



UNIVERSIDAD TÉCNICA DE AMBATO

**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E
INDUSTRIAL**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y
COMUNICACIONES**

TEMA:

**CLÚSTER DE ALTA DISPONIBILIDAD PARA EL SERVIDOR DE
AUTENTICACIÓN DE LA RED WI-FI DE LA FISEI**

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones.

SUBLÍNEA DE INVESTIGACIÓN:

Sistemas Distribuidos

AUTOR: Luis Felipe Chuncha Mastha
TUTOR: Ing. David Omar Guevara Aulestia, Mg.

Ambato - Ecuador
Julio, 2014

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

“Clúster de alta disponibilidad para el servidor de autenticación de la red WI-FI de la FISEI”, del señor Chuncha Mastha Luis Felipe, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato

Ambato Julio 02, 2014

EL TUTOR

Ing. David Omar Guevara Aulestia, Mg.

AUTORÍA

El presente trabajo de investigación titulado: “Clúster de alta disponibilidad para el servidor de autenticación de la red WI-FI de la FISEI”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Julio 02, 2014

Luis Felipe Chuncha Mastha

CC: 180415380-5

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentes: Ing. José Vicente Morales Lozada, Mg., Ing. Víctor Santiago Manzano Villafuerte, Mg. e Ing. Santiago Mauricio Altamirano Meléndez, Mg. revisó y aprobó el Informe Final del trabajo de graduación titulado “Clúster de alta disponibilidad para el servidor de autenticación de la red WI-FI de la FISEI”, presentado por el señor Luis Felipe Chuncha Mastha, de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. José Vicente Morales Lozada, Mg.

PRESIDENTE DEL TRIBUNAL

Ing. Santiago Manzano Villafuerte, Mg.

Ing. Santiago Altamirano Meléndez, Mg.

DOCENTE CALIFICADOR

DOCENTE CALIFICADOR

DEDICATORIA

A Dios, el dador de vida y creador de todas las cosas, por su mano de misericordia que me ha sostenido en las situaciones más difíciles de mi vida.

A mis Padres, quienes han sabido formarme en el camino del bien, por su amor abnegado y respaldo lo cual sé que nunca dejarán de darme.

A mis hermanos por estar a mi lado en las buenas y en las malas por sus consejos y ejemplo a seguir.

Felipe Chuncha.

AGRADECIMIENTO

A Dios, quien ilumina mi mente y guía mis pasos.

A mi familia por su apoyo incondicional en todas mis etapas de estudio.

A la Universidad Técnica de Ambato, especialmente a la querida Facultad de Ingeniería en Sistemas, Electrónica e Industrial, por abrirme las puertas en el desarrollo de mi vida profesional.

Al Ingeniero David Guevara, por todo su tiempo y paciencia en el desarrollo del presente proyecto, por su amistad sincera y sus consejos.

Al Ingeniero Eduardo Chaso, por la apertura y colaboración prestada en conjunto con todo el Departamento de Redes y Sistemas de la FISEI para la elaboración del presente proyecto.

Felipe Chuncha.

ÍNDICE

APROBACIÓN DEL TUTOR	ii
AUTORÍA	iii
APROBACIÓN COMISIÓN CALIFICADORA	iv
Dedicatoria	v
Agradecimiento	vi
Resumen	xv
Glosario de términos y acrónimos	xvii
Introducción	xxi
CAPÍTULO 1 El Problema	1
1.1 Tema de Investigación	1
1.2 Planteamiento del Problema	1
1.3 Delimitación	3
1.4 Justificación	3
1.5 Objetivos	4
1.5.1 General	4
1.5.2 Específicos	4
CAPÍTULO 2 Marco Teórico	5
2.1 Antecedentes Investigativos	5
2.2 Fundamentación Teórica	5
2.2.1 El Clúster	5
2.2.2 Elementos de un Clúster	6
2.2.3 Clasificación	7
2.2.4 Ventajas y desventajas de los clústeres	8
2.2.5 Clúster de alta disponibilidad	9

2.2.6	Configuración de alta disponibilidad	9
2.2.7	Funcionamiento de un Clúster de alta disponibilidad	11
2.2.8	Dinámica de alta disponibilidad	11
2.3	Propuesta de Solución	12
CAPÍTULO 3 Metodología		13
3.1	Modalidad Básica de la Investigación	13
3.1.1	Proyecto de Investigación Aplicada (I)	13
3.2	Recolección de Información	13
3.3	Procesamiento y análisis de datos	14
3.3.1	Procesamiento de la Información	14
3.3.2	Análisis e Interpretación de Resultados	14
3.4	Desarrollo del Proyecto	18
CAPÍTULO 4 Desarrollo de la Propuesta		20
4.1	Datos Informativos	20
4.1.1	Tema de la Propuesta	20
4.1.2	Institución Ejecutora	20
4.1.3	Beneficiarios	20
4.1.4	Ubicación	20
4.1.5	Equipo Responsable	21
4.2	Antecedentes de la Propuesta	21
4.3	Justificación	22
4.4	Objetivos	23
4.4.1	Objetivo General:	23
4.4.2	Objetivos Específicos:	23
4.5	Análisis de Factibilidad	23
4.5.1	Factibilidad Institucional	23
4.5.2	Factibilidad Técnica	23
4.5.3	Factibilidad Operativa	24
4.5.4	Factibilidad Económica	24
4.6	Fundamentación	24
4.6.1	Modelo jerárquico de la red Wi-Fi de la FISEI	24
4.6.2	Entorno virtual en Linux	26
4.6.2.1	Virtualización	26
4.6.2.2	Hypervisor XEN	28
4.6.2.3	Paravirtualización	29
4.6.3	Servidor RADIUS	30

4.6.3.1	Elementos de RADIUS	30
4.6.3.2	Funciones de RADIUS	31
4.6.3.3	FreeRADIUS	31
4.6.3.4	DaloRADIUS	32
4.6.4	Alta disponibilidad	33
4.6.4.1	Cálculo de la disponibilidad	34
4.6.4.2	Clúster de alta disponibilidad en máquinas virtuales	37
4.6.4.3	Soluciones de alta disponibilidad	37
4.6.4.4	Heartbeat como herramienta para Clúster de alta disponibilidad	42
4.6.5	Diseño del Clúster de alta disponibilidad para el servidor de autenticación en la red Wi-Fi de la FISEI.	43
4.6.6	Equipos de red para el Clúster de alta disponibilidad	45
4.6.6.1	Servidor Principal	45
4.6.6.2	Router	46
4.6.6.3	Access Point	50
4.6.6.4	HotSpot	51
4.6.7	Topologías de las redes inalámbricas	52
4.6.7.1	Topología modo Ad-hoc (IBSS)	52
4.6.7.2	Topología modo Infraestructura (BSS)	53
4.6.8	QoS y gestión de ancho de banda (AB)	54
4.6.8.1	QoS basada en directivas	54
4.6.8.2	Consideraciones de ancho de banda para la red Wi- Fi de la FISEI	55
4.7	Ejecución de la Propuesta	56
4.7.1	Diseño general de los entornos virtuales con el hypervisor XEN	56
4.7.2	Requerimientos del Clúster de alta disponibilidad para el servicio de autenticación de la red Wi-Fi de la FISEI	57
4.7.2.1	Hardware	57
4.7.2.2	Software	58
4.7.3	Herramientas de ejecución para la implementación del Clúster de alta disponibilidad	59
4.7.3.1	Instalación de máquina virtual mediante el hypervi- sor XEN con paravirtualización para el servidor de monitoreo de red.	59
4.7.3.2	Monitoreo de la red Wi-Fi de la FISEI	63
4.7.3.3	Protocolo SNMP	63

4.7.3.4	Instalación del software de monitoreo Cacti	64
4.7.3.5	Diseño físico del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi.	71
4.7.3.6	Diseño lógico del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi.	72
4.7.3.7	Instalación de máquina virtual mediante hypervisor XEN con paravirtualización para el servidor RA- DIUS del Nodo 1	72
4.7.3.8	Instalación del Servidor RADIUS en Nodo1	74
4.7.3.9	Instalación de DaloRADIUS en Nodo 1	78
4.7.3.10	Clonación del Nodo 1 (Servidor RADIUS)	79
4.7.3.11	Consideraciones antes de la Instalación del Clúster de alta disponibilidad	84
4.7.3.12	Instalación de Heartbeat y configuración del Clúster para el servicio HTTP	84
4.7.3.13	Configuración de Clúster para el servicio RADIUS	86
4.7.3.14	Configuración de alta disponibilidad de datos por replicación maestro a maestro en MySQL.	87
4.7.3.15	Configuración de dispositivos de red para HotSpot	91
4.7.3.16	Políticas de acceso para el servicio de Autenticación de la red Wi-Fi de la FISEL.	105
4.7.3.17	Directivas QoS en base a las políticas de uso de la red Wi-Fi de la FISEL.	106
4.7.3.18	Configuración de directivas QoS en DaloRADIUS	107
4.8	Discusión y Resultados de la Propuesta	110
4.8.1	Pruebas de alta disponibilidad de servicios	110
4.8.2	Pruebas de alta disponibilidad de datos	112
4.8.3	Visualización de monitoreo del tráfico de red en Cacti	114
4.9	Análisis Económico del Proyecto	114
CAPÍTULO 5 Conclusiones y Recomendaciones		116
5.1	Conclusiones	116
5.2	Recomendaciones	117
Bibliografía		118
ANEXOS		122

ÍNDICE DE TABLAS

4.1	Variables para el cálculo de la disponibilidad en un servicio.	34
4.2	Disponibilidad para un sistema 24×7 y tiempos de caída permitidos. .	36
4.3	Características principales de Heartbeat	38
4.4	Características principales de KeepAlived	39
4.5	Características principales de Ldirectord LVS	40
4.6	Características técnicas del servidor HP Proliant DL180-G6	45
4.7	Características técnicas del router Cisco RV180W	47
4.8	Características técnicas del router Mikrotik RB951G-2HnD	48
4.9	Características técnicas del router Cisco RV180W	49
4.10	Requerimientos hardware	58
4.11	Dinámica de AB - Usuario Invitado	106
4.12	Dinámica de AB - Estudiantes	107
4.13	Dinámica de AB – Profesores y administrativos	107
4.14	Escenario de pruebas – disponibilidad de servicios	112
4.15	Escenario de pruebas – disponibilidad de datos	113
4.16	Presupuesto	115

ÍNDICE DE FIGURAS

1.1	Árbol del problema	3
2.1	Elementos de un Clúster.	6
2.2	Configuración Activo-Activo	10
2.3	Configuración Activo-Pasivo	11
3.1	Tráfico en la red Wi-Fi del 2/12/2013	17
3.2	Tráfico en la red Wi-Fi del 23/12/2013	18
4.1	Modelo Jerárquico de red de la FISEI	25
4.2	Esquema general de virtualización	27
4.3	Esquema XEN –Hypervisor	29
4.4	Esquema de Paravirtualización con Xen	30
4.5	Esquema Básico de Autenticación AAA con RADIUS	31
4.6	Funcionamiento de Heartbeat para un Clúster de alta disponibilidad .	43
4.7	Diseño del Clúster de alta disponibilidad - FISEI	44
4.8	Servidor Principal de la FISEI - HP Proliant DL180-G6	45
4.9	Símbolo genérico del router para redes informáticas	46
4.10	Router Cisco RV180W	47
4.11	Router MikroTik RB951G-2HnD	48
4.12	Router MikroTik 450G	49
4.13	Símbolo genérico del Access Point para redes informáticas	51
4.14	Esquema básico de un HotSpot para servicios de Internet	52
4.15	Topología modo Ad-hoc (IBSS)	53
4.16	Topología modo Infraestructura (BSS)	54
4.17	Entornos virtuales con hypervisor XEN	57
4.18	Selección del idioma para instalación de Centos 5.9	61
4.19	Selección de configuración TCP/IP	61
4.20	Configuración manual TCP/IP	62
4.21	Selección text mode	62
4.22	Inicio de instalación automática	63
4.23	Guia de instalación web de Cacti	69

4.24	Selección del tipo de instalación para Cacti	70
4.25	Verificación de los componentes de instalación para Cacti	70
4.26	Logueo de ingreso web a Cacti	71
4.27	Diseño Físico del Clúster de alta disponibilidad	71
4.28	Diseño lógico del Clúster de alta disponibilidad	72
4.29	Configuraciones de Firewall	74
4.30	Configuración de red en Nodo2	82
4.31	Edición para dispositivos de red en Nodo2	82
4.32	Selección de dispositivo a configurar en Nodo2	83
4.33	Datos de red para Nodo2	83
4.34	Configuración de IP's para WAN y LAN para HotSpot	93
4.35	Configuración DNS para HotSpot	93
4.36	Ventana de configuración para dirección Gateway de la red	94
4.37	Visualización de configuraciones de Route	94
4.38	Ingreso a configuración de HotSpot	95
4.39	Interfaz de HotSpot	95
4.40	Interfaz de HotSpot Dirección de red LAN para HotSpot	95
4.41	Pool de direcciones de red de HotSpot	96
4.42	Certificación SSL en none para HotSpot	96
4.43	Servidor SMPT de HotSpot	96
4.44	Configuración servidor DNS de HotSpot	96
4.45	Nombre DNS de HotSpot	97
4.46	Configuración general de hsprof1	97
4.47	Configuración de Login en hsprof1	98
4.48	Configuración de RADIUS en hsprof1	98
4.49	Configuraciones RADIUS para HotSpot	99
4.50	Logueo de inicio en HotSpot	99
4.51	Conexión FTP-Mikrotik utilizando Filezilla	101
4.52	Homepage de inicio personalizado para HotSpot	105
4.53	Configuración de perfiles en DaloRADIUS - primera sección	108
4.54	Configuración de perfiles en DaloRADIUS - segunda sección	109
4.55	Adición de usuarios en DaloRADIUS	110
4.56	Heartbeat - Nodo1	111
4.57	Heartbeat - Nodo2	111
4.58	Replicación de datos en los dos nodos virtuales	112
4.59	Monitoreo del tráfico de red en los Hotspot	114
B.1	Habilitación SNMP para dispositivos MikroTik	125

B.2	Habilitación SNMP para Cacti	125
C.1	Dispositivos de red Wi-Fi en la FISEI - Edificio 1	126
C.2	Dispositivos de red Wi-Fi en la FISEI - Edificio 2	127

RESUMEN

El Clúster de alta disponibilidad es un conjunto de dos o más máquinas que tiene como característica principal el acceso continuo a los servicios y aplicaciones dentro de una entidad u organización. El siguiente proyecto de investigación presenta un proceso estratégico para llevar a cabo la implementación de un Clúster de alta disponibilidad de 2 nodos virtuales los cuales conforman el servidor de autenticación de la red Wi-Fi de la FISEI, sobre la plataforma libre GNU/Linux. El proyecto hace mención a los componentes más importantes del Clúster y de la misma manera expone los conceptos más relevantes del mismo. Además se muestran las instalaciones y configuraciones de los componentes que conforman el Clúster para poder llevarlo de forma integral a un escenario de pruebas y verificaciones. Finalmente se hace alusión a las conclusiones y recomendaciones desprendidas a lo largo del desarrollo de la propuesta de investigación.

ABSTRACT

The high availability cluster is a set of two or more machines which have as a main feature continued access to services and applications within a company or organization. The following research project presents a strategic process to carry out the implementation of a high availability cluster of two virtual nodes which form the authentication server on the free GNU/Linux platform of the Wi-Fi network of the FISEI. The draft mentions the most important components of the cluster and in the same manner exposes the most relevant concepts of this. Also it shows the installations and configurations of the components so that it is possible to verify the cluster operation comprehensively in a test scenario. Finally it draws conclusions and suggests recommendations detached throughout the development of the research proposal.

Glosario de términos y acrónimos

AAA: (Authentication, authorization, and accounting), siglas que hacen referencia a la autenticación, autorización y anotación o contabilidad de las funciones que realiza un servidor RADIUS.

AP: (Access point), punto de acceso. Se trata de un dispositivo utilizado en redes inalámbricas de área local WLAN para la conexión de dispositivos inalámbricos a esta red.

AB: Siglas que hacen referencia al Ancho de Banda.

Autenticación: Es el proceso de confirmación de algo o alguien como auténtico.

CEAACES: Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior.

Clonación: En informática es el proceso mediante el cual se puede duplicar una máquina o programa con las mismas características que el original.

Dirección IP: Es el número que identifica a un computador dentro de una red que usa el protocolo IP.

Distribución Linux: Es la distribución de software basada en el núcleo Linux.

DNS: (Domain Name System). Sistema de nombre de dominio, Se trata de una base de datos que vincula cada dominio web con su dirección IP correspondiente.

Failback: El proceso que se lleva a cabo una vez que el nodo pasivo empieza a escuchar nuevamente los latidos del nodo activo, entonces éste tomará el control nuevamente.

Failover: Significa tolerancia a fallos y se usa para determinar la capacidad de un sistema para seguir funcionando aun cuando se produce un fallo.

Firewall: Significa cortafuegos y se usa para aquellos sistemas encargados de bloquear los accesos no autorizados en una red.

Framework: Es una estructura conceptual y tecnológica de soporte definido el cual puede contener programas, biblioteca o lenguaje interpretado, entre otras herramientas, para así ayudar a desarrollar y unir los diferentes componentes de un proyecto.

FTP: Es el acrónimo inglés de File Transfer Protocol cuya traducción al español es Protocolo de Transferencia de Archivos y es como su nombre lo indica es el protocolo que se usa en la transferencia de archivos en una red TCP.

Gateway: (Puerta de enlace), es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

HA: Es el acrónimo inglés de High Availability cuya traducción al español es Alta Disponibilidad y se usa para indicar el grado de continuidad operacional de un sistema en un período de tiempo dado.

Homepage: Término en inglés con el cual se hace referencia a la página de inicio o portada es el URL o archivo local que carga cuando se inicia un navegador web, aunque este término o similares pueden referirse a la página principal de un sitio web.

HTTP: Es el acrónimo inglés de Hyper Text Transfer Protocol cuya traducción al español es Protocolo de Transferencia de Hipertexto y es usado para acceder las páginas Web.

HVM: Full Virtualization, es decir, virtualización completa utilizada en la plataforma con hypervisor XEN.

ICMP: (Internet Control Message Protocol), es un protocolo que permite administrar información relacionada con errores de los equipos en red.

Implementación: Es la realización o ejecución de un proyecto o un diseño.

Intercomunicación: Es la capacidad de enviar y recibir mensajes entre dos o más computadores en una red TCP/IP.

Interfaz: Es el medio de conexión física y funcional entre dos sistemas o dispositivos de cualquier tipo dando una comunicación entre distintos niveles.

Internet: Es la red mundial de computadores interconectados que usan el protocolo TCP/IP.

IP: Es el acrónimo inglés de Internet Protocol cuya traducción al español es Protocolo de Internet y es el protocolo encargado de la comunicación entre el origen y el destino en una red TCP/IP.

LAMP: Es el acrónimo usado para describir un sistema de infraestructura de internet que usa las siguientes herramientas: Linux, el sistema operativo; Apache, el servidor web; MySQL/MariaDB, el gestor de bases de datos; Perl, PHP, o Python, los lenguajes de programación.

LAN: (Local Area Network). Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).

Logueo: Es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario.

Migración: Consiste en mover uno o más recursos de un nodo del Clúster a otro.

MTBF: (Mean time between failure). Es el tiempo medio entre fallos.

MTTR: (Mean time to recover). Es el tiempo medio de recuperación

MV: (Virtual Machine). Máquina virtual.

MySQL: Es un sistema de gestión de bases de datos relacional, multihilo y multiusuario.

NAS: (Network Access Server). Es un punto de entrada que permite a los usuarios o clientes acceder a una red.

Nodo: Es una máquina o servidor miembro del Clúster.

Página Web: Es el acrónimo inglés de World Wide Web cuya traducción al español es Red Informática Mundial y consiste en un documento basado en hipertexto que permite.

PHP: Es un lenguaje de programación de uso general de código del lado del servidor originalmente diseñado para el desarrollo web de contenido dinámico.

Protocolo: Es un conjunto de reglas establecidas para la comunicación entre dispositivos.

QoS: (Quality of Service). Es la calidad de servicio en cuanto a la priorización de tráfico y la garantía de un ancho de banda mínimo.

RADIUS: (Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Replicación: Consiste en copiar o duplicar los datos de un nodo a otro.

Servicio: Es un conjunto de actividades que responden a las necesidades de un cliente.

Servidor: Es una computadora que provee uno o más servicios u otras computadoras.

SLA: (Service Level Agreement). Acuerdo de nivel de servicio, es el proceso responsable de identificar y delimitar los requerimientos de servicio de los clientes.

SNMP: (Simple Network Management Protocol). Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. TCP/IP: Es conjunto de protocolos que hacen posible la comunicación entre computadores.

TCP: Son las siglas del término en inglés Transmission Control Protocol cuya traducción al español es Protocolo de Control de Transmisión y es el protocolo encargado de garantizar que los mensajes sean entrados en su destino.

URL: Un localizador de recursos uniforme, es una secuencia de caracteres, de acuerdo a un formato modélico y estándar que se usa para nombrar recursos en Internet para su localización o identificación.

WAN: (Wide Area Network). Es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes.

Wi-Fi: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

VIP: Virtual IP.

INTRODUCCIÓN

Las tecnologías basadas en clústeres hoy en día juegan un papel muy importante en el ámbito de las ciencias y las ingenierías en cuanto al desarrollo y ejecución de aplicaciones que van desde la supercomputación hasta software adaptado a misiones críticas pasando por las aplicaciones, los servicios y las bases de datos.

De acuerdo a la aplicabilidad de los clústeres se han desarrollado diferentes líneas tecnológicas en este campo, en base a esto surge el concepto de Clúster de servidores virtuales el cual se implementa mediante la utilización de máquinas virtuales en red destinadas a efectuar un trabajo compartido en función de determinados objetivos como pueden ser, el balanceo de la carga, el rendimiento, o la disponibilidad de los servicios, este conjunto de servidores atiende el trabajo en el que la caída de uno de ellos no ocasionaría la caída total del sistema.

Una de las tecnologías clústering que permite el mantenimiento de servidores de manera que exista entre ellos el respaldo de la información para que esta nunca se pierda, se la conoce como “Clúster de alta disponibilidad”, este tipo de clústeres permiten que exista flexibilidad y robustez en ambientes de intercambio masivo de información así como para almacenamiento de datos sensibles. De la misma manera esta tecnología brinda una disponibilidad continua al momento de requerir un servicio.

Los clústeres de alta disponibilidad permiten un fácil acceso y manipulación de sus servidores en cuanto al mantenimiento que estos requieran de tal forma que una máquina del Clúster se la puede sacar de línea, apagarla o repararla sin comprometer el funcionamiento integral de los servicios que brinda el Clúster.

El presente proyecto de investigación trata sobre la implementación de la tecnología Clúster enfocado a brindar alta disponibilidad al servicio de autenticación de la red Wi-Fi de la FISEI.

CAPÍTULO 1

El Problema

1.1. Tema de Investigación

CLÚSTER DE ALTA DISPONIBILIDAD PARA EL SERVIDOR DE AUTENTICACIÓN DE LA RED WI-FI DE LA FISEI.

1.2. Planteamiento del Problema

Las comunicaciones a través de las redes hoy en día se han convertido en un ente vital en el trabajo diario del ser humano, el cual accede de forma continua a estos medios por los cuales circulan gran cantidad de datos los mismos que muchas veces son ignorados por los usuarios, ya que al no contar con procesos adecuados en el tratamiento de la información podrían traer complicaciones en la eficiencia de las redes. Tal es el caso en cuanto al continuo crecimiento que ha tenido el Internet a nivel mundial en los últimos años en el que no es difícil encontrarse con servidores que reciban miles o millones de conexiones diarias, teniendo que atender concurrentemente quizás a cientos o miles de ellas. Es así que la estructura de Internet se ve enfrentada cada día en la aplicación de procesos y estrategias necesarias, a fin de satisfacer las demandas crecientes por parte de los usuarios en cuanto al continuo y disponible servicio que se les debe ofrecer. Por lo mismo se deberán tomar medidas técnicas necesarias a fin de evitar futuros colapsos a nivel global.

La mayoría de países en el mundo se han ido actualizando a nivel tecnológico especialmente en lo que tiene que ver con las comunicaciones, y Ecuador no ha sido la excepción, ya que las entidades indistintamente si son estas públicas o privadas de acuerdo a su nivel, hacen uso de los beneficios que brindan las comunicaciones,

beneficios que permiten su desarrollo propio y a su vez el trabajo en función de una comunidad de usuarios los mismos que día a día se valen de sus servicios. Es por tanto, en la actualidad las organizaciones dependen cada vez más de los sistemas de comunicación, y como es obvio se desea que estos sean seguros y permanezcan disponibles el mayor tiempo posible. Para cualquier empresa o institución, una interrupción de sus redes de comunicación supone un serio problema. Esto puede darse debido a la alta exigencia que sufren sus equipos ocasionando la caída de sistemas o a su vez pueden darse fallas de tipo hardware, accidentes de conectividad, en fin las interrupciones en las comunicaciones pueden ser causadas por varios factores, ocasionando desavenencias y retardos de trabajo tanto en los operadores como en los usuarios beneficiados, factores que para algunos sectores pueden significar serias pérdidas económicas.

En cuanto a las entidades educativas dentro del país se tiene el caso de las Universidades las cuales emplean las comunicaciones a diario en el desarrollo de su trabajo cotidiano. En este caso al tomar en cuenta a la Universidad Técnica de Ambato y más específicamente la Facultad de Ingeniería en Sistemas Electrónica e Industrial – FISEI, se puede destacar la utilidad indispensable de las redes de comunicaciones por parte de los usuarios, especialmente la utilidad de la red Wi-Fi a la cual pueden acceder todos los estudiantes de la Facultad y que por lo mismo estos esperan un rendimiento adecuado de la red, libre de complicaciones en lo que tiene que ver con la disponibilidad, desempeño y atención a las múltiples necesidades de los mismos. Al enfocarse en el servicio de autenticación para el acceso a la red Wi-Fi de la FISEI tanto los estudiantes como las personas que tienen acceso a esta red mediante autenticación, requieren que este servicio sea eficiente y disponible todo el tiempo es decir libre de fallas o interrupciones en dicho servicio, por lo cual los sistemas hardware y software deben estar a la altura en la calidad que se quiere brindar con este servicio. Lamentablemente la Facultad no emplea el equipamiento necesario ni los mecanismos para brindar alta disponibilidad en ninguno de los servicios de redes, por lo que estos no se encuentran inmunes de cualquier peligro de fallas en la red.

A continuación con el árbol del problema se puede ver más a detalle el trasfondo del problema observando sus principales causas y consecuencias.

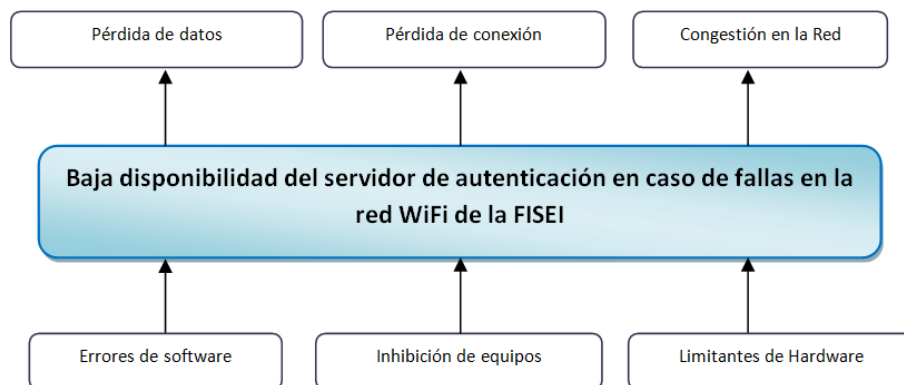


Figura 1.1: Árbol del problema
Fuente: El Investigador

1.3. Delimitación

Área Académica: Programación y Redes.

Línea de Investigación: Programación y Redes.

Sublínea de Investigación: Sistemas Distribuidos.

Espacio: Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato.

Tiempo: El tiempo estimado para la realización del proyecto de investigación tendrá un periodo de duración de 6 meses luego de la aprobación por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4. Justificación

La alta disponibilidad es un servicio muy requerido hoy en día por cualquier entidad debido a las características que este servicio brinda en cuanto a protección o recuperación de interrupciones o caídas, de forma automática y en un corto plazo de tiempo. Cada día, los usuarios utilizan más los servicios en las redes de comunicaciones por lo cual exigen que estos sean rápidos, íntegros e ininterrumpidos. Pero muchos de estos factores requieren una gran inversión que en diversos casos, no es factible realizarla, por tanto se tienen que continuar con los métodos de transmisión tradicionales.

De esta manera se ve imperativa la necesidad de crear en la FISEI una solución tecnológica de bajo costo, alto desempeño, tolerancia a fallos y disponibilidad continua, que supla a cabalidad las necesidades expuestas por los usuarios y que

ofrezca proyección en cuanto a su fortalecimiento. Por este motivo, se plantea un Clúster con dichas características las cuales permitirán ofrecer una alta atención a las múltiples peticiones de los usuarios de la facultad en el uso del servicio de autenticación en la red inalámbrica Wi-Fi.

Actualmente ninguno de los servidores que trabajan en beneficio de las redes de comunicaciones de la FISEI cuenta con los mecanismos necesarios, los cuales permitan dar alta disponibilidad a sus sistemas, por tal razón se pretende desarrollar el presente proyecto el cual representa un aporte innovador en materia de ahorro y eficacia tecnológica, por lo cual la Facultad y en sí, la misma Universidad serán las mayores beneficiadas.

Finalmente, tomando en cuenta que la implementación de clústeres en las redes causa un gran beneficio tecnológico, y echando ventaja de esto; al implementar un Clúster con las características de alta disponibilidad al servidor de autenticación de la FISEI, y por ser el primero, se podrá dar paso al desarrollo de nuevas ideas tecnológicas dentro de la Facultad para el mejor aprovechamiento de los recursos y por lo mismo se estará contribuyendo en el avance de las redes de comunicaciones y progreso tecnológico.

1.5. Objetivos

1.5.1. General

Implementar un Clúster para brindar alta disponibilidad al servidor de autenticación de la red Wi-Fi de la FISEI.

1.5.2. Específicos

- Determinar la estructura de un Clúster de alta disponibilidad compatible con el servidor de autenticación de la red Wi-Fi de la FISEI.
- Realizar un proceso de duplicación del servidor de autenticación de la red Wi-Fi de la FISEI para su integración en un Clúster de alta disponibilidad
- Establecer los medios de comunicación para mantener un Clúster de alta disponibilidad en base a la estructura determinada.
- Crear un Clúster de alta disponibilidad para lograr un servicio eficiente e ininterrumpido en el servidor de autenticación de la red Wi-Fi de la FISEI.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Una vez indagado en la Biblioteca así como en el repositorio digital de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, se puede afirmar que no se ha encontrado un Proyecto de Trabajo de Graduación de pregrado enfocado a la implementación de un Clúster de alta disponibilidad para algún servicio de la Facultad. Sin embargo en la Escuela Politécnica Nacional de Quito - Ecuador, se encontró el siguiente tema: “CONFIGURACIÓN DE UN CLÚSTER DE ALTA DISPONIBILIDAD Y BALANCEO DE CARGA EN LINUX PARA SATISFACER GRAN DEMANDA WEB Y SERVICIOS DE RESOLUCIÓN DE NOMBRES”, elaborado por el Sr. Bustos Burbano Andrés Gustavo, en el cual concluye lo siguiente: La alta disponibilidad en un ambiente de gran demanda Web y resolución de nombres tiene mucha importancia en diferentes aspectos, uno de ellos es la facilidad de realizar el mantenimiento de servidores. Una máquina de servidores se puede sacar de línea, apagarse o actualizarse o repararse sin comprometer los servicios que brinda el Clúster y sin afectar el desempeño del sistema en general.

2.2. Fundamentación Teórica

2.2.1. El Clúster

Es un conjunto de computadoras construidas mediante la utilización de componentes de hardware que se comportan como si fuesen una única computadora. La tecnología de Clúster ha evolucionado gracias al apoyo de actividades que van desde aplicaciones de supercómputo, software de misiones críticas, servidores web y comercio electrónico, hasta bases de datos de alto rendimiento, entre otros

usos. El cómputo con Clúster surge como resultado de la convergencia de varias tendencias actuales. Incluye disponibilidad de microprocesadores económicos de alto rendimiento y redes de alta velocidad, desarrollo de herramientas de software para cómputo distribuido de alto rendimiento y la creciente necesidad de potencia computacional para aplicaciones que la requieran [1].

2.2.2. Elementos de un Clúster

Los elementos con los que cuenta un Clúster son [2]:

- Un nodo activo, donde corren los servicios
- Un nodo pasivo que funciona como respaldo (Backup).
- Servidores reales o virtuales.
- Software de administración.
- Protocolos de comunicación y servicios.
- Conexiones de red.
- Ambientes de programación paralela.
- Middleware.

En la Figura 2.1 se puede observar el orden de los elementos que conforman un Clúster:

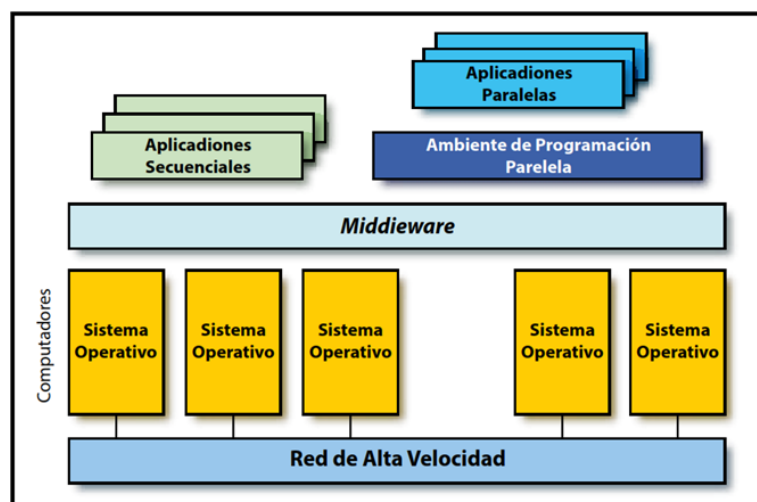


Figura 2.1: Elementos de un Clúster.

Fuente: http://inftec.metabiblioteca.org/index.php/inf_tec/article/view/57/33

2.2.3. Clasificación

Los clústeres dependiendo de su aplicabilidad pueden clasificarse de diferentes maneras. La clasificación más generalizada es la que se presenta a continuación:

- Alto rendimiento (HP, high performance).
- Alta disponibilidad (HA, high availability).
- Balanceo de carga (Load Balancing).
- Alta eficiencia (HR, high throughput).

De acuerdo a esta esta clasificación, los clústeres pueden ser definidos de la siguiente manera [3]:

a) Alto rendimiento (HP, high performance)

Los clústeres de Alto Rendimiento son aquellos en los cuales se ejecutan tareas que requieren una gran capacidad computacional, cantidades enormes de memoria o ambas a la vez. Llevar a cabo estas tareas puede comprometer los recursos del Clúster por largos periodos.

b) Alta disponibilidad (HA, high availability)

Los clústeres de Alta Disponibilidad son aquellos cuyo objetivo es proveer disponibilidad y confiabilidad. Estos clústeres tratan de brindar la máxima disponibilidad de los servicios que ofrecen. La confiabilidad se provee mediante un software que detecta fallos y permite recuperarse frente a ellos, mientras que en hardware se evita tener un único punto de fallos.

c) Balanceo de carga

Los clústeres de balanceo de carga son aquellos que permiten que un conjunto de servidores compartan la carga de trabajo y de tráfico a sus clientes. Está compuesto por uno o más ordenadores (llamados nodos) que actúan como front-end del Clúster y se ocupa de repartir las peticiones de servicio que reciba el Clúster a otros ordenadores que forman su back-end. Las características más destacadas de este tipo de Clúster son:

- Se puede ampliar su capacidad fácilmente añadiendo más ordenadores al Clúster.
- Robustez. Ante la caída de alguno de los ordenadores del Clúster, el servicio se puede ver mermado; pero mientras haya ordenadores en funcionamiento estos seguirán dando el servicio.

d) Eficiencia (HR, high throughput)

Los clústeres de eficiencia son aquellos cuyo objetivo de diseño, es ejecutar la mayor cantidad de tareas en el menor tiempo posible; existe independencia de datos entre las tareas individuales. El retardo entre los nodos del Clúster no es considerado un gran problema.

2.2.4. Ventajas y desventajas de los clústeres

Los clústeres en forma general cuentan con las siguientes ventajas y desventajas [4]:

Ventajas

- Disponibilidad: Capacidad para continuar operando ante la caída de alguno de los ordenadores del Clúster.
- Distribución en paralelo.
- Flexibilidad: Los balanceadores de carga no están amarrados a ninguna arquitectura específica, en lo que respecta a hardware.
- Costos: El diseño y montaje requiere de inversiones sumamente bajas comparadas con las alternativas de solución, las cuales son de un costo elevado.
- Escalabilidad: Capacidad para hacer frente a volúmenes de trabajo cada vez mayores, prestando así un nivel de rendimiento óptimo.
- Expansibilidad: Capacidad de aumentar sus capacidades a través de mejores técnicas.
- Transferencia de información y todo tipo de servicio por internet de forma rápida, a bajo costo e ininterrumpidamente.
- Incremento de velocidad de procesamiento ofrecido por los clústeres de alto rendimiento.
- Incremento del número de transacciones o velocidad de respuesta ofrecido por los clústeres de balanceo de carga.
- Incremento de la confiabilidad y la robustez ofrecido por los Clúster de alta disponibilidad.

Desventajas

- Empresas y entidades prefieren seguir utilizando el modelo cliente/servidor tradicional debido al espacio físico o a la inversión que representaría mudarse de tecnología.
- Espacio físico para el montaje del clústeres de balanceo de carga.

2.2.5. Clúster de alta disponibilidad

Un Clúster de alta disponibilidad es un conjunto de dos o más servidores, que se caracteriza por compartir el sistema de almacenamiento, y porque están constantemente monitorizándose entre sí. Si se produce un fallo del hardware o de los servicios de alguna de las máquinas que forman el Clúster, el software de alta disponibilidad es capaz de reiniciar automáticamente los servicios que han fallado en cualquiera de los otros equipos del Clúster. Y cuando el servidor que ha fallado se recupera, los servicios se migran de nuevo a la máquina original. Esta capacidad de los clústeres de restablecer en pocos segundos un servicio, manteniendo la integridad de los datos, permite que en muchos casos los usuarios no tengan por qué notar que se ha producido un problema. Cuando una avería de este tipo, en un sistema sin Clúster, podría ocasionar la caída de los servicios durante horas [5].

2.2.6. Configuración de alta disponibilidad

Configuración Activo - Activo

En una configuración activo/activo, todos los servidores del Clúster pueden ejecutar los mismos recursos simultáneamente. Es decir, los servidores poseen los mismos recursos y pueden acceder a estos independientemente de los otros servidores del Clúster. Si un nodo del sistema falla y deja de estar disponible, sus recursos siguen estando accesibles a través de los otros servidores del Clúster. La ventaja principal de esta configuración es que los servidores en el Clúster son más eficientes ya que pueden trabajar todos a la vez. Sin embargo, cuando uno de los servidores deja de estar accesible, su carga de trabajo pasa a los nodos restantes, lo que produce una degradación a nivel global del servicio ofrecido a los usuarios [6]. En la figura 2.2 se puede observar un Clúster de alta disponibilidad mediante una configuración Activo – Activo.

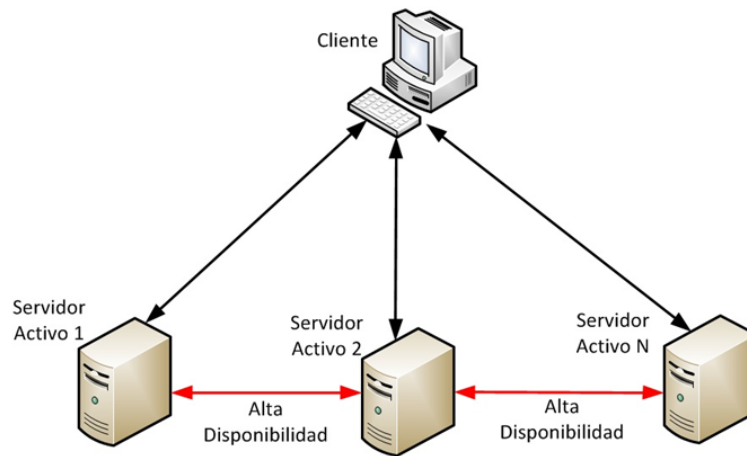


Figura 2.2: Configuración Activo-Activo
Fuente: El Investigador

Configuración Activo - Pasivo

Un Clúster de alta disponibilidad, en una configuración activo/pasivo, consiste en un servidor que posee los recursos del Clúster y otros servidores que son capaces de acceder a esos recursos, pero no los activan hasta que el propietario de los recursos ya no esté disponible. Las ventajas de la configuración activo/pasivo son que no hay degradación de servicio y que los servicios solo se reinician cuando el servidor activo deja de responder. Sin embargo, una desventaja de esta configuración es que los servidores pasivos no proporcionan ningún tipo de recurso mientras están en espera, haciendo que la solución sea menos eficiente que el Clúster de tipo activo/activo. Otra desventaja es que los sistemas tardan un tiempo en migrar los recursos (failover) al nodo en espera [6]. En la figura 2.3 se puede observar un Clúster de alta disponibilidad mediante una configuración Activo – Pasivo.

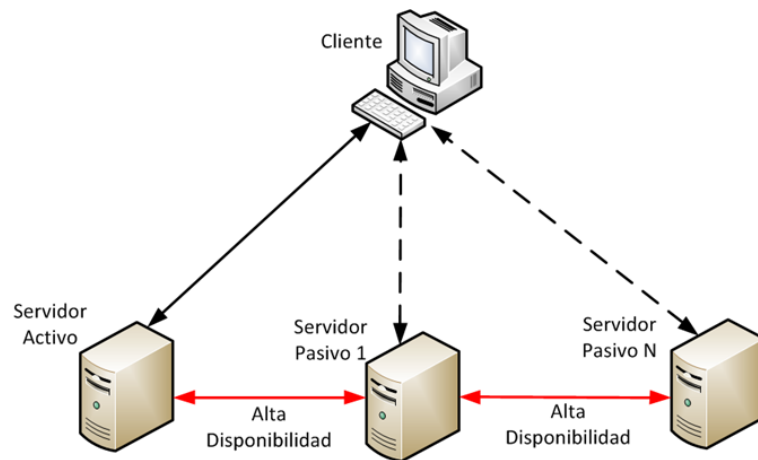


Figura 2.3: Configuración Activo-Pasivo
Fuente: El Investigador

2.2.7. Funcionamiento de un Clúster de alta disponibilidad

En un Clúster de alta disponibilidad, el software de Clúster realiza dos funciones fundamentales. Por un lado intercomunica entre sí todos los nodos, monitorizando continuamente su estado y detectando fallos. Y por otro lado administra los servicios ofrecidos por el Clúster, teniendo la capacidad de migrar dichos servicios entre diferentes servidores físicos como respuesta a un fallo [5].

2.2.8. Dinámica de alta disponibilidad

La disponibilidad es el grado en que una aplicación o servicio está disponible cuándo y cómo los usuarios esperan. La disponibilidad se mide por la percepción de una aplicación del usuario final. Los usuarios finales experimentan frustración cuando sus datos no están disponibles, y ellos no entienden o son capaces de diferenciar los complejos componentes de una solución global. Fiabilidad, valorización, continuas operaciones y detección de errores son características de una solución de alta disponibilidad [7].

a) Fiabilidad:

Al hablar de fiabilidad, se entiende por el funcionamiento correcto de los elementos del Clúster, es decir componentes hardware fiables de una solución de HA, el software fiable, incluida la base de datos, servidores y aplicaciones, es la parte crítica de una implementación de una solución de alta disponibilidad.

b) Recuperación:

Puede haber muchas opciones para recuperarse de un fracaso si ocurre alguno. Es importante determinar qué tipo de fallos pueden ocurrir en su entorno de alta disponibilidad y la forma de recuperarse de estos fallos en el tiempo que satisface las necesidades comerciales. Por ejemplo, si una tabla importante es eliminada de la base de datos, ¿qué medidas adoptaría para recuperarla? ¿Su arquitectura ofrece la capacidad de recuperarse en el tiempo especificado en un acuerdo de nivel de servicio (SLA)?

c) Detección de errores:

Si un componente en su arquitectura falla, entonces la rápida detección, de dicho componente es esencial en la recuperación de un posible fracaso inesperado. Si bien es posible que pueda recuperarse rápidamente de un corte de luz, si se lleva a otros 90 minutos para descubrir el problema, entonces usted no puede satisfacer su SLA. La monitorización del estado del entorno de trabajo requiere un software fiable, para ver de forma rápida y notificar al administrador de bases de datos (DBA) un problema.

d) Continuas operaciones:

El continuo acceso a sus datos es esencial, por muy pequeño o inexistente que sea el tiempo de caída del sistema, para llevar a cabo las tareas de mantenimiento. Actividades como mover una tabla de un lado a otro dentro de la base de datos, o incluso añadir nuevas CPU's a su hardware debe ser transparente para el usuario final en una arquitectura HA.

2.3. Propuesta de Solución

La implementación de un Clúster brindará alta disponibilidad de manera eficiente e ininterrumpida al servidor de autenticación de la red WI-FI en beneficio de los usuarios de la FISEI.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la Investigación

3.1.1. Proyecto de Investigación Aplicada (I)

La modalidad que se empleó en el presente proyecto de investigación fue de tipo Aplicada, puesto que la misma pretende dar soluciones reales y respuestas al problema en cuestión, mediante una solución práctica la cual permitirá a los usuarios de la FISEI gozar de un servicio de autenticación de la red Wi-Fi tolerante a fallos, es decir capaz de brindar alta disponibilidad en todo momento.

3.2. Recolección de Información

La recolección de la información tuvo inicio una vez que se presentó el proyecto de investigación, luego se realizó el reconocimiento físico del Departamento de Redes y Sistemas de la FISEI. A continuación se realizó la entrevista al director del Departamento de Redes y Sistemas de la FISEI a fin de recabar la información necesaria para el desarrollo del proyecto de investigación. Posteriormente se realizó una guía de información mediante la cual se pudo visualizar y tomar datos técnicos los cuales permitieron sustentar la validez en la aplicación del proyecto de investigación.

■ La entrevista:

La entrevista se la realizó de forma personalizada al Ing. Eduardo Chaso, director actual del Departamento de Redes y Sistemas de la FISEI.

- **La guía de Observación:**

En este punto se tomó importante información mediante el uso del software de monitoreo “Cacti” el cual permitió observar una relevante información actual de la red Wi-Fi de la FISEI.

3.3. Procesamiento y análisis de datos

3.3.1. Procesamiento de la Información

Luego de haber obtenido la información apropiada ésta vino a formar parte de un proceso, el mismo que consistió en lo siguiente:

- Revisión de la información recogida
- Manejo de información

3.3.2. Análisis e Interpretación de Resultados

La entrevista se la realizó de forma personal con el Ingeniero Eduardo Chaso, director del Departamento de Redes y Sistemas de la FISEI, al cual se le realizaron las siguientes preguntas:

Pregunta 1.

¿Cuenta actualmente la FISEI con el servicio de autenticación de usuarios en su red Wi-Fi?

Respuesta: Actualmente la Facultad no se encuentra trabajando con el servicio de autenticación de usuarios, debido a dos motivos, el primero es que el servidor sufrió una avería física en el equipo que realizaba la redirección es decir las peticiones de autenticación, y el segundo es debido al CEAACES, que por motivos de evaluación y acreditación de universidades, requiere que la utilización de la red inalámbrica sea de libre acceso para los estudiantes de la universidad.

Pregunta 2.

¿A su criterio y experiencia profesional, cree usted que se debería contar con un servicio de autenticación de usuarios el cual cuente con las características de alta disponibilidad para los usuarios de la red Wi-Fi de la FISEI?

Respuesta: Obviamente si, ya que el hecho que los usuarios no cuentan con ningún tipo de control o chequeo en la red Wi-Fi, esta ha venido decayendo

llegando a ser lenta y demasiado intermitente. Se puede decir que esto se debe a que muchos usuarios cuentan con mas de un dispositivo para conectarse a internet, muchos otros realizan grandes descargas de datos, etc., todas estas cosas conllevan a que la red Wi-Fi colapse a cada instante y el servicio de internet en la facultad sea deficiente. Entonces se puede decir que sería de mucho beneficio contar con un servicio de autenticación y mucho mejor si este cuenta con alta disponibilidad.

Pregunta 3.

¿Tiene el Departamento de Redes y Sistemas de la FISEI los recursos necesario para la implementación de un Clúster el cual permita dar alta disponibilidad al servicio de autenticación a la red Wi-Fi de la Facultad?

Respuesta: Actualmente la Facultad ya cuenta con equipos necesarios para poder abastecer la parte de infraestructura inalámbrica, a la vez se cuenta con un servidor bastante fuerte el cual podría cubrir lo que es el servicio RADIUS para la autenticación y a su vez la implementación de un Clúster de forma virtualizada.

Pregunta 4.

¿Cuenta actualmente de la red Wi-Fi de la FISEI con algún tipo de control en la asignación de ancho de banda a los usuarios?

Respuesta: Actualmente no existe ningún tipo de control en la asignación de ancho de banda por persona, y recalando la respuesta de la pregunta número 2, se puede decir que en si esto es muy perjudicial para toda la red Wi-Fi de la Facultad, ya que mientras algunos estarían utilizando demasiado ancho de banda, otros se verían desfavorecidos por la deficiencia que esto podría causar en la red.

Pregunta 5.

¿Tiene la red inalámbrica de la FISEI algún tipo de seguridad en cuanto al acceso de los usuarios a la web?

Respuesta: No, por las mismas razones expuestas anteriormente en cuanto al libre uso de la red inalámbrica de la FISEI cualquier persona puede acceder a esta red, sin embargo al ser de esta manera el ingreso y utilización de la red, esta se ve vulnerable a cualquier tipo de ataque o infiltración de información por usuarios con conocimientos avanzados pero con mala fe.

Pregunta 6.

¿Cree usted que se podrían crear políticas de seguridad y acceso las cuales podrían ayudar al control y beneficio de los usuarios en el uso de la red Wi-Fi de la FISEI?

Respuesta: Creo que si se podrían crear políticas de seguridad y acceso de usuarios para un control justo y equilibrado en el uso de la red Wi-Fi dentro de la Facultad, y a su vez estas políticas sean encaminadas de manera que no vayan en contra de las políticas indicadas por la CEAACES para las evaluaciones y acreditaciones de universidades, esto se lo podría realizar mediante la creación de perfiles o grupos de usuarios.

Análisis e interpretación de la entrevista

De acuerdo a las preguntas planteadas en la entrevista con el Ing. Eduardo Chaso, en un contexto general se puede apreciar que la utilización del servicio de Internet en la red Wi-Fi de la FISEI está siendo víctima de un uso desequilibrado e inequitativo entre sus usuarios, ya que al no existir ningún tipo de control en el acceso y utilización de la red, la misma no estaría brindando un servicio eficiente y continuo a sus usuarios, ya que unos podrían verse favorecidos pero a la vez otros afectados, debido a que en si toda la red inalámbrica vendría a colapsar por la mala utilización del servicio lo cual podría provocar incluso averías en los dispositivos de red. Por otra parte cabe señalar el hecho que la Facultad no se encuentra trabajando con un servidor de autenticación de usuarios en su red Wi-Fi por ende esta situación involucra la necesidad primordial de levantar el servidor RADIUS considerando que la Facultad cuenta con los equipos e infraestructura necesaria para levantar un servicio de autenticación de usuarios con alta disponibilidad poniendo especial atención en las políticas que se lleven a cabo a fin de que estas sean de beneficio para todos los usuarios y que a su vez sean consecuentes con las políticas que antepone el CEAACES en cuanto al acceso a las redes inalámbricas en las instituciones de educación superior.

Tráfico generado en la red Wi-Fi de la FISEI

También se realizó un monitoreo integral del tráfico en la red inalámbrica de la FISEI. Este proceso se lo llevó a cabo utilizando el software Cacti, el cual permitió monitorear el router Cisco RV180W que es el dispositivo principal para el acceso a la red inalámbrica en la Facultad, también a este dispositivo se encuentran conectados otros dispositivos en modo AP para cubrir los dos edificios de la Facultad. La toma

de los datos se la realizó desde el día 26 de Noviembre al 31 de Diciembre de 2013. Para este documento se han tomado muestras gráficas del monitoreo del tráfico en la red correspondientes a los días 2 y 23 de Diciembre.

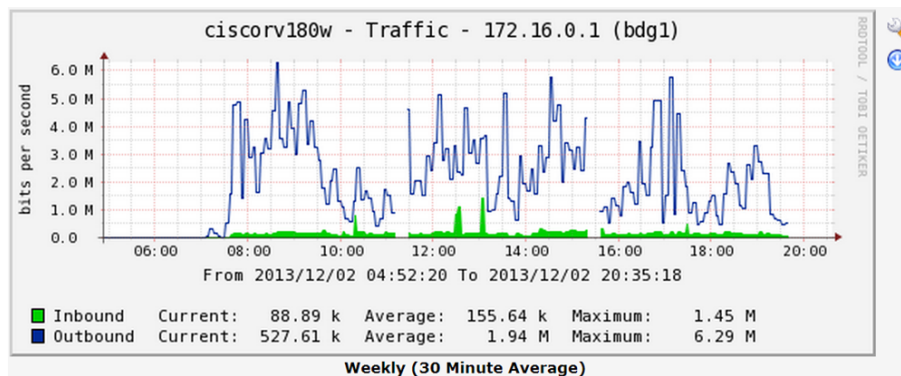


Figura 3.1: Tráfico en la red Wi-Fi del 2/12/2013
Fuente: El investigador

Gráfico 1. Tráfico generado en la red Wi-Fi de la FISEI el día 2 de Diciembre de 2013, en el que se observa el tiempo y la cantidad de bits por segundo que circulan a través del bridge LAN del router Cisco. **Análisis e interpretación**

Como se puede ver en la figura 3.1, en el tráfico generado el día 2 de Diciembre existieron varios picos de subida y bajada de forma brusca y estabilidad muy variada en la señal Outbound del tráfico generado en la red LAN, de acuerdo a esto se puede observar que la utilización del ancho de banda el cual se encuentra sin ningún control, puede ocasionar la existencia de cuellos de botella por alta congestión en la red, lo que afectaría directamente al rendimiento del equipo de red encargado de dar el servicio de Internet para la red inalámbrica, debido a estos inconvenientes este equipo puede colapsar dejando de funcionar correctamente por la sobrecarga de trabajo forzado generado desde los Access Point y a su vez afectando a los mismos.

Gráfico 2. Tráfico generado en la red Wi-Fi de la FISEI el día 23 de Diciembre de 2013 en el que se observa el tiempo y la cantidad de bits por segundo que circulan a través del bridge LAN del router Cisco.

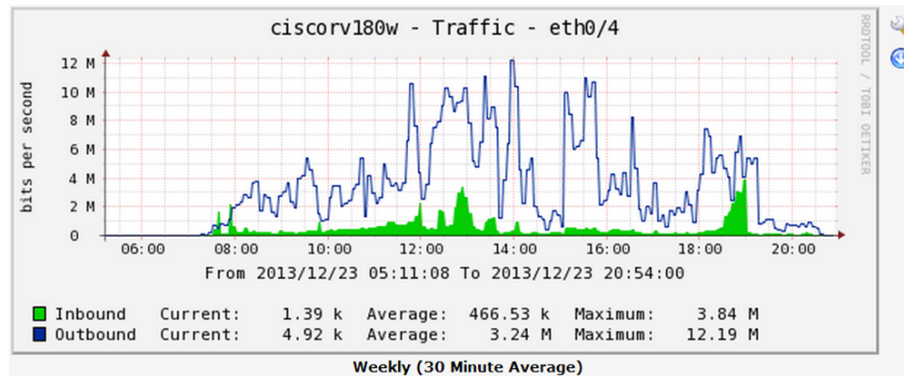


Figura 3.2: Tráfico en la red Wi-Fi del 23/12/2013
Fuente: El investigador

Análisis e interpretación

Como se puede ver en la figura 3.2, en el tráfico generado el día 23 de Diciembre, también existieron varios picos de subidas y bajadas bruscas, con estabilidad muy variada en la señal Outbound del tráfico en la red LAN, en esta ocasión llegaron hasta las 12 megas pico sin estabilidad, lo que demuestra que los usuarios no tienen una división de ancho de banda dinámico, es decir cualquier usuario puede tomar el ancho de banda que desee por lo cual esto podría causar un colapso en la red inalámbrica y por lo mismo los dispositivos podrían ser sobrecargados lo que causaría que estos dejen de funcionar regularmente o a su vez podría existir demasiada intermitencia en la conexión para el servicio de Internet.

3.4. Desarrollo del Proyecto

La FISEI cuenta con un Departamento de Redes y Sistemas a través del cual se generan las gestiones de comunicación. De acuerdo a la información emitida por este departamento, la FISEI no se encuentra trabajando con un servidor RADIUS para la autenticación de usuarios en su red inalámbrica. Debido a esta información y en función de los requerimientos planteados por el departamento de redes y sistemas de la FISEI para ofrecer un servicio eficiente y continuo a los usuarios en su red inalámbrica, es necesario el desarrollo de los siguientes puntos:

- Levantar un servidor RADIUS para la autenticación de usuarios en la red inalámbrica de la FISEI en base a los recursos físicos y lógicos con los cuales cuenta el Departamento de Redes y Sistemas.
- Realizar la duplicación de las características del servidor de autenticación en los diferentes nodos a implementar de acuerdo a los requerimientos del servicio de autenticación de la red Wi-Fi.
- En función de los requerimientos del servicio de autenticación de la red Wi-Fi, se debe realizar un estudio de la estructura de un Clúster de alta disponibilidad el cual deberá ser compatible con el servidor de autenticación de la red.
- En base a la determinación del Clúster de alta disponibilidad se debe efectuar la aplicación del mismo de acuerdo al establecimiento de mecanismos de comunicación e integración de los nodos o servidores mediante la aplicación de un software el cual permita realizar la creación de un Clúster de alta disponibilidad a los servicios de autenticación de usuarios.
- Realizar las configuraciones de comunicación en los diferentes dispositivos de red los cuales intervienen de forma directa con la aplicación del Clúster de alta disponibilidad para la FISEI.
- Crear un ambiente de pruebas y controles del funcionamiento correcto del Clúster el cual está diseñado para ofrecer alta disponibilidad en el servicio de autenticación de red Wi-Fi de la FISEI.

CAPÍTULO 4

Desarrollo de la Propuesta

4.1. Datos Informativos

4.1.1. Tema de la Propuesta

“Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI”

4.1.2. Institución Ejecutora

- Institución Educativa: Universidad Técnica de Ambato
- Nombre de la Institución: Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Tipo de Organización: Pública
- Departamento: Redes y Sistemas de la FISEI

4.1.3. Beneficiarios

- Universidad Técnica de Ambato
- Estudiantes, profesores y personal administrativo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

4.1.4. Ubicación

Provincia: Tungurahua

Cantón: Ambato

Dirección: Av. Los Chasquis y Río Payamino

Teléfono: 03 2415288

4.1.5. Equipo Responsable

Tutor: Ing. David Guevara

Investigador: Luis Felipe Chuncha Mastha

4.2. Antecedentes de la Propuesta

Una de las herramientas con las cuales la red Wi-Fi de la FISEI no ha contado antes es un software de monitoreo, el mismo que es necesario implementarlo a fin de poder observar el tráfico que se genera en la red inalámbrica para poder elevar juicios técnicos en base a los datos obtenidos del monitoreo.

A partir de las investigaciones realizadas en la FISEI de la UTA, se ha podido comprobar que es imprescindible contar con un servicio de autenticación el cual cuente con las características de alta disponibilidad en su red Wi-Fi para un mejor control en la asignación de ancho de banda, seguridad en la información, privilegios de acceso a la red, etc., de manera que se pueda dar un servicio de alta disponibilidad a fin de contar con sistema continuo y eficiente.

Dentro de los registros bibliográficos que posee la Biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, se encontró la Tesis con el siguiente tema:

“Red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial”, realizada por: Santiago Seilema Valladares, año 2011.

Se ha tomado como referencia de estudio esta tesis porque en la misma se destaca la implementación del servicio de autenticación para la red Wi-Fi de la FISEI utilizando un servidor RADIUS.

Cabe señalar que la actualidad la FISEI no se encuentra trabajando con un servicio de alta disponibilidad dirigido a la autenticación de usuarios ya que de acuerdo a las investigaciones realizadas, hace varios meses atrás se contaba aun con el servidor de autenticación con el que se podía realizar una serie de controles por usuario en la utilización de la red Wi-Fi y por lo mismo existía un poco más de estabilidad en la eficiencia de la red inalámbrica, sin embargo este servicio de lo

dejó de utilizar por averías de los equipos en la parte de redireccionamiento y a la par también se llevaron a cabo las evaluaciones y acreditaciones a las universidades por el CEAACES, entidad que requiere que los estudiantes de educación superior tengan acceso a Internet mediante el uso de las redes inalámbricas con un ancho de banda adecuado, como señala en el indicador *C.3.1: Conectividad* del Subcriterio C3: Acceso a internet, mencionando lo siguiente:

“Se considera que un alto porcentaje de estudiantes tienen acceso a computadores portátiles y por lo tanto el ancho de banda deberá permitir el acceso y el trabajo de los estudiantes durante su estadía en la universidad.” [8]

4.3. Justificación

Siendo consecuentes con la observación y análisis realizado, se puede notar que los defectos existentes en la red inalámbrica de la FISEI se los puede superar mediante la implementación de un Clúster de alta disponibilidad para el servicio de autenticación en la red Wi-Fi de la Facultad llevando a la par el empleo de políticas adecuadas en cuanto al acceso a la red inalámbrica las cuales sean congruentes con las políticas del CEAACES y a su vez sean de beneficio para los usuarios directos de la FISEI.

Contar con un servicio de alta disponibilidad para el servidor de autenticación de usuarios para la red Wi-Fi de la FISEI causa grandes beneficios tanto al administrador de la red como a los mismos usuarios. Por una parte el trabajar con el servidor RADIUS contribuye de manera eficiente y favorable en la administración de la red, pues al utilizar este servicio se pueden efectuar configuraciones adecuadas en la distribución del ancho de banda de manera equilibrada mediante perfiles y atributos de usuario. De la misma forma con la autenticación se podría controlar el acceso sobrecargado de dispositivos por usuario, ya que debido a la falta de control en estos aspectos existe intermitencia en la señal inalámbrica y por ende el servicio vendría a ser deficiente por lo cual muchos usuarios pueden estar molestos.

Ahora, con la implementación del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI, se elevarían los niveles de eficiencia de manera integral en toda la red inalámbrica de la Facultad puesto que el propósito del Clúster es brindar un servicio continuo e ininterrumpido, tolerante a fallos, y altamente disponible para el servicio de autenticación.

4.4. Objetivos

4.4.1. Objetivo General:

Implementar un Clúster de alta disponibilidad en un entorno virtualizado para el servidor de autenticación de la red Wi-Fi de la FISEI.

4.4.2. Objetivos Específicos:

- Crear entornos virtuales en el servidor principal de la FISEI para la instalación del servidor RADIUS para la autenticación de usuarios en la red Wi-Fi de la FISEI.
- Clonar el servidor RADIUS para su integración dentro del Clúster de alta disponibilidad.
- Instalar un Clúster de alta disponibilidad para lograr un servicio eficiente e ininterrumpido en el servidor de autenticación de la red WI-FI de la FISEI.
- Establecer políticas de acceso por autenticación a la red Wi-Fi de la FISEI que sean consecuentes con las políticas de acceso señaladas por el CEAACES y acordes al beneficio necesario para los usuarios de la FISEI.

4.5. Análisis de Factibilidad

4.5.1. Factibilidad Institucional

El implementar un proyecto el cual brinde alta disponibilidad al servidor de autenticación en la red Wi-Fi de la FISEI es de gran utilidad y beneficio para la Facultad ya que ésta a diferencia de otras facultades de la UTA, es una Facultad enfocada al avance en el conocimiento y desarrollo tecnológico y por ende, tanto los estudiantes como los profesores se encuentran en constante investigación por lo cual la red inalámbrica es de gran utilidad en el uso del Internet y por lo mismo se requiere que esta sea utilizada de la mejor manera para que sus usuarios tengan un servicio continuo y eficiente.

4.5.2. Factibilidad Técnica

La implementación del presente proyecto de investigación es técnicamente factible, ya que se basa en mecanismos avanzados en la configuración, control y ejecución de

tareas dispuestas para ofrecer un servicio de alta disponibilidad enfocados al servicio de autenticación y por lo mismo se puede decir que el proyecto es una alternativa de uso para cualquier empresa o institución orientados a ofrecer este tipo de servicios.

4.5.3. Factibilidad Operativa

En la parte operativa, la propuesta del proyecto es de gran factibilidad ya que se cuenta con la infraestructura física adecuada así como con los recursos humanos y tecnológicos para la implementación de un Clúster de alta disponibilidad para el servicio de autenticación en la red Wi-Fi de la FISEI, añadiendo que las autoridades de la Facultad muestran gran interés hacia la propuesta del proyecto de investigación pues lo que se requiere es que el servicio de acceso a la red inalámbrica así como la utilización de la misma sea eficiente, estable y continuo.

4.5.4. Factibilidad Económica

El presente proyecto de investigación es factiblemente económico ya que debido a la utilización de software libre se pueden hacer uso de estos recursos de manera gratuita. En cuanto al hardware, la Facultad cuenta con los equipos necesarios para la implementación del proyecto y los recursos adicionales que se requieran se encuentran cubiertos por el investigador.

4.6. Fundamentación

4.6.1. Modelo jerárquico de la red Wi-Fi de la FISEI

CISCO ha desarrollado una técnica para diseñar redes.

Anteriormente las redes tenían un punto central de interconexión y alrededor estaban todos tanto usuarios como periféricos, pero con el pasar del tiempo las cosas están cambiando puesto que cada vez hay más servicios y usuarios.

Es por eso que CISCO ha creado un modelo jerárquico [9], como muestra en el esquema de la figura 4.1 el cual se encuentra enfocado a la red general de la FISEI.

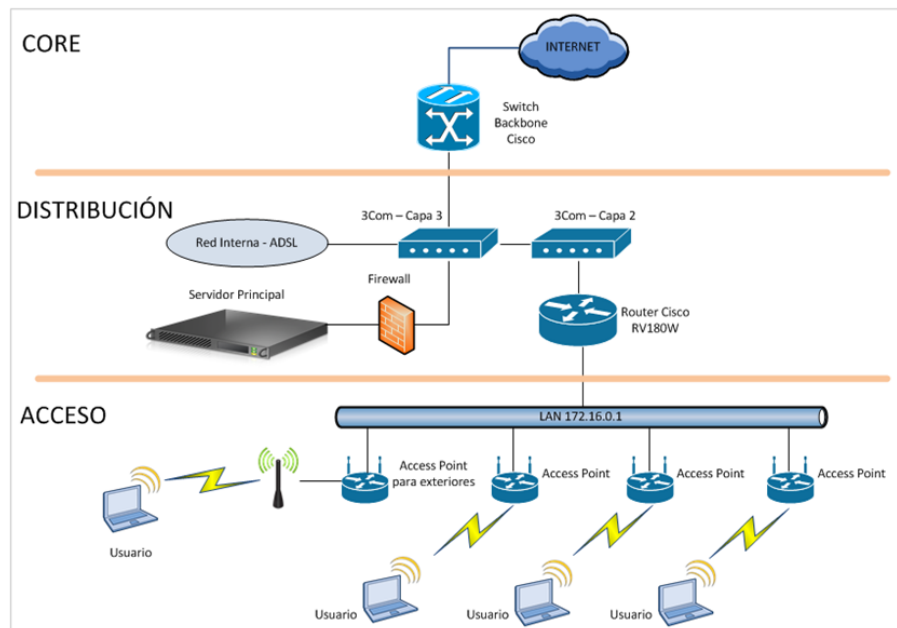


Figura 4.1: Modelo Jerárquico de red de la FISEI
Fuente: El Investigador

En donde:

- El nivel CORE es el backbone de la red. Este provee un acceso rápido entre los diferentes dispositivos de la red. Para ejecutar una tarea rápida se usan smart switches de alta velocidad.
- El nivel de DISTRIBUCIÓN es el que hace las más grandes funciones de distribución de tráfico. En este nivel se pueden usar routers si son grandes redes o switches. Sus funciones son:
 - Limitar el tráfico de broadcast.
 - Asegurar tráfico entre las capas.
 - Proveer una jerarquía en el direccionamiento del nivel 3 y el Routing Summarization
 - Intercambio entre los diferentes tipos de medio.

En esta parte es donde se implementan todas las políticas de direccionamiento del nivel 3, o sea, el nivel IP.

- El nivel de ACCESO se encarga principalmente de proveer las conexiones a los usuarios finales de red. Comúnmente este trabajo lo realizan los access point o switch, cuando se trata de pequeñas instalaciones también se usa un router.

Entonces de acuerdo a estas apreciaciones el proyecto ha realizar, en pos de implementar un Clúster de alta disponibilidad para el servicio de autenticación en la red Wi-Fi de la FISEI, viene a tomar lugar en el nivel de distribución, debido a las funciones de alta disponibilidad para servicios y datos, y en el nivel de acceso, a razón de la autenticación de usuarios.

4.6.2. Entorno virtual en Linux

La FISEI en la actualidad se encuentra utilizando la distribución libre CentOS v5.8 (Community ENTERprise Operating System) que es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat [10].

El trabajar en ambientes virtualizados Linux se constituye en la plataforma líder en el campo de la aplicación de servidores por su estabilidad y eficiencia a la hora de efectuar trabajos forzados a nivel informático.

4.6.2.1. Virtualización

La virtualización es un proceso el cual consiste en la creación de un entorno virtual, sobre una máquina real en el que se pueden trabajar con varios sistemas operativos los cuales pueden ser ejecutados en la misma máquina y a su vez estos pueden trabajar de manera independiente. Para realizar un proceso de virtualización es necesario contar con un software que proporcione soporte para instalación de otros sistemas operativos sobre la máquina real, estos funcionarán de manera encapsulada dentro del entorno virtual.

Al crear las máquinas virtuales, aunque no son otra cosa que archivos, estas se comportan como cualquier otro equipo de cómputo físico en el cual se puede instalar un Sistema Operativo, Aplicativos, etc. El software que implementa la virtualización permite que el hardware ejecute múltiples instancias de diferentes sistemas operativos de forma concurrente sin que interfieran entre sí, ni con las aplicaciones.

Es así que para la creación de un ambiente virtual es necesario contar con un sistema físico que será la máquina real y un sistema virtual o lógico el cual se ejecutará virtualizando sobre el sistema físico. Al disponer de suficientes recursos y altos requerimientos se pueden ejecutar varios sistemas virtuales sobre un único sistema físico. De la misma manera se puede trabajar en sentido contrario, es decir se puede

contar con varios recursos físicos (servidores o dispositivos de almacenamiento) los cuales pueden ser usados como un único recurso lógico [11].

A continuación se puede ver en la figura 4.2 un esquema general de un sistema virtualizado con sus componentes principales.

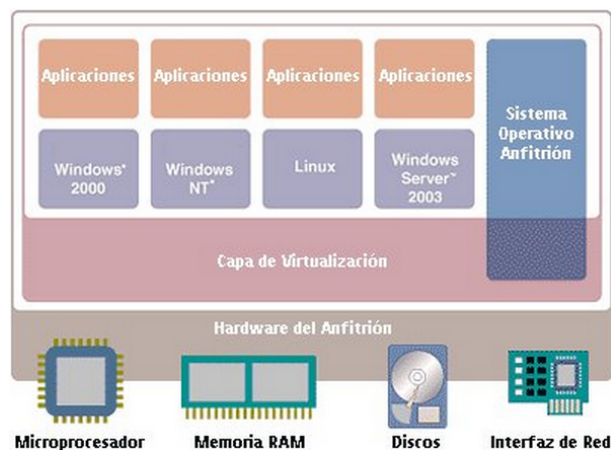


Figura 4.2: Esquema general de virtualización

Fuente: <http://www.radioexilio.com.ar/estaciondetransito/?p=14>

<http://recursostic.educacion.es/observatorio/web/es/software/servidores/1080-introduccion-a-la-virtualizacion-con-xen>

Ventajas y Desventajas de la virtualización

A continuación se destacan las ventajas y desventajas importantes a tomar en cuenta al momento de efectuar la virtualización [11].

■ Ventajas de la virtualización

- Simultáneamente los usuarios pueden trabajar con varios entornos diferentes e independientes. En una organización o empresa esto puede ser muy útil ya que los usuarios podrían trabajar más libremente en las máquinas virtuales y la máquina real sería de uso restringido donde el usuario tendría acceso limitado al tipo de información relevante de la organización.
- Si la estrategia de la organización es cambiar a menudo de aplicaciones, el uso de la virtualización permite conservar los puntos de trabajo idénticos y todos los cambios hacerlos sobre el entorno virtualizado y desde un servidor a través de la red. Esto permite que el servicio no se corte por este motivo y facilita la tarea de administración.
- Facilita también la realización de copias de seguridad y su recuperación.

- Optimiza la utilización de los recursos en aquellos servidores dedicados que proporcionan servicios sin grandes requerimientos.
- Otras ventajas serían la menor dependencia del hardware y la facilidad de cambio del puesto de trabajo.

En consecuencia se puede decir que la virtualización proporciona alta disponibilidad, ahorra costes, optimiza el uso y control sobre los recursos y mejora la seguridad de los sistemas virtualizados.

■ Desventajas de la virtualización

- Problemas de licencias en algunos casos. La utilización de la virtualización supone un cambio en cuanto a las políticas de licencias por usuario.
- Utilización de recursos. El software de virtualización tiene unos requerimientos de hardware muy exigentes, sobre todo en cuanto a capacidad de proceso y de memoria RAM. Esto supone una pérdida de rendimiento.
- Existe una dependencia del sistema operativo anfitrión y del sistema de virtualización elegido. Es decir, el anfitrión limita y es el punto débil del sistema ya que está compartido por todos los sistemas virtualizados.

4.6.2.2. Hypervisor XEN

El proyecto XEN fue creado en la universidad de Cambridge, en el año 2001 liderado por Ian Pratt, la primera versión 1.0 de XEN fue liberada en al año 2003, mas tarde en 2005 se funda la empresa XenSours Inc. para dirigir la comunidad de desarrolladores con el apoyo de otras empresas. En el mismo año se libera la versión 2.0.5. En año 2007 la empresa CITRIX compra XenSource (500 mill. \$) y convierte al equipo de desarrollo en parte del XenServer Product Group y también se libera la versión 3.1. La licencia con la cual se maneja XEN es GPL, código abierto, y tanto XenSource como otras empresas importantes como IBM, Sun, HP, Intel, AMD, RedHat, Novell, están involucradas en el mantenimiento y desarrollo de XEN. En la actualidad, XEN corre sobre arquitecturas x86, con procesadores Pentium 4 o más modernos, x86_64 (AMD64 y EM64T), IA-64 y POWER de IBM. Para otras plataformas es técnicamente posible y puede estar disponible en el futuro. La última versión de Xen, Xen 3.0.4, extiende el liderazgo en características y funcionalidad requerida para virtualizar los servidores que hoy en día se encuentran en los centros de datos de las empresas.

XEN básicamente es una herramienta de virtualización que se ejecuta por debajo del sistema operativo y actúa como hypervisor del mismo. El nombre el cual XEN les da a sus máquinas virtuales es “dominio” [12].

Hypervisor – Monitor de máquina virtual

- dom0 – Sistema operativo privilegiado de carácter administrativo para gestión de Xen.
- domU – Máquina virtual (PV o HVM) que corre encima del sistema Hypervisor

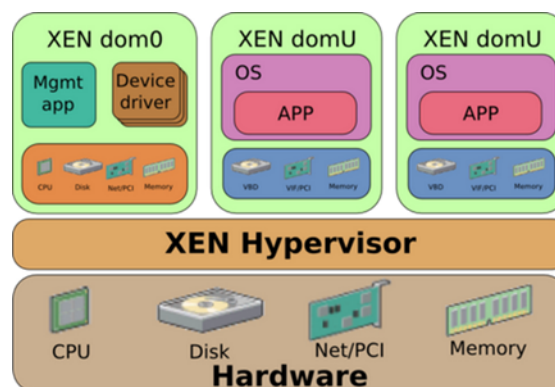


Figura 4.3: Esquema XEN –Hypervisor

Fuente: <http://sesolibre.com/2008/01/virtualizadores-o-convierte-tu-computadora-en-varias/>

En la plataforma XEN se utilizan dos maneras de virtualización:

- HVM o 'Full Virtualization', es decir, virtualización completa, lo cual consiste en la instalación de una máquina virtual como si fuera un host independiente.
- Paravirtualización, que consiste en utilizar un kernel modificado para que pueda comunicarse con el hypervisor de XEN. Este es el uso más habitual de XEN. A través del hypervisor XEN se comunica directamente con el hardware del equipo (CPU).

4.6.2.3. Paravirtualización

La paravirtualización es una técnica de virtualización mediante el cual, las instrucciones de la VM se ejecutan directamente en el procesador físico, puesto que emplea sistemas operativos modificados para ello.

La paravirtualización es una variante de la virtualización completa en la que el Hypervisor accede al sistema operativo directamente, es decir, la máquina virtual envía las instrucciones al procesador directamente, sin necesidad de ser traducidas.

De esta manera la gestión a nivel de código máquina se realiza de una forma considerablemente más eficiente, al ejecutarse directamente y por la misma razón el proceso de comunicación entre el hardware nativo y el sistema operativo de la MV es más eficiente que en el caso de la virtualización completa. Las herramientas las cuales permiten realizar esta técnica de virtualización, así como la virtualización completa son: XEN y UML [13].

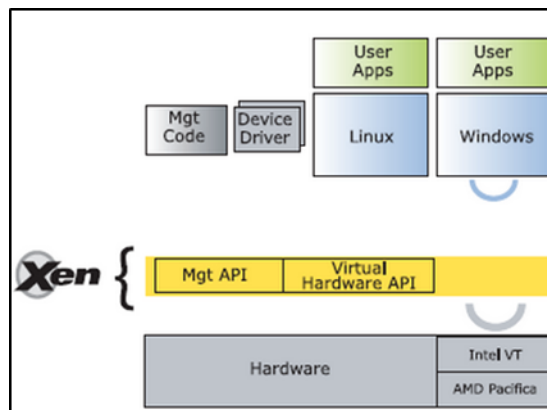


Figura 4.4: Esquema de Paravirtualización con Xen

Fuete: <http://www.jonathanecheverria.com/2009/07/28/herramientas-de-virtualizacion-xen-y-uml>

4.6.3. Servidor RADIUS

Un servidor RADIUS es el cual realiza el proceso de gestión de acceso a las redes. RADIUS (Remote Authentication Dial In User Service); Dial de autenticación remoto para acceso a servicios, es un protocolo estándar de seguridad para Internet, desarrollado por Livingston Enterprises el cual se encuentra especificado en los RFC 2865 y RFC 2866. Utiliza el puerto 1812 y 1813 UDP para establecer sus conexiones. El modelo que RADIUS utiliza es a modo cliente/servidor donde el papel de servidor lo desempeña RADIUS en el cual está contenida la información de los usuarios, almacenando sus contraseñas y sus perfiles, y un elemento de red designado como NAS (Network Access Server) [14].

4.6.3.1. Elementos de RADIUS

Los elementos básicos que componen un servidor RADIUS son los siguientes [14]:

- **Protocolo:** Basado en UDP, RFC 2865 y 2866 define el formato de trama RADIUS integrado con un mecanismo de transferencia de mensajes, y usa los puertos: 1812 de autenticación y 1813 de auditoria.

- **Servidor:** El RADIUS server es ejecutado desde el ordenador o estación de trabajo en el centro el cual mantiene la información para la autenticación de usuarios y servicio de acceso red.
- **Cliente:** El cliente RADIUS realiza las peticiones de NAS en toda la red.

4.6.3.2. Funciones de RADIUS

Básicamente las funciones que realiza un servidor RADIUS corresponden a las siglas "AAA" que significan: Autenticación, Autorización y Anotación. Estas funciones contenidas en el servidor no reciben conexiones directas de los usuarios sino que interactúan con las aplicaciones del cliente en otros equipos de la red [15].

- **Autenticación:** Es un proceso llevado a cabo entre dos entidades, donde una da a conocer su identidad y la otra verifica su autenticidad. Este servicio responde a la pregunta ¿Quién es el usuario?
- **Autorización:** Es el proceso para determinar si un usuario autenticado tiene los permisos necesarios para acceder a un recurso, es decir otorgarle o denegarle permisos dependiendo del resultado de la evaluación de autorización. Este servicio responde a la pregunta: ¿A qué está autorizado el usuario?
- **Anotación o Contabilidad:** Es el seguimiento que se hace a los recursos, cuando se ha autorizado el uso a un usuario o grupo de usuarios. Éste servicio proporciona una respuesta a la pregunta: ¿Qué hizo el usuario con el recurso?

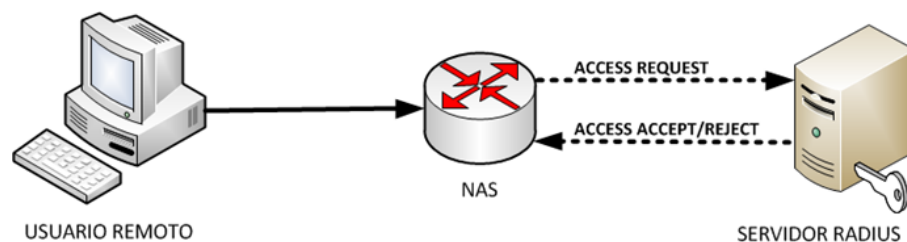


Figura 4.5: Esquema Básico de Autenticación AAA con RADIUS
Fuente: <http://echaleunvistazo.wordpress.com/category/mysql/>

4.6.3.3. FreeRADIUS

El proyecto FreeRADIUS el cual inició en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre orientada a servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen. Tiene la

capacidad de operar tanto en sistemas con recursos limitados así como en sistemas los cuales disponen de gran cantidad de usuarios.

La idea básica e inicial de FreeRADIUS es ofrecer un trabajo a nivel de servidor RADIUS el cual permita una mayor colaboración de la comunidad y que a su vez pueda cubrir las necesidades que otros servidores RADIUS no lo hacen. Actualmente FreeRADIUS incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Además a esto se incluye soporte para todos los protocolos comunes de autenticación y bases de datos [16].

■ **Características importantes de FreeRADIUS**

FreeRADIUS es el primer OpenSource Radius Server, entre sus principales características:

- Factibilidad de usar software de Base de Datos como: OpenLDAP, MySQL, PostgreSQL, Oracle entre otros.
- Soporta varios protocolos de autenticación como EAP, con EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, MSCHAPv2 y subtipos de Cisco LEAP. Todos estos protocolos son usados en la mayoría de los equipos wireless de equipos portátiles y access point del mercado, por lo que es un servidor bastante completo.
- Permite usar los estándares de encriptación WEP, WPA, WPA2, etc.

4.6.3.4. **DaloRADIUS**

DaloRADIUS es una aplicación avanzada de gestión de RADIUS web dirigida a la gestión de puntos de acceso (hotspot - captive portal) y despliegues de ISP de uso general. Cuenta con gestión de usuarios, informes, gráficos, contabilidad, un motor de la facturación y se integra con GoogleMaps para geo-localización [17].

■ **Características importantes de DaloRADIUS**

Entre las características más destacadas de DaloRADIUS se tienen las siguientes:

- DaloRADIUS está escrito en PHP y JavaScript, y utiliza una capa de abstracción de base de datos lo que significa que es compatible con muchos sistemas de bases de datos, entre ellos el MySQL popular, PostgreSQL, SQLite , MsSQL , y muchos otros.
- Está basado en la implementación FreeRADIUS con un servidor de base de datos que sirve como el back-end. Entre otras características,

implementa ACLs, integración GoogleMaps para la localización de HotSpot, puntos de acceso y muchas más características.

- DaloRADIUS es esencialmente una aplicación web para administrar un servidor RADIUS, en teoría podría administrar cualquier servidor RADIUS pero específicamente gestiona la administración de FreeRADIUS y su estructura de base de datos. A partir de la versión 0.9-3 DaloRADIUS ha introducido una aplicación a nivel de la capa de abstracción de base de datos basada en el paquete de PEAR :: DB de PHP que soportan una amplia gama de servidores de bases de datos. Actualmente la última versión que se ha liberado para DaloRADIUS es la 0.9-9 la cual está en función desde el año 2011.
- En lo que se refiere a la aplicación web, DaloRADIUS actúa como una consola de gestión para controlar todos los aspectos del servidor RADIUS, así como proporcionando amplias características comerciales y profesionales tales como información de contabilidad, informes gráficos, un motor de la facturación y una función para la integración del servicio GoogleMaps para la geo-localización de los servidores NAS y centros de HotSpots.

4.6.4. Alta disponibilidad

La alta disponibilidad básicamente es el grado en el que un servicio o aplicación está disponible cuándo y cómo los usuarios esperan. Es así que la disponibilidad en un servicio puede ser medido en función de las expectativas y las experiencias del usuario final. Los usuarios finales experimentan frustración cuando sus datos no están disponibles, y ellos no entienden o son capaces de diferenciar los complejos componentes de una solución global. Por tal razón el impacto que una entidad o negocio tangible puede sufrir por inactividad en algunos de sus servicios se puede expresar en términos de pérdida de información, disminución de la productividad, daños a la propiedad, costos de oportunidad, daños contractuales o pérdida de la buena fe. De esta manera el principal objetivo de una solución de alta disponibilidad dentro de la FISEI es minimizar o mitigar el impacto del tiempo de inactividad del servicio de Internet en la red Wi-Fi por autenticación, ya que al emplear una estrategia eficaz con este fin, equilibra de manera óptima los procesos y los acuerdos de nivel de servicio (SLA) con las capacidades técnicas y los costos de infraestructura los cuales la Facultad está destinada a ofrecer [7].

4.6.4.1. Cálculo de la disponibilidad

En términos generales la disponibilidad puede ser medida de acuerdo al grado en que una aplicación o servicio se encuentre disponible cuándo y cómo los usuarios esperan. La disponibilidad se mide por la percepción de una aplicación del usuario final. Específicamente la disponibilidad puede ser calculada porcentualmente conforme al tiempo en que la aplicación está realmente disponible para controlar las solicitudes de servicio en comparación con el tiempo de ejecución total disponible previsto [18].

En primera instancia se debe tener en cuenta el Acuerdo de Nivel de Servicio (SLA) en el cual se defina cuanto tiempo y en que horarios se debe contar con un servicio de forma activa, de acuerdo a esto en el cálculo de la disponibilidad intervendrán las variables que permitirán obtener la disponibilidad en forma porcentual de un servicio.

Para el cálculo de la disponibilidad se utilizan variables las cuales se detallan en la tabla 4.1 dada a continuación:

Tabla 4.1: Variables para el cálculo de la disponibilidad en un servicio.

Nombre	Acrónimo	Cálculo	Definición
Tiempo medio entre errores	MTBF	Horas / número de errores	Duración media de funcionamiento de la aplicación antes de que produzca errores.
Tiempo medio de recuperación	MTTR	Horas de reparación / número de errores	Tiempo medio necesario para reparar y restaurar el servicio después de que se produzca un error.

Fuente: [http://msdn.microsoft.com/es-es/library/aa291543\(v=vs.71\).aspx](http://msdn.microsoft.com/es-es/library/aa291543(v=vs.71).aspx)

De esta manera la fórmula para el cálculo de la disponibilidad es la siguiente:

$$Disponibilidad = \left(\frac{MTBF}{MTBF + MTTR} \right) * 100$$

De acuerdo a esta información se puede realizar un cálculo de la disponibilidad que se debe obtener dentro de la FISEI para el servicio de autenticación en la red Wi-Fi, tomando en cuenta al SLA dentro del periodo de un semestre el mismo que el servicio debe ofrecer continua disponibilidad a sus usuarios. De acuerdo al período académicos de la UTA el cual se aplica a las Facultades, se puede contar con un tiempo de servicio de 5 meses, además cabe señalar que la FISEI labora los 7 días

de la semana entre clases normales, maestrías y otros cursos de fin de semana, período en el cual debe estar disponible el servicio de autenticación en la red Wi-Fi de la FISEI. Haciendo un cálculo por hora se tendría lo siguiente:

Periodo de actividad durante 5 meses: 150 días

Periodo laboral diario: 14 horas

Por lo tanto el SLA de alta disponibilidad para el servicio de autenticación de la red Wi-Fi de la FISEI para con sus usuarios es:

$$SLA_{(FISEI)} = 150 * 14 = 2100h$$

Para determinar el tiempo medio entre errores y el tiempo medio de recuperación, cabe señalar que los errores que se puedan tener por los cuales se interrumpa la disponibilidad, podrían ser imprevistos, sean estos por causas naturales, cortes de energía, fallos en los equipos, etc., los mismos que en la mayoría de ocasiones son difíciles de prever.

De acuerdo a esto se estima un promedio de errores de 1 horas por mes destacado de la tabla 4.2, se tiene que:

$$MTBF = (\frac{2100h}{5}) = 420h$$

En donde:

2100, corresponde a las horas de acuerdo al SLA.

5, corresponde a los errores tomados de los 5 meses.

$$MTTR = (\frac{5h}{5}) = 1h$$

En donde:

5, corresponde a las horas estimadas de reparación

5, corresponde a los errores tomados de los 5 meses.

Por lo que la alta disponibilidad sería:

$$Disponibilidad = (\frac{420}{420+1}) * 100$$

$$Disponibilidad = (0.99762) * 100 = 99.762\%$$

Actualmente al elegir correctamente el hardware y software adecuados, puede ser relativamente sencillo diseñar un sistema con una disponibilidad del 98 % del tiempo, no obstante el paso del 98 % al 99 % y de aquí al 99,9999 % es una tarea compleja y a la par supone un aumento exponencial de requerimiento y coste total del sistema.

Por tal razón al momento de definir algún tipo de negociación o acuerdo SLA de disponibilidad con los usuarios, es necesario hacerlos consientes de las implicaciones técnicas y económicas que esto representa. En situaciones reales de la vida práctica se alcanza un compromiso para la disponibilidad pretendida acorde a los requerimientos y coste abordable. Es así que mientras los niveles de disponibilidad para un servicio sean más altos, son varias las cosas que suceden en el proyecto:

- En primera instancia, aumentan los costes de hardware de la aplicación debido a la redundancia de servidores, redes y discos.
- Luego se debe tomar en consideración que la identificación y eliminación de errores complejos viene a ser una tarea cada vez más difícil, por lo que se requiere de ingenieros capacitados en dicha área.
- Por otra parte una alta disponibilidad requiere una comprobación exhaustiva de cada uno de los procesos automáticos y manuales que pueden afectar a la aplicación mientras ésta se encuentra en servicio.

A continuación se presenta en la tabla 4.2, se observan los porcentajes de disponibilidad y tiempos de caída permitidos tomando en cuenta las 24 horas diarias.

Tabla 4.2: Disponibilidad para un sistema 24×7 y tiempos de caída permitidos.

Disponibilidad (%)	Tiempo offline/año	Tiempo offline/mes	Tiempo offline/día
90 %	36.5 días	73 hrs	2.4 hrs
95 %	18.3 días	36.5 hrs	1.2 hrs
98 %	7.3 días	14.6 hrs	28.8 min
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
99999 %	5.26 min	26.3 s	0.86 s
999999 %	31.5 s	2.62 s	0.08 s

Fuente: <http://everac99.wordpress.com/2008/08/19/alta-disponibilidad-que-es-y-como-se-logra/>

4.6.4.2. Clúster de alta disponibilidad en máquinas virtuales

Recordando que el Clúster es una agrupación de dos o más computadoras las mismas que se encuentran interconectados entre si y que normalmente trabajan de forma conjunta con algún propósito determinado. Desde el exterior en la mayoría de casos, el Clúster es visto como un único equipo el cual ofrece determinados servicios.

Ahora al relacionar de forma directa los conceptos de Clúster y virtualización, lo que se pretende es integrar a la red Wi-Fi de la FISEI es el establecimiento un Clúster de alta disponibilidad virtualizado, es decir que sus nodos sean máquinas virtuales ubicadas en un mismo equipo.

Tomando en cuenta todo lo visto hasta el momento acerca de virtualización no es difícil pensar que la tecnología Clúster puede ser implementada en entornos virtualizados para aprovechar de esta manera todas las ventajas particulares de estos entornos. De esta forma se puede apreciar que el Clúster es un caso especial en el que las ventajas importantes que aporta la virtualización pueden llegar a apreciarse más intensamente en lo que tiene que ver con ahorro en espacio y consumo energético, mayor porcentaje de utilización del hardware de los servidores, menor coste en la administración del Clúster, pero sobre todo, que los nodos del Clúster pasen a ser entes lógicos con todo lo que ello conlleva: rápida recuperación ante desastres, mejora de las políticas y rapidez de procesos como puesta en marcha, recuperación y copias de seguridad, gran escalabilidad, aumento de la seguridad, flexibilidad, etc. De esta manera se hace posible la implementación de un clústeres con tan sólo un único servidor físico (o varios si se deseara mayor redundancia y seguridad ante fallos en él), básicamente los nodos físicos de un Clúster real pasan a ser máquinas virtuales (nodos virtuales) alojadas en el servidor. Las máquinas virtuales pueden operar como nodos de un Clúster de igual forma a como lo harían los servidores físicos, ya que como se ha visto en estas máquinas es posible instalar sistemas operativos, aplicaciones servicios, etc., y para este caso un software destinado a dar alta disponibilidad al servicio de autenticación de la red Wi-Fi dentro de la FISEI [19].

4.6.4.3. Soluciones de alta disponibilidad

En cuanto a las soluciones GNU/Linux de alta disponibilidad se tienen varias soluciones tomando en cuenta las dos categorías que son alta disponibilidad de servicios y alta disponibilidad de datos, se destacan a continuación las soluciones de mayor trascendencia [20].

■ Soluciones de alta disponibilidad de Servicios

En lo que tiene que ver con las soluciones de alta disponibilidad para servicios las aplicaciones más destacadas son las que se muestran en las siguientes tablas 4.3, 4.4 y 4.5:

Tabla 4.3: Características principales de Heartbeat

Heartbeat	Definición	Heartbeat es un proyecto software que provee un framework flexible, destinado a mantener servicios de Alta Disponibilidad tanto para máquinas reales como virtuales.
	Modelo de Alta disponibilidad	Heartbeat implementa una configuración punto a punto entre nodos en un modelo activo / pasivo, al menos se necesitan dos máquinas que ejecuten Heartbeat simultáneamente.
	Funcionamiento	Heartbeat se basa en el envío y recepción de señales enviadas por los demonios de Heartbeat que se ejecutan en ambas máquinas, a estas señales se les conocen como “latidos”, lo que representa la detección de fallos en cada nodo. Heartbeat es el encargado de inicializar o detener el servicio al cual se le quiere prestar en alta disponibilidad. Este servicio es prestado a través del uso de una única IP en ambas máquinas, que en realidad no es más que la dirección IP Virtual (VIP).
	Comunicación	La comunicación entre los nodos activo y pasivo pueden efectuarse por medio de dos interfaces, el puerto serial (RS-232) o las tarjetas Ethernet. En el caso de tener servidores virtuales la comunicación se efectúa mediante el protocolo TCP/IP

Fuente: <http://roaksoax.files.wordpress.com/2009/03/thesis.pdf>

Tabla 4.4: Características principales de KeepAlived

KeepAlived	Definición	KeepAlived es una solución software la cual permite proporcionar alta disponibilidad con utilización del protocolo VRRP para el balanceo de carga basado en LVS, realizando un monitoreo de salud del Clúster para que en caso de fallo el Clúster siga en funcionamiento.
	Modelo de Alta disponibilidad	Permite implementar una configuración activo/pasivo para balanceadores de carga en LVS, además permite el monitoreo N nodos reales
	Funcionamiento	Teniendo en cuenta que KeepAlived cuenta con dos frameworks, el uno para verificación de salud en los nodos, el otro para el failover de alta disponibilidad. De igual manera que Hearbeat el servicio que KeepAlived presta es a través del uso de una única IP virtual la cual representa en conjunto a los nodos que conforman el Clúster.
	Comunicación	La comunicación entre los nodos reales puede efectuarse por medio de dos interfaces, el puerto serial (RS-232) o las tarjetas Ethernet.

Fuente: <http://roaksoax.files.wordpress.com/2009/03/thesis.pdf>

Tabla 4.5: Características principales de Ldirectord LVS

Ldirectord LVS	Definición	Ldirectord es una solución software que permite monitorear los servicios de un Clúster de balanceo de carga creados mediante LVS.
	Modelo de Alta disponibilidad	Permite implementar un configuración punto – multipunto ya que existe un nodo que se encarga de gestionar y repartir las conexiones (nodo máster LVS) entre todos los nodos slave del Clúster. El servicio de datos debe residir en todos los nodos slave. LVS puede llegar a soportar sin problemas hasta 200 nodos slave.
	Funcionamiento	Ldirectord es un paquete que se ejecuta en el máster LVS, que se encarga de testear el servicio de datos de los nodos slave y eliminarlos e insertarlos en el Clúster dinámicamente, si surge algún problema o si se repone el servicio según sea el caso.
	Comunicación	La comunicación entre los nodos reales puede efectuarse por medio de dos interfaces, el puerto serial (RS-232) o las tarjetas Ethernet.

Fuente: <http://roaksoax.files.wordpress.com/2009/03/thesis.pdf>

En este punto cabe señalar que el departamento de redes y sistemas de la FISEI cuenta con un servidor principal bastante robusto en el cual se pueden crear ambientes virtualizados para servidores. Tomando en cuenta que el Servidor principal ya cuenta con dos servidores virtuales para servicios en otras áreas de la FISEI; para el presente proyecto se han otorgado la creación de hasta 3 máquinas virtuales con las respectivas limitantes en las características de cada una. Como ya se conoce de acuerdo a lo detallado en el capítulo anterior, el destino de una de las 3 máquinas virtuales tiene como objetivo realizar el monitoreo de la red Inalámbrica, por lo tanto se tiene la oportunidad de trabajar con dos máquinas virtuales para la creación del Clúster de alta disponibilidad para el servicio de autenticación en la red Wi-Fi de la FISEI.

Por lo tanto acorde a las características principales de las soluciones de alta disponibilidad para servicios que se pueden observar en las tablas anteriores, y a los recursos brindados por el Departamento de Redes y Sistemas de la FISEI, la solución de alta disponibilidad que más se ajusta a las necesidades de este proyecto es la aplicación Heartbeat, ya que este software permite la creación de un Clúster con dos nodos con configuración activo/pasivo los cuales pueden ser implementados virtualmente. Además Heartbeat trabaja con un sistema de detección de fallos en nodos manteniendo de esta manera un servicio continuo.

■ Soluciones de alta disponibilidad de Datos

En cuanto a las soluciones de alta disponibilidad para datos entre las aplicaciones más destacadas se tienen:

- **MySQL Replication**

Es un módulo del servicio MySQL. Consiste en una replicación asíncrona unidireccional: un servidor actúa como maestro y uno o más actúan como esclavos, al momento cualquiera de los nodos se encuentre activo este vendría a actuar como maestro, por lo tanto se dice también que se puede realizar la replicación maestro - maestro. El servidor maestro escribe actualizaciones en el fichero de log binario, y mantiene un índice de los ficheros para rastrear las rotaciones de logs. Estos logs sirven como registros de actualizaciones para enviar a los servidores esclavos. Cuando un esclavo se conecta al maestro, informa al maestro de la posición hasta la que el esclavo ha leído los logs en la última actualización satisfactoria. El esclavo recibe cualquier actualización que ha tenido lugar desde entonces, y se bloquea y espera para que el master le envíe nuevas actualizaciones.

- **FreeNAS**

FreeNAS es un servidor NAS “Network-Attached Storage” gratuito, que soporta: protocolos Cifs (Samba), Ftp, Nfs, Rsync, autenticación de usuario local, RAID (0,1,5) por software con un completo interfaz de configuración Web. FreeNAS ocupa menos de 32MB una vez instalado en Compact Flash, disco duro o un dispositivo de memoria USB. FreeNAS está basado en FreeBSD que es un derivado de Unix, permitiendo clientes tanto de GNU/Linux como Windows y por supuesto Unix.

- **DRBD**

Software de replicación de dispositivos de bloque formando un RAID 1 a través de la red, es decir, replica los datos en distintas localizaciones. Datos de un sistema de archivos, de una base de datos, etc. Algunas de sus características son una replicación en tiempo real de manera continua, transparencia en las aplicaciones que estén almacenando datos en la unidad, posibilidad de recuperación de los datos ante un desastre, etc.

De la misma forma que en las soluciones de alta disponibilidad para servicios, al observar ahora las características de las soluciones de alta disponibilidad para datos, las tres soluciones pueden ser adaptables al presente proyecto, sin embargo cabe señalar que por mayor trascendencia y confiabilidad en el respaldo de datos [21] en ambientes virtuales, lo óptimo es trabajar con MySQL Replication como solución de alta disponibilidad para datos.

4.6.4.4. Heartbeat como herramienta para Clúster de alta disponibilidad

Heartbeat es una de las soluciones software de mayor trascendencia en el campo de la alta disponibilidad para servicios críticos a fin de que éstos se encuentren disponibles en ejecución de forma ininterrumpida a pesar de los fallos o problemas que puedan surgir durante su funcionamiento. Como se ha dicho mediante su uso es posible obtener alta disponibilidad de servicios, tomando en cuenta que estos servicios pueden mejorar sustancialmente el rendimiento general del sistema y por lo mismo todo esto conlleva con un coste de implementación y administrativo reducido.

Heartbeat trabaja con el modelo activo / pasivo entre nodos, de tal forma que un servicio puede ser migrado de forma rápida y transparente de un nodo del Clúster a otro por el motivo que fuese (por ejemplo ante un fallo en la alimentación del nodo o por motivos administrativos), logrando que éste solamente deje de estar operativo durante el tiempo en el que Heartbeat detecta el fallo y lleva a cabo la migración [19].

- **Comunicación y Funcionamiento**

El funcionamiento de Heartbeat se basa en el envío y recepción de señales enviadas por los demonios (servicios) de Heartbeat que se ejecutan en ambas máquinas, a estas señales se les conocen como “latidos” y de allí su nombre. Estas señales pueden establecer una comunicación punto a punto entre nodos mediante mensajes ICMP (Internet Control Message Protocol, por ejemplo

ping) de forma el uno puede monitorizar el estado del otro (y viceversa). Además, cada nodo monitoriza también en qué estado se encuentran los recursos que actualmente se están ejecutando, para la detección de posibles irregularidades y fallos. Por lo tanto el nodo activo se encuentra monitorizando el estado de los servicios configurados y el nodo pasivo, mientras que el nodo pasivo monitoriza solamente al nodo activo. La diferencia entre el nodo activo y el pasivo radica en la prioridad que tienen para ofrecer un servicio. Aquí, el nodo pasivo solo ofrecerá el servicio cuando deje de escuchar los latidos del nodo activo durante periodo de tiempo determinado, pasado el cual se supondrá que el nodo activo dejó de funcionar. Durante este proceso se efectuará el failover del Clúster [22].

El proceso failback se lleva a cabo una vez que el nodo pasivo empieza a escuchar nuevamente los latidos del nodo activo, entonces éste tomará el control nuevamente, a menos que dentro de la configuración de Heartbeat se haya colocado la directiva `auto_failback` en off. Esta directiva puesta en off, quiere decir que si el nodo activo (maestro) vuelve a funcionar, ya no retomará el control del servicio, sino se convertirá en el nuevo nodo (esclavo).

En la figura 4.6 se puede observar de manera detallada el funcionamiento de Heartbeat para un Clúster de alta disponibilidad [20].

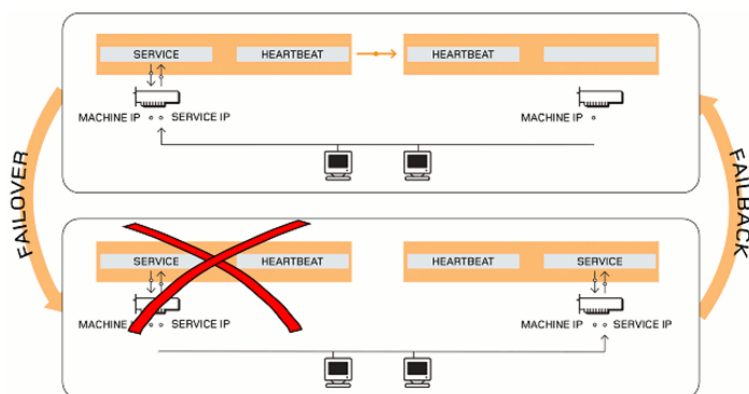


Figura 4.6: Funcionamiento de Heartbeat para un Clúster de alta disponibilidad
Fuente: <http://www.drbd.org/home/what-is-ha/>

4.6.5. Diseño del Clúster de alta disponibilidad para el servidor de autenticación en la red Wi-Fi de la FISEI.

Para conocer de manera integral la estructura del Clúster de alta disponibilidad así como sus diferentes componentes para poder incluirlo en la red de la FISEI, es

necesario contar con un diseño general del mismo con la finalidad de tener claras las ideas al momento de la ejecución de las diferentes instalaciones tanto en la parte física como en la parte lógica del proyecto.

Como se puede ver en la figura 4.7 el diseño se encuentra contando con dos máquinas virtualizadas bajo la plataforma de virtualización con hypervisor XEN, estas máquinas a la vez representan los nodos del Clúster que vendrían a ser los dos servidores RADIUS para la autenticación de usuarios en la red Wi-Fi los cuales al ser configurados dentro del Clúster de alta disponibilidad vienen a tomar la forma de un solo servidor RADIUS, también es necesario contar con otro servidor adicional encargado de las gestiones de monitoreo de la red.

Como ya se ha mencionado anteriormente la inclusión del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI toma lugar en los niveles de Distribución y de Acceso detallados en la figura 4.1. Teniendo presente esto, el diseño de la figura 4.7 cuenta con la utilización adicional de dos dispositivos MikroTik configurados a modo router para el enlace entre las redes WAN y LAN y a la vez cumpliendo las funciones de HotSpot para el acceso y redirección en la comunicación con el servidor RADIUS, el contar con estos dos dispositivos actuando como HotSpot significa tener mayor capacidad para el acceso simultaneo de usuarios a la red Wi-Fi de la FISEI.

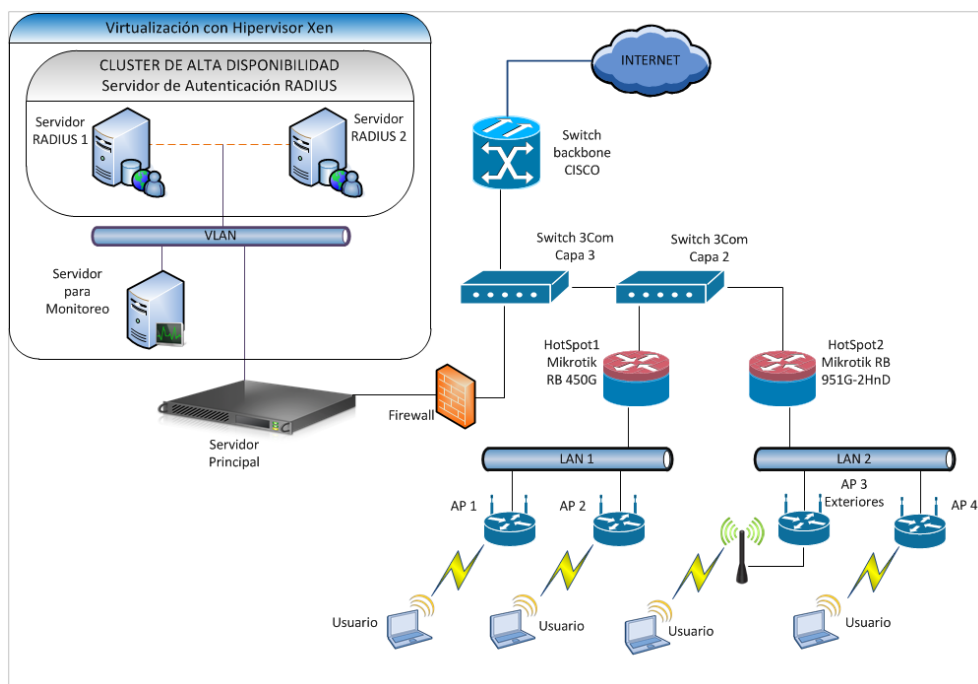


Figura 4.7: Diseño del Clúster de alta disponibilidad - FISEI
Fuente: El Investigador

4.6.6. Equipos de red para el Clúster de alta disponibilidad

4.6.6.1. Servidor Principal

"Server" ó servidor, también llamado "Host" ó anfitrión; es una computadora con muy altas capacidades de proceso, encargada de proveer diferentes servicios a las redes de datos, tanto inalámbricas como las basadas en cable; también permite accesos a cuentas de correo electrónico, administración de dominios empresariales, hospedaje y dominios Web entre otras funciones.

Los servidores de preferencia se deben montar en gabinetes especiales denominados Racks, dónde es posible colocar varios Servers en los compartimientos especiales y ahorrar espacio, además de que es más seguro porque permanecen fijos [23].



Figura 4.8: Servidor Principal de la FISEI - HP Proliant DL180-G6
Fuente: <http://comtel.com.ve/servidor/158-hp-proliant-dl160-g6.html>

A continuación en la tabla 4.6 se pueden ver sus características técnicas:

Tabla 4.6: Características técnicas del servidor HP Proliant DL180-G6

ESPECIFICACIONES	DESCRIPCIÓN
Procesador	Intel® Xeon® E5620 (4 core, 2.40 GHz, 12MB L3, 80W)
Tarjeta Madre	Intel® 5520 Chipset
Memoria	8GB / máximo 192Gb / 18 DIMM Slot
Tarjeta de Red	(1) 1GbE NC362i 2 Ports
Controladora	(1) Smart Array P410 SAS/SATA RAID
Disco Duro	1 TB
Unidad Óptica	5x 10/100/1000 Mbps
Fuente de Poder	30 dBm (1000 mW)
Form Factor	2.5 dBi
Garantía	Yes
Número de Parte	8...30 VDC (PoE port)
Dimensiones	448 x 682 x 43 mm
Peso	16.8 Kg

Fuente: <http://comtel.com.ve/servidor/158-hp-proliant-dl160-g6.html>

4.6.6.2. Router

El router es un dispositivo utilizado para la interconexión de redes informáticas, este dispositivo hace posible asegurar el enrutamiento de paquetes entre redes, es decir determina la ruta que deben tomar los paquetes de datos de acuerdo a las reglas que forman la tabla de enrutamiento [24].

■ Características generales del Router

- El router opera en la capa 3 del modelo OSI. Cabe recalcar que este dispositivo no debe ser confundido con un conmutador.
- Básicamente es un dispositivo de networking que se diferencia del resto por tener la capacidad de interconectar las redes internas y externas.
- La arquitectura de un router está formada por una cpu, memorias, bus de sistema, y distintas interfaces de entrada y salida, similar a la de una pc convencional.
- Una de las funciones principales del router es conocer las redes de otros dispositivos de este tipo, filtrar el tráfico en función de la información de capa de red del modelo OSI, determinar la mejor ruta para alcanzar la red de destino y reenviar el tráfico hacia la interfaz correspondiente.

El símbolo genérico del router para redes informáticas es el siguiente:



Figura 4.9: Símbolo genérico del router para redes informáticas

Fuente: Cisco Icon Library

■ Router Cisco RV180W

El router Cisco RV180W es el dispositivo de red el cual se ha encontrado operando dentro de la FISEI, el mismo ha sido destinado para mediar los servicios de internet a todos los usuarios de la red inalámbrica de la Facultad. A este dispositivo a la vez se encuentran conectados otros dispositivos como Access Point a fin de cubrir todas las áreas de las instalaciones de la FISEI.



Figura 4.10: Router Cisco RV180W

Fuente: http://www.cisco.com/en/US/prod/collateral/routers/ps10907/ps9923/ps11996/c78-697399_data_sheet.html

A continuación en la tabla 4.6 se pueden ver sus características técnicas:

Tabla 4.7: Características técnicas del router Cisco RV180W

ESPECIFICACIONES	DESCRIPCIÓN
WAN/DMZ	
Ethernet de 10/100/1000 Mbps	1 puerto
Red perimetral (DMZ, demilitarized zone)	Basada en software
LAN	
Puertos LAN Gigabit Ethernet de 10/100/1000 Mbps	Switch administrado de 4 puertos
Compatibilidad con redes VLAN	Sí
Routing y red	
Filtrado de MAC e IP	Sí
Activación y reenvío de puerto	Sí
IPv6	Sí
Protocolo de Información de Enrutamiento. (RIP, Routing Information Protocol) v1/RIP v2	Sí/Sí
Routing entre VLAN	Sí
Calidad de servicio (QoS)	Sí
Seguridad y VPN	
Firewall SPI	Sí
Conexiones QuickVPN/de sitio a sitio	10/10
Filtrado de URL/contenido	Sí
Administración	
Configuración basada en navegador (HTTP/HTTPS)	Sí
Protocolo SNMP (Simple Network Management Protocol, protocolo simple de administración de redes)	v1, v2c y v3
RAM	60 MB

Fuente:

http://www.cisco.com/en/US/prod/collateral/routers/ps10907/ps9923/ps11996/brochure_c02-699610_es.pdf

■ Router MikroTik RB951G-2HnD

Como se pudo ver en el dispositivo anterior este solo cuenta con una RAM de 60 MB por lo cual su capacidad para soportar una gran cantidad de usuarios en simultáneo se ve mermada. Es así que para el presente proyecto de investigación se ha optado por trabajar con el router MikroTik RB951G-2HnD el cual tiene una mayor cantidad de MB en RAM y por lo mismo este router permite soportar una mayor cantidad de usuarios conectados simultáneamente.



Figura 4.11: Router MikroTik RB951G-2HnD

Fuente:

http://www.dipolnet.com/routerboard_rb951g-2hnd_5x_10-100-1000mbs_wifi__N24951.htm

A continuación en la tabla 4.8 se pueden ver sus características técnicas:

Tabla 4.8: Características técnicas del router Mikrotik RB951G-2HnD

ESPECIFICACIONES	DESCRIPCIÓN
Name	RouterBoard 951G-2HnD
Code	N24951
Processor	Atheros 600 MHz
WiFi	802.11n (2.4 GHz)
FLASH memory	32 MB
RAM	128 MB
LAN ports	5x 10/100/1000 Mbps
Tx output power (WLAN)	30 dBm (1000 mW)
Antenna gain	2.5 dBi
USB	Yes
Power	8...30 VDC (PoE port)
AC/DC adapter	12 VDC / 1 A (output)
PoE	Yes
Software	RouterOS license level 4
Operating temperature	-20°C...50°C
Dimensions	113x138x29 mm
Weight	0.14 kg

Fuente:

http://www.dipolnet.com/routerboard_rb951g-2hnd_5x_10-100-1000mbs_wifi__N24951.htm

■ Router MikroTik RB450G

De la misma forma que el dispositivo anterior, para este proyecto de investigación también se va a contar con el router MikroTik RB450G, el mismo que posee una mayor capacidad en RAM siendo un dispositivo robusto y que a su vez permitiría mayor cantidad de usuarios en conexión simultánea.



Figura 4.12: Router MikroTik 450G

Fuente: <http://preciod.com/pe/mikrotik-rb-450g-el-mas-potente-cpu-680mhz-y-memoria-256mb-RQy10/venta-html>

A continuación en la tabla 4.9 se pueden ver sus características técnicas:

Tabla 4.9: Características técnicas del router Cisco RV180W

ESPECIFICACIONES	DESCRIPCIÓN
Name	RouterBoard 450G
CPU	Atheros AR7161 680MHz
Memory	256MB DDR SDRAM onboard memory
Boot loader	RouterBOOT
Data storage	onboard NAND memory chip, microSD card slot (on reverse)
Ethernet	Five 10/100/1000 Mbit/s Gigabit Ethernet ports supporting Auto-MDI/X
miniPCI	none
Extras	Reset switch, beeper, voltage and temperature monitors
Serial port	One DB9 RS232C asynchronous serial port
LEDs	Power and User LED
Power	Power over Ethernet: 14..28V DC (except power over datalines) Power jack: 10..28V DC
Dimensions	9 cm x 11.5 cm, 95 grams
Temperature	Operational: -45°C to +70°C
Power consumption	6.4W at maximum load
Humidity	Operational: up to 70 % relative humidity (non-condensing)
Operating System	MikroTik RouterOS v3, Level5 license

Fuente:

<http://www.data-alliance.net/servlet/-strse-282/MikroTik-RouterBoard-RB-fdsh-450G/Detail>

4.6.6.3. Access Point

Un Access Point o punto de acceso inalámbrico más conocido por las siglas WAP o AP en inglés: Wireless Access Point, en redes informáticas es un dispositivo que permite la interconexión entre dispositivos de comunicación inalámbrica para formar una red inalámbrica. Básicamente el Access Point se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming" (En redes inalámbricas, roaming se refiere a la capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad) [25].

■ Características generales del Access Point

- Hace posible la conexión de dispositivos inalámbricos a la WLAN, tales como: teléfonos celulares modernos, Laptops, Notebook, PDAs, etc., e inclusive otros Access Point para ampliar las redes.
- Además estos dispositivos cuentan con soporte para redes basadas en alambre (LAN - Local Area Network), que tienen un puerto RJ45 lo cual permite interconectarse con un Switch inalámbrico y de esta manera formar grandes redes entre dispositivos convencionales e inalámbricos.
- Su tecnología es a base de ondas de radio, capaces de traspasar muros, sin embargo entre cada obstáculo esta señal pierde fuerza y se reduce su cobertura.
- Estos dispositivos pueden tener otros servicios integrados tales como expansor de rango a fin de ampliar la cobertura de la red.
- El alcance máximo de cobertura de estos dispositivos depende del modelo y las características del equipo, siendo la unidad de medida el radio de alcance.
- Normalmente los Access Point cuentan con una antena externa para la correcta emisión y recepción de ondas, para de esta manera poder efectuar una correcta transmisión de la información.

En la figura 4.13 se puede observar el símbolo gráfico para un Access Point de redes de cómputo.



Figura 4.13: Símbolo genérico del Access Point para redes informáticas
Fuente: Cisco Icon Library

Para generar una cobertura total de la red Wi-Fi dentro de los dos edificios de la FISEI se utilizan este tipo de dispositivos con la finalidad de expandir la señal inalámbrica. Los AP's con los que actualmente la FISEI se encuentra trabajando son los siguientes:

- Un AP CISCO WAP200E (para exteriores)
- Un AP CISCO WAP4410N
- Dos AP's LINKSYS WAP54G

4.6.6.4. HotSpot

Un HotSpot, (en inglés "punto caliente") es un dispositivo de acceso el cual permite tener cobertura wireless (sin cables) a través de estándares Wi-Fi, con la finalidad de establecer una comunicación inalámbrica Wi-Fi entre un dispositivo "cliente" (Laptops, PDAs, Cámara de vigilancia, Teléfonos móviles, etc.) y el punto de acceso principal. Detrás de dicho punto de acceso comúnmente se encontrará un MODEM el cual proporcionara acceso a Internet, o a una red de trabajo. A más de las funciones habituales wireless su valor añadido es la capacidad de control y gestión de usuarios.

Cabe destacar que una característica importante del HotSpot es que hace de una forma fácil el acceso a la red Wi-Fi de cualquier usuario, empleado, cliente o visitante a través de un portal cautivo el cual aparece al abrir el explorador y que habitualmente solicita una identificación mediante User y Password [26].

A continuación se puede apreciar el esquema básico de un HotSpot dentro de una red LAN para servicios de Internet:

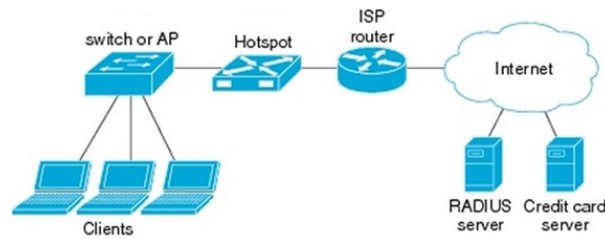


Figura 4.14: Esquema básico de un HotSpot para servicios de Internet

Fuente:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_building_broadband_service_manager/hotspot/1.0/user/guide/hs10_01.html

4.6.7. Topologías de las redes inalámbricas

La topología de una red es la arquitectura de la red, la estructura jerárquica que hace posible la interconexión de los equipos con estándar IEEE 802.11. Existen dos modos diferentes de operación para los dispositivos 802.11[27]:

- Ad - Hoc (IBSS - Independent Basic Service Set)
- Infraestructura (BSS - Basic Service Set).

4.6.7.1. Topología modo Ad-hoc (IBSS)

Esta modalidad consiste en la comunicación entre dos o más dispositivos inalámbricos los cuales no se encuentran conectados a través de un punto de acceso (Access Point - AP) a una red cableada. Por ejemplo al tener usuarios de laptop que deseen compartir archivos podrían poner una red ad-hoc usando NICs compatibles con 802.11 y compartir archivos a través del medio inalámbrico (WM) sin la necesidad de usar medios externos (por ejemplo discos floppy, tarjetas flash) [27].

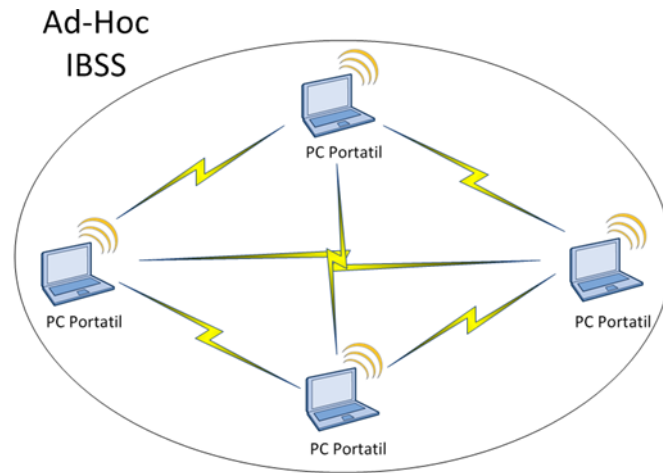


Figura 4.15: Topología modo Ad-hoc (IBSS)
Fuente: El Investigador

4.6.7.2. Topología modo Infraestructura (BSS)

Esta modalidad añade un equipo llamado punto de acceso (AP o Access Point en inglés) el cual realiza las funciones de coordinación centralizada de la comunicación entre los distintos terminales de la red. La topología infraestructura (BSS) es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto [28].

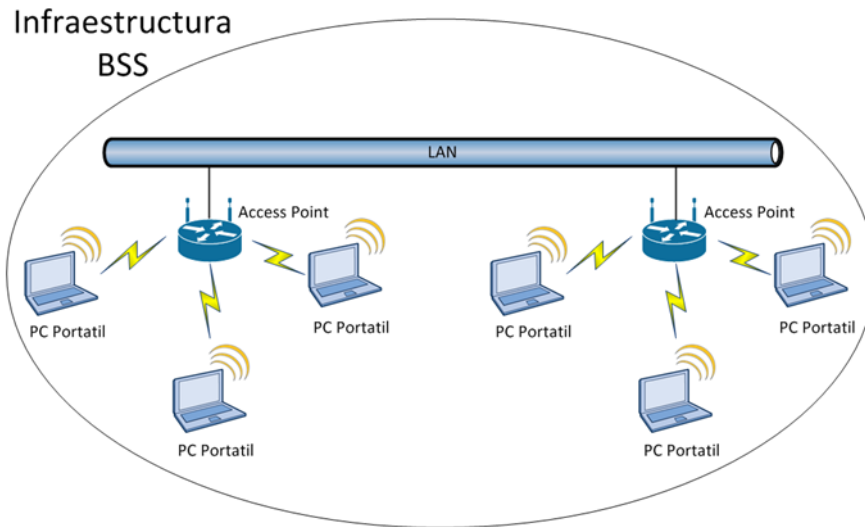


Figura 4.16: Topología modo Infraestructura (BSS)

Fuente: El Investigador

Para el presente proyecto de investigación la topología inalámbrica a utilizar es evidentemente la topología infraestructura (BSS) con el estándar IEEE 802.11 para el nivel de acceso, cubriendo de esta manera los dos edificios de la FISEI mediante la ubicación de los diferentes puntos de acceso. Cabe señalar que es estudio del número de APs así como la ubicación de los dispositivos en la Facultad, se encuentra detallada en la tesis “Red WLAN segura para la interconexión de los edificios de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial” , realizada por el Sr. Santiago Sailema.

4.6.8. QoS y gestión de ancho de banda (AB)

QoS es un conjunto de tecnologías para administrar el tráfico de red de forma rentable a fin de optimizar la experiencia del usuario tanto en entornos empresariales como en hogares y oficinas pequeñas. Las tecnologías de QoS permiten medir el ancho de banda, detectar cambios en las condiciones de la red (por ejemplo, congestión o disponibilidad del ancho de banda) y clasificar el tráfico por orden de prioridad o limitarlo [29].

4.6.8.1. QoS basada en directivas

A medida que crece el tráfico en una red, aumenta la competencia por los recursos limitados de ancho de banda entre el tráfico de menor prioridad y el tráfico generado por las aplicaciones sensibles a la latencia u otras las aplicaciones con

una importancia decisiva. Esta competencia genera un agotamiento del ancho de banda que puede ser especialmente problemático para los usuarios o los equipos con requisitos específicos de rendimiento de red. QoS basada en directiva permite especificar el control del ancho de banda de red en función del tipo de aplicación, los usuarios y los equipos. QoS basada en directivas se puede usar para administrar el tráfico a fin de ayudar a controlar los costos de ancho de banda, negociar los niveles de servicio con los proveedores de ancho de banda o los departamentos comerciales y para ofrecer una mejor experiencia del usuario final. Debido a que QoS basada en directiva está integrada en la Directiva de grupo, forma parte de la infraestructura de administración actual y, en consecuencia, es una solución cuya implementación resulta rentable [29].

4.6.8.2. Consideraciones de ancho de banda para la red Wi-Fi de la FISEI

Teniendo en cuenta que el ancho de banda es la velocidad con la que los datos son transferidos por una conexión, para realizar los respectivos cálculos del ancho de banda, se debe tener en cuenta los siguientes factores:

- Ancho de banda total disponible para la red.
- Ancho de banda asignado para usuarios.
- Número de usuarios en simultáneo

Por lo tanto se tiene la siguiente relación:

$$AB_{usuario} = \frac{AB_{disponible}}{Númerodeusuarios}$$

Considerando que el ancho de banda el cual es asignado para la red inalámbrica por parte del Departamento de Redes y Sistemas de la FISEI es 16 Mbps, y además tomando el valor de 128 Kbps simétricos como valor mínimo pero considerable para la navegación de los usuarios de la FISEI, se determina lo siguiente:

$$Númerodeusuarios = \frac{AB_{disponible}}{AB_{usuario}}$$

$$Númerodeusuarios = \frac{16384Kbps}{128Kbps}$$

$$Númerodeusuarios = 128usuarios$$

Tomando en cuenta estos datos, cabe recalcar que el valor mínimo de ancho de banda de los usuarios hace referencia al estado de la red en horas pico, pero a la vez señalando que la asignación de ancho de banda por usuario se ve considerablemente mayor en horarios regulares y de acuerdo a las directivas QoS para la dinámica de ancho de banda y a los criterios de compartición.

4.7. Ejecución de la Propuesta

Tomando en cuenta que al inicio de este proyecto investigación se encontró que la FISEI no contaba con un servidor RADIUS para efectuar los trabajos de autenticación de usuarios debido a averías en los equipos con los cuales se trabajaban anteriormente y a requerimientos del CEAACES en cuanto al acceso al Internet en las redes inalámbricas; se procede a efectuar los siguientes puntos a fin de levantar un Clúster de alta disponibilidad enfocado al servicio de autenticación el mismo que contenga políticas de acceso acordes a las demandas del CEAACES:

- Diseño general del Clúster de Alta disponibilidad para el servicio de autenticación de la red Wi-Fi de la FISEI.
- Instalación y configuración de Sistemas Operativos Centos 5.9 mediante paravirtualización dentro del servidor principal de la FISEI destinados a monitoreo de red y nodos del Clúster.
- Instalación y configuración de todas las herramientas necesarias para la implementación del Clúster de alta disponibilidad.
- Configuración de los dispositivos de red y NAS para el Clúster de alta disponibilidad.
- Aplicación de políticas de acceso a la red Wi-Fi de la FISEI en base a directivas QoS.

4.7.1. Diseño general de los entornos virtuales con el hypervisor XEN

Para llevar a cabo el proceso de ejecución del proyecto en lo que tiene que ver con las diferentes aplicaciones software, se requiere contar con un servidor para realizar las gestiones de monitoreo de la red Wi-Fi de la FISEI y obviamente con los servidores RADIUS que conforman los nodos para el Clúster de alta disponibilidad como se lo puede ver en la figura 4.17.

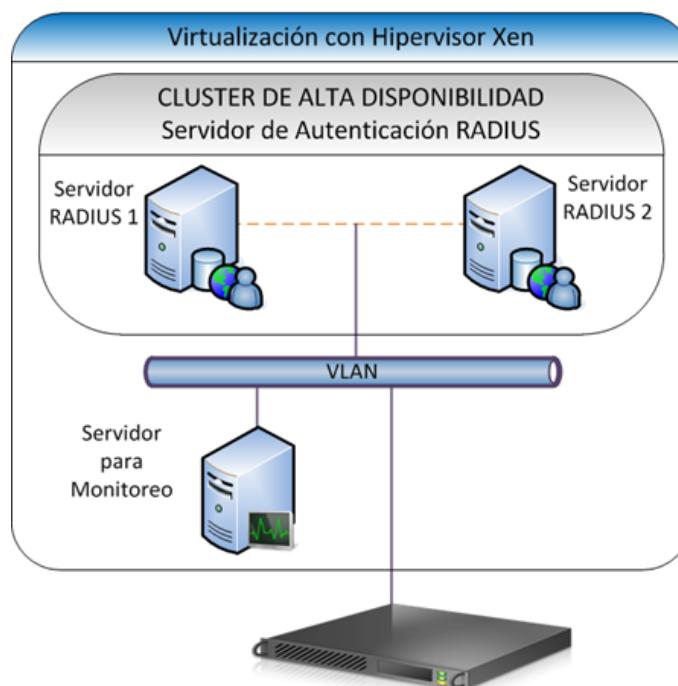


Figura 4.17: Entornos virtuales con hypervisor XEN
Fuente: El Investigador

4.7.2. Requerimientos del Clúster de alta disponibilidad para el servicio de autenticación de la red Wi-Fi de la FISEI

En lo que tiene que ver con la instalación del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI, para llevar a efecto estos procesos es necesario contar con una serie de requerimientos hardware y software son los cuales es posible la inclusión y funcionamiento del Clúster a fin de cubrir cualquier deficiencias que conlleva la utilización de la red inalámbrica por parte de los usuarios.

4.7.2.1. Hardware

A continuación en la siguiente tabla se detallan los requerimientos mínimos de hardware necesarios para implementación del Clúster de alta disponibilidad.

Tabla 4.10: Requerimientos hardware

Hardware	Características mínimas
Servidor	Intel Pentium 4
	Memoria RAM 2GB
	Disco duro de 120Gb
	Dos tarjetas de red
Router	Procesador 600 MHz
	RAM 128 MB
	Wi-Fi 802.11n (2.4 GHz)
	Soporte para configuración Hostpot
	Soporte para RADIUS Server
Access Point	Soporte de Multiples SSID's
	Access Point para soluciones Indoor
	Soporte de PoE (Power over Ethernet)
	Soporte WEP
	Soporte WPA, AES y 802.11i
	Seguridad Ampliada, con soporte de ACL, 802.1x y MAC Address
	Administración versátil, vía D-Link D-View, SNMP v3, Web, Telnet y AP

Fuente: El Investigador

4.7.2.2. Software

Teniendo en cuenta que en el servidor principal de la FISEI se encuentra instalado el Sistema Operativo Centos 5.8 el mismo que se encuentra trabajando con el Hipervisor XEN, en tal virtud las respectivas instalaciones de software estarán contenidas bajo esta plataforma, la cual es ideal para servidores y además es libre.

En cuanto a los requerimientos de software necesarios de instalación para el Clúster de alta disponibilidad en la FISEI se detalla lo siguiente:

- Hypervisor XEN
- VMs Paravirtualizadas
- LAMP
- FreeRADIUS
- DaloRADIUS
- Heartbeat

4.7.3. Herramientas de ejecución para la implementación del Clúster de alta disponibilidad

Para llevar a cabo el proceso de implementación del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI, se requiere la creación de entornos virtuales mediante la utilización del hypervisor XEN con paravirtualización en conjunto con la instalación y configuración de los software para las diferentes aplicaciones las cuales hacen posible levantar todos los servicios requeridos para el proyecto, de la misma manera se deben realizar las respectivas configuraciones en los equipos de red los cuales intervienen de forma directa con el Clúster de alta disponibilidad.

4.7.3.1. Instalación de máquina virtual mediante el hypervisor XEN con paravirtualización para el servidor de monitoreo de red.

El servidor de la FISEI se encuentra actualmente trabajando con la distribución libre Centos 5.8 y a su vez el mismo se encuentra utilizando el hypervisor xen-3.0.3-135.el5_8.5. De esta manera la opción más ideal para crear una máquina virtual es utilizar paravirtualización ya que permite tener un buen rendimiento en la utilización de servidores. Cabe señalar que las máquinas creadas con este tipo de virtualización son a la vez monitorizadas por el hypervisor XEN y administradas por la dom0. Esta instalación de esta primera máquina virtual tiene como objetivo realizar el monitoreo de la red inalámbrica a fin de ver el tráfico que se genera en esta red. Cabe destacar que los datos obtenidos del monitoreo han sido detallados en el capítulo 3 para la sustentación del problema. El nombre que se le ha dado a esta primera VM es dInalambrica.

Lo primero a realizar antes iniciar la instalación de la máquina virtual, es la creación del espacio en el disco con el nombre del servidor.

```
lvcreate -L10G dsk -ndInalambrica
```

Verificación

```
ls /dev/dsk/dInalambrica
```

Inicio de la Instalación

En primer lugar se ejecuta el siguiente comando:

```
virt-install --prompt
```

Al ejecutar este comando automáticamente aparecen una serie de preguntas de instalación las cuales se deben responder de acuerdo a la configuración que se desee.

En respuesta a las preguntas lo primero que se debe especificar es si se requiere trabajar con full virtualización por lo que se debe poner no, entendiéndose que lo que se requiere es trabajar con paravirtualización.

```
no
```

Especificar un nombre para la máquina es está siendo instalada.

```
dlnalambrica
```

También es necesario especificar el tamaño que se le quiere otorgar a la memoria RAM de la máquina

```
1048 MB
```

Especificar el directorio destino en donde se requiere realizar la instalación de la máquina.

```
/dev/dsk/dlnalambrica
```

Por último se coloca el URL del mirror desde donde se puede realizar la descarga.

```
http://mirror.esPOCH.edu.ec/centos/5.9/os/x86_64/
```

Luego de realizar este proceso de inmediatamente al reconocer el repositorio de descarga seleccionado aparece la primera ventana para el inicio de instalación de Centos 5.9, aquí se debe seleccionar el idioma para el proceso de instalación, como se ve en la figura 4.18.

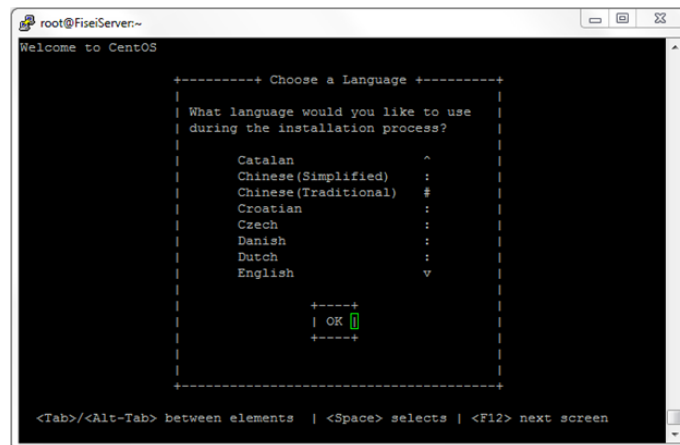


Figura 4.18: Selección del idioma para instalación de Centos 5.9
Fuente: El Investigador

En la siguiente ventana que aparece se realizan las configuraciones TCP/IP, entonces se elige la configuración manual para IPv4 como se muestra en la figura 4.19.

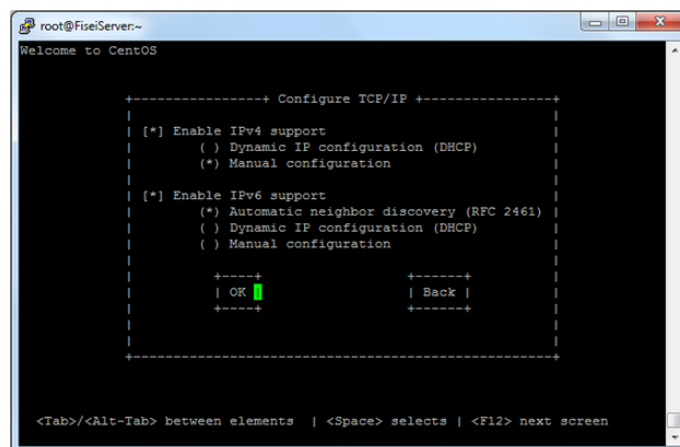


Figura 4.19: Selección de configuración TCP/IP
Fuente: El Investigador

Una vez seleccionada la configuración manual para IPv4 inmediatamente aparece otra ventana en donde se colocan con las respectivas direcciones de IPv4, para este caso la dirección IP a utilizar en el servidor para monitoreo es la 192.168.124.15, como se muestra en la figura 4.20.

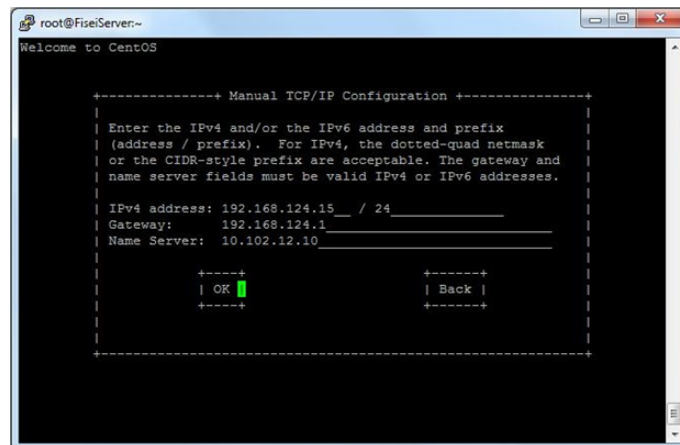


Figura 4.20: Configuración manual TCP/IP
Fuente: El Investigador

En la siguiente ventana se elige la opción: Use text mode, con la finalidad de trabajar en modo texto en la máquina virtual lo cual es ideal para servidores Linux, como se ve en la figura 4.21.

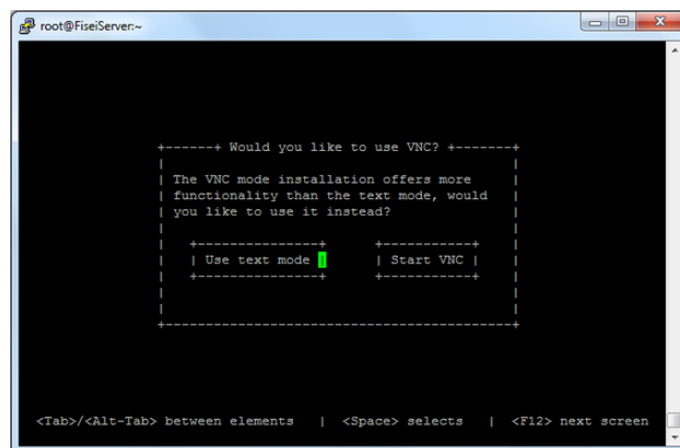


Figura 4.21: Selección text mode
Fuente: El Investigador

A continuación se presiona en OK para que se dé inicio a la instalación automática, a partir de esto en las siguientes ventanas que aparezcan simplemente se continúa intuitivamente hasta finalizar.

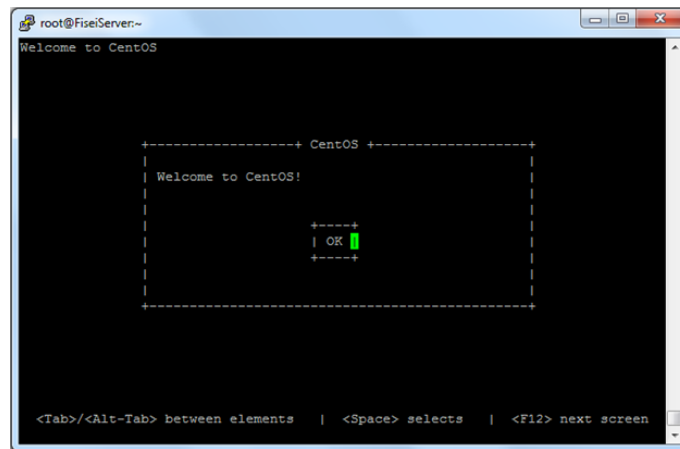


Figura 4.22: Inicio de instalación automática
Fuente: El Investigador

4.7.3.2. Monitoreo de la red Wi-Fi de la FISEI

Como se tenía en conocimiento la FISEI no contaba con un software de monitoreo para su red inalámbrica, y por lo mismo no se contaba una información detallada del funcionamiento de la red o del tráfico en la misma, es así que en caso de ocurrencia de fallas en la red se hacía complejo el determinar las posibles causas de dichas fallas o a su vez el lugar o los dispositivos donde se podría estar congestionado la red, por ejemplo la existencia de cuellos de botella u otros problemas, en fin pueden ser varias las razones por las que se podrían encontrar deficiencias en la red, por tal motivo se ve indispensable la creación de una máquina virtual la cual sea destinada para el uso específico de monitorización de la red Wi-Fi de la FISEI, como ya se ha mencionado anteriormente el software con el cual se están llevando las gestiones de monitoreo es “Cacti” que es una solución completa para la monitorización de redes diseñada para aprovechar el poder de almacenamiento y la funcionalidad para gráficas gracias a las aplicaciones RRDtool. Cacti es una herramienta desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios, además de tener información prácticamente a tiempo real sobre routers, switches o servidores, tráfico de interfaces, cargas, cpu, temperaturas, etc. El protocolo que utiliza Cacti para facilitar el intercambio de información de administración entre dispositivos de redes SNMP.

4.7.3.3. Protocolo SNMP

SNMP (Simple Network Management Protocol), es un protocolo de administración de red el cual trabaja en el nivel de aplicación para consulta a los diferentes elementos

los cuales conforma una red, (routers, switches, hubs, hosts, modems, impresoras, etc). Cada equipo conectado a la red ejecuta unos procesos (agentes), para que se pueda realizar una administración tanto remota como local de la red. Dichos procesos van actualizando variables (manteniendo históricos) en una base de datos, que pueden ser consultadas remotamente [30].

■ Estructura SNMP

SNMP cuenta con 4 componentes principales en su estructura:

- Estación (o consola) de administración
- Agente de administración
- Base de información de administración
- Protocolo de administración

De esta manera SNMP facilita la comunicación entre la estación administradora y el agente de un dispositivo de red (o nodo administrado), permitiendo que los agentes transmitan datos estadísticos (variables) a través de la red a la estación de administración.

■ Versiones SNMP

- Versión 2: La versión 1 con el fin de reducir la carga de tráfico adicional para la monitorización y solucionar los problemas de monitorización remota o distribuida (con las RMON), ha dado paso a una nueva versión v2 en 1993. Cabe recalcar que las versiones de SNMP son compatibles, en el sentido que SNMPv2 puede leer SNMPv1.
- Versión 3: El mecanismo de autenticación (validación) que utiliza SNMPv1 un parámetro llamado “comunidad”, de manera que si la estación administradora y el agente lo conocen, estos pueden interactuar, esta protección puesto que el texto el cual se muestra es visible y además puede explotarse en fuerza bruta. Debido a esto, para evitar la falta de seguridad en las transmisiones (con cifrado y autenticación), se ha creado una capa o parche complemento a SNMPv1 y v2 llamado versión v3, la cual añade a los mensajes SNMP (v1 y v2) una cabecera adicional.

4.7.3.4. Instalación del software de monitoreo Cacti

Para la instalación y funcionamiento de Cacti es necesaria la instalación de los servicios LAMP, así como otros paquetes adicionales los cuales se describen a continuación.

- httpd
- php
- php-mysql
- php-snmp
- mysql
- mysql-server
- net-snmp

Apache: Servidor Web para mostrar gráficos de redes creadas por PHP y RRDtool.

MySQL: Servidor de base de datos para almacenar la información de los cactus.

PHP: Módulo de script para crear gráficos usando RRDtool.

PHP-SNMP: Extensión de PHP para SNMP para acceder a los datos.

NET-SNMP: SNMP (Simple Network Management Protocol) se utiliza para la gestión de la red.

RRDtool: Herramienta de base de datos para gestionar y recuperar datos de series de tiempo, como la carga de CPU, ancho de banda de red, etc.

Inicio de la Instalación

Antes de comenzar el proceso de instalación es necesario estar registrados como root en la VM y realizar las respectivas comprobaciones de red a fin de verificar que se puedan realizar las descargas de datos sin problemas. Una vez efectuado esto, se realiza lo siguiente:

Agregar un nuevo repositorio yum, mediante la creación un nuevo archivo:

```
vi /etc/yum.repos.d/dag.repo
```

En este archivo se redacta lo siguiente:

```
[dag]
name=Dag RPM Repository for Red Hat Enterprise Linux
baseurl=http://apt.sw.be/redhat/el5/en/x86_64/dag
gpgcheck=1
gpgkey=http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
enabled=1
```

Esto se lo realiza para evitar problemas al momento de la instalación cuando los repositorios por defecto no contienen los diferentes paquetes requeridos.

Instalación de Apache

```
yum install httpd httpd-devel
```

Instalación de MySQL

```
yum install mysql mysql-server
```

Instalación de PHP junto con paquetes necesarios

```
yum install php-mysql php-pear php-common php-gd php-devel  
php php-mbstring php-cli php-mysql
```

Instalación de PHP-SNMP

```
yum install php-snmp
```

Instalación de NET- SNMP

```
yum install net-snmp-utils p net-snmp-libs php-pear-Net-SMTP
```

Instalación de RRDTool

```
yum install rrdtool
```

Una vez que se ha instalado los requerimientos para utilización de Cacti, se inicializan los servicios de Apache MySQL y SNMP.

```
service httpd start  
service mysqld start  
service snmpd start
```

A continuación se configuran estos servicios para que estos puedan arrancar con el sistema.

```
chkconfig httpd on  
chkconfig mysqld on  
chkconfig snmpd on
```

En este punto es necesario instalar y permitir la utilización de repositorio EPEL con el URL adecuado, es decir de acuerdo a la versión de Centos que se esté utilizando. Para esto se utiliza el comando wget y rpm.

```
wget http://download.fedoraproject.org/pub/epel/5/x86_64/epel
-release-5-4.noarch.rpm

rpm -ivh epel-release-5-4.noarch.rpm
```

Una vez instalado el repositorio, se puede instalar la aplicación Cacti utilizando el siguiente comando:

```
yum install cacti
```

Seguido a esto se configura el servicio MySQL para Cacti, para lo cual primero es necesario setear una nueva contraseña para MySQL, esto se lo puede hacer utilizando la siguiente línea:

```
mysqladmin -u root password esf5891to
```

Se debe tomar en cuenta que este comando sirve solo para la nueva instalación de MySQL.

Una vez hecho lo anterior es necesario loguearse en el servidor Mysql con la contraseña que se ha creado, para poder crear una base de datos con el usuario Cacti.

```
mysql -u root -p
mysql>create database cacti;
mysql>GRANT ALL ON cacti.* TO cacti@localhost IDENTIFIED BY '
PASSWORD';
mysql>FLUSH privileges; mysql>quit;
```

A continuación se instalan las tablas para Cacti en la base de datos que se ha creado, para esto primero se averigua la ruta del archivo de base de datos que recién se ha creado utilizando el comando RPM:

```
rpm -ql cacti | grep cacti.sql
```

Esto permite encontrar el archivo cacti.sql indicando su dirección.

```
/usr/share/doc/cacti-0.8.8b/cacti.sql
```

Una vez que se ha localizado el archivo cacti.sql, se escribe el siguiente comando para introducir las tablas:

```
mysql -u cacti -p cacti < /usr/share/doc/cacti-0.8.8b/cacti.
sql
```

Seguido a esto se configura el archivo db.php de la base de datos MySQL para Cacti.

```
vi /etc/cacti/db.php
```

En este archivo se configuran el nombre de usuario y la contraseña las cuales se han establecido anteriormente.

```
/* make sure these values reflect your actual database/host/  
   user/password */  
$database_type = "mysql";  
$database_default = "cacti";  
$database_hostname = "localhost";  
$database_username = "cacti";  
$database_password = "esf5891to";  
$database_port = "3306";  
$database_ssl = false;
```

A continuación se configura el servidor Apache para Cacti, para esto se ubica en el archivo cacti.conf.

```
vi /etc/httpd/conf.d/cacti.conf
```

Para permitir el acceso a la aplicación cacti desde la red local o por IP, se configura lo siguiente:

```
Alias /cacti /usr/share/cacti  
<Directory /usr/share/cacti/>  
    <IfModule mod_authz_core.c>  
        # httpd 2.4  
        Require host localhost  
    </IfModule>  
    <IfModule !mod_authz_core.c>  
        # httpd 2.2  
        Order deny,allow  
        Deny from all  
        Allow from all
```

Para que estos cambios tomen efecto, se reinicia servicio Apache.

```
service httpd restart
```

Finalmente se descomenta la línea del script poller.php que sale cada 5 minutos recogiendo los datos de los host conocidos que están siendo utilizados por Cacti para mostrar los gráficos, para ello se ingresa al siguiente archivo de configuración:

```
vi /etc/cron.d/cacti
```

descomentando:

```
##*/5 * * * * cacti /usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1
```

Una vez que se ha realizado la parte de instalación del servicio de monitoreo, se procede a la instalación la aplicación Cacti vía web, para esto es necesario poner la dirección IP del servidor donde se encuentra localizado Cacti. 192.168.124.15/cacti

La primera ventana que aparece para el proceso de la instalación web de Cacti se la puede observar en la figura 4.23 donde se muestra una guía de instalación, en esta ventana lo único que se hace es simplemente dar clic en el botón Next >> para continuar con la instalación.

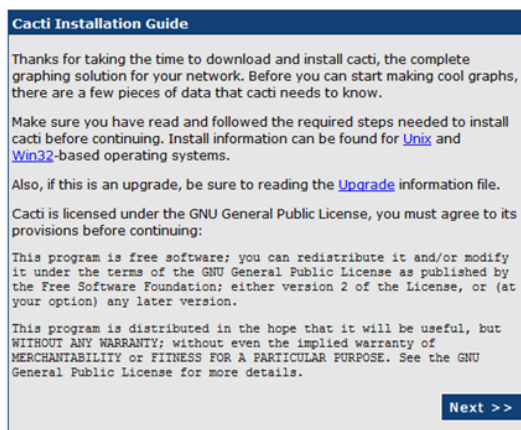


Figura 4.23: Guia de instalación web de Cacti
Fuente: El Investigador

Continuando con la instalación en la siguiente ventana que aparece se procede a escoger el tipo de instalación que se desea, en este caso se debe escoger New Install y de la misma manera para continuar con la instalación se da clic en Next >>, como se puede ver en la figura 4.24.

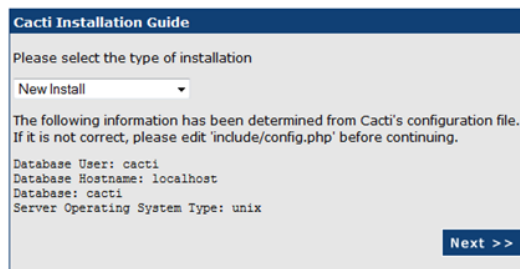


Figura 4.24: Selección del tipo de instalación para Cacti
Fuente: El Investigador

Finalmente aparecerá otra ventana en la que se verifica que todos componentes de instalación para Cacti estén correctos, aquí se puede verificar que la instalación que se ha hecho en el servidor esté bien ya que aparece de color verde la palabra FOUND al encontrar satisfactoriamente los componentes para Cacti, de no ser así aparecería NOT FOUND en rojo para componentes que no se encuentren. Si no existe ningún problema, se procede a dar clic en Finish para terminar con la instalación web de Cacti como se puede ver en la figura 4.25.

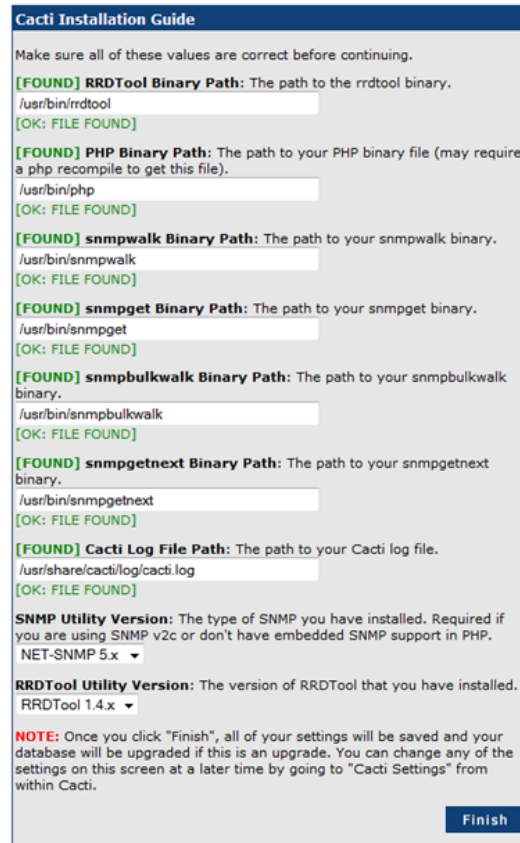


Figura 4.25: Verificación de los componentes de instalación para Cacti
Fuente: El Investigador

Una vez terminada la parte de instalación web de Cacti se puede ingresar con el User Name y el Password a las diferentes configuraciones de administración de Cacti.

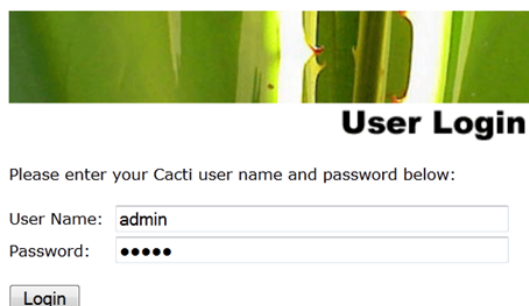


Figura 4.26: Logueo de ingreso web a Cacti
Fuente: El Investigador

4.7.3.5. Diseño físico del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi.

La ejecución de la propuesta la cual se plantea es básicamente la instalación y configuración de dos servidores RADIUS virtuales (VM's o nodos) los mismos que se encuentren intercomunicados entre sí mediante una aplicación (Heartbeat) la cual permita crear un Clúster y que a su vez esta aplicación permita dar alta disponibilidad a los servicios necesarios en cada servidor. De la misma forma se plantea una alta disponibilidad de datos mediante el concepto de replicación maestro a maestro entre servidores. A continuación en la figura 4.27 se puede ver de forma gráfica el diseño del Clúster de alta disponibilidad para el servicio de autenticación de la red Wi-Fi de la FISEI.

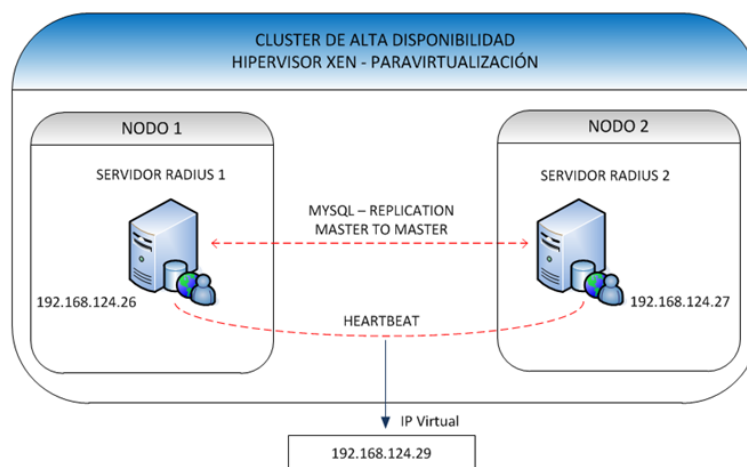


Figura 4.27: Diseño Físico del Clúster de alta disponibilidad
Fuente: El Investigador

4.7.3.6. Diseño lógico del Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi.

Para la implementación del Clúster destinado a dar alta disponibilidad al servidor de autenticación de la red Wi-Fi de la FISEI es necesario tener en cuenta que la alta disponibilidad se debe llevar a efecto tanto para los servicios requeridos como para los datos los cuales conforman de manera integral los nodos a ser clusterizados, como se muestra en la figura 4.28. En cuanto a los servicios requeridos en función de dar alta disponibilidad al servidor de autenticación para este caso se tiene dos:

- Servicio para HTTP
- Servicio para RADIUS

En este caso la aplicación a utilizar para llevar a efecto el Clúster de alta disponibilidad es Heartbeat.

En los que tiene que ver con la alta disponibilidad para los datos se cuenta con la utilidad de replicación de datos en MySQL con configuración maestro a maestro.

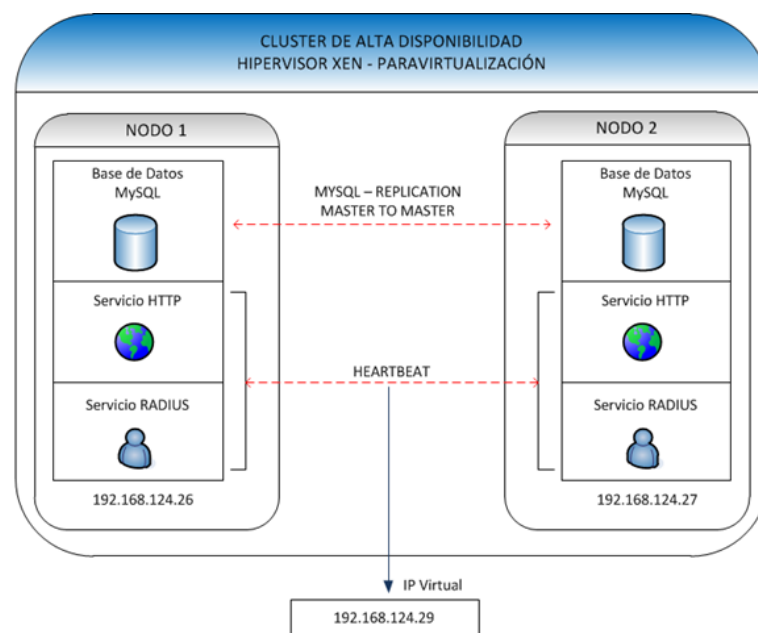


Figura 4.28: Diseño lógico del Clúster de alta disponibilidad
Fuente: El Investigador

4.7.3.7. Instalación de máquina virtual mediante hypervisor XEN con paravirtualización para el servidor RADIUS del Nodo 1

En este punto se debe crear una nueva máquina virtual para establecer el primer servidor el cual vendría a ser el Nodo 1 del Clúster. Este proceso es similar al que

se lo realizó en un punto anterior en la creación de la VM para monitoreo, pero esta vez con el nombre Servm1 para el Nodo 1. Dicho esto el proceso de instalación se lo hace de la misma forma:

Creación de un espejó en disco.

```
lvcreate -L10G dsk -nServm1
```

Verificación

```
ls /dev/dsk/Servm1
```

Inicio de la Instalación

Primero se ejecuta el comando de instalación

```
virt-install --prompt
```

Como ya se conoce, al ejecutar este comando se pueden elegir las configuraciones adecuadas de acuerdo a las preguntas que se presenten.

Lo primero a especificar es si se requiere trabajar o no con full virtualización, por los que se debe poner no, entendiéndose que lo que se requiere es trabajar con paravirtualización.

```
no
```

A continuación se escribe el nombre de la máquina es está siendo instalada.

```
Servm1
```

Se especifica además el tamaño que se le quiere otorgar a la memoria RAM de la máquina.

```
1048 MB
```

Continuo a esto se especifica el lugar de destino en donde se requiere realizar la instalación de la máquina, con el directorio.

```
/dev/dsk/Servm1
```

Por último se coloca el URL del mirror desde donde se puede realizar la descarga.

http://mirror.esPOCH.edu.ec/centos/5.9/os/x86_64/

Luego a esto se presentan una serie de ventanas en las cuales se deben realizar las configuraciones adecuadas para continuar con el proceso de instalación de la VM. En este punto se puede ajustar a las mismas imágenes de la guía de instalación de la VM dInalambrica, con la diferencia que la IP de esta VM es: 192.168.124.26

Configuraciones Adicionales

Algo importante a tomar en cuenta para la máquina virtual que se ha creado es deshabilitar el Firewall y SELinux, con eso se evita cualquier tipo de inconvenientes durante las instalaciones y configuraciones. Esto se logra ingresando en las configuraciones generales de la máquina utilizando setup y luego se elige Firewall Configuration.

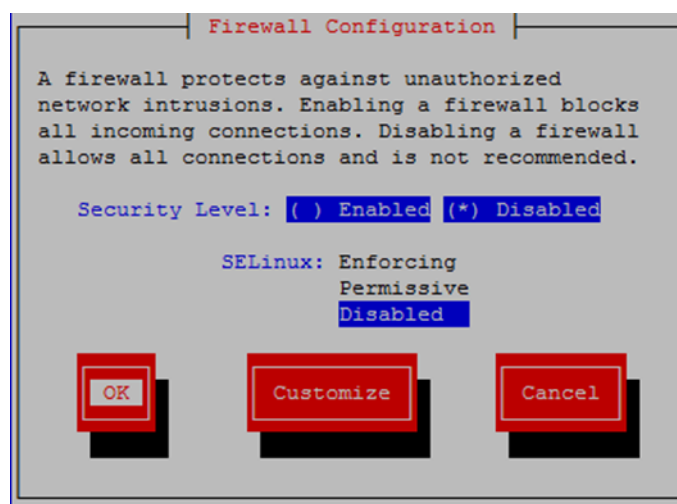


Figura 4.29: Configuraciones de Firewall
Fuente: El Investigador

4.7.3.8. Instalación del Servidor RADIUS en Nodo1

Para la instalación de un servidor RADIUS es indispensable contar con un software que sea confiable y eficiente para brindar servicios de autenticación. Como ya se ha detallado anteriormente en la teoría FreeRADIUS es altamente flexible y configurable capaz de ofrecer un trabajo a nivel de servidor RADIUS. Por ende en este proyecto se ha optado por trabajar con la utilización de este software.

■ Inicio de la Instalación

Para levantar un servidor RADIUS, de igual manera como se lo hizo con Cacti, este proyecto requiere contar con los servicios LAMP y otros paquetes adicionales los cuales permitirán realizar una configuración completa y funcional del servidor RADIUS.

```
yum install freeradius2 freeradius2-mysql freeradius2-  
utils mysql-server mysql php-mysql php php-pear-DB  
httpd openssl mod_ssl
```

Una vez instalado los diferentes servicios y aplicaciones, se los configura para que estos puedan arrancar con el sistema.

```
chkconfig mysqld on  
chkconfig radiusd on  
chkconfig httpd on
```

■ Configuraciones para RADIUS

Se edita en el archivo radiusd.conf, en el cual es necesario descomentar la línea 700.

```
vi /etc/raddb/radiusd.conf  
  
$INCLUDE sql.conf  
$INCLUDE sql/mysql/counter.conf (Opcional)
```

Se edita el archivo default, en donde es necesario descomentar las líneas 177, 406 y 454.

```
vi /etc/raddb/sites-available/default
```

Se edita en el archivo inner-tunnel, para descomentar las líneas 131 y 255.

```
vi /etc/raddb/sites-available/inner-tunnel
```

En el archivo clients.conf, se coloca la clave secreta del servidor RADIUS.

```
vi /etc/raddb/clients.conf  
  
secret = ra4826us (Clave 1)
```

Por último se debe reiniciar FreeRADIUS para que las nuevas configuraciones tomen efecto.

```
service radiusd restart
```

Si se tiene algún problema se puede ejecutar FreeRADIUS en debug mode (modo de depuración) para encontrar algún problema de autenticación, para realizar esto se ejecuta:

```
radiusd -X
```

■ Configuraciones de base de datos en MySQL para RADIUS

Se inicia la instancia MySQL

```
/etc/init.d/mysqld start
```

Se configura el servicio MySql para Cacti, para lo cual primero es necesario setear una nueva contraseña para MySql, esto se lo puede hacer utilizando la siguiente línea:

```
mysqladmin -u root password esf7913to
```

Cabe señalar que este comando sirve solo para la nueva instalación de MySql.

Continuo a esto se ingresa a MySQL para crear una base de datos para el servidor radius.

```
mysql -uroot p
```

Se crea la base de datos y se otorgan los privilegios de usuarios a radius.

```
mysql> CREATE DATABASE radius;
mysql> GRANT ALL ON radius.* TO radius@localhost
IDENTIFIED BY "esf7913to";
mysql> flush privileges;
mysql> exit
```

Se construyen además los esquemas para la base de datos del radius.

```
mysql -uradius -p radius < /etc/raddb/sql/mysql/schema.
sql
mysql -uradius -p radius < /etc/raddb/sql/mysql/nas.sql
mysql -uradius -p radius < /etc/raddb/sql/mysql/wimax.sql
mysql -uradius -p radius < /etc/raddb/sql/mysql/ippool.
sql
mysql -uradius -p radius < /etc/raddb/sql/mysql/cui.sql
```

Se edita el archivo `sql.conf`, en donde se introducen los detalles de la base datos MySQL que se acabó de crear y a su vez se descomenta la línea `readclients = yes`

```
vi /etc/raddb/sql.conf

# Connection info:
server = "localhost"
port = 3306
login = "radius"
password = "esf7913to"

readclients = yes
```

■ Creación de un usuario de prueba

Es conveniente crear un usuario de prueba en la base de datos de radius para poder verificar la conexión con el servidor RADIUS. Para esto se ejecuta lo siguiente:

Se ingresa al servicio MySQL con el password respectivo, para esto se ejecuta lo siguiente:

```
mysql uradius -p
```

Es preciso ubicarse en la base de datos de radius.

```
use radius;
```

Para la creación del usuario de prueba se en MySQL se especifica lo siguiente:

```
mysql> INSERT INTO radcheck (UserName, Attribute, Value)
VALUES ('felipe', 'Password', 'us1739rio');
```

La siguiente línea permite visualizar el usuario creado.

```
select * from radcheck;
```

Una vez terminado este proceso se debe salir del servicio MySQL, para lo cual se ejecuta lo siguiente:

```
exit;
```

Finalmente para que las configuraciones tomen efecto se da reinicio el servicio radius.

```
service radiusd restart
```

Se puede comprobar la conexión del usuario creado utilizando la siguiente línea:

```
radtest felipe 12345 localhost 1812 ra4826us (Clave 1)
```

Al estar correcta la conexión del usuario creado, se tiene el siguiente resultado:

```
Sending Access-Request of id 104 to 192.168.124.29 port
1812
    User-Name = "felipe"
    User-Password = "12345"
    NAS-IP-Address = 127.0.0.1
    NAS-Port = 1812
    Message-Authenticator = 0
        x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 192.168.124.29
port 1812, id=104, length=20
```

4.7.3.9. Instalación de DaloRADIUS en Nodo 1

Como se vio anteriormente en la teoría, DaloRADIUS es un herramienta versátil y eficiente en lo que tiene que ver con administración RADIUS vía web. Para llevar a cabo la instalación de DaloRADIUS se realiza lo siguiente:

Se descargan los paquetes de instalación de DaloRADIUS desde los repositorios disponibles.

```
wget http://sourceforge.net/projects/daloradius/files/latest/  
download?source=files
```

Una vez descargado los paquetes de instalación se los descomprimen, puesto que estos tienen la extensión `.tar.gz`; para ello se utiliza la siguiente línea:

```
tar zxvf daloradius-0.9-9.tar.gz
```

Se pasa el archivo .sql de DaloRADIUS a la base de datos radius.

```
mysql -uradius -p radius < daloradius-0.9-9/contrib/db/fr2-  
mysql-daloradius-and-freeradius.sql
```

Se configura el archivo daloradius.conf.php, para añadir el nombre de usuario en la base de datos y la contraseña.

```
vi daloradius-0.9-9/library/daloradius.conf.php  
  
$configValues['DALORADIUS_VERSION'] = '0.9-9';  
$configValues['FREERADIUS_VERSION'] = '2';  
$configValues['CONFIG_DB_ENGINE'] = 'mysql';  
$configValues['CONFIG_DB_HOST'] = 'localhost';  
$configValues['CONFIG_DB_PORT'] = '3306';  
$configValues['CONFIG_DB_USER'] = 'radius';  
$configValues['CONFIG_DB_PASS'] = 'esf7913to';  
$configValues['CONFIG_DB_NAME'] = 'radius';  
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';  
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
```

Finalmente es necesario mover daloradius al directorio raíz web.

```
mv daloradius-0.9-9 /var/www/html/daloradius
```

Adicionalmente para otorgar permisos de configuración al servidor apache se puede realizar lo siguiente:

```
chown -R apache:apache /var/www/html/daloradius/library/  
daloradius.conf.php
```

4.7.3.10. Clonación del Nodo 1 (Servidor RADIUS)

Para obtener el segundo servidor paravirtualizado se va a utilizar el concepto de clonación de máquinas en XEN esto permitirá obtener un segundo servidor con las mismas características a fin de que exista la mayor exactitud en la aplicación del Clúster.

La clonación de máquinas se lo debe llevar a cabo desde el servidor principal en el cual se encuentra la dom0, para esto se debe comprobar que la máquina que va hacer clonada se encuentre deshabilitada en la dom0, una manera rápida para apagar la máquina es utilizado el comando destroy en el caso de que esta se encuentre activa.

Para poder visualizar el sistema operativo privilegiado (dom0) y todas las máquinas virtuales que se encuentran activas en el sistema XEN Hypervisor, se ejecuta el comando xm list:

```
[root@FiseiServer ~]# xm list
```

Name	ID	Mem(MiB)	VCPUs	State	Time(s)
Domain-0	0	3384	8	r-----	663089.4
Servm1	2	1024	1	-b-----	0.2
dlnalambrica	4	1024	1	-b-----	11.7
dproxy	3	2048	1	-b-----	189950.3
uoceni	1	512	1	-b-----	14740.5

Como se puede observar, el servidor Servm1 está activo, entonces se puede utilizar el siguiente comando para apagarlo de manera inmediata:

```
xm destroy Servm1
```

Se crea el volumen del disco con el mismo tamaño que la primera máquina con el nombre de la nueva máquina, en esta ocasión el nombre asignado para la nueva máquina virtual (Nodo 2) es: Servm2.

```
lvcreate -L10G dsk nServm2
```

Se copia exactamente igual el disco Servm1 al disco Servm2 para eso se utiliza la siguiente línea:

```
dd if=/dev/dsk/Servm1 of=/dev/dsk/Servm2
```

Cabe señalar que este proceso toma varios minutos. Luego de esto se muestra en pantalla la siguiente información:

```
20971520+0 records in
20971520+0 records out
10737418240 bytes (11 GB) copied , 1719,04 seconds , 6,2 MB/s
```

A continuación se copia el archivo de configuración del Servm1 al con el nombre el nuevo disco que se ha clonado.

```
cp /etc/xen/Servm1 /etc/xen/Servm2
```

Para levantar el servidor que se ha clonado se ejecuta el siguiente comando:

```
xm create Servm2
```

Ejecutando nuevamente el comando `xm list` se puede comprobar que el servidor clonado ya se encuentra activo:

```
[root@FiseiServer ~]# xm list
```

Name	ID	Mem(MiB)	VCPUs	State	Time(s)
Domain-0	0	4922	8	r-----	67504.1
Servm1	2	1024	1	-b-----	0.2
Servm2	3	1024	1	-b-----	0.2
dlnalambrica	4	1024	1	-b-----	11.7
dproxy	1	1024	1	r-----	105204.2
uoceni	5	512	1	-b-----	2459.9

Luego se edita el archivo de Servm2 en el que se configuran lo siguientes parámetros:

- name
- uuid
- disk
- vif

```
vi /etc/xen/Servm2

name = "Servm2"
uuid = "961d117b-b6f6-c631-b5aa-4af80ce0e530"
maxmem = 1024
memory = 1024
vcpus = 1
bootloader = "/usr/bin/pygrub"
on_poweroff = "destroy"
on_reboot = "restart"
on_crash = "restart"
disk = [ "phy:/dev/dsk/Servm2,xvda,w" ]
vif = [ "mac=00:16:3e:0a:4e:82,bridge=xenbr0,script=vif-bridge" ]
```

Una vez hecho esto se ingresa al Servm2 para realizar otras configuraciones en la máquina, para esto se ejecuta el siguiente comando:

```
xm console Servm2
```

Lo primero que se configura en el Servm2 es el nombre de la máquina, ya que por defecto al realizar la clonación esta viene con el nombre de la primera máquina es decir Servm1. Entonces para cambiar el nombre se edita en el siguiente directorio.

```
vi /etc/sysconfig/network

NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=Servm2
```

Configuraciones de red para el nuevo servidor clonado (Nodo 2)

Para modificar parámetros de red, se ejecuta setup.

```
setup
```

Se ingresa en Network configuration (configuración de red), como se ve en la figura 4.30.

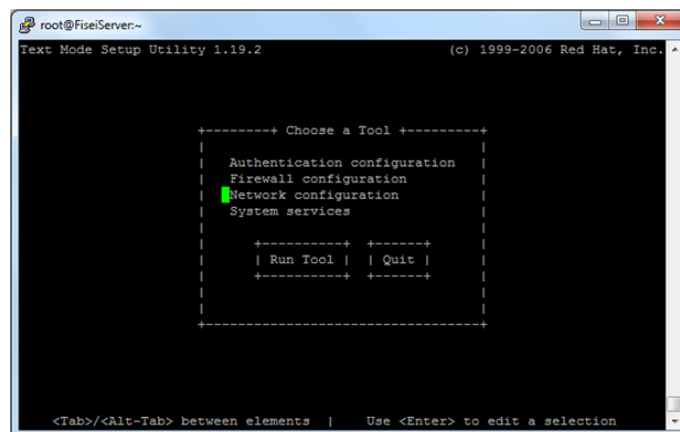


Figura 4.30: Configuración de red en Nodo2
Fuente: El Investigador

Se ingresa en Edit Devices, como se muestra en la figura 4.31.

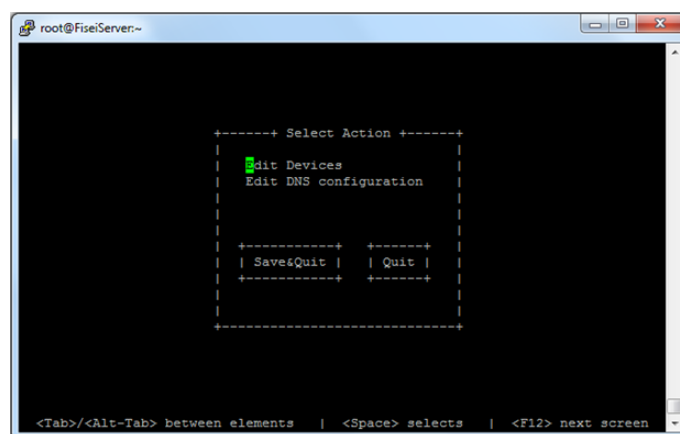


Figura 4.31: Edición para dispositivos de red en Nodo2
Fuente: El Investigador

Como se puede apreciar en la figura 4.32 al clonar el Servm1 (Nodo1), este crea en el Servm2 (Nodo2) un back up eth0.bak con los datos de la interfaz del Servm1. Lo que se hace es simplemente dejar una sola interfaz de red la cual contenga la IP del Servm2 y borrar el back up del Servm1 y luego guardar los cambios realizados.

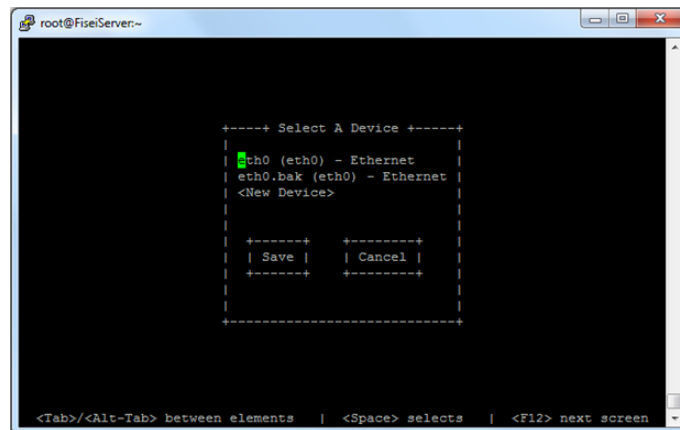


Figura 4.32: Selección de dispositivo a configurar en Nodo2
Fuente: El Investigador

Al seleccionar las configuraciones para eth0, se ingresan los respectivos valores para los campos y se guardan los cambios. La IP para el servidor de esta máquina virtual (Nodo 2) es: 192.168.124.27

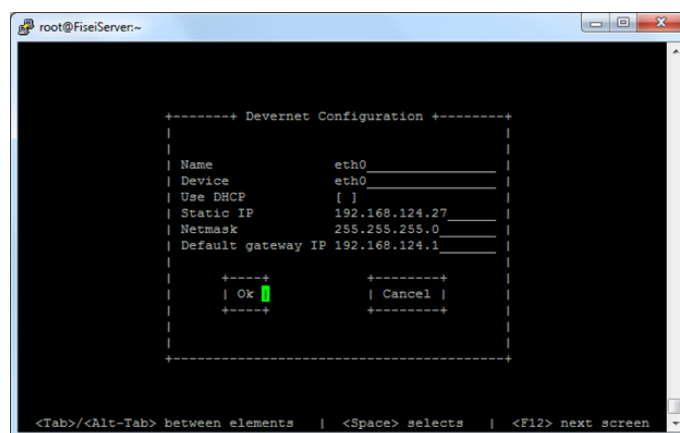


Figura 4.33: Datos de red para Nodo2
Fuente: El Investigador

Continuo a esto se reinician los servicios de red en la máquina.

```
service network restart
```

Otra configuración adicional en el Nodo 2 es colocar el nombre de la máquina (Servm2) en el archivo hosts, como se muestra en a continuación:

```
vi /etc/hosts
```

```
# Do not remove the following line , or various programs
```

```
# that require network functionality will fail.
127.0.0.1      Servm2 localhost.localhost localhost
::1           localhost6.localhost6 localhost6
```

4.7.3.11. Consideraciones antes de la Instalación del Clúster de alta disponibilidad

Algunos aspectos a tomar en cuenta para la creación de un Clúster son los siguientes:

Nodo 1	Hostname: vm07	IP address: 192.168.124.26
Nodo 2	Hostname: vm08	IP address: 192.168.124.27

Al aplicar lo siguiente:

```
uname -n
```

debe retornar: Servm1 (el nombre del nodo en el que se está ejecutando)

Se elige una dirección IP virtual. Ej: 192.168.124.29

Se configura el archivo hosts de cada nodo.

```
vi /etc/hosts
```

En este archivo se agregan las IPs de cada nodo

```
192.168.124.26    Servm1
192.168.124.27    Servm2
```

También es necesario desactivar las iptables en cada nodo.

```
service iptables stop
chkconfig iptables off
```

4.7.3.12. Instalación de Heartbeat y configuración del Clúster para el servicio HTTP

Lo primero a realizar es la descarga del paquete heartbeat, para esto se utiliza el siguiente comando:

```
yum install heartbeat
```

Continuo a esto se lleva a cabo la configuración de los siguientes archivos:

- authkeys
- ha.cf
- haresources

Antes de efectuar las configuraciones en estos archivos, se los copian al directorio: `etc/ha.d`

```
cp /usr/share/doc/heartbeat-2.1.3/authkeys /etc/ha.d/
cp /usr/share/doc/heartbeat-2.1.3/ha.cf /etc/ha.d/
cp /usr/share/doc/heartbeat-2.1.3/haresources /etc/ha.d/
```

En la configuración de `authkeys`, se utiliza la autenticación método 2 (sha1).

```
vi /etc/ha.d/authkeys
```

Aquí se añaden las siguientes líneas:

```
auth 2 2

sha1 test-ha
```

También se cambian los permisos de `authkeys`.

```
chmod 600 /etc/ha.d/authkeys
```

Configurando el archivo `ha.cf`; este es el archivo más importante en la configuración.

```
vi /etc/ha.d/ha.cf
```

Aquí se añaden las siguientes líneas:

```
logfile /var/log/ha-log
logfacility local0
keepalive 2
deadtime 30
initdead 120
bcast eth0
udpport 694
auto_failback on
node Servm1
node Servm2
```

Configurando el archivo `haresources`; este archivo contiene los servicios a los cuales se requiere dar alta disponibilidad.

```
vi /etc/ha.d/haresources
```

Aquí se añade la siguiente línea:

```
Servm1 192.168.124.29 httpd
```

Se copia el contenido del directorio /etc/ha.d/ del Nodo 1 al Nodo 2.

```
scp -r /etc/ha.d/ root@Servm2:/etc/
```

Se configura el archivo del servicio al cual se le quiere dar alta disponibilidad. En este caso es httpd.conf

```
vi /etc/httpd/conf/httpd.conf
```

Para añadir la siguiente línea:

```
Listen 192.168.124.29:80
```

Se copia este archivo al Nodo 2

```
scp /etc/httpd/conf/httpd.conf root@Servm2:/etc/httpd/conf/
```

4.7.3.13. Configuración de Clúster para el servicio RADIUS

Una vez instalado Heartbeat en cada uno de los nodos se deben realizar las siguientes configuraciones respectivas en los siguientes archivos:

- radius.conf
- clients.conf
- haresources

En el archivo radius.conf se agrega la IP address que va a escuchar, en este caso será la IP virtual que está siendo utilizada para heartbeat. Esto se lo puede aumentar en la línea 273.

```
vi /etc/raddb/radiusd.conf
```

```
ipaddr = 192.168.124.29
```

Se copia el archivo radiusd.conf del Nodo 1 al Nodo 2.

```
scp /etc/raddb/radiusd.conf root@Servm2:/etc/raddb/
```

En el archivo clients.conf se agrega un cliente con la IP virtual que se está manejando para heartbeat. Esto se lo puede añadir en la línea 205.

```
vi /etc/raddb/clients.conf

client 192.168.124.29/24 {
    secret          = ra4826us
    shortname       = Servm1
}
```

Se copia el archivo clients.conf del Nodo 1 al Nodo 2.

```
scp /etc/raddb/clients.conf root@Servm2:/etc/raddb/
```

Se debe editar el archivo haresources.

```
vi /etc/ha.d/haresources
```

Para agregar el servicio radius seguido del servicio http en la siguiente línea:

```
Servm1 192.168.124.29 httpd radiusd
```

El Nodo 2 debe tener la misma línea en el archivo haresources.

```
Servm1 192.168.124.29 httpd radiusd
```

4.7.3.14. Configuración de alta disponibilidad de datos por replicación maestro a maestro en MySQL.

Para que las bases de datos de los nodos del Clúster se encuentren actualizados permanentemente, es necesario realizar un proceso de replicación de la información a nivel de servidor maestro a maestro para que de esta forma se brinde un servicio de alta disponibilidad de datos para MySQL, en este caso los nodos deben estar sincronizados entre sí, de modo si uno cae, el otro pueda tomar el relevo y así no se pierdan los datos para el servicio de MySQL, para realizar este proceso se parte del concepto de servidor maestro-esclavo.

Algunos aspectos a tomar en cuenta para la replicación de datos en MySQL son los siguientes:

Nodo 1	Maestro 1 / Esclavo 2	IP address: 192.168.124.26
Nodo 2	Maestro 2 / Esclavo 1	IP address: 192.168.124.27

El archivo de la base de datos la cual va hacer auditada es: my.cnf

Nodo 1

(Maestro 1 a Esclavo 1)

Se edita el archivo my.cnf para configurar el Nodo 1 como maestro 1

```
vi /etc/my.cnf

log-bin
binlog-do-db=radius # entrada de la base de datos que debe
                    ser replicado
binlog-ignore-db=mysql # entrada de la base de datos que
                       debe ser ignorado
binlog-ignore-db=test

server-id=1

[mysql.server]
user=mysql
basedir=/var/lib
```

Se crea una cuenta de replicación en el esclavo 1 en MySQL.

```
mysql> grant replication slave on *.* to 'cluster'@192
      .168.124.27 identified by 'slave1';
mysql> quit;
```

Para que la configuraciones tomen efecto se debe reiniciar MySQL.

```
service mysqld restart
```

Nodo 2

(Maestro 1 a Esclavo 1)

Se edita el archivo my.cnf para configurar el Nodo 2 como esclavo 1.

```
vi /etc/my.cnf

server-id=2

master-host=192.168.124.26
master-user=cluster
```

```

master-password=slave1
master-port=3306

```

```

[mysql.server]
user=mysql
basedir=/var/lib

```

Para que las configuraciones tomen efecto se debe reiniciar MySQL.

```
service mysqld restart
```

Para verificar la cuenta se realiza lo siguiente:

```

mysql> start slave;
mysql> show slave status\G;

```

Verificando en el maestro en el Nodo 1. Se ejecuta lo siguiente:

```
mysql> show master status;
```

File	Position	Binlog_Do_DB	Binlog_Ignore_DB
mysqld-bin.000011	98	radius	

```
1 row in set (0.00 sec)
```

Nodo 2

(Maestro 2 a Esclavo 2)

Se edita el archivo my.cnf para configurar el Nodo 2 como maestro 2.

```

vi /etc/my.cnf

server-id=2

master-host=192.168.124.26

```

```

master-user=cluster
master-password=slave1
master-port=3306

log-bin          #Información para que el Nodo 2 sea Maestro
binlog-do-db=radius

[mysql.server]
user=mysql
basedir=/var/lib

```

Se crea una cuenta de replicación en el esclavo 2 en MySQL.

```

mysql> grant replication slave on *.* to 'cluster'@192
      .168.124.26 identified by 'slave2';
mysql> quit;

```

Para que las configuraciones tomen efecto se reinicia el servicio MySQL.

```

service mysqld restart

```

Nodo 1

(Maestro 2 a Esclavo 2)

Se edita el archivo my.cnf para configurar el Nodo 1 como esclavo 2.

```

vi /etc/my.cnf

log-bin
binlog-do-db=radius  #entrada de la base de datos que debe
                    ser replicado
binlog-ignore-db=mysql # entrada de la base de datos que
                    debe ser ignorado
binlog-ignore-db=test

server-id=1

master-host=192.168.124.27  #Información para que el Nodo 1
                    sea Esclavo
master-user=cluster
master-password=slave2
master-port=3306

```

```
[mysql.server]
user=mysql
basedir=/var/lib
```

Para que las configuraciones tomen efecto se reinicia el servicio MySQL.

```
service mysqld restart
```

Para verificar la cuenta se realiza lo siguiente:

```
mysql> start slave;
mysql> show slave status\G;
```

Verificando en el maestro en el Nodo 2. Se ejecuta lo siguiente:

```
mysql> show master status;
```

File	Position	Binlog_Do_DB	Binlog_Ignore_DB
mysqld-bin.000015	744089	radius	mysql, test

1 row in set (0.00 sec)

4.7.3.15. Configuración de dispositivos de red para HotSpot

Con respecto al NAS (Network Access Service) o acceso a la red, la idea en este proyecto es contar con dispositivos de acceso los cuales se encuentren configurados como HotSpot, es así que los dispositivos con los cuales se cuenta para llevar a cabo este trabajo son dos equipos router board MikroTik los cuales cuentan con 4 puestos LAN cada uno, lo que permitiría tener una escalabilidad de hasta 8 APs. Cabe señalar que los dos equipos MikroTik aun siendo de diferentes series cuentan con la misma versión en su sistema operativo que es el RouterOS v5.26, por lo tanto las configuraciones en los dos, son las mismas. Los equipos para HotSpot son el MikroTik RB450G y el RB951G-2HnD.

Cabe señalar que estos dispositivos HotSpot tienen como finalidad principal el redireccionamiento de las peticiones de autenticación de usuarios hacia el servidor Radius en donde se llevan a cabo las gestiones de acceso a la red Wi-Fi de la FISEI.

El método de seguridad que se emplea para llevar a cabo el proceso de autenticación es mediante hashing, el mismo toma efecto en los routers MikroTik, entonces cuando llegan datos de usuario a los HotSpot, a estos se les genera un hash, a su vez este hash es comparado con el hash generado por el radius client de los HotSpot, por tanto si el hash del radius y el hash de información de usuario ingresado es el mismo, este se autentica.

Las configuraciones de HotSpot se detallan a continuación:

Se ingresa al Sistema operativo del MikroTik, este proceso se lo puede hacer via web o mediante la aplicación winbox la cual se la puede descargar libremente desde la página oficial de MikroTik. Para realizar configuraciones avanzadas como puede ser un HotSpot es aconsejable realizar las configuraciones vía winbox.

Una vez ya en el sistema operativo del dispositivo, se eliminan todas las configuraciones existentes dentro de:

DHCP Client: (Clic: IP → DHCP Client)

DHCP Server: (Clic: IP → DHCP Server)

Pool: (Clic: IP → Pool)

Bridge: (Clic: Bridge)

Addresses: (Clic: IP → Addresses)

Se configuran las direcciones IP de WAN y LAN haciendo clic en la pestaña IP → Addresses, como se muestra en la figura 4.34.

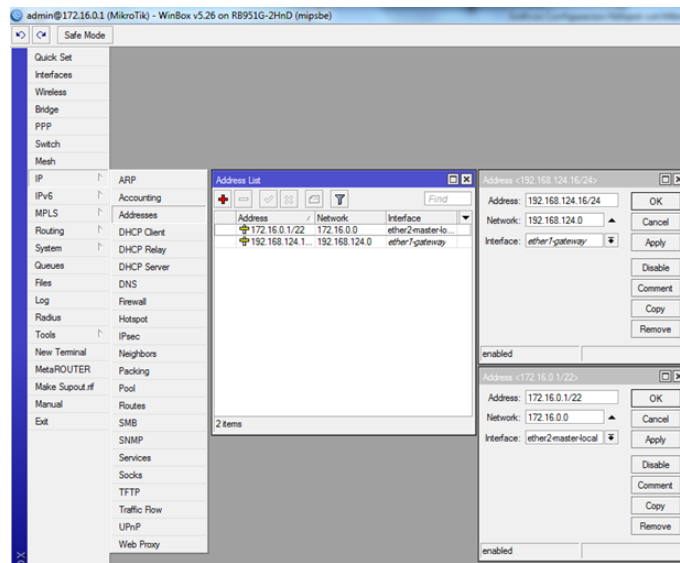


Figura 4.34: Configuración de IP's para WAN y LAN para HotSpot
Fuente: El Investigador

Se ingresa el DNS respectivo de la red dando clic en IP → DNS, como se muestra en la figura 4.35.

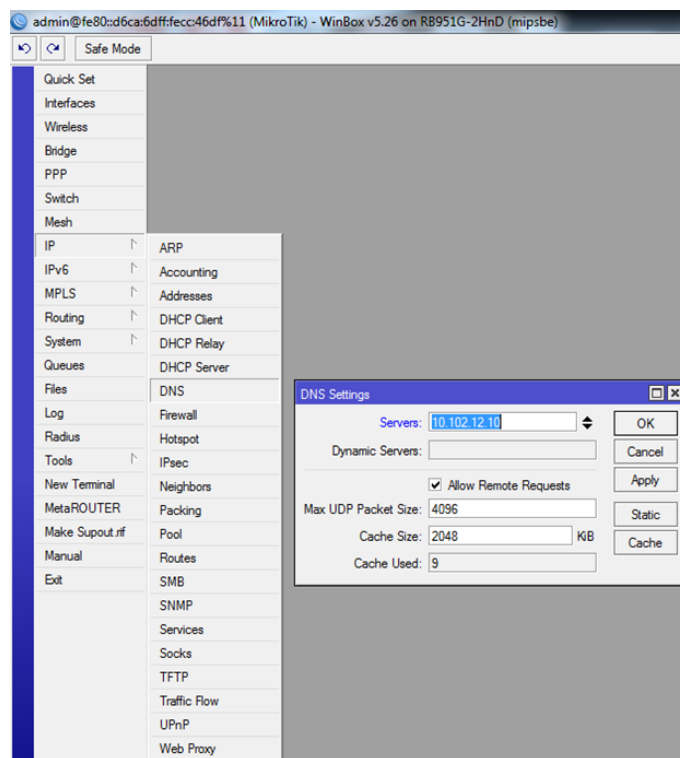


Figura 4.35: Configuración DNS para HotSpot
Fuente: El Investigador

Se da clic en IP → Routes como se ve en la figura 4.36, en donde se ingresa solamente

el Gateway de la red, para realizar esto primero se da clic en el botón con signo + de color rojo.

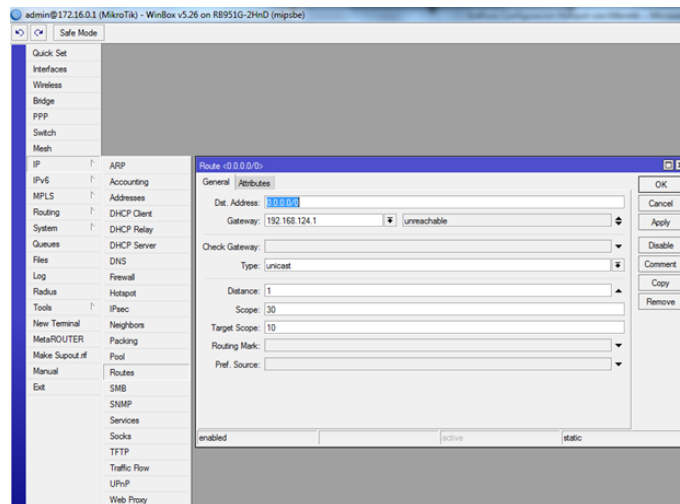


Figura 4.36: Ventana de configuración para dirección Gateway de la red
Fuente: El Investigador

En la figura 4.37 se muestra la ventana que aparece luego de dar OK en la configuración del Gateway.

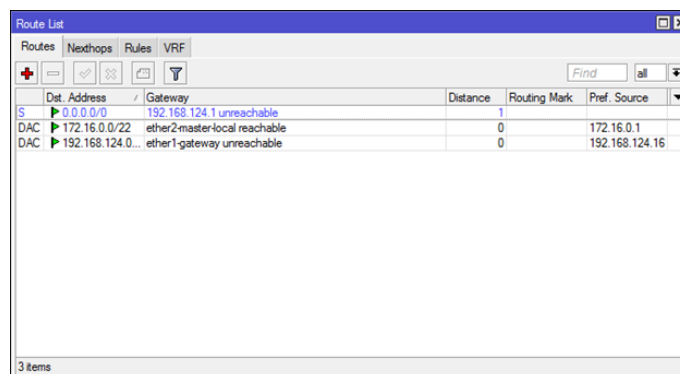


Figura 4.37: Visualización de configuraciones de Route
Fuente: El Investigador

A continuación se configura el HotSpot, para lo cual se debe ingresar en la pestaña IP → Hotspot, después de debe dar clic en el botón Hotspot Setup para realizar las configuraciones respectivas.

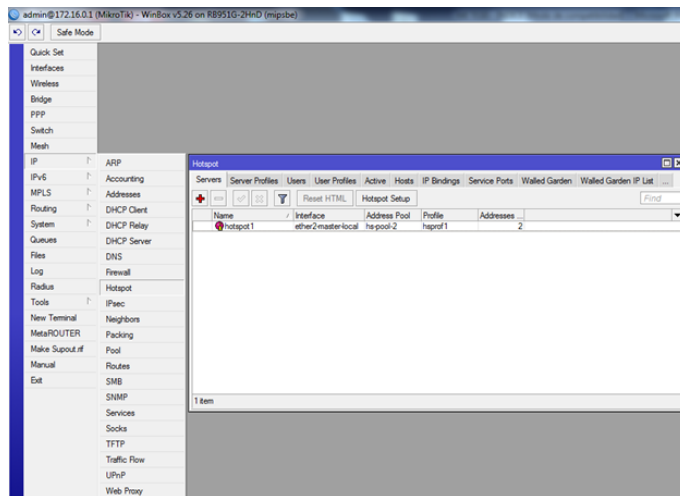


Figura 4.38: Ingreso a configuración de HotSpot
Fuente: El Investigador

Seguido a esto se especifica la interfaz para NAS de los usuarios, por lo general en este punto se elige la interfaz ether2 del Mikrotik la cual representa un bridge con las demás interfaces de LAN.

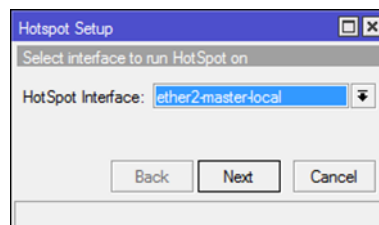


Figura 4.39: Interfaz de HotSpot
Fuente: El Investigador

Se especifica la dirección de red local para la Interfaz del HotSpot.

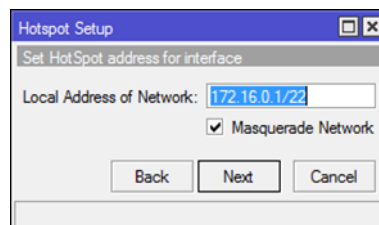


Figura 4.40: Interfaz de HotSpot Dirección de red LAN para HotSpot
Fuente: El Investigador

Se define el pool o rango de direcciones de red LAN para el HotSpot.

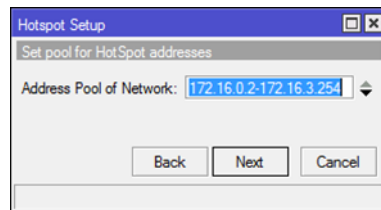


Figura 4.41: Pool de direcciones de red de HotSpot
Fuente: El Investigador

En la siguiente ventana al momento sólo se debe elegir none, puesto que no se cuenta con un certificado SSL.

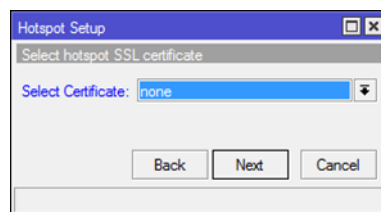


Figura 4.42: Certificación SSL en none para HotSpot
Fuente: El Investigador

En la ventana a continuación se deja la configuración tal como está, es decir : 0.0.0.0, ya que no se cuenta con un servidor SMTP.

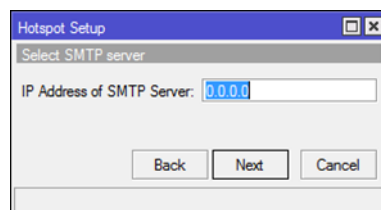


Figura 4.43: Servidor SMPT de HotSpot
Fuente: El Investigador

A continuación se especifica el DNS el cual se configuró anteriormente.

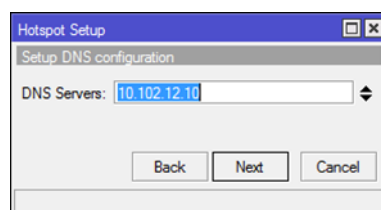


Figura 4.44: Configuración servidor DNS de HotSpot
Fuente: El Investigador

Finalmente en la siguiente ventana se coloca el nombre de DNS para la red de HotSpot, en este punto cabe señalar que al momento de poner en función el HotSpot cuando se requiere ingresar a alguna página web se realiza la redirección a la página del servidor HotSpot local.

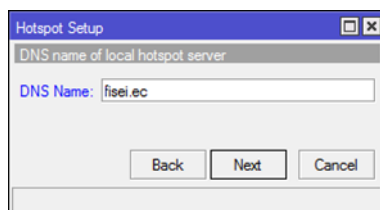


Figura 4.45: Nombre DNS de HotSpot
Fuente: El Investigador

Una vez creado el HotSpot es necesario dirigirse hacia la pestaña Server Profiles y dar doble clic en el HotSpot creado, este aparecerá con el nombre de hspof1, luego se realizan las configuraciones detalladas en la pestaña General como se ve en la figura 4.46.

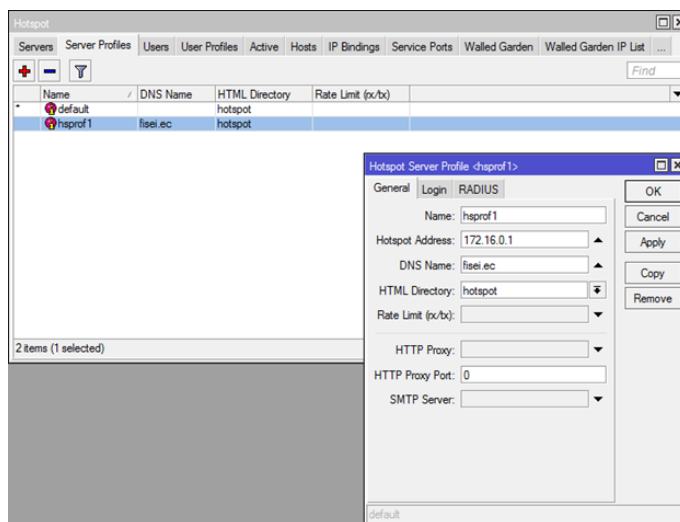


Figura 4.46: Configuración general de hspof1
Fuente: El Investigador

También en la pestaña Login se especifican las configuraciones detalladas en la figura 4.47.

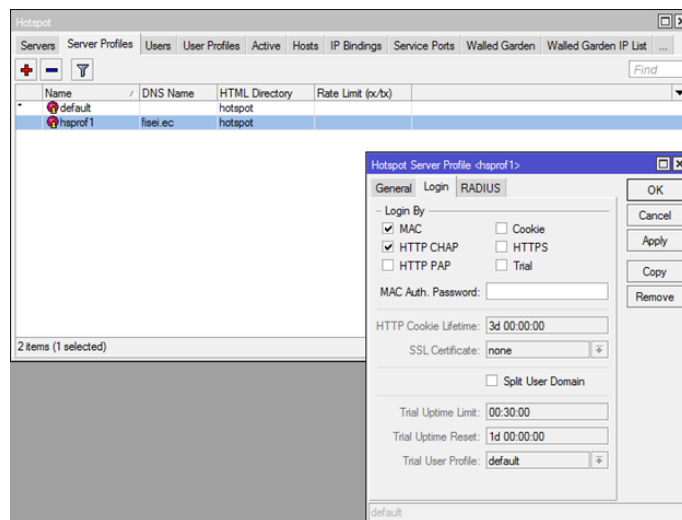


Figura 4.47: Configuración de Login en hsprof1
Fuente: El Investigador

En la pestaña RADIUS se señala: Use RADIUS, especificando la utilización del servidor RADIUS con el HotSpot, como se ve en la figura 4.48.

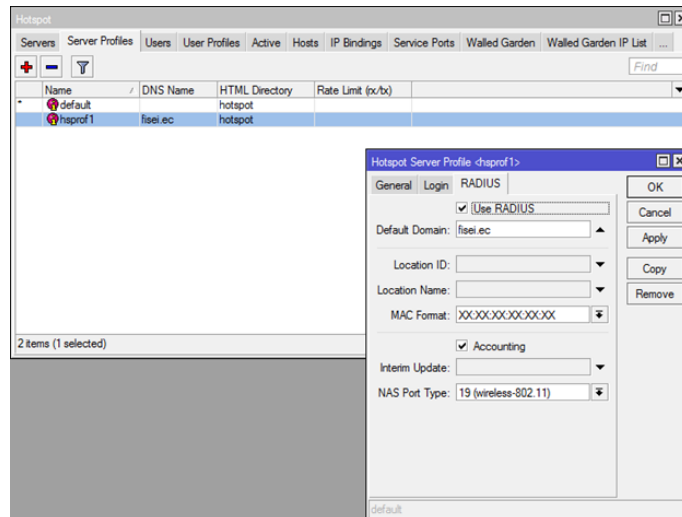


Figura 4.48: Configuración de RADIUS en hsprof1
Fuente: El Investigador

Por último se da clic en la pestaña Radius del menú de inicio, aquí se da clic en el botón con el signo + de color rojo para especificar las configuraciones de conexión con el servidor RADIUS. Esto se lo detalla en la figura 4.49.

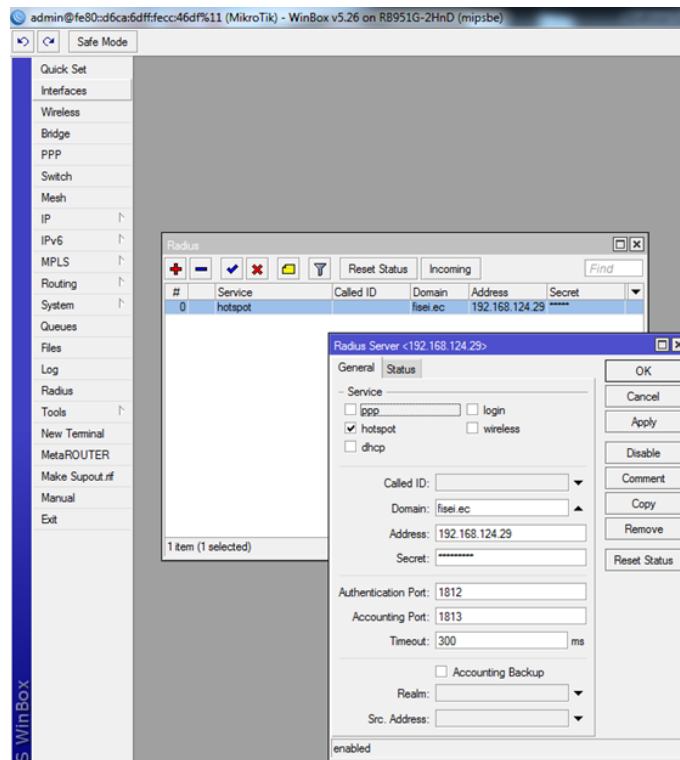


Figura 4.49: Configuraciones RADIUS para HotSpot
Fuente: El Investigador

Una vez realizado este proceso se puede comprobar el funcionamiento del HotSpot en el navegador. Para verificar esto tan solo basta con tratar de ingresar a alguna página de internet, en ese momento inmediatamente se pedirá el logueo para la autenticación de usuario. Esto se lo puede ver en la figura 4.50.



Figura 4.50: Logueo de inicio en HotSpot
Fuente: El Investigador

Configuraciones de rediseño de homepage para logueo en el HotSpot

Como se puede ver en esta figura anterior, la imagen del logueo con HotSpot, viene por defecto en las configuraciones del equipo, y por lo mismo se ve la necesidad de crear un propio homepage de logueo el cual contenga un diseño adecuado referente a la FISEI y además se puedan visualizar las diferentes políticas de utilización de la red Wi-Fi para los usuarios.

Para este punto se puede utilizar el programa Filezilla Client que es un cliente FTP multiplataforma de código abierto y software libre, licenciado bajo la Licencia Pública General de GNU. Soporta los protocolos FTP, SFTP y FTP sobre SSL/TLS (FTPS). Inicialmente fue diseñado para funcionar en Microsoft Windows, pero desde la versión 3.0.0, gracias al uso de wxWidgets, es multiplataforma, estando disponible además para otros sistemas operativos, entre ellos GNU/Linux, FreeBSD y Mac OS X [31].

Con la utilidad de este software se puede extraer el archivo de configuración de HotSpot del MikroTik y por ende configurarlo de acuerdo a las necesidades propias, en este caso lo que se pretende es poder rediseñar el homepage de inicio de logueo para HotSpot. Para llevar a efecto lo mismo y una vez corriendo la aplicación Filezilla se debe realizar la conexión con el dispositivo MikroTik, esto se lo puede lograr introduciendo el Host, Username, Password, y el Port del dispositivo, una vez efectuada la conexión correcta se debe situar en la carpeta hotspot del MikroTik para extraerla como se puede ver en la figura 4.51.

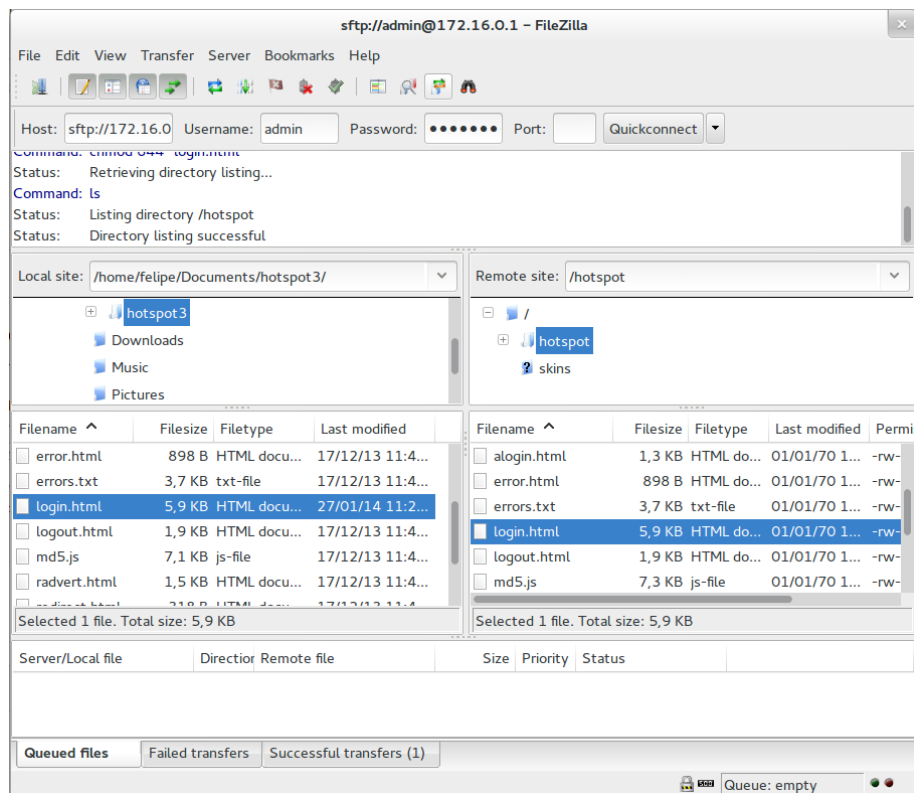


Figura 4.51: Conexión FTP-Mikrotik utilizando Filezilla
Fuente: El Investigador

Una vez obtenida la carpeta hotspot del MikroTik es posible realizar cualquier configuración en el archivo login.html contenido en esta carpeta, este archivo es el cual contiene las líneas de código con las cuales está configurado el hompage que viene por defecto para HotSpot del MikroTik.

Además dentro de la carpeta hotspot existe otra carpeta con el nombre img en la cual se debe ingresar cualquier imagen que se quiera utilizar en las configuraciones de homepage para el logue en el HotSpot del MikroTik.

Cabe señalar que este proceso es el mismo para los dos MikroTik's que se están utilizando ya que como se conoce los dos tienen la misma versión en su sistema operativo.

Codificación en Brackets para el diseño del homepage

Para efectuar estas configuraciones se puede utilizar diferentes software de programación para HTML5 y JavaScript que son los lenguajes con los cuales se encuentra codificado el HotSpot de MikroTik. Para este caso se está utilizando el software Brackets que es un editor de código útil para HTML, CSS y JavaScript está

también escrito con HTML, CSS y JavaScript por lo que al tratarse de un proyecto de código abierto aquellos usuarios con mayores conocimientos pueden crear plugins a fin de personalizar el editor a sus necesidades.

Cabe señalar que en la programación realizada para personalizar un propio homepage para el HotSpot solo se deben modificar u agregar líneas las cuales permitan rediseñar la visualización de la página de logueo, ya que en las líneas de código que vienen por defecto en el HotSpot de MikroTik también contienen las configuraciones de funcionamiento. En el siguiente código se puede apreciar las líneas que se han agregado las mismas que se especifican mediante el texto “mis configuraciones” las configuraciones personalizadas. La programación realizada para una visualización personalizada en el HotSpot es la siguiente:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>FISEI</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="pragma" content="no-cache" />
<meta http-equiv="expires" content="-1" />
<style type="text/css">
body {
    color: #737373; font-size: 10px; font-family: verdana;
    background-image: url(img/bur.jpg); background-attachment: fixed;
        background-repeat: no-repeat; background-position: center;
        background-color: transparent;}

textarea, input, select {
background-color: #FDFBFB;
border: 1px solid #BBBBBB;
padding: 2px; margin: 1px;
font-size: 14px;
color: #808080;
}
a, a:link, a:visited, a:active { color: #AAAAAA; text-decoration: none;
    font-size: 10px; }
a:hover { border-bottom: 1px dotted #c1c1c1; color: #AAAAAA; }
img { border: none;}
td { font-size: 14px; color: #7A7A7A; }
</style>

</head>

<!-- mis codificaciones -->

<body>
    <h1><font style="color:# ffffff; font-size:40px;"><p style="text-align:center;">Facultad de Ingeniería en Sistemas Electrónica e
        Industrial</p></font></h1>
</body>
```

```

<!-- mis codificaciones -->

<body>
$( if chap-id )
    <form name="sendin" action="$(link-login-only)" method="post">
        <input type="hidden" name="username" />
        <input type="hidden" name="password" />
        <input type="hidden" name="dst" value="$(link-orig)" />
        <input type="hidden" name="popup" value="true" />
    </form>

    <script type="text/javascript" src="/md5.js"></script>
    <script type="text/javascript">
    <!--
    function doLogin() {
        document.sendin.username.value = document.login.username.value;
        document.sendin.password.value = hexMD5('$(chap-id)' + document.
            login.password.value + '$(chap-challenge)');
        document.sendin.submit();
        return false;
    }
    //-->
    </script>
$(endif)

<!-- código original

<div align="center">
<a href="$(link-login-only)?target=lv&dst=$(link-orig-esc)">Latviski
    </a>
</div>

código original -->

<table width="95%" style="margin-left:20px; margin-top: 0%;">
    <tr>

<!-- mis codificaciones -->

        <td width="33%" align="center" valign="middle" style="font-size
            :16px;">
        <p style="text-align:justify;"><em><font style="color:#ffffff;">
            Con la finalidad de ofrecer un mejor servicio en el uso de
            la red Wi-Fi dentro de la FISEI se han realizado las
            siguientes políticas con respecto al uso del ancho de
            banda.<br/>
            <ul style="text-align:justify;">
            <li type="disc">Los usuarios invitados cuentan con un
                máximo de bajada y subida de: <B>512 Kbps simétrico con
                compartición 8 a 1</B></li>
            <li type="disc">Los estudiantes de la FISEI cuentan con un
                máximo de bajada y subida de:<B> 1 Mbps simétrico con
                compartición 8 a 1</B></li>
            <li type="disc">Los profesores y administrativos cuentan
                con un máximo de bajada y subida de:<B> 1,5Mbps
                simétrico con compartición 10 a 1</B></li>
            </ul>

```

```

        <p style="text-align: justify;">Para poder autenticarte y
        obtener tu rango de subida y bajada puedes dirigirte al
        Departamento de Redes y Sistemas y registrar la MAC de
        tu equipo.</p>
    </font>
</em></p>
</td>

<!-- mis codificaciones -->

<td width="33%" align="center" valign="middle">
<div class="notice" style="color: #ffffff; font-size: 14px"><!-- Por
favor, inicie sesión para acceder a internet --><br />$(if trial ==
'yes') Free trial available, <a style="color: #FF8080" href="$(link-
login-only)?dst=$(link-orig-esc)&username=T-$(mac-esc)">click
here</a>.$(endda if)</div><br />
<table width="280" height="280" style="border: 1px solid #cccccc;
padding: 0px;" cellpadding="0" cellspacing="0">
<tr>

<td align="center" valign="bottom" height="150" colspan="2">
    <p style="text-align: center; color: #ffffff;">Por favor, inicie sesión
    para acceder a internet</p>
    <form name="login" action="$(link-login-only)" method="post"
        $(if chap-id) onSubmit="return doLogin()" $(endif)>
        <input type="hidden" name="dst" value="$(link-orig)" />
        <input type="hidden" name="popup" value="true" />

        <table width="100" style="background-color: #ffffff">
            <tr><td align="right">login</td>
            <td><input style="width: 80px" name="username" type="text"
                value="$(username)" /></td>
            </tr>
            <tr><td align="right">password</td>
            <td><input style="width: 80px" name="password" type="
                password" /></td>
            </tr>
            <tr><td>&nbsp;</td>
            <td><input type="submit" value="OK" /></td>
            </tr>
        </table>
    </form>
</td>
</tr>

        <tr><td align="center"><a href="http://fisei.uta.edu.ec"
            target="_blank" style="border: none;"></a></td></tr>
        </table>

    <br /><div style="color: #ffffff; font-size: 14px">Departamento
    de Redes y Sistemas</div>
    $(if error)<br /><div style="color: #FF8080; font-size: 9px">$(
    error)</div>$(endif)
</td>

<!-- mis codificaciones -->

```

```

<td width="33%" align="center" valign="middle">
  <em><font style="color:#ffffff; font-size:16px;">
    <p style="text-align:justify;">
      El usuario invitado es una cuenta que permite a cualquier
      persona que no pertenece a la FISEI utilizar internet
      libremente, a continuación se provee de dichas
      credenciales.<br/><br/><B>Usuario:</B> &nbsp; invitado<br
      /><br/><B>Password:</B> invitado</p>
      <p style="text-align:justify;">
        <!--<B>Nota:</B><br/></p> -->

    </font></em>
  </td>

<!-- mis codificaciones -->

</tr>
</table>
<script type="text/javascript">
<!--
  document.login.username.focus();
//--> </script>
</body>
</html>

```

De acuerdo a las diferentes modificaciones para el homepage de inicio para el HotSpot, la visualización ahora se la tiene de la siguiente manera:



Figura 4.52: Homepage de inicio personalizado para HotSpot

Fuente: El Investigador

4.7.3.16. Políticas de acceso para el servicio de Autenticación de la red Wi-Fi de la FISEI.

Con finalidad de obtener un servicio eficiente y disponible de forma continua en la autenticación de ingreso a la red Wi-Fi de la FISEI y a su vez siendo congruentes

con las políticas que el CEAACES requiere en las universidades, se ve la necesidad de crear 3 tipos de usuarios:

- El Usuario Invitado: Es el usuarios el cual tiene acceso a la Red Wi-Fi con un usuario y contraseña común, proporcionado en la misma página de inicio (homepage) y de autenticación para el ingreso a la red inalámbrica de la FISEI. Es decir este usuario puede ser cualquier estudiante de la universidad el cual pueda ingresar a la red Wi-Fi sin ningún problema.
- Estudiantes: Los estudiantes de la FISEI, cuentan con un registro de autenticación por MAC valido para PCs portátiles.
- Profesores y Administrativos: Cuentan con un ingreso de autenticación por usuario y contraseña asignados de forma individual.

4.7.3.17. Directivas QoS en base a las políticas de uso de la red Wi-Fi de la FISEI.

Tomando en cuenta el valor del ancho de banda mínimo requerido para una navegación aceptable de los usuarios de la red Wi-Fi de la FISEI y de acuerdo con las políticas efectuadas para el servicio de autenticación, en las siguientes tablas se especifican las directivas QoS en base a valores máximos y mínimos de distribución de ancho de banda dinámico los cuales se asignan a los usuarios ubicados en los tres perfiles respectivamente, todo esto en función de la utilización de la red con congestión y sin congestión de tráfico.

- Usuario Invitado

El usuario invitado cuenta con una asignación de Ancho de Banda especificados en la tabla 4.11 con compartición 8 a 1.

Tabla 4.11: Dinámica de AB - Usuario Invitado

Usuario Invitado (con congestión de tráfico)	
AB min up (subida)	128 Kbps
AB min down (bajada)	128 Kbps
Usuario Invitado (sin congestión de tráfico)	
AB max up (subida)	512 Kbps
AB max down (bajada)	512 Kbps

Fuente: El Investigador

- Estudiantes

Los estudiantes cuentan con la asignación de Ancho de Banda especificados en la tabla 4.12 con compartición 8 a 1

Tabla 4.12: Dinámica de AB - Estudiantes

Estudiantes (con congestión de tráfico)	
AB min up (subida)	128 Kbps
AB min down (bajada)	128Kbps
Estudiantes (sin congestión de tráfico)	
AB max up (subida)	1.0 Mbps
AB max down (bajada)	1.0 Mbps

Fuente: El Investigador

- Profesores y Administrativos

Los estudiantes cuentan con la asignación de Ancho de Banda especificados en la tabla 4.13 con compartición 10 a 1.

Tabla 4.13: Dinámica de AB – Profesores y administrativos

Profesores y administrativos (con congestión de tráfico)	
AB min up (subida)	128 Kbps
AB min down (bajada)	128 Kbps
Profesores y administrativos (sin congestión de tráfico)	
AB max up (subida)	1.5 Mbps
AB max down (bajada)	1.5 Mbps

Fuente: El Investigador

4.7.3.18. Configuración de directivas QoS en DaloRADIUS

De acuerdo a las directivas QoS determinadas para los tres grupos, se lleva a efecto la configuración de perfiles en el administrador web de RADIUS, es decir en DaloRADIUS, para se realiza lo siguiente:

Primero se ingresar en el navegador web la dirección donde se encuentra instalado en servidor RADIUS en este caso al ya contar el Clúster se debe ingresar la dirección de la IP virtual con la cual se está trabajando en Heartbeat, para este caso esta dirección es la 192.168.124.29. Entonces se escribe lo siguiente en el navegador: 192.168.124.29/daloradius, y enter.

Inmediatamente aparecerá la página de logueo en DaloRADIUS, seguido a esto se ingresa el admin y el password respectivos. Una vez ingresado al administrador web

se da clic en la pestaña Management y luego clic en New Profile, para la configuración de los respectivos perfiles. Cabe recalcar que para este proyecto se cuentan con tres perfiles: Invitado, Estudiantes, Docentes y administrativos. Luego se pone el nombre correspondiente del perfil. Además debajo del nombre se tienen dos secciones para la asignación de atributos para los perfiles. En la primera sección “Locate Attribute via Vendor/Attribute”, se escoge el atributo WISPr dando clic en la pestaña de Vendor como se puede ver en la figura 4.53, aquí se selecciona una por una las opciones de Bandwidth dando clic en Add Attribute; una vez seleccionadas todas se realizan las respectivas asignaciones de ancho de banda. Este proceso se lo realiza para los tres perfiles.

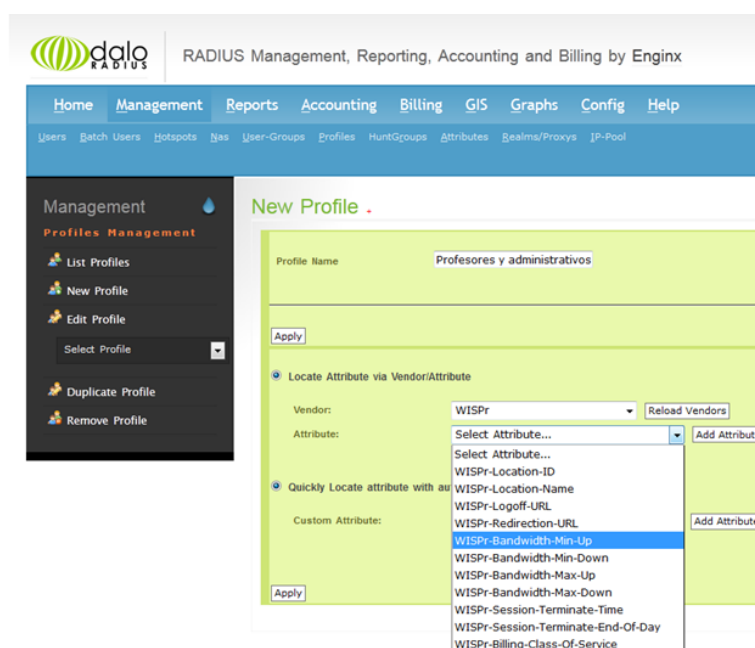


Figura 4.53: Configuración de perfiles en DaloRADIUS - primera sección
Fuente: El Investigador

Cabe tener cuenta que al crear el perfil del usuario invitado y de Profesores y administrativos es necesario crear el atributo Idle-Timeout que se encuentra en la segunda sección “Quickly Locate Attribute with autocomplete input”, seguido a esto se da clic en el botón Add Attribute como se muestra en la figura 4.54, con la finalidad de que si el usuario no se encuentra utilizando o navegando en la red, se le descarte el logueo de su máquina y así se pueda liberar espacio en red para el ingreso y navegación de otros usuarios. Cabe señalar que el usuario invitado tiene un tiempo de 10 min (600 seg.). Los Profesores y administrativos tienen un tiempo de 15 min (900 seg.)

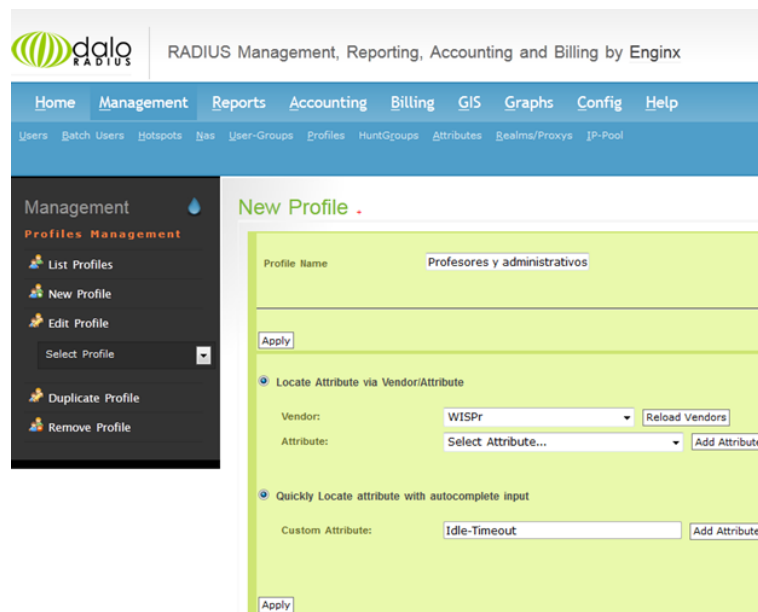


Figura 4.54: Configuración de perfiles en DaloRADIUS - segunda sección
Fuente: El Investigador

Una vez configurado los perfiles para los usuarios de los grupos respectivamente, estos deben ser asignados a las cuentas de los usuarios ya sean por registro MAC o por usuario y contraseña.

DaloRADIUS permite tres tipos de autenticación que son:

- Username Authentication: Autenticación con usuario y contraseña.
- MAC Address Authentication: Autenticación por MAC.
- Ping Code Authentication: Autenticación por código ping.

Para este caso como ya se conoce solo se requieren de los dos primeros tipos de autenticación. Para realizar el proceso de registro de usuarios se va a la pestaña Management luego se elige la opción Users y en el menú de la parte izquierda se elige la opción New User, continuo a esto se elige el tipo de registro para usuarios y a la vez se coloca en Group el tipo de perfil de grupo. Además se tienen las demás pestañas para colocar la información personal de usuarios u otros atributos, como se puede ver en la figura 4.55.

Figura 4.55: Adición de usuarios en DaloRADIUS
Fuente: El Investigador

4.8. Discusión y Resultados de la Propuesta

Como ya se tiene en conocimiento, la propuesta del presente proyecto trata sobre la implementación de un Clúster para brindar alta disponibilidad de manera eficiente e ininterrumpida al servidor de autenticación de la red WI-FI en beneficio de los usuarios de la FISEI.

Dicho esto y una vez implementado de manera total el Clúster de alta disponibilidad sobre una plataforma virtual, el siguiente paso consiste en verificar que todos los componentes dentro del Clúster se encuentren en funcionamiento de manera correcta, tanto en la disponibilidad de servicios como en la replicación de datos correspondientes al servidor de autenticación de la red Wi-Fi de la FISEI. La verificación del funcionamiento integral de Clúster permite a su vez obtener los resultados para poder elevar criterios técnicos consecuentes a los mismos.

4.8.1. Pruebas de alta disponibilidad de servicios

Como ya se conoce, la aplicación la cual permitió dar alta disponibilidad para servicios fue Heartbeat. De acuerdo a la figura 4.28 los servicios los cuales se encuentran configurados para dar alta disponibilidad entre el Nodo1 y el Nodo2 son: HTTP y RADIUS. Por lo tanto al tener los dos servidores encendidos se puede

verificar el funcionamiento de Heartbeat con el cual se genera la IP virtual del Clúster la misma que permite la comunicación con el exterior, según la figura 4.56 esta IP virtual se encuentra en función desde el Nodo1 que es el Nodo Activo y en el todos los servicios de alta disponibilidad.

```

root@Serv1~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:81
          inet addr:192.168.124.26  Bcast:192.168.124.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe0a:4e81/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:718746 errors:0 dropped:0 overruns:0 frame:0
          TX packets:474302 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:168172790 (160.3 MiB)  TX bytes:122799802 (117.1 MiB)

eth0:0    Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:81
          inet addr:192.168.124.29  Bcast:192.168.124.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4292 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4292 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:309481 (302.2 KiB)  TX bytes:309481 (302.2 KiB)

root@Serv1~#

root@Serv2~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:82
          inet addr:192.168.124.27  Bcast:192.168.124.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe0a:4e82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:556463 errors:0 dropped:0 overruns:0 frame:0
          TX packets:399102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:138399795 (131.9 MiB)  TX bytes:94875464 (90.4 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4281 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:307181 (299.9 KiB)  TX bytes:307181 (299.9 KiB)

root@Serv2~#

```

Figura 4.56: Heartbeat - Nodo1
Fuente: El Investigador

Dado el caso en el que al Nodo1 se lo dé de baja o requiera mantenimiento, el Nodo2 debe entrar en función levantando los servicios de alta disponibilidad en función de la IP virtual del Clúster. Cabe señalar que el efecto es el mismo al simplemente detener el servicio heartbeat. Esto se lo puede apreciar en la figura 4.57.

```

root@Serv1~# service heartbeat stop
Stopping High-Availability services: [ OK ]

root@Serv1~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:81
          inet addr:192.168.124.26  Bcast:192.168.124.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe0a:4e81/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:768569 errors:0 dropped:0 overruns:0 frame:0
          TX packets:515391 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:179716892 (171.3 MiB)  TX bytes:132639156 (126.4 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4699 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:339527 (331.5 KiB)  TX bytes:339527 (331.5 KiB)

root@Serv1~#

root@Serv2~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:82
          inet addr:192.168.124.27  Bcast:192.168.124.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe0a:4e82/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:594223 errors:0 dropped:0 overruns:0 frame:0
          TX packets:434831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:147654655 (140.8 MiB)  TX bytes:103598330 (98.7 MiB)

eth0:0    Link encap:Ethernet  HWaddr 00:16:3E:0A:4E:82
          inet addr:192.168.124.29  Bcast:192.168.124.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4684 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4684 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:336673 (328.7 KiB)  TX bytes:336673 (328.7 KiB)

root@Serv2~#

```

Figura 4.57: Heartbeat - Nodo2
Fuente: El Investigador

En la tabla 4.13 se pueden observar los escenarios de pruebas y resultados en el proceso de alta disponibilidad de servicios entre el Nodo1 y el Nodo2 de acuerdo a la configuración con el modelo Activo - Pasivo, de ello se puede observar que la utilización de la aplicación Heartbeat para el Clúster de alta disponibilidad ha tenido una adecuada compatibilidad con los nodos que representan el Servidor RADIUS.

Tabla 4.14: Escenario de pruebas – disponibilidad de servicios

Estado de los nodos del Clúster	IP virtual	Servicios de alta disponibilidad	Tiempo Failover	Resultado de prueba
Nodo1 = ON Nodo2 = ON / OFF	Nodo1: 192.168.124.29	Nodo1: HTTP - RADIUS	< 1seg	OK
Nodo1 = OFF Nodo2 = ON	Nodo2: 192.168.124.29	Nodo2: HTTP - RADIUS	< 1seg	OK

Fuente: El Investigador

4.8.2. Pruebas de alta disponibilidad de datos

Como ya se conoce, la alta disponibilidad de datos se lo llevó a cabo mediante la replicación de datos en MySQL. De la misma forma que en la disponibilidad de servicios se puede realizar una verificación del funcionamiento correcto de la replicación de datos en los dos Nodos con los cuales se está trabajando. Esta verificación se lo puede apreciar en la figura 4.58, y para llevar a efecto este proceso, se está contando con una replicación Maestro a Maestro. Para comprender de manera sencilla este concepto, simplemente se puede decir que en cualquier nodo del Clúster en el cual se esté llevando a cabo la prestación de servicios o ingresando los datos, por ejemplo el Nodo1, este replica de manera automática sus datos en el Nodo2 y viceversa, en el caso de que solamente un Nodo se encuentre en funcionamiento y en este se estén ingresando los datos, el momento en el que se enciende el otro nodo, inmediatamente toma en efecto la replicación sin demora.

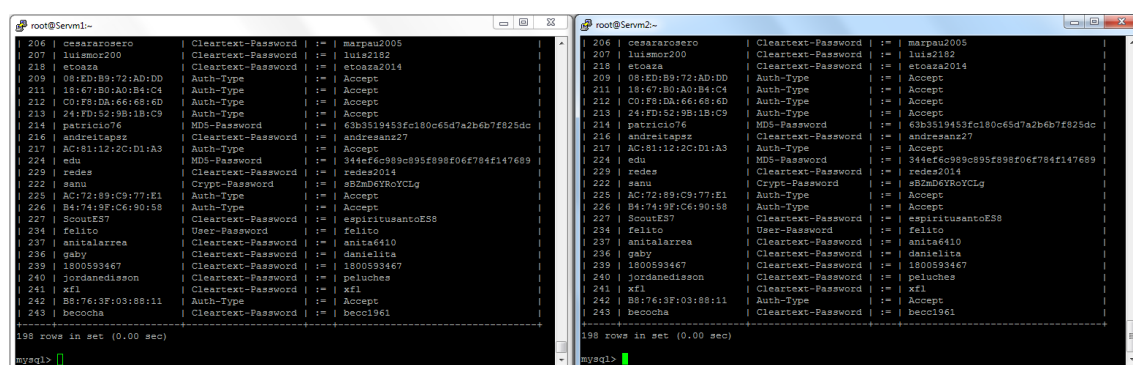


Figura 4.58: Replicación de datos en los dos nodos virtuales

Fuente: El Investigador

En cuanto a la verificación de la replicación conociendo que en determinados momentos cualquiera de los dos servidores puede ser el maestro y el otro el esclavo o viceversa, de esta forma para conocer los tiempos de replicación entre nodos se

necesita conocer el patrón de consultas y determinar empíricamente con pruebas la relación entre las lecturas (lecturas por segundo, o `max_reads`) y las escrituras (`max_writes`) en un típico maestro y típico esclavo.

Al tener en cuenta que la replicación entre servidores está dada por un enlace punto a punto y que estas replicaciones de datos vienen dadas a grandes velocidades, de acuerdo a pruebas comprobadas que se han realizado para este tipo de configuraciones en cuanto a los tiempos de replicación de datos entre servidores, se tiene lo siguiente [32]:

Si $N = 0$ (que significa que no se tiene replicación), el sistema puede tratar unas $1200/11 = 109$ escrituras por segundo.

Si $N = 1$, se tienen 184 escrituras por segundo.

Si $N = 8$, se tienen 400 escrituras por segundo.

Si $N = 17$, se tienen 480 escrituras por segundo.

Donde N es el número de servidores o nodos esclavos.

Eventualmente, mientras N se aproxima al infinito (y el presupuesto va en aumento), se puede llegar a cerca de 600 escrituras por segundo, incrementando el rendimiento del sistema 5.5 veces. Sin embargo, con sólo ocho servidores, se incrementa cerca de cuatro veces.

En la tabla 4.14 se pueden observar los escenarios de pruebas y resultados en el proceso de replicación de datos entre el Nodo1 y el Nodo2 de acuerdo a la configuración de replicación maestro a maestro.

Tabla 4.15: Escenario de pruebas – disponibilidad de datos

Estado de los nodos del Clúster	Replicación de datos	Tiempo - Replicación	Resultado de Replicación
Nodo1 = Maestro Nodo2 = Esclavo	Replicación: Nodo1 en Nodo2	< 1seg por cada escritura	OK
Nodo1 = Esclavo Nodo2 = Maestro	Replicación: Nodo2 en Nodo1	< 1seg por cada escritura	OK
Nodo1 = Maestro Nodo2 = OFF	Replicación: Nodo1 en Nodo2 si Nodo2 = ON	184 escrituras por segundo	OK
Nodo1 = OFF Nodo2 = Maestro	Replicación: Nodo2 en Nodo1 si Nodo1 = ON	184 escrituras por segundo	OK

Fuente: El Investigador

4.8.3. Visualización de monitoreo del tráfico de red en Cacti

Teniendo presente que previa la instalación del Clúster de alta disponibilidad se implementó un servidor virtual para efectuar el monitoreo del tráfico en red Wi-Fi de la FISEI mediante el software Cacti, el servicio de monitoreo con el Clúster ya implementado se aplica a los HotSpots que son los dispositivos de acceso a la red inalámbrica de la Facultad. En la figura 4.59 se puede ver el tráfico generado en los HotSpot MikroTik 951G-2nD el día 21 de Enero, 2014. MikroTik 450G el día 24 de Enero, 2014.

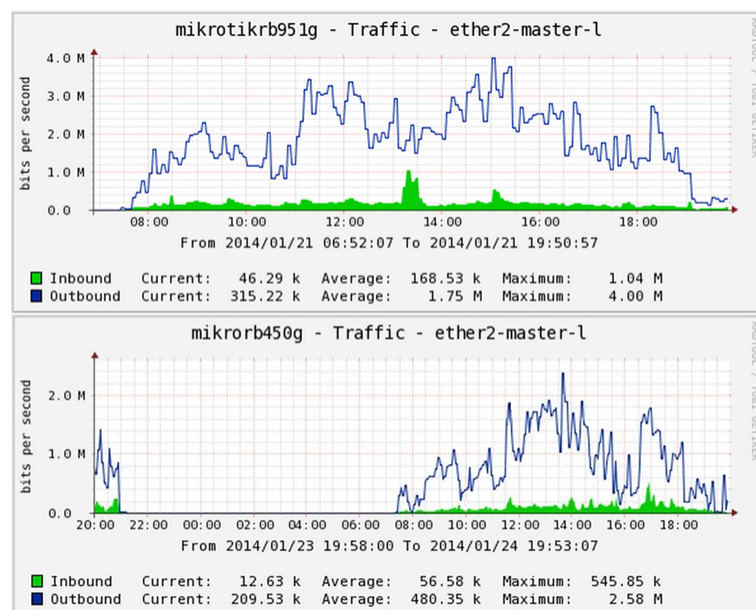


Figura 4.59: Monitoreo del tráfico de red en los Hotspot
Fuente: El Investigador

Como se puede apreciar en el gráfico del tráfico que se genera en la red Wi-Fi, existe mayor estabilidad en cuanto a los picos de subida y bajada en la utilización del ancho de banda existiendo una correlación más estable en las señales de tráfico que se generan en la red debido a la asignación controlada de ancho de banda y autenticación, punto que beneficia al nivel de acceso y a la disponibilidad de servicios para los usuarios de la FISEI.

4.9. Análisis Económico del Proyecto

En el aspecto económico concerniente al presente proyecto de investigación, la mayoría de los recursos necesarios para la implementación son proporcionados por la misma Facultad, básicamente por el Departamento de Redes y Sistemas, sin embargo

para un mejor abastecimiento en el acceso simultáneo de usuarios a la red Wi-Fi de la FISEI, se han provisto 2 dispositivos MikroTik los cuales se encuentran cubiertos por el investigador.

Tabla 4.16: Presupuesto

Ítem	Cantidad	Valor Unitario	Valor Total
MikroTik RB951G-2HnD	1	\$ 111.42	\$ 111.42
Gestión de envío		\$ 4.46	\$ 4.46
MikroTik RB450G	1	\$ 178.08	\$ 178.08
Gestión de envío		\$ 5.00	\$ 5.00
TOTAL			\$ 298.96

Fuente: El Investigador

Debido a que la FISEI no es una entidad o empresa con fines de lucro, no se busca realizar un análisis de recuperación de la inversión, más lo único que se pretende es brindar un servicio eficiente y de calidad en beneficio de toda la comunidad universitaria.

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

En función del desarrollo y resultados obtenidos de la propuesta se concluye lo siguiente:

- Contar con la herramienta Cacti para la monitorización del tráfico que se genera en la red inalámbrica de la FISEI es de suma utilidad ya que permite optimizar las gestiones de administración de la red en cuanto a la detección y solución de problemas que puedan presentarse reduciendo de esta manera el tiempo y los recursos en el trabajo.
- Gracias a las características de configuración, así como sus variadas prestaciones y por su óptima eficiencia al momento de ejecutar los servicios AAA, FreeRADIUS se constituye en la mejor opción para el control y equilibrio en la utilización de la red inalámbrica de la FISEI, además de ajustarse eficazmente en la configuración de sistemas clusterizados.
- El hipervisor XEN posee gran estabilidad y eficiencia para el establecimiento de entornos virtuales mediante paravirtualización capaces de soportar clustervización garantizando servicios de alta disponibilidad en función de los requerimientos de los usuarios.
- La utilización de la aplicación Heartbeat posee gran flexibilidad al momento de ajustarse sobre ambientes virtuales cumpliendo sus funciones regulares como un sistema tolerante a fallos a fin de brindar alta disponibilidad de servicios mediante la creación de una VIP para una comunicación eficiente con el exterior.
- Las gestiones de alta disponibilidad de datos se ajustan de manera correcta a las configuraciones efectuadas mediante la utilización de replicación de nodos

en MySQL a través del modelo maestro a maestro.

5.2. Recomendaciones

- Para contar con la eficiencia y estabilidad necesaria en cuanto al uso y manejo de servidores virtuales es recomendable trabajar sobre la plataforma Linux que sin lugar a dudas es la primera opción para la ejecución de este tipo de proyectos.
- En la aplicación de Heartbeat para el Clúster la alta disponibilidad entre servidores virtuales, se recomienda hacer uso de un enlace punto a punto entre los servidores, de esta manera se puede asegurar el monitoreo constante entre cada uno efectuándose de esta manera la tolerancia a fallos.
- En la configuración maestro a maestro para la replicación de datos en MySQL se recomienda utilizar un enlace punto a punto ya que al ser un enlace dedicado se evitan las colisiones de paquetes al momento de hacer la replicación de los datos.
- Es de suma importancia efectuar un mantenimiento lógico integral del Clúster de alta disponibilidad en los servidores virtuales con la finalidad de verificar que los servicios se estén ejecutando de la forma adecuada y de ser posible a su vez se puedan realizar las respectivas actualizaciones de los mismos.
- Debido a que los HotSpot's se encuentran en los routers MikroTik y estos son los que generan el servicio DHCP para la red inalámbrica, se debe tener presente que pueden existir factores de configuración en los routers-HotSpot para compatibilidad con el servidor RADIUS en el caso que se quiera modificar o agregar algún tipo de requerimiento al sistema.
- En caso que el administrador de red requiera ingresar de manera remota al sistema principal, se recomienda efectuar una conexión segura a través de Internet mediante la utilización del protocolo SSL para la interfaz web de administración DaloRadius.

Bibliografía

- [1] R. Buyya, *High Performance Cluster Computing: Architectures and Systems*. Prentice Hall, Upper SaddleRiver, NJ, USA, 1999, vol. 1.
- [2] M. Gallardo, *Diseño de una solución para servidores de alta disponibilidad y balanceo de carga con Open Source*. Proyecto de Grado, Universidad Alfredo Pérez Guerrero, Ecuador, 2011.
- [3] G. Cáceres, *Estrategia de implementación de un Clúster de alta disponibilidad de n nodos sobre Linux usando software libre*. Proyecto de Grado, Universidad San Francisco de Quito, Ecuador, 2012.
- [4] M. M. Sinisterra, T. M. D. Henao, and E. G. R. López, “Clúster de balanceo de carga y alta disponibilidad para servicios web y mail,” *Revista Informador Técnico*, no. 76, pp. 93–102, 2012.
- [5] P. Clavijo, “Clústers de alta disponibilidad (ha),” *Lintips*, 2012. [Online]. Available: <http://www.lintips.com/?q=node/119>
- [6] EcuRed, “Clúster de alta disponibilidad (ha),” *Equipo EcuRed*, 2011. [Online]. Available: http://www.ecured.cu/index.php/Cluster_de_alta_disponibilidad
- [7] Epistemowikia, “Arquitectura alta disponibilidad,” *Revista Hiperenciclopédica de Divulgación del Saber*, no. 4, 2012. [Online]. Available: http://campusvirtual.unex.es/cala/epistemowikia/index.php?title=Arquitectura_alta_disponibilidad
- [8] CEAACES, “Modelo general para la evaluación de carreras con fines de acreditación,” p. 61, 2011.
- [9] T. Redes y mas, “Diseño de redes, modelo jerárquico,” *Configurar Redes Linux y Cisco*, 2011. [Online]. Available: <http://www.redesymas.org/2011/05/disenio-de-redes-modelo-jerarquico.html>
- [10] T. The CentOS Project, “Centos linux,” *New Look. New CentOS*, 2012. [Online]. Available: <http://www.centos.org/>

- [11] E. Mifsud, “Introducción a la virtualización con xen,” *Observatorio Tecnológico*, 2012. [Online]. Available: <http://recursostic.educacion.es/observatorio/web/es/software/servidores/1080-introduccion-a-la-virtualizacion-con-xen>
- [12] E. Llaguno, “Virtualizadores o convierte tu computadora en varias,” *SesoLibre*, 2008. [Online]. Available: <http://sesolibre.com/2008/01/virtualizadores-o-convierte-tu-computadora-en-varias/>
- [13] T. XenProject, “Paravirtualization (pv),” *Linux Foundation Collaborative Projects*, 2012. [Online]. Available: [http://wiki.xenproject.org/wiki/Paravirtualization_\(PV\)](http://wiki.xenproject.org/wiki/Paravirtualization_(PV))
- [14] TeleInfo, “Servidores radius,” *Blog Tele Info 08*, 2008. [Online]. Available: <http://trabajotele08.blogspot.com/>
- [15] S. Velásquez, B. Castro, and A. Velandia, “Implementación de un servidor de autenticación radius en un ambiente de pruebas para la red inalámbrica de la upb–sede laureles,” *Universidad Pontificia Bolivariana. Medellín, Colombia*, pp. 23–31, Unknown year.
- [16] T. FreeRADIUS, “The freeradius project,” *FreeRADIUS The world’s most popular RADIUS Server*, 2013. [Online]. Available: <http://freeradius.org/>
- [17] T. DaloRADIUS, “Daloradius,” *DaloRADIUS Community*, 2007. [Online]. Available: <http://daloradius.com/>
- [18] E. Vargas and S. BluePrints, “High availability fundamentals,” *Sun Blueprints series*, pp. 1–17, 2000.
- [19] E. Villar, *Virtualización de servidores de telefonía IP en GNU/Linux*. Universidad de Almería, 2010.
- [20] A. Rodríguez, *Diseño de un modelo para la implementación de Servidores Web de Alta Disponibilidad*. Universidad Católica de Santa María, Perú, 2008.
- [21] S. González Durán, “Respaldos en mysql usando replicación,” *Linux Total*, 2012. [Online]. Available: http://www.linuxtotal.com.mx/index.php?cont=info_admon_019
- [22] F. J. Méndez, *Diseño e implementación de un sistema VoIP de alta disponibilidad y alto rendimiento*. Universidad de Almería, 2009.
- [23] T. Informática-Moderna, “El servidor para redes - server,” *Temas de Informática Moderna*, 2013. [Online]. Available: <http://www.informaticamoderna.com/Servidor.htm>

- [24] T. Adminso, “Dispositivos de interconexión,” *Administración de Sistemas Operativos*, 2012. [Online]. Available: http://www.adminso.es/index.php/3._Dispositivos_de_Interconexión#Router
- [25] T. Informática-Moderna, “El servidor para redes - server,” *Temas de Informática Moderna*, 2013. [Online]. Available: http://www.informaticamoderna.com/Acces_point.htm
- [26] T. WifiSafe, “Hotspot - sistema de gestión de acceso a una red,” *WifiSafe, Productos y soluciones Wireless*, 2010. [Online]. Available: <http://www.wifisafe.com/hotspot/index/conceptos/que-es-un-hotspot>
- [27] A. Carrasco and J. Ropero, “Topologías inalámbrica,” *Universidad de Sevilla, España*, pp. 01–24, 2010.
- [28] L. García, “Topologías de las redes inalámbricas,” *Manejo de Redes*, no. 76, 2011. [Online]. Available: <http://plgarcia.blogspot.com/2011/06/definicion.html>
- [29] T. Microsoft, “Introducción a la calidad de servicio (qos),” *TechNet para Microsoft*, 2012. [Online]. Available: <http://technet.microsoft.com/es-es/library/hh831679.aspx>
- [30] P. E. Valle, “Snmp: Simple network management protocol,” *Departamento de Electrónica - UTFSM*, 2007. [Online]. Available: http://profesores.elo.utfsm.cl/~tarredondo/info/networks/Presentacion_snmp.pdf
- [31] T. TYPO3 from AOE, “Filezilla the free ftp solution,” *FileZilla Project*, 2012. [Online]. Available: <https://filezilla-project.org/>
- [32] T. MySQL Reference Manual, “Replicación en mysql,” *Documentación MySQL*, 2011. [Online]. Available: <https://dev.mysql.com/doc/refman/5.0/es/replication-faq.html>

Anexos

Anexo A

Modelo de la Entrevista

UNIVERSIDAD TÉCNICA DE AMBATO FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL CARRERA DE ELECTRÓNICA Y COMUNICACIONES

Entrevista para la tesis: “Clúster de alta disponibilidad para el servidor de autenticación de la red Wi-Fi de la FISEI”, dirigida el Ing. Eduardo Chaso, director del Departamento de Redes y Sistemas de la FISEI.

Banco de Preguntas:

Pregunta 1.

¿Cuenta actualmente la FISEI con el servicio de autenticación de usuarios en su red Wi-Fi?

Pregunta 2.

¿A su criterio y experiencia profesional, cree usted que se debería contar con un servicio de autenticación de usuarios el cual cuente con las características de alta disponibilidad para los usuarios de la red Wi-Fi de la FISEI?

Pregunta 3.

¿Tiene el Departamento de Redes y Sistemas de la FISEI los recursos necesario para la implementación de un Clúster el cual permita dar alta disponibilidad al servicio de autenticación a la red Wi-Fi de la facultad?

Pregunta 4.

¿Cuenta actualmente de la red Wi-Fi de la FISEI con algún tipo de control en la asignación de ancho de banda a los usuarios?

Pregunta 5.

¿Tiene la red inalámbrica de la FISEI algún tipo de seguridad en cuanto al acceso de los usuarios a la web?

Pregunta 6.

¿Cree usted que se podrían crear políticas de seguridad y acceso las cuales podrían ayudar al control y beneficio de los usuarios de la red Wi-Fi de la FISEI?

Gracias por su colaboración.

Anexo B

Configuración SNMP en los equipos MikroTik para monitoreo en Cacti:

Para levantar la conexión de Cacti con los dispositivos HotSpot y realizar el monitoreo de tráfico en la red, se requiere contar con 3 variables específicas y necesarias, estas son:

- **Habilitación SNMP:** Contenido de la unidad de datos del protocolo
- **Comunidad:** Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private".
- **Versión:** Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1).

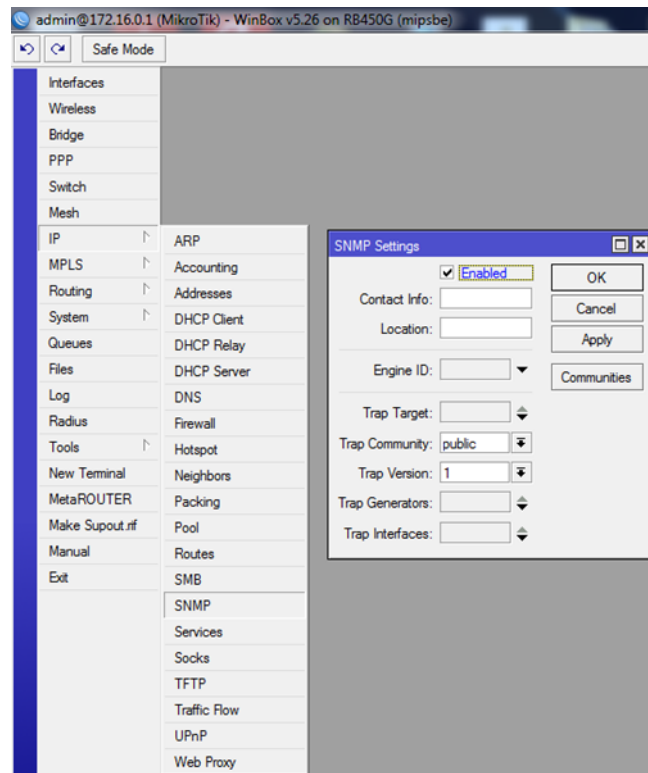


Figura B.1: Habilitación SNMP para dispositivos MikroTik
Fuente: El Investigador

De la misma forma en la aplicación Cacti se configuran las mismas variables.

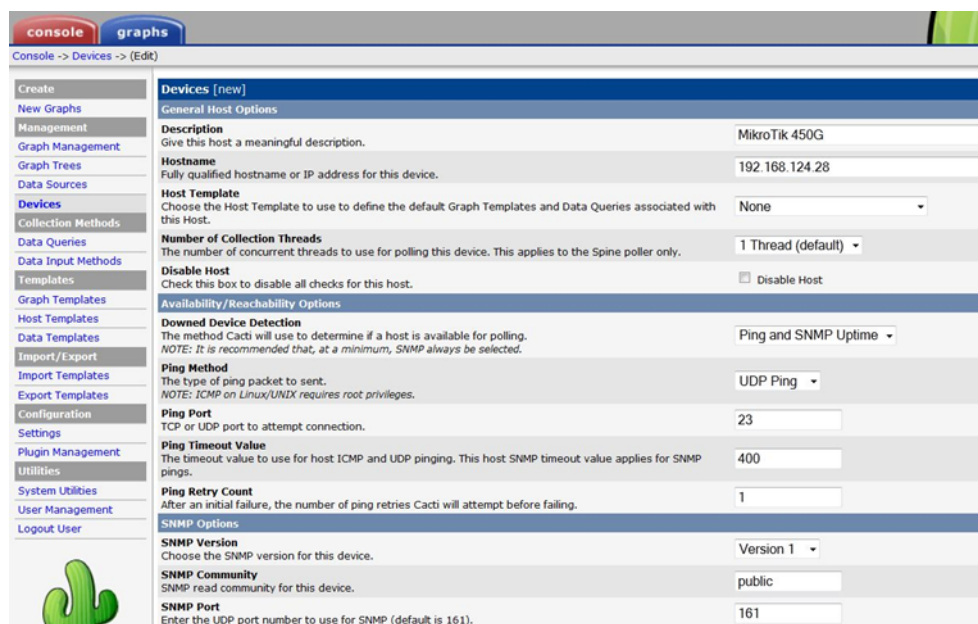


Figura B.2: Habilitación SNMP para Cacti
Fuente: El Investigador

Anexo C

Distribución física de los dispositivos en la red Wi-Fi en la FISEI

En las figuras C.1 y C.2 se puede ver la ubicación de los dispositivos que cubren la red Wi-Fi en los dos edificios de la FISEI.

En el Edificio 1 se encuentran distribuidos los Access Point de la siguiente forma:

- AP1: LINKSYS WAP54G. Decanato - Segundo Piso
- AP2: LINKSYS WAP54G. Biblioteca - Primer Piso
- AP3: CISCO WAP200E (para exteriores). Ágora de la FISEI - Segundo Piso

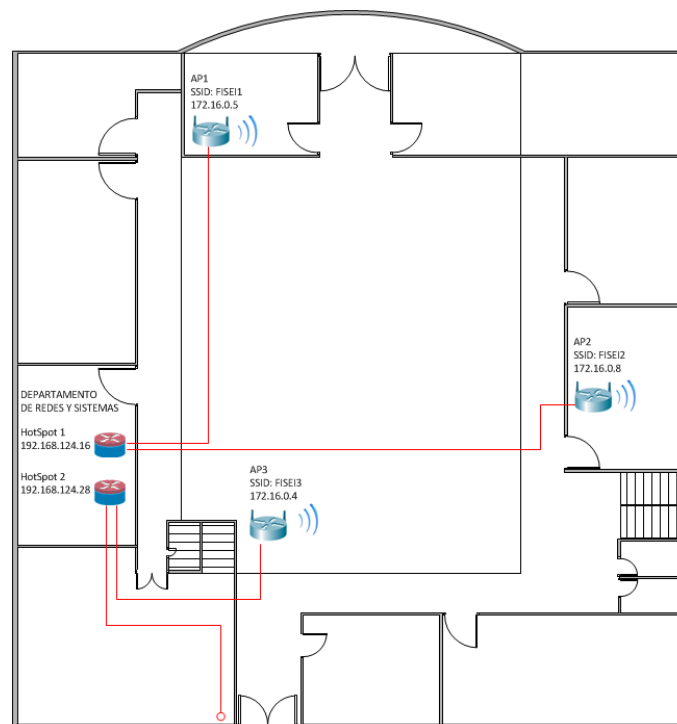


Figura C.1: Dispositivos de red Wi-Fi en la FISEI - Edificio 1

Fuente: El Investigador

En el Edificio 2 se encuentra trabajando un Access Point.

- AP4: CISCO WAP4410N. Segundo Piso

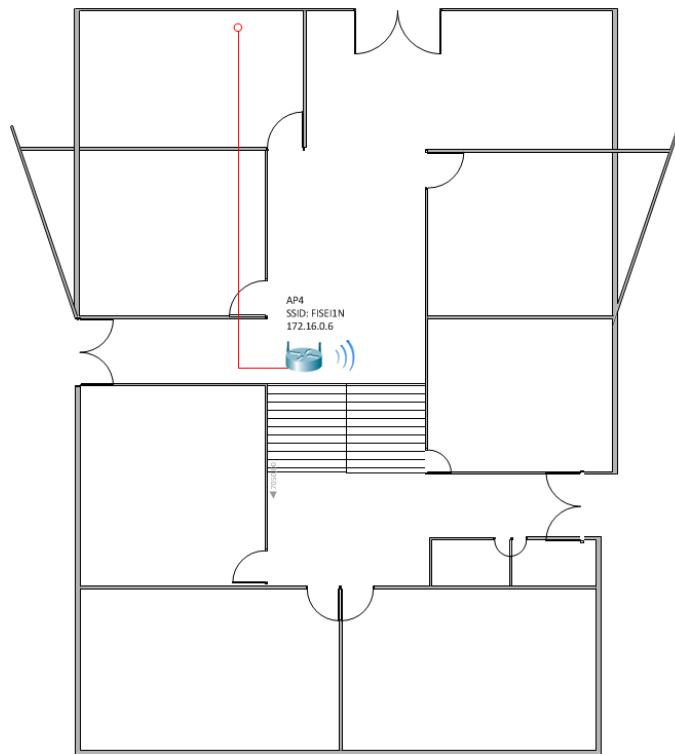


Figura C.2: Dispositivos de red Wi-Fi en la FISEI - Edificio 2
Fuente: El Investigador