 OBJETIVOS

5.1 General

Proponer un diseño de una red LAN para la empresa bits americas s.a.s

5.2 Específicos

1. Caracterizar la red LAN existente dentro de la empresa.
2. Diseñar topologías de la red LAN y soluciones que cumplan con lo requerido por el cliente.
3. Simular y documentar el diseño propuesto para su correcta verificación.
4. Documentar el cálculo de los costos que tendría la implementación del rediseño.

6 REQUERIMIENTOS

6.1 Funcionales

A continuación, se listan los requerimientos funcionales del sistema.

- El sistema debe segmentar el tráfico de datos según el rol del usuario: Administrativos, Comerciales, Desarrolladores, Servidores, Wifi invitados , Wifi Empresa.
- El sistema debe recibir las solicitudes de cada rol de usuario para entregar respuestas eficientes y seguras.
- El sistema debe garantizar acceso a internet Wireless a aproximadamente 20 invitados. asegurando que estos no consigan acceder a la información propia de la empresa.

6.2 De calidad

A continuación, se listan los requerimientos de calidad del sistema.

- El sistema debe contar con un mínimo de velocidad de 100Mbps por cada puerto de acceso.
- El sistema debe permitir una navegación disponible las 24 horas.
- El sistema debe tener mantenimiento cada 6 meses.
- El sistema debe ser escalable a 3 años con un factor de crecimiento del 10%
- El sistema debe tener documentada la topología física y lógica del diseño propuesto.

6.3 Restrictivos

A continuación, se listan los requerimientos de restricción del sistema.

- El sistema debe manejar la norma IEEE 802.11i implementando WPA2.
- La empresa espera la documentación del diseño no la implementación de este.
- El sistema debe utilizar Ipv4 porque la empresa no ve la necesidad de migrar a Ipv6.
- La solución propuesta para el diseño de la red no incluirá software especializado para la gestión o monitorización de esta.

7 DISEÑO FUNCIONAL

7.1 Caja con entradas y salidas

Se define un sistema en bloques que cuenta con una entrada y una salida como se muestra a continuación:



Figura 14, Sistema representado en bloques

Entrada del sistema:

E1: Conexión a internet entregada por el ISP con un ancho de banda a determinar en los resultados y conclusiones de este documento.

Salida del sistema:

S1: Dar a los empleados de la compañía acceso, disponibilidad y seguridad a los servicios de la empresa los cuales son:

- Navegación
- Telefonía
- Video conferencia

- Acceso Remoto
- Impresión
- Correo electrónico

En general el sistema que se quiere obtener es una red LAN para la compañía Bits Américas, sin embargo, es importante definir propuestas de solución que permitan el desarrollo del sistema, por ello se proponen las siguientes dos propuestas de solución.

7.2 Propuestas de solución

7.2.1 Propuesta de solución 1

En la primera propuesta de solución al diseño de una red LAN para la empresa Bits americas se presenta el diseño de la figura 15, la cual consta de 5 bloques los cuales son:

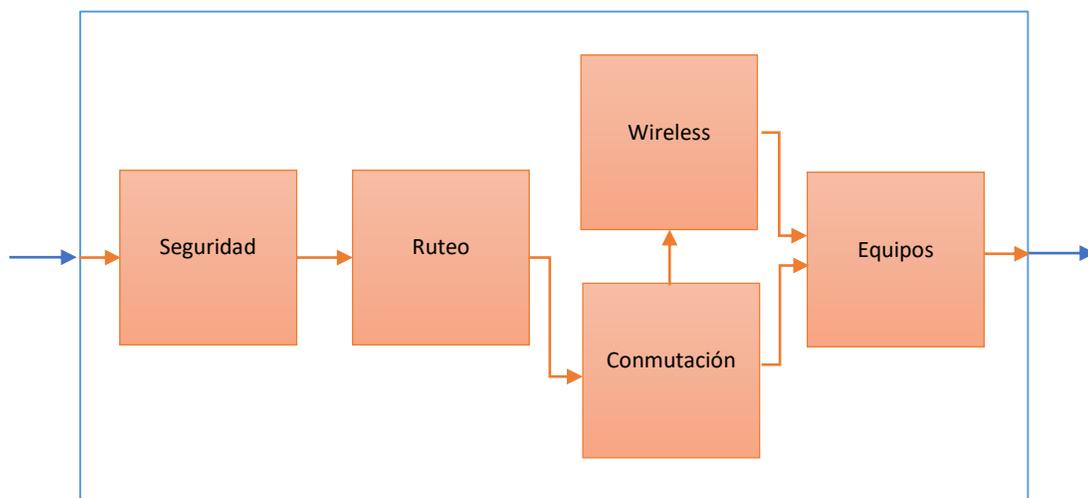


Figura 15, Propuesta de solución 1

7.2.2 Propuesta de solución 2

En la segunda propuesta de solución al diseño de una red LAN para la empresa Bits americas se presenta el diseño de la figura 16, la cual consta de 4 bloques los cuales son:

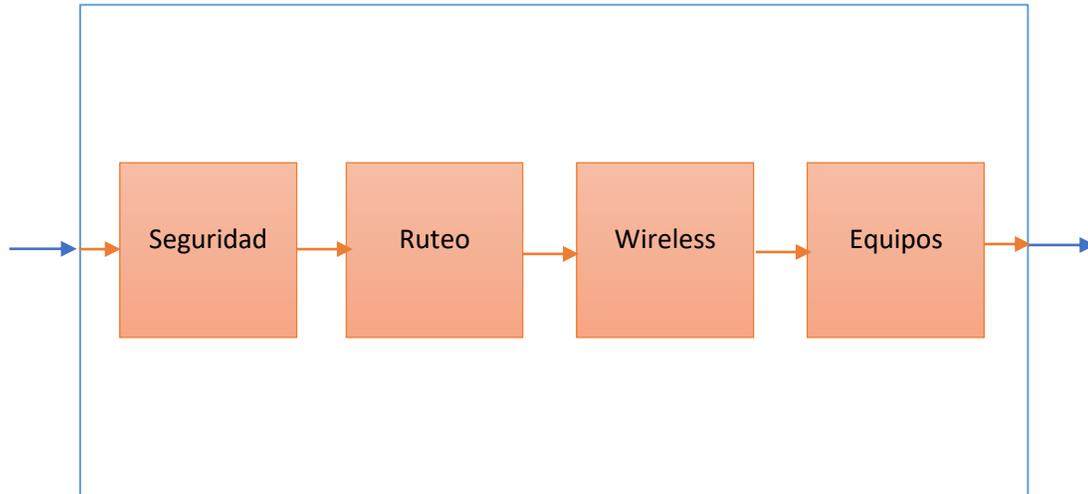


Figura 16, Propuesta de solución 2

7.3 Funciones de cada caja

7.3.1 Propuesta de solución 1

Subsistema Seguridad: Etapa encargada de bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Subsistema Ruteo: Etapa encargada de direccionar las comunicaciones por el camino o ruta más apropiado en cada momento.

Subsistema Conmutación: Etapa encargada de proporcionar múltiples vías de acceso sin pérdida de calidad.

Subsistema Wireless: Etapa que interconecta varias máquinas cliente sin la necesidad de un cable

Subsistema Equipos: Conjunto de estaciones de trabajo, servidores, impresoras, teléfonos IP y dispositivos móviles.

7.3.2 Propuesta de solución 2

Subsistema Seguridad: Etapa encargada de bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Subsistema Ruteo: Etapa encargada de direccionar las comunicaciones por el camino o ruta más apropiado en cada momento.

Subsistema Wireless: Etapa encargada de proporcionar múltiples vías de acceso sin pérdida de calidad y sin la necesidad de un cable

Subsistema Equipos: Conjunto de estaciones de trabajo, servidores, impresoras y teléfonos IP.

7.4 Sumatoria de funciones vs función del sistema

7.4.1 Propuesta de solución 1

El diagrama por bloques de esta propuesta se observa en la figura 15, en donde el bloque Seguridad recibe la conexión a internet entregada por el ISP, sobre la cual realiza el bloqueo de las comunicaciones no autorizadas, y a su vez permite el acceso autorizado a la red interna de la empresa. Después de esta etapa se encuentra el bloque Ruteo, el cual garantiza el direccionamiento de las comunicaciones por el camino o ruta más apropiado en cada momento para mínimo 100 usuarios. En seguida se encuentra el bloque Conmutación con el que se asegura la interconexión física mediante cable de estos 100 usuarios mínimo. Adicionalmente se encuentra el bloque Wireless, el cual permite la conexión de estos usuarios de manera inalámbrica simultáneamente a la conexión cableada, añadiendo la posibilidad de conectar 100 dispositivos más. Finalmente se encuentra el bloque Equipos, el cual está conformado por estaciones de trabajo, servidores, impresoras, teléfonos IP y dispositivos móviles, los cuales darán a los empleados de la compañía acceso, disponibilidad y seguridad a los servicios de la empresa, definidos en S1.

7.4.2 Propuesta de solución 2

El diagrama por bloques de esta propuesta se observa en la figura 16, el cual es similar al de la propuesta de solución 1, pero diverge en que se propone una solución inalámbrica, en la cual el bloque Wireless realizará la interconexión inalámbrica de mínimo 200 dispositivos, que al final darán a los empleados de la compañía acceso, disponibilidad y seguridad a los servicios de la empresa, definidos en S1.

7.5 Selección de propuesta

Con base en las explicaciones de las dos propuestas de solución, se seleccionó el primer diseño el cual se encuentra en la figura 15, debido a que presenta ventajas como un total aprovechamiento del ancho de banda y una menor latencia en las conexiones porque en la conexión totalmente inalámbrica propuesta en la figura 16, existe atenuación de la señal que se produce por las paredes, también sufre las interferencias con otros canales del espectro radioeléctrico que provocan que su velocidad de conexión merme.

Además, la conexión de cable es más segura para el paso de la información. No es posible ponerse en modo "escucha activa" e interceptar la información que va de las estaciones de trabajo hacia los equipos de red, y posteriormente sale hacia su destino.

Finalmente, la primera propuesta de solución se adapta más a las necesidades de la empresa porque se basa en combinar conexión inalámbrica con cable de red. De esta forma liberamos un poco el espectro Wifi de dispositivos que se conectan, que cada día son más. Lo más apropiado es dejar a los equipos más exigentes en su ancho de banda por la conexión cableada, ya que es una compañía que depende de una buena infraestructura de red para desempeñarse de manera correcta.

8 DISEÑO DETALLADO

A continuación, se realiza el diseño de una propuesta a la red LAN de la empresa BITS AMERICAS SAS basada en el mejoramiento del rendimiento de los equipos y la capacidad del medio. Se debe realizar un diseño de red que tenga características de escalabilidad permitiendo el crecimiento de la empresa a 3 años con un factor de crecimiento del 10% y que permita la interconexión de los diferentes departamentos de la organización, por lo que es importante conocer el tipo de tráfico que cada área maneja.

La propuesta de diseño no permitirá únicamente la conexión de computadoras, sino que va a tener en cuenta características que hagan a la red manejable, fiable y segura.

Según Microsoft, para el diseño de la red LAN se requieren diferentes tipos de dispositivos tanto para la red alámbrica como la inalámbrica y listan en una tabla los dispositivos principales, así como su uso, finalidad, beneficios y desafíos.

Servicio	Dispositivo principal	Uso principal	Beneficios	Desafío
Red de área local (LAN) alámbrica	Conmutadores	Conectar servidores, dispositivos y PCs	Conectividad LAN de alta velocidad	Cablear la LAN
Conectividad alámbrica segura en la LAN	Puntos de acceso alámbricos (APs)	Conectar dispositivos habilitados de manera inalámbrica (tales como PCs portátiles, Tablet PCs y PDAs)	Movilidad del cliente	Seguridad Velocidad de la transmisión
Conexión segura a Internet	Firewall	Proporcionar acceso de entrada y salida a Internet	Conectarse con clientes y proveedores Acceso remoto	Seguridad

Figura 17, Descripción de dispositivos necesarios en una red LAN

Es por esto por lo que se seguirán los siguientes pasos para diseñar la red:

- Diseñar la red alámbrica e inalámbrica
- Proporcionar acceso seguro a internet

8.1 Diseño de la red alámbrica e inalámbrica

Antes de empezar a escoger la topología física o lógica de la red, es importante conocer la empresa y lo que la compone, por esto, para llevar una buena planeación primero para la red alámbrica de la LAN se llevaran a cabo 3 tareas claves:

1. Calcular el número de clientes, servidores y dispositivos
2. Planear el diseño de la red
3. Seleccionar el hardware de la red

8.1.1 Calcular el número de clientes, servidores y dispositivos

Como es de esperarse, la compañía tiene clientes, servidores y dispositivos que para funcionar en conjunto incluyen dispositivos de red tales como firewalls, puntos de acceso

inalámbricos, enrutadores, conmutadores, impresoras, estaciones de trabajo entre otros. Es por esto por lo que es importante establecer como línea base el número de dispositivos alámbricos con el que contará la red para determinar el número de puertos mínimos necesarios por parte de los dispositivos de red para dar soporte.

Sin embargo, para conocer el valor del número de clientes es necesario tener en cuenta la escalabilidad de la empresa, en este caso, con un factor de crecimiento del 10% a 3 años se calculará el número de estaciones de trabajo se estiman al 2022.



Figura 18, Crecimiento estimado a 3 años en el personal de BITS AMERICAS SAS

Como se puede apreciar en la Figura 18, se estima que en el 2022 habrá 133 empleados, es decir, 133 puertos necesarios únicamente para dar acceso a los trabajadores. Además, se debe tener en cuenta los servidores, firewalls, teléfonos, impresoras, AP's y salas.

A continuación, se lista en una tabla el número exacto de clientes, servidores y dispositivos que se requiere tener en cuenta en el planteamiento del diseño:

Tabla 1, Cálculo de número de clientes, servidores y dispositivos en BITS AMERICAS SAS

Clientes a 3 años	Servidores	Impresoras	Salas y puntos adicionales	AP's	Teléfonos	TOTAL [puertos]
133	3	1	7	6	10	160

8.1.2 Planear el diseño de la red

Para hacer una planeación objetiva de la red, es necesario tener en cuenta los requerimientos de esta, es por esto por lo que es necesario conocer los servicios con los que tiene que contar la red para satisfacer las necesidades de sus usuarios.

Las aplicaciones que se utilizarán dentro de la red se pueden dividir en:

- Aplicaciones que requieren acceso a internet:
 - Navegación, descargas y carga de archivos
 - Videoconferencias
 - Correo electrónico
 - Telefonía IP
- Aplicaciones que requieren acceso a intranet:
 - Almacenamiento de información (Servidores)
 - Impresión

Con la información que se tiene hasta el momento se puede empezar a dimensionar el tráfico que circulará por la red y así tener los cálculos exactos del ancho de banda que será necesario asignar a cada estación de trabajo para que los usuarios desempeñen sus labores a cabalidad.

Para asegurar el buen funcionamiento de la red en las estaciones de trabajo, es necesario asegurar que las máquinas dispongan del ancho de banda apropiado.

Para empezar, se tomó como referencia los servicios que necesita la compañía y se segmentó en aquellos que requieren acceso a internet y los que requieren acceso a la intranet, y así, para determinar el ancho de banda de cada servicio se consideraron los índices de simultaneidad basados en la siguiente gráfica.

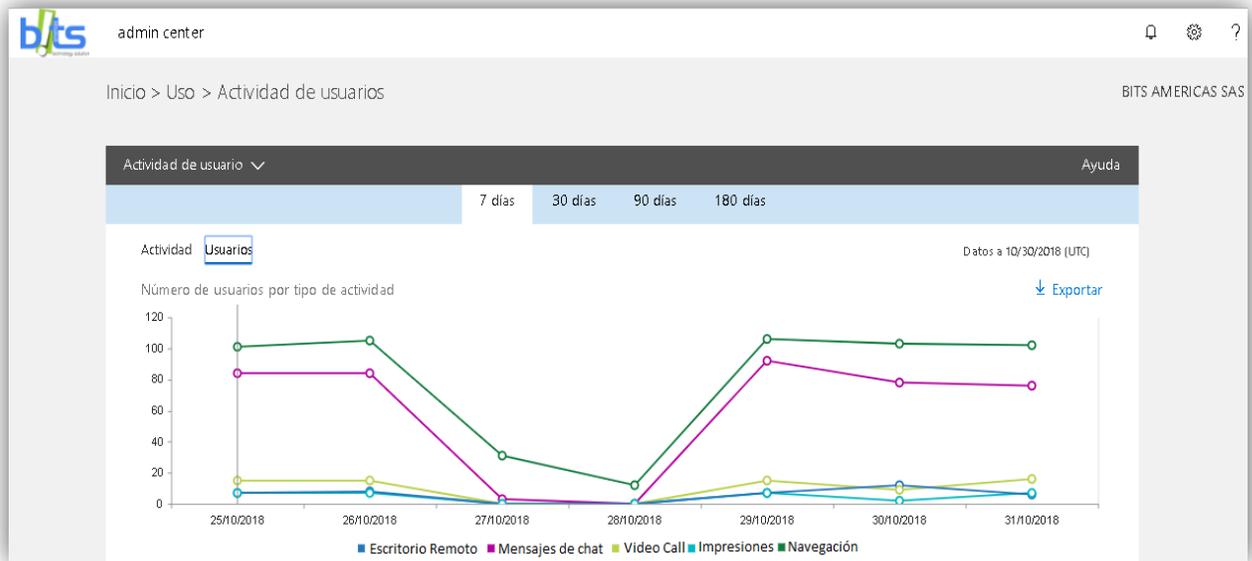


Figura 19, Numero de usuarios pico por tipo de actividad en una semana

En la figura anterior, se puede apreciar el número de usuarios pico que usan un determinado servicio en un determinado día.

La finalidad de usar esta información suministrada por el administrador de la red Edgar Correa, es proponer un índice de simultaneidad para cada servicio basado en el pico de usuarios que utilizan dicho servicio y establecer esa cantidad de usuarios como el máximo que podrán estar al m

ismo tiempo usando ya sea la navegación, mensajería, impresión, escritorio remoto, video conferencia, telefonía o correo. Permitiendo así, garantizar un ancho de banda que permita en un momento determinado la disponibilidad de la red para que los 133 usuarios que se estiman estarán a 3 años en las instalaciones de la empresa podrían llegar a utilizar un servicio al mismo tiempo.

A continuación, se muestra en una tabla el índice de simultaneidad para cada servicio basado en el máximo de usuarios que los usan.

Tabla 2, Estudio de simultaneidad de usuarios

	Aplicación	Usuarios con acceso al servicio	Simultaneidad %	Usuarios en simultaneo
Internet	Navegación, descargas y carga de archivos	133	10%	13
	Video conferencia	65	23%	15
	Correo electrónico	133	7%	10
	Telefonía IP	30	17%	5
	Mensajería Instantánea	133	80%	106
Intranet	Escritorio remoto	50	20%	10
	Impresión	20	35%	7

Cabe resaltar que el índice de simultaneidad por cada servicio fue contrastado en una reunión que se realizó con el ingeniero Edgar Correa, de acuerdo con la cantidad de usuarios que utilizan un determinado servicio al mismo tiempo.

En cuanto a los servicios que requieren acceso a internet, a continuación, se mostrarán los respectivos cálculos del ancho de banda.

- *Cálculo del ancho de banda para el servicio de navegación, carga y descarga de archivos*

Según SpeedCurve basados en datos recolectados por HTTP Archive, el tamaño promedio de las paginas web en 2018 fue de 3MB, y la velocidad promedio de carga fue de 2.4 segundos por cada 500KB. Con una simultaneidad de 10% se garantiza que 13 personas pueden cargar paginas web exactamente al mismo tiempo, caso infrecuente ya que es muy poco probable que mas de 13 personas ejecuten la búsqueda o carga de página al mismo tiempo.

$$C_{Nd} = \frac{500KB}{1 \text{ Descarga}} * \frac{8bits}{1Byte} * \frac{1 \text{ Descarga}}{2.4 \text{ segundos}} * \frac{1Mbps}{1024kbps} = 1.66Mbps$$

La ecuación anterior muestra que es necesario un ancho de banda de 1.66Mbps por usuarios en simultaneo. Es decir que, si 13 personas abren una página web exactamente el mismo tiempo, esta se demore 14.4 segundos en cargar para cada una.

- *Cálculo del ancho de banda para el servicio de video conferencia*

Bits Americas utiliza la herramienta Microsoft Teams como aplicación de comunicación con sus teletrabajadores y clientes. Sin embargo, muchos de los empleados utilizan también Skype como medio de comunicación.

En la documentación de Skype, se lista el ancho de banda requerido dependiendo del tipo de llamada que se requiere hacer para un buen rendimiento y experiencia de usuario.

La siguiente figura muestra la velocidad mínima y recomendada de carga y descarga requerida.

Call type	Minimum download / upload speed	Recommended download / upload speed
Calling	30kbps / 30kbps	100kbps / 100kbps
Video calling / Screen sharing	128kbps / 128kbps	300kbps / 300kbps
Video calling (high-quality)	400kbps / 400kbps	500kbps / 500kbps
Video calling (HD)	1.2Mbps / 1.2Mbps	1.5Mbps / 1.5Mbps

Figura 20, Tabla de ancho de banda requerido por Microsoft teams y Skype

En la figura 20 se escoge el tipo de llamada **"Video calling/Screen sharing"** el cual requiere un ancho de banda mínimo de 128Kbps tanto de descarga como de carga. Lo que indica que por persona son necesarios aproximadamente 300kbps para sostener una video llamada donde se comparta pantalla que es una de las características mas usadas por los usuarios de la empresa al mostrar sus desarrollos a los trabajadores remotos o clientes que están en sus propios sitios de trabajo.

Al final, como la estimación se hará sobre la aplicación oficial que es Microsoft teams, el ancho de banda requerido para este servicio será:

$$C_V = \frac{300Kbps}{1 \text{ llamada}}$$

El ancho de banda necesario para garantizar que 15 usuarios estén en video conferencia al mismo tiempo es de $2.4Mbps$ por usuario en simultaneo.

- *Cálculo del ancho de banda para el servicio de mensajería instantánea*

Para el servicio de mensajería instantánea se utiliza la aplicación de Microsoft Teams, la cual tiene un límite de 65,536 caracteres por mensaje, lo que equivale a 512Kbits máximo por mensaje. Aunque es muy poco probable que un usuario pueda enviar un mensaje de este tamaño, por lo tanto, se tomó la velocidad promedio a la que se escriben los caracteres, que es de 100 palabras de 10 caracteres por minuto, equivalentes a 16.7 caracteres por segundo es decir que el ancho de banda requerido es:

$$C_{MI} = 16.7 \text{ caractres} * 8\text{bits} = 133.33\text{bps}$$

El ancho de banda necesario para garantizar que 106 personas puedan estar enviando un mensaje en Teams es de 133bps.

- *Cálculo del ancho de banda para el servicio de correo electrónico*

Toda la información que se maneja en el correo electrónico tiene que ver exclusivamente con las actividades que desempeña la empresa tanto con sus clientes como sus actividades internas. La capacidad requerida para esta aplicación se realizó tomando 10 correos de la bandeja de entrada de un trabajador que contenían texto e imágenes normales y sacando el promedio del peso entre esta muestra, con lo que se obtuvo un tamaño promedio de 500KB. Con esta información se realizó el respectivo calculo.

$$C_{CE} = \frac{500\text{KB}}{1 \text{ Correo}} * \frac{8\text{bits}}{1\text{Byte}} * \frac{1 \text{ Correo}}{5 \text{ segundos}} = 0.8\text{Mbps}$$

El ancho de banda necesario para garantizar que 10 personas puedan estar sincronizando su bandeja de entrada o enviando un correo al mismo tiempo es de 0.8Mbps por usuario en simultaneo.

- *Cálculo del ancho de banda para el servicio de acceso a los servidores por escritorio remoto*

User scenario	Windows Server 2003 (RDP 5.2)	Windows Server 2008 (RDP 6.0)	Windows Server 2008 (RDP 6.1)	% performance gain: 2008 (RDP 6.0) vs 2003 (RDP 5.2)	% Performance gain: 2008 (RDP 6.1) vs 2003 (RDP 5.2)
Executive PPT	164.33	117.33	97.82	28.60	40.48
Simple PPT	60.93	51.46	33.43	15.54	45.14
Typing and Scrolling	1.69	1.69	1.56	0.12	7.73
Scrolling	0.70	0.64	0.57	8.12	17.88
Internet Explorer	7.98	6.45	5.59	19.23	29.99

Figura 21, Tabla de ancho de banda en KBps consumido por RDC

Para el servicio de escritorio remoto, es necesario tener un mínimo de 97.82 KBps como se parecía en la figura 21. Por lo tanto, es recomendable tener como mínimo 128Kbps para cada terminal que utilizará esta aplicación, este valor se traza con base a la aplicación *Desktop remote* de Microsoft. [11]

$$C_{ER} = 128KBps * 8 bits = 1Mbps$$

- *Cálculo del ancho de banda para el servicio de telefonía IP*

Para la telefonía IP, se utilizará una planta que recibe el servicio de 10 líneas que se conectarán al switch para manejar telefonía sobre IP.

Se tomará en cuenta que para las llamadas de voz se requieren como mínimo 100Kbps [12] para asegurar un rendimiento óptimo en llamadas de voz.

Es decir, que multiplicando el ancho de banda necesario por una llamada por el número de usuarios que se tendrán al mismo tiempo el resultado es el siguiente:

$$C_{TIP} = = 100Kbps$$

- *Cálculo del ancho de banda para el servicio de impresión*

Se estima que para el servicio de impresión se hacen solicitudes para archivos de 100KB y se quiere que tarden como máximo 10 segundos en llegar a la impresora.

$$C_{IM} = \frac{100KB}{1 \text{ mpresion}} * \frac{8bits}{1Byte} * \frac{1 \text{ impresion}}{10 \text{ segundos}} = 80Kbps$$

Conforme al dimensionamiento del tráfico realizado anteriormente, se tiene a continuación una tabla que describe el ancho de banda total que se requiere para los servicios que dependen de internet y otra para los servicios dependientes de la intranet.

Tabla 3, Ancho de banda total necesario para internet

CAPACIDAD DE ANCHO DE BANDA SERVICIOS DEPENDIENTES DE INTERNET [Kbps] por usuario	
Navegación, descargas y carga de archivos	1700
Video conferencia	300
Correo electrónico	800
Telefonía IP	100
Mensajería Instantánea	0.133

Tabla 4, Ancho de banda total necesario para intranet

CAPACIDAD DE ANCHO DE BANDA SERVICIOS DEPENDIENTES DE LA INTRANET [Kbps] por usuario	
Escritorio remoto	1024
Impresión	80

Para realizar el estimado del ancho de banda necesario, se va a plantear el peor de los escenarios posibles, que consiste en que la mayoría de los usuarios permitidos estén utilizando los servicios que mas ancho de banda requieren. Es decir que todos los usuarios que pueden hacer uso de Navegación, descargas y carga de archivos estén haciendo uso de ese servicio, a la vez que todos los que pueden enviar Correos electrónicos estén enviando uno, y así sucesivamente hasta completar los 133 usuarios proyectados.

Tabla 5, Calculo Ancho de banda servicios dependientes de internet

Servicio	Ancho de banda por servicio por usuario	Usuarios en Simultaneo	Ancho de banda por servicio en Kbps
Navegación, descargas y carga de archivos	1700	13	22,100
Video conferencia	300	15	1,500
Correo electrónico	800	10	8,000
Telefonía IP	100	5	500
Mensajería Instantánea	0.133	90	11.97
TOTAL		133	32,111.97

Para el cálculo del ancho de banda para los servicios dependientes de la intranet se realiza el mismo procedimiento.

Tabla 6, Cálculo Ancho de banda servicios dependientes de la intranet

Servicio	Ancho de banda por servicio por usuario	Usuarios en Simultaneo	Ancho de banda por servicio en Kbps
Escritorio remoto	1024	10	10,240
Impresión	80	7	560
TOTAL		17	10,800

Si se hace la suma de la capacidad necesaria para intranet y para internet, el resultado del ancho de banda se extiende a 42,911.97kbps, lo que equivale a **42Mbps**, lo que nos da la información necesaria para entrar a estudiar el cableado estructurado.

8.1.3 Selección del cableado estructurado de la red

Uno de los factores más importantes para que una red funcione correctamente está en seleccionar el tipo de cableado con el que se estructurará la red alámbrica.

Teniendo en cuenta el cálculo del ancho de banda que la red requiere que se hizo anteriormente y la norma EIA/TIA 568A la cual se describe como "*Una norma que especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante*" [13]. Además de proporcionar los requerimientos mínimos para el cableado y haciendo recomendaciones para:

- La topología
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Para poder aplicar la norma correctamente se necesita estudiar el sitio físico sobre planos donde la red estará ubicada.

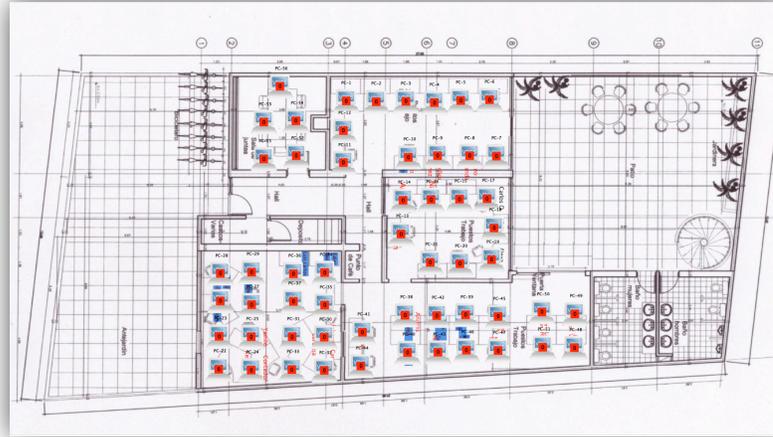


Figura 22, Primer piso

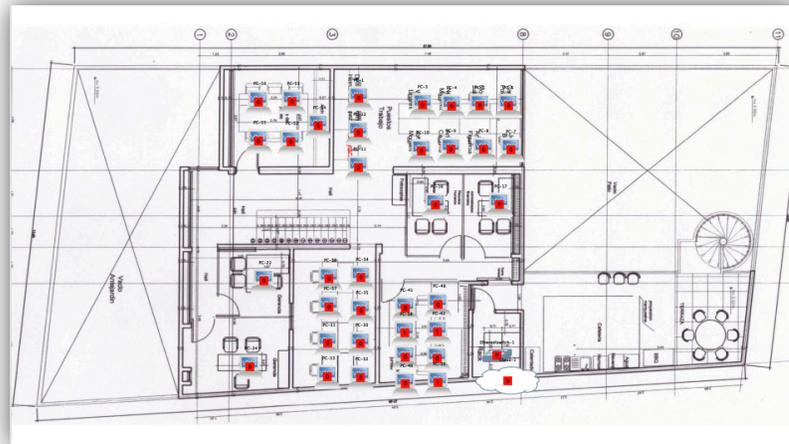


Figura 23, Segundo piso

Como se puede apreciar en la figura 22 se muestran las estaciones de trabajo con las que contará el primer piso las cuales son un total de 56 puestos y en la figura 23 las estaciones de trabajo del segundo piso la cual cuenta con 40 puestos.

Así, con la información de las estaciones de trabajo con las que contará el edificio, y el ancho de banda requerido por cada servicio, se puede hacer el respectivo análisis del tipo de

cable y la velocidad de transmisión que es requerida para que dichos servicios funcionen correctamente.

- *Identificación del tipo de cable y sus características*

La norma EIA/TIA 568A reconoce 4 medios de transmisión que puede usarse de forma individual o en combinación:

- Cable UTP de 100ohm
- Cable STP de 150ohm
- Cable de fibra óptica multimodo y monomodo

De antemano se descartará la fibra óptica por cuestiones de costo e implementación ya que no se ve la necesidad de implementar fibra al cableado estructurado, sin embargo, cabe resaltar que el enlace del proveedor de internet (Une) es un canal dedicado de fibra óptica.

Las opciones restantes son UTP y STP las cuales entraremos a analizar en cuanto a relación costo/beneficio cuál de las dos es la mejor opción para implementar dentro de la red LAN que se está diseñando.

- Ventajas del cable UTP (14)

- Una cubierta metálica protege los cables de interferencia electromagnética, esta característica permite mejorar y da un empuje a la velocidad de transmisión de datos. Este bloquea la interferencia de los motores de varios dispositivos.
- Reduce considerablemente el crosstalk
- Permite manejar velocidades de transmisión de hasta 1Gbps

- Ventajas del cable STP (14)

- No es necesario pagar por una cubierta metálica lo que traduce que cuesta mucho menos que el STP.
- La instalación es mucho más sencilla ya que no es tan robusto con el STP lo que traduce en menor costo de implementación
- Cuenta con una protección a las interferencias electromagnéticas al tener par trenzado.
- Permite manejar velocidades de transmisión de hasta 1Gps

En conclusión, el cable STP hace exactamente lo mismo que el UTP solo que viene con características de protección a interferencia mucho mayor que el UTP. Sin embargo, no se considera implementar un cable que tenga ese tipo de protección ya que el cableado de la red LAN para BITS AMERICAS SAS no estará expuesto a interferencias electromagnéticas más allá de las que generarían los motores de los ventiladores que tendrán los mismos dispositivos de red ya que se apartará un cuarto oscuro exclusivo para la red donde se almacenarán todos los dispositivos del backbone de la red. Es decir, se tomará como alternativa el cable UTP Categoría 6 que está hecho con los estándares más altos y un diseño de mayor rendimiento en la alineación de los pines de contacto que reduce considerablemente el ruido ocasionado por el crosstalk, así se contrarresta lo que el UTP no tiene en comparación al STP. Además, que proporciona un rendimiento de hasta 250MHz y es adecuado con 10/100/1000 BASE T y TX, lo que es conveniente para el diseño de nuestra red ya que el ancho de banda requerido por maquina está por encima de los 20Mbps.[15]

Con el tipo y categoría del cable ya elegidos y teniendo en cuenta la infraestructura del sitio donde estará ubicada la red, se puede diseñar la topología la cual fue dibujada en un boceto y cuyo fundamento se basa en la arquitectura de red jerárquica que propone CISCO para que las redes sean modulares, flexibles, escalables, redundantes y administrables.

A continuación, se muestra el boceto de la propuesta que se plantea manejar:

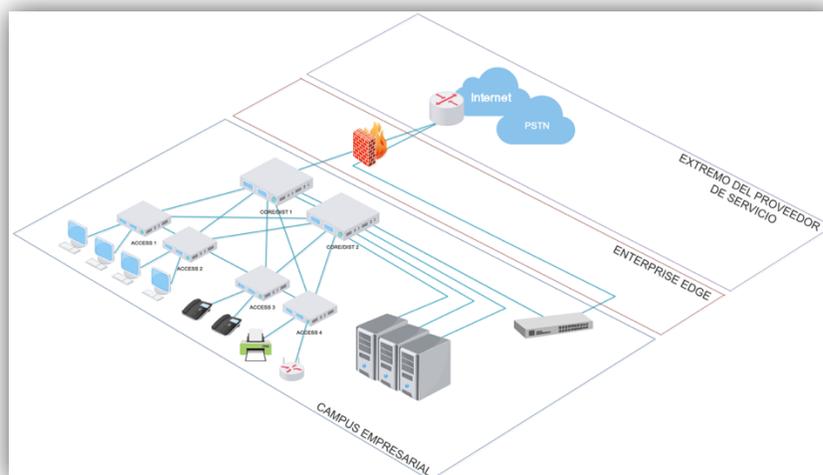


Figura 24, Boceto de topología de red

Como se puede apreciar, se planea unificar la capa de Core y distribución ya que la infraestructura no es demasiado grande, lo que permite tener en un solo switch estas dos capas y en una externa las de acceso. Además, ubicar los servidores en una zona desmilitarizada (DMZ) y el servicio de telefonía IP como utilizará un modem diferente al que provee el servicio a internet, se conectará a una planta telefónica que administrará las 10 líneas telefónicas que la empresa tiene contratadas para asignarle a los teléfonos que por medio de la red harán la petición cuando sea requerida.

Es importante tener en cuenta que se piensa en 4 switch de acceso capa 2 de 48 puertos para abastecer la densidad de puertos que requiere la red (160 puertos), y el switch capa 3 que será el backbone de la red está pensado de 48 puertos ya que se piensa utilizar el 3COM 4800G con el que cuenta la empresa ya que cumple con los requisitos mínimos que ya hemos calculado. Esta información se mostrará en el siguiente apartado.

8.1.4 *Seleccionar el hardware de la red*

Antes de entrar a seleccionar el hardware requerido para el correcto funcionamiento de la red es importante conocer, los dispositivos con los que cuenta actualmente la empresa. Esto con el fin de reconocer si alguno de estos nos es útil reutilizar para que el costo de la propuesta sea mucho menor.

Empezaremos por listar los componentes de la sede 1:

- **Sede principal**

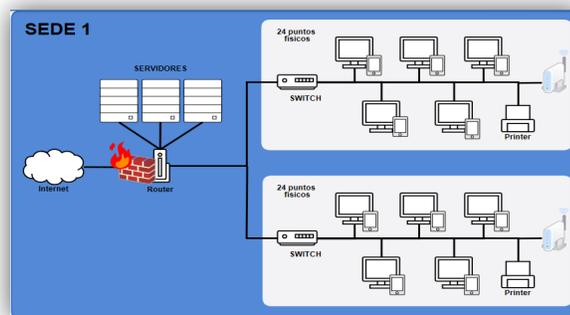


Figura 25, Topología red actual sede principal

La sede principal se encuentra ubicada en Bogotá y cuenta con un total de 48 puntos de red distribuidos a través de las instalaciones con una topología de red en estrella extendida con un ancho de banda de canal dedicado de 40M por UNE.

A continuación, se listan los dispositivos que la componen y sus características:

- **Router CISCO RV042**

Interfaces	
Puertos	4 puertos LAN 10/100/1000 RJ-45 2 puertos WAN 10/100/1000 RJ-45
Rendimiento	
Rendimiento NAT	800Mbps
Rendimiento VPN con IPsec	75Mbps
Tipo de Conexión a Internet	
Protocolos de routing	Estático, RIPv1, RIPv2, RIP para IPv6
Protocolos de red	DHCP, StaticIP, PPPoE, PPTP, DNS relay
Seguridad	
Firewall	SPI, DoS, Suplantación de IP, alerta de correo electrónico de ataque de pirata informático.
Bloqueo	Java, Cookies, ActiveX, Proxy HTTP
Filtrado de contenido	Bloqueo estático de dirección URL o por palabras clave

VLAN	Vlans basadas en puertos
Puerto	Puerto DMZ
VPN (Virtual Private Network)	
IpSec	50 túneles Ipsec de sitio a sitio para conectividad de sucursales
QuickVPN	50 túneles QuickVPN para acceso remoto de clientes
PPTP	5 túneles PPTP para acceso remoto
Cifrado	DES, 3DES, AES, AES-128, AES-192
QoS (Quality of Service)	
Tipos de priorización	Prioridad basada en la aplicación en el puerto WAN
QoS basada en el servicio	Compatible con nivel de prioridad o control de velocidad
Control de tráfico	Se puede configurar el ancho de banda ascendente y descendente por servicio
Prioridad	A cada servicio se puede asignar una ruta hacia uno de los 3 niveles de prioridad
Administración	
Interfaz de usuario WEB	Administración de dispositivo basado en navegador simple (HTTP/HTTPS)

Protocolo de administración	SNMP v1, v2, Bonjour
Registro de eventos	Syslog, alertas de correo electrónico, monitor de estado túnel VPN

- **2 Switches TP-link TL-SG1024**

Puertos	24 puertos tipo RJ-45 ethernet
Protocolos de red compatibles	CSMA/CD, TCP/IP
Tasa de transferencia soportada	10/100/1000Mbps
Capacidad de conmutación	48Gbit/s
POE	N/A
Tamaño de la tabla de direcciones	8000 entradas
Jumbo Frame	10 KBytes
Administración	N/A

- **Servidor HP DL580 5° generación**

Procesador	6-Core Intel Xeon 7400 chipset
Memoria RAM	32Gb DDR3
Red	NC373i
Almacenamiento	2 TB

Interfaces	Serial=1, USB2.0=5, RJ-45=2, Video=2, Mouse=1, Teclado=1
------------	---

- **Servidor HP ML110 9° generación**

Procesador	6-Core Intel Xeon E5-2603v4
Memoria RAM	32Gb DDR4
Red	HP Embedded Dual Port 361i Adapter
Almacenamiento	2 TB
Interfaces	Serial=1, USB2.0=8, RJ-45=2, Video=1, Mouse=1, Teclado=1

- **Servidor DELL power Edge T105**

Procesador	AMD Opteron doble núcleo serie- 1200
Memoria RAM	8Gb DDR2
Red	HP Embedded Dual Port 361i Adapter

Almacenamiento	1 TB
Interfaces	Serial=1, USB2.0=7, RJ-45=1, Video=1, Mouse=1, Teclado=1

- **Wireless Access Point: un Unifi y un D-Link**

UNIFI AP	
Puertos	1 Puerto LAN a 10/100Mbps
Estandares	IEEE 802.11b /g / n
Seguridad	WEP, WPA/WPA2

D-Link AP	
Puertos	1 Puerto LAN a 10/100Mbps
Estandares	IEEE 802.11b /g / n
Seguridad	WEP, WPA/WPA2

Cabe resaltar que los switch de esta sede son alquilados, los dispositivos con los que cuenta realmente la compañía son:

- Router
- Servidores
- Access points

- **Segunda sede**

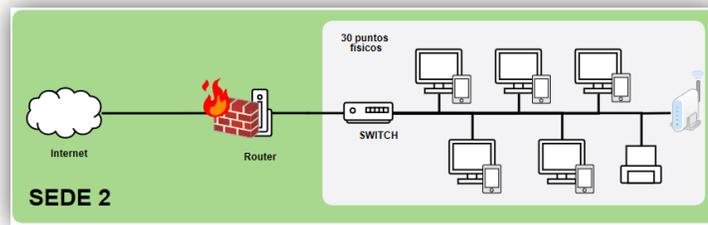


Figura 1, Topología actual sede dos

La segunda sede también se encuentra ubicada en Bogotá y cuenta con un total de 25 puntos de red distribuidos a través de las instalaciones con una topología de red en estrella extendida con un ancho de banda de canal dedicado de 20M por UNE.

A continuación, se listan los dispositivos de la segunda sede y sus respectivas características:

- **Router CISCO RV082**

Interfaces	
Puertos	8 puertos LAN 10/100/1000 RJ-45 2 puertos WAN 10/100/1000 RJ-45
Rendimiento	
Rendimiento NAT	200Mbps
Rendimiento VPN con IPsec	97Mbps
Tipo de Conexión a Internet	
Protocolos de routing	Estático, RIPv1, RIPv2, RIP para IPv6
Protocolos de red	DHCP, StaticIP, PPPoE, PPTP, DNS Relay
Seguridad	

Firewall	SPI, DoS, Suplantación de IP, alerta de correo electrónico de ataque de pirata informático.
Bloqueo	Java, Cookies, ActiveX, Proxy HTTP
Filtrado de contenido	Bloqueo estático de dirección URL o por palabras clave
VLAN	Vlans basadas en puertos
Puerto	Puerto DMZ
VPN (Virtual Private Network)	
IpSec	100 tuneles Ipsec de sitio a sitio para conectividad de sucursales
QuickVPN	50 tuneles QuickVPN para acceso remoto de clientes
PPTP	5 tuneles PPTP para acceso remoto
Cifrado	DES, 3DES, AES, AES-128, AES-192
QoS (Quality of Service)	
Tipos de priorización	Prioridad basada en la aplicación en el puerto WAN
QoS basada en el servicio	Compatible con nivel de prioridad o control de velocidad
Control de tráfico	Se puede configurar el ancho de banda ascendente y descendente por servicio

Prioridad	A cada servicio se puede asignar una ruta hacia uno de los 3 niveles de prioridad
Administración	
Interfaz de usuario WEB	Administración de dispositivo basado en navegador simple (HTTP/HTTPS)
Protocolo de administración	SNMP v1, v2, Bonjour
Registro de eventos	Syslog, alertas de correo electrónico, monitor de estado túnel VPN

- **1 Switch 3COM 4800G**

Puertos	48 puertos tipo RJ-45 ethernet
Protocolos de red compatibles	CSMA/CD, TCP/IP
Tasa de transferencia soportada	10/100/1000Mbps
Capacidad de conmutación	192 Gbit/s
POE	IEEE802.3af
Tamaño de la tabla de direcciones	32000 entradas
Jumbo Frame	Soportado
VLAN	Basadas en ACLs, Vlan de invitados, 1024 virtual IP, Mapeo de VLAN (1:1, n:1, 2:2)

Administración	Single console interface (CLI), SNMP, Remote configuration via TELNET
----------------	---

- **Wireless Access Point: Trendnet**

Puertos	1 Puerto LAN a 10/100/1000Mbps
Estandares	IEEE 802.11n, 802.11b 802.3u
Seguridad	64/128-bit WEP, WPA/WPA2

En esta sede los dispositivos si son propios de la compañía.

- *Selección del firewall*

En vista de que la empresa necesita una seguridad perimetral, se propone hacer uso del router RV082 de cisco con el que cuenta la empresa para establecer un perímetro seguro y contemplarlo como firewall, lo cual permite ahorrar dinero para hacer la adquisición de los switches.

Las características de firewall con las que cuenta el router son las siguientes:



Figura 26, Cisco RV082

Tabla 7, Características router/firewall RV082

Firewall	SPI, Denegación de servicios (DoS), ping de la muerte, suplantación de IP, Alerta de correo electrónico para los ataques de hackeo.
Reglas de acceso	Hasta 50 entradas
Redireccionamiento de puertos	Hasta 30 entradas
Activación de puertos	Hasta 30 entradas
Bloqueo	Java, cookies, activeX, proxy HTTP
Filtrado de contenido	Bloqueo de url estatica o mediante palabras claves
VPN	100 tuneles de IP sec sitio a sitio para la conectividad de sucursales
Quick VPN	50 tuneles QuickVpn para el acceso de clientes remotos

- *Selección de los switch capa 3*

Para la elección de los switch capa 3 que se utilizarán como Core/distribución según el modelo jerárquico de redes, se propone hacer uso del switch 3COM 4800G con el que cuenta la compañía y hacer la adquisición de uno adicional que sería el de respaldo para hacer la red redundante. Estos switches cuentan con puertos de hasta 1Gbps y características capa 3 que lo hacen una excelente opción para el desempeño de la red que se está proponiendo.

A continuación, se listan las características más relevantes de este switch:

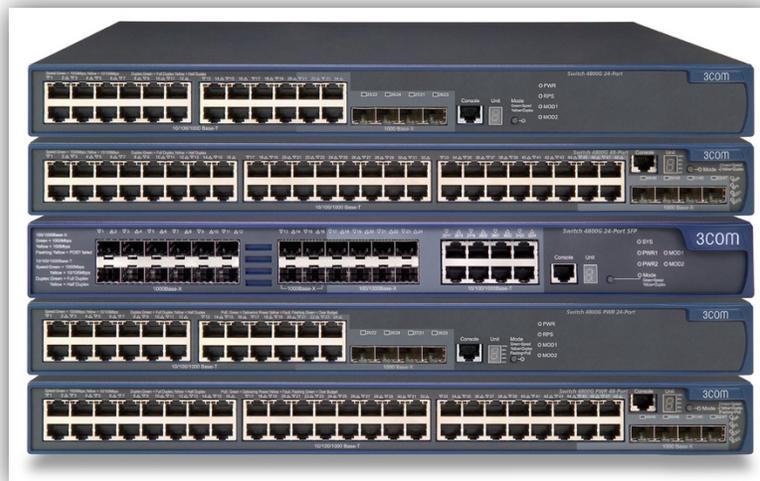


Figura 27, Familia Switch 3COM 4800G

Tabla 8, Características Switch 3COM 4800G 48 port

Puertos	48 puertos tipo RJ-45 ethernet
Protocolos de red compatibles	CSMA/CD, TCP/IP
Tasa de transferencia soportada	10/100/1000Mbps
Capacidad de conmutación	192 Gbit/s
POE	IEEE802.3af
Tamaño de la tabla de direcciones	32000 entradas
Jumbo Frame	Soportado
VLAN	Basadas en ACLs, Vlan de invitados, 1024 virtual IP, Mapeo de VLAN (1:1, n:1, 2:2)
Administración	Single console interface (CLI), SNMP, Remote configuration via TELNET

Sin embargo, hay que tener en cuenta que hace falta uno de los dos switches para completar el diseño redundante que se propone.

El costo de un switch 3COM 4800G de 48 puertos está en el mercado en diferentes precios comparados a continuación:

Tabla 9, Precios del switch 3COM 4800G 48port

Ebay	3.006.646 pesos colombianos
Mercado libre	5.000.467 pesos colombianos
Cnet	1.000.000 pesos colombianos (Refurbished)

En conclusión, se elige la alternativa de Ebay que es segura y se prioriza ya que una versión reacondicionada del producto puede llegar a causar muchos problemas.

- *Selección de los switch capa 2*

Para la elección de los switch capa 2, es necesario que sean administrables para dar control a cada puerto y administrar el ancho de banda que se va a asignar a cada puerto de los switches de acceso.

Además, es importante tener las siguientes recomendaciones:

- **Conteo del puerto:** Calcular el número de puertos que se requieren para cumplir con los requisitos actuales. Anticipe el crecimiento en el número de clientes y utilice los conmutadores en donde el conteo de puerto se puede escalar.

En esta ocasión se necesitan 160 puertos como mínimo para la red teniendo en cuenta.

- **Velocidades del puerto:** Los puertos auto sensibles a 10/100 Mbps son el requisito mínimo. Utilice Gigabit Ethernet en los servidores y en otros PC de alto rendimiento cuando se requiera un mayor ancho de banda.

La velocidad que se espera para los switches de acceso son de un máximo de 100Mbps y las tres opciones cuentan con 48 puertos 10/100Mbps y 2 a 10/100/1000Mbps, cumpliendo el requerimiento.

- **Puertos de enlace ascendente de alta velocidad:** Utilice Gigabit Ethernet u otros puertos de enlace ascendentes de alta velocidad para conectar los conmutadores que se encuentran en ubicaciones diferentes.

Se utilizarán los enlaces Gigabit Ethernet para conectar los switches de acceso a los switches de Core/distribución.

- **Administración y supervisión remota:** En entornos grandes (más de 30 clientes), los conmutadores con opciones integradas de administración y supervisión remota son muy útiles especialmente en la resolución de problemas de la red.

Se implementará supervisión remota para la administración y supervisión de los switches.

Se contemplan las siguientes opciones para el switch capa 2 que se requiere:

Tabla 10, Comparación switch capa 2

Switch Hpe J9775A Gigabit Ethernet 2530- 48G 52 Puertos	\$ 3.839.900 pesos colombianos
Switch Administrable 48+4G Gigabit Uplink Tp-Link TL-SL3452	\$ 1.914.000 pesos colombianos
Cisco Sf20048p 48 Puertos 10100 Poe 2	\$ 2.039.000 pesos colombianos

En conclusión, las 3 referencias que se incluyeron cumplen con los requerimientos establecidos para el switch capa 2, los cuales tienen que ser administrables y contar con un mínimo de 100Mbps en cada puerto.

Entrando en análisis, se elige el switch TP-LINK TL-SL3252 debido a su cómodo precio de costo y que en comparación con los otros que tienen más características que en realidad no son relevantes para la propuesta de diseño que se plantea aquí.



Figura 28, TP-LINK TL-SL3452

Tabla 11, Características TP-LINK TL-SL3452

Interfaz	48 Puertos RJ45 10/100Mbps (Negociación automática/Auto MDI/MDIX) 2 Puertos RJ45 10/100 / 1000Mbps (Negociación automática/Auto MDI/MDIX) 2 Ranuras SFP Gigabit 1 puerto de consola
Medios de la red	10BASE-T: UTP categoría 3, 4, 5 cables (100m máximo) 100BASE-TX / 1000Base-T: UTP categoría 5, 5e, 6 o por encima del cable (100 metros como máximo) 1000BASE-X: MMF, SMF

QoS	<p>Soporte 802.1p prioridad CoS/DSCP</p> <p>Apoyo 4 queues de prioridad</p> <p>Programación de queues: SP, WRR, SP+WRR</p> <p>Puerto/ Flujo basado en límite de velocidad</p> <p>VLAN de voz</p>
VLAN	<p>Soporta hasta 4K VLAN simultáneamente (de 4K VLAN IDs)</p> <p>Puerto/MAC/VLAN basada en protocolo-GARP/GVRP</p> <p>Gestión de configuración de VLAN</p>
Access control list	<p>L2~L4 filtrado de paquetes basado en origen y destino de dirección MAC, dirección IP, puertos TCP/UDP, 802.1p, DSCP, protocolo y VLAN ID</p> <p>Basado en rango de tiempo</p>
Security	<p>Encuadre IP-MAC-Port-VID</p> <p>Autenticación basada en puerto IEEE 802.1X/ MAC, Radio, VLAN Invitado</p> <p>DoS Defensa</p> <p>Inspección dinámico ARP (DAI)</p> <p>SSH v1/v2</p> <p>SSL v2/v3/TLSv1</p> <p>Seguridad Portuaria</p> <p>Broadcast/Multicast/control de tormentas unicast desconocido</p>

8.1.5 Configuración Básica de los dispositivos

Antes de iniciar con las configuraciones de seguridad, enrutamiento, vlan, direccionamiento, se realizan las configuraciones básicas, entre las cuales están las asignaciones de nombre de host, contraseñas de acceso remoto o por consola de los equipos como también el modo de configuración de estos (Modo privilegiado) y el banner de advertencia.

Es importante configurar un nombre único a cada switch para ser documentado y poder identificarlo en caso de fallas o de alguna configuración que sea requerida.

A continuación, se muestra una tabla de los nombres que se le configurarán a los respectivos equipos:

Tabla 12, nombre de los dispositivos

Equipo	Nombre
Switch capa 3	Core-dis(1)
Switch capa 3 redundante	Core-dis(2)
Switch capa 2	Swaccess1
Switch capa 2	Swaccess2
Switch capa 2	Swaccess2

En las redes de producción se suele utilizar la configuración de un banner que se le muestra al usuario en consola al momento de acceder a los equipos que tienen restricción de acceso dentro de la compañía, dicho mensaje, tiene un significado muy importante legal.

Acorde con lo anterior, se plantea utilizar por defecto un mensaje que cumpla con la finalidad de dicho banner y que será configurado a todos los dispositivos administrables en la red. Sin embargo, se le recomendará a la empresa ponerse en contacto con un área jurídica para configurar un mensaje acorde para la empresa.

A continuación, se muestra el mensaje transitorio que se le ha configurado a los dispositivos:

Tabla 13, banner de presentación

<p>---BITS AMERICAS S.A.S---SOLO PERSONAL AUTORIZADO---</p>
--

Una de las configuraciones básicas más importantes y primera herramienta de seguridad para los dispositivos es la asignación de la contraseña tanto del modo privilegiado *execmode*, la de consola y las conexiones remotas.

A continuación, se muestra la contraseña que se le ha configurado a todos los dispositivos por defecto con el fin de dejarla establecida, pero recomendando a la compañía insertar las contraseñas a su consideración.

Tabla 14, configuración de contraseñas de modo privilegiado

Seguridad modo privilegiado	Password: bits	Exec time-out 10
Seguridad consola	Password: bits	Exec time-out 10
Seguridad conexión remota	Password: bits	Exec time-out 10

Los comandos utilizados para las configuraciones básicas se pueden consultar en el anexo C.

8.1.6 Configuración de enlaces troncales

En el diseño que se propone se tiene contemplado la creación de Vlans, cada interfaz de los switch dependiendo de las necesidades estará configurado para permitir el tráfico de datos de la Vlans que tenga configurada. Dichas interfaces se deben poner en modo de acceso (mode Access).

Sin embargo, existen interfaces por las que circulará todo el tráfico de la red y se conectan con otros switches, a esas interfaces se les conoce como enlaces troncales y deben configurarse en modo trunk.

En la propuesta de diseño se configuraron las siguientes interfaces en modo troncal:

Tabla 15, Configuración de enlaces troncales

Dispositivo	Interfaces troncales
Switch core-dis	F0/1, F0/2, F0/3, G0/1, G0/2
Switch core-dis redundante	F0/1, F0/2, F0/3, G0/1, G0/2
Switch acceso 1	G0/1, G0/2, F0/24
Switch acceso 2	G0/1, G0/2, F0/24
Switch acceso 3	G0/1, G0/2, F0/24

Los comandos utilizados para configurar los enlaces troncales se pueden consultar en el anexo C.

8.1.7 Configuración protocolo troncal virtual

Una de las configuraciones más recomendadas cuando se utiliza redes virtuales dentro de una red LAN que está compuesta por dispositivos capa 2 y capa 3 es el protocolo troncal virtual (VTP) con el cual se busca que todas las Vlans de la red tengan una configuración consistente en toda la red y facilitar al área de soporte de la empresa una herramienta para crear Vlans desde un punto de la red y no tener que crearlas en cada uno de los dispositivos (tarea tediosa).

Para configurar VTP en la red LAN, se necesita configurar un dispositivo como servidor (Mode server) que será el punto de administración, creación de Vlans y finalmente el que compartirá la información de estas. los demás equipos, cuya configuración también requiere tener establecidas las Vlans, se disponen como clientes (Mode client). Estos dispositivos recibirán la información que tenga configurada el servidor.

A continuación, se muestra que dispositivos se configuraron como clientes y cual se escogió para ser el servidor:

Tabla 16, Configuración VTP

Dispositivo	Interfaces troncales	Dominio
Switch core-dis	Server	Bits.com
Switch core-dis redundante	Client	
Switch acceso 1	Client	
Switch acceso 2	Client	
Switch acceso 3	Client	

Los comandos utilizados para configurar VTP en los dispositivos se pueden consultar en el anexo C.

8.1.8 Definición y configuración de redes virtuales (VLANs)

Con el objetivo de optimizar el consumo de recursos de la red, para este diseño se diseñaron VLANs con la intención de implementar seguridad de información entre las diferentes áreas y la reducción de tráfico broadcast entre los dispositivos.

Se analizo la distribución de los grupos de usuarios que la compañía tiene y se definieron las siguientes Vlan con sus respectivos integrantes:

- WIFI-Empresa (Vlan 10)
- Invitados (Vlan 20)
- Administración (Vlan 30)
- Fabrica (Vlan 40)
- Ventas (Vlan 50)
- Salas (Vlan 60)

- VoIP (Vlan 70)
- Servers (Vlan 100)
- Administrador de red (Vlan 101)

Para la configuración de las Vlans basta con escoger el switch que se configuro como servidor VTP (core-dist (1)) para que dinámicamente se replique la información de Vlans en la base de datos de los equipos cliente.

Además de crear las Vlans dentro del dispositivo servidor, es necesario asignar a las Vlans los puertos en modo de acceso de los switches de acceso capa 2 para que los clientes que se conecten a dichos puertos pertenezcan a su respectiva Vlans.

Todas las Vlans creadas corresponden a tráfico de datos, dado que, para el tráfico de voz, se debe diferenciar del tráfico de datos y así poder garantizarle las características y QoS requeridas para que la red soporte las exigencias de la telefonía IP.

Los comandos utilizados para configurar las Vlans en los dispositivos se pueden consultar en el anexo C.

8.1.9 Direccionamiento IP

En la propuesta de diseño de la red se postula utilizar la IP privada clase B 172.16.0.0/16 dado que actualmente se utiliza una dirección privada clase A que no se ve necesario implementar debido a la cantidad de usuarios que la compañía presenta y que teniendo en cuenta un dispositivo Wireless por cada usuario de la red no superará los 326 host.

La dirección privada 172.16.0.0/16 asegura 65534 host lo que significa que se cuentan con la cantidad de direcciones privadas disponibles para cualquier requerimiento de la entidad sin necesidad de desperdiciar direcciones, sino que se utilice realmente las necesarias utilizando el método CIDR que está basado en la técnica VLSM (Variabilidad de la longitud de la máscara de subred)

A continuación, se listan las direcciones IP de red asignadas a cada una de las Vlans implementadas en la red:

Tabla 17, direccionamiento IP

Subnet Name	Needed Size	Allocated Size	Address	Mask	Dec Mask	Assignable Range	Broadcast
WIFI corp	133	254	172.16.0.0	/24	255.255.255.0	172.16.0.1 - 172.16.0.254	172.16.0.255
Fabrica	100	126	172.16.1.0	/25	255.255.255.128	172.16.1.1 - 172.16.1.126	172.16.1.127
VoIP	30	30	172.16.1.128	/27	255.255.255.224	172.16.1.129 - 172.16.1.158	172.16.1.159
Administración	22	30	172.16.1.160	/27	255.255.255.224	172.16.1.161 - 172.16.1.190	172.16.1.191
Comercial	11	14	172.16.1.192	/28	255.255.255.240	172.16.1.193 - 172.16.1.206	172.16.1.207
Invitados	10	14	172.16.1.208	/28	255.255.255.240	172.16.1.209 - 172.16.1.222	172.16.1.223
Salas	10	14	172.16.1.224	/28	255.255.255.240	172.16.1.225 - 172.16.1.238	172.16.1.239
Network Admin	7	14	172.16.1.240	/28	255.255.255.240	172.16.1.241 - 172.16.1.254	172.16.1.255
Servidores	3	6	172.16.2.0	/29	255.255.255.248	172.16.2.1 - 172.16.2.6	172.16.2.7

Al utilizar VLSM y una máscara de subred de 16bits para los hosts, podemos darnos cuenta de que la cantidad total de direcciones IP que la red principal (172.16.0.0/16) puede ofrecer es de 65534. Estamos usando aproximadamente un 1% de las direcciones disponibles al necesitar 326 IPs. Esto con el fin de tener disponible dentro de la red escogida más direcciones cuando sea necesario, pero utilizando las direcciones que realmente se necesitaran por lo menos en los últimos 3 años.

Con base a la información en la tabla, se puede apreciar que existe un pool de direcciones IP destinada para cada Vlan, sin embargo, dicho pool, tendrá 3 direcciones que no se podrán utilizar, las cuales son, la de red, broadcast y la que asignemos como Gateway de salida de cada Vlan, que, en este caso, será la última del rango disponible.

Es por esto por lo que se implementara el Protocolo de enrutamiento dinámico (DHCP) para asignar respectivamente las direcciones disponibles dentro de cada Vlan a cada usuario que se conecte. Sin embargo, habrá direcciones estáticas, por ejemplo, la Vlan servidores cuyas direcciones no sirven dinámicas porque son dispositivos que se acceden de manera continua o la Vlan de administración de red la cual tendrá asignadas direcciones IP a cada dispositivo para ser administrable.

A continuación, se listan los pool de direcciones o direcciones estáticas que se configurarán para cada Vlan:

Tabla 18, Asignación de VLANS

ID Vlan	Usuario	Dirección IP
Vlan 10	Access point 1	172.16.1.113/29
	Access point 2	172.16.1.114/29
	Access point 3	172.16.1.115/29
Vlan 20	Usuarios Desarrolladores 1/84	Rango: 172.16.0.129/25 a 172.16.0.253/25
Vlan 30	Usuarios Administradores 1/20	Rango: 172.16.1.1 /27 a 172.16.1.29/27
Vlan 40	Access point 1	172.16.1.105/29
	Access point 2	172.16.1.106/29
	Access point 3	172.16.1.107/29
Vlan 50	Usuarios Ventas 1/20	Rango: 172.16.1.65/28 a 172.16.1.77/28
Vlan 100	Servidor EMAIL	172.16.1.81/28

	Servidor DNS	172.16.1.82/28
	Servidor WEB	172.16.1.83/28
	Servidor FTP	172.16.1.84/28
Vlan 101	Usuario Admin	172.16.1.97/29
	Swacceso 1	172.16.1.98/29
	Swacceso 2	172.16.1.99/29
	Swacceso 3	172.16.1.100/29
	Switch core-dist (2)	172.16.1.101/29

Los comandos utilizados para configurar las Vlans en los dispositivos se pueden consultar en el anexo C.

9 PLAN DE PRUEBAS DEL SISTEMA

Es importante tener en cuenta que el plan de pruebas para este proyecto de grado difiere un poco de los demás, debido a que el proyecto se limita a la propuesta de diseño de red LAN. Es por ello por lo que las pruebas se realizarán al finalizar cada etapa del diseño y se ejecutarán sobre la simulación de la red.

9.1 Plan de pruebas IP Estáticas

Tabla 19, Plan de pruebas IP Estáticas

Objetivo	Verificar la correcta asignación de las direcciones IP a los dispositivos que se definieron tendrán direcciones estáticas.
-----------------	--

Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer
Procedimiento	<ul style="list-style-type: none"> • Emitir el comando <IPconfig> en el CMD de cada servidor conectado a la red • Verificar que este configurado el protocolo STATIC IP. • Verificar que cada servidor tenga definido su respectiva dirección IP, mascara de subred, Gateway y servidor DNS.
Salida esperada	Los servidores están totalmente configurados con su respectiva dirección IP estática, mascara de subred, Gateway de salida y servidor DNS.

9.2 Plan de pruebas DHCP

Tabla 20, Plan de pruebas DHCP

Objetivo	Verificar la correcta asignación de las direcciones IP a cada una de las terminales de trabajo y los dispositivos de conmutación y enrutamiento.
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer.
Procedimiento	<ul style="list-style-type: none"> • Emitir el comando <IPconfig> en el CMD de cada cliente conectado a la red • Verificar que este configurado el protocolo DHCP. • Emita el comando <Show running-config> en los dispositivos capa 3.

	<ul style="list-style-type: none"> • Verificar que tenga configurado el protocolo DHCP, tenga excluidas las direcciones IP de broadcast y Gateway • Verificar que tenga definido el pool de direcciones IP para cada Vlan que se utilizaran para asignar a cada cliente conectado.
Salida esperada	Los clientes conectados a la red tienen configurada una dirección IP dinámica de acuerdo con el pool de direcciones definidas en el servidor DHCP (Switch capa 3)

9.3 Plan de pruebas de VLSM

Tabla 21, Plan de pruebas VLSM

Objetivo	Verificar la correcta asignación de la subred a cada uno de los terminales de trabajo, los dispositivos que conmutan y servidores de red
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer
Procedimiento	<ul style="list-style-type: none"> • Emitir el comando <IPconfig> en el CMD de cada cliente conectado a la red y los servidores • Verificar que las direcciones pertenezcan a la subred configurada según VLSM. • Emita el comando <Show ip interface brief> en los conmutadores capa 2 y capa 3 para ver la configuración de las IP

Salida esperada	Los clientes conectados a la red, los servidores y dispositivos conmutadores, tienen configurada su dirección IP de acuerdo con la subred que tienen configurada
------------------------	--

9.4 Plan de pruebas VTP

Tabla 22, Plan de pruebas VTP

Objetivo	Verificar la correcta implementación y propagación del protocolo troncal virtual
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer
Procedimiento	<ul style="list-style-type: none"> • Ingresar al switch configurado como servidor y emitir el comando <show vtp status> • Verificar que efectivamente el protocolo este activo y que su rol sea <i>Server</i> • Verificar que tenga configurado el dominio bits.com • Ingresar al resto de los switches los cuales deben estar configurados como clientes y emitir el comando <show vtp status> • Verificar que efectivamente el protocolo este activo y su rol sea <i>client</i> • Verificar que tenga configurado el dominio bits.com • Verificar que las Vlans creadas en el dispositivo servidor se propaguen con todo e

	información a los demás dispositivos configurados como clientes
Salida esperada	El protocolo VTP está activo y tiene su respectivo servidor y clientes

9.5 Plan de pruebas VLAN

Tabla 23, Plan de pruebas VLANs

Objetivo	Verificar la correcta creación de las Vlan y que se cumpla con el objetivo de independizar a los usuarios por cada grupo de la compañía
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer.
Procedimiento	<ul style="list-style-type: none"> • En los dispositivos capa 2 y capa 3 emitir el comando <Show vlan brief> • Verificar que dichos dispositivos tengan configuradas las siguientes Vlan: <ul style="list-style-type: none"> ○ Vlan 10 Wifienterprise ○ Vlan 20 Administration ○ Vlan 30 Development ○ Vlan 40 Guess ○ Vlan 50 Sales ○ Vlan 100 Servers ○ Vlan 101 Networkadmin • Verificar que dichas vlans tengan configuradas las interfaces de salida en cada switch.

	<ul style="list-style-type: none"> • Verificar que cada Vlan tenga configurada si respectiva subred.
Salida esperada	Las Vlans están completamente creadas y configuradas en la red

9.6 Plan de pruebas de Ping

Tabla 24, Plan de pruebas PING

Objetivo	Verificar la reducción en los tiempos de respuestas de la red y conectividad de esta.
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer.
Procedimiento	<ul style="list-style-type: none"> • Ingresar al CMD de los diferentes clientes conectados en la red. • Emitir el comando <ping #ip> hacia alguna dirección IP de cualquier dispositivo dentro de la red. • Verificar que exista respuesta del host de destino al que se quiere acceder y que los tiempos sean menores a 1ms.
Salida esperada	Respuesta de los dispositivos de los clientes conectados con tiempos de respuestas menores a 1ms permitiendo conectividad entre los usuarios de la red.

9.7 Plan de pruebas de disponibilidad y protocolo STP

Tabla 25, Plan de pruebas STP y disponibilidad

Objetivo	Verificar que la red puede continuar su operación normal aun cuando falle uno de los enlaces entre las diferentes áreas.
Entrada	Consola de los diferentes dispositivos de la red en el simulador packet tracer.
Procedimiento	<ul style="list-style-type: none"> • Verificar que los enlaces redundantes estén configurados y en modo troncal en los diferentes dispositivos capa 2 y capa 3 • Verificar que si un enlace se cae, la red establezca comunicación por sus enlaces redundantes enviando la información y mostrando la alta disponibilidad. • Verificar que no existan bucles ni loops que interfieran en la comunicación de datos
Salida esperada	Los enlaces redundantes de la red funcionan haciendo que la red cuente con alta disponibilidad

10 IMPLEMENTACIÓN

La implementación en este proyecto se basa en las simulaciones que se hicieron para validar que la propuesta funciona correctamente, es por esto por lo que, a continuación, se muestra el esquema implementado en el simulador de redes GNS3, donde se utilizaron Switches capa 2 y capa 3 que cuentan con las características de los dispositivos que se piensan implementar.

La simulación inicia teniendo configurado el ambiente. GNS3 recomienda que los dispositivos que se utilicen se corran en una máquina virtual que se puede implementar junto con el programa llamada GNS3 VM.

Por esta razón, se descarga el software VMWARE FUSION que permite crear máquinas virtuales y se crea la máquina virtual para GNS3.

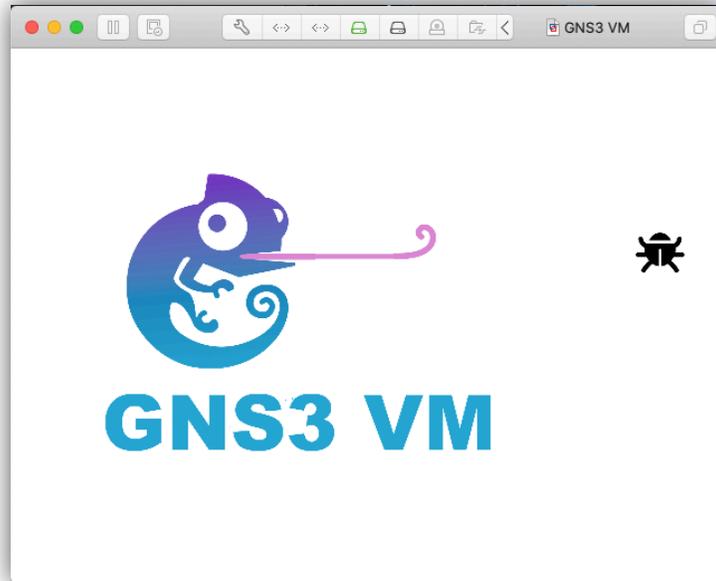


Figura 29, Máquina virtual para GNS3

Una vez la máquina virtual carga, esta muestra las configuraciones iniciales con las que se puede trabajar en la máquina virtual.

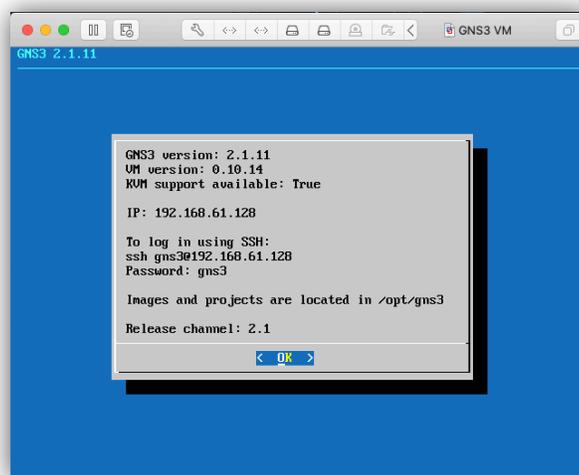


Figura 30, GNS3 VM Información

Es importante tener en cuenta que muchos de los dispositivos necesitan tener activa la opción KVM que es la herramienta que permite la virtualización de dispositivos, es por eso que está en TRUE.

Volviendo a la interfaz de GNS3, se importan dispositivos capa 2 y capa 3 para simular los switches, creándolos como interfaces IOU, lo que significa que son IOS que corren sobre UNIX, estas imágenes tienen una desventaja y es que son algo inestables, pero para las simulaciones de características capa 2 y capa 3 son ideales y contienen las características que necesitamos para este diseño.

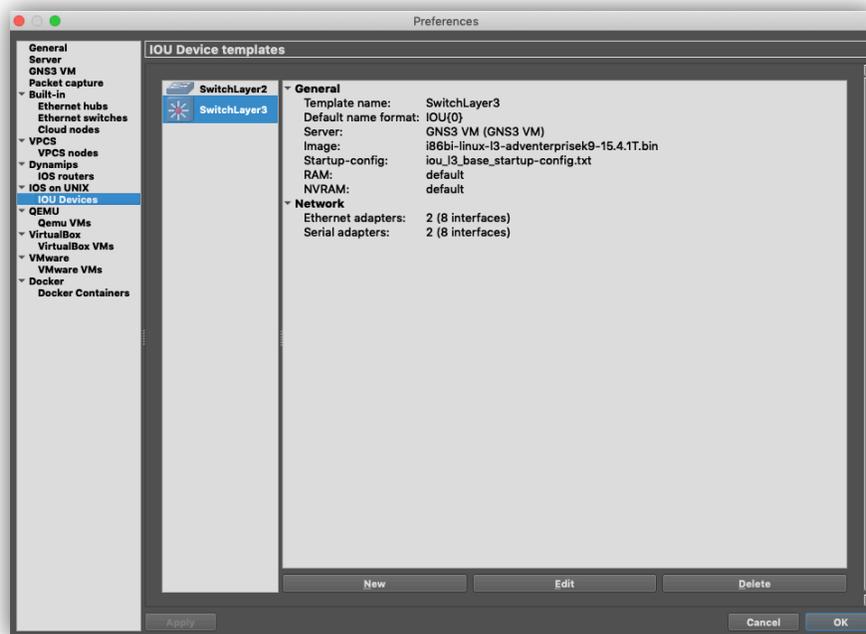


Figura 31, Agregando los switches capa 2 y capa 3 con IOU

Una vez se tienen los dispositivos listos para utilizar, se agregan en la mesa de trabajo donde se pueden interconectar unos con otros. A continuación, se muestra la topología que se utilizó para el diseño de la red.

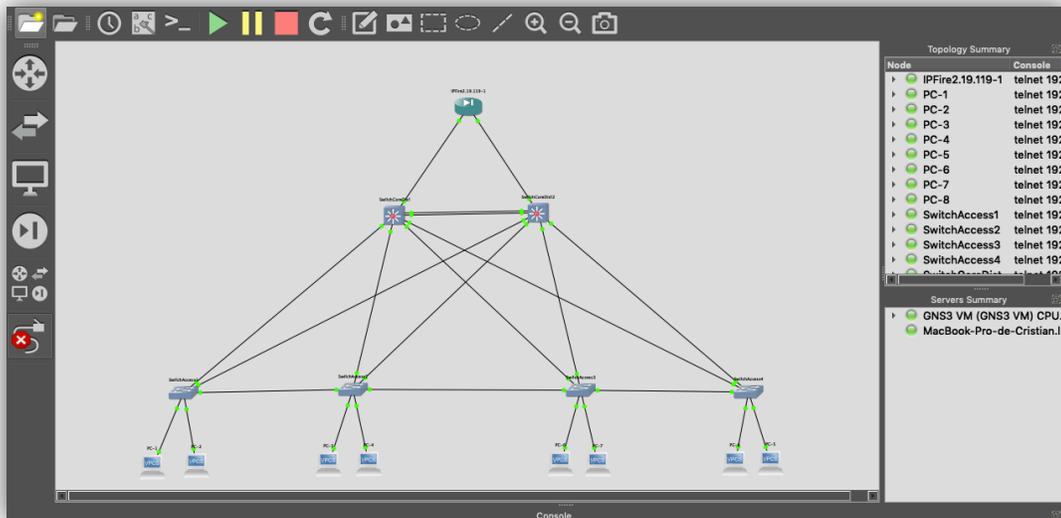


Figura 32, Topología de red diseñada

Se agregan switch capa 2 y capa 3 para la simulación que permiten tener propiedades tales como VLANs, Enrutamiento, SPT, VTP para hacer la configuración respectiva y hacer que la topología cumpla con los requerimientos que la empresa necesita.

Se utiliza la arquitectura jerárquica de red que CISCO propone a partir de capas, la capa de acceso la cual consta de 4 switch los cuales están interconectados entre sí para dar redundancia a la red y de donde se desprenden los usuarios finales de la red como lo son todos los empleados.

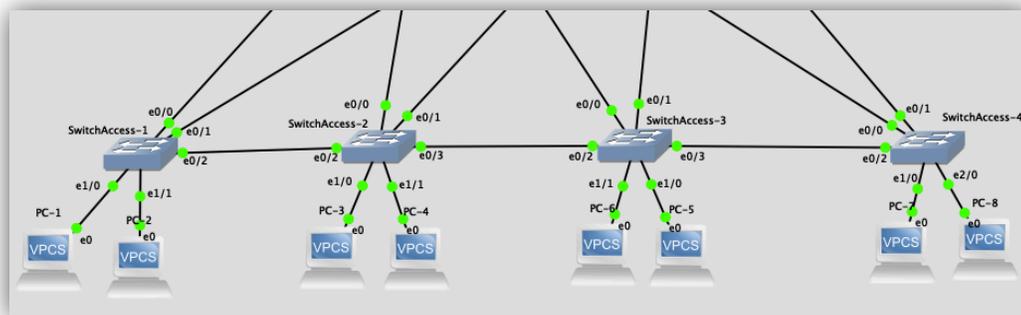


Figura 33, Capa de acceso topología red LAN BITS AMERICAS

Para cada switch de acceso se configuran los enlaces troncales y los de acceso, en este caso se configuraron las interfaces Ethernet 0/0 a la Ethernet 0/3 como enlaces

troncales y las Ethernet 1/0-3, 2/0-3 y 3/0-3 como enlaces de acceso para las respectivas Vlan según sea el caso.

```
VLAN10 WIFI_Empresa 192.168.1.0/29
VLAN20 Invitados 192.168.0.240/29
VLAN30 Administración 192.168.0.128/27
VLAN40 Fabrica 192.168.0.0/25
VLAN50 Ventas 192.168.0.192/28
VLAN60 Salas 192.168.0.208/28
VLAN70 VoIP 192.168.0.160/27
VLAN100 Servidores 192.168.0.248/29
VLAN101 Administración 192.168.0.224/28

SwitchAccess-1:
interfaces ethernet 0/0 - 3 TRUNK
interfaces ethernet 1/0 - 3 Access VLAN 10
interfaces ethernet 2/0 - 3 Access VLAN 20
interfaces ethernet 3/0 - 3 Access VLAN 30

SwitchAccess-2:
interfaces ethernet 0/0 - 3 TRUNK
interfaces ethernet 1/0 - 3 Access VLAN 40
interfaces ethernet 2/0 - 3 Access VLAN 40
interfaces ethernet 3/0 - 3 Access VLAN 40

SwitchAccess-3:
interfaces ethernet 0/0 - 3 TRUNK
interfaces ethernet 1/0 - 3 Access VLAN 50
interfaces ethernet 2/0 - 3 Access VLAN 60
interfaces ethernet 3/0 - 3 Access VLAN 70
```

Figura 34, Vlan y configuración de enlaces

En cuanto a la capa de Core y distribución por el tamaño de la red no se vio necesario hacerlas por separado, por esto se pensó en 2 switch capa 3 que permitirán dar acceso a los usuarios de la red basado en políticas de seguridad.

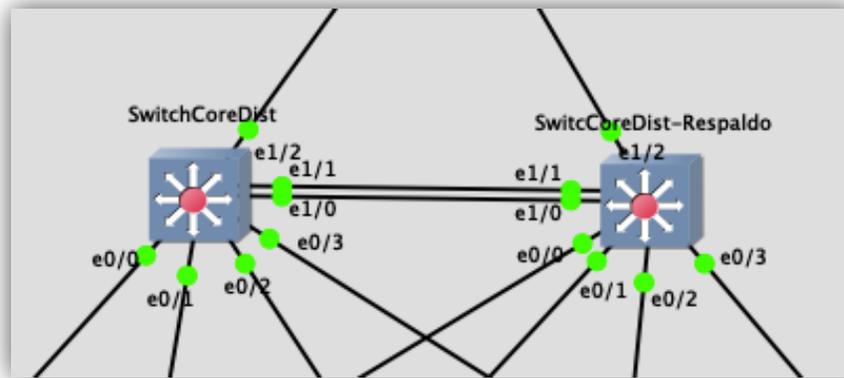


Figura 35, Capa de Core/dist topología red LAN BITS AMERICAS

Al igual que en la capa de acceso las interfaces Ethernet 0/0 a la Ethernet 0/3 y con las interfaces Ethernet 1/0 a la 1/3, se configuraron como enlaces troncales donde estos reciben todo el tráfico de datos de los switches de acceso y aquí es donde se enruta el tráfico interno para conectar las VLANS, además se tiene un enlace redundante entre los switch de Core que permite anticipar cualquier fallo en la red.

En la simulación se colocó un PC de la VLAN 101 (Administración de red) para centralizar la administración de dispositivos vía telnet,

Cada dispositivo tiene su respectiva consola de configuración, donde se aplican las respectivas configuraciones mostradas en el ANEXO C del documento.

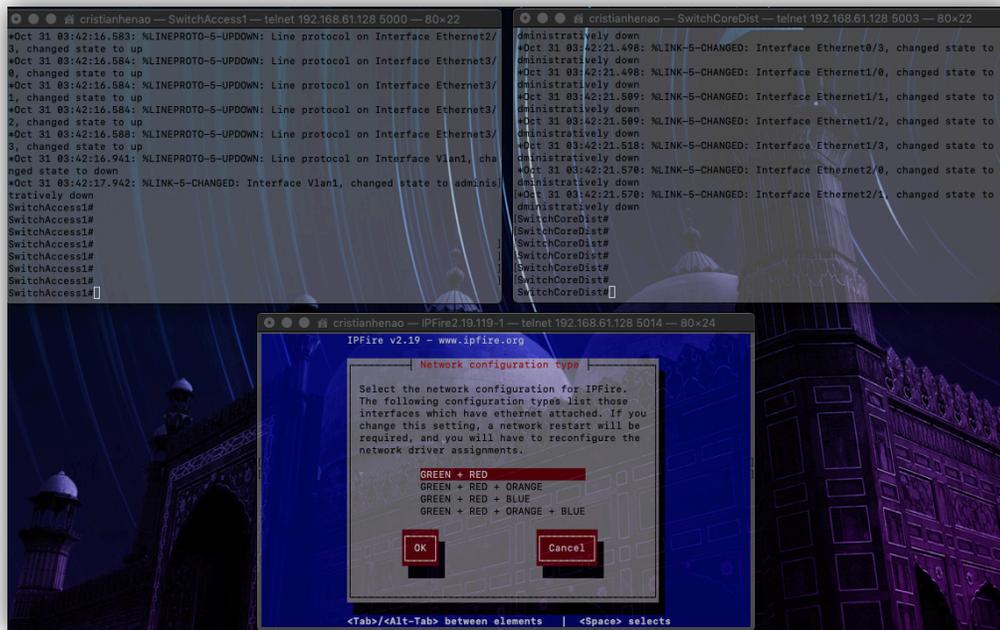


Figura 36, Consola de los dispositivos

La simulación se encuentra anexa en el documento para más información y para poder observar el funcionamiento de la red a profundidad.

11 DISEÑO INDUSTRIAL

11.1 Análisis de la actividad y el contexto

11.1.1 Análisis del contexto

Para el correcto análisis del contexto se empezará por aclarar que la empresa actualmente tiene planes de mudarse a finales de noviembre a una nueva sede en donde se unirán las dos sedes en Bogotá que actualmente están.

A continuación, se muestran los planos de organización de la nueva sede tanto el primero como el segundo piso.



Figura 37, Piso 1

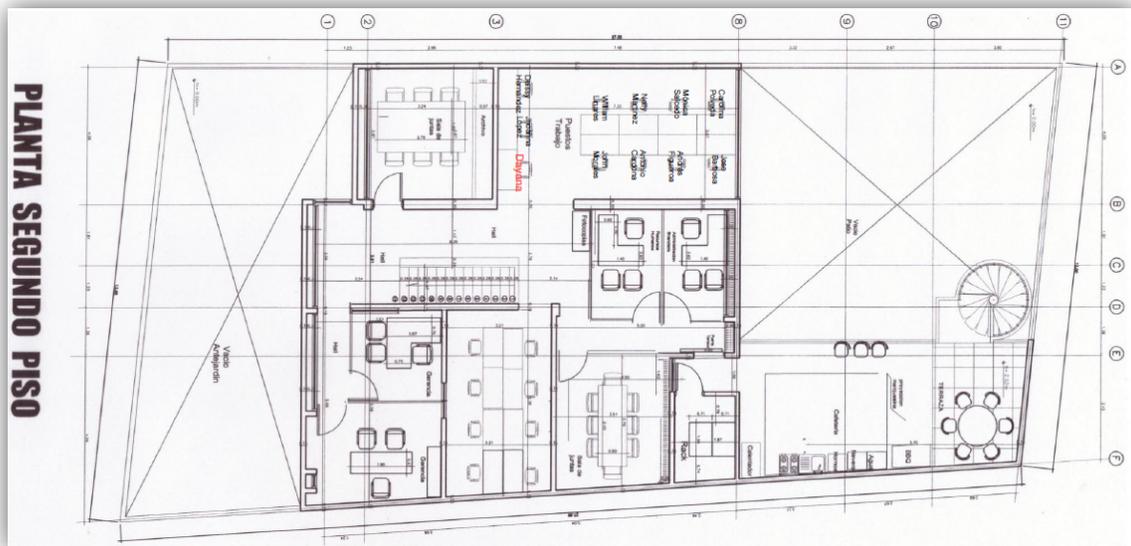


Figura 38, Piso 2

Es por esto por lo que se tendrá en cuenta un diseño industrial básico que permita tener en cuenta factores como ubicación de la red en la nueva instalación, Cantidad de puertos físicos que se requieren para que cada oficina, espacio de trabajo o sala de reuniones cuente con los

suficientes puntos de acceso. Además del cableado estructurado, su correcto y presentable flujo a través de la empresa y También, las características que tendrá el área restringida donde se ubicarán los Rack que almacenarán los servidores, switches y routers.

A continuación, se listan algunos de los servicios más importantes que la empresa ofrece y dependen de infraestructura de red:

- **Video conferencia:** Se realizan entre clientes y trabajadores de la empresa que se encuentran en teletrabajo o trabajan en diferentes ciudades.
- **Correo:** El email se maneja directamente con OFFICE 365 de Microsoft.
- **Servicios de impresión:** El servicio de impresión se hace con dos impresoras ubicadas una en cada sede.
- **Acceso remoto:** Se utiliza para administrar la parte contable de la empresa utilizando conexión a escritorio remoto de Windows.

Los usuarios que componen la red son:

- Administrativos (15)
- Comerciales (20)
- TI (45)
- Soporte TI (3)

El tráfico que circula por la red es el siguiente:

- Internet.
- Datos.
- Telefonía.

11.1.2 Casos de uso

A continuación, se listan los casos de uso típicos con los que contaría la infraestructura de red:

- Los usuarios tienen un acceso físico en su puesto de trabajo al llegar a la oficina.

- Los usuarios administradores acceden remotamente a través del escritorio remoto de Windows a los servidores locales de la compañía.
- Los desarrolladores utilizan la información de base de datos de los servidores locales para realizar los códigos.
- Todos los usuarios acceden a internet para solicitar los servicios en la nube (OneDrive), donde tienen los repositorios de información.
- Todos los usuarios acceden a internet para solicitar los servicios en la nube (Zoho), que es una herramienta de gestión de proyectos.
- Todos los usuarios utilizan la infraestructura de red para entablar comunicación con los trabajadores remotos o clientes por medio de aplicaciones como Skype ó Zoom.
- Todos los usuarios de la red acceden por el WIFI a la red con sus dispositivos móviles.

A continuación, se listan los casos de uso atípicos con los que contraría la infraestructura de red:

- La empresa contrata nuevos empleados que no tiene donde ubicar en la nueva sede por falta de puertos físicos que permitan el acceso a internet.
- Hay un apagón y los usuarios quedan sin acceso a internet.
- El acceso a la red inalámbrica de la red no está disponible y los usuarios no pueden acceder al WIFI.
- En las salas de junta no existen puertos de conexión por cada puesto de la mesa.
- Los puertos físicos asignados a cada puesto de trabajo pueden estar expuesto a daño.
- Usuarios no autorizados ingresan al cuarto de racks y pueden alterar o robar información

11.2 Requerimientos industriales

11.2.1 Requerimientos de uso

A continuación, se listan los requerimientos de uso que presentará el sistema.

- La red tendrá que estar ubicada en un cuarto aparte a los puestos de trabajo para que el ruido que generan los ventiladores este aislado del personal.
- Los dispositivos de red como routers, switches o servidores tendrán que contar con clave de acceso para poderlos configurar.

- El cuarto donde se vallan a ubicar los racks de servidores, conmutadores y enrutadores debe estar bajo llave.
- A los racks se les deberá hacer mantenimiento cada 6 meses.
- El área donde se ubiquen los racks debe contar con ventilación para evitar sobrecalentamiento de los equipos en función.
- El puerto RJ45 que llegara a cada puesto de trabajo debe contar por lo menos con un metro de distancia para que el usuario pueda tener una libertad de movimiento aceptable.

11.2.2 Requerimientos de función

A continuación, se listan los requerimientos de función que presentará el sistema.

- La red debe estar distribuida en la empresa por regata para la planta del primer piso y por el techo falso para el segundo piso, evitando así, cualquier incidente con el cableado.
- La red debe proveer conectividad a los usuarios de esta las 24 horas del día 7 días a la semana.

11.2.3 Requerimientos de estructura

A continuación, se listan los requerimientos de estructura que presentará el sistema.

- Los equipos que componen la red deben estar cubiertos por los racks, que deben contar con buena ventilación y tener seguridad de llaves.
- Los racks deben contar con slots de ubicación y entre estos debe haber un espacio mínimo de 30cm para evitar el calentamiento de los equipos por la temperatura generada por estos mismos.

11.2.4 Requerimientos Legales y normativos

A continuación, se listan los requerimientos legales y normativos que presentará el sistema.

- El sistema debe estar regido bajo la norma ISO 17799.

- El sistema debe estar redigo bajo la norma EIA/TIA 568.

11.2.5 Requerimientos de identificación

A continuación, se listan los requerimientos de identificación que presentará el sistema.

- El área de la red estará identificada por un letrero ubicado a un metro del piso y en la puerta del mismo sitio.
- Cada equipo del rack debe contar con su respectiva identificación, Nombre de cada servidor, Router, Switches y demás componentes con los que cuente la red.

11.3 Materiales, procesos y normativas

11.3.1 Materiales de Protección

Es importante tener en cuenta que la protección a los equipos que componen la red es un factor importante y hay que tenerlo en cuenta por temas de seguridad debido a que se pueden evitar manipulaciones sin permiso o simplemente evitar que los dispositivos internos se deterioren con facilidad o se caigan, por esto a continuación se muestra el rack de seguridad que podría ser útil en la implementación de la red:

NavePoint 22U IT Wall Mount Network Server Data Cabinet Rack Glass Door Locking Casters.

Dimensions	41" H x 24" W x 24" D
Item weight	37kg
Weight capacity	47kg
Material	Robusta estructura de marco soldada
Others	Rieles con pernos estilo jaula y Se adapta al equipo estándar de montaje en rack de 19 ".



Figura 39, Rack a utilizar

11.3.2 Cableado

Como toda red, se cuentan con puertos físicos que se originan en el switch de acceso, pero debe atravesar toda la infraestructura de la empresa de forma presentable para llegar a cada puesto de trabajo.

Como se cuentan con 2 plantas, se propone utilizar techo falso en el segundo piso y regata en el primero.



Figura 40, Cableado por regata



Figura 41, Cableado por techo falso

Además, es importante tener en cuenta el tipo de cableado que se puede utilizar. como el proyecto se piensa orientar a utilizar tecnología Ethernet, se necesitará cable UTP con cabeza RJ45, a continuación, se listan las categorías disponibles y sus especificaciones.

Especificaciones Cat3, Cat4, Cat5, Cat5e, Cat6, and Cat7

Category	Type	Spectral R/W	Length	Lan Applications	Notes
CAT3	UTP	16MHz	100m	10Base-T, 4Mbps	For telephone
CAT4	UTP	20MHz	100m	16Mbps	Rare
CAT5	UTP	100MHz	100m	100Base-T, ATM, CDDI	LAN Use
CAT5e	UTP	100MHz	100m	100Base-T	LAN Use
CAT6	UTP	250MHz	100m		Emerging
CAT7	ScTP	600MHz	100m		

Figura 42, Especificaciones categoría cable UTP

Según las especificaciones de cada categoría de cable UTP, se aconseja elegir la categoría 5E que tiene una conexión 100base-T (Fast ethernet) recomendada para una conmutación óptima y cuya aplicación está orientada a redes LAN.

Cctv Cable De Red Utp Categoría 5e Exterior



Figura 43, Cable UTP categoría 5E

Tabla 26, Características cable UTP Cat 5E

Lenght	305 metros
Categoría	5E

11.3.3 Procesos

A pesar de que este proyecto se limita únicamente a la propuesta de diseño de la red LAN a la empresa BITS AMERICAS S.A.S. El posible proceso de producción de este se tendría que hacer junto a las directivas de la compañía para evaluar el presupuesto que serían capaces de invertir en el proyecto, estimar el tiempo de realización que podría llegar a tomar de 1 a 2 semanas para garantizar la calidad del servicio y organización de la red.

11.3.4 Normativas

- EIA/TIA

En la década de los 80 la TIA (Telecommunications Industry Association) y la EIA (Electronic Industries Association). Empezó a desarrollar métodos de cableado de edificios con el fin de desarrollar un sistema de cableado semejante que permite la integración de diferentes fabricantes y múltiples entornos.

Este estándar define la manera como diseñar, construir y administrar un sistema de cableado estructurado con muy buen rendimiento. Esta norma define el uso de cable UTP, STP y fibra Monomodo y multimodo. Existen estándares como T568A y T568B, pero para esta solución se usará T568A con el propósito de que se puedan tener diferentes proveedores estableciendo un estructurado genérico, que el cliente tenga protección de su inversión realizada con un tiempo mínimo de 10 años.

EL estándar T568A se aplica para los requerimientos mínimos del cableado estructurado en una oficina, topología de la red y distancias recomendadas y conexiones que aseguren la interconexión y parámetros que determinen el rendimiento por esto se usará este estándar.

- ISO (Organización Internacional para la Normalización).

Es una Organización internacional que tiene una extensa gama de estándares, Desarrollo el modelo OSI que es un modelo de referencia para la creación de redes. En 1994 ISO establece la norma 11801 en la cual se define los estándares para la instalación de dispositivos y conexiones.

Unas de las ventajas de ISO es que facilita la detección de fallas, porque al momento que se produzcan solo afectara a la estación que depende de esa conexión, también permite una mayor flexibilidad para expansión, eliminación y cambios de usuario del sistema. Se usan conexiones de UTP que a pesar de que son más costosas evitan pérdidas económicas al producirse caídas del sistema porque solo se afectara el dispositivo implicado en la conexión

ISO 11801 reitera lo propuesto por EIA/TIA el cual define clases de aplicación y es el estándar de cableado de telecomunicaciones para edificios.

11.4 Planificación de la producción

11.4.1 Primera alternativa

Para este diseño se cuenta con el rack de servidores, router y switches ubicado en el primer piso de la empresa al lado del grupo de soporte y junto con 47 estaciones de trabajo y 3 Access point que están ubicados por departamento y el segundo piso que cuenta con 40 estaciones de trabajo y 2 Access point también separados por departamento, para este diseño se propone establecer el cableado estructurado a través del piso con canaletas para llegar a cada puesto de trabajo y para el segundo piso atravesar el cableado por el techo y también mandarlo por canaletas a cada puesto de trabajo de los 40 empleados allí.

A continuación, se muestra la posible distribución por plantas del cableado a través de la estructura de la empresa:

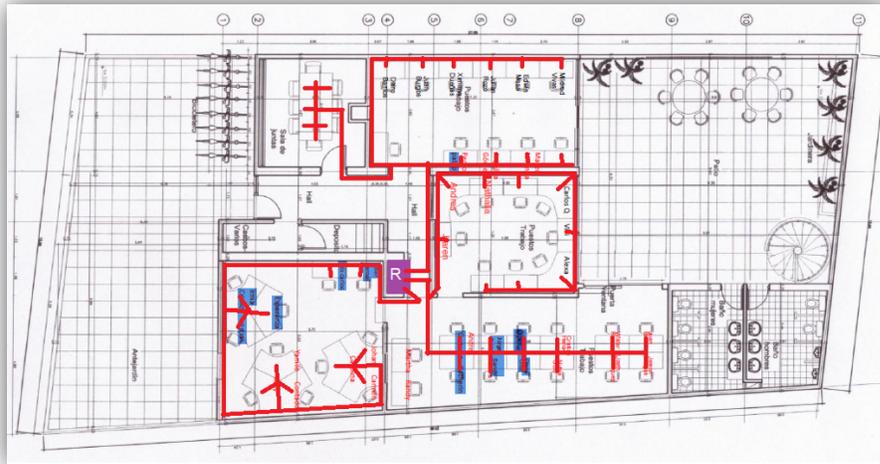


Figura 44, Primera alternativa de cableado

11.4.2 Segunda alternativa

El rack de servidores está aislado en un cuarto aparte.	1	0.3	4	0.8	20%
Se cumple con la norma EIA/TIA 568	5	1	5	1	20%
El cuarto donde se vallan a ubicar los racks de servidores, conmutadores y enrutadores debe estar bajo llave	1	0.4	5	2	40%
El rack de servidores debe estar ubicado en el primer piso por contener equipos de gran peso	5	0.5	1	0.1	10%

Debe estar aislado del personal de trabajo debido al ruido que provocan los ventiladores	2	0.2	4	0.4	10%
Total		2.4		4.3	100%

Como se puede apreciar en la tabla, se escoge de manera radical la segunda alternativa debido a que es la que tiene mejor evaluación frente a los requerimientos de producción y facilita tanto la implementación como la presentación de la red a través de la empresa, Adicionalmente se tendrá un mejor control al estar en un área restringida debido a lo delicado que es el tema de la seguridad de la información.

Es importante resaltar que esta documentación se presentara a la empresa ara ser evaluada y luego si analizar su alcance y tiempo de realización.

11.5 Diseño detallado

11.5.1 Definición de componentes principales

A continuación, se definen los componentes principales a utilizar en el desarrollo de la propuesta de solución:

Tabla 28, Componentes a utilizar

IMAGEN	NOMBRE	DESCRIPCIÓN
--------	--------	-------------

	<p>ROUTER CISCO RV082</p>	<p>Enrutador de dos puertos WAN y 4 puertos LAN con funcionalidad de switch de 10/100/1000 Mbps</p>
	<p>SWITCH 3COM 4800G</p>	<p>Conmutador de capa 2 y capa 3 con capacidad de switcheo de 10/100/1000 Mbps y funcionalidad de Stack.</p>
	<p>ACCESS POINT MOJO C-130</p>	<p>Punto de acceso de hasta 800Mbps para un radio de 2,4GHz con capacidad de operación total de 802.3at POE</p>
	<p>CABLE UTP CAT 5E</p>	<p>Cable de par trenzado con capacidad de transferencia de 100 base T.</p>

La documentación del diseño industrial se encuentra adjunta en el anexo D.

12 RESULTADOS

Como resultado del diseño que se plantea en este documento, se realizaron las siguientes implementaciones en la propuesta entregada a la empresa:

Se utilizó un diseño jerárquico teniendo en cuenta 4 switch capa 2 (Capa de acceso) y dos switch capa 3 (Capa Core/distribución) de la red, con lo que se obtuvo mejoras en las velocidades y rendimiento de la red. Debido a que en la conmutación de paquetes es más eficiente en este tipo de redes en comparación con las redes de capa 3.

También, este redimiendo fue optimizado con la implementación de EthernetChannel que permitió que el ancho de banda se unificará en los switch de Core percibidos por la red al utilizar dos enlaces Fastethernet como si fueran uno solo.

Además, la implementación de VLANs lo que permitió tener un control mayor sobre los grupos de usuarios que maneja la compañía, esto con el fin de dividir el tráfico que circula por la red y los dominios de broadcast para optimizar el rendimiento de la red y la escalabilidad de la red ya que se tuvo en cuenta que para los próximos 3 años se espera un crecimiento del 10% por año, lo que ocasionó el análisis de los switches que se escogieron 4 de acceso cada uno de 48 puertos para un total de 192 puertos necesitando 160.

La alta disponibilidad de la red, que se logró creando entre cada uno de los switches en el diseño enlaces redundantes con los cuales se obtuvo esta resiliencia, dicha disponibilidad fue probada en las simulaciones y en el anexo C, se documentó todos los scripts utilizados con los comandos necesarios para configurar cada uno de los dispositivos implementados en esta propuesta, además, se entrega la simulación de la red.

13 DISCUSIÓN

A continuación, las recomendaciones que se le hacen a la empresa BITS AMERICAS SAS como adicional para la mejora constante a la red que se propone aquí, se sugiere que es importante mantener actualizada la documentación de los puntos de red, con lo que se evitarían volver a asignar puntos en desorden que afectan la adecuación y gestión de la LAN.

Además, mantener siempre al día el direccionamiento IP asignado a cada dispositivo activo dentro de la red para evitar fallas por la duplicidad o asignación equivocada de las IP que el servidor DHCP brinda.

La utilización de un software para acceso remoto, que ayude a la funcionalidad de escritorio remoto con buenos niveles de seguridad, como Remote Desktop y adquirir un software de gestión de red que permita agilizar la identificación de las fallas, que genere reportes e informes para realizar el mantenimiento preventivo de acuerdo con las causas de fallas que más se repitan.

Realizar pruebas planificadas para identificar la capacidad de la red para recuperarse de fallas críticas y probar su característica de resiliencia y también realizar mantenimiento preventivo del cableado de la red, para evitar que se degraden las condiciones físicas de la instalación

Por último, aplicar las mejores prácticas para la gestión de incidentes, para permitir a la empresa mejorar los procesos y procedimientos para la atención de fallas como por ejemplo realizar y mantener la documentación de los incidentes atendidos, lo que permitirá en un futuro arreglar los mismos incidentes de manera más óptima y eficaz.

14 CONCLUSIONES

Gracias al protocolo VTP implementado se hace mucho más fácil el trabajo de implementar las VLANs dentro de la red, esta característica fue determinante para la separación del tráfico de la empresa, permitiéndole a los administradores de la red una manera más sencilla de percibir y controlar la manera en que funciona la red, esto permite, si es necesario la configuración o creación de más VLAN que se configurarían directamente en el switch de Core y no equipo por equipo.

Además, al realizar este proyecto de grado se pudieron aprender demasiados temas que no se abordaron dentro de las materias de la carrera, permitiendo así, adquirir conocimientos que le permitan a uno ejercer más adelante como diseñador de redes de área local.

Al diseñar una red LAN jerárquica, permite que las personas encargadas de controlar la red puedan identificar de manera más eficiente el origen de las fallas que posiblemente pueda presentar la red, esto debido a que un diseño jerárquico es modular, escalable y flexible. Con esto se busca reducir los altos tiempos de atención a los incidentes presentados.

También, al utilizar el modelo de arquitectura de red cisco, se puede entender mejor cómo funcionan los módulos que componen una red en su totalidad, y permite, además, percibir fácilmente que modulo vienen el problema al presentar fallas.

Con las pruebas que se realizaron en la simulación de la red, se pudo corroborar el cumplimiento de los requerimientos del cliente, entre los cuales se encuentra la optimización del rendimiento en la red y características muy importantes como lo son la disponibilidad y la escalabilidad.

15 REFERENCIAS DOCUMENTALES

- (1) Edgar Correa. Tiempo extra en porcentaje que están tomando los proyectos por solicitudes de soporte en la red de bits américas s.a.s. 2017.
- (2) Tiempo CEE. Cuatro de cada diez empresas en el país no están preparadas para un ciberataque. Available at: <http://www.portafolio.co/negocios/empresas/ciberataque-empresas-preparadas-colombia-492281>. Accessed Nov 4, 2017.
- (3) Cisco. Introduction to LAN Protocols. WC-M 2012 Oct 16,.
- (4) Ecured. Red de área local (LAN). Available at: https://www.ecured.cu/EcuRed:Enciclopedia_cubana
- (5) Cisco. CCNA Exploration 4.0 Modulo 1, Aspectos básicos de networking. 2007.
- (6) Justo Carracedo Gallardo. Seguridad en redes telemáticas. ; 2004.
- (7) Jaime Cardenas Arturo Puestas Lila Chavez Edwin Gamarra. Proyecto Final de Redes 1. 2009; Available at: <https://redesuss.wordpress.com/>. Accessed Nov 11, 2017.
- (8) Cisco. CCNA Exploration 4.0 Modulo 3, Conmutación y conexión inalámbrica de LAN. 2008.

(9) Cisco. Cisco Validated Design, Campus Resumen de diseño ; : cisco systems; 2014.

(10) Cisco. Cisco Validated Design, Campus LAN and WLAN design guide. : cisco systems; 2016.

(11) Microsoft, Available at:

http://download.microsoft.com/download/4/d/9/4d9ae285-3431-4335-a86e-969e7a146d1b/rdp_performance_whitepaper.docx

(12) test de velocidad, Available at: <https://www.testdevelocidad.es/internet-carga-descarga/>

(13) BignewSoftware, Available at:

<http://bignewsoftware.blogspot.com/2011/04/norma-eia-tia-568a-568b.html>

(14) Firefold, Available at: <https://www.firefold.com/blog/stp-vs-utp-cables-comparison>

(15) OpenUp, Available at: <https://www.openup.es/informacion-de-cables-cat5-cat5e-cat6-cat7-cat7a-y-cat8/>