

**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO**

CARRERA: INGENIERÍA ELECTRÓNICA

Tesis previa a la obtención del título de: INGENIEROS ELECTRÓNICOS

**TEMA:
DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA LA
UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR**

**AUTORES:
MANUEL ALEJANDRO MORENO JIMÉNEZ
LUIS ANDRÉS TIPÁN AGUAS**

**DIRECTOR:
JORGE ENRIQUE LÓPEZ LOGACHO**

Quito, abril del 2015

**DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO
DEL TRABAJO DE TITULACIÓN**

Nosotros, autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de titulación y su reproducción sin fines de lucro.

Además, declaramos que los conceptos, análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Quito, abril del 2015

Manuel Alejandro Moreno Jiménez

C.I: 171712710-2

Luis Andrés Tipán Aguas

C.I: 172321681-6

DEDICATORIA

Dedico este trabajo de titulación a todos los que creyeron en mí, especialmente a mis padres y hermanas que han sido un gran apoyo para poder culminar mi carrera, siendo ellos mi motivación de seguir adelante y esforzarme cada día para seguir progresando como persona y como profesional.

Gracias por ser como son, por todo ese cariño que me han sabido brindar durante estos años.

Luis Andrés Tipán Aguas

Con todo mi cariño y mi amor para las personas que hicieron todo en la vida para que yo pudiera lograr mis sueños, por motivarme y darme la mano cuando sentía que el camino se terminaba, a ustedes por siempre mi corazón y mi agradecimiento Papá y Mamá.

A tu paciencia y comprensión, preferiste sacrificar tu tiempo para que yo pudiera cumplir con el mío. Por tu bondad y sacrificio me inspiraste a ser mejor para ti, ahora puedo decir que este trabajo de titulación lleva mucho de ti, gracias por estar siempre a mi lado, Rocío.

A mi hijo que algún día llegará a ser mejor que yo.

Manuel Alejandro Moreno Jiménez

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO 1	2
PARÁMETROS DEL PROYECTO	2
1.1. Estructura funcional de la Universidad Politécnica Salesiana	2
1.2. Planteamiento del problema.....	4
1.3. Objetivos	4
1.3.1. Objetivo general	4
1.3.2. Objetivos específicos	4
1.4. Justificación.....	5
1.5. Alcances	5
CAPÍTULO 2	7
ESTADO DEL ARTE	7
2.1. Definición de una red de área local.....	7
2.1.1. Necesidad de una red de área local	7
2.1.2. Características de una red de área local.....	7
2.2. Topología física.....	8
2.2.1. Topología tipo bus.....	8
2.2.2. Topología tipo anillo	9
2.2.3. Topología tipo estrella.....	9
2.4.1. Funcionalidad	10
2.4.2. Escalabilidad	10
2.4.3. Adaptabilidad	11
2.4.4. Redundancia.....	11
2.4.5. Facilidad de administración.....	11
2.5. Calidad de servicio (QoS)	11
2.5.1. Parámetros de calidad de servicio	12

2.5.2. Requerimientos de calidad de servicio de las aplicaciones	12
2.5.3. Servicios QoS.....	13
2.5.3.1. Enrutamiento selectivo	13
2.5.3.2. Control de tráfico	13
2.5.3.3. Acceso remoto a redes de comunicaciones	13
2.5.3.4. Administración de ancho de banda	14
2.5.3.5. Balanceo de carga	14
2.6. Seguridad en las redes.....	14
2.6.1. Seguridad tipo física.....	15
2.6.2. Seguridad tipo lógica.....	15
2.6.3. Niveles de seguridad informática	16
2.7. Universidad Politécnica Salesiana sede quito campus Sur.	17
2.7.1. Ubicación.	17
2.7.1.1 Bloque A	17
2.7.1.2 Bloque B	19
2.7.1.3 Bloque C	20
2.7.1.4 Bloque D	21
2.7.1.5 Bloque E.....	22
2.7.1.6 Bloque F.....	23
2.7.1.7 Bloque H	24
2.7.1.8 Bloque G	25
2.8. Diseño de red jerárquico	26
2.9. Análisis de la situación actual e infraestructura de la red	26
2.9.1 Capa de core y distribución.....	27
2.9.2. Capa distribución y acceso	27
2.9.2.1 Redes virtuales en el campus.	30
2.9.3. Topología inalámbrica	33
2.9.4. Cobertura de dispositivos (access point).....	34
2.9.5. Cobertura access point exteriores.....	34
2.9.5.1. Bloque A.....	34

2.9.5.2. Bloque B	36
2.9.6. Cobertura access point interiores	38
2.9.6.1. Administración	38
2.9.6.2. Biblioteca	39
2.9.6.3. Análisis del tráfico actual	40
CAPÍTULO 3.....	41
DISEÑO DE LA RED LAN	44
3.1. Criterios de diseño lan para la red de alta disponibilidad	44
3.2. Número de usuarios en la red.....	44
3.2.1 Expansión futura	46
3.3. Equipos a usar	47
3.3.1. Marca de los equipos.....	47
3.3.2. Cantidad de equipos	48
3.3.2.1. Distribución de los equipos por bloque.....	48
3.4. Especificaciones técnicas de los equipos	50
3.4.1. Especificaciones técnicas del core-cisco 6506e.....	51
3.4.2. Especificaciones técnicas de distribución cisco 3750.....	53
3.4.3. Especificaciones técnicas acceso-cisco 2960.....	55
3.4.4 Especificaciones técnicas cisco asa 5515-x	56
3.4.5 Especificaciones técnicas cisco s380 web security appliance.....	57
3.4.6 Especificaciones técnicas cisco 2500 series wireless controller.....	58
3.4.7. Especificaciones técnicas antenas cisco aironet 1520 outdoor	60
3.4.8. Especificaciones técnicas antenas cisco aironet 2600 input	61
3.5. Uso de poe.....	62
3.6. Solución inalámbrica.....	63
3.6.1 Cobertura inalámbrica exterior todo el campus	63
3.6.1.1. Funcionalidad general de la red propuesta	64
3.7. Servicios y aplicaciones	65

3.7.1. Seguridad a nivel de acls	67
3.7.2. Alta disponibilidad	67
3.7.2.1 Disponibilidad actual.....	68
3.7.2.2 Disponibilidad a obtenerse con la propuesta de diseño.....	69
3.8. Simulador gns3	69
3.8.1 Topología física.....	70
3.8.2 Topología lógica.....	71
3.8.3 Topología de conectividad en gns3	72
3.9 Configuración de la simulación	73
3.9.1. Pasos detallados de la configuración de GLBP.....	73
3.9.2. Configuración de dispositivos.....	76
3.9.3. Análisis de resultados.....	76
CAPÍTULO 4.....	81
DISEÑO DE LA RED LAN	81
4.1. Análisis técnico	81
4.2. Beneficios primordiales de orden técnico	82
4.3. Análisis económico	83
4.3.1 Valores referenciales	83
CONCLUSIONES.....	87
RECOMENDACIONES.....	88
LISTA DE REREFERENCIAS.....	89

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Organigrama Funcional TI-Rectorado	2
<i>Figura 2.</i> Topología de red tipo Bus	8
<i>Figura 3.</i> Topología de red tipo Anillo.....	9
<i>Figura 4.</i> Topología de red tipo Estrella.....	10
<i>Figura 5.</i> Amenazas para la seguridad en la red	14
<i>Figura 6.</i> Gráfico de distribución cuartos de comunicación bloque A	18
<i>Figura 7.</i> Gráfico de distribución cuartos de comunicación bloque B	20
<i>Figura 8.</i> Gráfico de distribución cuartos de comunicación bloque C	21
<i>Figura 9.</i> Gráfico de distribución cuartos de comunicación bloque D	22
<i>Figura 10.</i> Gráfico de distribución cuartos de comunicación bloque E	23
<i>Figura 11.</i> Gráfico de distribución cuartos de comunicación bloque F.....	24
<i>Figura 12.</i> Gráfico de distribución cuartos de comunicación bloque H.....	25
<i>Figura 13.</i> Modelo de diseño jerárquico.....	26
<i>Figura 14.</i> Infraestructura actual de la red Core y Bloque A.....	27
<i>Figura 15.</i> Infraestructura actual de la red Bloque B, C, D, E, F, H	28
<i>Figura 16.</i> Distribución de VLAN.....	32
<i>Figura 17.</i> Topología inalámbrica	33
<i>Figura 18.</i> Área física de la UPS, Sede Quito – Campus Sur.....	34
<i>Figura 19.</i> Área física de la UPS, Sede Quito – Campus Sur.....	35
<i>Figura 20.</i> Área física de la UPS, Sede Quito – Campus Sur.....	36
<i>Figura 21.</i> Área física de la UPS, Sede Quito – Campus Sur.....	37
<i>Figura 22.</i> Interior del bloque A.	38
<i>Figura 23.</i> Área física de la UPS, Sede Quito – Campus Sur.....	39
<i>Figura 24.</i> Análisis de tráfico en el Switch de core	40
<i>Figura 25.</i> Amenazas en la red	41
<i>Figura 26.</i> Vulnerabilidad tipo SQL injection.....	411
<i>Figura 27.</i> Vulnerabilidad tipo cross-site scripting	412
<i>Figura 28.</i> Vulnerabilidad tipo HTTP trace support detected	412
<i>Figura 29.</i> Recursos de contenido HTTP trace support detected	413
<i>Figura 30.</i> Usuarios conectados en la red inalámbrica	466
<i>Figura 31.</i> Distribución de los equipos bloque A	49

<i>Figura 32.</i> Distribución de los equipos bloques B,C,D,E,F	49
<i>Figura 33.</i> Distribución de los equipos bloques H,G	50
<i>Figura 34.</i> Cuadrante de Gartnet	51
<i>Figura 35.</i> Cobertura de la red inalámbrica realizada con covera zone.....	63
<i>Figura 36.</i> Cobertura inalámbrica exterior solución.....	64
<i>Figura 37.</i> Distancia de cobertura CISCO Aironet 1520.....	65
<i>Figura 38.</i> Topología de conectividad física	71
<i>Figura 39.</i> Topología de conectividad lógica	71
<i>Figura 40.</i> Topología física de la red LAN	72
<i>Figura 41.</i> Tráfico INT sin GLBP	77
<i>Figura 42.</i> Tráfico INT con GLBP	77
<i>Figura 43.</i> Ping Host-Host con GLBP	78
<i>Figura 44.</i> Ping Host-Host sin GLBP	78
<i>Figura 45.</i> Tiempos de latencia con GLBP	79
<i>Figura 46.</i> Tiempos de latencia sin GLBP.....	80

ÍNDICE DE TABLAS

Tabla 1. <i>Parámetros de calidad de servicio QoS</i>	12
Tabla 2. <i>Requerimientos de calidad de servicios</i>	12
Tabla 3. <i>Usos arquitectónicos</i>	17
Tabla 4. <i>Sistema de distribución MDF, SDF e IDF en el bloque A</i>	17
Tabla 5. <i>Sistema de distribución SDFs en el bloque B</i>	19
Tabla 6. <i>Sistema de distribución SDF en el bloque C</i>	20
Tabla 7. <i>Sistema de distribución SDF en el bloque D</i>	21
Tabla 8. <i>Sistema de distribución SDF en el bloque E</i>	22
Tabla 9. <i>Sistema de distribución SDF en el bloque F</i>	23
Tabla 10. <i>Sistema de distribución SDF en el bloque H</i>	24
Tabla 11: <i>Sistema de distribución SDF campus sur</i>	28
Tabla 12. <i>Sistema de distribución redes virtuales campus sur</i>	30
Tabla 13. <i>Intensidades de Señales bloque A parte frontal</i>	35
Tabla 14: <i>Intensidades de Señales bloque A parte posterior</i>	36
Tabla 15. <i>Intensidades de Señales bloque A lateral sur</i>	37
Tabla 16. <i>Intensidades de Señales bloque A lateral norte</i>	37
Tabla 17: <i>Intensidades de Señales</i>	38
Tabla 18: <i>Intensidades de Señales</i>	39
Tabla 19: <i>Alertas software vega</i>	43
Tabla 20. <i>Sistema de distribución de usuarios campus sur</i>	45
Tabla 21. <i>Puntos de red a futuro</i>	46
Tabla 22. <i>Plataforma tecnología</i>	48
Tabla 23: <i>Especificaciones técnicas del CORE-CISCO 6506e</i>	52
Tabla 24. <i>Especificaciones técnicas de distribución-CISCO 3750</i>	53
Tabla 25. <i>Especificaciones técnicas acceso-CISCO 2960</i>	55
Tabla 26. <i>Especificaciones técnicas CISCO ASA 5515-x</i>	56
Tabla 27. <i>Especificaciones técnicas CISCO s380 web security appliance</i>	57
Tabla 28. <i>Especificaciones técnicas CISCO 2500 series wireless controller</i>	59
Tabla 29. <i>Especificaciones técnicas antenas CISCO Aironet 1520 outdoor</i>	60
Tabla 30. <i>Especificaciones técnicas antenas CISCO aironet 2600 input</i>	61
Tabla 31. <i>Intensidades de Señales red inalámbrica</i>	63
Tabla 32. <i>Servicios y Aplicaciones Actuales</i>	66

Tabla 33. <i>Servicios y Aplicaciones Adicionales</i>	66
Tabla 34. <i>Acuerdo de nivel de servicio (SLA)</i>	68
Tabla 35. <i>Análisis de las características primordiales de orden técnico</i>	81
Tabla 36. <i>Costos referenciales de equipamiento cisco</i>	83
Tabla 37. <i>Costos referenciales de enlaces de Internet</i>	84
Tabla 38. <i>Costos referenciales de enlaces de Datos</i>	84
Tabla 39. <i>Análisis Económico</i>	85
Tabla 40. <i>Interpretación del VAN y TIR</i>	86

ÍNDICE DE ECUACIONES

Ecuación 1. Fórmula de la disponibilidad	67
Ecuación 2. Fórmula del VAN	86
Ecuación 3. Fórmula del TIR	86

ÍNDICE DE ANEXOS

Anexo 1. Análisis de necesidades de renovación de equipos de cómputo (pc) de la sede Quito campus Sur.....	91
Anexo 2. Gráficos ancho de banda usados en la Universidad Politécnica Salesiana sede quito campus Sur usando el software PRTG	96
Anexo 3. ACLs y direccionamiento propuesto para la red propuesta de alta disponibilidad.....	105
Anexo 4. Configuración de los equipos y gráficos del funcionamiento de la red simulada utilizando el protocolo GLBP.....	115

RESUMEN

El crecimiento de la red de datos en los próximos años con la implementación de los nuevos servicios propuestos por la Universidad Politécnica Salesiana Sede Quito Campus Sur obligan a contar con una red eficiente.

Por esta razón este proyecto plantea el diseño de una red de alta disponibilidad, que consiste en una red de datos basada en la infraestructura actual para lo cual se realizará un levantamiento de la topología física y lógica para efectuar un estudio de la carga de tráfico en los horarios críticos y así obtener datos de la demanda de tráfico actual que posee la Universidad Politécnica Salesiana, con esto se realizará un dimensionamiento de la red (velocidad de transmisión, cobertura inalámbrica, calidad de servicio, etc.) por medio de una simulación.

El proyecto tiene como objetivo principal el resolver los problemas de los usuarios en la red de datos y satisfacer las necesidades para el acceso a las aplicaciones y servicios que se tendrán en los próximos años en la Universidad Politécnica Salesiana Sede Quito Campus Sur.

ABSTRACT

The growth in data network in the coming years with the implementation of new services offered by the Salesian Polytechnic University South Campus Headquarters Quito force us to have an efficient network.

For this reason, this project proposes the design of a high availability network, which consists of a data network based on the existing infrastructure for which a survey of the physical and logical topology is made for a study of the traffic load in critical data and get current traffic demand having the Salesian University, with this a network dimensioning is performed (transmission speed, wireless coverage, service quality, etc.). Schedules through a simulation.

The project's main objective is to solve user problems in the data network and meet the needs for access to applications and services have in the coming years in the Salesian University South Campus headquarters Quito.

INTRODUCCIÓN

El apareamiento de nuevas aplicaciones y servicios para los usuarios dentro de la red de datos que se va a tener en los próximos años en la Universidad Politécnica Salesiana Campus Sur propone diferentes retos para la administración de la información y las comunicaciones por la cual es necesario diseñar una red de alta disponibilidad que permita la integración de cualquier aplicación o sistema de servicios que ayude a cumplir con los requerimientos de los usuarios.

En el capítulo 1, se analizará el problema planteado, los objetivos generales y específicos, la justificación, alcances y el análisis del estado actual de la red de datos.

En el capítulo 2, se describe el análisis del estado inicial de la Universidad Politécnica Salesiana Sede Quito Campus Sur, igualmente contiene argumentos importantes para el diseño de red que se realizará posteriormente para conseguir una red de alta disponibilidad, de igual forma también se explica definiciones y conceptos afines a redes, sus principales características y la importancia de las mismas incluyendo de manera importante la seguridad.

El capítulo 3, contiene el análisis de los requerimientos para el diseño de la red de alta disponibilidad a partir de la situación actual de la red de la Universidad Politécnica Salesiana Sede Quito Campus Sur, se incluyen simultáneamente los criterios de diseño para la red tomando en cuenta una expansión a futuro de la red de 3 a 10 años.

En el capítulo 4, se realizará un análisis técnico-económico tomando en cuenta las áreas para las alternativas de diseño propuestas en el capítulo anterior. Además se incluye un análisis económico de la solución desarrollada, con el objetivo de conseguir una proximidad de los precios existentes en el mercado nacional.

Finalmente se incluyen las conclusiones y recomendaciones procedentes del presente estudio, para comprender varios aspectos importantes relacionados con el diseño de la red LAN donde se incluirán anexos que permitan visualizar de manera adecuada la mejora realizada por este proyecto.

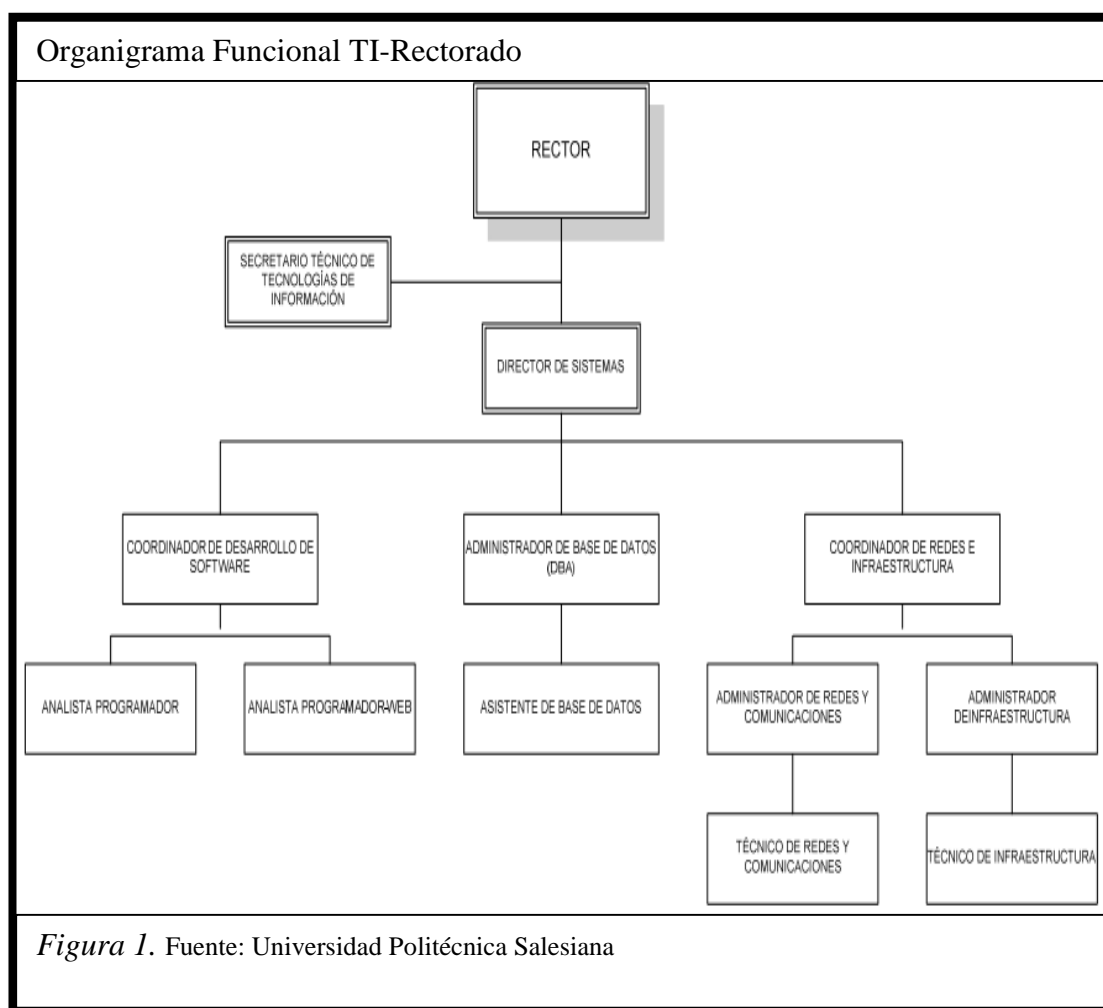
CAPÍTULO 1

PARÁMETROS DEL PROYECTO

1.1. Estructura funcional de la Universidad Politécnica Salesiana

La Universidad Politécnica Salesiana creada mediante Ley N° 63 expedida por el Congreso Nacional y publicada en el registro oficial N° 499 del 5 de agosto de 1994, es una institución autónoma, de educación superior particular, católica, cofinanciada por el Estado. Es una persona jurídica de derecho privado, con finalidad social y sin fines de lucro. Su domicilio principal y matriz se halla en la ciudad de Cuenca, con sedes en las ciudades de Quito y Guayaquil. (Estatuto de la Universidad Politecnica Salesiana, 2014, pág. 1)

La Universidad Politécnica Salesiana tiene una estructura orgánica funcional del área de TI-Rectorado de la siguiente manera.



Las ocupaciones de los puestos mostrados en el organigrama se detallan a continuación:

Rector: coordinar y asesorar asuntos en el desarrollo tecnológico y científico de la Universidad Politécnica Salesiana.

Secretario técnico: apoyar a las diferentes áreas para conseguir una adecuada infraestructura.

Director de sistemas: garantizar la disponibilidad de los servicios de Tecnología de la Información de la Universidad Politécnica Salesiana.

Coordinador de desarrollo de software: asegurar la disponibilidad, coordinar el desarrollo y mantenimiento de las aplicaciones informáticas requeridas de la Universidad Politécnica Salesiana.

Administrador de base de datos: garantizar la disponibilidad de las Bases de datos de la Universidad Politécnica Salesiana.

Coordinador de redes e infraestructura: planificar, definir, coordinar y supervisar el mantenimiento de la operatividad de la infraestructura de telecomunicaciones, servidores y de equipos de usuario de la Universidad Politécnica Salesiana.

Analista Programador: desarrollar software de acuerdo a las necesidades de la Universidad Politécnica Salesiana.

Administrador de redes y comunicaciones: garantizar el funcionamiento de las comunicaciones, red y seguridad informática de la Universidad Politécnica Salesiana.

Administrador de Infraestructura: garantizar el correcto funcionamiento de la Infraestructura de telecomunicaciones de la Universidad Politécnica Salesiana.

Técnico de redes y comunicaciones: ofrecer soporte al usuario y mantener el control de los cambios realizados. (Salesiana, 2015)

Las Tecnologías de la Información (TI) bajo la dependencia mostrada en la figura 1 tiene como función principal prestar soporte técnico a toda la Universidad Politécnica Salesiana en el ámbito de la información y las comunicaciones.

1.2. Planteamiento del problema

Hoy en día, el crecimiento tecnológico ha dado lugar a la evolución de las aplicaciones, generando que las redes de datos requieran más disponibilidad, para así ser capaz de adaptarse a los cambios por el crecimiento del tráfico de información y así evitar que existan posibles problemas tales como: falencias a nivel físico (atenuación de la señal, insuficiente ancho de banda, interferencia inalámbrica), falencias a nivel de red (configuración de dispositivos incorrecta, problemas de autenticación y seguridad, ancho de banda insuficiente), falencias a nivel de Switches y VLAN (asignación de VLAN incorrectamente, problemas de prioridad de tráfico, uso excesivo).

1.3. Objetivos

1.3.1. Objetivo general

- Diseñar una red de alta disponibilidad, orientada a los servicios prestados por el Departamento de Tecnologías de la Información para la Universidad Politécnica Salesiana Sede Quito campus Sur.

1.3.2. Objetivos específicos

- Determinar los requerimientos del estado actual de la red de datos para satisfacer los servicios prestados por el Departamento de Tecnologías de la Información en la Universidad Politécnica Salesiana Sede Quito campus Sur.
- Identificar las vulnerabilidades que existen en la red actual tanto en equipos como a nivel de firewall.
- Diseñar la red de alta disponibilidad para la Universidad Politécnica Salesiana Sede Quito campus Sur.
- Verificar el desempeño de la red diseñada respecto a la red actual en base a: tráfico, cobertura, ancho de banda, velocidad de transmisión, QoS para llegar a la disponibilidad del 99.9%.
- Analizar la factibilidad técnica y económica del proyecto para su futura implementación.

1.4. Justificación

Actualmente, el uso creciente de la tecnología ha dado lugar a un incremento en la cantidad de usuarios en la red de telecomunicaciones, esto se debe básicamente al aumento en la cantidad de dispositivos en el mundo, por lo cual, se requiere mejoramiento en equipos de networking, mayor ancho de banda para el acceso a las aplicaciones y redundancia en la red de datos, que permita cumplir con los requerimientos de los usuarios.

Para que no existan consecuencias tales como el aumento de pérdida de paquetes, lentitud en la transferencia de archivos, aumento en la vulnerabilidad de la seguridad y congestión de la red de datos por el crecimiento de la red que se va a tener en los próximos años con la implementación de los nuevos servicios propuestos por la Universidad Politécnica Salesiana Sede Quito Campus Sur que son los siguientes: seguridad perimetral, masificación de cobertura inalámbrica, implementación de sistemas de control de accesos, incremento de equipos informáticos para usuarios, video conferencia, entre otros.

Esto genera la necesidad de contar con una red de alta disponibilidad para así ser capaz de adaptarse a los cambios por el crecimiento del tráfico de información a través de la infraestructura de la red actual.

1.5. Alcances

Este proyecto, genera un modelo de mejoras en la red de datos para satisfacer las necesidades de acceso a los nuevos servicios y aplicaciones que se implementaran en los próximos años en la Universidad Politécnica Salesiana sede Quito campus Sur siendo útil para todos los usuarios.

Para lo cual se diseñará una red de alta disponibilidad, orientada a los servicios prestados por el Departamento de Tecnologías de la Información que actualmente ofrece los siguientes servicios:

- Sistema de Matriculación
- AVAC
- VoIP

- WIFI
- Portal Institucional
- Cámaras IP

Debido a las vulnerabilidades que en la actualidad presentan las redes inalámbricas se debe considerar identificar las amenazas que existen en la red actual tanto en equipos como a nivel de firewall para que su desempeño sea óptimo. Por último, gracias a la alta disponibilidad de la red, se conseguirá que los usuarios puedan conectarse a Internet desde cualquier lugar en la Universidad Politécnica Salesiana Sede Quito Campus Sur, y en cualquier momento con una calidad de servicio eficaz.

CAPÍTULO 2

ESTADO DEL ARTE

En el capítulo presente se describe el análisis del estado inicial de la Universidad Politécnica Salesiana Sede Quito Campus Sur, igualmente contiene argumentos importantes para el diseño de red que se realizará posteriormente para conseguir una red de alta disponibilidad, de igual forma también se explica definiciones y conceptos afines a redes, sus principales características y la importancia de las mismas incluyendo de manera importante la seguridad.

2.1. Definición de una red de área local

Una red de área local o LAN (Local Area Network), es la interconexión de uno o varios equipos informáticos dentro de un área geográfica limitada, la cual permita a los usuarios compartir recursos e intercambiar datos y aplicaciones. Las redes de área local son comúnmente usadas en edificios, oficinas o campus ya que su objetivo principal es transferir archivos sin la necesidad de un disco físico, en rangos de datos mucho más rápidos que una conexión de Internet.

2.1.1. Necesidad de una red de área local

Hoy en día, el crecimiento tecnológico ha dado lugar a la evolución de las aplicaciones, generando recursos indispensables dentro de los diferentes campos ya sea científico, educativo, medico, de investigación, etc. Una gran ventaja de las redes de área local reside en que cada día es mayor la cantidad de información que se procesa de una manera local, por lo que surge la necesidad de interconectarlas entre sí para compartir información y recursos.

2.1.2. Características de una red de área local

Una red de área local tiene las siguientes características fundamentales:

- Su índice de error es muy bajo, lo cual implica que es un sistema fiable.
- Trabaja centralmente en un área geográfica limitada.

- Suministra conectividad continua a los servicios locales.
- Maneja la red de forma privada con administración local
- Admite el multiacceso a medios con un alto ancho de banda.
- Acopla dispositivos físicamente adyacentes

2.2. Topología física

Una topología física de red es una representación gráfica de cómo están combinados los host para comunicarse. Existe un número de componentes a tomar en cuenta para determinar cuál topología es la más adecuada para emplearse en las estaciones de trabajo para conectarse entre sí.

Existen otras clases generales de topología utilizadas en redes de área local: topología tipo bus, topología tipo anillo, topología tipo estrella. A partir de estas se derivan otras topologías que reciben su nombre dependiendo del uso que se le quiera dar a la red.

2.2.1. Topología tipo Bus

Consiste en conectar los host a un único canal de comunicación lo cual permite que todos los host reciban la información que se transmite, es decir un host transmite y todos los host restantes lo escuchan, pero solo recibe la información el host al cual va encaminada dicha información. Por otra parte este tipo de topología es muy simple pero presenta varias dificultades, debido que si se envía información a dos host a la vez la red colapsa y se interrumpe la comunicación dejando de funcionar la red.

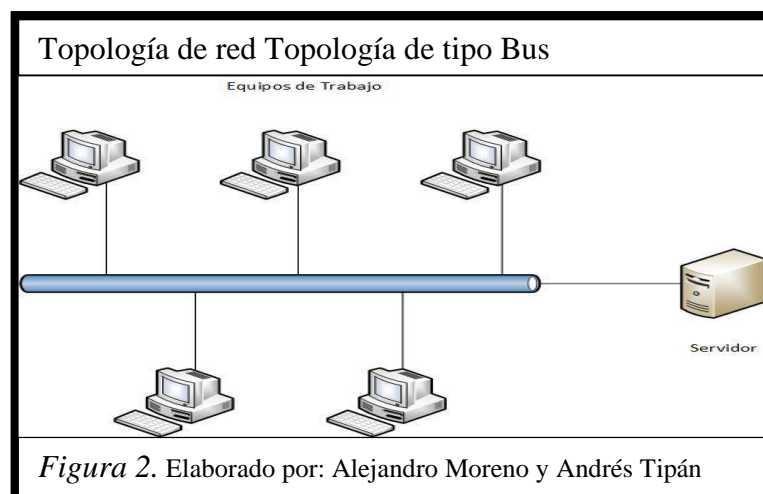
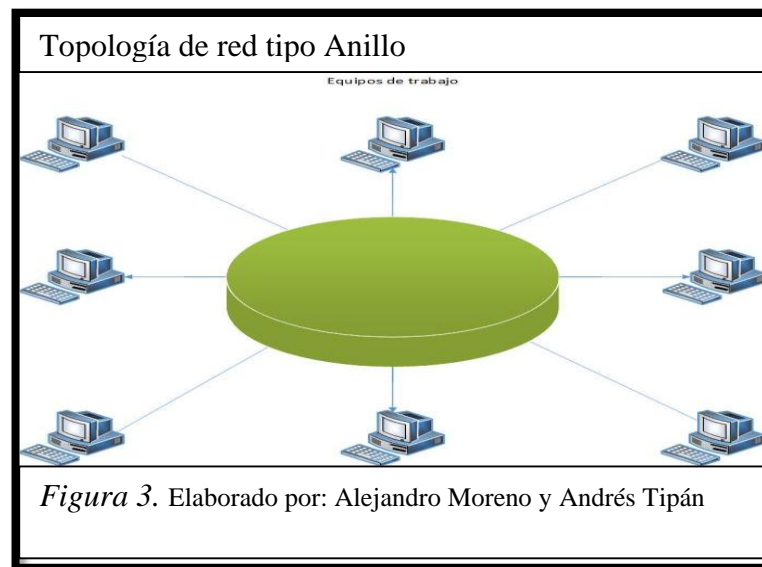


Figura 2. Elaborado por: Alejandro Moreno y Andrés Tipán

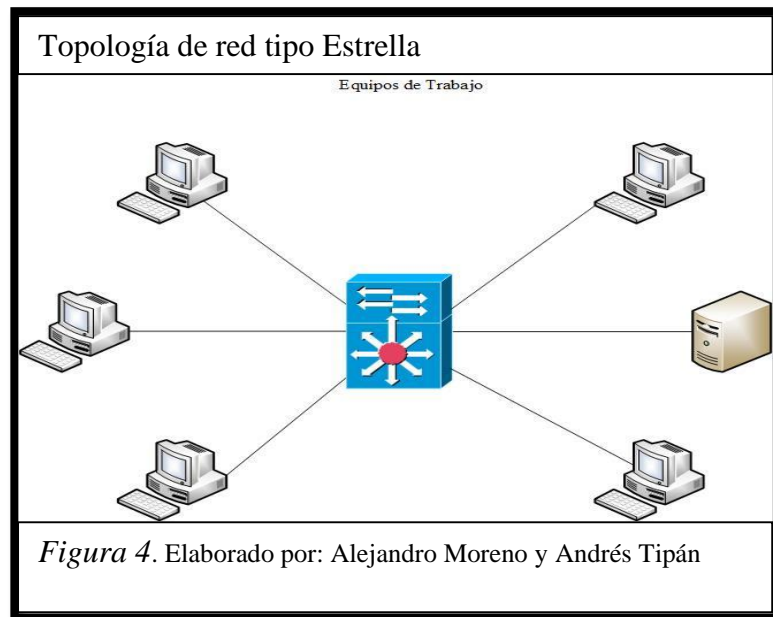
2.2.2. Topología tipo anillo

Consiste en conectar los host en serie formando un anillo cerrado, es decir funciona por un único canal de comunicación es parecida a la lógica de la topología de tipo bus, ya que ambas manejan un solo canal de comunicación. Además en esta topología tipo anillo, el mensaje se trasmite en una sola dirección y es leído por cada uno de los host individualmente y retransmitido al anillo en caso de no ser el destinatario final de los mensajes, esta topología tiene un mensajero central llamado token el cual gira alrededor del anillo constantemente sin parar y en una sola dirección. Posee la misma desventaja que la topología de bus de que si se rompe el cable la red deja de funcionar.



2.2.3. Topología tipo estrella

Se caracteriza por ser una red en la cual sus estaciones de trabajo están conectadas directamente a un único punto central que dirige el tráfico al lugar adecuado. Este tipo de topología se utiliza sobre todo para redes de área local. Cabe mencionar que la Universidad Politécnica Salesiana sede Quito campus Sur posee este tipo de topología en su infraestructura de red.



2.2.4. Topología lógica

Una topología lógica de red es la forma en que los hosts se comunican a través del medio físico, los tipos más usuales de topologías lógicas son:

Broadcast (Ethernet), el cual permite que cada host envíe sus datos hacia los demás host del medio de red.

Transmisión de tokens (Token Ring), el cual transmitir un token eléctrico de forma consecutiva a cada host del medio de red en caso de que el host no tenga ningún dato para enviar, trasmite el token hacia el siguiente host.

2.4. Requerimientos para el diseño de una red

2.4.1. Funcionalidad

La funcionalidad es el conjunto de características que hacen que la red trabaje de manera útil, es decir la red debe proveer conectividad que permita cumplir con los requerimientos de los usuarios y satisfacer las necesidades para el acceso a las aplicaciones con una velocidad y confiabilidad razonables.

2.4.2. Escalabilidad

La escalabilidad es la capacidad que tiene la red para expandirse rápidamente y adaptarse a cambios sin perder calidad en los servicios ofrecidos. La escalabilidad

tiene un factor importante en el crecimiento de la red. Si tiene como objetivo crecer en el número de usuarios tiene que mantener su rendimiento actual.

2.4.3. Adaptabilidad

La adaptabilidad es la capacidad para ajustarse a los cambios en la red, es decir, en el diseño de la red se debe tomar en cuenta las tecnologías futuras y equipos que permitan tener flexibilidad, para poder aumentar de tamaño sin alterar el rendimiento de la red.

2.4.4. Redundancia

La redundancia permite que las redes sean tolerantes a las fallas y puedan recuperarse rápidamente, en caso de que se produzcan dichas fallas, los dispositivos, servicios o conexiones redundantes puedan realizar el trabajo de aquellos en los que se produce la falla.

2.4.5. Facilidad de administración

La red debe ser eficiente, para administrar su funcionamiento y monitoreo con el objetivo de asegurar una estabilidad en la red y que facilite un servicio rápido que permita maximizar el trabajo.

2.5. Calidad de servicio (QoS)

Una red de comunicaciones es un factor importante en cualquier organización exitosa, debido a que estas redes transportan una gran cantidad de aplicaciones y datos. Por lo tanto las redes deben proporcionar servicios seguros y garantizados.

La Calidad de servicio QoS (Quality of Service), es el conjunto de técnicas para manejar los recursos de red y garantizar un valor límite de algunos de los parámetros de QoS para lograr una solución exitosa.

2.5.1. Parámetros de calidad de servicio

Tabla 1. *Parámetros de calidad de servicio QoS*

Parámetro	Unidades	Definición
Ancho de Banda	bps	Indica la máxima cantidad de datos que se puede enviar a través de una conexión de red.
Retardo o latencia	ms	El tiempo medio que tarda un dato en estar disponible desde que se realiza su petición.
Variación de retardo (Jitter)	ms	La variación que se puede producir en retardo entre paquetes de la misma comunicación.
Tasa de pérdidas (loss rate)	%	La proporción de paquetes perdidos respecto de los enviados

Nota. QoS=calidad de servicio

Elaborado por: Alejandro Moreno y Andrés Tipán

2.5.2. Requerimientos de calidad de servicio de las aplicaciones

Tabla 2. *Requerimientos de calidad de servicios*

Tipo de aplicación	Ancho de banda	Retardo	Jitter	Tasa de pérdidas
Interactivo (telnet, www)	Bajo	Bajo	Medio/Alto	Media
Batch (e-mail, ftp)	Alto	Alto	Alto	Alta
Telefonía	Bajo	Bajo	Bajo	Baja
Video interactivo	Alto	Bajo	Bajo	Baja
Video unidireccional (streaming)	Alto	Medio/Alto	Bajo	Baja
Frágil (ej. emulación de circuitos)	Bajo	Bajo	Medio/Alto	Nula

Nota. (TANENBAUM, 2003, pág. 397)

Elaborado por: Alejandro Moreno y Andrés Tipán

2.5.3. Servicios QoS

Incontable tecnología ha sido desarrollada hoy en día para acceder a las redes de comunicaciones, por tal motivo QoS tiene un papel importante en el soporte de nuevas aplicaciones con demanda de servicios más precisos tales como:

- Enrutamiento selectivo
- Control de tráfico
- Acceso remoto a redes de comunicaciones
- Administración de ancho de banda
- Balanceo de carga

2.5.3.1. Enrutamiento selectivo

Debe ser capaz de manejar los cambios que provocan ciertos servicios de uso regular, como la transferencia de archivos, colas de impresión, correos pesados, ya que estos servicios pueden quitar ancho de banda disponible y causan congestión en las redes.

2.5.3.2. Control de tráfico

Es el proceso que permite identificar el tráfico existente en la red y dividirlo en diferentes categorías, según el tipo de servicio se asigna a una clase de tráfico específico. En función a la clasificación del tráfico es posible optar por un descarte selectivo de paquetes, para resguardar el tráfico de las clases de alta prioridad.

2.5.3.3. Acceso remoto a redes de comunicaciones

Mediante el control de acceso remoto a redes de comunicaciones se puede acceder a recursos que ofrece uno más host, como transferencia de archivos, dispositivos periféricos, configuraciones, etc. Además se debe contar con un sistema de seguridad confiable para garantizar que la red está protegida contra instrucciones maliciosas.

2.5.3.4. Administración de ancho de banda

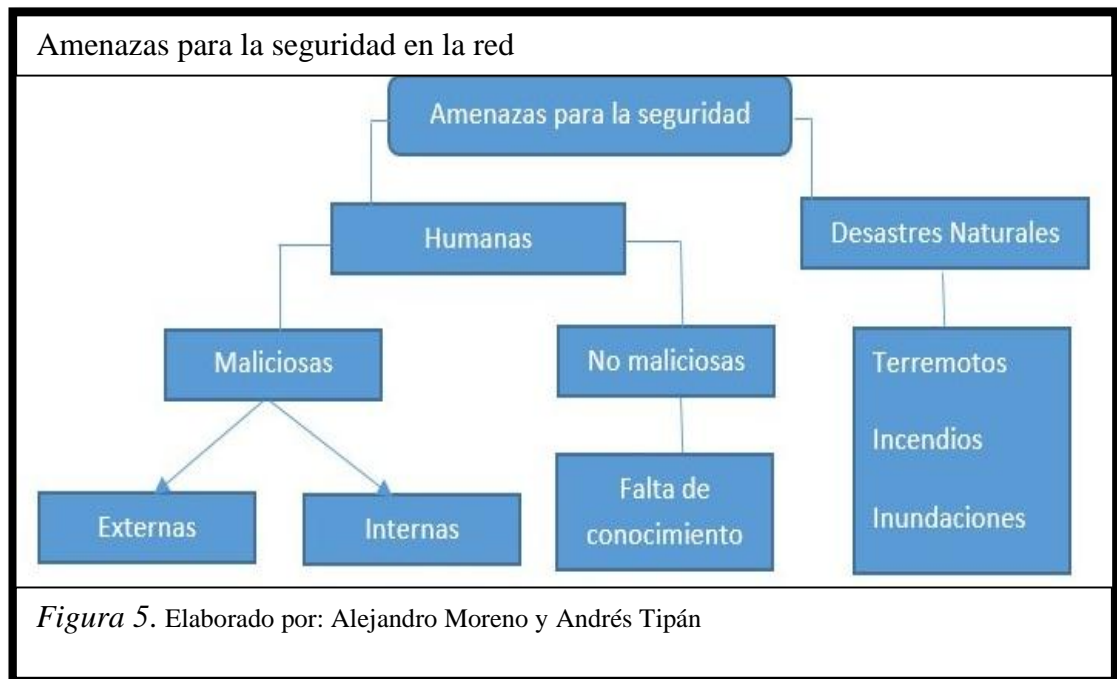
Mediante el servicio de QoS se intenta asegurar el flujo de datos en la red, estableciendo prioridades del ancho de banda máximo del total disponible, es decir administrar adecuadamente el ancho de banda para cada servicio y obtener el máximo provecho de ellas.

2.5.3.5. Balanceo de carga

Permite una mejor utilización de los recursos de la red, estableciendo políticas de enrutamiento de tráfico definidas por el administrador de la red permite el balanceo de la carga en horas pico, para facilitar el intercambio de tareas y la carga de trabajo entre los distintos host de la red.

2.6. Seguridad en las redes

El concepto de seguridad en redes surge como resultado de la necesidad de reducir riesgos debido a las amenazas sobre la red, una amenaza es todo aquello que puede vulnerar la seguridad de un entorno de sistemas de información.



Para lograr un sistema considerado seguro es preciso abordar los siguientes aspectos que se mencionan a continuación:

- Confidencialidad: Asegurar que nadie más lo vea
- Integridad: Garantizar que nadie más lo cambie
- Autenticación: Afirmar quien dice ser

Esto con la necesidad de impedir que usuarios no autorizados accedan a información no permitida evitando daños y minimizando riesgos, concernientes a la seguridad. También dependiendo de las amenazas o peligros, la seguridad se divide en seguridad física y seguridad lógica.

2.6.1. Seguridad tipo física

La seguridad física de los sistemas informáticos consiste en la protección de instalaciones y lo que contengan mediante barreras físicas que permitan detectar y defenderse de ataques con el objetivo de evitar o minimizar daños.

La seguridad física pretende conseguir los siguientes objetivos:

- Orientada a resolver las amenazas ocasionadas tanto por el hombre como por la naturaleza.
- Implementar blindajes contra robos.
- Control de acceso a los lugares donde se sitúan los host.
- Resguardar la seguridad de las personas y organizaciones.
- Reducir las pérdidas de datos a un mínimo nivel aceptable y asegurar la adecuada recuperación.

2.6.2. Seguridad tipo lógica

La seguridad lógica de los sistemas informáticos consiste en procedimientos adecuados del sistema para proteger el acceso a los datos y que la información solo pueda ser vista por aquellas personas autorizadas para hacerlo.

La seguridad lógica pretende conseguir los siguientes objetivos:

- Confirmar que los datos transmitidos sean recibidos sólo por el destinatario al cual ha sido enviada y que la información recibida sea la misma que la transmitida.
- Verificar que se estén utilizando los archivos y programas correctos.
- Restringir el acceso a los archivos y programas para que no puedan ser modificados.

2.6.3. Niveles de Seguridad Informática

Los niveles de seguridad informática representan los tipos de seguridad del sistema operativo y se especifican desde el mínimo nivel de seguridad al máximo. Estos niveles han sido la base del progreso de estándares europeos (ITSEC/ITSEM) e internacionales (ISO/IEC).

- Nivel D (protección mínima), está reservada para sistemas que no cumplen con ninguna especificación de seguridad.
- Nivel C1 (protección discrecional), se pide identificación de usuarios que permite el acceso a diferente información, cada usuario puede manejar su información privada.
- Nivel C2 (protección de acceso controlado), cuenta con características adicionales que crean un ambiente de acceso controlado.
- Nivel B1 (seguridad etiquetada), soporta seguridad multinivel, como la secreta y ultra secreta.
- Nivel B2 (protección estructurada), es la primera que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel inferior.
- Nivel B3 (dominios de seguridad), refuerza a los dominios con la instalación de hardware.
- Nivel A (protección verificada), es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales.

Esto con el objetivo de mantener la privacidad e integridad de la información que se maneja a través de las redes de comunicaciones. (Borguello, 2014)

2.7. Universidad Politécnica Salesiana sede Quito Campus Sur.





2.7.1. Ubicación.

La Universidad Politécnica Salesiana Campus Sur se encuentra localizada al Sur de la ciudad de Quito en la Av. Rumichaca y Av. Morán Valverde s/n, y está conformada de 8 bloques identificados como: Bloque A, Bloque B, Bloque C, Bloque D, Bloque E, Bloque F, Bloque H, Bloque G, este último bloque recientemente construido y por entregar.

2.7.1.1 Bloque A

El edificio Bloque A está conformado por: una planta baja y 5 pisos, en el cual los cuartos de comunicaciones se encuentran ubicados en el cuarto piso, quinto piso y en la planta baja ubicados en la sala de profesores y en la biblioteca, estas áreas están distribuidas según los siguientes usos arquitectónicos.

Tabla 3. Usos arquitectónicos

Símbolos	Nombres
	BACKBONE
	SDF o MDF
	CABLEADO HORIZONTAL
	ENTRADA o SALIDA

Nota. MDF=marco de distribución principal

Elaborado por: Alejandro Moreno y Andrés Tipán

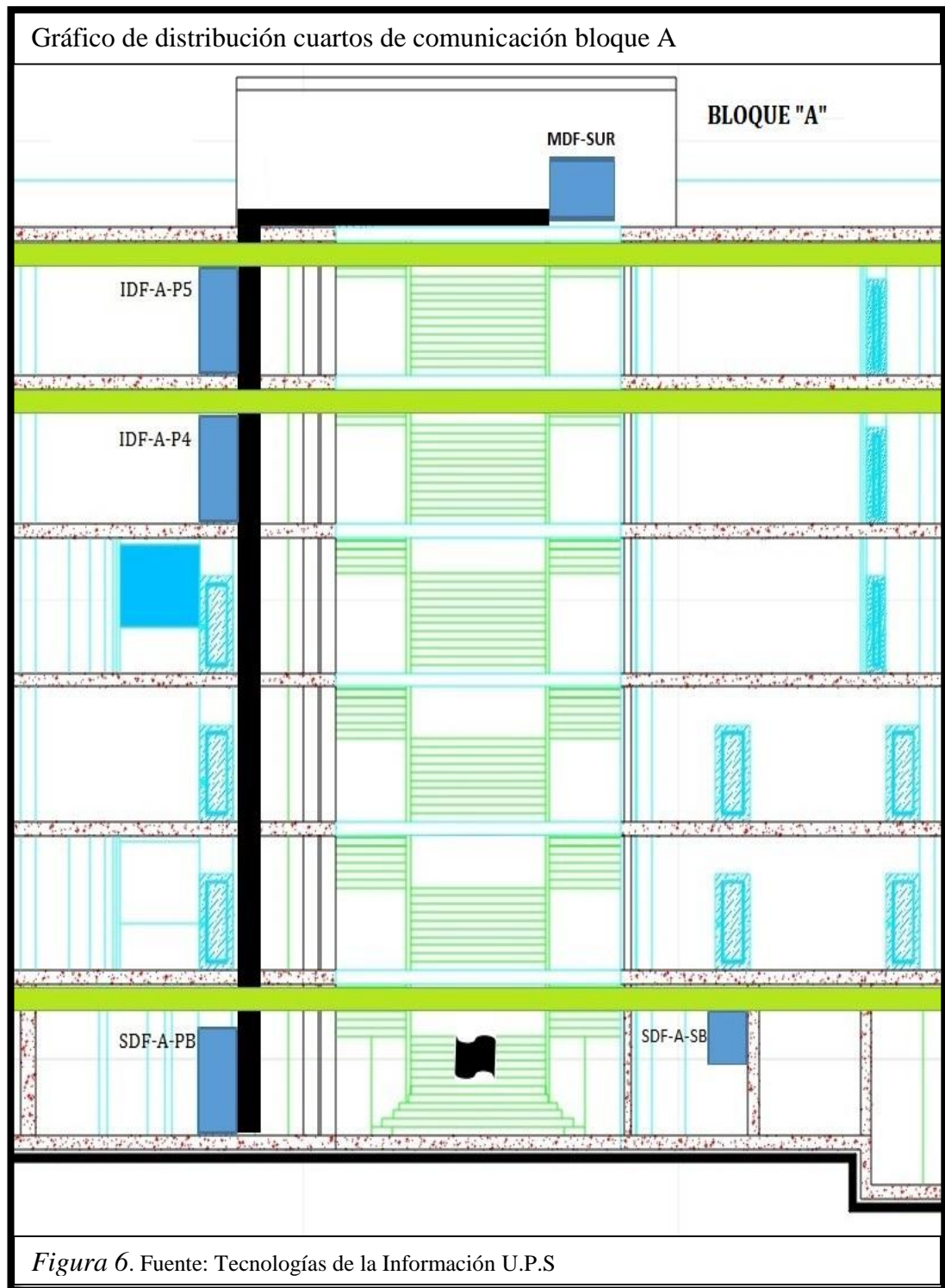
A continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque A dónde:

Tabla 4. Sistema de distribución MDF, SDF e IDF en el bloque A

MDF, SDF e IDF	Departamentos bloque A
MDF-A	Centro de cómputo, informática
SDF-A-PB SDF-A-PB-24p	Financiero, administrativo, vicerrectorado
SDF-A-SB	Biblioteca
IDF-A-P4, P5	CECASIS

Nota. IDF=distribuidor intermedio

Elaborado por: Alejandro Moreno y Andrés Tipán



En el data center de la Universidad Politécnica Salesiana se encuentran instalados 5 armarios de rack de piso de 42 unidades de rack (UR) cada uno, en estos se encuentran instalados los equipos del núcleo de la red (core) de la infraestructura de red del campus y los servidores locales.

El backbone desde el MDF a sus IDFs y SDFs emplea fibra óptica multimodo (62.5/125 micrones), para una longitud de onda de 1300 nm. Un ancho de banda 500 MHz/Km y atenuación máxima 1.5 dB/Km a una velocidad de transmisión de 1 Gbps que atraviesa un ducto desde el quinto a la planta baja pasando por los cuartos de telecomunicaciones que cuentan con 2 racks de piso de 42 UR en el quinto y cuarto piso en la planta baja cuentan con un rack de piso de 42 UR e incluso biblioteca cuenta con un rack de pared de 12 UR, en el cableado horizontal la velocidad de transmisión es de 100Mbps utilizando UTP desde los cuartos de telecomunicaciones hacia los host en los laboratorios del CECASIS, sala de profesores, dirección administrativa, tesorería, CIMA, Sala de video conferencia.

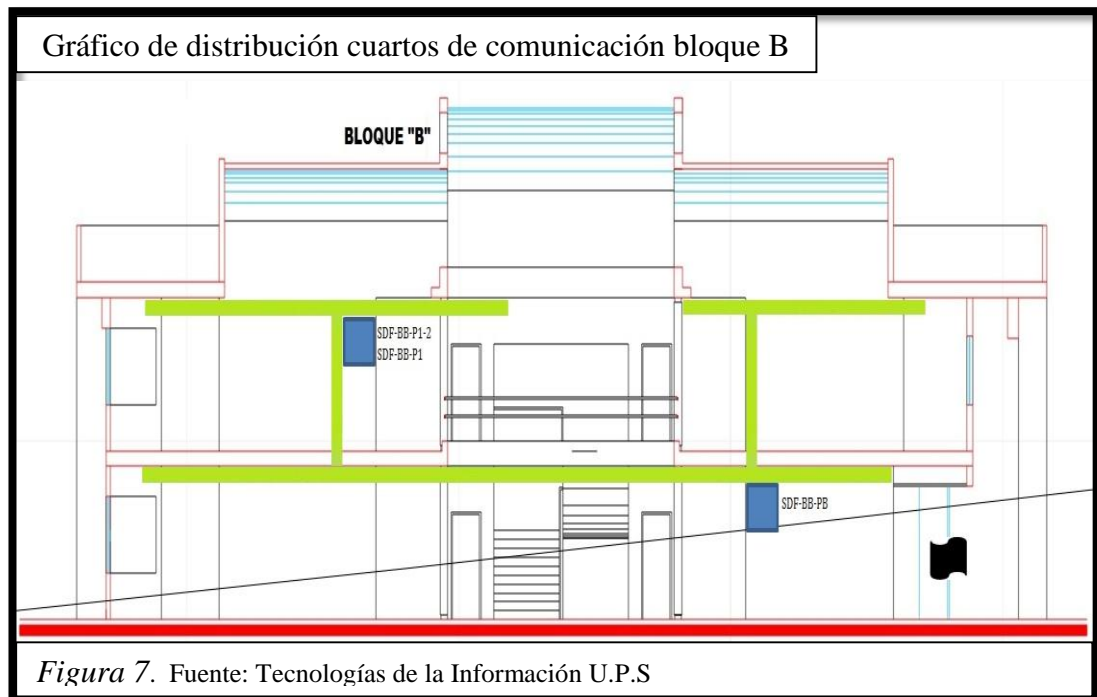
2.7.1.2 Bloque B

El edificio bloque B está conformado por: una planta baja y un piso donde se encuentra colocado un rack de pared situado en la sala de profesores en el primer piso, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque B dónde:

Tabla 5. *Sistema de distribución SDFs en el bloque B*

SDFs	Departamentos bloque B
SDF-BB-P1-2	secretaria, direcciones de carrera
SDF-BF-P1	sala profesores
SDF-BB-PB	Bienestar estudiantil

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



Este bloque posee dos rack de pared de 12 UR el MDF se conecta al SDF del primer piso por medio de fibra óptica a una velocidad de transmisión de 1Gbps y este al SDF de planta baja por medio de UTP a una velocidad de transmisión de 100Mbps, desde el primer piso el cableado horizontal da servicio a: Sala de profesores 1, direcciones de carrera, secretaria, el de planta baja a: Sala de profesores 2, bienestar estudiantil.

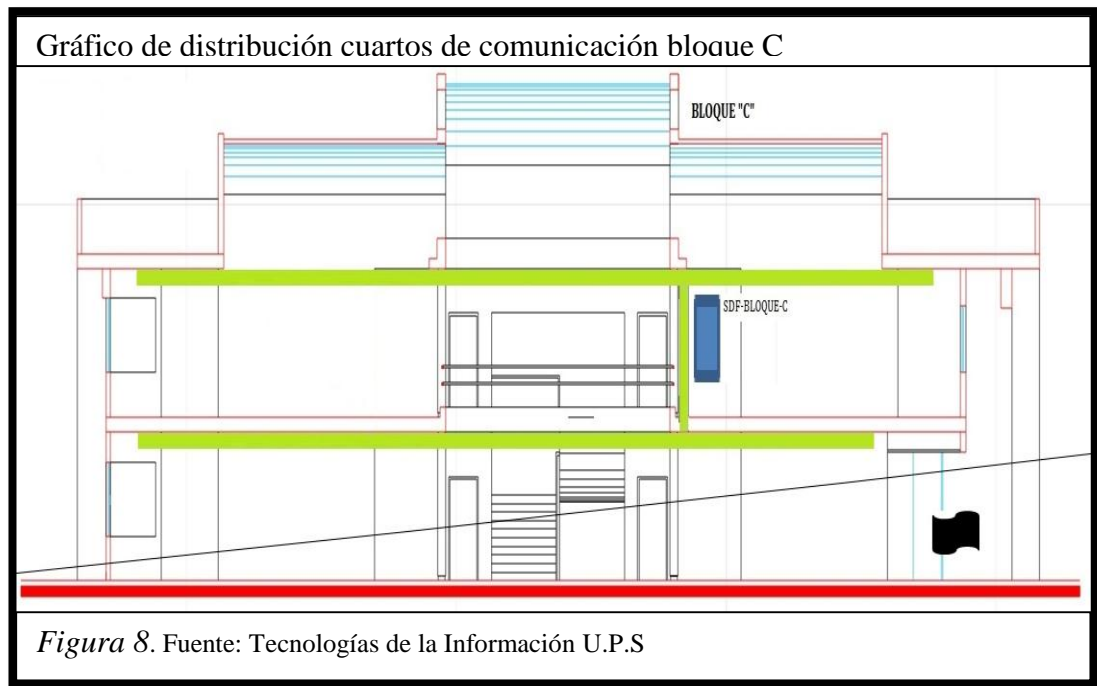
2.7.1.3 Bloque C

El edificio bloque C está conformado por: una planta baja y un piso donde se encuentra colocado un rack de pared situado en el departamento de idiomas en el segundo piso, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque C dónde:

Tabla 6. *Sistema de distribución SDF en el bloque C*

SDF	Departamentos bloque C
SDF-C-P1	departamento de idiomas, laboratorio de idiomas, laboratorios de electrónica

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



Este bloque posee un rack de pared de 25 UR el MDF se conecta al SDF por medio de fibra óptica a una velocidad de transmisión de 1Gbps está ubicado en el departamento de idiomas, el cableado horizontal desde aquí da servicio por medio de UTP a una velocidad de transmisión de 100Mbps a todos los laboratorios de electrónica y al mismo departamento de idiomas.

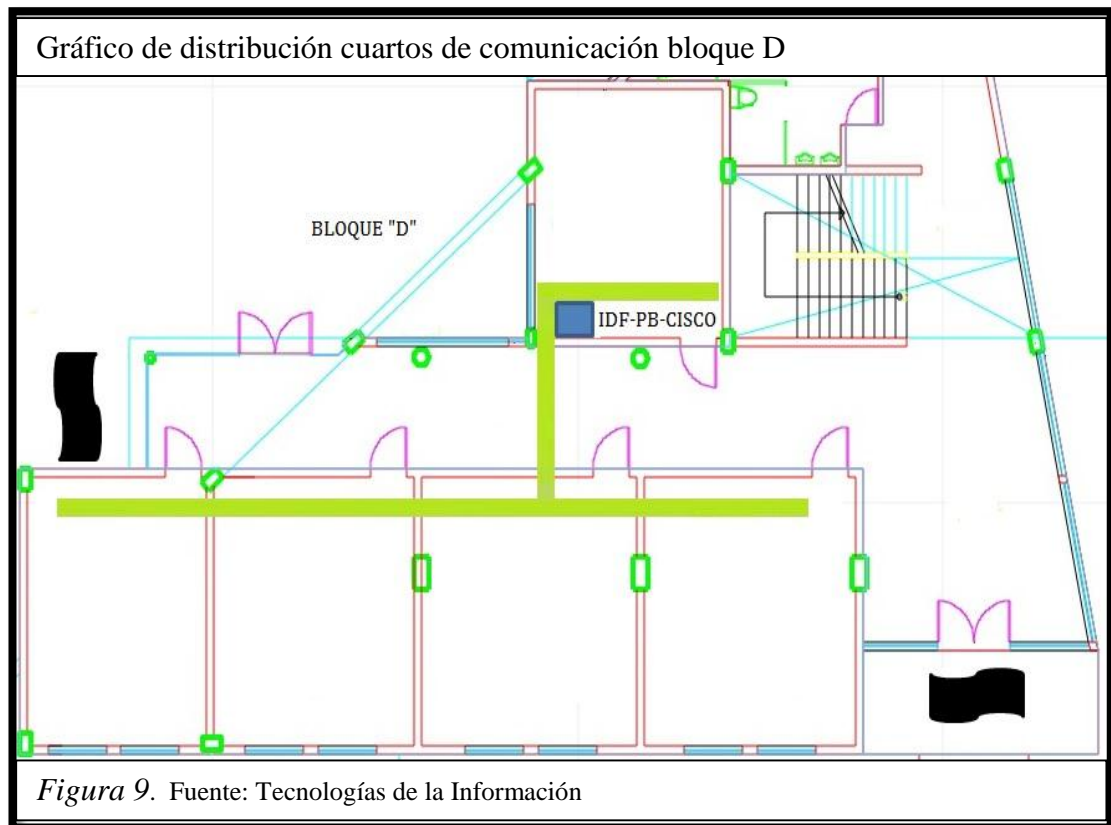
2.7.1.4 Bloque D

El edificio Bloque D está conformado por: una planta baja y un piso donde se encuentra colocado un rack de pared situado en el laboratorio 3 de CISCO en el primer piso, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque D dónde:

Tabla 7. Sistema de distribución SDF en el bloque D

SDF	Departamentos bloque D
SDF-D-PB	CISCO, SUN, microsoft, auditorio

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



Este bloque posee un rack de pared de 12 UR el MDF se conecta al SDF por medio de fibra óptica a una velocidad de transmisión de 1Gbps está ubicado en el laboratorio 3 de CISCO en la planta baja, el cableado horizontal desde aquí da servicio por medio de UTP a una velocidad de transmisión de 100Mbps a todos los laboratorios de CISCO, BLADE, SUN, y Auditorio.

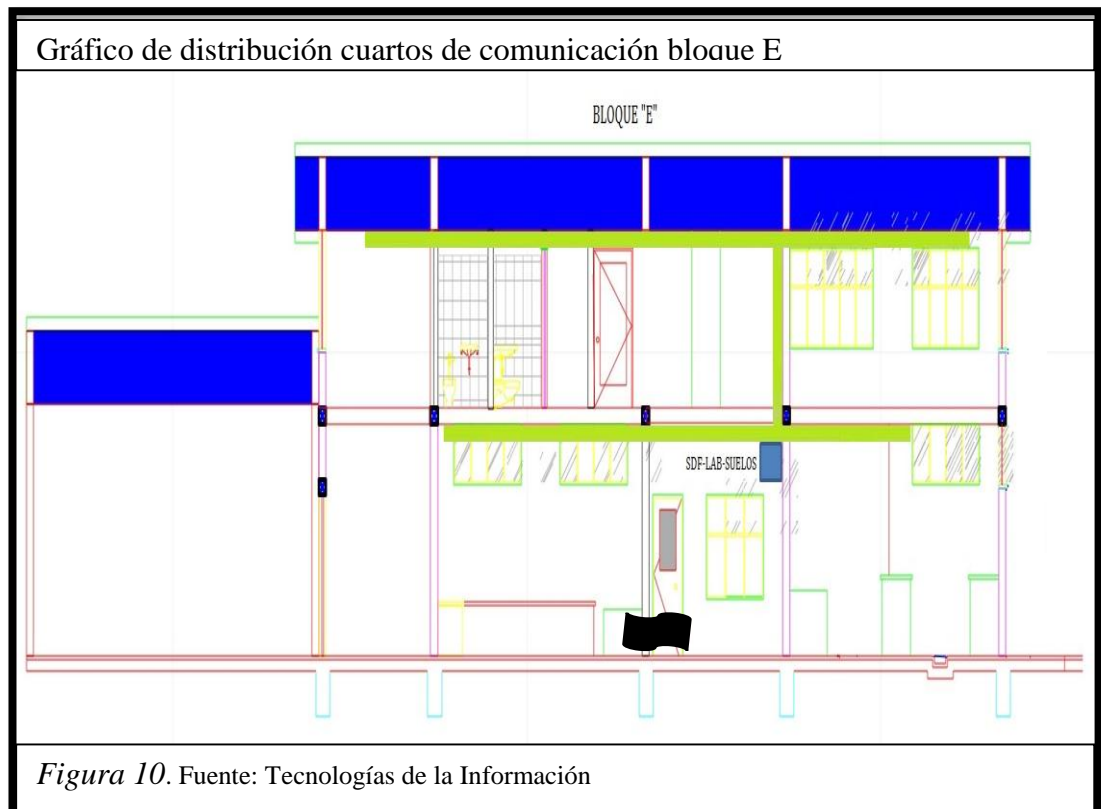
2.7.1.5 Bloque E

El edificio Bloque E está conformado por: un piso donde se encuentra colocado un rack de pared situado en el laboratorio de suelos en la planta baja, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque E dónde:

Tabla 8. *Sistema de distribución SDF en el bloque E*

SDF	Departamentos bloque E
SDF-E-PB	laboratorio de civil

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



Este bloque posee un rack de pared de 6 UR se conecta al SDF del bloque C por medio de fibra óptica a una velocidad de transmisión de 1Gbps, está ubicado en el laboratorio de suelos en la planta baja, el cableado horizontal desde aquí da servicio por medio de UTP a una velocidad de transmisión de 100Mbps a todos los laboratorios y oficinas en este bloque.

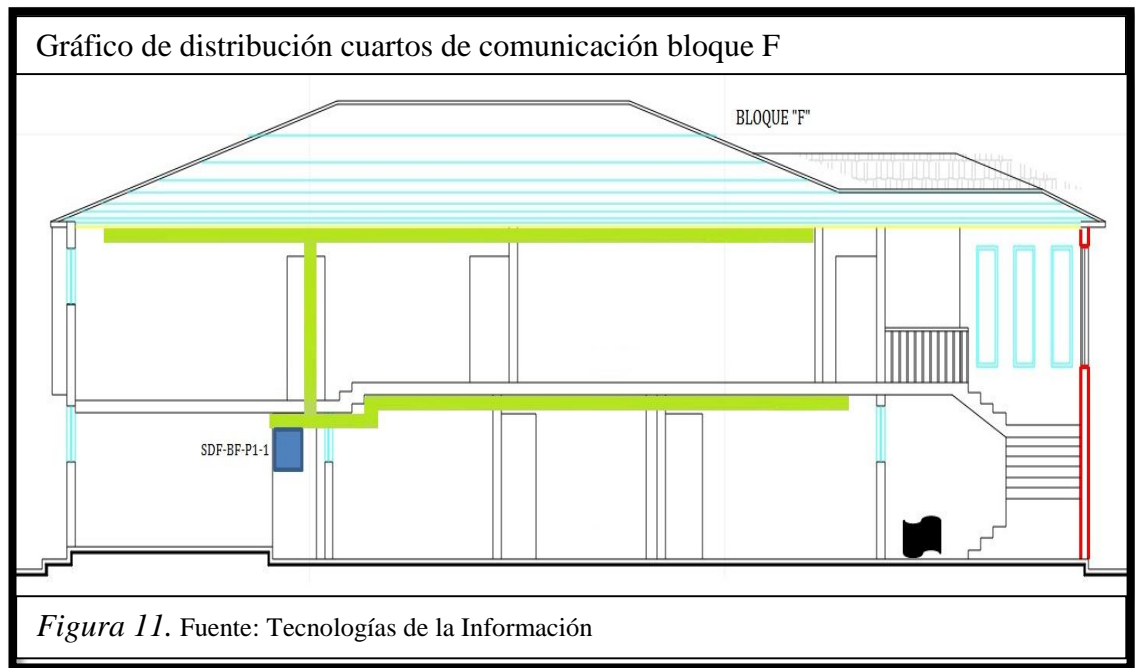
2.7.1.6 Bloque F

El edificio Bloque F está conformado por: una planta baja y un piso donde se encuentra colocado un rack de pared situado en el departamento de ambiental planta baja, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque F dónde:

Tabla 9. *Sistema de distribución SDF en el bloque F*

SDF	Departamentos bloque F
SDF-F-PB	laboratorios de ambiental

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



Este bloque posee un rack de pared de 12 UR se conecta al SDF del bloque C por medio de fibra óptica a una velocidad de transmisión de 1Gbps, está ubicado en el laboratorio de ambiental en la planta baja, el cableado horizontal desde aquí da servicio por medio de UTP a una velocidad de transmisión de 100Mbps a todos los laboratorios, oficinas y sala de profesores en este bloque.

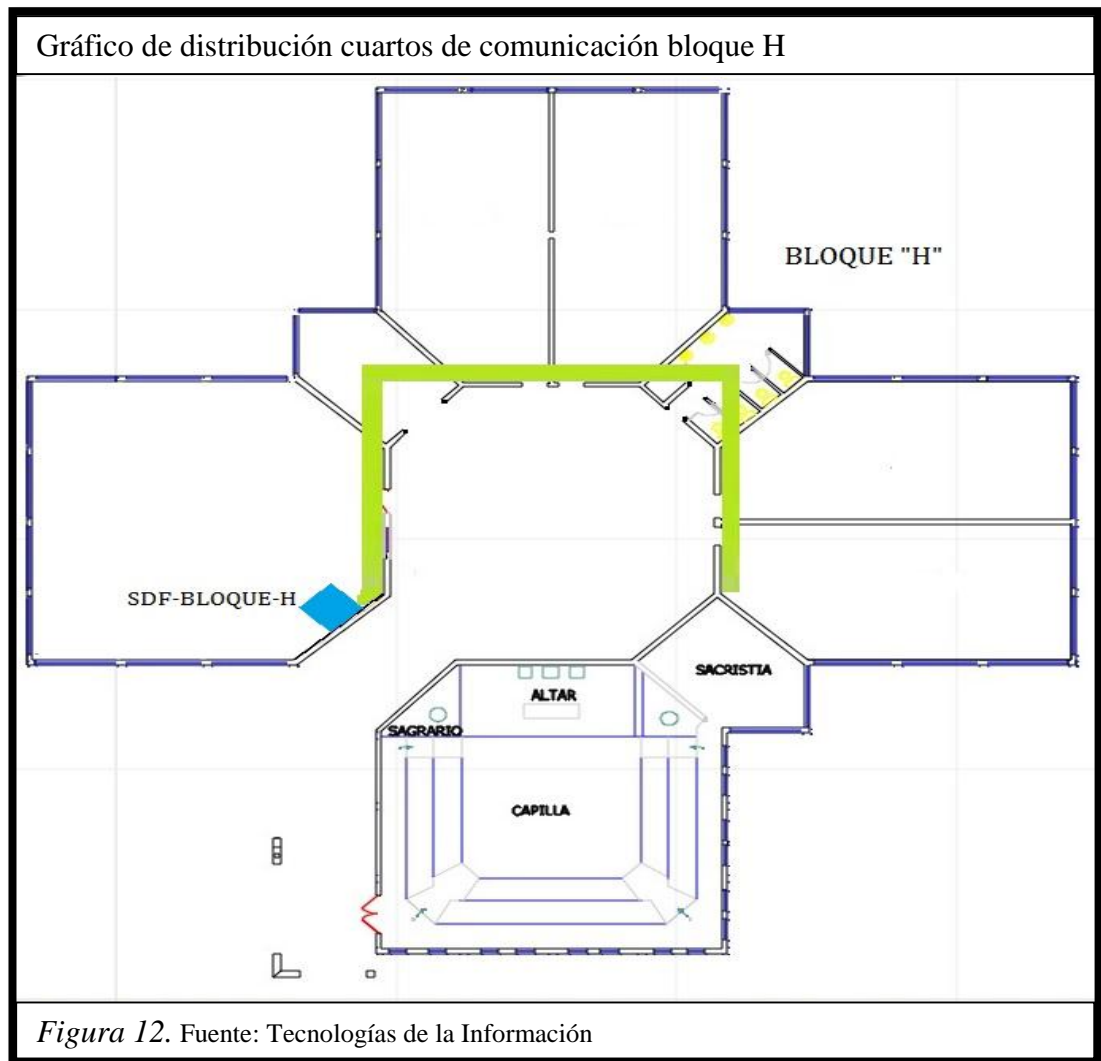
2.7.1.7 Bloque H

El edificio Bloque H está conformado por: una planta baja y un piso donde se encuentra colocado un rack de pared situado en el departamento de pastoral en el primer piso, a continuación se detalla la simbología utilizada en la distribución de los cuartos de comunicación bloque H dónde:

Tabla 10. Sistema de distribución SDF en el bloque H

SDF	Departamentos bloque H
SDF-H-PB	pastoral

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán



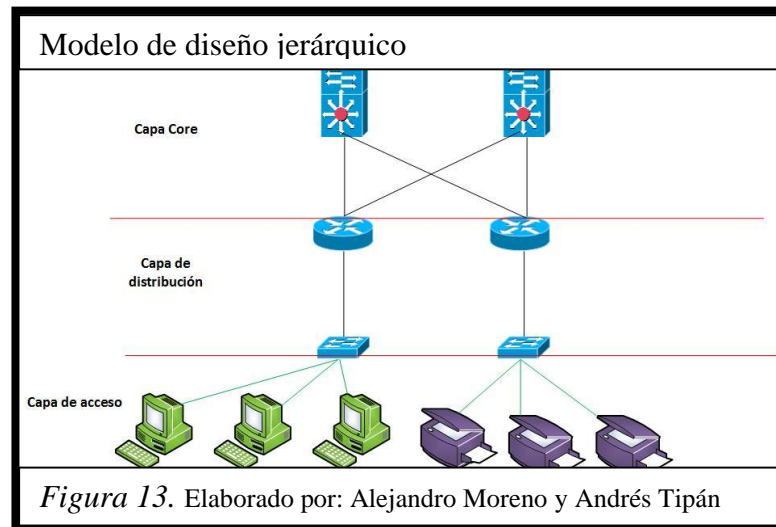
Este bloque posee un rack de pared de 12 UR el MDF se conecta al SDF por medio de fibra óptica a una velocidad de transmisión de 1Gbps, está ubicado en el departamento de pastoral, el cableado horizontal desde aquí da servicio por medio de UTP a una velocidad de transmisión de 100Mbps a todo el bloque.

2.7.1.8 Bloque G

El edificio Bloque G recientemente construido y por entregarse, actualmente se están realizando arreglos por lo que no se encuentra determinado planos de cuarto de comunicaciones.

2.8. Diseño de red jerárquico

El diseño actual de la infraestructura de networking en la Universidad Salesiana Campus Sur sede Quito está establecida de acuerdo a la función que desempeña cada uno de los equipos dentro de las capas de diseño de networking que son: core, distribución y acceso, actualmente en la infraestructura existe un modelo colapsado core-distribución.



La capa core se encarga de proporcionar transporte óptimo entre sitios es decir, desviar el tráfico lo más rápido posible hacia los servidores apropiados

La capa distribución proporciona conectividad basada en una determinada política es decir, determina cuándo y cómo los paquetes pueden acceder a los servicios principales de la red.

La capa de acceso también se le conoce como capa de puesto de trabajo porque es el punto en el que cada usuario se conecta a la red.

2.9. Análisis de la situación actual e Infraestructura de la red

Con el objetivo de diseñar una topología de red de alto desempeño para la Universidad Politécnica Salesiana Sede Quito campus Sur, se realizará un estudio a través del cual se logre identificar las debilidades y limitaciones que posee la actual infraestructura de red.

2.9.1 Capa de Core y distribución

La actual infraestructura cuenta con un MDF(Main Distribution Facility) un switch cisco WS-C6506-E con el nombre MDF-SUR este es un switch multicapa el cual cuenta con 48 interfaces para SFP's (transceivers) de fibra óptica y con 48 interfaces GigabitEthernet para UTP, este se encuentra ubicado en el quinto piso del bloque A, de la misma manera en este equipo se encuentran creadas la redes virtuales (VLANs), desde aquí se brinda los servicios de Backbone (Núcleo de la red) conectándose a los IDFs y SDFs dentro del campus sur y se conectan los routers de frontera para salida de datos hacia otros campus e Internet.

2.9.2. Capa distribución y acceso

En estas capas los switch de distribución son cisco WS-C2960 de 48 puertos los IDF (Intermediate Distribution Facility) se encuentran en el bloque D en el laboratorio de CISCO con el nombre IDF-PB-CISCO y en el 4to y 5to piso del bloque A con los nombres IDF-A-P4, IDF-A-P5 y los de acceso son los SDF (Sub-Distribution Facility).

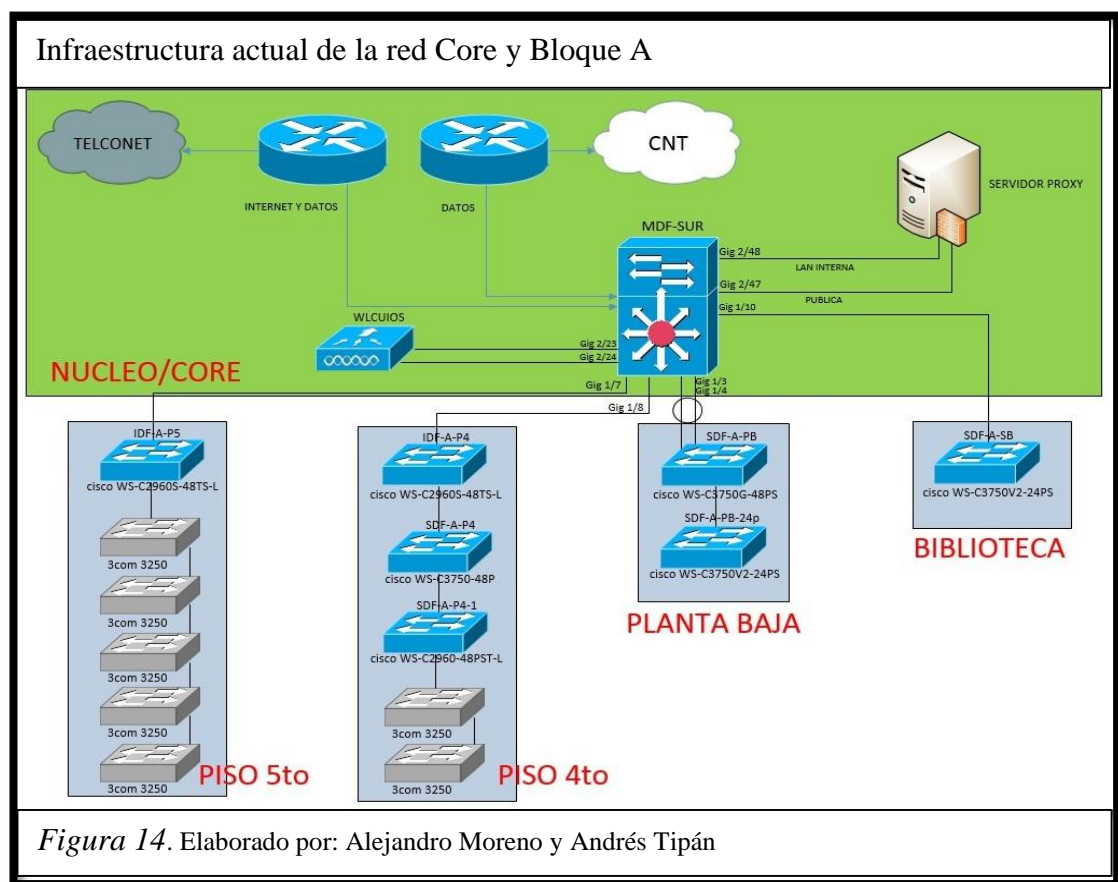
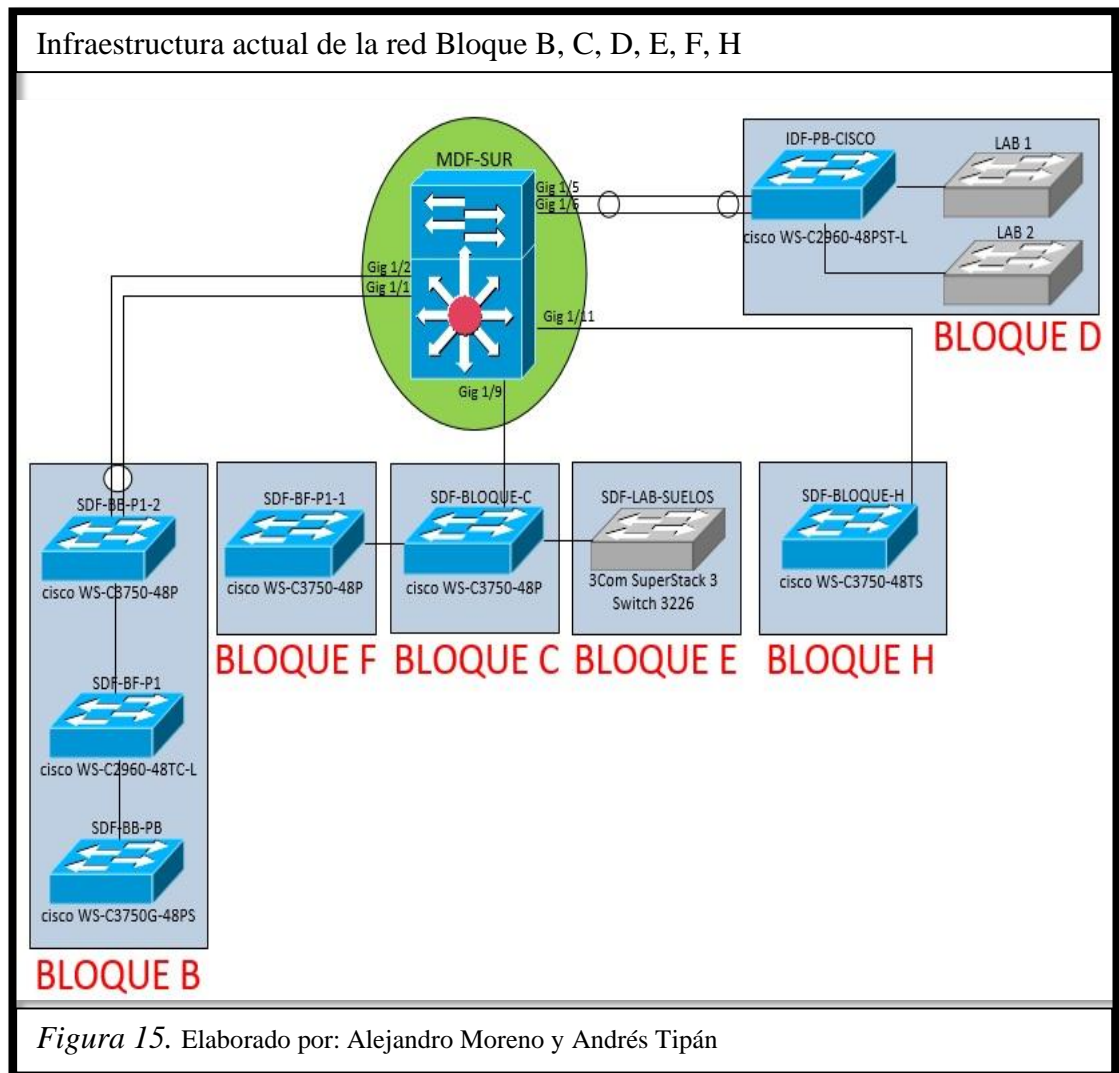


Figura 14. Elaborado por: Alejandro Moreno y Andrés Tipán



La topología de conectividad que se utiliza en esta red, es de tipo estrella extendida, la propia que está conformada en su mayoría por switch's de Capa 3, ya que utilizan VLANs para una mejor organización de las estaciones para usuarios.

Tabla 11: *Sistema de distribución SDF campus sur*

CECASIS CUARTO PISO “BLOQUE A”		
IDF-A-P4	WS-C2960	48P-4P_FO
SDF-A-P4	CISCO, CATALYST 3750 POE	48P-10/100Mbps 4P-FO 48
SDF-A-P4-1	CISCO CATALYST 2960 POE	48P-10/100Mbps 4P-FO

	3COM 3250 3COM 3250	48P 10/100 48P 10/100
CECASIS QUINTO PISO”BLOQUE A”.		
IDF-A-P5	CISCOWS-C2960	48P-4P_FO
	3COM 3250	48P 10/100
	3COM 3250	48P 10/100
	3COM 3250	48P 10/100
	3COM 3250	48P 10/100
SALA DE PROFESORES “BLOQUE A”.		
SDF-A-PB	CISCO CATALYST 3750G POE cisco WS- C3750V2-24PS	48P_4P-FO 24P
BIBLIOTECA “BLOQUE A”.		
SDF-A-SB	CISCO CATALYST 3750 V2 POE	24P_4P-FO
SECRETARIA “BLOQUE B”.		
SDF-BB-P1-2	CISCO CATALYST 3750 POE	48P 4P-FO
SDF-BB-P1	CISCOWS-C2960	48P 4P-FO
SDF-BB-PB	CISCO CATALYST 3750G POE	48P_4P-FO
LABORATORIOS DE ELECTRÓNICA “BLOQUE C”.		
SDF-BLOQUE-C	CATALYST 3750 POE	48P 4P-FO
LABORATORIOS DE CISCO “BLOQUE D”		
IDF-PB-CISCO	CISCOWS-C2960	48P_ 4P-FO

LABORATORIO DE SUELOS”BLOQUE E”.		
SDF-LAB-SUELOS	3COM 3226	24P
AMBIENTAL”BLOQUE F”.		
SDF-BF-P1-1	CATALYST 3750 POE	48P 4P-FO
PASTORAL”BLOQUE H”.		
SDF-BLOQUE-H	CATALYST 3750	48P_4P-FO

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

2.9.2.1 Redes virtuales en el campus.

Actualmente el campus dispone de 32 redes virtuales o VLAN enrutadas en el core cuya distribución se encuentran en la figura 16 y direccionamiento en la tabla 12, separando los segmentos lógicos de la red y permitiendo dar acceso de Internet en cualquier punto del campus.

Tabla 12. *Sistema de distribución redes virtuales campus sur*

VLAN	NOMBRE	DIRECCIÓN IP GATEWAY	MASCARA
Vlan1	Default	172.17.32.1	255.255.255.0=24
Vlan2	DMZ	172.17.33.254	255.255.255.0=24
Vlan3	ADMINISTRATIVA	172.17.34.254	255.255.255.0=24
Vlan4	ESTUDIANTES	172.17.37.253	255.255.254.0=23
Vlan5	CISCO	172.17.39.254	255.255.254.0=23
Vlan6	SUN	172.17.40.254	255.255.255.0=24
Vlan7	SALAPROF	172.17.131.254	255.255.254.0=23
Vlan8	SALA-INTERNET	172.17.41.126	255.255.255.192=26
Vlan9	MICROSOFT	172.17.43.254	255.255.255.0=24
Vlan10	WIRELESS	172.17.211.254	255.255.252.0=22

Vlan11	IPT	172.17.45.254	255.255.255.0=24
Vlan12	SALA-CECASIS	172.17.41.190	255.255.255.192=26
Vlan13	VLAN-VIDEO	172.17.41.254	255.255.255.192=26
Vlan14	VLAN-HP	172.17.42.254	255.255.255.128=25
Vlan15	ELECTRONICA	172.17.47.254	255.255.255.0=24
Vlan16	VLAN-TELCONET		
Vlan17	WLAN-IPCAM-CECASIS		
Vlan18	WLAN-IPCAM-ELECTRONICA	172.17.128.126	255.255.255.192=26
Vlan19	INVESTIGACION	172.17.128.62	255.255.255.192=26
Vlan20	INTERNET-LOCAL	172.17.128.190	255.255.255.192=26
Vlan21	CIMA-SRV	172.17.128.254	255.255.255.192=26
Vlan22	RUI	172.17.129.62	255.255.255.192=26
Vlan23	LAB-IDIOMAS	172.17.132.254	255.255.255.0=24
Vlan24	WLAN-SUR	172.17.133.254	255.255.255.0=24
Vlan25	CAMARAS-IP-UIOS	172.17.134.126	255.255.255.128=25
Vlan26	EVENTOS	172.17.135.254	255.255.255.0=24
Vlan27	###LAB-FISICA-UIO###	172.17.136.126	255.255.255.128=25
Vlan28	INTERNET-CECASIS	172.17.136.254	255.255.255.128=25
Vlan29	GIETEC	172.17.140.254	255.255.255.0=24
Vlan30	DOCENTES-TIEMP-COMP	172.17.143.254	255.255.254.0=23
Vlan31	EDUROAM	172.17.145.254	255.255.254.0=23
Vlan138	CAMARAS-APS	172.17.139.254	255.255.255.0=24

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Distribución de VLAN

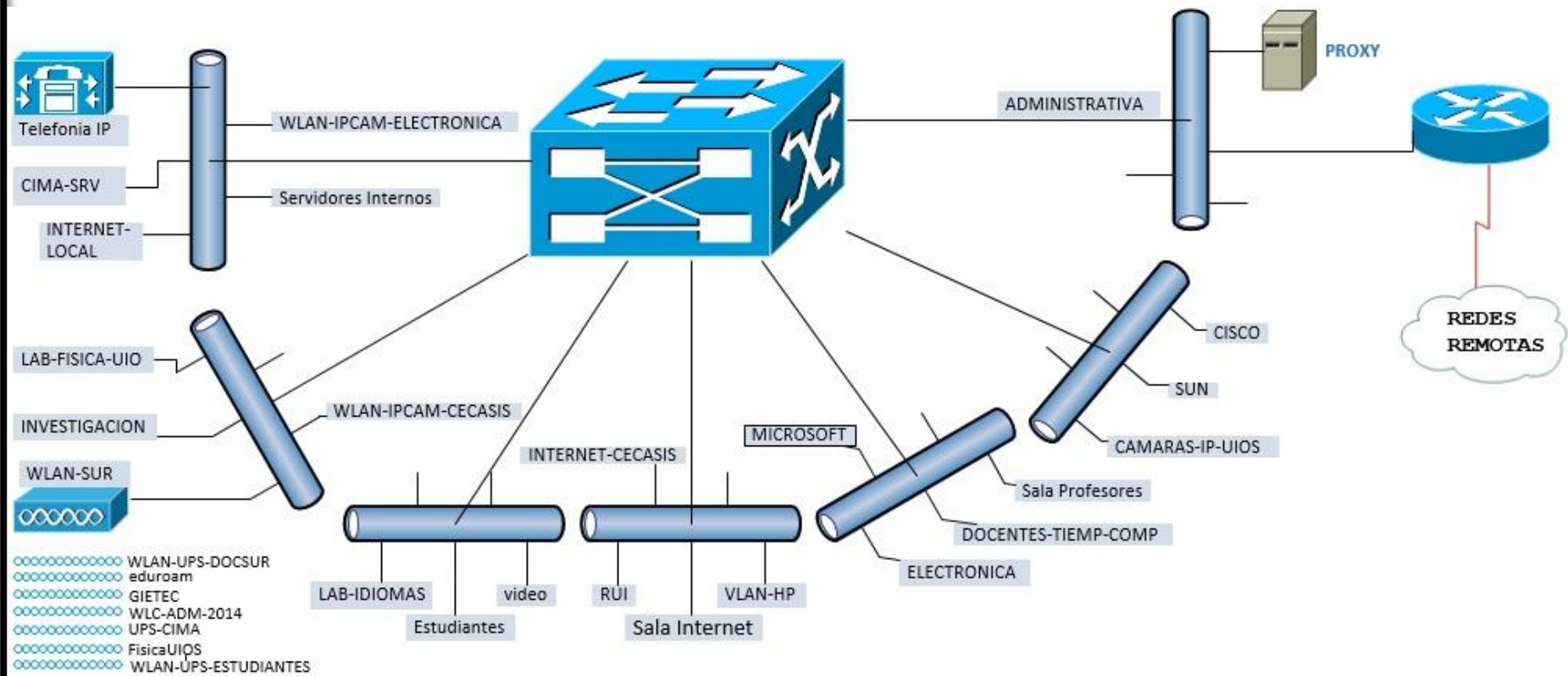


Figura 16. Elaborado por: Alejandro Moreno y Andrés Tipán

2.9.3. Topología inalámbrica

La Universidad Politécnica Salesiana Sede Quito Campus Sur en los últimos años ha tenido un crecimiento significativo de estudiantes, por lo que al menos el 70% de los estudiantes tienen acceso a la red por medio de dispositivos móviles como laptops, celulares, tabletas, entre otros. “El ingeniero Juan Carlos Domínguez Ayala manifestó en la entrevista realizada que el crecimiento de números de usuarios en la red LAN ha sido alta en los últimos años, esto se detalla en el anexo 2” (Dominguez, 2014), por tal motivo es totalmente necesario la implementación de tecnología inalámbrica para mejorar el rendimiento de los servicios y aplicaciones a través de la red. A continuación se puede observar en la figura 17 la topología física de la red inalámbrica de la Universidad Politécnica Salesiana sede Quito Campus Sur.

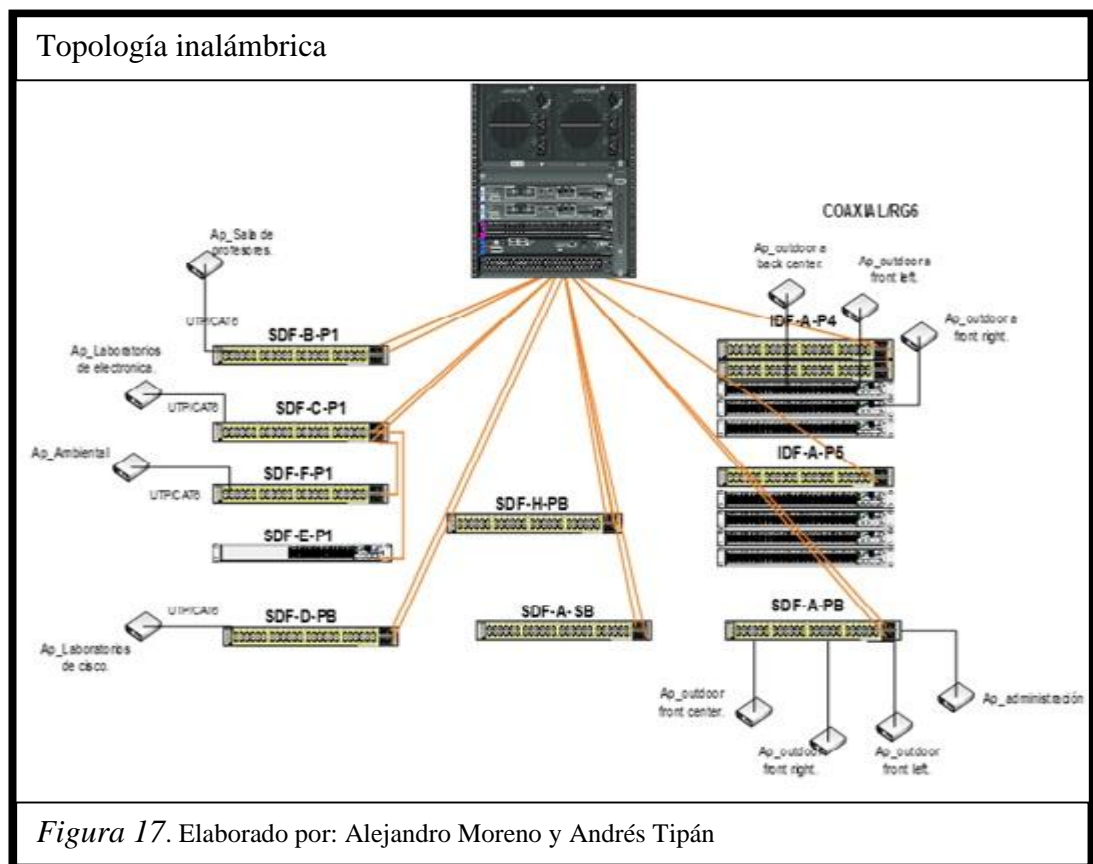


Figura 17. Elaborado por: Alejandro Moreno y Andrés Tipán

Los Access Point que integran la red inalámbrica, se encuentran ubicados tanto en la parte exterior de los bloques como en la parte interior de cada uno de estos.

A continuación se especifican los diferentes tipos de Access Point que brindan el servicio de red inalámbrica en el Campus.

Son 13 Access Point, los cuales están conformados por tres series:

- 2 Access Point de la serie 1252
- 2 Access Point de la serie 1131
- 9 Access Point de la serie 1310

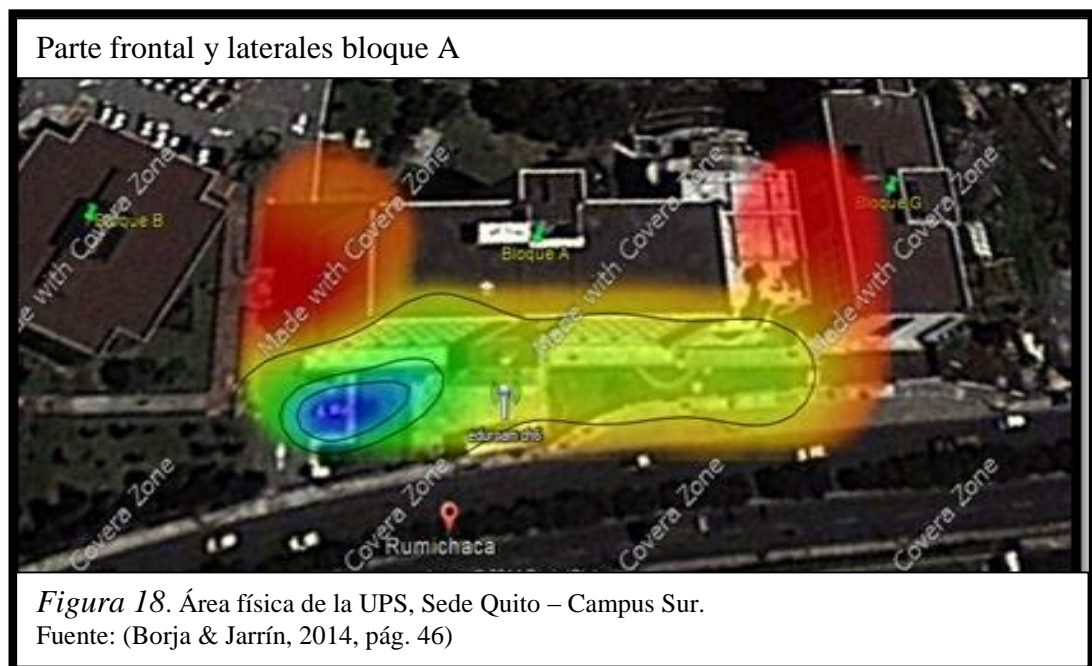
2.9.4. Cobertura de dispositivos (Access Point)

A continuación se realizará un análisis de cobertura en la Universidad Politécnica Salesiana sede Quito campus Sur, donde se indica el nivel de intensidad de la señal que tiene cada uno de los access point en los diferentes bloques, esto con el propósito de indicar el lugar donde existe menor cobertura y así poder instalar los access point necesarios para brindar una mayor cobertura.

2.9.5. Cobertura access point exteriores

2.9.5.1. Bloque A

Análisis de la cobertura de la parte exterior del bloque A, donde se encuentran 3 AP_Outdoor, ubicados en la parte superior del poste de luz situado en la entrada y en el sector posterior del bloque A.

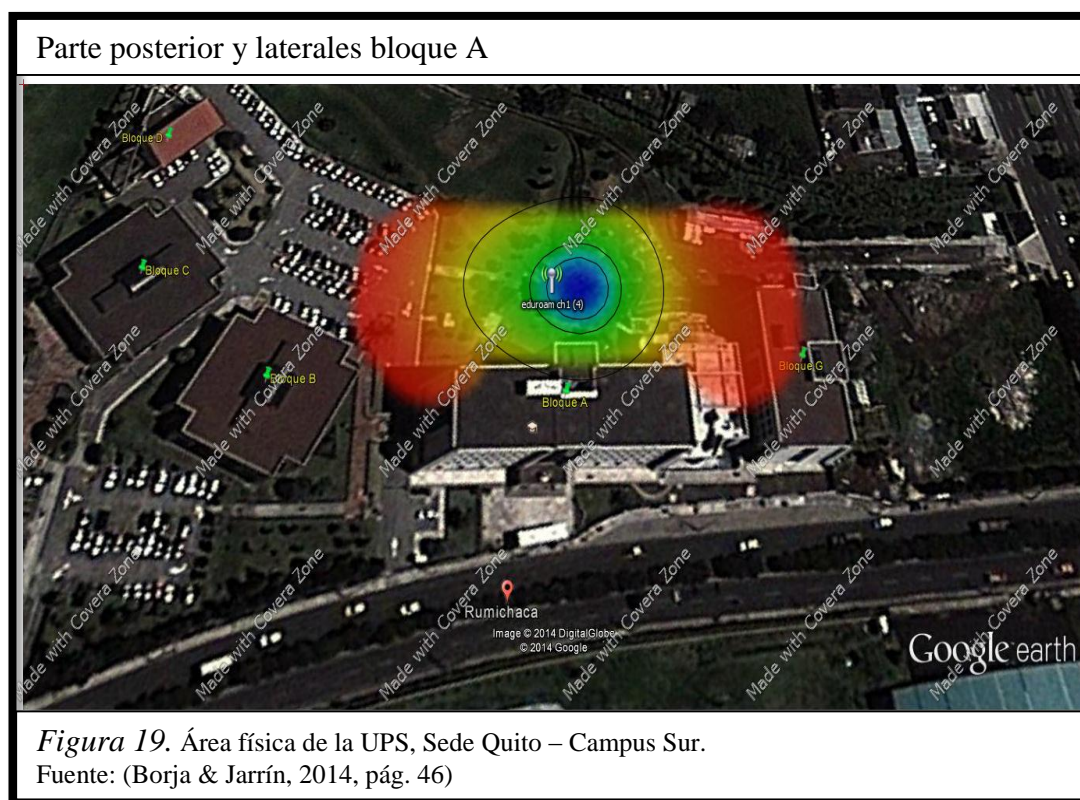


En el tabla 13 se puede apreciar los niveles de intensidad de la señal, donde el color azul muestra una intensidad de señal fuerte, el color verde muestra una intensidad de señal menos fuerte, el color verde claro muestra una intensidad de señal baja, el amarillo muestra una intensidad muy baja y el color rojo muestra una intensidad de señal escasa con poca opción de conectarse a la red.

Tabla 13. *Intensidades de Señales bloque A parte frontal.*

Color de la Intensidad de la Señal	Potencia
Azul	-47dBm
Verde	-51dBm
Verde claro	-56dBm
Amarillo	-73dBm
Rojo	-91dBm

Nota: (Borja & Jarrín, 2014, pág. 45)



Intensidades de la señal para la parte posterior y laterales del bloque A.

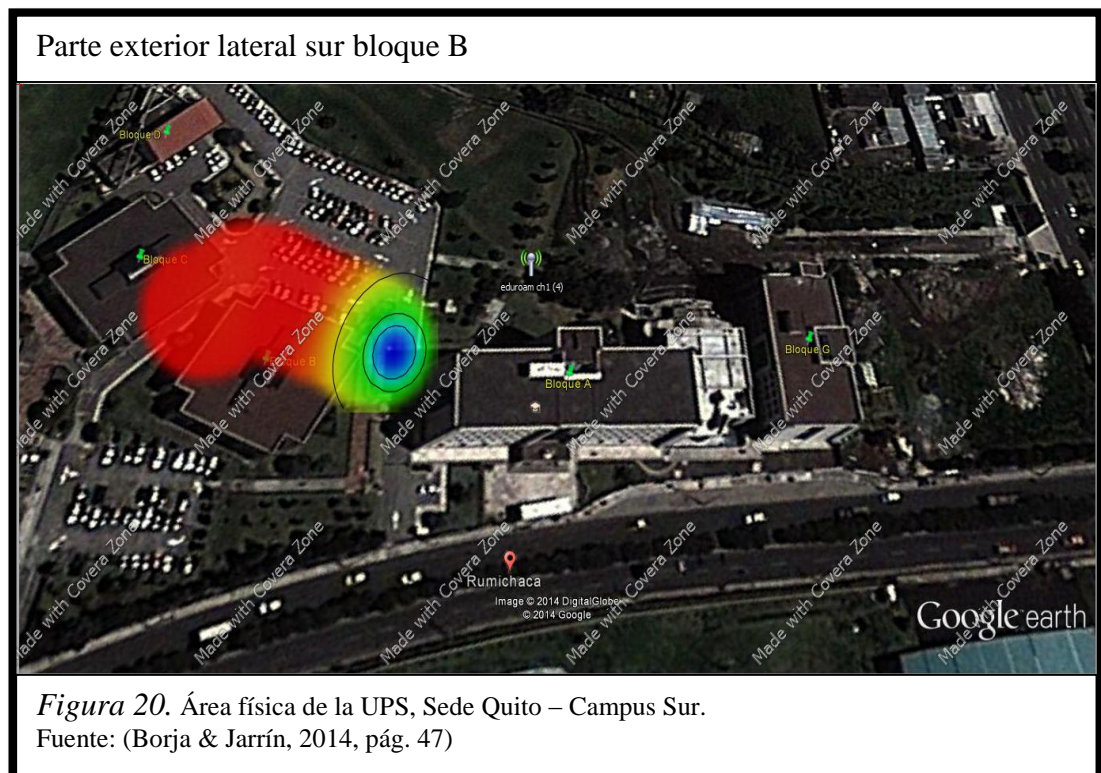
Tabla 14: *Intensidades de Señales bloque A parte posterior.*

Color de la Intensidad de la Señal	Potencia
Azul	-64dBm
Verde	-66dBm
Verde claro	-68dBm
Amarillo	-75dBm
Rojo	-82dBm

Nota: (Borja & Jarrín, 2014, pág. 46)

2.9.5.2. Bloque B

Análisis de la cobertura de la parte exterior del bloque B, donde se muestra la intensidad de señal propagada por el AP_Outdoor, dirigida a estos sectores que se encuentra ubicado en la parte superior del poste de luz situado a la entrada y en sector posterior del bloque A.

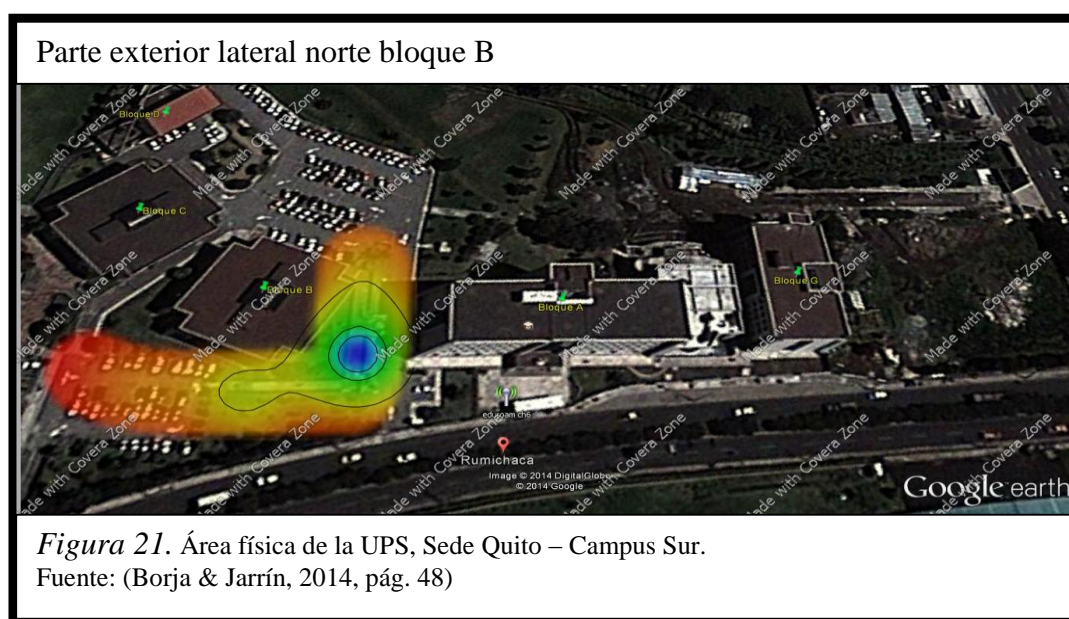


Intensidades de la señal para la parte exterior y lateral sur del bloque B.

Tabla 15. *Intensidades de Señales bloque A lateral sur.*

Color de la Intensidad de la Señal	Potencia
Azul	-69dBm
Verde	-70dBm
Verde claro	-71dBm
Amarillo	-75dBm
Rojo	-80dBm

Nota: (Borja & Jarrín, 2014, pág. 47)



Intensidades de la señal para la parte exterior y lateral norte del bloque B.

Tabla 16. *Intensidades de Señales bloque A lateral norte.*

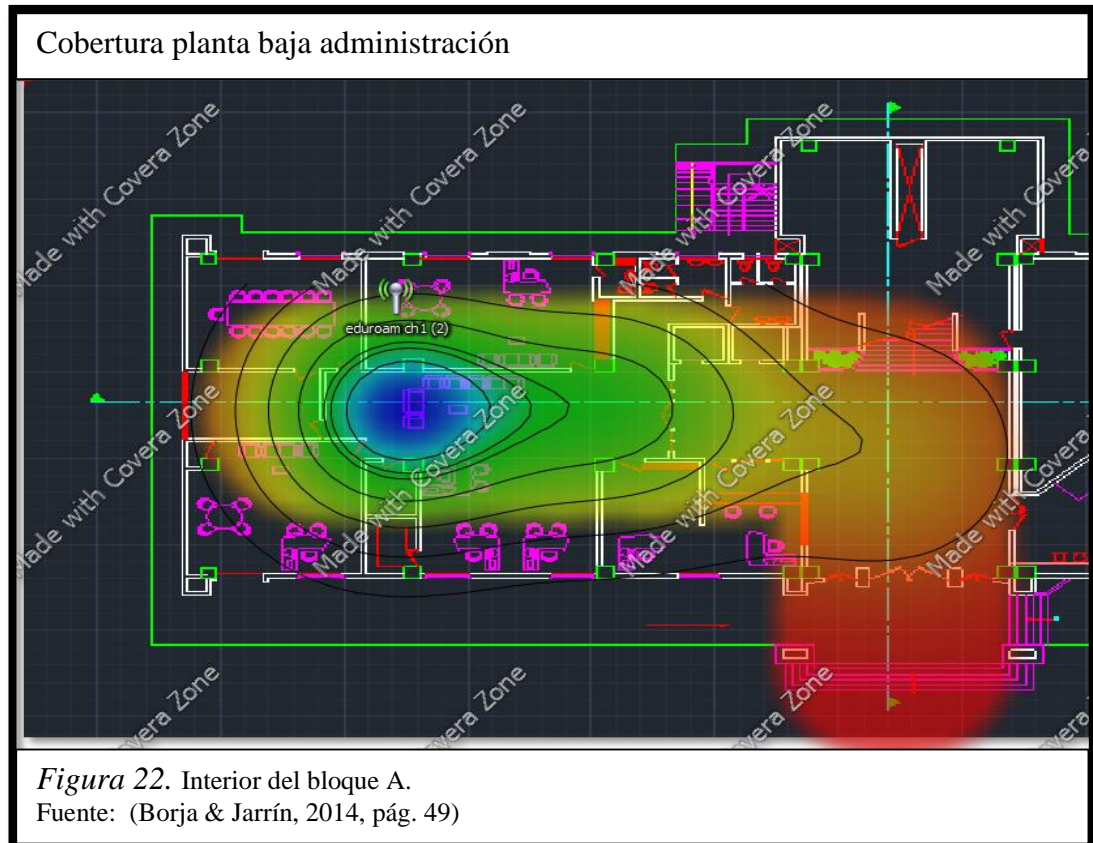
Color de la Intensidad de la Señal	Potencia
Azul	-55dBm
Verde	-58dBm
Verde claro	-62dBm
Amarillo	-75dBm
Rojo	-89dBm

Nota: (Borja & Jarrín, 2014, pág. 48)

2.9.6. Cobertura access point interiores

2.9.6.1. Administración

Análisis de cobertura realizado en la planta baja del bloque A, donde se muestra la intensidad de señal propagada por el AP_Indoor, el cual está ubicado en la parte superior de la pared en la sala de profesores.



A continuación se detalla la intensidades de la señal que se adquirió en el análisis de cobertura realizado en el área de sala de profesores, administración.

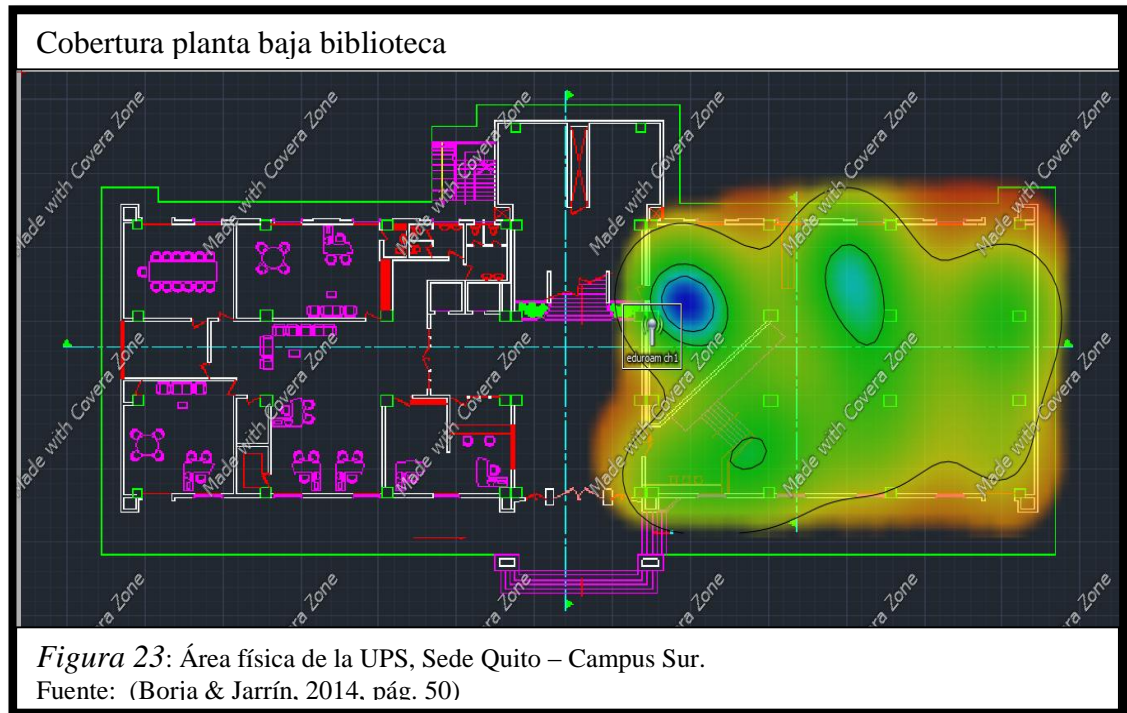
Tabla 17: *Intensidades de Señales.*

Color de la Intensidad de la Señal	Potencia
Azul	-27dBm
Verde	-32dBm
Verde claro	-37dBm
Amarillo	-58dBm
Rojo	-78dBm

Nota: (Borja & Jarrín, 2014, pág. 49)

2.9.6.2. Biblioteca

Análisis de cobertura realizado en la planta baja del bloque A, donde se muestra la intensidad de señal propagada por el AP_Indoor, el cual está ubicado en la parte superior de la pared en la sala de profesores.



A continuación se detalla la intensidad de la señal que se adquirió en el análisis de cobertura realizado en el área de sala de biblioteca.

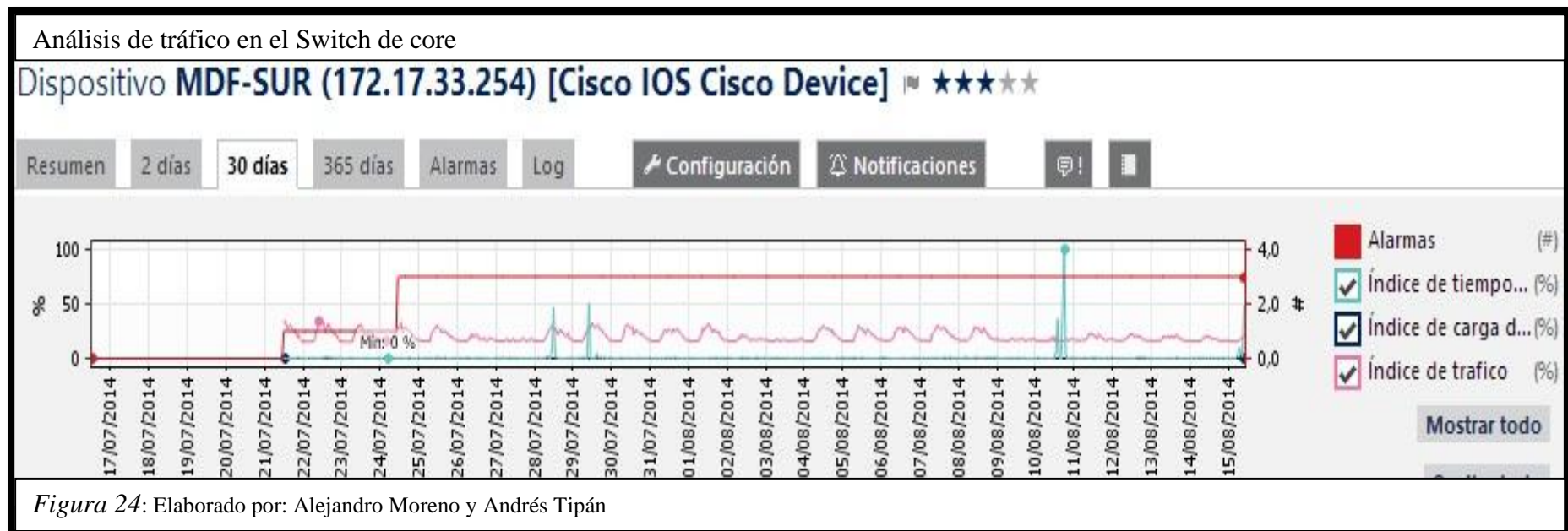
Tabla 18: *Intensidades de Señales.*

Color de la Intensidad de la Señal	Potencia
Azul	-27dBm
Verde	-32dBm
Verde claro	-37dBm
Amarillo	-55dBm
Rojo	-74dBm

Nota. (Borja & Jarrín, 2014, pág. 50)

2.9.6.3. Análisis del tráfico actual

En la figura 24 se observa el tráfico de ancho de banda en las horas pico de la Universidad Politécnica Salesiana sede Quito campus Sur, los cuales son: en horario matutino a las 12:30 PM, en horario vespertino a las 5:00 PM, esto se efectuó por el periodo de un mes donde se observa que el índice de tráfico no supera el 50% de lo que soporta el switch de core.



Con el software PRTG se ha escaneado la granja de servidores para ver el tráfico de ancho de banda que se genera en cada uno de los puertos del switch de core esto se encuentra detallado en el anexo 2

2.9.6.4. Vulnerabilidades

Las vulnerabilidades son amenazas que afectan la disponibilidad e integridad de la red, por tal motivo es importante identificar las vulnerabilidades para dimensionar los riesgos a los cuales está expuesta la red de datos y especificar las medidas de seguridad apropiadas para su corrección.

En la figura 25 se observa la presencia de elementos que perjudican el uso adecuado de la red de la Universidad Politécnica Salesiana sede Quito campus Sur.



Figura 25. Elaborado por: Alejandro Moreno y Andrés Tipán

Esta aplicación escaneó las vulnerabilidades de código abierto que prueban la seguridad de aplicaciones web, donde se puede determinar la existencia de vulnerabilidades como Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File Inclusion, Integer Overflow, entre otras.

En la figura 26 se muestra una vulnerabilidad detectada tipo SQL Injection, estas vulnerabilidades están presentes cuando se utiliza entrada suministrada externamente para construir una consulta SQL. Si no se toman precauciones, la entrada suministrada externamente (por lo general de parámetros GET y POST) puede modificar la cadena de consulta de manera que realiza acciones no deseadas. Estas acciones incluyen la

obtención no autorizada de leer o escribir el acceso a los datos almacenados en la base de datos, así como la modificación de la lógica de la aplicación.

Vulnerabilidad tipo SQL Injection	
Classification	Input Validation Error
Resource	http://www.ups.edu.ec/destacado
Parameter	entryId
Method	GET
Detection Type	Blind Arithmetic Evaluation Differential
Risk	High

Figura 26. Elaborado por: Alejandro Moreno y Andrés Tipán

En la figura 27 se muestra una vulnerabilidad detectada de tipo Cross-site scripting (XSS), son un tipo de vulnerabilidades que afectan a las aplicaciones web que pueden resultar que los controles de seguridad implementados en los navegadores sean eludidas.

Vulnerabilidad tipo Cross-site scripting (XSS)	
Classification	Input Validation Error
Resource	/http:/
Parameter	p_p_lifecycle
Method	GET
Risk	High

Figura 27. Elaborado por: Alejandro Moreno y Andrés Tipán

En la figura 28 se muestra una vulnerabilidad detectada de tipo HTTP TRACE es un método HTTP que solicita que el servidor de eco de la petición TRACE al cliente. Esto incluye las cabeceras que se enviaron junto con la solicitud.

Vulnerabilidad tipo HTTP Trace Support Detected	
Classification	Configuration Error
Resource	Apache
Method	TRACE
Risk	Medium
<i>Figura 28.</i> Elaborado por: Alejandro Moreno y Andrés Tipán	

Se identificó la existencia de una vulnerabilidad tipo TRACE/ la misma que se evidencia en la figura 29.

Recursos de contenido HTTP Trace Support Detected
<pre>TRACE / HTTP/1.1 Connection: keep-alive SQUEEMISH: OSS1FR4GE Accept-Encoding: gzip,deflate Host: www.ups.edu.ec User-Agent: UserAgent Cookie2: \$Version=1 Cookie: COOKIE_SUPPORT=true; GUEST_LANGUAGE_ID=es_ES; JSESSIONID=6F7B21AAC074A4340D68B888F7F7F8C1.worker6 X-IMForwards: 20 Via: 1.1 wsasur.ups.edu.ec:80 (Cisco-WSA/8.5.0-497)</pre>
<i>Figura 29.</i> Elaborado por: Alejandro Moreno y Andrés Tipán

Para el análisis de las vulnerabilidades se utilizó el software Vega, que funciona como un escáner automatizado y como un proxy de interceptación, ambos tipos de módulos son capaces de generar alertas.

Tabla 19: *Alertas software vega.*

High	código malicioso puede ser capaz de manipular el contenido de la página
Médium	ataques que pueden ser capaces de utilizar sitios web para obtener información de los cookies.
Low	ataques dirigidos para adivinar nombres de usuarios en la red

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

CAPÍTULO 3

DISEÑO DE LA RED LAN

El capítulo 3, contiene el análisis de los requerimientos para el diseño de la red de alta disponibilidad a partir de la situación actual de la red de la Universidad Politécnica Salesiana Sede Quito Campus Sur, se incluyen simultáneamente los criterios de diseño para la red tomando en cuenta una expansión a futuro de la red de 3 a 10 años.

3.1. Criterios de diseño LAN para la red de alta disponibilidad

Para el diseño de la red de alta disponibilidad se tomaran los aspectos que se indican a continuación.

- Número de usuarios en la red de datos.
- Expansión futura que se tendrá con la implementación de nuevas aplicaciones y servicios.
- Equipos a usar en el diseño.
- Cobertura de dispositivos (access point) en la infraestructura física.
- Aplicaciones y servicios que correrán sobre la infraestructura de la red.
- Seguridad a nivel de acs.
- Alta disponibilidad

3.2. Número de usuarios en la red

Usuario en informática, se dice a todo dispositivo que se conecta a la red, por tal motivo es importante para el diseño de la red conocer el número exacto de usuarios que tiene la red.

A continuación se indicará la densidad de usuarios con puntos de red fijos que posee cada bloque, esto es importante para establecer cuántos puertos deben tener los Switch de acceso en los pisos para el diseño de la red.

Tabla 20. Sistema de distribución de usuarios campus sur

Bloque A	#usuarios	Total
Soporte Técnico	2	371
FEUPS	3	
Dirección Administrativa	2	
Información	2	
Tesorería	3	
CECASIS	340	
Biblioteca	19	
Bloque B	#usuarios	Total
Secretaria Campus Sur	7	34
Sala de Profesores Bloque B	12	
Dirección Civil	1	
Dirección Sistemas	1	
Dirección Electrónica	1	
Dirección Ambiental	1	
Secretaria Direcciones de Carrera	3	
Sala Reuniones tras direcciones de Carrera	3	
Gerencia	1	
Fiscalización Civil	2	
Bienestar	2	
Bloque C	#usuarios	Total
Idiomas	29	79
Laboratorios de electrónica	50	
BLOQUE D	#USUARIOS	TOTAL
Laboratorio CISCO 1	16	50
Laboratorio CISCO 2	16	
Laboratorio CISCO 3	18	
Bloque E	#usuarios	Total
Estudio Suelos	8	8
Bloque F	#usuarios	Total
Sala de profesores del bloque f planta baja	4	12
Auxiliar Laboratorio Ambiental	3	
Sala de profesores del bloque f primer piso	5	
Bloque G	#usuarios	Total
Centro de Graduación	1	3
Docentes Civil	2	
Bloque H	#usuarios	Total
Pastoral	8	8
TOTAL		565

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

3.2.1 Expansión futura

En el diseño de red se tiene previsto un crecimiento del 50 % de usuarios finales, debido a la expansión actual y futura que se está teniendo con la implementación de los nuevos servicios y aplicaciones que se implementaran en la Universidad Politécnica Salesiana Sede Quito Campus Sur.

El 50 % se obtuvo del análisis de las necesidades de renovación de equipos de cómputo de la Universidad Politécnica Salesiana Sede Quito Campus Sur y el número de usuarios conectados en las redes inalámbricas, esto se detalla en el anexo 2.

Tabla 21. *Puntos de red a futuro*

Total de puntos de red actual	565
Expansión futura de 50% de puntos de red	282,5
Total de puntos de red futura	847,5

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Usuarios conectados en la red inalámbrica		
Top WLANs		
Profile Name	# of Clients	
WLAN-UPS-ESTUDIANTES	248	Detail
WLAN-UPS-DOCSUR	80	Detail
WLC-BIBLIOTECA-UIOS	15	Detail
RED-ADM	4	Detail
GIETEC	3	Detail

Figura 30. Elaborado por: Alejandro Moreno, Andrés Tipán

Es decir que los puntos de red a futuro vendrán a aumentar en un 50%, así pasará de 565 a 848 puntos de red.

3.3. Equipos a usar

Para realizar el diseño de red, acorde a la necesidad de los usuarios de la Universidad Politécnica Salesiana sede Quito campus Sur, se ha considerado una estimación de tráfico actual y futuro, además de la expansión futura que se provee tener en los próximos años con la implementación de nuevos servicios y aplicaciones, por lo que se utilizará equipos marca CISCO.

3.3.1. Marca de los equipos

Para la adquisición de equipos se ha tomado en cuenta la marca CISCO por las siguientes razones:

- CISCO es una empresa líder en equipamiento de infraestructura de red a nivel mundial.
- Tiene varios socios a nivel nacional, algunos de estos son: IBM, DESCAL, SINETCOM, COMWARE, CIBERCALL, entre otros
- Documentación clara y muy difundida.
- Nivel de core muy usado en Latinoamérica y en empresas del país.
- Cuenta con academias de educación, donde se capacita y certifica a profesionales de networking.

Además es importante mencionar, que la actual infraestructura de red cuenta en la mayor parte de su diseño con esta marca por lo que sería de gran ventaja para un rediseño el poder ocupar estos equipos y ahorrar costos.

3.3.2. Cantidad de equipos

Tabla 22. *Plataforma tecnología*

Equipos	Cantidad
Switch de core CISCO 6506e	2
Switch de distribución CISCO 3750	12
Switch de acceso CISCO 2960	29
CISCO aironet 1520 outdoor	9
CISCO aironet 2600 input	42
CISCO 2500 wireless controller	1

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

3.3.2.1. Distribución de los equipos por bloque

El diseño de la red de alta disponibilidad tiene el fin de optimizar la comunicación entre host y los servicios de la red LAN en la Universidad Politécnica Salesiana sede Quito campus Sur. Por lo que finalmente, se decidió adicionar otro switch de core CISCO 6506e para ofrecer redundancia en caso de haber fallos con el switch de core principal, también se propone utilizar switch de distribución CISCO 3750 y switch de acceso CISCO 2960, esto con el propósito de hacer uso de los equipos que posee actualmente la red LAN y disminuir precios en la inversión de la nueva infraestructura de red.

A continuación en las figuras 31, 32, 33 se muestra como estarán distribuidos los equipos por bloques, los cuales van a estar conectados desde los MDF hacia los IDF a través de fibra óptica multimodo (62.5/125 micrones), para una longitud de onda de 1300 nm, ancho de banda 500 (MHz/Km) y atenuación máxima 1.5 (dB/Km) a una velocidad de transmisión de 1 Gbps que atraviesa un ducto desde el quinto a la planta baja y hacia los demás bloques, pasando por los cuartos de telecomunicaciones desde aquí da servicio por medio de UTP a los SDF a una velocidad de transmisión de 1Gbps.

Distribución de los equipos bloque A

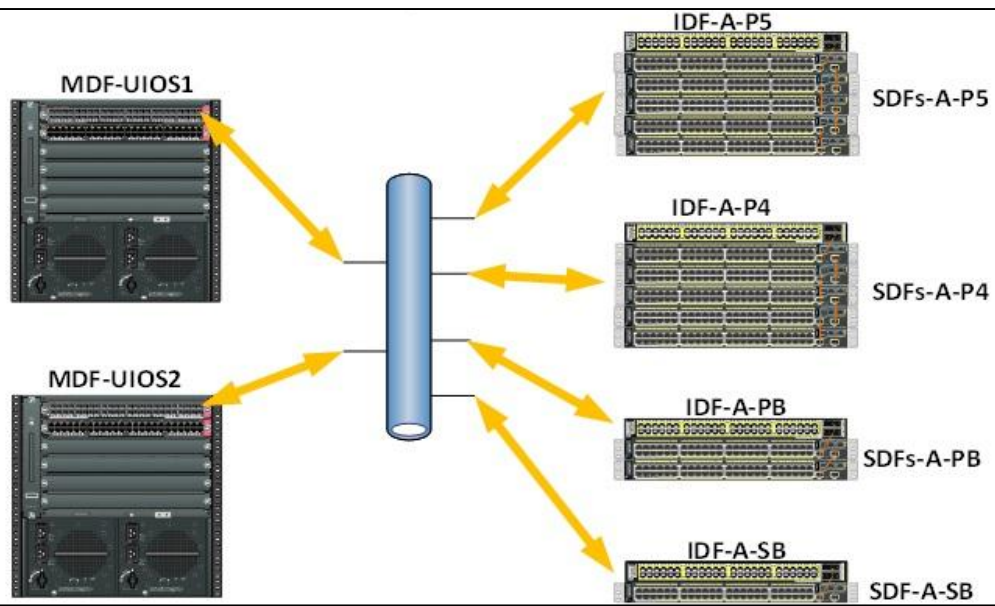


Figura 31. Elaborado por: Alejandro Moreno y Andrés Tipán

Distribución de los equipos bloques B, C, D, E, F.

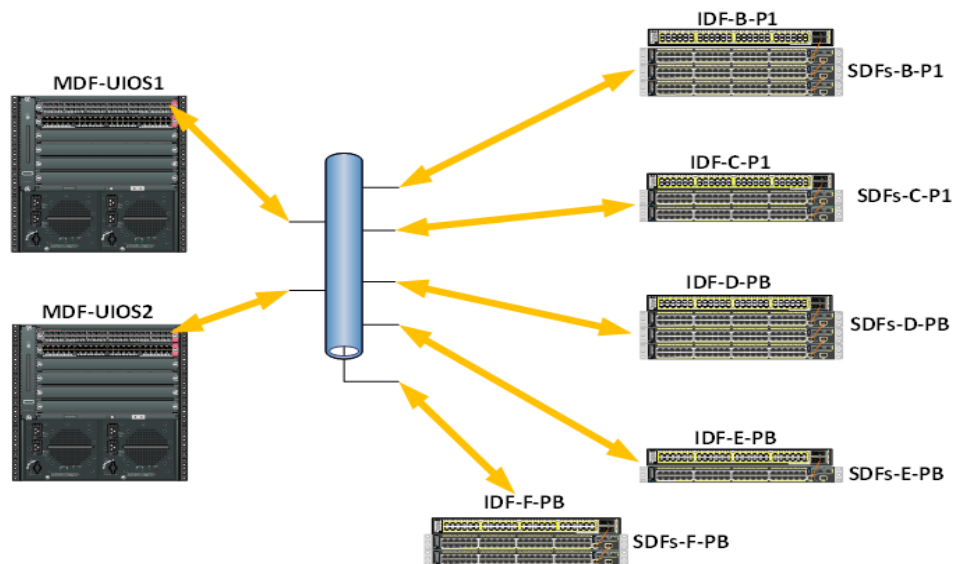
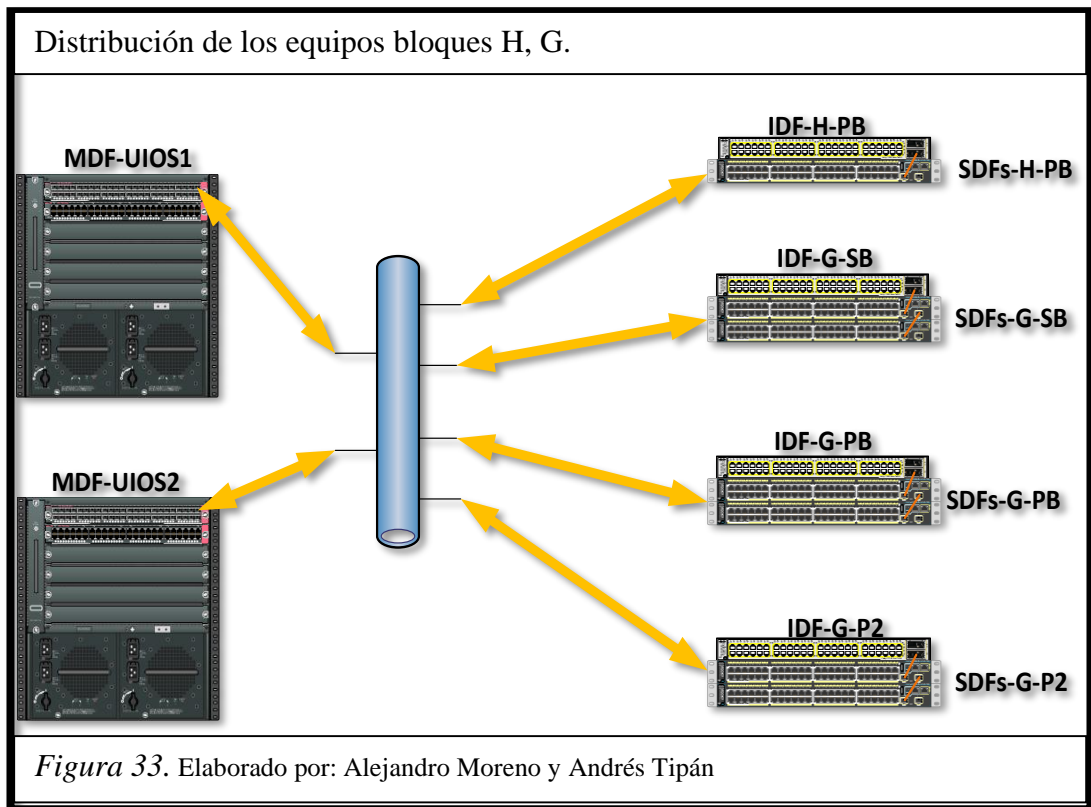


Figura 32. Elaborado por: Alejandro Moreno y Andrés Tipán



3.4. Especificaciones técnicas de los equipos

En el mercado actual existen varias marcas para equipos de networking así como son CISCO, HUAWEI, HP, ALCATEL, DLINK, etc.

Aun que se ha escogido la marca CISCO por todas las características y especificaciones adjuntas, también es conocido que CISCO es una de las empresas mejor nombradas como líder en el cuadrante de Gartner como se observa en la figura 34.

Magic Quadrant

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure



Figura 34. Fuente: (Gartner, 2015)

3.4.1. Especificaciones técnicas del core-CISCO 6506e.

El equipo ofrece máxima disponibilidad con redundancia rápida y reconexión dinámica a través de motores de supervisión.

Tabla 23: *Especificaciones técnicas del CORE-CISCO 6506e*

General	Especificación
Tipo de dispositivo	Conmutador
Tipo incluido	Montable en bastidor- 12 U
Cantidad de módulos instalados (Max.)	2(instalados)/6 max.
Anchura	43.7 cm
Profundidad	46 cm
Altura	51.1 cm
Conexión de redes	
Cantidad de puertos	48 x Ethernet, 10 Base-T, Ethernet 100 Base-Tx, Ethernet 1000Base-T
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de gestión remota	SNMP, RMON
Tecnología de conectividad	Cableado
Tamaño de tabla de dirección MAC	128k de entradas
Cumplimiento normas	IEEE 802.3, IEEE 802.3U, IEEE 802.3ab
Memoria	
Memoria flash	32 MB flash
Características	
Alta disponibilidad	
Gateway Load Balancing Protocol	
Hot Standby Router Protocol (HSRP)	
Multimodule EtherChannel technology	
Rapid Spanning Tree Protocol (RSTP)	
Multiple Spanning Tree Protocol (MSTP)	
Per-VLAN Rapid Spanning Tree	
Rapid convergence Layer 3 protocols	

Módulos de servicios avanzados
Content services gateway
CSM
Firewall module
IDS module
IP Security (IPSec) VPN module
Network analysis module
Persistent storage device
SSL module
Wireless LAN services module

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Como se puede observar en la tabla 23 este equipo posee características de gran desempeño además, ofrece una innovación adicional el Virtual Switching System (VSS) lo cual permitirá tener ampliación de la capacidad del ancho de banda del sistema de hasta 1,4 Tbps, por tal motivo se decidió ocupar el equipo CISCO 6506e en el core de la red propuesta.

3.4.2. Especificaciones técnicas de distribución CISCO 3750

Los equipos CISCO Catalyst 3750 son switches apilables (stackable), y soportan la tecnología de Cisco Energy-Wise lo que ayuda a reducir costos de energía y la huella de carbono.

Tabla 24. *Especificaciones técnicas de distribución-CISCO 3750*

General	Especificación
Tipo de dispositivo	Conmutador
Tipo incluido	Montable en rack- 1U
Anchura	44.5 cm
Profundidad	46 cm
Altura	4.5 cm
Conexión de redes	

Cantidad de puertos	24 y 48 10/100/1000
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, TFTP, SSH, CLI, TFTP
Tecnología de conectividad	Cableado
Alimentación	CA 120/230 V (50/60 Hz) - PoE
Cumplimiento normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP).
Memoria	
Memoria RAM	256 MB
Memoria flash	32 MB flash
Características	
Conmutación Layer 2, asignación dirección dinámica IP, soporte de DHCP, Ethernet (PoE), soporte ARP, soporte VLAN, soporte para Syslog, Broadcast Storm Control, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Access Control List (ACL), Quality of Service (QoS), Dynamic ARP Inspection (DAI), PoE+, Per-VLAN Spanning Tree Plus (PVST+), EIGRP Stub Routing, Uni-Directional Link Detection (UDLD), Shaped Round Robin (SRR), Protocolo de control de adición de enlaces (LACP), Remote Switch Port Analyzer (RSPAN)	

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Dadas a las especificaciones técnicas y características de la tabla 24 se observa el gran desempeño que ofrece el equipo CISCO 3750 y la documentación clara y muy difundida que posee, por esta razón se decidió ocupar en la capa distribución de la red propuesta.

3.4.3. Especificaciones técnicas acceso-CISCO 2960

El switch CISCO 2960 ofrece una extensa gama de procesos de autenticación, cifrado de datos, y Network admisión control (NAC), sobre la base de usuarios, puertos y direcciones MAC.

Tabla 25. *Especificaciones técnicas acceso-CISCO 2960*

General	Especificación
Tipo de dispositivo	Conmutador
Tipo incluido	Montable en rack- 1U
Anchura	44.5 cm
Profundidad	29.9 cm
Altura	4.5 cm
Conexión de redes	
Cantidad de puertos	24 y 48 10/100/1000
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Tecnología de conectividad	Cableado
Alimentación	Poe - CA 120/230 V (50/60 Hz)
Cumplimiento normas	EEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w
Memoria	
Memoria RAM	128 MB
Memoria flash	64 MB flash
Características	
Conmutación Layer 2, auto-sensor por dispositivo, asignación dirección dinámica IP, negociación automática, soporte BOOTP, soporte ARP, equilibrio de carga, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, soporte DiffServ, Broadcast Storm Control, soporte IPv6,	

Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Access Control List (ACL), Quality of Service (QoS), Protocolo de control de adición de enlaces (LACP), Port Security, MAC Address Notification, Remote Switch Port Analyzer (RSPAN)

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Como se aprecia en las especificaciones técnicas de la tabla 25, este equipo posee grandes características, además que el equipo CISCO 2960-X es un es un nuevo modelo propuesto por CISCO que son Switches de acceso rentable, escalable, inteligente, por lo cual se recomienda ocupar en la capa acceso.

3.4.4 Especificaciones técnicas CISCO ASA 5515-x

Es un dispositivo que proporciona servicios de seguridad altamente integrados para redes de todos los tamaños, además de VPN de próxima generación.

Tabla 26. *Especificaciones técnicas CISCO ASA 5515-x*

General	Especificación
Tipo de dispositivo	Dispositivo de seguridad
Altura (unidad de bastidor)	1U
Anchura	42.9 cm
Profundidad	39.5 cm
Altura	4.2 cm
Peso	6.1 kg
Memoria RAM	8 GB
Cantidad de puertos	6
Protocolo de interconexión de datos	Gigabit Ethernet
Alimentación	CA 120/230 V (50/60 Hz)
Capacidad	
Peers VPN IPsec : 250	
Peers VPN SSL : 2	

Sesiones concurrentes : 250000
Interfaces virtuales (VLAN) : 100
Contextos de seguridad : 2
Características
Capacidad del cortafuegos: 1.2 Gbps
Capacidad de VPN (3DES/AES) : 250 Mbps
Tasa de conexiones : 15000 conexiones por segundo
Rendimiento del cortafuegos + prevención de intrusiones : 400 Mbps

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

En la tabla 26, se observa que el CISCO ASA 5515-X ha sido diseñado para ofrecer un rendimiento superior con una eficiencia operativa excepcional dando soluciones de seguridad de alto rendimiento rentable que puede crecer con necesidades cambiantes de la red.

3.4.5 Especificaciones técnicas CISCO s380 web security appliance

El equipo CISCO s380, ayuda a asegurar y controlar el tráfico de Internet, al tiempo que simplifica la implementación y reducción de costos en la red.

Tabla 27. *Especificaciones técnicas CISCO s380 web security appliance*

General	Especificación
Tipo de dispositivo	Dispositivo de seguridad
Factor de forma	Montable en bastidor-2U
Anchura	48.3 cm
Profundidad	73.7 cm
Altura	8.9 cm
Procesador	1xIntel xeon Es-2600 series 2Ghz
Memoria RAM	16 GB
Disco duro	600 GBx4- SATA 3Gb/s

Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de gestión remota	Telnet, HTTP, HTTPS, SSH, CLI
Interfaces	4 x 1000Base-T - RJ-45 1 x management - RJ-45 2 x USB 2.0 - Type A 1 x 1000Base-T (administración)
Alimentación	CA 120/230 v
Capacidad	
Conexión / cantidad de usuarios: 1500-6000	
Características	
Negociación automática, soporte LDAP, análisis de antivirus, protección anti-spam, Prevención de pérdida de datos (DLP)	

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Como se aprecia en las especificaciones técnicas de la tabla 27, este dispositivo proporciona seguridad web, control de aplicaciones, proxy-cache, además protege a todos los usuarios independientemente de su ubicación esto a través de la integración con Cisco AnyConnect, también es capaz de generar informes de cómo está funcionando la red.

3.4.6 Especificaciones técnicas CISCO 2500 series wireless controller

El equipo CISCO 2500 serie wireless controller, es un controlador inalámbrico que proporciona la comunicación en tiempo real entre los puntos de acceso CISCO Aironet para simplificar el despliegue y operación de redes inalámbricas.

Tabla 28. *Especificaciones técnicas CISCO 2500 series wireless controller*

General	Especificación
Tipo de dispositivo	Dispositivo de gestión de red
Factor de forma	Externo- 1U
Anchura	20.32 cm
Profundidad	27.15 cm
Altura	4.39 cm
Cantidad de puertos	4
Memoria RAM	16 GB
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de conmutación	Ethernet
Protocolo de transporte	TCP/IP, UDP/IP, ICMP/IP, IPSec, ARP, BOOTP, DHCP
Protocolo de gestión remota	SNMP 1, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, SSH
Interfaces	1 x management - RJ-45 2 x 1000Base-T - RJ-45
Alimentación	CA 120/230 v, admite POE
Método de autenticación	
RADIUS, certificados X.509, TACACS, Extensible Authentication Protocol (EAP)	
Características	
Soporte de DHCP, soporte ARP, soporte VLAN, soporte IPv6, Sistema de prevención de intrusiones (IPS), soporte SNTP, soporte Wi-Fi Multimedia (WMM), soporte de Trivial File Transfer Protocol (TFTP), Quality of Service (QoS)	

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

En la tabla 28 de las especificaciones técnicas, se observa que este controlador proporciona las políticas de seguridad necesarias, sistema de prevención de intrusiones inalámbricas (WIPS), gestión de RF y Calidad de Servicio (QoS) para voz y video.

3.4.7. Especificaciones técnicas antenas CISCO Aironet 1520 outdoor

Las antenas CISCO aironet 1520, son una plataforma de malla flexible, segura y escalable que está diseñado para despliegues en grandes áreas de gran tamaño.

Tabla 29. *Especificaciones técnicas antenas CISCO Aironet 1520 outdoor*

General	Especificación
Tipo de dispositivo	Punto de acceso inalámbrico
Factor de forma	Externo
Anchura	30.5 cm
Profundidad	19.8 cm
Altura	16.3 cm
Velocidad de transferencia de datos	300 Mbps
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n
Banda de frecuencia	2.4 Ghz, 5 Ghz
Alimentación	PoE
Cumplimiento de normas	IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11g, IEEE 802.1x, IEEE 802.11i, Wi-Fi CERTIFIED, IEEE 802.11n
Interfaces	1 x 1000Base-T - RJ-45 1 x antena - N connector
Algoritmos de cifrado	LEAP, AES, TLS, PEAP, TTLS, TKIP, WPA, WPA2
Método de autenticación	
Certificados X.509, Extensible Authentication Protocol (EAP)	
Características	
Auto-sensor por dispositivo, filtrado de dirección MAC, soporte DFS, pasarela VPN, tecnología MIMO, Quality of Service (QoS), modo de puente inalámbrico, tecnología CleanAir, tecnología ClientLink	

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Con el objetivo de mejorar el uso de todos los dispositivos y aplicaciones móviles que se utilizan en el entorno de la Universidad Politécnica Salesiana, se utilizará CISCO Aironet 1520 outdoor por sus especificaciones técnicas observadas en la tabla 29.

3.4.8. Especificaciones técnicas antenas CISCO Aironet 2600 input

La serie CISCO Aironet 2600 establece un nuevo estándar para la tecnología inalámbrica, ofreciendo un gran rendimiento, funcionalidad y fiabilidad a un precio competitivo.

Tabla 30. *Especificaciones técnicas antenas CISCO aironet 2600 input*

General	Especificación
Tipo de dispositivo	Punto de acceso inalámbrico
Factor de forma	Externo
Anchura	22.1 cm
Profundidad	22.1 cm
Altura	5.4 cm
Memoria RAM	256 MB
Memoria Flash	32 MB
Velocidad de transferencia de datos	450 Mbps
Protocolo de interconexión de datos	IEEE 802.11a,b,g,n
Banda de frecuencia	2.4 Ghz, 5 Ghz
Directividad	Omnidireccional
Antena	Interna integrada
Nivel de ganancia	4 dBi
Cumplimiento de normas	IEEE 802.11b, IEEE 802.11a, IEEE 802.3af, IEEE 802.11d, IEEE 802.11g
Interfaces	1 x 1000Base-T - RJ-45 1 x management - RJ-45
Algoritmos de cifrado	AES, TLS, PEAP, TKIP, WPA,WPA2
Método de autenticación	

MS-CHAP v.2, Extensible Authentication Protocol (EAP), EAP-FAST
Características
Soporte DFS, tecnología MIMO, soporte Wi-Fi Multimedia (WMM), tecnología CleanAir, Maximum Ratio Combining (MRC), tecnología ClientLink 2.0

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

El equipo CISCO Aironet 2600 input, debido a las características mencionadas en la tabla 30, este dispositivo mejora notablemente el rendimiento de las redes inalámbricas, reduciendo los huecos de cobertura inalámbrica y además permitirá incrementar la productividad en el entorno de la Universidad Politécnica Salesiana.

3.5. Uso de POE

Power over ethernet (POE), tecnología que permite la suministro de energía eléctrica a los dispositivos de una LAN, es decir es la alimentación eléctrica que se suministra a los switch´s y router´s.

Las ventajas de la utilización de POE son las siguientes:

- No necesita instalación de punto eléctrico cerca del dispositivo que debe ser energizado.
- Se puede apagar o reiniciar los dispositivos finales mediante el uso de comandos en el puerto.
- Uso del Protocolo Simple de Administración de Red (SNMP).
- Uso de un cable de red UTP para ofrecer servicio de red y alimentación eléctrica. Es posible conectar teléfonos IP, wireless, switch, router y demás dispositivos que con tecnología POE

3.6. Solución inalámbrica

3.6.1 Cobertura inalámbrica exterior todo el campus

Como se observa en la figura 31 la cobertura no es uniforme y se centraliza más en el bloque A, por tal motivo la red inalámbrica a proponerse debe ofrecer una mayor cobertura en el campus para lo cual se tomará las siguientes medidas.

Se proyectará y bosquejará el esquema de red inalámbrica a implementarse, para determinar la ubicación física de las antenas y así brindar una mayor cobertura en el campus.

Se realizarán las mejoras de seguridades de acceso a la red inalámbrica a través de los protocolos de acceso existentes para estas tecnologías y se integrará al nuevo esquema de la red LAN propuesta.

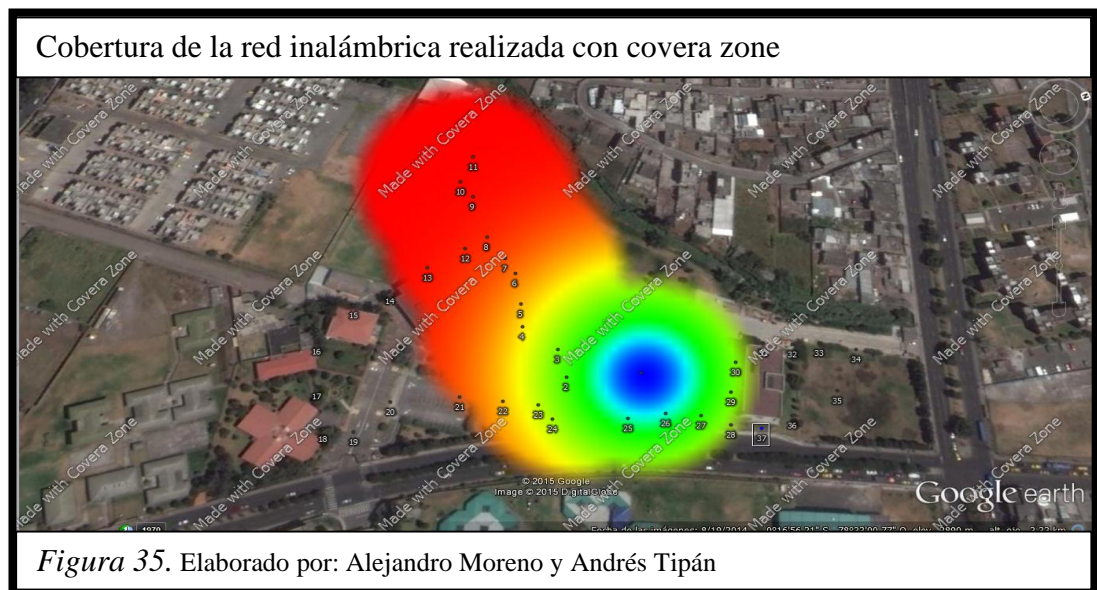


Tabla 31. Intensidades de Señales red inalámbrica

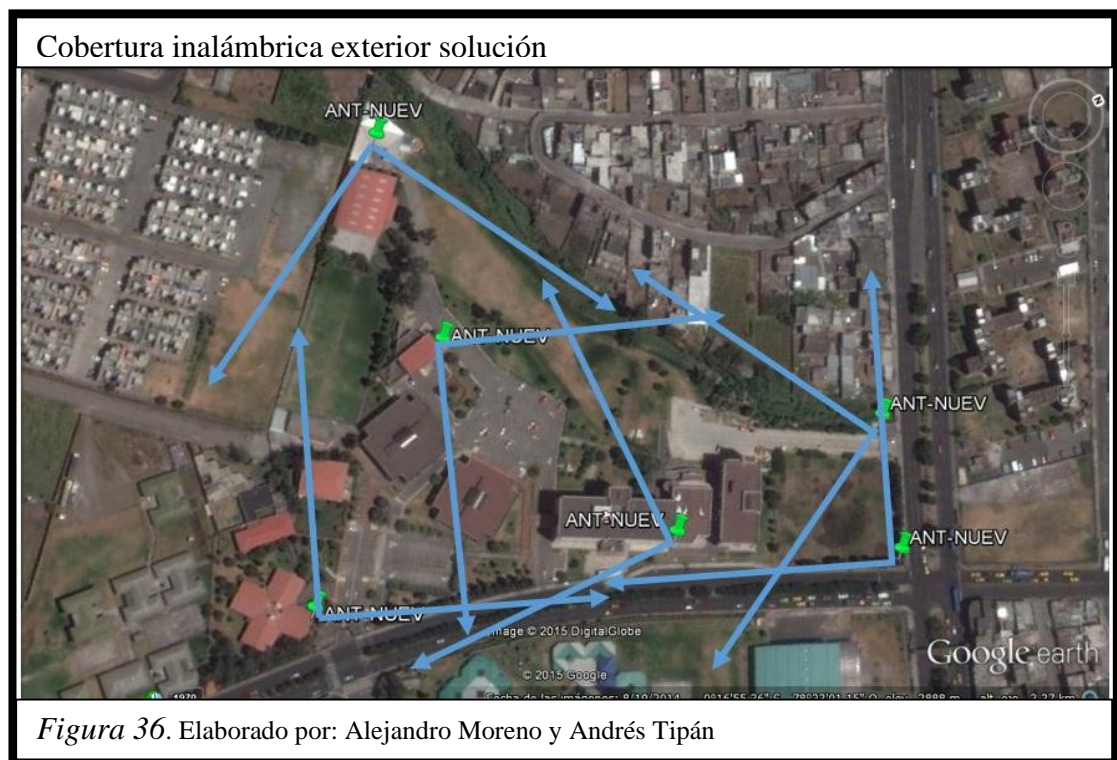
Color de la Intensidad de la Señal	Potencia
Azul	-69dBm
Verde	-71dBm
Verde claro	-73dBm
Amarillo	-80dBm
Rojo	-87dBm

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

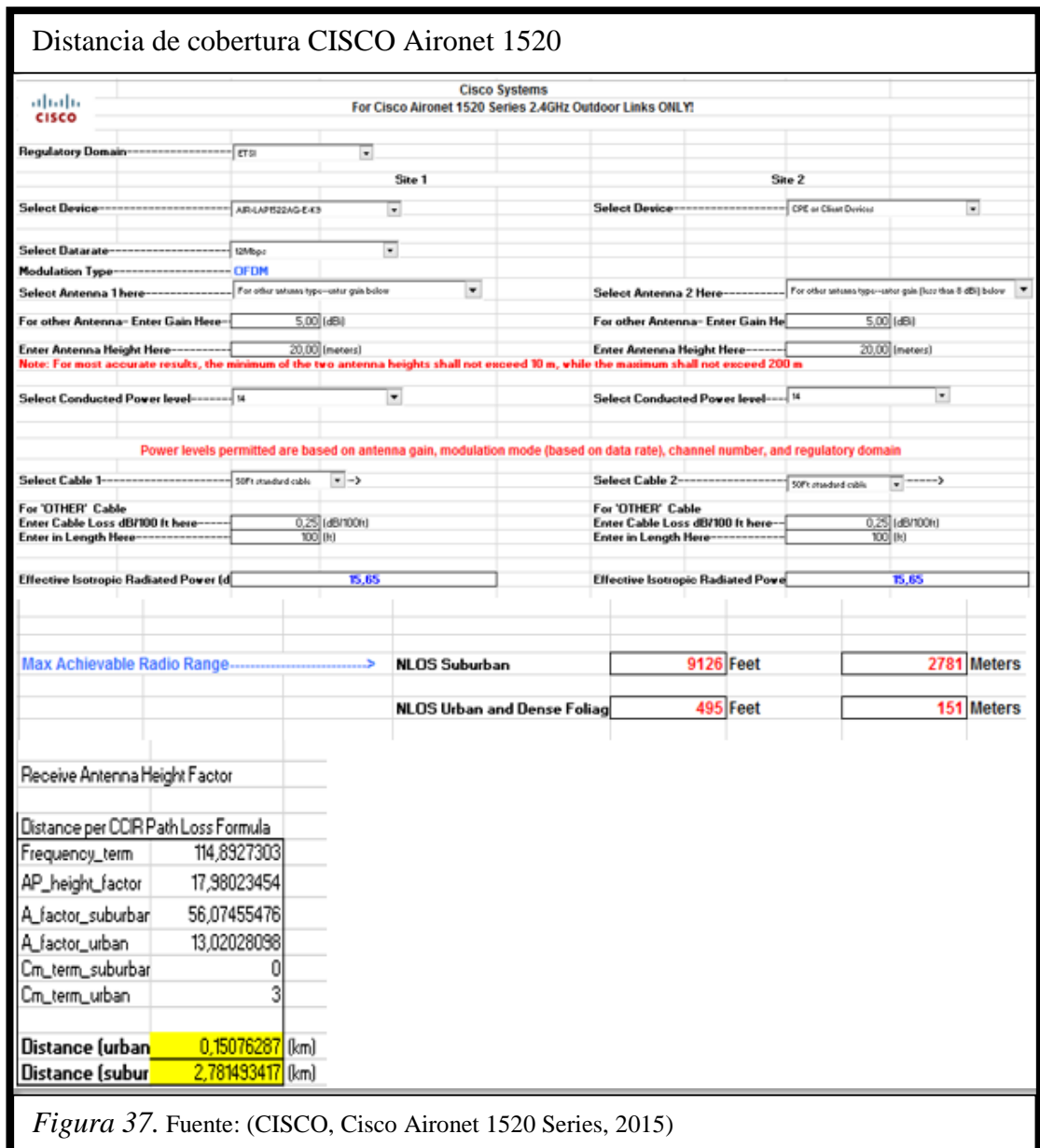
La red inalámbrica a proponerse debe permitir establecer políticas de seguridad y QoS de manera general, ya que las redes inalámbricas son más susceptibles a los ataques de intrusos.

3.6.1.1. Funcionalidad general de la red propuesta

La red inalámbrica a proponerse debe dar redundancia de cobertura para poder tener mayor conectividad y moverse dentro de toda la red de campus sin perder conectividad para lo cual se utilizará las antenas CISCO Aironet 1520 outdoor y se ubicaran de acuerdo a lo expuesto en la figura 36.



Las antenas estarán ubicadas a una altura referencial de 20 m por encontrarse en una zona urbana y cubrirán un área de cobertura aproximada de 150 m aproximadamente, esto con la finalidad de estar dentro del rango de cobertura de un 85% al 100%, los 150m se obtuvo de Cisco Systems For Cisco Aironet 1520 Series 2,4 GHz Outdoor Links ONLY.



3.7. Servicios y Aplicaciones

Continuamente se tiene problemas de saturación de la red, esto se debe muchas veces a la gran cantidad de carga que produce los servicios y aplicaciones que corren por la red, es por eso que es importante conocer los servicios, aplicaciones actuales y futuras que se va a tener en la red los cuales se pueden observar en las tablas 32, 33 esto con el fin de mejorar el rendimiento con el diseño de red propuesto.

Tabla 32. *Servicios y Aplicaciones Actuales*

SERVICIOS Y APLICACIONES ACTUALES		
SERVICIOS	APLICACIONES	
SNA	SNA	Sistema Nacional Académico
SIGAC	SIGAC	Sistema Integrado de Gestión Administrativa Contable
SQUAD	SQUAD	Sistema de gestión de talento humano
	SACET	Monitoreo de Llamadas
Vigilancia	NUO	Monitoreo de Seguridad
	ACCESS TOOL	Control Asistencia Administrativo y Docente
ACTIVE DIRECTORY	WIN SERVER 2008	Active Directory
	TIVOLI	Respaldo en cintas
respaldos	FILE SERVER	File Server
DNS	WIN SERVER 2008	Domain Name System
DHCP		Protocolo de Configuración Dinámica de Host
SNMP		Protocolo Simple de Administración de Red o SNMP
FTP		Protocolo de transferencia de archivos
telefonía IP	TELEFONIA	Telefonía a través de red IP
Antivirus	Fsecure	Servidor local antivirus

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Tabla 33. *Servicios y Aplicaciones Adicionales*

SERVICIOS Y APLICACIONES ADICIONALES		
SERVICIOS	APLICACIONES	
Control de Asistencia		Control de Asistencia Estudiantes y Docentes
Aumento a la DMZ	Servidores	Aumento de servidores
Cobertura inalámbrica	Access Point	Aumento en cobertura Inalámbrica
Vigilancia		Aumento de cámaras
Control web	WSA	Web security appliance
Monitoreo de tráfico	Blue Coat	Paket shaper

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Por lo tanto el diseño de red debe dotar a la Universidad Politécnica Salesiana sede Quito campus Sur de sistemas de redundancia y alta disponibilidad de red que impida la caída de los servicios y aplicaciones.

3.7.1. Seguridad a nivel de acls

ACL (access control list), lista de control de acceso es una forma de establecer permisos de acceso apropiados a un determinado objeto, además las ACL permiten aumentar la productividad y la eficiencia de los equipos de red y su principal objetivo es filtrar tráfico de red, por tal motivo en el diseño de red propuesto se ha configuradas ACLs extendidas nombradas en el core las cuales se detalla en el anexo3.

3.7.2. Alta disponibilidad

La alta disponibilidad se refiere a garantizar el grado necesario de continuidad de servicio en que una aplicación o servicio está disponible para que los usuarios puedan utilizarlos en condiciones óptimas y sin interrupciones.

Para medir la disponibilidad se debe tomar en cuenta, que todo sistema debe haber establecido un acuerdo de nivel de servicio (SLA) donde se describa el tiempo y horarios que se debe estar conectado a la red. La disponibilidad de un sistema se la puede calcular mediante la siguiente ecuación.

$$\text{Disponibilidad} = \left(\frac{A - B}{A} \right) \times 100 \%$$

Ecuación 1. Fórmula de la disponibilidad

Esto quiere decir que la disponibilidad es el tiempo activo real para el tiempo esperado por el 100 %, donde:

A= Horas implicadas de disponibilidad o que esta trabajado el sistema

B= Número de horas fuera de servicio o caída del sistema

El valor del resultado se expresará en función de la cantidad de nueves que brinda la solución.

Tabla 34. Acuerdo de nivel de servicio (SLA)

Porcentaje de disponibilidad	Tiempo de inactividad al año	Tiempo de inactividad al mes	Tiempo de inactividad al día
99%	3.7 días	7.3 hrs	14.4 min
99.5%	1.8 días	3.66 hrs	7.22 min
99.9%	8.8 hrs	43.8 min	1.46 min
99.95%	4.4 hrs	21.9 min	43.8 s
99.99%	52.6 min	4.4 min	8.6 s
99.999%	5.26 min	26.3 s	0.86 s

Nota. (Activa, 2014)

Elaborado por: Alejandro Moreno y Andrés Tipán

Cabe aclarar que los porcentajes de disponibilidad que pasan del 99.5 % son difíciles alcanzarlos ya que es necesario invertir más capital en adquisición de equipos para crear redundancia en la red y poder mejorar la disponibilidad.

3.7.2.1 Disponibilidad actual

Para el cálculo de disponibilidad actual en la Universidad Politécnica Salesiana sede Quito campus Sur, se la ha realizado de la siguiente manera.

Se tomó en cuenta SLA de 24x365 para aplicaciones y servicios con mayor disponibilidad y exigencia por ejemplo las cámaras de video vigilancia. Esto quiere decir que son servicios que tienen que estar disponibles las 24 horas del día por los 365 días del año entonces:

$$\text{Disponibilidad} = \left(\frac{A-B}{A} \right) \times 100 \%$$

Donde A = (24x365) = 8.760 Horas/año

Para el cálculo de B que son las horas fuera de servicio se ha tomado en cuenta los siguientes problemas:

- Mantenimiento preventivo 4 horas
- Mantenimiento correctivo no planeado 8 horas
- Migraciones de equipos 6 horas
- Fallas en disco horas 4 horas
- Fallas eléctricas 2 horas

Donde $B = (4+8+6+4+2) = 24$ horas

$$\text{Disponibilidad} = \left(\frac{8.760-24}{8.760} \right) \times 100 \%$$

Disponibilidad = 99,7 %

Lo que significa que el tiempo de inactividad del sistema al año es de 26,3 hrs.

3.7.2.2 Disponibilidad a obtenerse con la propuesta de diseño

Con el presente diseño se quiere conseguir un mayor desempeño de la red para llegar a la disponibilidad del 99.9%, esto quiere decir que el tiempo de inactividad al año sería de 8 a 9 horas, esto con el fin específico del mejoramiento de la red, para satisfacer las necesidades de acceso a los nuevos servicios y aplicaciones que se implementaran en los próximos años en la Universidad Politécnica Salesiana sede Quito campus Sur siendo útil para todos los usuarios.

3.8. Simulador GNS3

GNS3 es un emulador gráfico de enrutadores, el cual permite diseñar topologías de red, configurar dispositivos, insertar paquetes y simulaciones de conectividad todo aquello desde las propias consolas incluidas.

Para ello GNS3 está basado en Dynamips, emulador de routers CISCO, dando soporte a plataformas 1700, 2600, 3600, 3700 y 7200, permitiendo ejecutar imágenes del IOS estándar, esto con el fin de proporcionar simulaciones complejas y precisas.

GNS3 incluye varias características tales como:

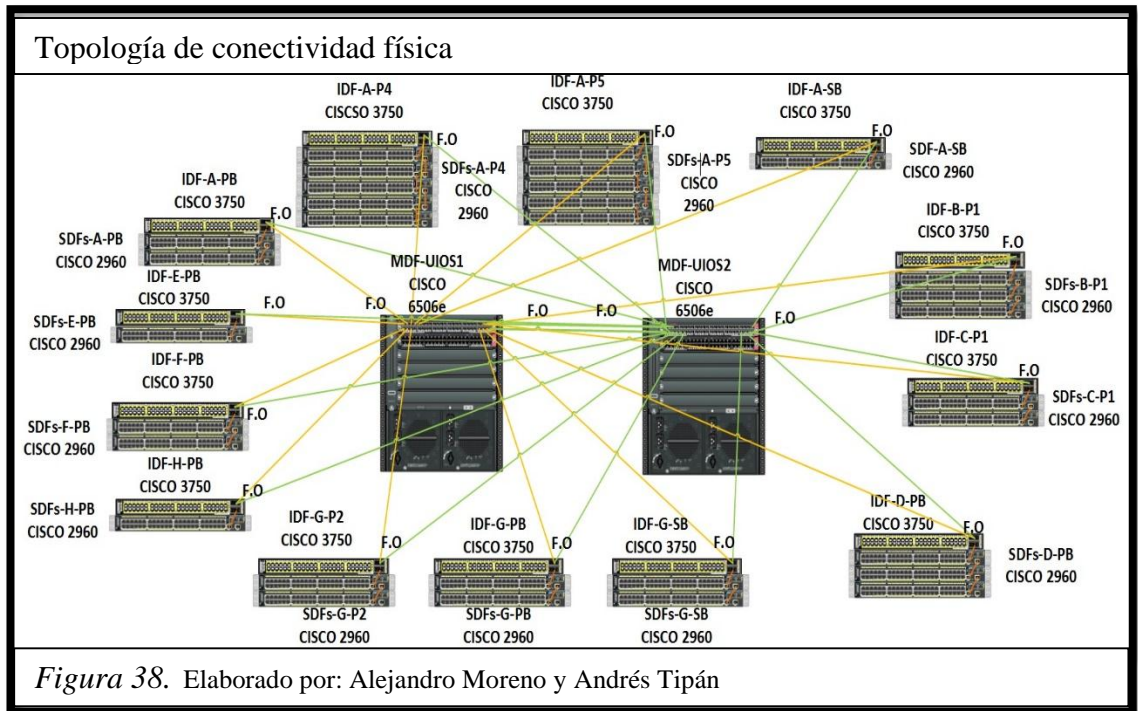
- Captura de paquetes de datos utilizando Wireshark, el cual permite monitorear la red.
- Diseño de alta calidad y topologías de red complejas.
- La emulación de varias plataformas de CISCO IOS del router, IPS, firewalls PIX y ASA.
- Simulación de la simple Ethernet, ATM y Frame Relay interruptores.
- La conexión de la red simulada en la infraestructura real.

Además, GNS3 tiene el propósito de ser usado como un producto educativo, debido a que es un programa gratuito para la enseñanza de cómo funcionan las redes como administraras.

El equipo usado para la simulación de la red de alta disponibilidad es un pc con procesador core i7, con una memoria de 8 GB, esto debido a que el emulador GNS3 consume gran cantidad de memoria por la utilización de los IOS, lo cual permite tener un entorno de trabajo real.

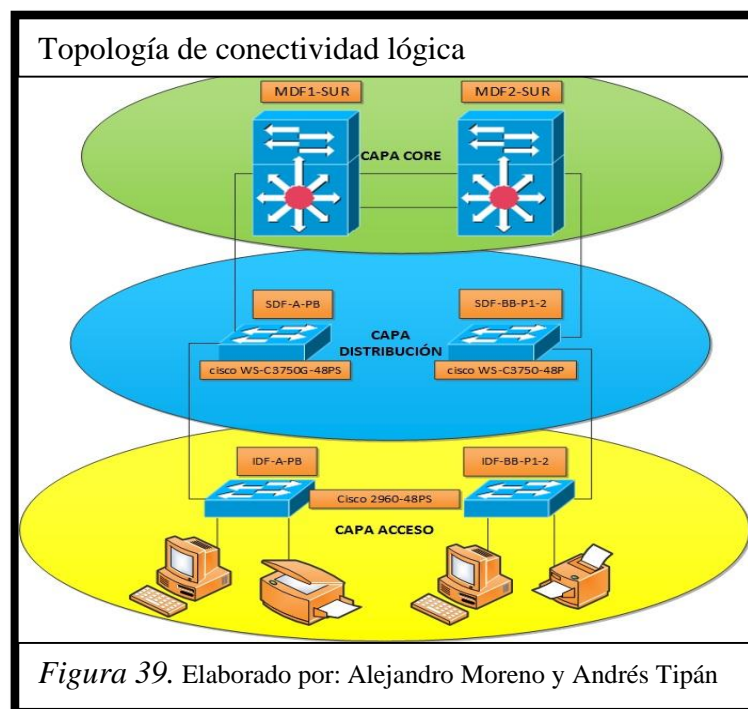
3.8.1 Topología física

La topología física de conectividad que se utiliza en la red de alta disponibilidad es de tipo estrella extendida como se muestra en la figura 38, la propia que está conformada en su mayoría por switch's core-CISCO 6506e, distribución-CISCO 3750, acceso-CISCO 2960, los cuales están conectados a través de fibra óptica (F.O).



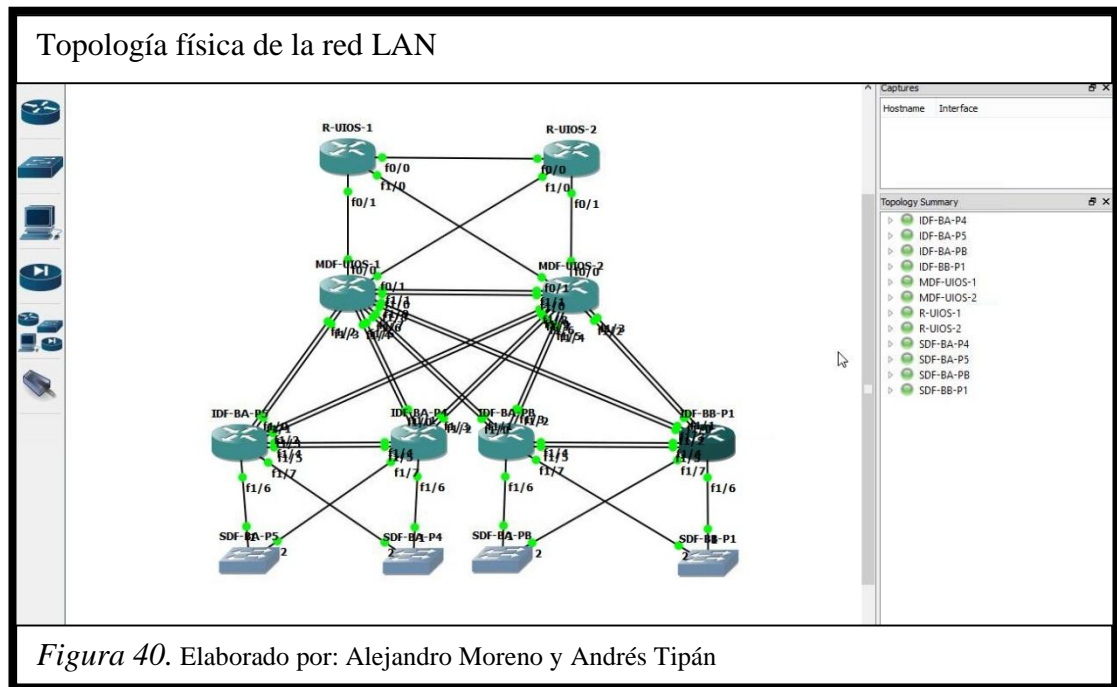
3.8.2 Topología lógica

La topología lógica de conectividad utiliza el diseño de red jerárquico, establecida de acuerdo a la función que desempeña cada uno de los equipos dentro de las capas de diseño de networking como se muestra en la figura 39.



3.8.3 Topología de conectividad en GNS3

La topología de la simulación en GNS3 permitirá conocer cómo están conectados los equipos, con las interfaces de cada uno de los dispositivos que se utilizará para la simulación de la red de alta disponibilidad.



Los dispositivos de infraestructura que se utilizaron en la topología física para la simulación son los siguientes:

- **Router 7200** : Con velocidades de procesamiento de hasta 2 millones de paquetes por segundo, así como un número sin precedentes de servicios IP de alto contacto, ideales para redes WAN / MAN, dispositivo de borde para empresas.
- **Switch 3600**: Con acceso de multiservicios modulares para oficinas de grandes dimensiones, medianas, pequeñas y proveedores de servicios de Internet. Brinda soluciones para datos, vídeo de voz, y enrutamiento de datos multiprotocolo.
- **PC**: Con lo necesario para que soporte la simulación, con un procesador core i7, con una memoria RAM de 8 GB y disco duro de 500gb.

3.9 Configuración de la simulación

GLBP (gateway load balancing protocol) permite balancear la carga determinando diferentes direcciones MAC a una misma IP virtual, esto con la finalidad de tener una manera privilegiada de gestionar redundancia de enrutamiento IP, por esta razón en los equipos de la simulación se configuró el protocolo GLBP, ya que este protocolo permite gestionar redundancia de enrutamiento IP y además posee balanceo de carga el cual permite que todas mis conexiones y equipos estén trabajando de manera óptima.

3.9.1. Pasos detallados de la configuración de GLBP

Paso 1: enable, habilita el modo EXEC privilegiado.

Ejemplo:

```
MDF-UIOS > enable
```

Paso 2: configure terminal, entra en el modo de configuración global.

Ejemplo:

```
MDF-UIOS # configure terminal
```

Paso 3: interface type number, especifica un tipo de interfaz y el número, y entra en el modo de configuración de interfaz.

Ejemplo:

```
MDF-UIOS (config)# interface vlan 2
```

Paso 4: ip address *ip-address mask* [**secondary**], especifica una dirección IP primaria o secundaria para una interfaz.

Ejemplo:

```
MDF-UIOS (config-if)# ip address 172.17.1.254 255.255.255.0
```

Paso 5: glbp group timers [**msec**] *hellotime* [**msec**] *holdtime*, configura el intervalo entre los paquetes sucesivos de saludo enviados por el AVG (Active Virtual Gateway) en un grupo GLBP

Ejemplo:

```
MDF-UIOS config-if# glbp 2 timers 5 18
```


- El tiempo de mantenimiento argumento específica el intervalo en segundos antes de que la puerta de entrada virtual y promotor de la información virtual en el paquete de saludo se considera válido.
- El opcional (msec) palabra clave especifica que el siguiente argumento se expresará en milisegundos, en lugar de los segundos predeterminados.

Paso 6: `glbp group timers redirect redirect timeout`, configura el intervalo de tiempo durante el cual el AVG (Active Virtual Gateway) continúa para redirigir a los clientes a una AVF(Active Virtual Forward). El valor predeterminado es 600 segundos (10 minutos).

Ejemplo:

```
MDF-UIOS (config-if)# glbp 2 timers redirect 1800 28800
```

- El tiempo de espera argumento específica el intervalo en segundos antes de que un promotor virtual secundario deja de ser válida. El valor predeterminado es 14.400 segundos (4 horas).

Nota

- El valor cero para la redirección argumento no se puede quitar de la gama de valores aceptables porque las configuraciones preexistentes del software Cisco IOS que ya utilizan el valor cero podrían verse afectados negativamente durante una actualización. Sin embargo, no se recomienda un ajuste de cero y, si se usa, se traduce en un temporizador de redireccionamiento que nunca caduca. Si el temporizador de redirección no caduca, y el dispositivo falla, sigan asignadas al dispositivo que ha fallado en lugar de ser redirigido a la copia de seguridad nuevos huéspedes.

Paso 7: `glbp group load-balancing [host-dependent | round-robin | weighted]`, especifica el método de balanceo de carga utilizado por la GLBP.

Ejemplo:

```
MDF-UIOS (config-if)# glbp 2 load-balancing host-dependent
```

Paso 8: `glbp group priority level`, establece el nivel de prioridad de la puerta de entrada dentro de un grupo GLBP.

Ejemplo:

```
MDF-UIOS (config-if)# glbp 10 priority 254
```

- El valor predeterminado es 100.

Paso 9: `glbp group preempt [delay minimum seconds]`, configura el dispositivo para asumir como Active Virtual Gateway para un grupo GLBP si tiene una prioridad más alta que la actual de Active Virtual Gateway.

Ejemplo:

```
MDF-UIOS (config-if)# glbp 2 preempt delay minimum 60
```

- Este comando está desactivado por defecto.
- Use la opción de retardo y mínimos de palabras clave y el segundo argumento para especificar un intervalo mínimo de retardo en segundos antes de que el sobreseimiento de la Active Virtual Gateway se lleva a cabo.

Paso 10: `glbp group client-cache maximum number [timeout minutes]`, Utilice el número de argumento para especificar el número máximo de clientes que el caché celebrará para este grupo GLBP. El rango es de 8-2000

Ejemplo:

```
MDF-UIOS (config-if)# glbp 2 client-cache maximum 1200 timeout 245
```

(Opcional) Activa la caché del cliente GLBP.

- Este comando está desactivado por defecto.
- Use la opción de tiempo de espera minuto palabra clave y los argumentos para configurar la cantidad máxima de tiempo que una entrada de cliente puede permanecer en la caché del cliente GLBP después de la información de los clientes de la última actualización. El rango es de 1 a 1440 minutos (un día).

Nota

- Para las redes IPv4, Cisco recomienda establecer un valor de tiempo de espera caché del cliente GLBP que es ligeramente más largo que el máximo esperado al valor de tiempo de espera de caché por el Protocolo de resolución de direcciones (ARP).

Paso 11: `glbp group name redundancy-name`, permite redundancia IP mediante la asignación de un nombre al grupo GLBP

Ejemplo:

```
MDF-UIOS (config-if)# glbp 2 name abc123
```

- El cliente redundancia GLBP debe configurarse con el mismo nombre de grupo GLBP para que el cliente la redundancia y el grupo GLBP pueden conectarse.

Pasó 12: exit, sale del modo de configuración de interfaz, y devuelve el dispositivo al modo de configuración global

Ejemplo:

```
MDF-UIOS (config-if)# exit
```

Pasó 13: no glbp sso, (Opcional) Desactiva apoyo GLBP de SSO.

Ejemplo:

```
MDF-UIOS (config)# no glbp sso
```

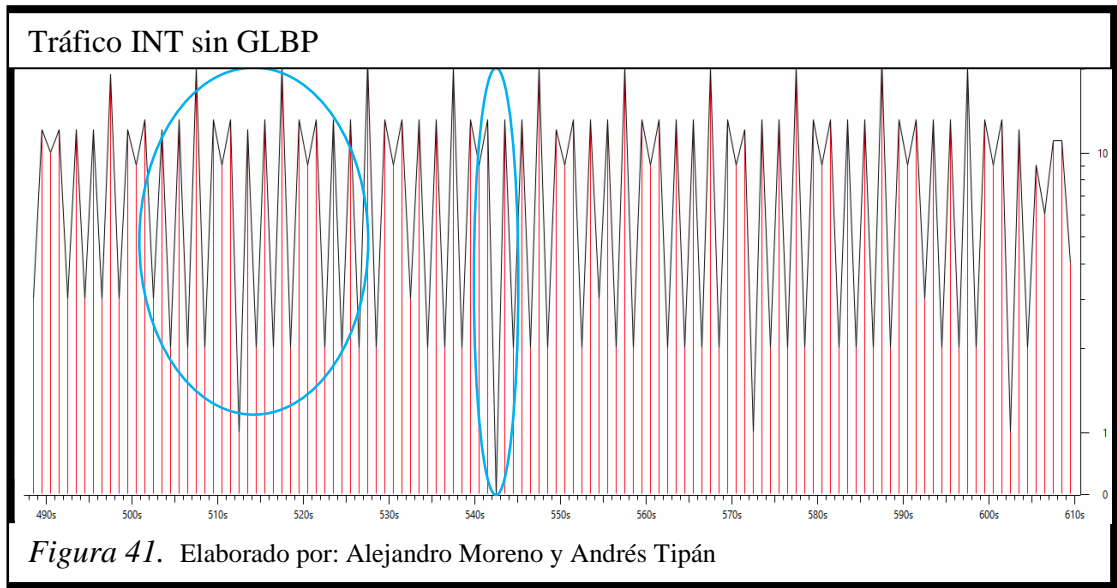
3.9.2. Configuración de dispositivos

En la consola de los dispositivos se podrá observar las configuraciones que se han utilizado en cada uno de los dispositivos de la simulación y como están funcionando cada uno de estos. Esto se encuentra en el Anexo 4.

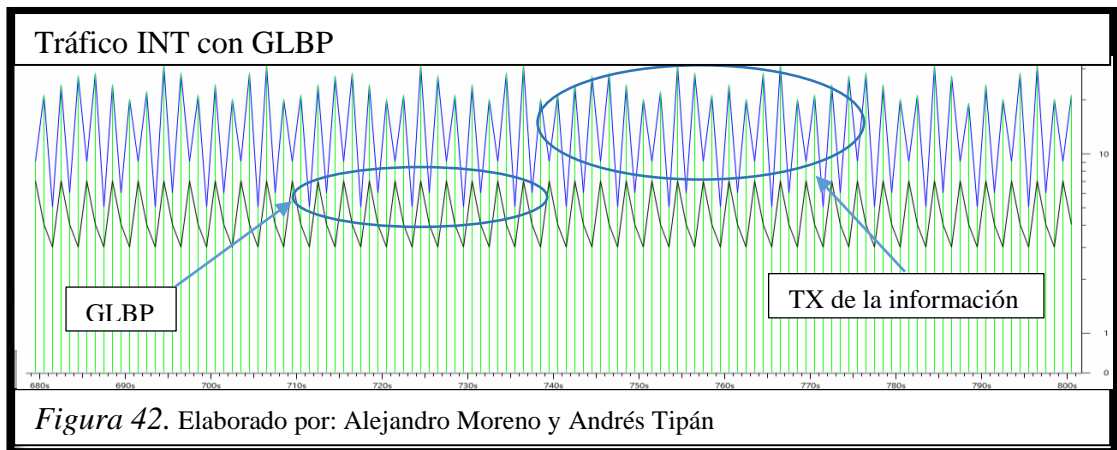
3.9.3. Análisis de resultados

A continuación en la figura 41 se observa el tráfico desde el enlace de distribución y acceso sin GLBP, haciendo ping de host a host dentro de la red de campus con carga de 1554 y con un número de paquete aproximado de 1000 donde se observa un flujo de tráfico constante pero desordenado e incluso existen pérdidas, por tal motivo se observa los picos y valles.

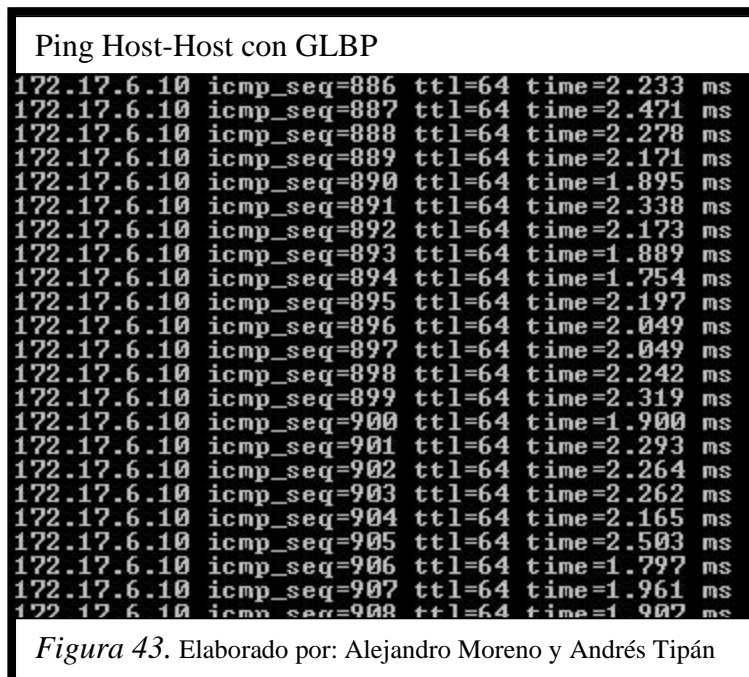
Con el propósito de evitar picos y valles en el tráfico de red, STP reconfigura la red y redirecciona las rutas de datos a través de la activación de la ruta en espera.



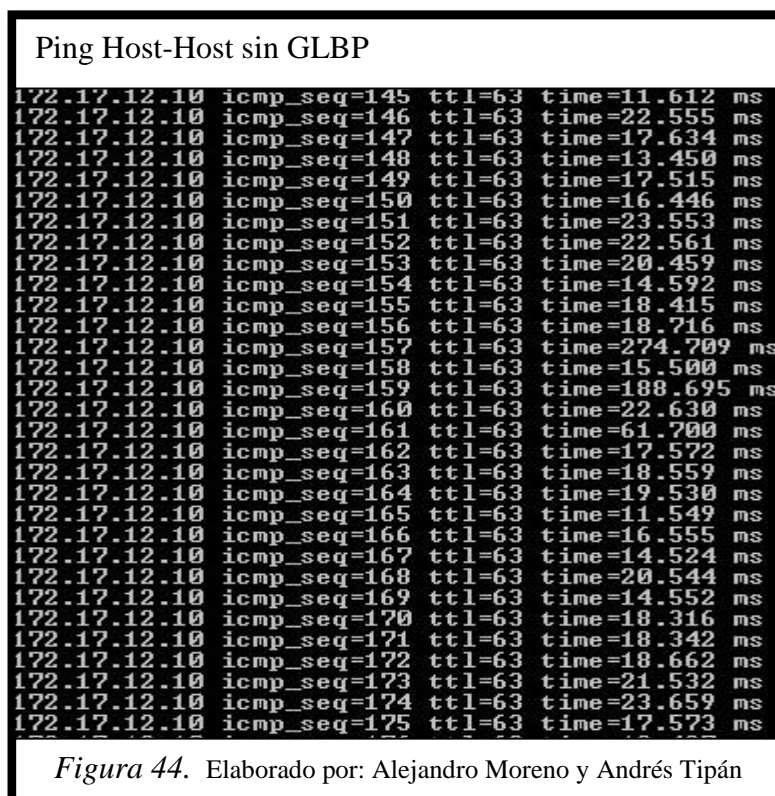
A continuación en la figura 42 se observa el tráfico desde el enlace de distribución y acceso con GLBP, haciendo ping de host a host dentro de la red de campus con carga de 1554 y número de paquete aproximado de 1000, donde se observa que el uso del protocolo GLBP durante toda la transmisión de la información realiza balanceo de carga, por lo tanto no existe pérdidas considerables obteniendo un flujo de información estable.



La figura 43 es una muestra del ping realizado de host-host donde se observa un tiempo de respuesta considerablemente bajo con una media de 2.135(ms) utilizando GLBP.



La figura 44 es una muestra del ping realizado de host-host sin GLBP donde se observa un tiempo de respuesta considerablemente alto con respecto al obtenido el cual tiene una media de 38.219(ms).

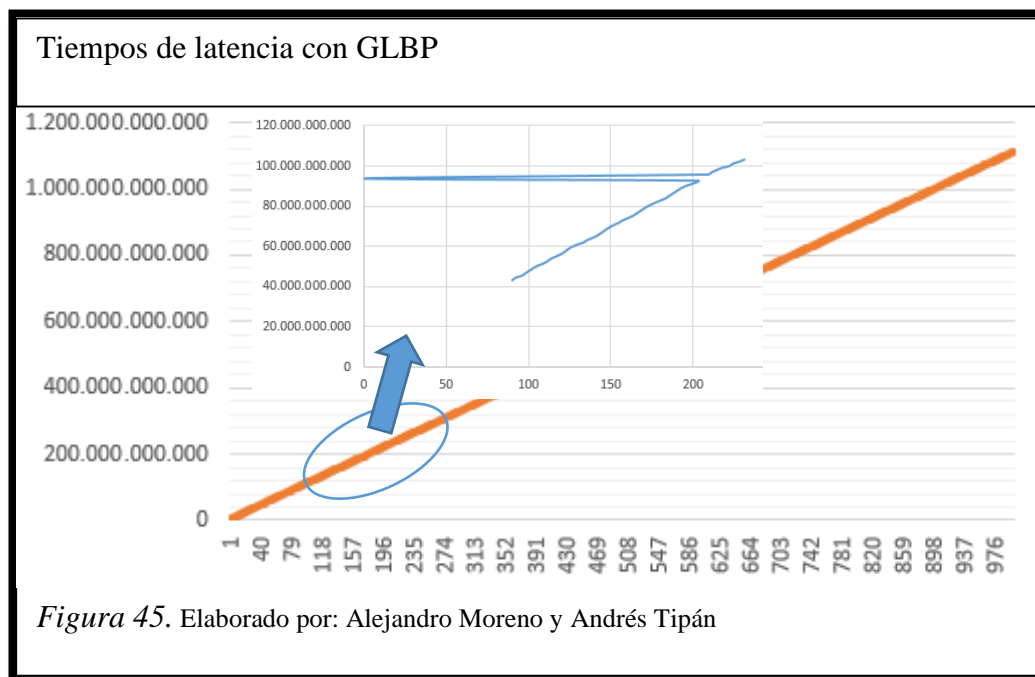


En el análisis de resultados se observa el funcionamiento de la red de alta disponibilidad con las configuraciones de STP (spanning tree protocol), que evita se formen bucles en topologías de red debido a la presencia de enlaces redundantes que son necesarios para tener una alta disponibilidad del servicio, además

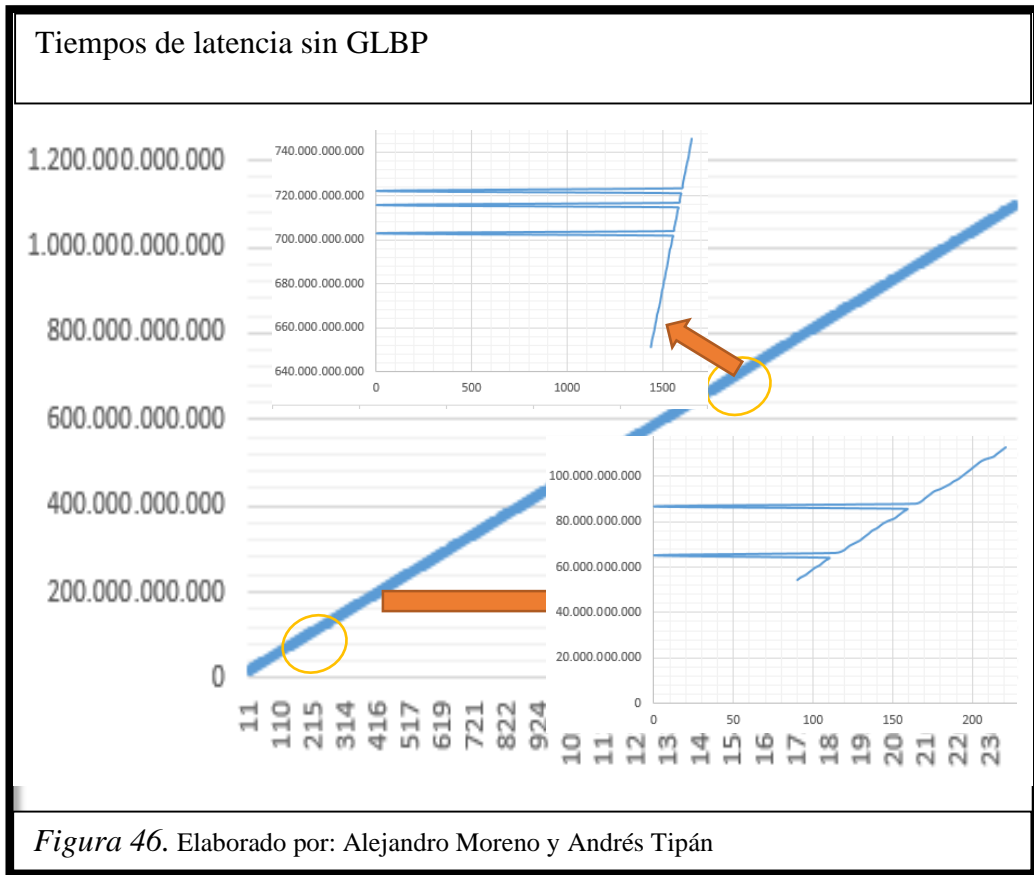
El uso de GLBP con su Active Virtual Gateway (AVG) ayuda a que no existan o disminuyan considerablemente las pérdidas de paquetes a través de la red usada.

En el análisis de resultados se utilizó el software wireshark, que es un analizador de paquetes de red que permite la captura de tramas y paquetes que transitan por las interfaces de red.

En las figuras 45 y 46 se observa la relación de tiempo versus número de paquetes en los cuales se puede apreciar prácticamente una línea recta, esto ocurre porque al momento de graficarla descarta los paquetes que pasan por cero ya que son despreciables.



En la figura 45, se encuentra un intervalo pequeño donde se observar el único pasó por cero o paquete perdido, los demás puntos se encuentran oscilando en la línea recta ya que sus diferencias son mínimas.



En la figura 46, se encuentran dos intervalos pequeños donde se observan los pasos por cero o paquetes perdidos, los demás puntos se encuentran oscilando en la línea recta a pesar que sus diferencias son mayores como se lo indica en la figura 44.

CAPÍTULO 4

DISEÑO DE LA RED LAN

En el presente capítulo, se realizará un análisis técnico-económico tomando en cuenta las áreas para las alternativas de diseño propuestas en el capítulo anterior. Además se incluye un análisis económico de la solución desarrollada, con el objetivo de conseguir una proximidad de los precios existentes en el mercado nacional.

Finalmente se incluyen las conclusiones y recomendaciones procedentes del presente estudio, para comprender varios aspectos importantes relacionados con el diseño de la red LAN donde se incluirán anexos que permitan visualizar de manera adecuada la mejora realizada por este proyecto.

4.1. Análisis técnico

En este análisis se procederá a establecer las características primordiales de orden técnico para la adquisición de equipos CISCO planteadas para el diseño de red de alta disponibilidad para la Universidad Salesiana sede Quito campus Sur.

Tabla 35. *Análisis de las características primordiales de orden técnico*

Factores determinantes del éxito	Peso	Calificación	Ponderación
Fortalezas			
Equipamiento de infraestructura de red a nivel mundial	0.1	4	0.4
Documentación clara y muy difundida.	0.04	2	0.08
Nivel de core muy usado en Latinoamérica.	0.1	3	0.3
Tiene varios socios a nivel nacional. (IBM, SINETCOM, DESCA, entre otros)	0.1	3	0.3
Calidad superior y certificación	0.1	4	0.4

Debilidades			
Constante desarrollo de tecnología	0.1	2	0.2
Costo de sus equipos	0.2	3	0.6
Aumento de calidad de servicios nuevos	0.06	1	0.06
Las licencias tienen un precio alto	0.2	3	0.6
Total	1		2.94

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Como se observa en la tabla 35 el valor del peso ponderado es de 2.94, lo cual establece que si la calificación supera a 2.5 la atractivita del proyecto es favorable.

4.2. Beneficios primordiales de orden técnico

El diseño de red de alta disponibilidad tiene un fin específico, el mejoramiento de la red de datos para satisfacer las necesidades de acceso a los nuevos servicios y aplicaciones que se implementaran en los próximos años en la Universidad Politécnica Salesiana sede Quito campus Sur siendo útil para todos los usuarios ya que permitirá:

- Mejorar los procesos de matrículas, administración de red, video conferencias, acceso a bases de datos, etc.
- Optimizar el acceso a consultas en la biblioteca y aulas virtuales, para beneficio de los estudiantes de la Universidad Politécnica Salesiana con el fin de brindar una mejor calidad de educación.
- Ofrecer las condiciones necesarias en las aulas como en los laboratorios de la Universidad Politécnica Salesiana, de tal forma que se garantice una educación acorde a los requerimientos actuales.

4.3. Análisis económico

En la planificación para la red de alta disponibilidad se ha realizado un análisis económico para conocer la rentabilidad y factibilidad del mismo, además con este análisis se podrá determinar qué tan rentable es el proyecto antes de una toma de decisiones referentes a actividades de inversión.

4.3.1 Valores referenciales

En la tabla 36 se mostrará los costos referenciales de equipamiento, esto tiene como objetivo el mostrar una idea del precio que podrá alcanzar el proyecto antes de tomar una decisión.

Resumen de costos

Tabla 36. *Costos referenciales de equipamiento cisco*

Producto	Precio Unit.	Unidad	Total
Requerimiento actual de Switches de core			
CISCO 6506 chasis	18.017,00	2	36034
Requerimiento actual de Switches de distribución			
CISCO 3750	4.555,00	12	54660
Requerimiento actual de Switches de acceso			
CISCO 2960	2.285,00	29	66265
Requerimiento actual de antenas exteriores			
CISCO aironet 1520 outdoor	2.199,00	9	19791
Requerimiento actual de antenas interiores			
CISCO aironet 2600 input	483,00	42	20286
Requerimiento actual dispositivos de gestión de red			
CISCO 2500 wireless controller	5.895,00	1	5895
Requerimiento actual dispositivos de seguridad			
CISCO asa 5515-x	5.084,00	1	5084

CISCO s380 web security appliance	8.992,04	1	8992,04
CISCO 2801	838,00	2	1676
Total en equipos			218.683,04

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

En las tablas 37 y 38, se mostrará los costos referenciales de los enlaces de datos e internet cuyos valores fueron obtenidos de cotizaciones de los proveedores de la Universidad Politécnica Salesiana.

Tabla 37. Costos referenciales de enlaces de Internet

Proveedor	Localidad	Medio físico	Interfaz	Ancho de banda (kbps)	Renta mensual servicio
Andinanet	U.P.S	F.O.	RJ45	4076	\$ 4.000,00
Telconet	U.P.S	F.O.	RJ45	4076	\$ 4.000,00
Total sin impuestos					\$ 4.000,00
IVA (12%)					\$ 480
Total					4.480,00

Nota. (Juan Carlos Dominguez, 2008, pág. 169)

Tabla 38. Costos referenciales de enlaces de Datos

Campus A	Campus B	Tipo	Medio físico	Interfaz	Ancho de banda (kbps)	Inscripción e instalación	Renta mensual servicio
Girón UPS Quito	Sur UPS Quito	Local	TDM	F.O.	2048	900	700.00
Total sin impuestos							700.00
IVA (12%)							84.00
Total							784.00

Nota. (Juan Carlos Dominguez, 2008, pág. 169)

Tabla 39. Análisis Económico

	año 0	año 1	año 2	año 3	año 4	año 5	año 6	año 7	año 8	año 9	año 10
Ingresos											
Número de viajes ahorrados		83	85	88	90	93	96	99	102	105	108
Costo por viaje		390	390	390	390	390	390	390	390	390	390
Ahorros por viajes		32.271,65	33.239,80	34.236,99	35.264,10	36.322,02	37.411,68	38.534,03	39.690,06	40.880,76	42.107,18
Número de minutos		365.678,52	376.684,87	387.948,34	399.586,79	411.574,39	423.921,63	436.639,27	449.738,45	463.230,61	477.127,52
Costo minuto		0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02
Ahorro en telefonía		7.313,57	7.532,98	7.758,97	7.991,14	8.231,49	8.478,43	8.732,79	8.994,77	9.264,61	9.542,55
Ahorros duplicación hardware	65.525,19										
Ahorro mantenimiento		7.901,87	7.901,87	7.901,87	7.901,87	7.901,87	7.901,87	7.901,87	7.901,87	7.901,87	7.901,87
Total de ahorros previstos	65.525,19	47.487,09	48.674,65	49.879,83	51.157,71	52.455,38	53.791,99	55.168,69	56.586,69	58.047,24	59.551,60
Ingreso por valor de desecho					14.878,37						
Total Ingresos	65.525,19	47.487,09	48.674,65	49.897,83	66.035,48	52.455,38	53.791,99	55.168,69	56.586,69	58.047,24	59.551,60
	año 0	año 1	año 2	año 3	año 4	año 5	año 6	año 7	año 8	año 9	año 10
Egresos											
Inversion en equipos	218.683,04										
Inversion por instalacion telf											
Inversion por instalacion datos	100										
Inversion por instalacion internet	100										
Inversion en capital de trabajo	1000										
Gastos en capacitación		4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00	4.000,00
Gastos enlace de datos		47.040,17	48.451,37	49.904,91	51.402,06	52.944,12	54.532,45	56.168,42	57.853,47	59.589,08	61.376,75
Gastos movilizaciones		1.040,00	1.040,00	1.040,00	1.040,00	1.040,00	1.040,00	1.040,00	1.040,00	1.040,00	1.040,00
Total Egresos	219.883,04	52.080,17	53.491,37	54.944,91	56.442,06	57.984,12	59.572,45	61.208,42	62.893,47	64.629,08	66.416,75
FLUJO NETO	-154.357,85	-4.593,08	-4.816,72	-5.047,08	9.593,42	-5.528,74	-5.780,46	-6.039,73	-6.306,78	-6.581,84	-6.865,15
	año 0	año 1	año 2	año 3	año 4	año 5	año 6	año 7	año 8	año 9	año 10
Ahorros Intangibles											
Ahorro en dólares		71.643,14	73.792,43	76.006,21	78.286,39	80.634,99	83.054,03	85.545,66	88.112,03	90.755,39	93.478,05
Flujo con ahorros intangibles	-154.357,85	76.236,22	78.609,15	81.053,29	68.692,97	86.163,73	88.834,49	91.585,38	94.418,80	97.337,22	100.343,20
Calculo del VAN	\$ 65.775,87										
Calculo del TIR	50%										

Nota. (DOMÍNGUEZ AYALA JUAN CARLOS, 2008, pág. 188)

El presupuesto referencial, se lo realizó con un sobredimensionamiento de los equipos pensando en una expansión futura de la red de 3 a 10 años en la Universidad Politécnica Salesiana sede Quito campus Sur con la finalidad de obtener equipos adicionales por cualquier aspecto emergente. Además se realizará los cálculos del flujo de caja para obtener el VAN (valor neto actual) y TIR (Tasa interna de retorno), con el propósito de ver la viabilidad de la red propuesta.

$$VAN = \sum_{t=1}^n \frac{Vt}{(1+k)^t} - I_0$$

Ecuación 2. Fórmula del VAN

$$TIR = \frac{-I + \sum_{i=1}^n Fi}{\sum_{i=1}^n i * Fi}$$

Ecuación 3. Fórmula del TIR

Tabla 40. Interpretación del VAN y TIR

Fórmula	Interpretación
VAN	<p>VAN > 0; la inversión produce ganancias</p> <p>VAN < 0; la inversión produce pérdidas</p> <p>VAN = 0; la inversión no produce ni pérdidas ni ganancias</p>
TIR	<p>TIR ≥ r; se aceptara el proyecto</p> <p>TIR < r; se rechazara el proyecto</p>

Nota. Elaborado por: Alejandro Moreno y Andrés Tipán

Al realizar el análisis económico del proyecto, se observa en la tabla 39 que el VAN (valor neto actual) es un valor positivo, lo que significa que la inversión que se requiere para la implementación de la red de alta disponibilidad es completamente justificada.

CONCLUSIONES

- Después de realizar el análisis técnico-económico de la nueva infraestructura de red, se concluye que todos los bloques de la Universidad Politécnica Salesiana Sede Quito Campus Sur podrán contar con un servicio de red de alta disponibilidad gracias a la topología tipo estrella extendida que se diseñó y simuló entre los Switches de Core y los Switch de Acceso mediante el protocolo spanning-tree el cual controla los enlaces redundantes de la topología mencionada.
- En base al análisis realizado de la red simulada, se observó de manera detallada gráficas estadísticas indicado la mejorar que se obtuvo a través de enlaces redundantes y con la implementación del protocolo GLBP, siendo esto de ayuda para observar el funcionamiento de la red propuesta vs la red actual ya que GLBP es una manera privilegiada de gestionar redundancia de enrutamiento IP y está diseñado para permitir una administración transparente de la puerta de enlace predeterminada, además GLBP posee balanceo de carga el cual permite que todas las conexiones y equipos estén trabajando de manera óptima.
- La importancia de una red de alta disponibilidad en la actualidad propone diferentes retos para la administración de la información y las comunicaciones por la cual es necesario que permita la integración de aplicación o sistema de servicios que ayude a cumplir con los requerimientos de los usuarios, por tal motivo la inversión que se requiere para la implementación de la red de alta disponibilidad es justificable por los beneficios que brindará la misma, como la escalabilidad, mayor velocidad, mayor seguridad, accesibilidad total, mejor administración, entre otras ventajas que brindará esta red.

RECOMENDACIONES

- Se recomienda se haga uso del protocolo llamado VSS (virtual switching system) en el core CISCO 6506 e, ya que permite comunicar los MDF a velocidades de transmisión aproximada de 10 Gbps, además de crear un equipo virtual que me permite tener una administración unificada, esto con la finalidad de eliminar uno de los puntos simples de falla, es decir que si un equipo deja de funcionar en la red los host no lo notarían porque el Gateway que se crea es virtual.
- En la configuración del protocolo GLBP se debe tomar en cuenta que previo a su configuración la red debe estar funcionando al 100%, es decir con el uso de STP y los protocolos de enrutamiento (OSPF, EIGRP y rutas estáticas).
- En caso de adquirir nuevos equipos de conectividad, se recomienda la verificación de los IOS y compatibilidad con el equipamiento puesto en la infraestructura de red propuesta por la red de alta disponibilidad.
- Es importante implementar políticas de seguridad internas que estén acordes al nuevo equipamiento e infraestructura de red, y de esta manera poder evitar que usuarios no autorizados puedan acceder a las configuraciones y cambiarlas.
- Se recomienda el cambio del cableado estructurado existente dado que el tiempo de vida útil de 10 años estaría por culminar y este debe soportar de 2 a 3 generaciones de equipos activos sin generar pérdidas ni atenuaciones por lo cual se recomienda cambiar a un cableado actual certificado para poder aprovechar de mejor manera la nueva infraestructura de la red LAN en la Universidad Politécnica Salesiana Sede Quito Campus Sur.
- Se recomienda que a futuro se realice investigaciones acerca de las nuevas tecnologías inalámbricas tales como: IrDA, Wi-Max, SMART WIRELESS, ya que el uso de redes inalámbricas proporciona mayores ventajas que las redes cableadas.

LISTA DE REREFERENCIAS

- Borja, R., & Jarrín, J. (2014). *Implementación e integración de la red wlan de la Universidad Politécnica Salesiana (ups), Sede Quito-Campus Sur, al proyecto internacional EDUROAM*. Quito.
- CISCO. (18 de 06 de 2014). *First Hop Redundancy Protocols Configuration Guide, Cisco IOS Release 15M&T*. Obtenido de Contents:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp-gshut.html
- CISCO. (12 de 1 de 2015). *Cisco Catalyst 2960 Series Switches*. Obtenido de <http://www.cisco.com/c/en/us/products/switches/catalyst-2960-series-switches/index.html>
- CISCO. (12 de 1 de 2015). *Cisco Catalyst 3750 Series Switches*. Obtenido de <http://www.cisco.com/c/en/us/products/switches/catalyst-3750-series-switches/index.html>
- CISCO. (12 de 1 de 2015). *Cisco Catalyst 6506-E Switch*. Obtenido de <http://www.cisco.com/c/en/us/products/switches/catalyst-6506-e-switch/index.html>
- CISCO. (21 de 01 de 2015). *GLBP - Gateway Load Balancing Protocol*. Obtenido de http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html
- Domínguez Ayala, Juan Carlos, c. I. (2008). *Análisis y diseño técnico económico de la red de interconexión de las redes en los Campus Girón, Sur, Kennedy y Cayambe de la Universidad Politecnica Salesiana Sede Quito*. Quito.
- Educacion.ucv.cl. (15 de 06 de 2014). Obtenido de Diseño de redes:
http://educacion.ucv.cl/prontus_formacion/site/artic/20070627/asocfile/ASOCFILE220070627174213.pdf
- Felipe, M. Á. (15 de 06 de 2014). *Implantación de soluciones de Alta Disponibilidad*. Obtenido de Seguridad y Alta Disponibilidad:
<http://mgarciafelipe.files.wordpress.com/2012/03/ud-6-implantacion-de-soluciones-de-alta-disponibilidad-miguelangelgarcia.pdf>

Kenneth D. Stewart III, A. A. (2009). *Diseño y soporte de redes de computadoras*.
Madrid (España): PEARSON EDUCACIÓN, S.A.

McGraw-Hill, O. M. (2002). *Manual de referencia Redes*. Madrid (España):
INTERAMERICANA DE ESPAÑA, S.A.U.

ANEXOS

Anexo 1. Análisis de necesidades de renovación de equipos de cómputo (pc) de la Sede Quito Campus Sur

Dirección técnica de tecnologías de la información

Renovación de equipos de escritorio (Computadoras) para laboratorios, administrativos y personal docentes de dedicación a la UPS sede Quito.

a. Tabla de resumen. Número de personal docente a tiempo completo de la Sede-Quito

Rol	Campus	Dedicación	Subtotal
Docente	Sur	Exclusiva o tiempo completo	35

A continuación en la tabla siguiente usted puede visualizar datos en detalle con el número de máquinas Core i5, i7, i3 y dual Core. De los docentes tiempo completo instalados actualmente en la sala de profesores.

Tabla resumen	
MAQ. SEDE-QUITO	SUBTOTAL
I5-I7-I3	43
DUAL CORE	34
TOTAL	77

En esta tabla puede visualizar el número de máquinas restando las que actualmente estas instaladas (i3, i5, i7).

Referencias:

DOCENTES-TC: Total de Docentes a tiempo completo

DOCENTES-M: total de máquinas (I3, I5, I7) instaladas actualmente en la sala de profesores.

Descripción	Subtotal
DOCENTES-TC	390
DOCENTES-M	43
TOTAL	347

b. Detalle la ubicación de equipos en los laboratorios.

Descripción máq.	Campus-áreas	# Lab	Número
Core 2 Quad	SUR-SECASIS	6	28
Core 2 Quad	SUR-SECASIS	8	28
Core 2 Quad	SUR-SECASIS	13	28
		Total	84
Core 2 Quad	SUR-ELECTRÓNICA	ANALÓGICA	
Core 2 Quad	SUR-ELECTRÓNICA	ELÉCTRICA	
Core 2 Quad	SUR-ELECTRÓNICA	AUTOMATIZACIÓN	
Core 2 Quad	SUR-ELECTRÓNICA	TELECOMUNICACIONES	
Core 2 Quad	SUR-ELECTRÓNICA	MPS	
Core 2 Quad	SUR-ELECTRÓNICA	CONTROL	
	SUR-ELECTRÓNICA	CIR. ELÉCTRICOS	
	SUR-ELECTRÓNICA	INST. CIVILES	
	SUR-ELECTRÓNICA	INST. INDUSTRIALES	
	SUR-ELECTRÓNICA	ELECT. DE POTENCIA	
		Total	
Pentium 4	SUR-AMBIENTAL	QUIMICA ANALÍTICA 2	
Pentium 4	SUR-AMBIENTAL	QUIMICA ANALÍTICA 1	
		Total	

Tabla de resumen. Número de máquinas de c/laboratorios por áreas de la Sede-Quito

Tabla de resumen

Campus	Áreas	Subtotal
Sur	SECASIS	84
Sur	Eléctrica	33
Sur	Ambiental	2

c. Tabla en detalle de equipos para el área administrativa.

Descripción maq.	Campus	Campus-lab	Número
Core 2 duo	Sur	Administrativos	5

Tabla de resumen área administrativa.

Tabla de resumen personal administrativo		
Campus	Descripción	Subtotal
Sur	Administrativos.	5

Resumen

- El número total, de máquinas para los laboratorios de la Sede-Quito es: 336 computadoras.
- El número de máquinas para usuarios administrativos sede-Quito es: 68 computadoras.
- El número de docentes a tiempo completo de la Sede-Quito es: 347 equipos para docentes.
- El número de equipos para STOCK recomendados son 19 equipos
- El número total de equipos a adquirir en la sede Quito son: 7

Números de usuarios conectados en las redes inalámbricas 12 PM

License Level	base
System Name	WLCUIOS
Up Time	380 days, 16 hours, 28 minutes
System Time	Thu Apr 24 10:05:38 2014
Internal Temperature	+27 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	UIOS
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 1%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	● 1	● 0	Detail
802.11b/g/n Radios	12	● 12	● 0	Detail
All APs	12	● 12	● 0	Detail

Client Summary

Current Clients	354	Detail
Excluded Clients	1	Detail
Disabled Clients	0	Detail

Top WLANs

Profile Name	# of Clients	
WLAN-UPS-ESTUDIANTES	248	Detail
WLAN-UPS-DOCSUR	80	Detail
WLC-BIBLIOTECA-UIOS	15	Detail
RED-ADM	4	Detail
GIETEC	3	Detail

Most Recent Traps

User DOCENTE logged Out. Client MAC:d4:cb:af:01:77:ea, Client IP:172.17.131.68, AP MAC:00:1f:c2:00:00:00
Coverage hole pre alarm for client[1] 8c:7b:9d:be:8e:df on 802.11b/g interface of AP 00:1f:c2:00:00:00

User DOCENTE logged Out. Client MAC:4c:3c:16:6d:7e:a6, Client IP:172.17.130.133, AP MAC:00:1f:c2:00:00:00
Coverage hole pre alarm for client[1] 8c:7b:9d:be:8e:df on 802.11b/g interface of AP 00:1f:c2:00:00:00

Coverage hole pre alarm for client[1] a8:26:d9:94:5e:45 on 802.11b/g interface of AP 54:75:00:00:00:00

[View All](#)

This page refreshes every 30 seconds.

License Level	base
System Name	WLCUIOS
Up Time	384 days, 17 hours, 37 minutes
System Time	Mon Apr 28 11:15:08 2014
Internal Temperature	+28 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	UIOS
CPU(s) Usage	0%
Individual CPU Usage	0%/0%, 1%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	● 1	● 0	Detail
802.11b/g/n Radios	12	● 12	● 0	Detail
All APs	12	● 12	● 0	Detail

Client Summary

Current Clients	299	Detail
Excluded Clients	1	Detail
Disabled Clients	0	Detail

Top WLANs

Profile Name	# of Clients	
WLAN-UPS-ESTUDIANTES	213	Detail
WLAN-UPS-DOCSUR	59	Detail
WLC-BIBLIOTECA-UIOS	15	Detail
GIETEC	4	Detail
WLAN-ADMV2	3	Detail

Most Recent Traps

Coverage hole pre alarm for client[1] 50:ea:d6:5d:71:86 on 802.11b/g interface of AP 00:3a:00:00:00:00

Coverage hole pre alarm for client[1] b8:03:05:d9:21:0f on 802.11b/g interface of AP 00:3a:00:00:00:00

Coverage hole pre alarm for client[1] 20:54:76:58:69:8b on 802.11b/g interface of AP 00:3a:00:00:00:00

Coverage hole pre alarm for client[1] f0:6b:ca:da:bf:3d on 802.11b/g interface of AP 00:3a:00:00:00:00

Client Excluded: MACAddress:c8:3d:97:bd:ff:5b Base Radio MAC :00:1f:ca:cb:23:00 Slot: 0

[View All](#)

This page refreshes every 30 seconds.

Números de usuarios conectados en las redes inalámbricas 5 PM

License Level	base
System Name	WLCUIOS
Up Time	367 days, 22 hours, 17 minutes
System Time	Fri Apr 11 15:54:32 2014
Internal Temperature	+31 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	UIOS
CPU(s) Usage	1%
Individual CPU Usage	0%/0%, 3%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	2	● 2	● 0	Detail
802.11b/g/n Radios	13	● 13	● 0	Detail
All APs	13	● 13	● 0	Detail

Client Summary

Current Clients	84	Detail
Excluded Clients	1	Detail
Disabled Clients	0	Detail

Top WLANs

Profile Name	# of Clients	
WLAN-UPS-ESTUDIANTES	48	Detail
WLAN-UPS-DOCSUR	14	Detail
WLC-BIBLIOTECA-UIOS	14	Detail
RED-ADM	3	Detail
WLAN-ADMV2	3	Detail

Most Recent Traps

Client Excluded: MACAddress:00:19:7e:36:1e:1b Base Radio MAC :54:75:d0:3f:bf:80 Slot:
 Coverage hole pre alarm for client[1] 00:e0:7c:02:60:8b on 802.11b/g interface of AP 54:75:
 Coverage hole pre alarm for client[1] e8:8d:28:88:cd:91 on 802.11b/g interface of AP 54:75:
 Client Excluded: MACAddress:00:19:7e:36:1e:1b Base Radio MAC :00:22:90:51:2e:70 Slot:
 Interference Profile Updated to Pass for Base Radio MAC: 00:3a:99:d0:7d:70 and slotNo: 0
[View All](#)

This page refreshes every 30 seconds.

License Level	base
System Name	WLCUIOS
Up Time	386 days, 22 hours, 19 minutes
System Time	Wed Apr 30 15:56:41 2014
Internal Temperature	+28 C
802.11a Network State	Enabled
802.11b/g Network State	Enabled
Local Mobility Group	UIOS
CPU(s) Usage	0%
Individual CPU Usage	0%/1%, 0%/1%
Memory Usage	43%

Access Point Summary

	Total	Up	Down	
802.11a/n Radios	1	● 1	● 0	Detail
802.11b/g/n Radios	12	● 12	● 0	Detail
All APs	12	● 12	● 0	Detail

Client Summary

Current Clients	121	Detail
Excluded Clients	0	Detail
Disabled Clients	0	Detail

Top WLANs

Profile Name	# of Clients	
WLAN-UPS-ESTUDIANTES	64	Detail
WLAN-UPS-DOCSUR	30	Detail
WLC-BIBLIOTECA-UIOS	15	Detail
WLAN-ADMV2	7	Detail
RED-ADM	3	Detail

Most Recent Traps

Coverage hole pre alarm for client[1] bc:44:86:ec:2b:69 on 802.11b/g interface of AP 00:22:
 Coverage hole pre alarm for client[1] 5c:3c:27:87:f4:3e on 802.11b/g interface of AP 00:22:
 Coverage hole pre alarm for client[1] 24:fd:52:e0:7a:b7 on 802.11b/g interface of AP 00:22:
 Coverage hole pre alarm for client[1] 00:1c:bf:40:50:6c on 802.11b/g interface of AP 00:22:
 Coverage hole pre alarm for client[1] 80:57:19:41:6e:39 on 802.11b/g interface of AP 00:1:
[View All](#)

This page refreshes every 30 seconds.

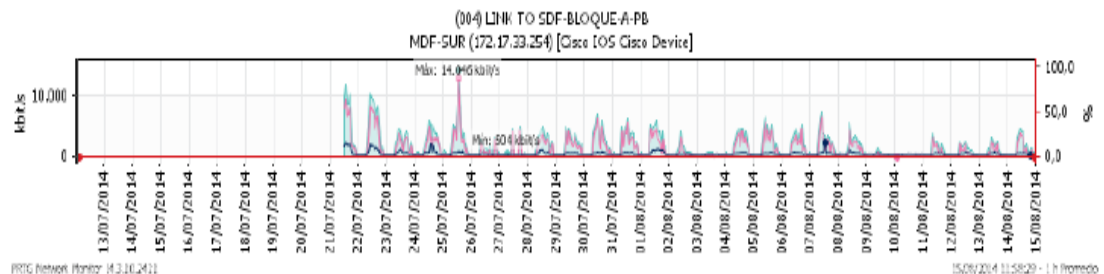
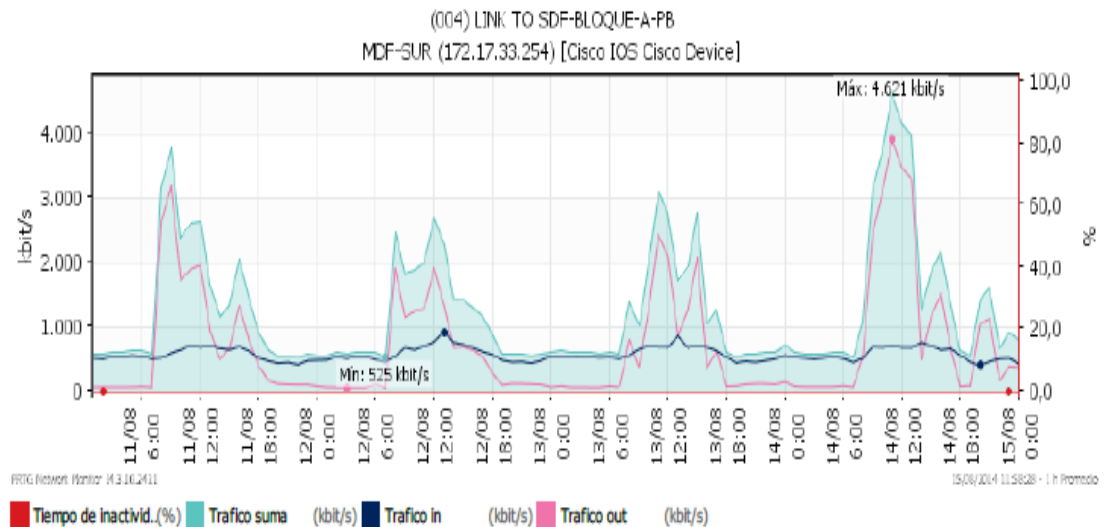
Anexo 2. Gráficos ancho de banda usados en la Universidad Politécnica Salesiana sede Quito campus Sur usando el software PRTG.

SWITCH DE CORE

Con el software PRTG, se realizó un estudio al switch de core escaneando sus todos sus puertos, para ver el consumo de ancho de banda que se obtiene mientras trabajan normalmente en la Universidad Politecnica Salesiana sede Quito campus Sur.

Bloque A-PB

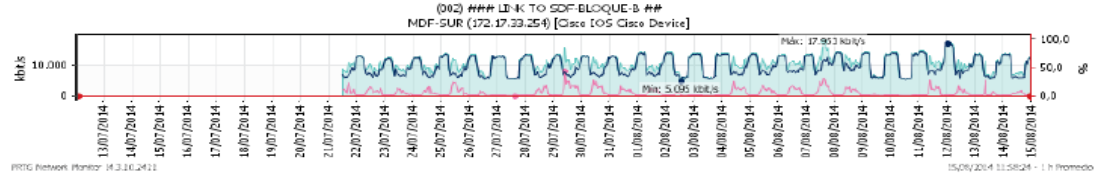
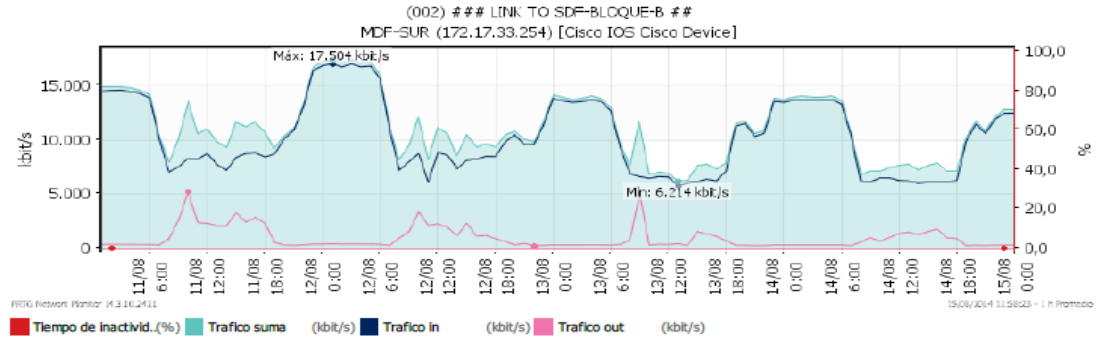
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00					
Horas de reporte:	24 / 7					
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)					
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]					
Estadísticas de tiempo disponible:	Disponible:	100 %	[3d23h48m20s]	Falla:	0 %	[0s]
Estadísticas de petición:	Buena:	100 %	[5751]	Fallo:	0 %	[0]
Promedio (Trafico suma):	1.287 kbit/s					
Total (Trafico suma):	54.188.278 KByte					



Canal	Promedio	Total
Trafico suma	1.287 kbit/s	54.188.278 KByte
Trafico in	578 kbit/s	24.338.062 KByte
Trafico out	709 kbit/s	29.850.216 KByte

Bloque B

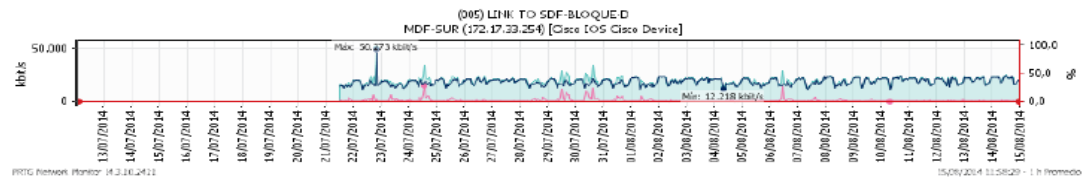
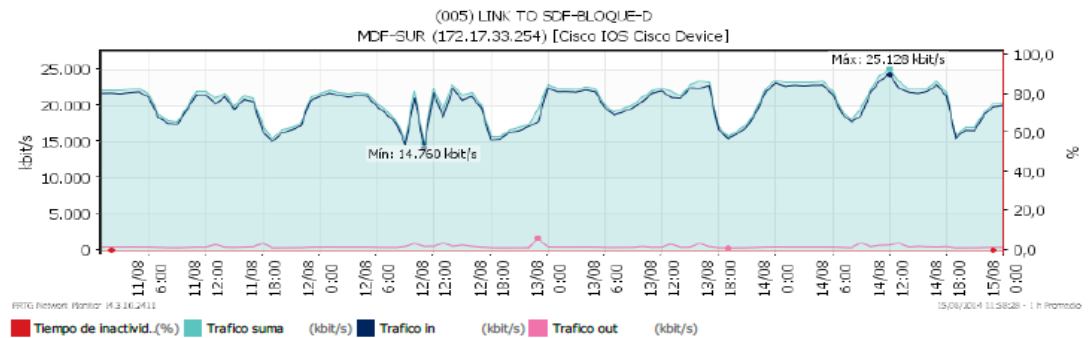
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % █ [3d23h48m18s]	Falla: 0 % █ [0s]
Estadísticas de petición:	Bueno:	100 % █ [5751]	Fallo: 0 % █ [0]
Promedio (Trafico suma):	11.236 kbit/s		
Total (Trafico suma):	473.248.168 KByte		



Canal	Promedio	Total
Trafico suma	11.236 kbit/s	473.248.168 KByte
Trafico in	10.304 kbit/s	433.974.127 KByte
Trafico out	932 kbit/s	39.274.041 KByte

Bloque D

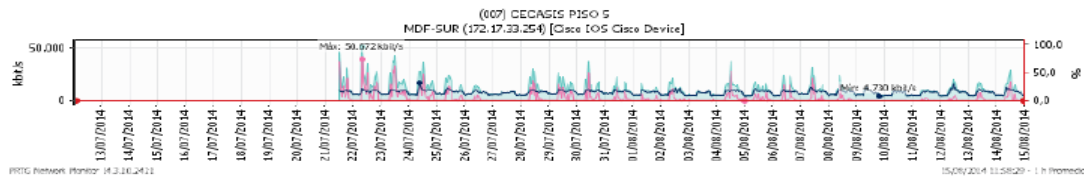
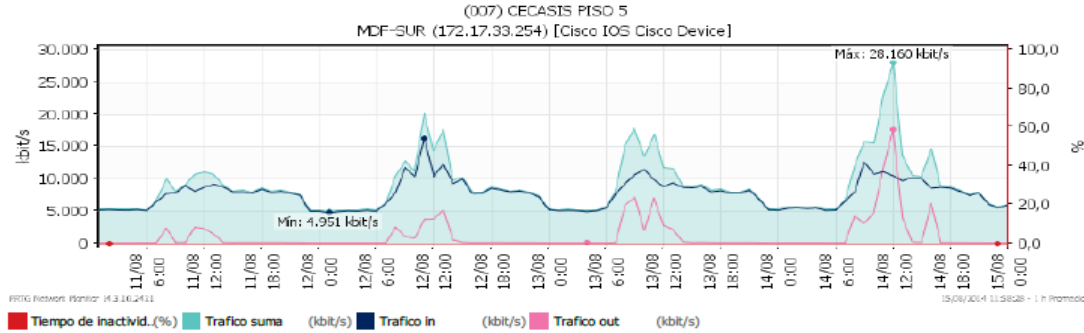
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % █ [3d23h48m21s]	Falla: 0 % █ [0s]
Estadísticas de petición:	Bueno:	100 % █ [5751]	Fallo: 0 % █ [0]
Promedio (Trafico suma):	20.543 kbit/s		
Total (Trafico suma):	865.252.340 KByte		



Canal	Promedio	Total
Trafico suma	20.543 kbit/s	865.252.340 KByte
Trafico in	20.043 kbit/s	844.186.366 KByte
Trafico out	500 kbit/s	21.065.973 KByte

CACASIS-P5

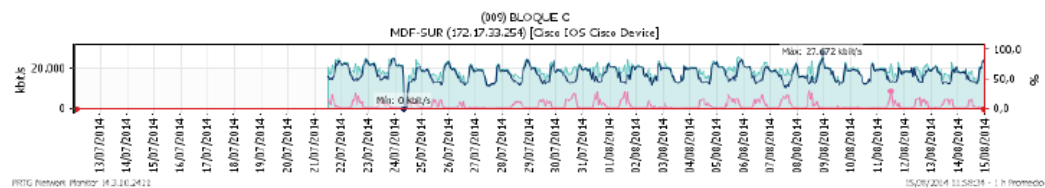
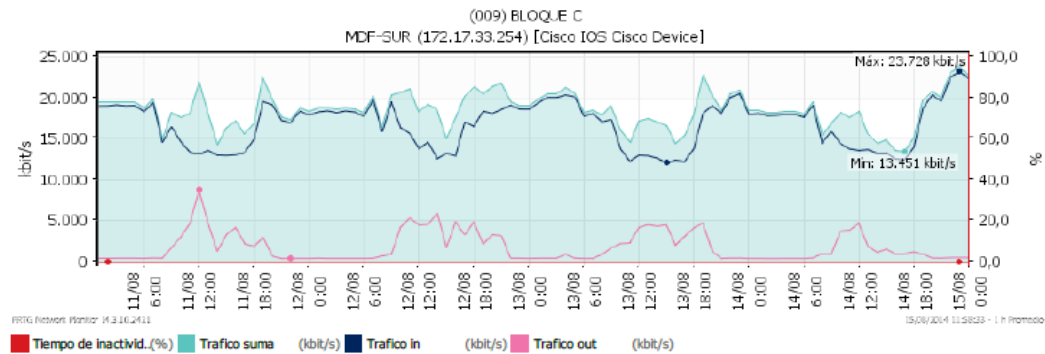
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m23s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	8.913 kbit/s		
Total (Trafico suma):	375.393.317 KByte		



Canal	Promedio	Total
Trafico suma	8.913 kbit/s	375.393.317 KByte
Trafico in	7.672 kbit/s	323.131.117 KByte
Trafico out	1.241 kbit/s	52.262.200 KByte

Bloque C

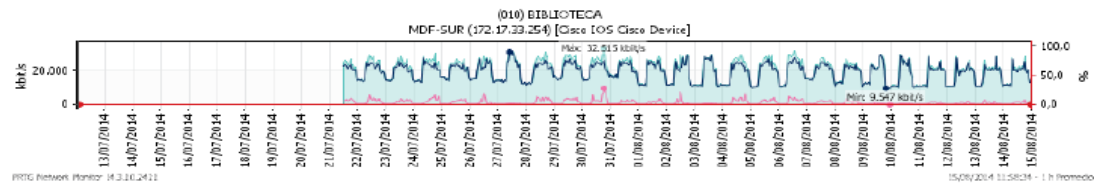
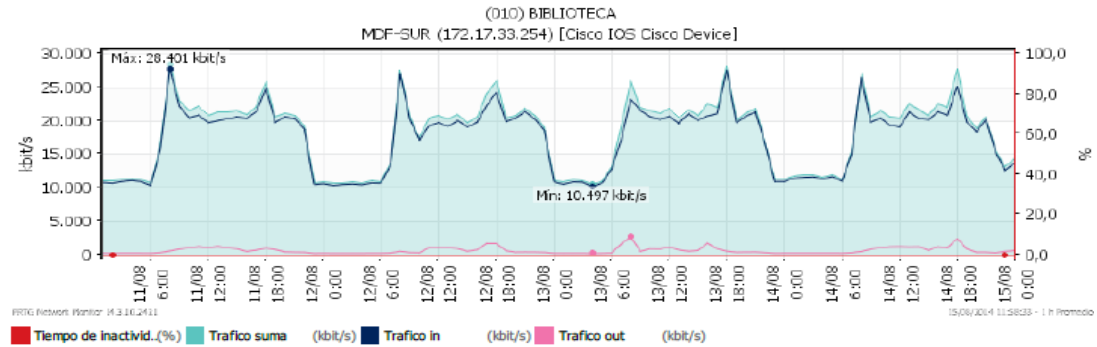
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m25s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	18.545 kbit/s		
Total (Trafico suma):	781.075.296 KByte		



Canal	Promedio	Total
Trafico suma	18.545 kbit/s	781.075.296 KByte
Trafico in	16.750 kbit/s	705.481.079 KByte
Trafico out	1.795 kbit/s	75.594.217 KByte

Biblioteca

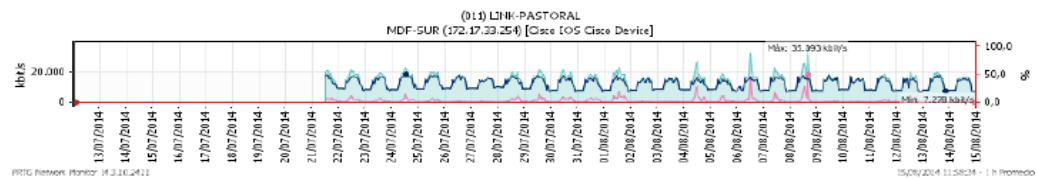
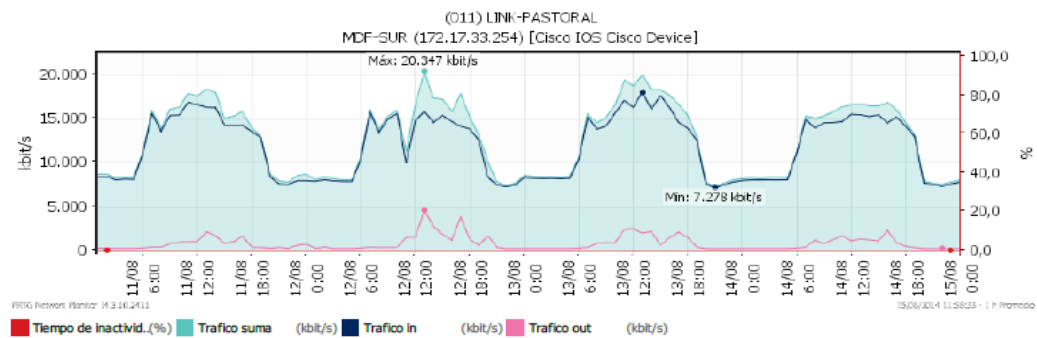
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m26s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	18.156 kbit/s		
Total (Trafico suma):	764.698.627 KByte		



Canal	Promedio	Total
Trafico suma	18.156 kbit/s	764.698.627 KByte
Trafico in	17.464 kbit/s	735.540.568 KByte
Trafico out	692 kbit/s	29.158.059 KByte

Pastoral

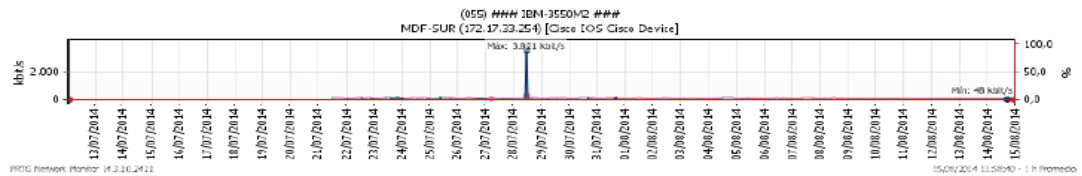
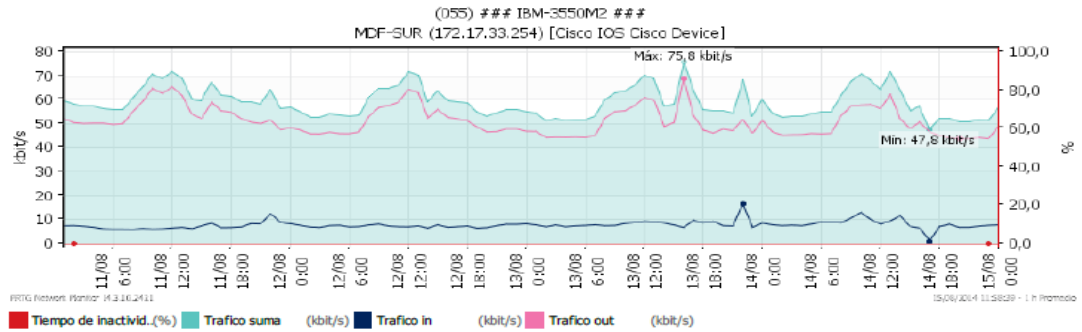
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m27s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	12.540 kbit/s		
Total (Trafico suma):	528.176.638 KByte		



Canal	Promedio	Total
Trafico suma	12.540 kbit/s	528.176.638 KByte
Trafico in	11.746 kbit/s	494.731.628 KByte
Trafico out	794 kbit/s	33.445.010 KByte

IBM-3550M2

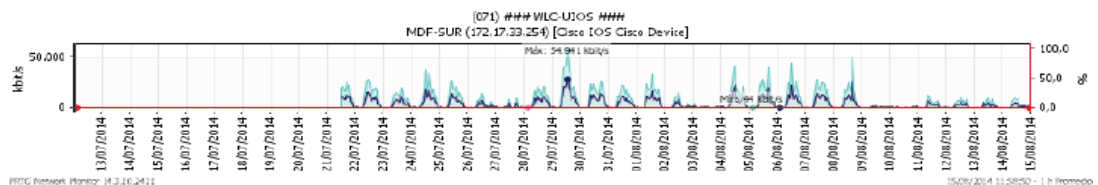
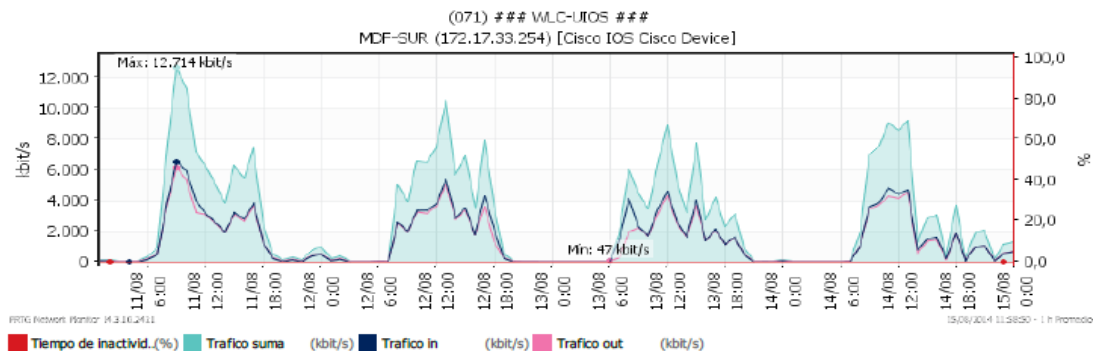
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m31s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	59 kbit/s		
Total (Trafico suma):	2.486.744 KByte		



Canal	Promedio	Total
Trafico suma	59 kbit/s	2.486.744 KByte
Trafico in	8 kbit/s	328.551 KByte
Trafico out	51 kbit/s	2.158.193 KByte

WLC-UIOS

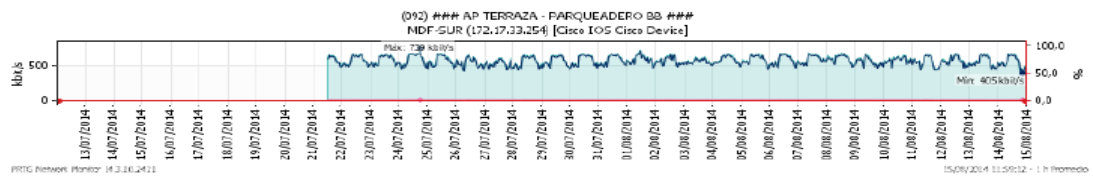
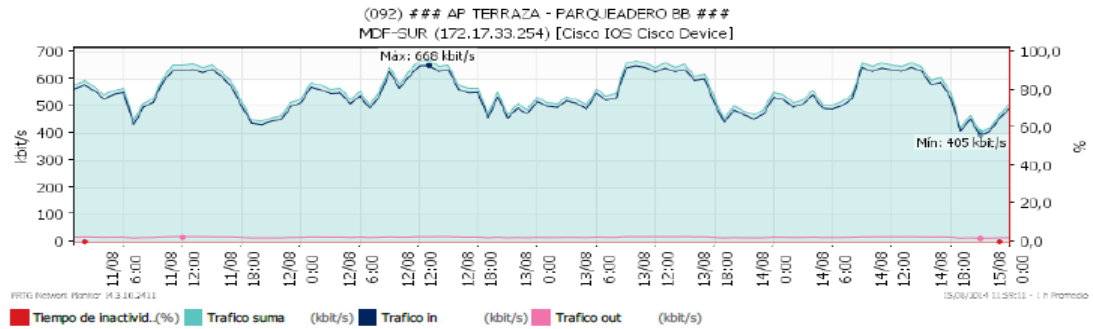
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m42s]	Falla: 0 % [0s]
Estadísticas de petición:	Buena:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	2.847 kbit/s		
Total (Trafico suma):	119.897.428 KByte		



Canal	Promedio	Total
Trafico suma	2.847 kbit/s	119.897.428 KByte
Trafico in	1.473 kbit/s	62.043.519 KByte
Trafico out	1.374 kbit/s	57.853.909 KByte

AP-Terraza

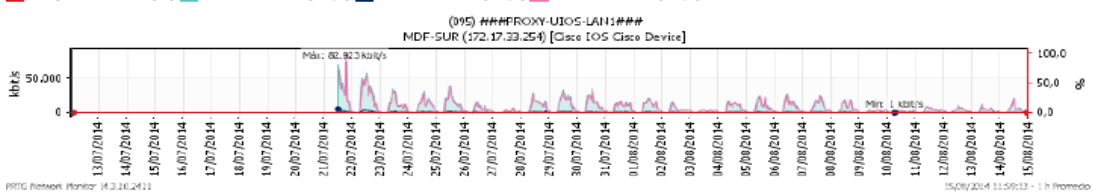
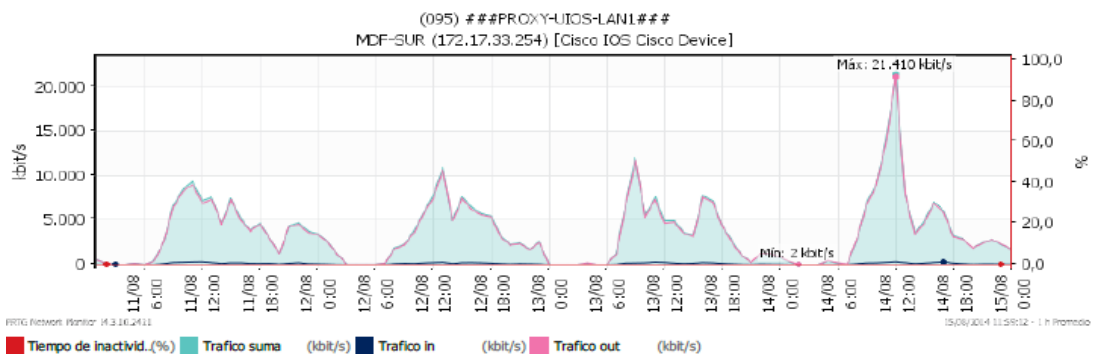
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h49m0s]	Falla: 0 % [0s]
Estadísticas de petición:	Bueno:	100 % [5751]	Fallo: 0 % [0]
Promedio (Trafico suma):	560 kbit/s		
Total (Trafico suma):	23.581.676 KByte		



Canal	Promedio	Total
Trafico suma	560 kbit/s	23.581.676 KByte
Trafico in	544 kbit/s	22.913.848 KByte
Trafico out	16 kbit/s	667.828 KByte

PROXY-UIOS

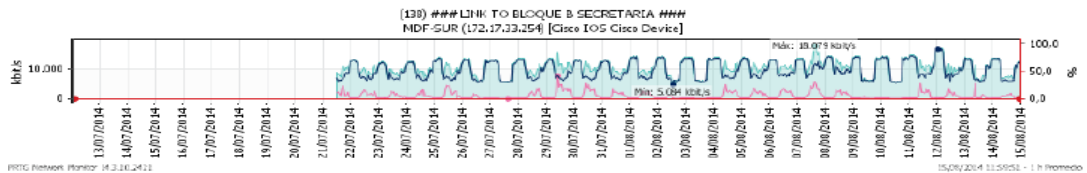
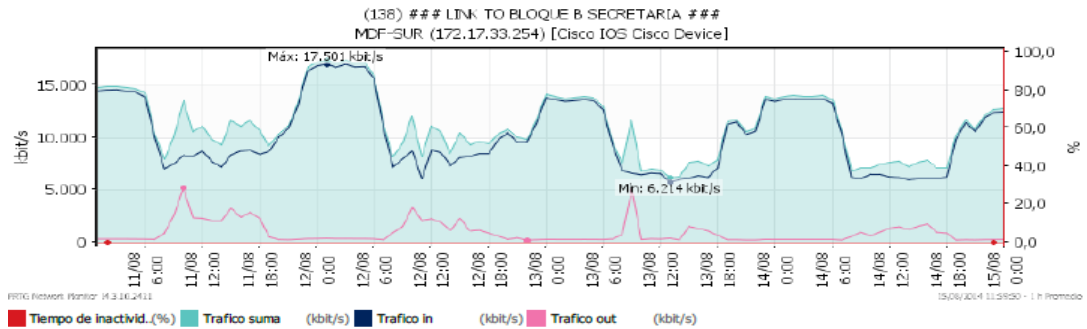
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h50m3s]	Falla: 0 % [0s]
Estadísticas de petición:	Bueno:	100 % [5753]	Fallo: 0 % [0]
Promedio (Trafico suma):	3.608 kbit/s		
Total (Trafico suma):	152.005.621 KByte		



Canal	Promedio	Total
Trafico suma	3.608 kbit/s	152.005.621 KByte
Trafico in	100 kbit/s	4.213.761 KByte
Trafico out	3.508 kbit/s	147.791.860 KByte

Secretaría

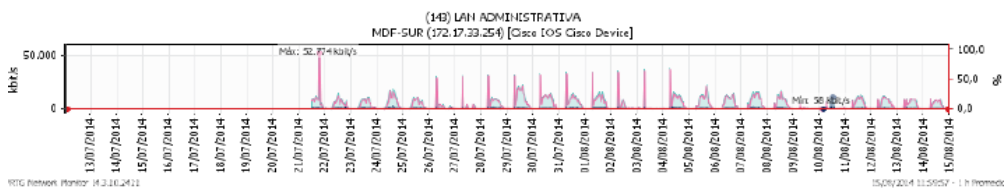
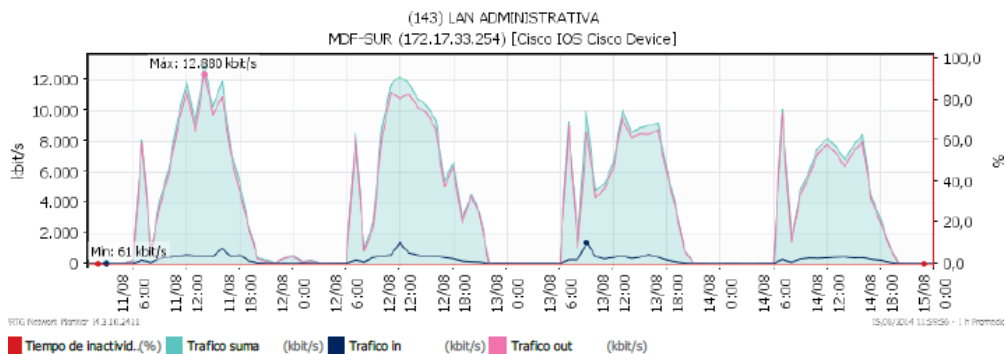
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % ■ [3d23h48m36s]	Falla: 0 % ■ [0s]
Estadísticas de petición:	Bueno:	100 % ■ [5751]	Fallo: 0 % ■ [0]
Promedio (Trafico suma):	11.236 kbit/s		
Total (Trafico suma):	473.237.298 KByte		



Canal	Promedio	Total
Trafico suma	11.236 kbit/s	473.237.298 KByte
Trafico in	10.304 kbit/s	433.967.986 KByte
Trafico out	932 kbit/s	39.269.313 KByte

LAN-Administrativa

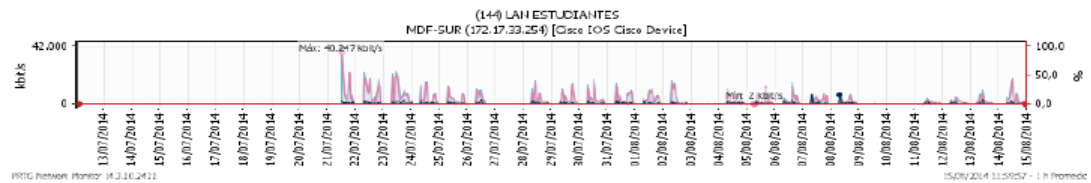
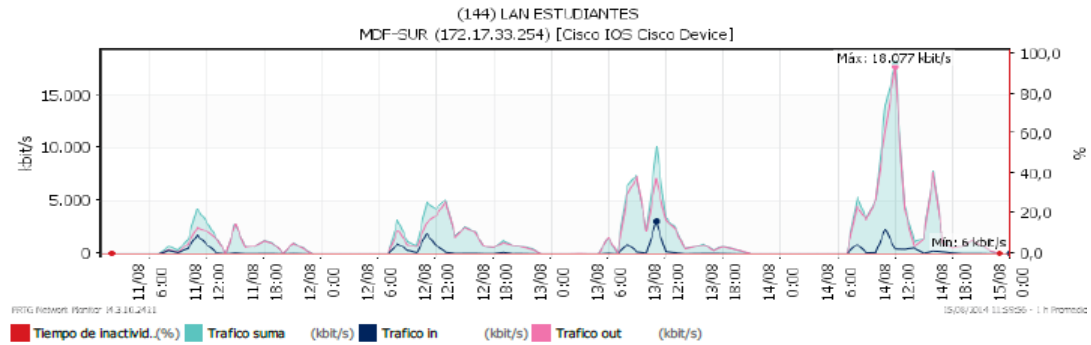
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible:	100 % ■ [3d23h48m40s]	Falla: 0 % ■ [0s]
Estadísticas de petición:	Bueno:	100 % ■ [5751]	Fallo: 0 % ■ [0]
Promedio (Trafico suma):	4.043 kbit/s		
Total (Trafico suma):	170.268.937 KByte		



Canal	Promedio	Total
Trafico suma	4.043 kbit/s	170.268.937 KByte
Trafico in	258 kbit/s	10.858.073 KByte
Trafico out	3.785 kbit/s	159.410.864 KByte

LAN-Estudiantes

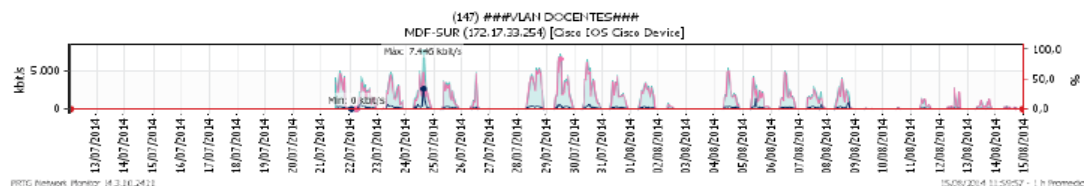
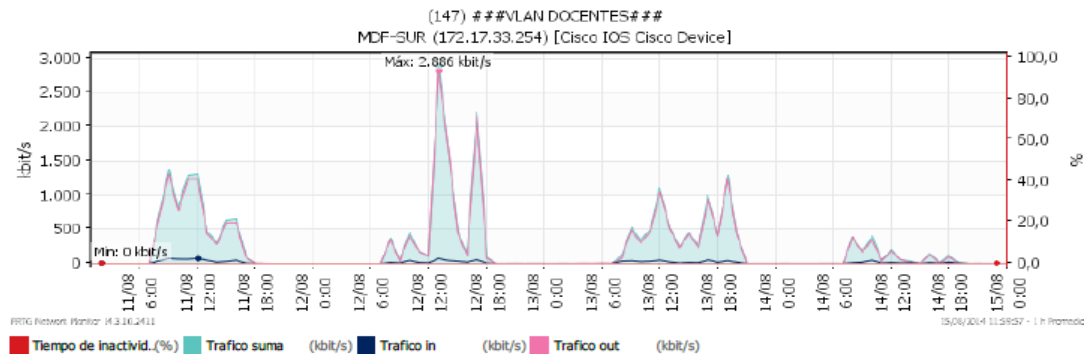
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible: 100 % [3d23h48m41s]	Falla: 0 % [0s]	
Estadísticas de petición:	Buena: 100 % [5751]	Fallo: 0 % [0]	
Promedio (Trafico suma):	1.579 kbit/s		
Total (Trafico suma):	66.484.096 KByte		



Canal	Promedio	Total
Trafico suma	1.579 kbit/s	66.484.096 KByte
Trafico in	193 kbit/s	8.142.903 KByte
Trafico out	1.385 kbit/s	58.341.193 KByte

VLAN-Docentes

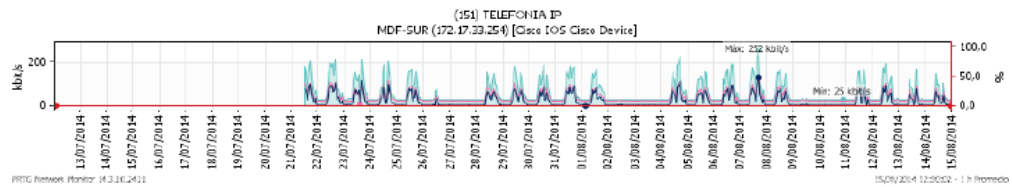
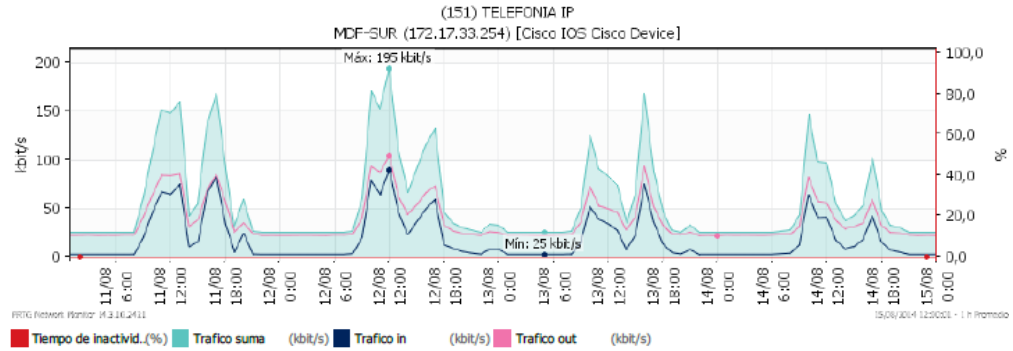
Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00		
Horas de reporte:	24 / 7		
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)		
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]		
Estadísticas de tiempo disponible:	Disponible: 100 % [3d23h48m44s]	Falla: 0 % [0s]	
Estadísticas de petición:	Buena: 100 % [5751]	Fallo: 0 % [0]	
Promedio (Trafico suma):	261 kbit/s		
Total (Trafico suma):	10.991.369 KByte		



Canal	Promedio	Total
Trafico suma	261 kbit/s	10.991.369 KByte
Trafico in	14 kbit/s	584.368 KByte
Trafico out	247 kbit/s	10.407.001 KByte

Telefonia IP

Plazo de tiempo de reporte:	11/08/2014 0:00:00 - 15/08/2014 0:00:00			
Horas de reporte:	24 / 7			
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)			
Sonda, grupo, aparato:	Local probe > Campus Sur > MDF-SUR (172.17.33.254) [Cisco IOS Cisco Device]			
Estadísticas de tiempo disponible:	Disponible:	100 % [3d23h48m48s]	Falla:	0 % [0s]
Estadísticas de petición:	Bueno:	100 % [5751]	Fallo:	0 % [0]
Promedio (Trafico suma):	56 kbit/s			
Total (Trafico suma):	2.342.727 KByte			



Canal	Promedio	Total
Trafico suma	56 kbit/s	2.342.727 KByte
Trafico in	18 kbit/s	778.686 KByte
Trafico out	37 kbit/s	1.564.040 KByte

Anexo 3. ACLs y direccionamiento propuesto para la red propuesta de alta disponibilidad.

ip access-list extended SUN	permit udp any any eq 5353	permit udp any any eq 20000
permit tcp any any eq 443	permit udp any any eq 10002	permit tcp any any range 50000 52000
permit tcp any any eq www	permit udp any any eq 10003	permit ip any 172.17.4.0 0.0.1.255 log
permit udp any any eq domain	permit tcp any any eq 10004	permit tcp any any eq 3144
permit udp any any eq bootpc	permit udp any any range 50000 52000	permit tcp any any eq 5307
permit udp any any eq bootps	permit tcp any any eq 22	permit ip any 172.17.46.0 0.0.0.255 log
permit tcp any any eq ftp	permit udp any any eq 22	permit ip any 172.17.28.128 0.0.0.127 log
permit tcp any any eq ftp-data	permit icmp any any	permit ip any host 172.17.2.99
permit tcp any any range 8000 8006	permit tcp any any eq 11000	
permit tcp any any eq 5909	permit tcp any any eq 8030	ip access-list extended acl-CECASIS
permit udp any any eq 5909	permit udp any any eq 8030	permit ip 172.17.4.0 0.0.1.255 172.17.28.128
permit tcp any any eq 5353	permit tcp any any eq 20000	0.0.0.127
		permit udp any any eq bootpc

permit udp any any eq bootps	permit ip any host 172.17.1.10 log	permit tcp any host 172.17.4.5 eq 135
permit tcp any any eq 8080	permit tcp any any eq 3128	permit tcp any host 172.17.4.5 eq 389
permit tcp any any eq 4646	permit ip any 172.17.40.0 0.0.0.255	permit udp any host 172.17.4.5 eq 389
permit udp any any eq 4646	permit ip any 172.17.29.0 0.0.1.255 log	permit tcp any host 172.17.4.5 eq 445
permit udp any any eq 5093	permit ip any host 172.17.4.1 log	permit udp any host 172.17.4.5 eq 445
permit tcp any any eq 5093	permit ip any host 172.17.4.5 log	permit tcp any host 172.17.4.5 eq 636
permit tcp any any eq 8085	permit tcp any host 172.17.1.10 eq 3128	permit tcp any host 172.17.4.5 eq 3268
permit udp any any eq domain	permit tcp any host 172.17.1.10 eq www	permit tcp any host 172.17.4.5 eq 137
permit ip any 172.17.46.0 0.0.0.255 log	permit tcp any host 172.17.1.10 eq 443	permit udp any host 172.17.4.5 eq netbios-ns
permit ip any 172.17.23.0 0.0.3.255 log	permit tcp any host 172.17.4.5 eq domain	permit tcp any host 172.17.4.5 eq 138
permit icmp any any	permit udp any host 172.17.4.5 eq domain	permit udp any host 172.17.4.5 eq netbios-dgm
permit ip any 172.17.8.0 0.0.1.255 log	permit tcp any host 172.17.4.5 eq 88	permit tcp any host 172.17.4.5 eq 139
permit tcp any any eq 22 log	permit udp any host 172.17.4.5 eq 88	permit udp any host 172.17.4.5 eq netbios-ss

ip access-list extended acl-CISCO

permit udp any any eq domain	permit udp any any eq bootps	permit tcp host 172.17.35.37 any eq 443
permit udp any any eq bootpc	permit tcp any any eq 15871	permit udp host 172.17.35.37 any eq domain
permit udp any any eq bootps	permit ip any 172.17.46.0 0.0.0.255 log	permit tcp host 172.17.35.33 any eq www
permit ip host 172.17.7.253 any log	permit tcp any any eq telnet	permit tcp host 172.17.35.33 any eq 443
permit tcp any any eq telnet	permit tcp any any eq 22	permit udp host 172.17.35.33 any eq domain
permit tcp any any eq 22	permit icmp any any	permit tcp host 172.17.35.34 any eq www
permit ip any host 172.17.1.6	permit tcp any host 172.17.1.5 eq www log	permit tcp host 172.17.35.34 any eq 443
permit ip any 172.17.46.0 0.0.0.255 log	permit ip any host 172.17.2.99	permit udp host 172.17.35.34 any eq domain
	deny ip any host 69.195.138.144	permit tcp host 172.17.35.35 any eq www
	deny ip host 69.195.138.144 any	permit tcp host 172.17.35.35 any eq 443

ip access-list extended acl-RUI

permit udp any any eq domain	permit tcp any 172.17.0.0 0.0.255.255 eq www	permit udp host 172.17.35.35 any eq domain
permit udp any any eq bootpc	permit tcp any 172.17.0.0 0.0.255.255 eq 443	permit tcp host 172.17.35.39 any eq www
	permit tcp host 172.17.35.37 any eq www	permit tcp host 172.17.35.39 any eq 443

permit udp host 172.17.35.39 any eq domain	ip access-list extended acl-salabiblio	permit tcp 172.17.12.64 0.0.0.63 host
permit tcp host 172.17.35.41 any eq www	permit tcp 172.17.12.64 0.0.0.63 host	172.17.2.100 eq 5800
permit tcp host 172.17.35.41 any eq 443	172.17.2.50 eq 4646	permit tcp 172.17.12.64 0.0.0.63 host
permit udp host 172.17.35.41 any eq domain	permit udp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq domain
	172.17.2.50 eq 4646	permit udp 172.17.12.64 0.0.0.63 host
	permit tcp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq domain
ip access-list extended acl-copp-match-igmp	172.17.2.50 eq 5900	permit tcp 172.17.12.64 0.0.0.63 host
permit igmp any any	permit tcp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq 88
	172.17.2.50 eq 3600	permit udp 172.17.12.64 0.0.0.63 host
	permit tcp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq 88
ip access-list extended acl-copp-match-pim-	172.17.2.50 eq 5800	permit tcp 172.17.12.64 0.0.0.63 host
data	permit tcp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq 135
deny pim any host 224.0.0.13	172.17.2.100 eq 5900	permit tcp 172.17.12.64 0.0.0.63 host
permit pim any any	permit tcp 172.17.12.64 0.0.0.63 host	172.17.1.6 eq 389
	172.17.2.100 eq 3600	permit udp 172.17.12.64 0.0.0.63 host
		172.17.1.6 eq 389

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 445

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 445

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 636

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 3268

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 137

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq netbios-ns

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 138

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq netbios-dgm

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq 139

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.6 eq netbios-ss

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq domain

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq domain

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 88

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 88

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 135

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 389

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 389

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 445

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 445

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 636

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 3268

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 137

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq netbios-ns

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 138

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq netbios-dgm

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq 139

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.1 eq netbios-ss

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq domain

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq domain

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 88

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 88

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 135

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 389

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 389

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 445

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 445

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 636

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 3268

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 137

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq netbios-ns

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 138

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq netbios-dgm

permit tcp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq 139

permit udp 172.17.12.64 0.0.0.63 host
172.17.1.3 eq netbios-ss

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 445

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 445

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 137

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq netbios-ns

```
permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 138

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq netbios-dgm

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 139

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq netbios-ss

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 8080

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 8080

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq www

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 80
```

```
permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 8081

permit udp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 8081

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 5900

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 3600

permit tcp 172.17.12.64 0.0.0.63 host
172.17.2.99 eq 5800

permit ip any host 172.17.1.5

permit tcp any any eq 4646

permit udp any any eq 4646

permit udp any any eq 5093

permit tcp any any eq 5093
```

```
permit udp any any eq domain

permit udp any any eq bootpc

permit udp any any eq bootps

permit tcp any any eq ftp

permit tcp any any eq ftp-data

permit ip any 172.17.46.0 0.0.0.255 log
```

ip access-list extended acl-salaprofesores

```
permit tcp 172.17.10.0 0.0.1.255 172.16.1.128
0.0.0.127 eq 8888

permit tcp 172.17.10.0 0.0.1.255 172.16.1.128
0.0.0.127 eq 1521

permit tcp 172.17.10.0 0.0.1.255 172.16.1.128
0.0.0.127 eq www
```

permit tcp 172.17.10.0 0.0.1.255 172.16.1.128 0.0.0.127 eq 443	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 138	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 8081
permit tcp 172.17.10.0 0.0.1.255 172.16.1.128 0.0.0.127 eq lpd	permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq netbios-dgm	permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 8081
permit ip 172.17.10.0 0.0.1.255 host 172.16.1.147	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 139	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 5900
permit ip 172.17.10.0 0.0.1.255 host 172.16.1.131	permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq netbios-ss	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 3600
permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 445	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 8080	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 5800
permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 445	permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 8080	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.100 eq 5900
permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 137	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq www	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.100 eq 3600
permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq netbios-ns	permit udp 172.17.10.0 0.0.1.255 host 172.17.2.99 eq 80	permit tcp 172.17.10.0 0.0.1.255 host 172.17.2.100 eq 5800

permit udp any any eq bootpc

permit udp any any eq bootps

permit tcp 172.17.10.0 0.0.1.255 host
172.17.1.1 eq domain

permit udp 172.17.10.0 0.0.1.255 host
172.17.1.1 eq domain

permit tcp any any eq 443

permit tcp any any eq www

permit udp any any eq domain

permit tcp any any eq ftp

permit tcp any any eq ftp-data

permit tcp any any eq 8080

permit tcp any any eq 8085

permit tcp any any range 8080 8085

permit ip any 172.17.46.0 0.0.0.255 log

ip access-list extended acl-wlanS

permit udp any any eq domain

permit udp any any eq bootpc

permit udp any any eq bootps

permit tcp any any eq 443

permit tcp any any eq www

permit ip any 172.17.46.0 0.0.0.255 log

ip access-list extended hp

permit udp any any eq domain

permit udp any any eq bootpc

permit udp any any eq bootps

permit ip any 172.17.8.0 0.0.0.255 log

permit ip any host 172.17.2.99

permit ip any 172.17.46.0 0.0.0.255 log

!

VLAN	NOMBRE	DIRECCIÓN IP GATEWAY	MASCARA	RED	/MASK
Vlan1	Default	172.17.0.254	255.255.255.0=24	172.17.0.0	/24
Vlan2	DMZ	172.17.1.254	255.255.255.0=24	172.17.1.0	/24
Vlan3	ADMINISTRATIVA	172.17.3.254	255.255.254.0=23	172.17.2.0	/23
Vlan4	LABORATORIOS-EST	172.17.5.254	255.255.254.0=23	172.17.4.0	/23
Vlan5	CISCO	172.17.7.254	255.255.254.0=23	172.17.6.0	/23
Vlan6	SUN	172.17.9.254	255.255.254.0=23	172.17.8.0	/23
Vlan7	SALA DOCENTES	172.17.11.254	255.255.254.0=23	172.17.10.0	/23
Vlan8	SALA-INTERNET	172.17.12.62	255.255.255.192=26	172.17.12.0	/26
Vlan10	WIRELESS EST	172.17.20.254	255.255.248.0=21	172.17.13.0	/21
Vlan11	WIRELESS DOCENTES	172.17.22.254	255.255.254.0=23	172.17.21.0	/23
Vlan12	CECASIS	172.17.26.254	255.255.252.0=22	172.17.23.0	/22
Vlan13	VLAN-VIDEO	172.17.27.62	255.255.255.192=26	172.17.27.0	/26
Vlan14	VLAN-HP	172.17.28.126	255.255.255.128=25	172.17.28.0	/25
Vlan15	ELECTRONICA	172.17.30.254	255.255.254.0=23	172.17.29.0	/23
Vlan16	VLAN-TELCONET	172.17.31.254	255.255.255.0=24	172.17.31.0	/24
Vlan19	INVESTIGACION	172.17.32.254	255.255.255.0=24	172.17.32.0	/24
Vlan20	Vo-IP	172.17.34.254	255.255.254.0=23	172.17.33.0	/23
Vlan22	RUI	172.17.35.254	255.255.255.0=24	172.17.35.0	/24
Vlan24	WLAN-SUR	172.17.36.254	255.255.255.0=24	172.17.36.0	/24
Vlan25	CAMARAS-IP-UIOS	172.17.37.254	255.255.255.0=24	172.17.37.0	/24
Vlan26	EVENTOS	172.17.38.254	255.255.255.0=24	172.17.38.0	/24
Vlan27	###LAB-FISICA-UIO###	172.17.39.254	255.255.255.0=24	172.17.39.0	/24
Vlan28	INTERNET-CECASIS	172.17.40.254	255.255.255.0=24	172.17.40.0	/24
Vlan29	GIETEC	172.17.41.254	255.255.255.0=24	172.17.41.0	/24
Vlan30	EDUROAM	172.17.43.254	255.255.254.0=23	172.17.42.0	/23
Vlan31	OUT-LAN	172.17.44.254	255.255.255.0=23	172.17.44.0	/24

Anexo 4. Configuración de los equipos y gráficos del funcionamiento de la red simulada utilizando el protocolo GLBP.

Configuración de los router de core.

Script configuración del equipo R-UIOS-1

```
!  
hostname R-UIOS-1  
!  
!  
interface FastEthernet0/0  
ip address 10.0.0.33 255.255.255.248  
!  
interface FastEthernet0/1  
ip address 10.0.0.2 255.255.255.248  
!  
interface FastEthernet1/0  
ip address 10.0.0.26 255.255.255.248  
!  
!  
interface FastEthernet2/0  
ip address 10.0.0.41 255.255.255.248  
!  
router ospf 2  
log-adjacency-changes  
network 10.0.0.0 0.255.255.255 area 1  
network 172.17.0.0 0.0.255.255 area 1  
!  
End
```

Script configuración del equipo R-UIOS-2

```
hostname R-UIOS-2  
!  
!  
interface FastEthernet0/0  
ip address 10.0.0.34 255.255.255.248  
!  
interface FastEthernet0/1  
ip address 10.0.0.18 255.255.255.248  
!  
interface FastEthernet1/0  
ip address 10.0.0.10 255.255.255.248  
!  
interface FastEthernet2/0  
ip address 10.0.0.49 255.255.255.248  
!  
router ospf 2  
log-adjacency-changes  
network 10.0.0.0 0.255.255.255 area 1  
network 172.17.0.0 0.0.255.255 area 1  
!  
End
```

Configuración de los switch de core

Script configuración del equipo MDF-UIOS

```
hostname MDF-UIOS
!  
vlan accounting input
!  
vlan 99
  name MNG
!  
vlan 2
  name DMZ
!  
vlan 3
  name ADM
!  
vlan 4
  name EST
!  
vlan 5
  name CISCO
!  
vlan 6
  name SUN
!  
vlan 7
  name sala-profes
!  
!
```

```
vlan 8
  name sala-intern
!  
!  
spanning-tree vlan 2 priority 4096
spanning-tree vlan 3 priority 4096
spanning-tree vlan 4 priority 4096
spanning-tree vlan 5 priority 4096
spanning-tree vlan 6 priority 4096
spanning-tree vlan 7 priority 4096
spanning-tree vlan 8 priority 4096
spanning-tree vlan 99 priority 10
!  
vtp mode server
vtp domain UIOS
!  
interface Port-channel5
  switchport trunk native vlan 99
  switchport mode trunk
!  
interface Port-channel4
  switchport trunk native vlan 99
  switchport mode trunk
!  
interface Port-channel3
  switchport trunk native vlan 99
  switchport mode trunk
!  
!
```

```
interface Port-channel2
  switchport trunk native vlan 99
  switchport mode trunk
!  
interface Port-channel1
  switchport trunk native vlan 99
  switchport mode trunk
!  
interface FastEthernet0/0
  ip address 10.0.0.1 255.255.255.248
!  
interface FastEthernet0/1
  ip address 10.0.0.9 255.255.255.248
!  
interface FastEthernet1/0
  switchport trunk native vlan 99
  switchport mode trunk
  channel-group 1 mode on
!  
interface FastEthernet1/1
  switchport trunk native vlan 99
  switchport mode trunk
  channel-group 1 mode on
!  
interface FastEthernet1/2
  switchport trunk native vlan 99
  switchport mode trunk
  channel-group 5 mode on
```

```

!
interface FastEthernet1/3
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 5 mode on
!
interface FastEthernet1/4
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 4 mode on
!
interface FastEthernet1/5
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 4 mode on
!
interface FastEthernet1/6
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet1/7
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet1/8
 switchport trunk native vlan 99
 switchport mode trunk

```

```

channel-group 2 mode on
!
interface FastEthernet1/9
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 2 mode on
!
interface Vlan2
 ip address 172.17.1.254 255.255.255.0
 glbp 2 ip 172.17.1.252
 glbp 2 priority 250
 glbp 2 preempt
 glbp 2 load-balancing host-dependent
!
interface Vlan3
 ip address 172.17.3.254 255.255.254.0
 glbp 3 ip 172.17.3.252
 glbp 3 priority 250
 glbp 3 preempt
 glbp 3 load-balancing host-dependent
!
interface Vlan4
 ip address 172.17.5.254 255.255.254.0
 glbp 4 ip 172.17.5.252
 glbp 4 priority 250
 glbp 4 preempt
 glbp 4 load-balancing host-dependent
!
interface Vlan5

```

```

 ip address 172.17.7.254 255.255.254.0
 glbp 5 ip 172.17.7.252
 glbp 5 priority 250
 glbp 5 preempt
 glbp 5 load-balancing host-dependent
!
interface Vlan6
 ip address 172.17.9.254 255.255.254.0
 glbp 6 ip 172.17.9.252
 glbp 6 priority 250
 glbp 6 preempt
 glbp 6 load-balancing host-dependent
!
interface Vlan7
 ip address 172.17.11.254 255.255.254.0
 glbp 7 ip 172.17.11.252
 glbp 7 priority 250
 glbp 7 preempt
 glbp 7 load-balancing host-dependent
!
interface Vlan8
 ip address 172.17.12.62 255.255.255.192
 glbp 8 ip 172.17.12.60
 glbp 8 priority 250
 glbp 8 preempt
 glbp 8 load-balancing host-dependent
!
interface Vlan99
 ip address 10.1.1.1 255.255.255.0

```

```

glbp 1 ip 10.1.1.254
glbp 1 priority 250
glbp 1 preempt
glbp 1 load-balancing host-dependent
!
router ospf 2
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 1
network 172.17.0.0 0.0.255.255 area 1
!
End

```

Script configuración del equipo MDF-UIOS-2

```

hostname MDF-UIOS-2
!
!
vlan accounting input
!
vlan 99
name MNG
!
spanning-tree vlan 2 priority 8192
spanning-tree vlan 3 priority 8192
spanning-tree vlan 4 priority 8192
spanning-tree vlan 5 priority 8192
spanning-tree vlan 6 priority 8192

```

```

spanning-tree vlan 7 priority 8192
spanning-tree vlan 8 priority 8192
spanning-tree vlan 99 priority 100
!
vtp mode client
vtp domain UIOS
!
interface Port-channel1
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel5
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel4
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel3
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel2
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/0
ip address 10.0.0.17 255.255.255.248

```

```

!
interface FastEthernet0/1
ip address 10.0.0.25 255.255.255.248
!
interface FastEthernet1/0
switchport trunk native vlan 99
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/1
switchport trunk native vlan 99
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/2
switchport trunk native vlan 99
switchport mode trunk
channel-group 5 mode on
!
interface FastEthernet1/3
switchport trunk native vlan 99
switchport mode trunk
channel-group 5 mode on
!
interface FastEthernet1/4
switchport trunk native vlan 99
switchport mode trunk
channel-group 4 mode on
!

```

```

interface FastEthernet1/5
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 4 mode on
!
interface FastEthernet1/6
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet1/7
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet1/8
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet1/9
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 2 mode on
!
interface Vlan2
 ip address 172.17.1.253 255.255.255.0
 glbp 2 ip 172.17.1.252
 glbp 2 load-balancing host-dependent
!
interface Vlan3
 ip address 172.17.3.253 255.255.254.0
 glbp 3 ip 172.17.3.252
 glbp 3 load-balancing host-dependent
!
interface Vlan4
 ip address 172.17.5.253 255.255.254.0
 glbp 4 ip 172.17.5.252
 glbp 4 load-balancing host-dependent
!
interface Vlan5
 ip address 172.17.7.253 255.255.254.0
 glbp 5 ip 172.17.7.252
 glbp 5 load-balancing host-dependent
!
interface Vlan6
 ip address 172.17.9.253 255.255.254.0
 glbp 6 ip 172.17.9.252
!
 glbp 6 load-balancing host-dependent
!
interface Vlan7
 ip address 172.17.11.253 255.255.254.0
 glbp 7 ip 172.17.11.252
 glbp 7 load-balancing host-dependent
!
interface Vlan8
 ip address 172.17.12.61 255.255.255.192
 glbp 8 ip 172.17.12.60
 glbp 8 load-balancing host-dependent
!
interface Vlan99
 ip address 10.1.1.2 255.255.255.0
 glbp 1 ip 10.1.1.254
 glbp 1 load-balancing host-dependent
!
router ospf 2
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 1
 network 172.17.0.0 0.0.255.255 area 1
!
End

```

Configuración de los switch de distribución

Script configuración del equipo IDF-BA-P5

```
hostname IDF-BA-P5
!
vlan 99
 name MNG
!
vtp mode client
vtp domain UIOS
!
interface Port-channel5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface Port-channel2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet1/0
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet1/1
 switchport mode trunk
 channel-group 1 mode on
```

```
!
interface FastEthernet1/2
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 5 mode on
!
interface FastEthernet1/3
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 5 mode on
!
interface FastEthernet1/4
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet1/5
 switchport trunk native vlan 99
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet1/6
 switchport mode trunk
!
interface FastEthernet1/7
 switchport mode trunk
!
interface Vlan99
```

```
 ip address 10.1.1.3 255.255.255.0
!
router ospf 2
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 1
 network 172.17.0.0 0.0.255.255 area 1
!
End
```

Script configuración del equipo IDF-BAP4

```
hostname IDF-BAP4
!
vlan 99
 name MNG
!
vtp mode client
vtp domain UIOS
!
interface Port-channel4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface Port-channel3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface Port-channel1
```

```

switchport mode trunk
!
interface FastEthernet1/0
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/1
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/2
switchport trunk native vlan 99
switchport mode trunk
channel-group 4 mode on
!
interface FastEthernet1/3
switchport trunk native vlan 99
switchport mode trunk
channel-group 4 mode on
!
interface FastEthernet1/4
switchport trunk native vlan 99
switchport mode trunk
channel-group 3 mode on
!
interface FastEthernet1/5
switchport trunk native vlan 99
switchport mode trunk
channel-group 3 mode on

```

```

!
interface FastEthernet1/6
switchport mode trunk
!
interface FastEthernet1/7
switchport mode trunk
!
interface Vlan99
ip address 10.1.1.4 255.255.255.0
!
router ospf 2
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 1
network 172.17.0.0 0.0.255.255 area 1
!
End

```

Script configuración del equipo IDF-BA-PB

```

!
hostname IDF-BA-PB
!
vlan 99
name MNG
!
vtp mode client
vtp domain UIOS
!
interface Port-channel3

```

```

switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel4
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet1/0
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/1
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/2
switchport trunk native vlan 99
switchport mode trunk
channel-group 3 mode on
!
interface FastEthernet1/3
switchport trunk native vlan 99
switchport mode trunk
channel-group 3 mode on
!
interface FastEthernet1/4

```



```

switchport trunk native vlan 99
switchport mode trunk
channel-group 4 mode on
!
interface FastEthernet1/5
switchport trunk native vlan 99
switchport mode trunk
channel-group 4 mode on
!
interface FastEthernet1/6
switchport mode trunk
!
interface Vlan99
ip address 10.1.1.5 255.255.255.0
!
router ospf 2
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 1
network 172.17.0.0 0.0.255.255 area 1
!
End

```

Script configuración del equipo IDF-BB-P1

```

!
hostname IDF-BB-P1
!
vlan 99
name MNG

```

```

!
vtp mode client
vtp domain UIOS
!
interface Port-channel2
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel5
switchport trunk native vlan 99
switchport mode trunk
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet1/0
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/1
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet1/2
switchport trunk native vlan 99
switchport mode trunk
channel-group 2 mode on
!
interface FastEthernet1/3

```

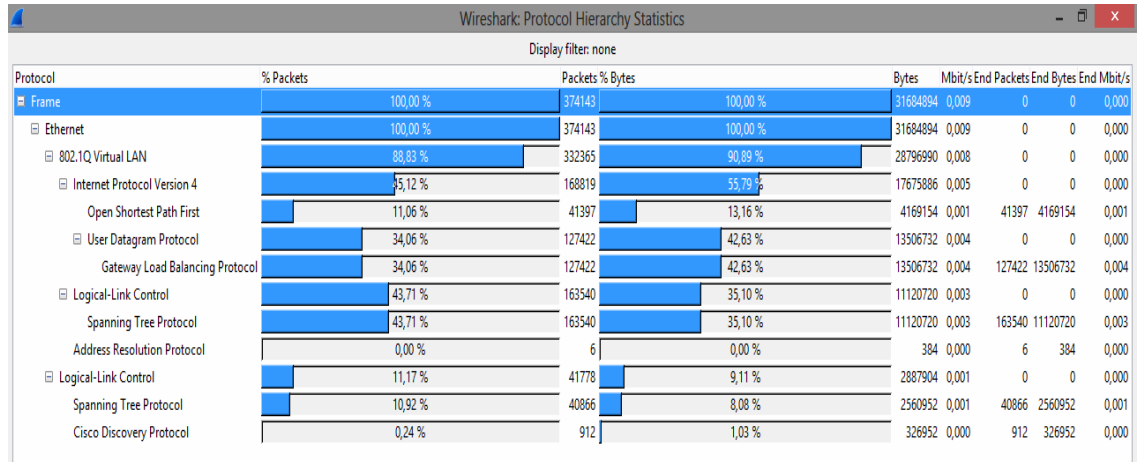
```

switchport trunk native vlan 99
switchport mode trunk
channel-group 2 mode on
!
interface FastEthernet1/4
switchport trunk native vlan 99
switchport mode trunk
channel-group 5 mode on
!
interface FastEthernet1/5
switchport trunk native vlan 99
switchport mode trunk
channel-group 5 mode on
!
interface FastEthernet1/6
switchport mode trunk
!
interface FastEthernet1/7
switchport mode trunk
!
interface Vlan99
ip address 10.1.1.6 255.255.255.0
!
router ospf 2
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 1
network 172.17.0.0 0.0.255.255 area 1
!
End

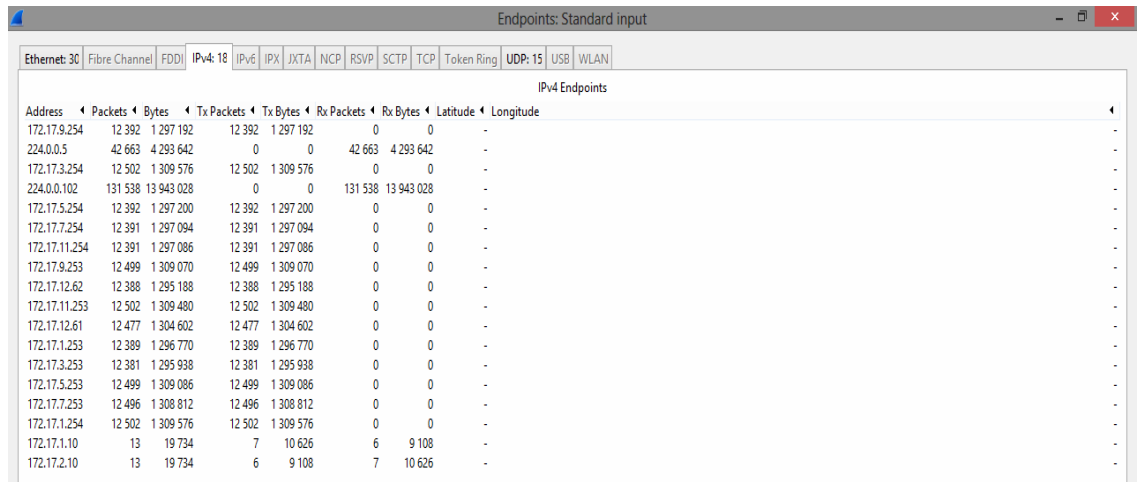
```

Graficas de funcionamiento de la simulación.

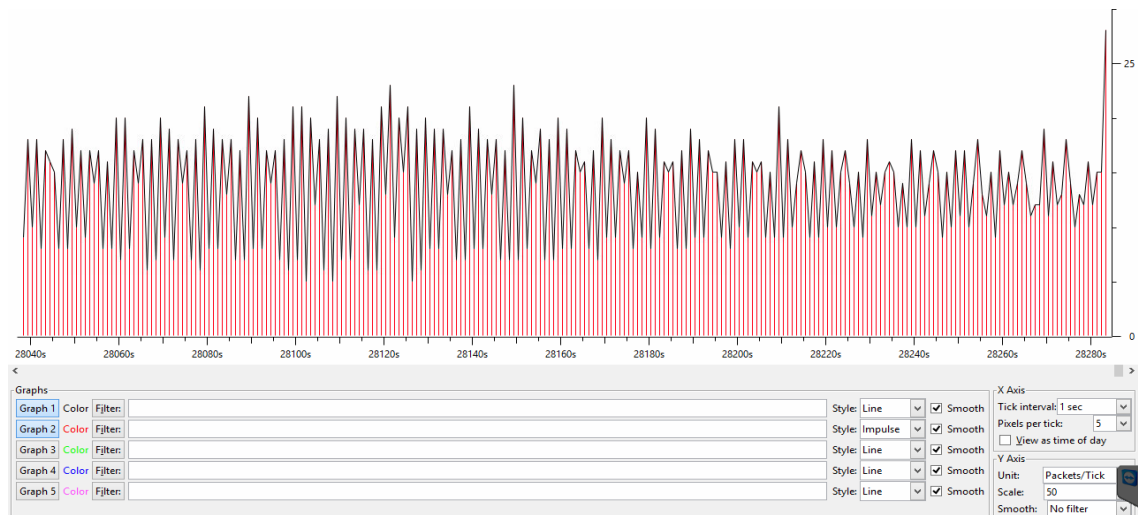
Uso de protocolos en IDF-BA-P5 INT F1/7



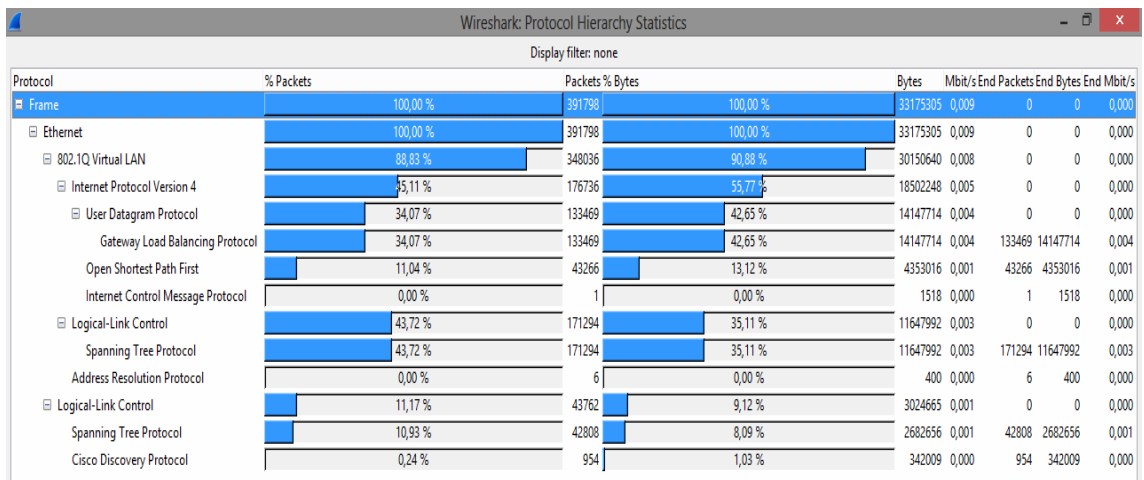
Paquetes y direcciones IP en IDF-BA-P5 INT F1/7



Flujo de información en IDF-BA-P5 INT F1/7



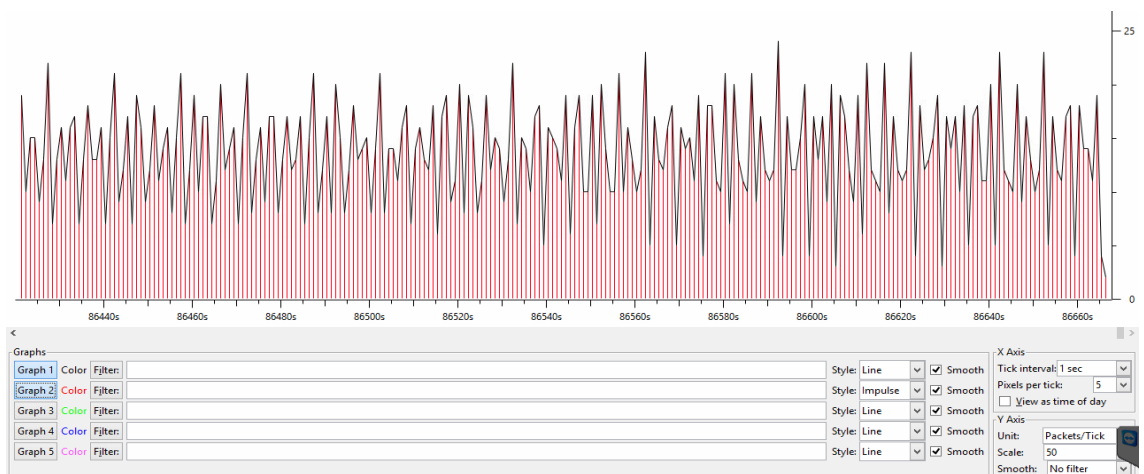
Uso de protocolos en IDF-BA-P4 INT F1/7



Paquetes y direcciones IP en IDF-BA-P4 INT F1/7

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
172.17.5.253	38 398	4 021 868	38 398	4 021 868	0	0	-	-
224.0.0.102	404 227	42 848 062	0	0	404 227	42 848 062	-	-
172.17.7.254	38 081	3 986 358	38 081	3 986 358	0	0	-	-
224.0.0.5	131 040	13 191 468	0	0	131 040	13 191 468	-	-
172.17.7.253	38 392	4 021 372	38 392	4 021 372	0	0	-	-
172.17.1.254	38 419	4 024 518	38 419	4 024 518	0	0	-	-
172.17.9.254	38 081	3 986 358	38 081	3 986 358	0	0	-	-
172.17.3.254	38 418	4 024 412	38 418	4 024 412	0	0	-	-
172.17.5.254	38 080	3 986 260	38 080	3 986 260	0	0	-	-
172.17.11.254	38 080	3 986 252	38 080	3 986 252	0	0	-	-
172.17.9.253	38 391	4 021 326	38 391	4 021 326	0	0	-	-
172.17.12.62	38 072	3 981 264	38 072	3 981 264	0	0	-	-
172.17.11.253	38 400	4 022 416	38 400	4 022 416	0	0	-	-
172.17.12.61	38 340	4 009 632	38 340	4 009 632	0	0	-	-
172.17.1.253	38 059	3 983 818	38 059	3 983 818	0	0	-	-
172.17.3.253	38 056	3 983 676	38 056	3 983 676	0	0	-	-
172.17.1.10	1	1 518	1	1 518	0	0	-	-
172.17.2.10	1	1 518	0	0	1	1 518	-	-

Flujo de información en IDF-BA-P4 INT F1/7



Uso de protocolos en IDF-BA-PB INT F1/6

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100,00 %	1190425	100,00 %	100813225	0,009	0	0	0	0	0	0,000
Ethernet	100,00 %	1190425	100,00 %	100813225	0,009	0	0	0	0	0	0,000
802.1Q Virtual LAN	88,85 %	1057670	90,90 %	91635230	0,008	0	0	0	0	0	0,000
Internet Protocol Version 4	5,11 %	537029	55,78 %	56231682	0,005	0	0	0	0	0	0,000
User Datagram Protocol	34,06 %	405486	42,63 %	42981516	0,004	0	0	0	0	0	0,000
Gateway Load Balancing Protocol	34,06 %	405486	42,63 %	42981516	0,004	405486	42981516	0,004	42981516	0,004	0,004
Open Shortest Path First	11,05 %	131542	13,14 %	13248648	0,001	131542	13248648	0,001	131542	13248648	0,001
Internet Control Message Protocol	0,00 %	1	0,00 %	1518	0,000	1	1518	0,000	1	1518	0,000
Logical-Link Control	43,73 %	520627	35,12 %	35402636	0,003	0	0	0	0	0	0,000
Spanning Tree Protocol	43,73 %	520627	35,12 %	35402636	0,003	520627	35402636	0,003	520627	35402636	0,003
Address Resolution Protocol	0,00 %	14	0,00 %	912	0,000	14	912	0,000	14	912	0,000
Logical-Link Control	11,15 %	132755	9,10 %	9177995	0,001	0	0	0	0	0	0,000
Spanning Tree Protocol	10,91 %	129858	8,07 %	8137972	0,001	129858	8137972	0,001	129858	8137972	0,001
Cisco Discovery Protocol	0,24 %	2897	1,03 %	1040023	0,000	2897	1040023	0,000	2897	1040023	0,000

Paquetes y direcciones IP en IDF-BA-PB INT F1/6

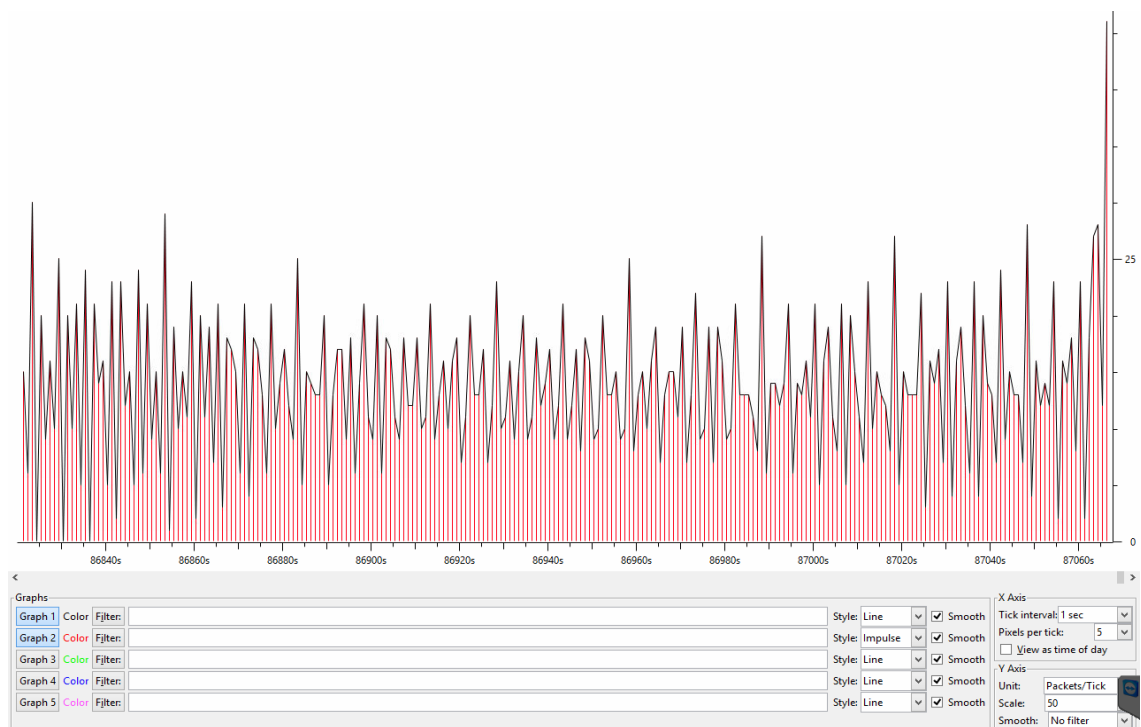
Endpoints: Standard input

Ethernet: 30 Fibre Channel: FDDI: IPv4: 18 IPv6: IPX: JXTA: NCP: RSVP: SCTP: TCP: Token-Ring: UDP: 15 USB: WLAN:

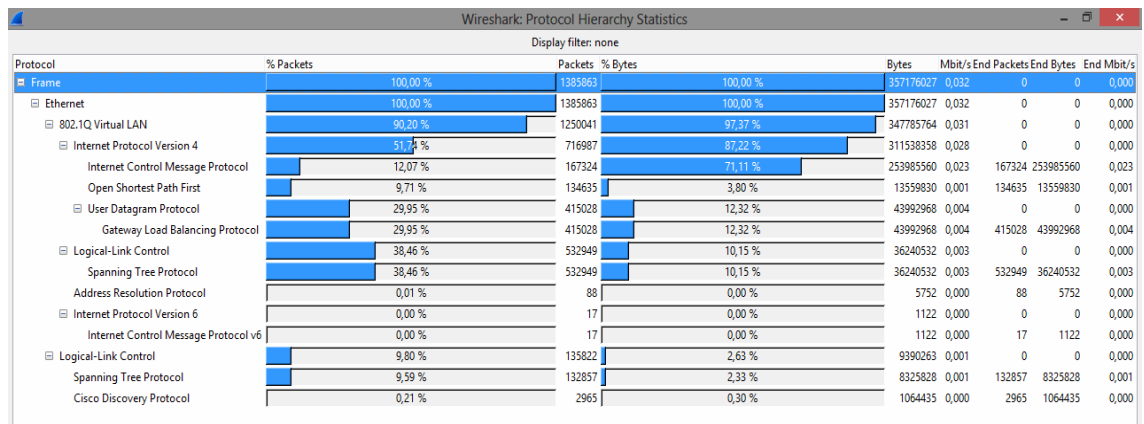
IPv4 Endpoints

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
172.17.1.253	38 215	4 000 738	38 215	4 000 738	0	0	-	-
224.0.0.102	405 801	43 014 906	0	0	405 801	43 014 906	-	-
172.17.3.253	38 216	4 000 764	38 216	4 000 764	0	0	-	-
172.17.5.253	38 551	4 038 406	38 551	4 038 406	0	0	-	-
172.17.7.253	38 546	4 038 028	38 546	4 038 028	0	0	-	-
172.17.1.254	38 576	4 041 452	38 576	4 041 452	0	0	-	-
172.17.12.61	38 497	4 026 330	38 497	4 026 330	0	0	-	-
224.0.0.5	131 633	13 257 566	0	0	131 633	13 257 566	-	-
172.17.11.253	38 551	4 038 734	38 551	4 038 734	0	0	-	-
172.17.9.253	38 547	4 038 230	38 547	4 038 230	0	0	-	-
172.17.3.254	38 576	4 041 452	38 576	4 041 452	0	0	-	-
172.17.5.254	38 232	4 002 540	38 232	4 002 540	0	0	-	-
172.17.7.254	38 234	4 002 752	38 234	4 002 752	0	0	-	-
172.17.9.254	38 234	4 002 752	38 234	4 002 752	0	0	-	-
172.17.11.254	38 234	4 002 752	38 234	4 002 752	0	0	-	-
172.17.12.62	38 225	3 997 542	38 225	3 997 542	0	0	-	-
172.17.1.10	1	1 518	1	1 518	0	0	-	-
172.17.2.10	1	1 518	0	0	1	1 518	-	-

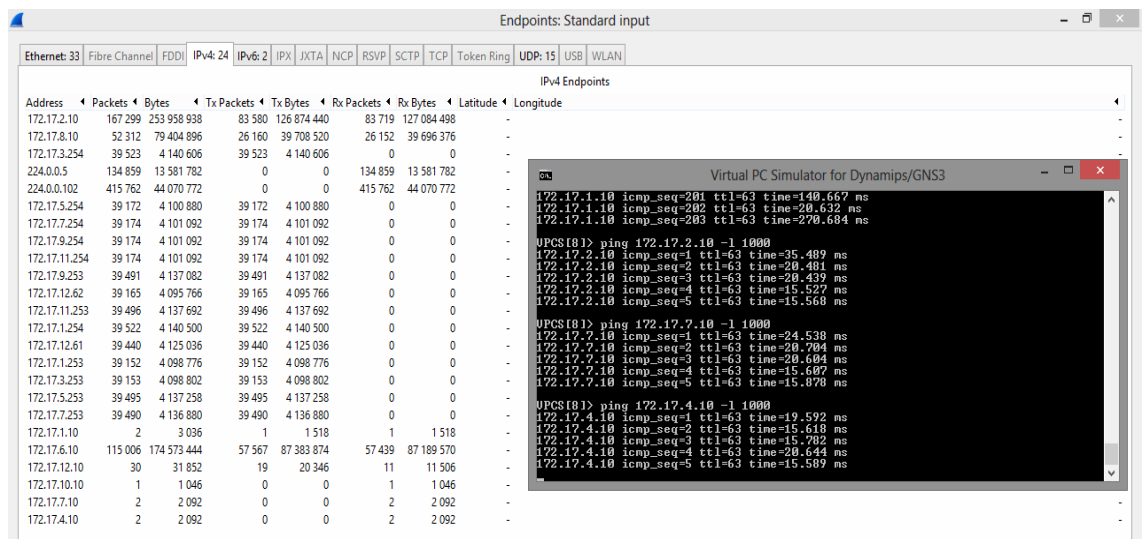
Flujo de información en IDF-BA-PB INT F1/6



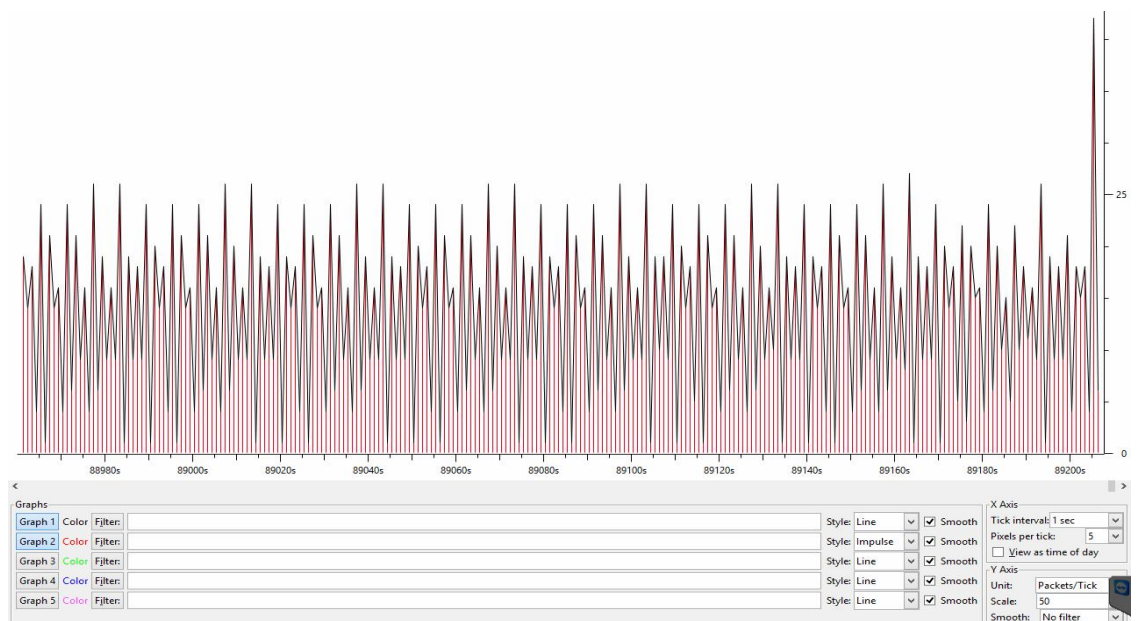
Uso de protocolos en IDF-BB-P1 INT F1/7



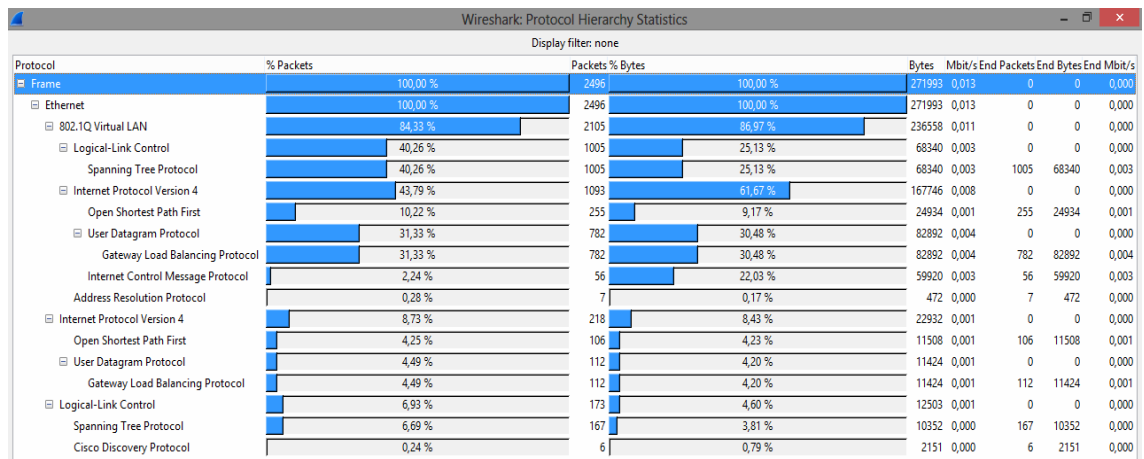
Paquetes y direcciones IP en IDF-BB-P1 INT F1/7



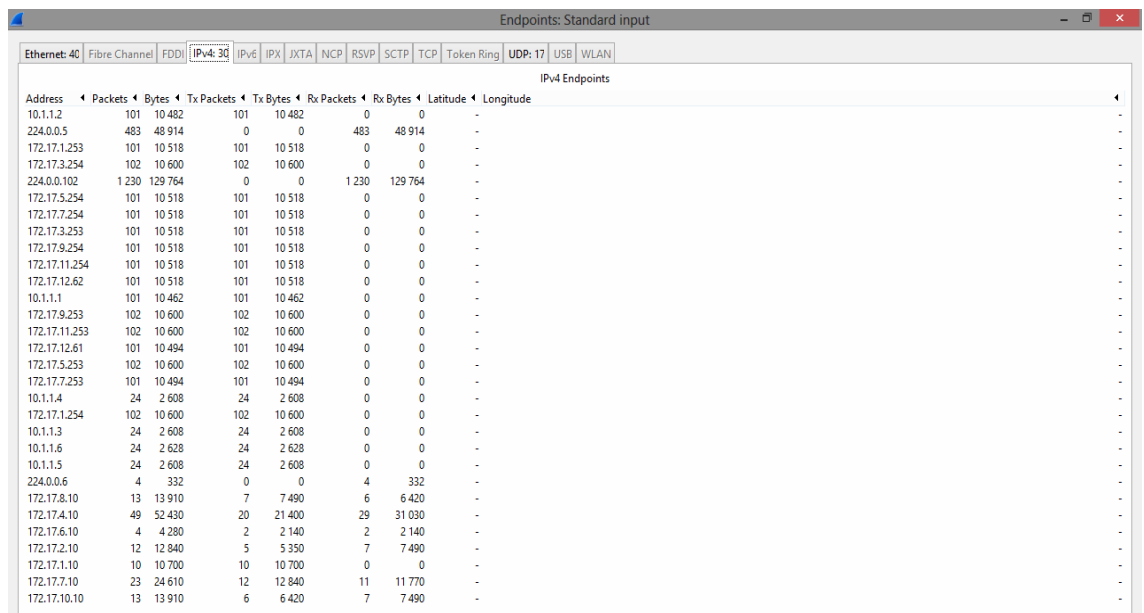
Flujo de información en IDF-BB-P1 INT F1/7



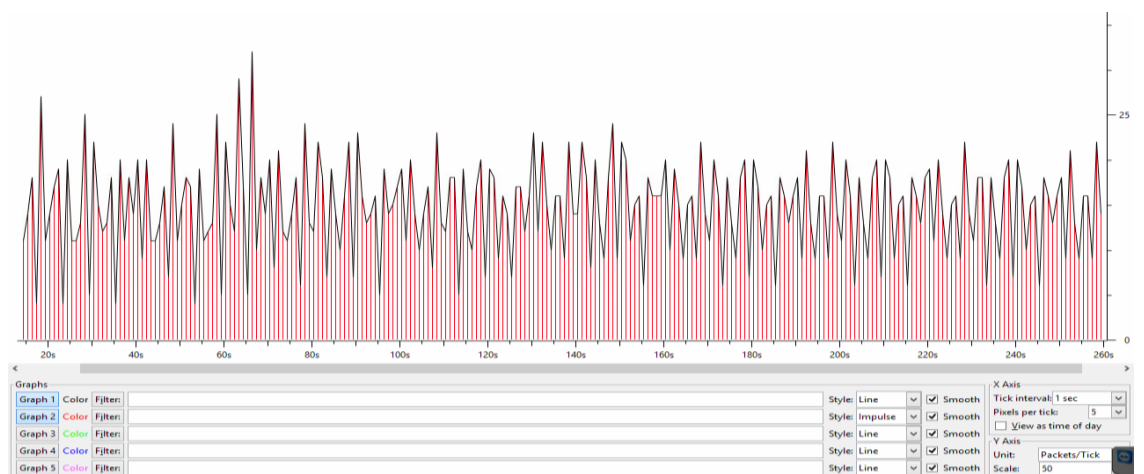
Uso de protocolos en MDF-UIOS INT F1/3



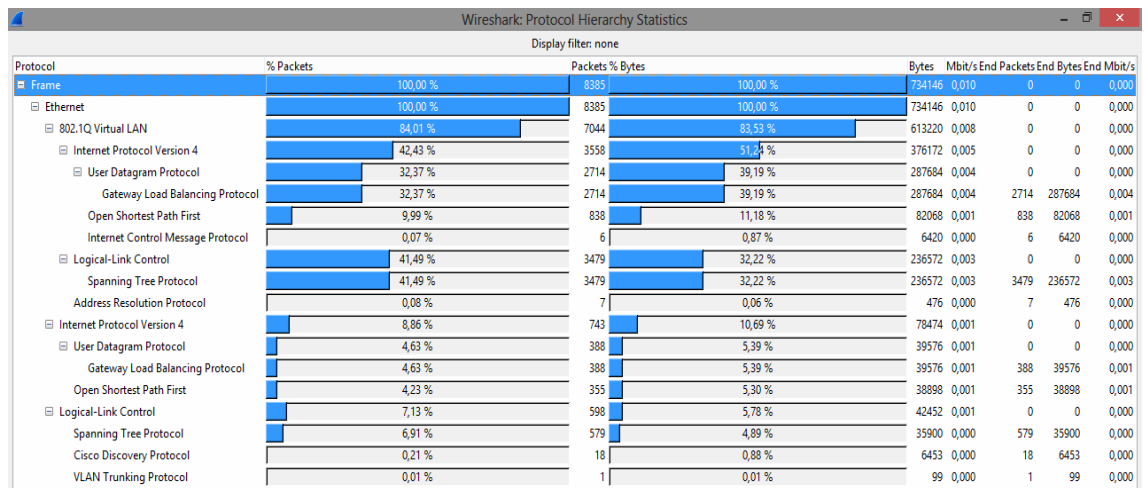
Paquetes y direcciones IP en MDF-UIOS INT F1/3



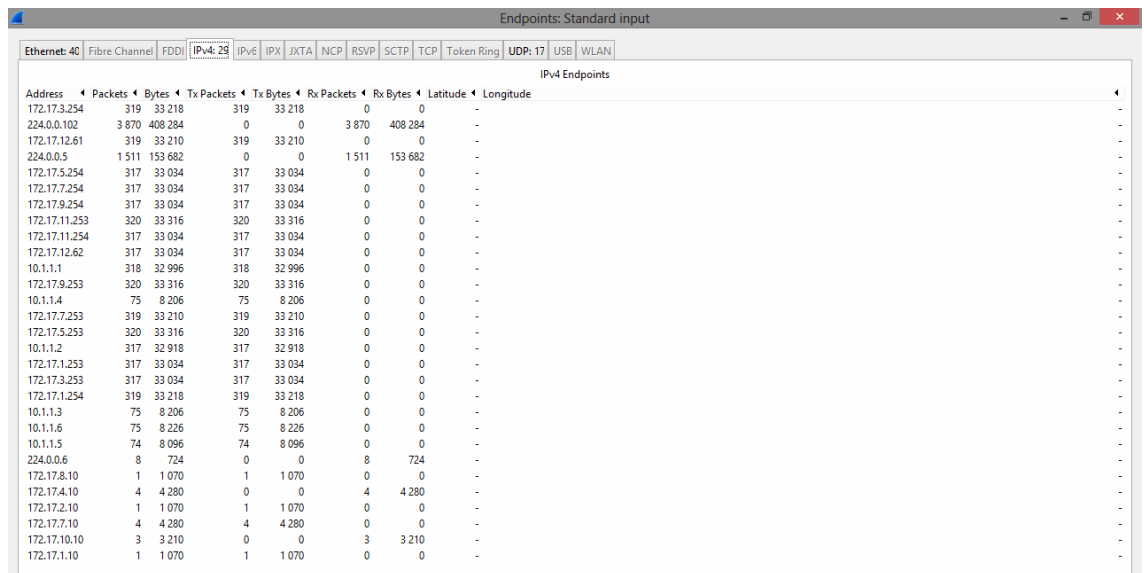
Flujo de información en MDF-UIOS INT F1/3



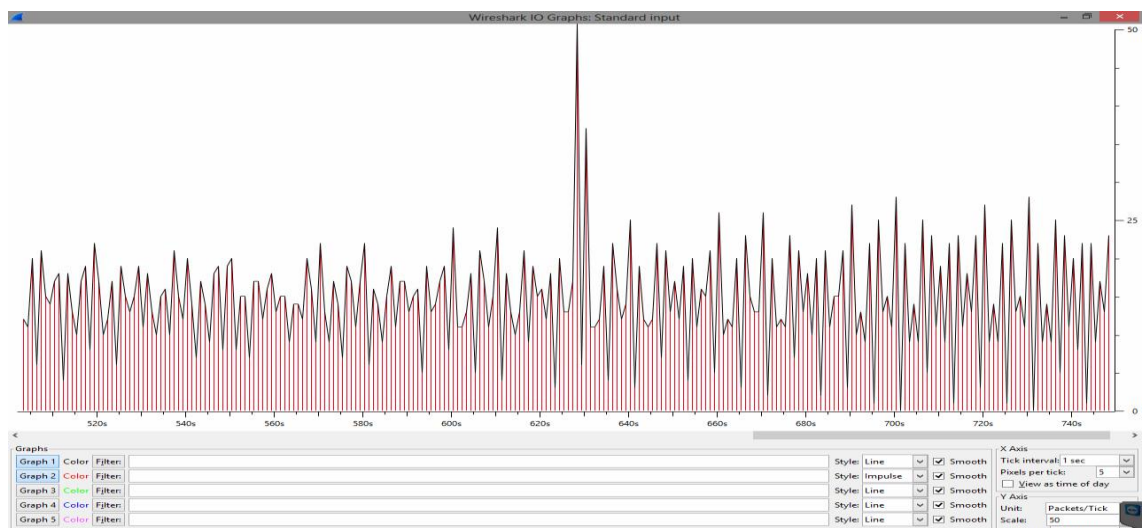
Uso de protocolos en MDF-UIOS INT F1/7



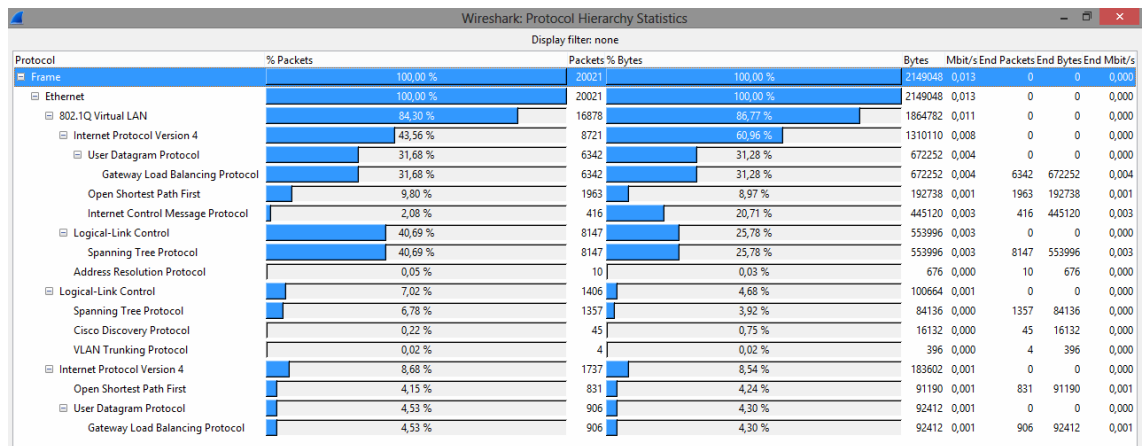
Paquetes y direcciones IP en MDF-UIOS INT F1/7



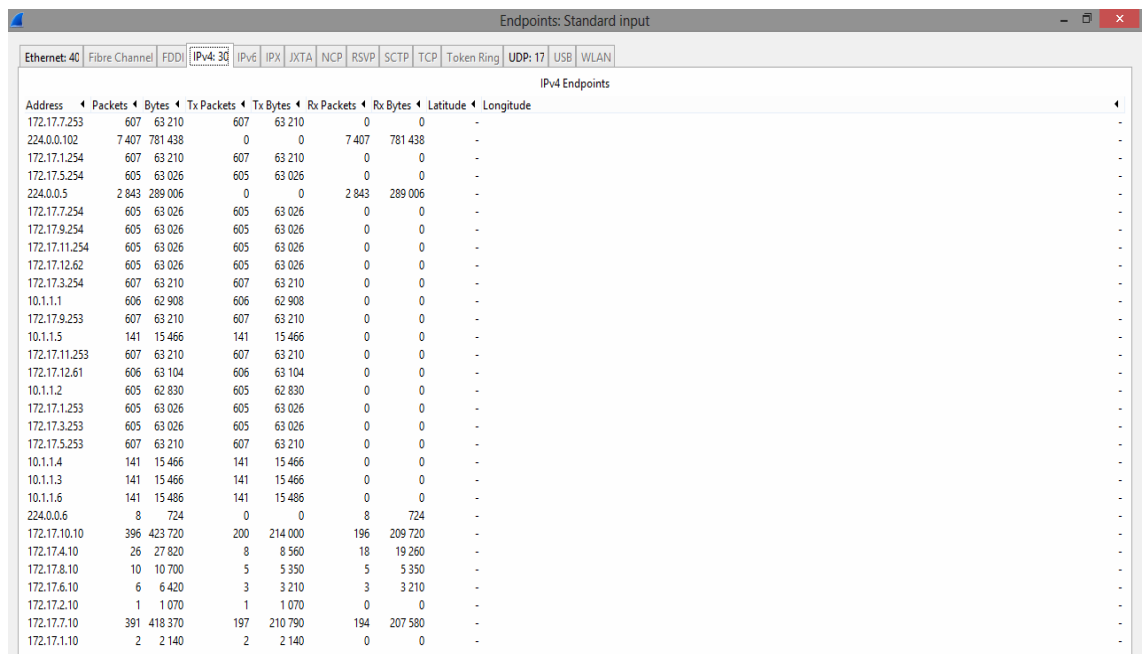
Flujo de información en MDF-UIOS INT F1/7



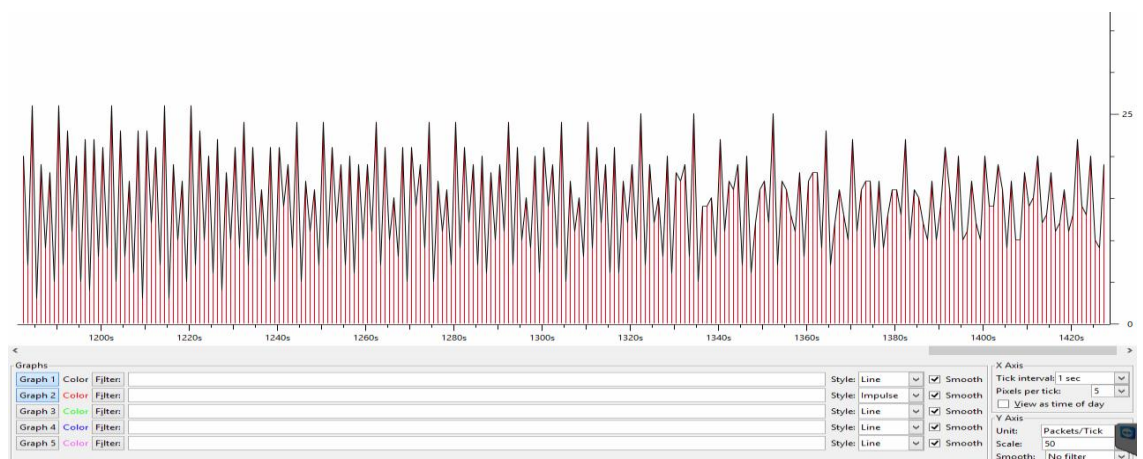
Uso de protocolos en MDF-UIOS INT F1/9



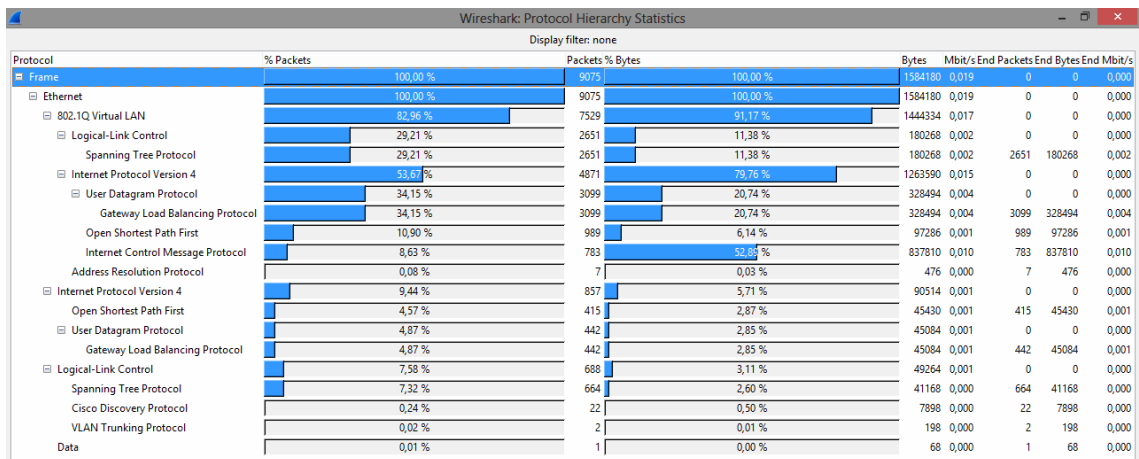
Paquetes y direcciones IP en MDF-UIOS INT F1/9



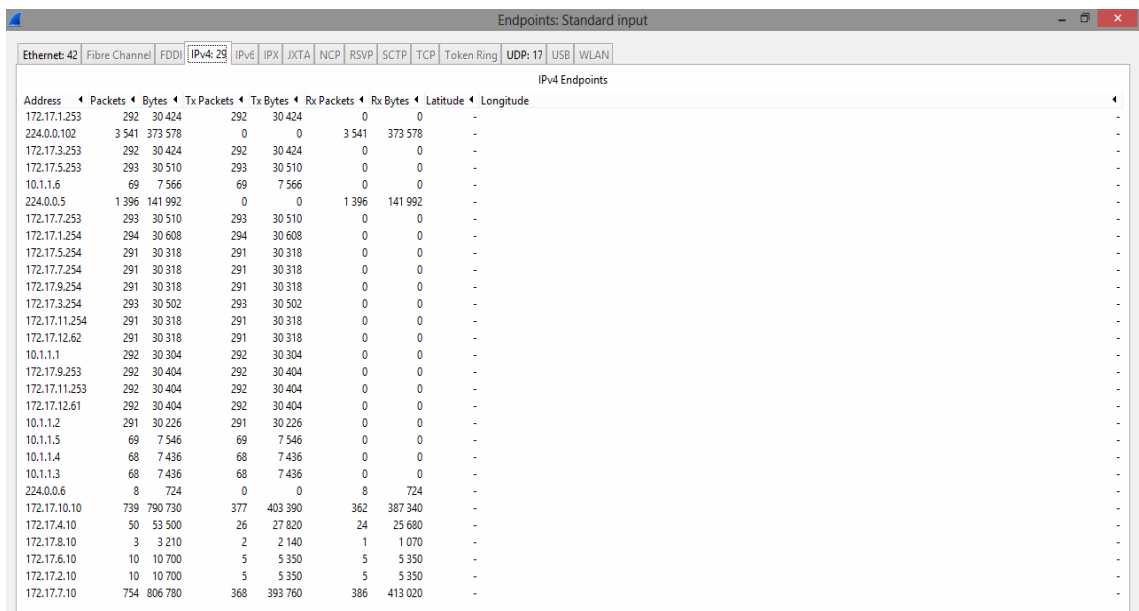
Flujo de información en MDF-UIOS INT F1/9



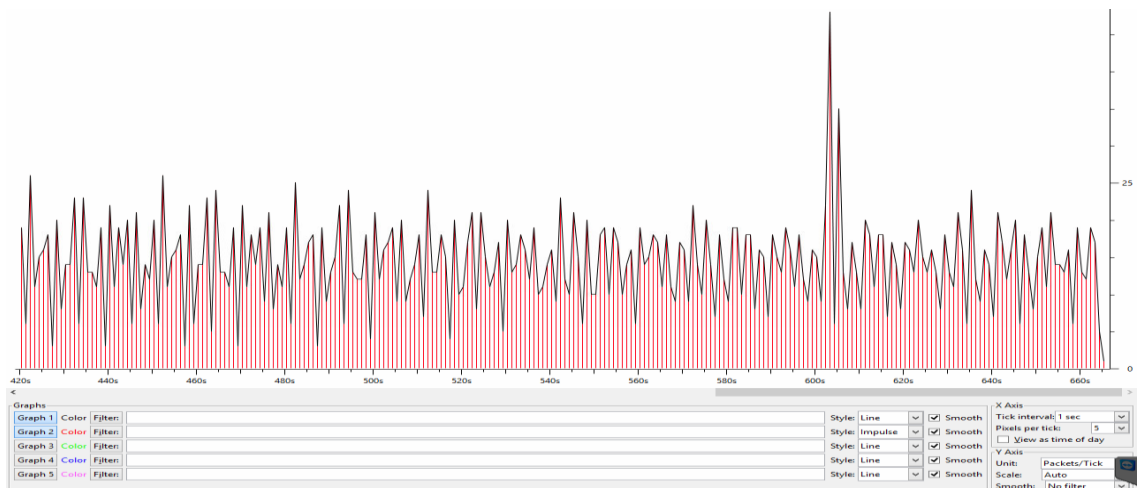
Uso de protocolos en MDF-UIOS INT F1/1



Paquetes y direcciones IP en MDF-UIOS INT F1/1



Flujo de información en MDF-UIOS INT F1/1



Uso de protocolos en enlace GATEWAY-OUT-INTERNET

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End	Packets	End	Bytes	End	Mbit/s
Frame	100,00 %	16938	100,00 %	19379678	0,018	0	0	0	0,000		
Ethernet	100,00 %	16938	100,00 %	19379678	0,018	0	0	0	0,000		
Internet Protocol Version 4	87,79 %	14870	98,91 %	19168240	0,018	0	0	0	0,000		
Internet Control Message Protocol	74,14 %	12558	93,12 %	18434864	0,017	12558	18434864	0,017			
Open Shortest Path First	11,49 %	1947	0,97 %	187706	0,000	1947	187706	0,000			
Data	2,15 %	365	2,82 %	545670	0,000	365	545670	0,000			
Logical-Link Control	1,72 %	291	0,53 %	102871	0,000	0	0	0,000			
Cisco Discovery Protocol	1,72 %	291	0,53 %	102871	0,000	291	102871	0,000			
Configuration Test Protocol (loopback)	10,31 %	1747	0,54 %	104820	0,000	0	0	0,000			
Data	10,31 %	1747	0,54 %	104820	0,000	1747	104820	0,000			
Data	0,18 %	30	0,02 %	3747	0,000	30	3747	0,000			

Paquetes y direcciones IP en enlace GATEWAY-OUT-INTERNET

Conversations: Standard input

Ethernet: 10 | Fibre Channel | FDDI | IPv4 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP | Token Ring | UDP | USB | WLAN

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets B-A	Bytes B-A	Rel Start	Duration	bps A-B	bps B-A
172.17.1.10	186.3.120.241	751	555 378	316	271 788	435	283 590	0,000000000	1972,5017	1102,31	1150,17
186.3.120.247	224.0.0.5	982	95 160	982	95 160	0	0	3,765678000	8735,9742	87,14	N/A
186.3.120.241	224.0.0.5	960	90 920	960	90 920	0	0	5,821171000	8733,6255	83,28	N/A
172.17.2.10	186.3.120.241	160	242 240	80	121 120	80	121 120	81,376619000	88,1183	10996,12	10996,12
172.17.4.10	186.3.120.241	320	484 480	160	242 240	160	242 240	200,420788000	582,7303	3325,59	3325,59
172.17.1.254	186.3.120.241	19	2 166	9	1 026	10	1 140	618,221395000	6,2394	1315,51	1461,68
0.0.1.10	186.3.120.241	1	70	1	70	0	0	816,275496000	0,0000	N/A	N/A
172.17.12.10	186.3.120.241	11 689	17 697 146	5 845	8 849 330	5 844	8 847 816	2118,554078000	6621,1958	10692,12	10690,29
186.3.120.241	186.3.120.247	8	2 080	4	732	4	1 348	2638,654126000	3847,1869	1,52	2,80

Flujo de información en enlace GATEWAY-OUT-INTERNET

