

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

FACULTAD DE CIENCIAS E INGENIERIAS FÍSICAS Y FORMALES

PROGRAMA PROFESIONAL DE INGENIERÍA DE SISTEMAS



PROPUESTA DE UNA RED SEGURA PARA LA INTERCONEXIÓN Y COOPERACIÓN DE LAS COMISARIAS Y MUNICIPALIDADES DE AREQUIPA UTILIZANDO LOS PROTOCOLOS VPN Y OLSR CON SERVIDOR RADIUS Y MONITOREO NAGIOS

Tesis presentada por los Bachilleres:

**MOISÉS VLADIMIR CÁRDENAS TORREBLANCA
FREDY EMIGDIO QUISPE RUELAS**

**Para optar por el Título Profesional:
INGENIERO DE SISTEMAS**

**AREQUIPA-PERÚ
2015**

PRESENTACIÓN

Señora Directora de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica Santa María.

S.D

De conformidad con lo establecido en la Dirección de la Escuela Profesional de Ingeniería de Sistemas que Ud. dignamente dirige, presentamos a su consideración y a las señores miembros del jurado del presente trabajo de investigación: **PROPUESTA DE UNA RED SEGURA PARA LA INTERCONEXIÓN Y COOPERACION DE LAS COMISARIAS Y MUNICIPALIDADES DE AREQUIPA UTILIZANDO LOS PROTOCOLOS VPN Y OLSR CON SERVIDOR RADIUS Y MONITOREO NAGIOS**, requisito indispensable para optar el Título Profesional de Ingeniero de Sistemas.

Esperamos que el presente trabajo sea de conformidad y que cumpla con los requisitos académicos y técnicos correspondientes.

Arequipa, Diciembre del 2015

Moisés Vladimir Cárdenas Torreblanca

Fredy Emigdio Quispe Ruelas



AGRADECIMIENTOS

*A todas aquellas personas que han colaborado con la elaboración y culminación
del presente trabajo de investigación.*

Dedicatoria

A nuestra familia, quienes nos han apoyado a lo largo de nuestro crecimiento personal y profesional.





“La comunicación funciona para los que trabajan en ella”

John Powell

ÍNDICE

Presentación	02
Agradecimientos	03
Dedicatoria	04
Epígrafe	05
Índice o Tabla de Contenidos	06
Índice de Figuras	07
Índice de Cuadros	08
RESUMEN	09
ABSTRACT	10
INTRODUCCIÓN	11
CAPÍTULO 1: DESCRIPCIÓN DEL PROYECTO	12
1.1. Objetivos	12
1.2. Alcances y Limitaciones	12
1.3. Fundamentos Teóricos	13
1.3.1. Antecedentes del proyecto	13
1.3.2. Bases Teóricas del proyecto	14
1.4. Técnicas y Herramientas	55
1.5. Aspectos Relevantes del Desarrollo.	55
CAPÍTULO 2: DOCUMENTACIÓN TÉCNICA	56
2.1 Plan del Proyecto Informático.	56
2.2. Especificación de requisitos del Proyecto de TIC's	58
2.3. Especificación de diseño	58
2.4. Documentación técnica de programación.	79
2.5. Pruebas de Ejecución.	79
CONCLUSIONES	86
RECOMENDACIONES	87
BIBLIOGRÁFICAS	88
INFORMATOGRAFIA	89
APÉNDICE(S)	90

ÍNDICE DE FIGURAS.

Gráfico 1.1.	Clasificación de los estándares antes según su área de cobertura.	14
Gráfico 1.2.	Especificación del WLAN ac	18
Gráfico 1.3.	Topología de Red en 802.11	20
Gráfico 1.4.	Topología de Red en 802.11 con Access Point	20
Gráfico 1.5.	Relevos parte de disminuir la cantidad de nodos repetidores	22
Gráfico 1.6.	Direccionamiento con ZRP	23
Gráfico 1.7.	Esquema de una red VPN	24
Gráfico 1.8.	Elementos de una VPN	29
Gráfico 1.9.	VPN de acceso remoto.	33
Gráfico 1.10.	Diagrama VPN con nat	34
Gráfico 1.11.	Diagrama del protocolo PPTP	36
Gráfico 1.12.	Diagrama del protocolo L2TP	38
Gráfico 1.13.	Estructura del paquete Radius	42
Gráfico 1.14.	Interacción de Nagios con los archivos de configuración	48
Gráfico 1.15.	Arquitectura de Nagios y plug-ins Nagios Core Documentation	54
Gráfico 2.1.	Identificación de puntos o nodos	59
Gráfico 2.2.	Identificación Grifo 1	59
Gráfico 2.3.	Identificación Grifo 2	60
Gráfico 2.4.	Vista Global de Estaciones	60
Gráfico 2.5.	Proceso de Transmisión	61
Gráfico 2.6.	Distancia de Redes Grifo 1	62
Gráfico 2.7.	Distancia de Redes Grifo 2	62
Gráfico 2.8.	Interconexión y Comunicación	63
Gráfico 2.9.	Instalación de Nagios	69
Gráfico 2.10.	Configuración Password del usuario Nagios admin	69
Gráfico 2.11.	Administrador Web de Nagios	70
Gráfico 2.12.	Monitorización de equipo local	70
Gráfico 2.13.	Repositorio plugin	71
Gráfico 2.14.	Ingreso de comandos	72
Gráfico 2.15.	Ingreso página web de administración de Nagios	73
Gráfico 2.16.	Routers de sucursales conectadas a internet	73
Gráfico 2.17.	Captura de paquetes con wireshark	79
Gráfico 2.18.	Software de Monitoreo	79
Gráfico 2.19.	Software de Monitoreo (continuación)	80
Gráfico 2.20.	Grifo sin interconexión	81
Gráfico 2.21.	Interconexión y Comunicación Segura	81
Gráfico 2.22.	Tiempo de Interconexión y Comunicación de Datos	82
Gráfico 2.23.	Medición de Tiempo de Respuesta	82

INDICE DE CUADRO

Cuadro 1.1. Significado de los campos del paquete OLSR	21
Cuadro 1.2. Cuadro Comparativo VPN	25
Cuadro 1.3. Cuadro Comparativo TACAS vs RADIUS	40
Cuadro 1.4. Significado de los campos del paquete RADIUS	42
Cuadro 1.5. Significado de los campos del paquete NAGIOS	46
Cuadro 1.6. Cuadro comparativo (programas de monitoreo)	47



RESUMEN

En la actualidad la constante evolución de la tecnología, en cuanto a las redes Inalámbricas y cableadas nos brinda la oportunidad de poder comunicar diferentes puntos lo cual conlleva a que dichos puntos puedan compartir información a una alta velocidad y en tiempo real.

Pero como todo gran avance también conlleva a un problema muy importante que viene hacer la inseguridad de las redes, he ahí donde la presente tesis se aboca ya que queremos dar a conocer uno de los muchos métodos que se puede implementar para poder salvaguardar la información de los usuarios y así lograr que la información que se transmite en las redes sea confiable y segura.

Se propone una arquitectura de red que está abocada a poder unir las Municipalidades de Arequipa y a su vez también que cada una de las Municipalidades se comunique de manera segura con sus respectivas comisarías y proponiendo con un plan piloto, unir la Municipalidad de José Luis Bustamante y Rivero con su respectiva comisaria y a dos centros de distribución de combustible (grifos).

Dichos puntos se podrán comunicar de manera rápida y eficiente y sobre todo estar seguro que la información que están compartiendo o transmitiendo sea confiable y segura, además garantizando que no cualquier usuario se logre conectar a la red sin una previa autorización y como último dicha arquitectura de red cuenta con un medio con el cual se logra monitorear de manera constante la red garantizando una respuesta rápida y eficiente a la hora de poder corregir un problema en la red.

Palabras claves: Interconexión – Comunicación – VPN – Radius – Nagios

ABSTRACT

Today the constant evolution of technology, in terms of wired and wireless networks gives us the opportunity to communicate different points which leads to these points can share information at high speed and in real time.

But like all great progress also leads to a very important issue that comes to the insecurity of networks, here is where this thesis Aboca because we want to present one of many methods that can be implemented to safeguard information users and thus ensure that the information is transmitted in the network is reliable and safe.

A network architecture that is bound to be able to join the municipalities of Arequipa and in turn each of the municipalities to communicate securely with their respective police stations and proposing a pilot, joined the Municipality of José Luis Bustamante is proposed and Ribero with their respective Commissioner and two fuel distribution centers (taps).

These points can communicate quickly and efficiently and above all be sure that the information you are sharing or transmitting it is reliable and safe, and ensures that not every user is achieved connect to the network without prior authorization and as a last such architecture network has a means by which it is achieved constantly monitor the network to ensure fast and efficient when to correct a problem with the network response.

Keywords: Interconnection - Communication - VPN - Radius - Nagios



INTRODUCCIÓN

El presente proyecto busca analizar las opciones y proponer alternativas para brindar una arquitectura de red segura, entre las municipalidades y sus respectivas comisarías de Arequipa, utilizando los protocolos VPN, OLSR y servidor Radius con monitoreo Nagios, lo cual brinda un método de mejorar la inseguridad de la Red Inalámbrica y la red cableada, mediante los diferentes medios de comunicación, se tiene conocimiento de que existe un incremento de asaltos en las empresas distribuidoras de combustible, muchas veces causan pérdidas humanas y materiales. Es necesario la realización de la presente propuesta por la inexistencia de métodos que garantiza una respuesta inmediata de las autoridades policiales o de seguridad ciudadana.

En el CAPÍTULO 1, se da a conocer los conceptos básicos sobre las Redes inalámbricas, Estándar IEEE 802.11, Modelo de referencia TCP/IP, Entrada de Red, el Protocolo VPN, el Servidor RADIUS y la Aplicación NAGIOS además de plantear los alcances y limitaciones que se encontraron para desarrollar la arquitectura de red.

En el CAPÍTULO 2, se detalla todo la documentación técnica necesaria para el desarrollo del plan del proyecto Informático y los requisitos importantes para poder realizar la arquitectura de red, como también la metodología que se llevó a cabo para la implementación de dicha arquitectura. Y finalmente se plantea los logros alcanzados como también las recomendaciones del caso para el mejoramiento o la optimización del plan del proyecto informático.

CAPÍTULO 1

DESCRIPCIÓN DEL PROYECTO

1.1. OBJETIVOS

1.1.1. General

Propuesta de una red segura para la interconexión y Cooperación de las Comisarias y Municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor Radius y monitoreo Nagios.

1.1.2. Específicos

1. Precisar la efectividad que brindará el protocolo VPN para intercomunicar las municipalidades y comisarías de la ciudad de Arequipa.
2. Comprobar la seguridad inalámbrica que brinda el protocolo OLSR y servidor Radius mediante la captura de paquetes.
3. Identificar mediante el programa Nagios las posibles fallas y problemas que se suscitan en la arquitectura de la Red.

1.2. ALCANCES Y LIMITACIONES

1.2.1. Alcances

- Brindar una arquitectura de red en la cual la información viaje de manera segura entre los diferentes nodos.
- La Información generada se constituye en un valioso aporte con miras a la ejecución e implementación de nuevos proyectos de intercomunicación a nivel local.
- Generar la realización e implementación de conexión VPN en toda la ciudad de Arequipa.
- El tiempo de ejecución es corto, ya que es un plan piloto en el distrito de José Luis Bustamante y Rivero, en el cual se logra interconectar dos centros de distribución de combustible de dicho distrito con su respectiva comisaria.
- La Utilización de otros sistemas para interconectar las diferentes Municipalidades y se complementa con el uso del TeamSpeak y Ventrilo¹, ya

1 <http://www.brighthub.com/office/collaboration/articles/75044.aspx>

que se conecta a un servidor el cual identifica a los usuarios y mediante él se maneja una intercomunicación.

1.2.2. Limitaciones

- La falta de equipos de red como Access Point, router, cables de red en la comisaria y grifos, por falta de presupuesto.
- La falta de un ordenador en la Municipalidad, para la implementación del servidor Radius y el Monitoreo Nagios.
- Los grifos del Distrito de José Luis Bustamante y Rivero no cuentan con una conexión dedicada con la comisaria o el serenazgo del distrito, y algunos no cuentan ni con internet.

1.3. Fundamentos Teóricos

1.3.1. Antecedentes del proyecto

Riquelme C. H, en su estudio “Modelo para extender redes inalámbricas de banda ancha con tecnología WIMAX en entornos rurales” (2015), el análisis se apoya en la utilización de una herramienta de simulación, donde los resultados ayudaran a demostrar que el rendimiento de la Red refleja un buen desempeño y se comprueba la teoría de conmutación con multisaltos.

La inseguridad que vive hoy en día la ciudad de Arequipa, por el crecimiento de la población de manera rápida, y en vista de los últimos acontecimientos de violencia que ponen en riesgo a los ciudadanos de diferentes distritos, como también la dificultad que tienen las municipalidades y sus respectivas comisarias para poder cooperar entre ellas y así para poder ejecutar obras, en las cuales puede beneficiar a más de un distrito de la ciudad de Arequipa.

El siguiente paso fue profundizar sobre el funcionamiento de protocolos de comunicación que puedan garantizar la seguridad de la información en vista que para la ejecución de obras o difundir información esta no se vea alterado en el camino o sea robada por terceras personas u organizaciones.

Esto fue lo necesario para poder comenzar la investigación a fin de poder garantizar la información y proponer una arquitectura de red en la cual beneficiara en gran medida a la ciudad de Arequipa.

Con el conocimiento técnico del funcionamiento y vulnerabilidades de los

protocolos investigados se decidió por los protocolos OLSR para una Red Móvil Urbana y VPN para una red WAN que comunicara las municipalidades y sus respectivas comisarias además de proponer un servidor Radius para garantizar la Autenticación de los usuarios y para la disponibilidad y la aplicación Nagios.

1.3.2. Bases Teóricas del proyecto

1. ESTADO DEL ARTE

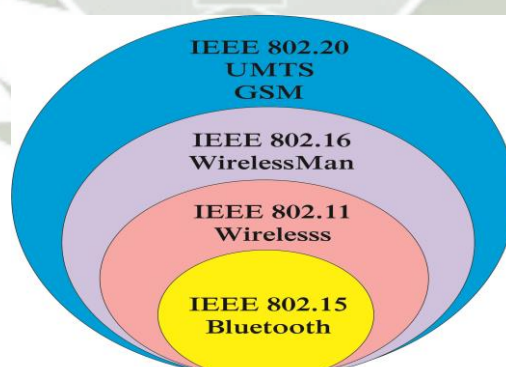
1.1. REDES INALÁMBRICAS

Si nosotros nos ponemos a buscar algún artículo referente a internet todos nos dan una idea pero el nacimiento de las redes inalámbricas se dan como experiencia que datan de 1979 cuando unos científicos de IBM elaboran por primera vez una red con tecnología infrarroja, pero hasta 1985 empiezan avances de redes en bandas de frecuencia eso llevo a que ingenieros eléctricos y electrónicos de la IEEE. Se repartan en diferentes trabajos de desarrollo de estándares.

A través de los años las redes inalámbricas fueron tomando aspectos diferentes, debido a que se formaron distintos grupos de trabajo. Gracias a ello se hace posible la estandarización, seda la creación y fabricación de equipos, según sus necesidades y usos que se le pueda dar.

En distintos estándares creados por la IEEE se encuentran IEEE 802.11x, IEEE 802.15x, IEEE 802.16x) gracias a estos estándares se promueve las redes inalámbricas según la clase, la que más utilizamos día a día es la IEEE 802.11x.

Gráfico 1.1. Clasificación de los estándares antes según su área de cobertura.



Fuente: Diseñado en base a Estándar IEEE 802.11

1.1.1. Estándar IEEE 802.11

Este estándar surge en 1997 es el primer estándar, por el cual se sientan las bases tecnológicas para el resto. Define las características de una red de área local inalámbrica (WLAN). Wi-Fi que significa ("Fidelidad inalámbrica")

IEEE 802.11: IEEE 802.11 en sus variantes 802.11 a, b, g ofrecía hasta el año 2009 una velocidad máxima de 54 Mbps. A partir de octubre del 2009 con el advenimiento del estándar 802.11 n supera los 100 Mbps. El organismo internacional generador de estos estándares es el conocido como Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

Arquitectura del estándar 802.11

Las especificaciones del estándar definido por el IEEE denominado 802.11x (x comprende letras que definen las variantes de la norma 802.11 a, 802.11 b, 802.11 g, 802.11 n), abarcan las capas física (Capa 1) y la subcapa de acceso al medio (MAC) de la capa de enlace del modelo OSI.

Veamos algunos detalles que nos ayudarán a entender el funcionamiento y acotar los problemas con los que nos vamos a encontrar.²

❖ Estándares Wi-Fi

- **802.11a**

Hay una alta densidad de usuarios finales como aeropuertos centros de convenciones y lugares públicos que utilizan el estándar 802.11a

Wifi5: El estándar 802.11 (llamado WiFi 5) admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mbps).

- Ofrece excelente soporte para aplicaciones que requieran un amplio ancho de banda, la interferencia significativa de la banda de 2.4Ghz.
- Hay una alta densidad de usuarios finales como aeropuertos centros de convenciones y lugares públicos que utilizan el estándar 802.11a.
- Una de sus ventajas es que su transfiere a 54Mbps 802.11a.
- Por todo lo mencionado es que nos enfocamos en el estándar 802.11a.

802.11b

Wifi: El estándar 802.11 es el más utilizado actualmente. Ofrece un rendimiento total máximo de 11 Mbps (6 Mbps en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto.

² Consulta http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf

- **802.11c**

Combinación del 802.11 y el 802.1d: El estándar combinado 802.11c no ofrece ningún interés para el público general. Es solamente una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).

- **802.11d**

Internacionalización: El estándar 802.11d es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.

- **802.11e**

Mejora de la calidad del servicio: El estándar 802.11e está destinado a mejorar la calidad del servicio en el nivel de la capa de enlace de datos. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.

- **802.11f**

Itinerancia: El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el protocolo IAPP que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como itinerancia.

- **802.11g**

El estándar 802.11g ofrece un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mbps en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con

el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.

- **802.11h**

El estándar 802.11h tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la h de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.

- **802.11i**

El estándar 802.11i está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el AES (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.

- **802.11r**

El estándar 802.11r se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.

- **802.11j**

El estándar 802.11j es para la regulación japonesa lo que el 802.11h es para la regulación europea.

- **802.11ac**

Una de la característica es que los componentes utilizados en el estándar **ac** consumen menos energía, lo que es bueno para dispositivos que funcionan con baterías como ordenadores portátiles, teléfonos móviles y tablets.

Mayor alcance, (con una banda de 5 GHz), los routers ac pueden alcanzar distancias mayores. De ello es responsable la tecnología “Beamforming”, que focaliza la señal de radio.

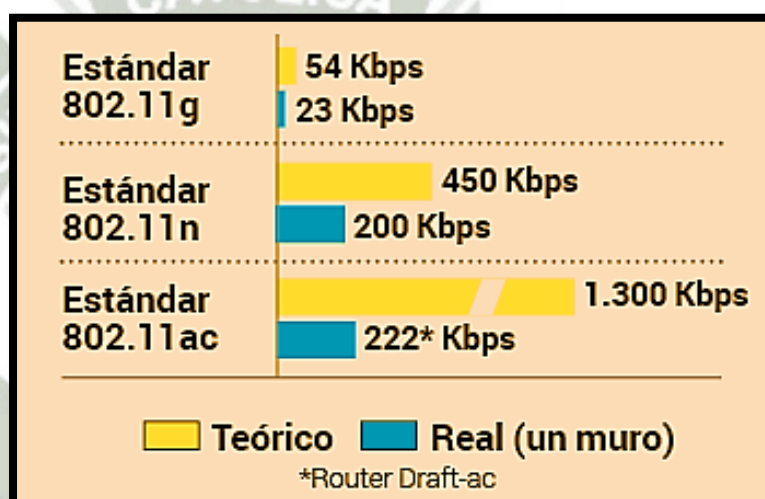
Qué lo hace tan rápido, Canales de radio más anchos: cuanto más ancho es el canal de radio, más “carriles” hay disponibles en la autopista de datos

y más alta es la velocidad posible. En lugar de utilizar 40 MHz de ancho de canal, la tecnología ac puede funcionar con 80 o incluso 160 MHz.

Antenas múltiples: cuantas más antenas, mayor velocidad máxima se puede alcanzar. Los routers ac actuales transfieren, al mismo tiempo, hasta seis flujos de datos espaciales (“spatial streams”) mediante tres antenas.

Únicamente de esta manera se puede alcanzar la velocidad máxima. La especificación del WLAN ac puede incluso incluir hasta cuatro antenas. Velocidad WiFi.

Gráfico 1.2. Especificación del WLAN ac



Fuente: Estándar IEEE 802.11 ac

El número de antenas determina la velocidad de los datos que llegan al receptor. La velocidad máxima del WLAN ac (teórica de 1,3 Gbps, en la práctica alrededor de 0,2 Gbps) sólo se consigue con tres antenas.

Pero muchos routers inalámbricos baratos, teléfonos inteligentes y adaptadores USB solo tienen una: es decir, solo se puede conseguir un tercio de la velocidad máxima soportada

Dispositivos con WiFi ac

Para una velocidad ac completa, tanto tu router como el dispositivo receptor tienen que ser compatibles con esta tecnología. Los más antiguos

seguirían funcionando, pero a la velocidad actual. Estos son algunos dispositivos ya compatibles con esta nueva tecnología:

Routers: Apple Airport Extreme/Time Capsule, AVM Fritz Box 7490 (desde verano), Buffalo WZRD1800H, D -Link 810L-868L, Linksys EA6700, Netgear 6200/6300, Speedport W724V.

Notebooks: Apple Macbook Air (nueva versión), Alienware 17, Asus G750. Ya están disponibles adaptadores asociados de Linksys, Netgear y de Trendnet.

Smartphones: En cuanto a este tipo de dispositivos móviles, los primeros teléfonos inteligentes compatibles con la nueva tecnología WLAN ac son el modelo HTC One y, también, el Samsung Galaxy S5. También la mayoría de smartphones de alta gama de última generación.³

❖ Topología de Red en 802.11

El estándar IEEE 802.11 define el concepto de Conjunto Básico de Servicio (BSS, Basic Service Set) que consiste en dos o más nodos inalámbricos o estaciones que se reconocen una a la otra y pueden transmitir información entre ellos.

Radio Enlace

Lado de Transmisión

- Potencia de Transmisión, pérdidas en el cable, ganancia de antena

Lado Receptor

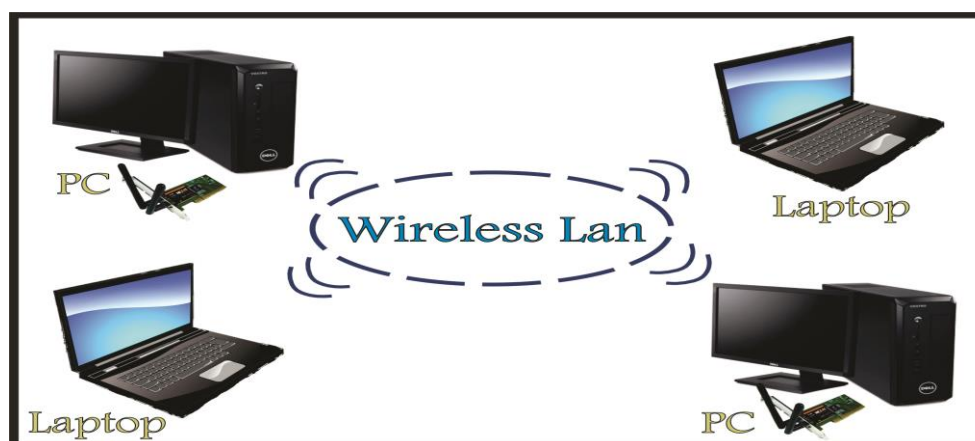
- Ganancia de antena, pérdidas en el cable, sensibilidad del receptor
- Cuanto más baja sea la sensibilidad, mejor será la recepción del radio
- Potencia de salida del radio (la tarjeta inalámbrica, estación base)

Un BSS puede intercambiar información de dos modos diferentes:

³ <http://computerhoy.com/noticias/internet/que-es-wifi-80211ac-que-hace-tan-rapido-8789>

1. Cada nodo se comunica con el otro en forma directa y sin ninguna coordinación. Este modo es comúnmente llamado Ad-Hoc o IBSS (Independent Basic Service Set). Este modo solo permite la transmisión entre los nodos inalámbricos y no resuelve el problema de extender una LAN cableada.

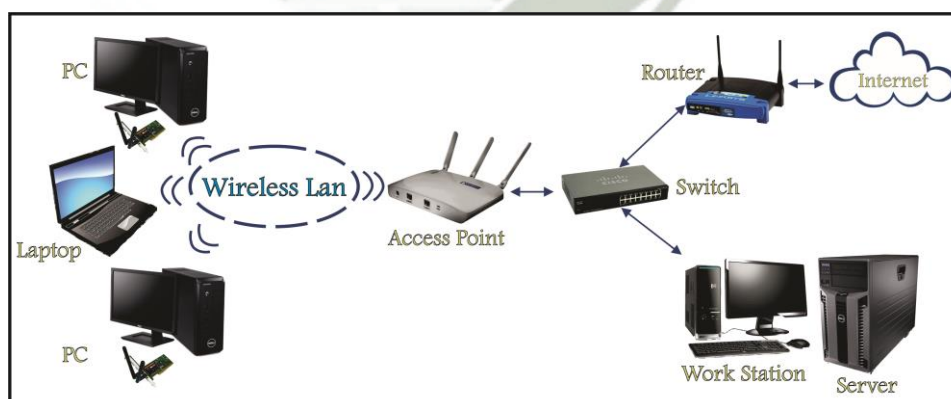
Gráfico 1.3. Topología de Red en 802.11



Fuente: Elaboración propia.
Estándar IEEE 802.11 X de las WLAN

2. Existe un elemento llamado comúnmente AP (Access Point) que coordina la transmisión entre los nodos inalámbricos. Este modo es llamado modo Infraestructura y permite vincular la red inalámbrica con la red cableada ya que el AP actúa como bridge entre las dos redes. La existencia de varios AP conectados a un sistema de distribución (DS: Distribution System), que puede ser una LAN cableada es lo que denominamos EBSS (Extended Basic Service Set). La tecnología 802.11 permite el roaming entre los distintos AP.⁴

Gráfico 1.4. Topología de Red en 802.11 con Access Point



Fuente: Elaboración propia.

⁴ Estándar 802.11 Consulta

<http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi>

A. Optimized Link State Routing (OLSR)

Conocido como protocolo de encaminamiento para nuestros nodos o clientes, una de las razones que soporta esa decisión son la estandarización y el desempeño de protocolo.

En el Area MANet's

Se tiene 3 protocolos de referencia los cuales son:

AODV: Su característica principal es cuando las rutas se generan bajo demanda de nodos que desean incorporarse en una red ad-hoc y redes malla, gracias a ellos tiene una capacidad interesante, para redes con una alta movilidad de nodos, con ellos permite que no se altere las tablas de enrutamiento, ya que cada vez que se genera una comunicación dicha tabla es generada. El protocolo en mención recibe atención por IETF (Internet Engineering Task Force) un grupo de trabajo de ingeniería en internet, y se ha venido desarrollando por parte de los trabajos iniciados con el RFC 3561, la última vez que se reviso fue en el 2009, ahora todas esas revisiones han quedado en borradores, y no fue generado un nuevo RFC que haga referencia al protocolo.

La Desventaja principal y descarte de este protocolo es que al generar nuevas rutas de comunicación, como correos electrónicos, navegación, mensajería instantánea y otros hace que se genere sobrecarga, en las conexiones principales de internet (backbone) por todo lo mencionado no resulta conveniente.

Cuadro 1.1. Significado de los campos del paquete OLSR

Campo	Descripción
Protocolo	Mecanismo estándar de enrutamiento pro-activo, que trabaja en forma distribuida para establecer las conexiones entre los nodos en una red inalámbrica ad hoc.
Enrutamiento	Protocolos pro-activos consiste en que es posible mantener tablas actualizadas de enrutamiento en todo momento. Por otro lado, la desventaja de un protocolo pro-activo consiste en que se requiere una carga adicional en la red inalámbrica debido a la transmisión periódica de mensajes de control.
Mecanismo	Hay varias formas de escoger los multipoint relays de un nodo, pero independientemente de la forma de elección, el conjunto de MPRs de un nodo debe verificar que son capaces de alcanzar a todos los vecinos situados a una distancia de 2 saltos del nodo que los calcula
Autenticador	Los mensajes son enviados periódicamente por cada nodo de la red a sus nodos vecinos, pero nunca son retransmitidos más allá del primer salto (1 hop) desde su emisor (alcance local). Estos mensajes contienen la lista de vecinos conocidos por el nodo emisor así como la identidad de los multipoint relays seleccionados por transmisor

OLSR: Protocolo proactivo, que quiere decir que transmite una gran cantidad de tráfico en forma de paquetes para mantener un enlace actualizado en las bases de datos, por la actualización constante se eliminan los retrasos al inicio de cualquier comunicación.

También OLSR resuelve la sobrecarga que hay en el tráfico de información gracias a una técnica de relevos o conocidas como multipunto o MPR.

Relevos parte de disminuir la cantidad de nodos repetidores, como actualizaciones de la tabla como se ve en el gráfico 1.5

Un nodo puede ser elegido como relevo Multipunto (MPR) y puede alcanzar en 2 saltos a sus vecinos, cuando se le designa MRP el nodo toma la responsabilidad de transmitir a todos sus vecinos la información de actualización de la tabla de Estado-Enlace.

Gráfico 1.5: Relevos parte de disminuir la cantidad de nodos repetidores



Fuente: Elaboración propia

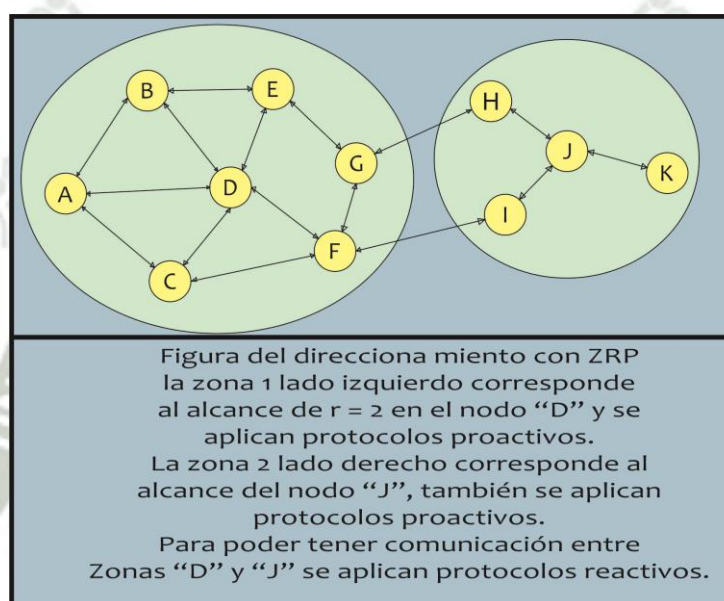
El Protocolo OLSR también fue diseñado para trabajar en entornos de radio transmisión, y para evitar colisiones en las actualizaciones entre nodos incluye un retardo de reenvío que es un retardo aleatorio en el tiempo, en el que las actualización de la tabla de estado enlace debe ser retenida en cache.

ZRP: Llamado también protocolo híbrido, en el cual se da protocolos de encaminamiento por vector distancia o también de estado enlace dependiendo de la topología que se forme por los nodos.

Su trabajo es de dividir una zona de red en zonas de alcance e implementar protocolos proactivos como OLSR en el interior de zonas definidas e implementa algoritmos reactivos para la interconexión o comunicación de las zonas.

Las zonas se definen por la letra **r** debido a que es el radio de la zona en saltos a partir de un nodo central. Como se puede ver en el siguiente gráfico.

Gráfico 1.6. Direccionamiento con ZRP



Fuente: Elaboración propia

El protocolo ZRP, actualmente no ha recibido mucha atención de la comunidad inclusive se puede decir que es una plataforma de desarrollos de protocolos.

Los protocolos descritos, trabajan con algoritmos por vector distancia.⁵

1.2. PROTOCOLO VPN

En nuestra días, la tecnología avanza rápidamente, esto implica que en toda organización haya que considerar las tecnologías aplicadas a la seguridad y velocidad de las redes, puesto que esto determina la confiabilidad del paso de la información a través de los dispositivos virtual (VPN), del inglés "Virtual Private Network"

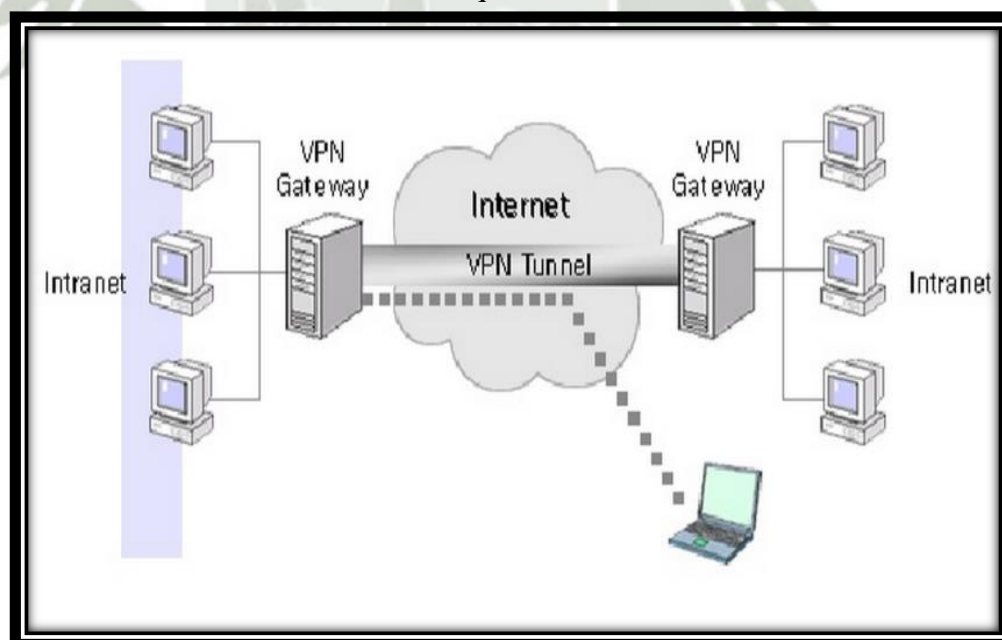
⁵ <https://books.google.com.pe/books?isbn=1409284638>

Se trata de una red de comunicaciones privada implantada sobre una infraestructura pública tal como x.25, atm o frame relay. Este tipo de VPN es denominada de nivel 2. Sin embargo, la tecnología emergente de redes privadas virtuales se basa en los protocolos de nivel 3 (nivel de red del modelo OSI), más específicamente en IP. Esta tecnología busca implementar redes de servicio privadas particionado redes públicas o compartidas del IP, donde la red pública IP más conocida y difundida mundialmente es internet.⁶

1.2.1. Definición de una VPN

Una Red Privada Virtual (VPN) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes áreas geográficas. Es una red de datos de gran seguridad que utilizando Internet como medio de transmisión permite la transmisión de información confidencial entre la empresa y sus sucursales, sus socios, sus proveedores, sus distribuidores, sus empleados o sus clientes. Aunque Internet es una red pública abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.⁷

Gráfico 1.7. Esquema de una red VPN



Fuente: 1992-2013 Cisco Systems Inc

⁶ Copyright International Business Machines Corporation 2002, 2007

⁷ 1992-2013 Cisco Systems Inc

Una Red Privada Virtual (VPN) conecta los componentes de una red sobre otra, por medio de la conexión de los usuarios de distintas redes a través de un "túnel" que se construye sobre Internet o sobre cualquier otra red pública, negociando un esquema de encriptación y autenticación de los paquetes de datos para el transporte, permitiendo el acceso remoto a servicios de red de forma transparente y segura con el grado de conveniencia y seguridad que los usuarios conectados elijan. Con Routers para lograr esa encriptación y autenticación. Es así como las Redes Privadas Virtuales (VPN) se convierten en un componente importante dentro de un ambiente corporativo que tiene como objetivo utilizar una infraestructura de redes públicas para la comunicación en vez de utilizar conexiones privadas o estructuras de acceso remoto que poseen un costo elevado, permitiendo compartir y transmitir información de formas segura y confidencial entre una municipalidad y sus semejantes, socios, proveedores, etc.

Cuadro 1.2. Cuadro comparativo de VPN (giganews, 2015)

	PPTP	L2TP/IPsec	OpenVPN	Chameleon
Encriptación VPN	128 bits	256 bits	160 bits 256 bits	256 bits
Compatible con las apps de VyprVPN	<u>Windows</u> <u>Mac</u> <u>Android</u>	<u>Windows</u> <u>Mac</u> <u>Android</u> <u>iOS</u>	<u>Windows</u> <u>Mac</u> <u>Android</u>	<u>Windows</u> <u>Mac</u> <u>Android</u>
Compatible con configuración manual	Windows Mac OS X Linux iOS Android DD-WRT	Windows Mac OS X Linux iOS Android	Windows Mac OS X Linux Android	Windows Mac OS X Android
Seguridad VPN	Encriptación básica	La máxima encriptación. Comprueba la integridad de los datos y encapsula los datos dos veces.	La máxima encriptación. Autentifica los datos con certificados digitales.	La máxima encriptación. Autentifica los datos con certificados digitales.
Velocidad de VPN	Rápido debido a la encriptación más baja.	Necesita más proceso de la CPU para encapsular los datos dos veces.	Protocolo con mejor rendimiento. Velocidades elevadas, incluso en conexiones con alta latencia y a	El protocolo que ofrece mejor rendimiento. Frustra la inspección profunda de paquetes.

			grandes distancias.	Altas velocidades incluso en conexiones con alta latencia y en grandes distancias.
Estabilidad	Funciona bien en la mayoría de puntos de acceso Wi-Fi, muy estable.	Compatible con dispositivos NAT.	La más fiable y estable, incluso tras routers inalámbricos, en redes no fiables, y en puntos de acceso Wi-Fi.	Oculta el tráfico de VPN para que no pueda ser identificada como una conexión VPN (por medio de la inspección profunda de paquetes) ni bloqueada.
Compatibilidad	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Nativo en la mayoría de los sistemas operativos de dispositivos de sobremesa, portátiles y tablets.	Compatible con la mayoría de los sistemas operativos de ordenadores de sobremesa y dispositivos Android móviles y tabletas.	Compatible con la mayoría de los sistemas operativos de ordenadores de sobremesa y dispositivos Android móviles y tabletas.
Conclusión	PPTP es un protocolo rápido, fácil de usar. Es una buena elección si su dispositivo no soporta OpenVPN.	L2TP/IPsec es una buena elección si su dispositivo no soporta OpenVPN y la seguridad es la prioridad máxima.	OpenVPN es el protocolo recomendado para equipos de sobremesa incluyendo Windows, Mac OS X y Linux. El máximo rendimiento - rápido, seguro y fiable.	<u>Chameleon</u> es excelente para usuarios de VPN que están siendo bloqueados en países como China, o si está sufriendo problemas de velocidad debido a la reducción del ancho de banda.

Comentario: Como podemos se observó en la tabla de comparación de VPN, la decisión más importante porque se eligió L2TP/IPsec es por ser compatible con diferentes plataformas y también por tener la máxima encriptación que comprueba la integridad de los datos y encapsula los encapsula dos veces asegurando que la información sea completamente segura a la hora de viajar por la red.

1.2.2. Características Funcionales

Para que una VPN proporcione la comunicación que se espera, el sistema que se implante ha de contemplar varios aspectos de funcionamiento para determinar que será una buena solución.

♦ **Transparente a las aplicaciones:**

Las aplicaciones no necesitan adaptarse a este nuevo mecanismo sin afectar el correcto funcionamiento de las aplicaciones.

♦ **Confidencialidad:**

Los datos que circulan por el canal sólo pueden ser leídos por el emisor y el receptor. La manera de conseguir esto es mediante técnicas de encriptación.

♦ **Autenticación:**

El emisor y el receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Esto puede conseguirse mediante firmas digitales o aplicando mecanismos desafío-respuesta.

♦ **Integridad:**

Capacidad para validar los datos, esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Para esto se pueden utilizar firmas digitales.

♦ **No repudio:**

Cuando un mensaje va firmado, el que lo firma no puede negar que el mensaje lo emitió él.

♦ **Control de acceso:**

Capacidad para controlar el acceso de los usuarios a distintos recursos.

◆ **Viabilidad:**

Capacidad para garantizar el servicio. Por ejemplo para las aplicaciones de tiempo real.

1.2.3. Elementos principales de una VPN

Servidor VPN

Es un servidor que se pone como Gateway en la salida de Internet de la red. Permite conectarse con otros servidores VPN generando túneles de comunicación seguros con otras redes o usuarios remotos, proporcionando una conexión de acceso remoto VPN o una conexión de enrutador a enrutador.

Cliente VPN

El cliente VPN permite la comunicación privada virtual iniciada desde el cliente de la red (VPN). Es en si una computadora que inicia una conexión VPN con un servidor VPN.

Un cliente VPN o un enrutador tiene una conexión de enrutador a enrutador a través de una red pública, así es como los usuarios finales logran la comunicación dentro de un ambiente de la empresa que requieren una conexión segura del extremo usuario a anfitrión.

Túnel

Porción de la conexión en la cual sus datos son encapsulados.

Conexión VPN

Es la porción de la conexión en la cual sus datos son encriptados. Para conexiones VPN seguras los datos son encriptados y encapsulados en la misma porción de la conexión.

Protocolos del Túnel

Se utiliza para administrar los túneles y encapsular los datos privados. Los datos que son enviados por el túnel deben de ser encriptados para que sea una conexión VPN.

Datos del Túnel (Tuneled Data)

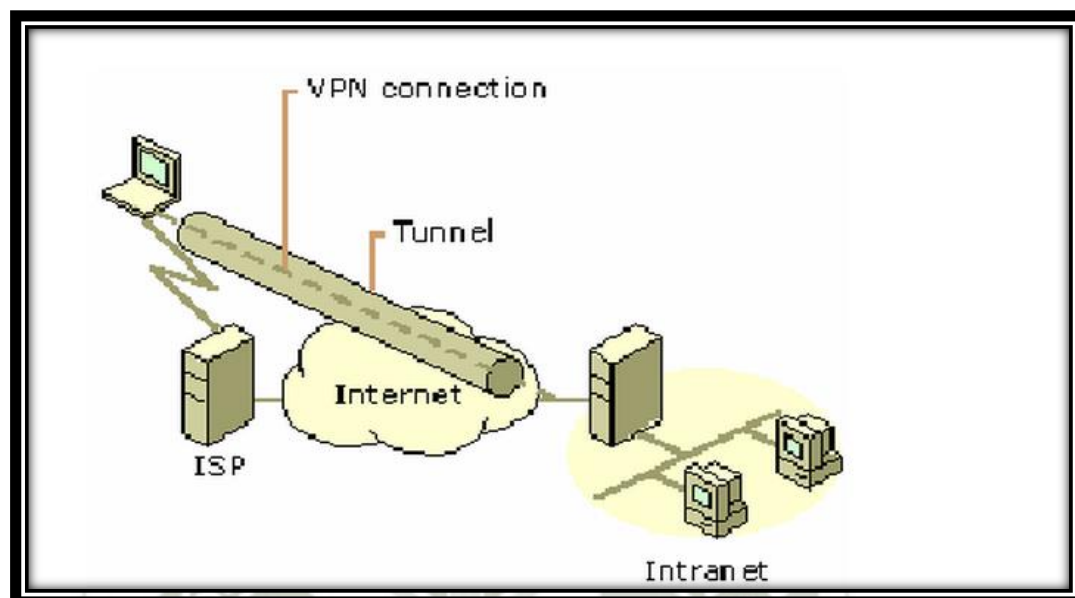
Datos que son generalmente enviados a través de un enlace VPN.

Red de Transito

La red pública o compartida que es cruzada por los datos encapsulados.

Generalmente una red IP. La red de tránsito debe ser Internet o una intranet IP privada.⁸

Gráfico 1.8. Elementos de una VPN



Fuente: HABRAKEN, Joe. "Routers Cisco". Editorial Prentice Hall. España

1.2.4. Requerimientos Básicos de las VPN

Por lo general, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la misma. La solución deberá permitir la libertad para que los clientes roaming o remotos autorizados se conecten con facilidad a los recursos corporativos de la red de área local (LAN). Así como las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de N). Por último, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público. Lo mismo se aplica en el caso de datos sensibles que viajan a través de una red corporativa. Por lo tanto, una VPN debe presentar los siguientes requerimientos básicos:

Autenticación de usuario.

La solución deberá verificar la identidad de un usuario y restringir el acceso de la VPN a usuarios autorizados. Además, deberá proporcionar registros de auditoria y registros contables para mostrar quién accedió a qué información, y cuándo lo hizo.

⁸ HABRAKEN, Joe. "Routers Cisco". Editorial Prentice Hall. España

Administración de dirección.

La solución deberá asignar una dirección al cliente en la red privada, y asegurarse de que las direcciones privadas se mantengan así.

Encriptación de datos.

Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

Administración de llaves.

La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

Soporte de protocolo múltiple.

La solución deberá manejar protocolos comunes utilizados en las redes públicas; éstos incluyen protocolo de Internet. Una solución de VPN de Internet basada en un Protocolo de túnel de punto a punto (PPTP).⁹

1.2.5. Tipos de VPN**VPNs Y ACCESO REMOTO (Remote Access VPN)**

La mayoría de las compañías necesitan proveer acceso remoto a los empleados. Generalmente se utiliza una conexión dial-up (DUN) del cliente al servidor de acceso remoto (RAS) vía módems. Para acceso remoto VPN hay que considerar, la tecnología en la Workstation cliente, qué sucede entre el cliente y el servidor VPN, el servidor VPN y finalmente la relación con el usuario remoto. El usuario remoto puede ser un empleado o individuo de menor confianza (un consultor a compañero de negocios).

Usualmente, el cliente de la Workstation estará corriendo bajo el SO Windows, pero podrá ser una estación MAC, Linux o Unix. SOs pre W2K y Workstation que no sean Microsoft imponen algunas limitaciones sobre los tipos de protocolos VPN y autenticaciones que se pueden usar.

Para SOs pre-Win2k se pueden eliminar algunas de estas limitaciones haciendo un download desde Microsoft.

⁹ HABRAKEN, Joe. "Routers Cisco". Editorial Pretince Hall. España

Cómo accede el usuario remoto al VPN Server vía Internet no es de importancia. Pero si debe considerarse el ancho de banda apropiado para que la conexión tenga sentido. Normalmente los proveedores de Internet (ISP) no bloquean los protocolos que se utilizan. Sólo puede haber problemas en el caso de que el usuario remoto trate de conectarse al VPN Server (vía Internet) desde dentro de una red (un empleado visitando un cliente o proveedor) y deba pasar un firewall. Para este tipo de situaciones, una solución es un http-tunnel, que permite llegar a Internet vía el puerto 80 de http y entonces establecer el túnel VPN. Una vez que el usuario remoto "disca" al número IP del servidor VPN se ingresa a la etapa de autenticación y autorización. Básicamente: ¿quiénes usted?: Nombre de usuario y password y luego, ¿de qué modo lo autorizo a entrar en la red? (horario, protocolo).

Toda ésta infraestructura deberá ser configurada por el administrador para garantizar seguridad. Según el protocolo en uso y el SO en el servidor VPN y usuario remoto, existirán diferentes modos de autenticar (passwords tradicionales, certificados de usuario, tokens o biometrica).

Finalmente si se desea que el usuario remoto pueda acceder a la intranet o si se lo limitará a áreas específicas. Se puede implementar esta "restricción" de diferentes modos: en el Server VPN, en los routers, o en las workstations y servers usando IPSec y políticas asociadas. En servidores VPN con W2K existe la posibilidad de usar Remote Accesses Policies (RAP). En W2K uno puede por ejemplo restringir a usuarios o grupos de usuarios en el servidor VPN un grupo local o de dominio. Por ejemplo, si un consultor de Oracle entra en Intranet, se restringe el acceso al servidor correspondiente creando un grupo llamando Oracle Consultants, y se agregan las cuentas de usuarios. Entonces mediante la consola de Routing and Remote Access (RRAS) se agrega una política de acceso remoto, se lo linkea al grupo Consultas y se agrega un filtro IP a la política que limite el tráfico del usuario remoto a destino, el servidor Oracle.

SITE-TO-SITE VPN (VPN entre sitios)

Site-to-site conecta la LAN de una empresa que posee diferentes ubicaciones geográficas, para ello emplea un link VPN a través de Internet, reemplazando así líneas dedicadas que en general son muy caras. Todo lo que se necesita es un servidor W2K en cada sitio conectado a la LAN local.

Este escenario no requiere autenticación de usuario pero sí deben autenticarse los servidores VPN entre sí.

Cuando se establece la conexión VPN, uno de los servidores VPN asume el rol de cliente e inicia una conexión con otro servidor VPN.

Después de establecida la conexión VPN, los usuarios de cada sitio pueden conectarse a los servidores como si estuvieran en la misma red local.

De acuerdo con el protocolo y el SO instalado en los servidores VPN, se puede basar la autenticación site-to-site en contraseñas asociadas con cuentas de usuario creadas para cada servidor, en llaves secretas pre-acordadas o en certificados para cada máquina emitidos por una autoridad certificadora (CA, Certificate Authority).¹⁰

EXTRANET VPN

Permite conectar la red de una empresa con uno o más "partners". Este escenario es muy similar a site-to-site aunque existen pequeñas diferencias. Básicamente la confianza entre ambas partes es diferente. Se permitirá a una sucursal acceder a todos los recursos de la red corporativa (site-to-site), pero es posible limitarlos para un partner. Normalmente se les restringirá a sólo unos cuantos servidores de la red. Con el tipo de restricción ya descritos en Remote Access, podemos solucionar el problema. La segunda diferencia con site-to-site es que muy probablemente nuestro "partner" use una solución VPN diferente. Aparece aquí un problema de interoperabilidad a resolver. Para ello, se deberá atender, por ejemplo, a qué protocolos se usan en ambas soluciones VPNs y a qué tipo de autenticación se usará.¹¹

1.2.6. Topologías de VPN

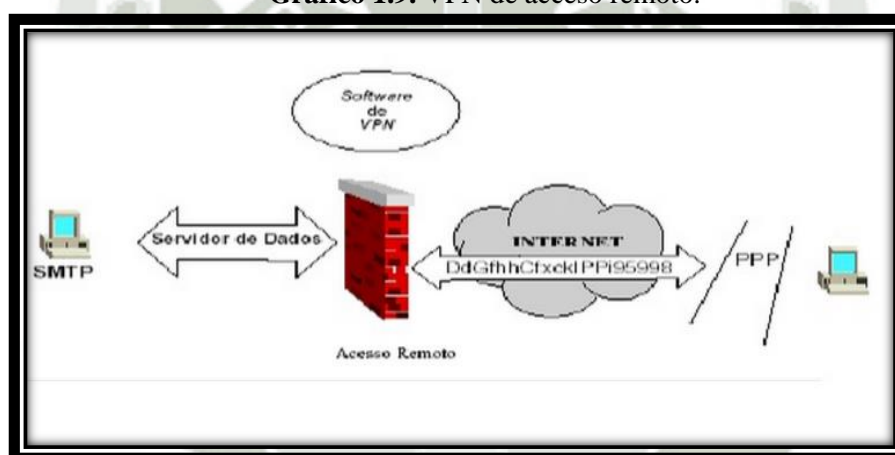
Existen muchos tipos de topologías de VPN que pueden adecuarse a las necesidades de una organización o se adaptan a una configuración de red que ya existe. Estas topologías pueden ser definidas a través de acceso remoto (por ejemplo, una laptop tratando de acceder a un servidor de su organización), conexión entre dos LANs (Local Área Network), a través de Intranet e Extranet, utilizando una tecnología Frame Relay e ATM, VPN con Black-Box, VPN utilizando NAT (Network Address Translation). Examinaremos ahora cómo funcionan algunas de las topologías de VPN más usadas.

¹⁰ <http://www.cisco.com/>

Topología de VPN utilizando acceso remoto (firewall -cliente)

Este tipo de VPN es el más común y más usado en nuestros tiempo. Nace de la necesidad de un cliente externo que se necesita conectarse a la red interna de una organización. Para que esto sea posible, la organización precisara tener un firewall instalado conteniendo los softwares necesarios para implementar a VPN. El cliente tiene que tener también instalado un software de criptografía compatible con el software del firewall. La comunicación ocurre cuando un cliente necesita de una organización confidencial con la organización, y sin embargo no se encuentre localizado dentro de la empresa, o tal puede surgir si el cliente necesita acceder al servidor de organización a partir de una red externa. La figura inferior ilustra cómo se establece este tipo de comunicación.¹²

Gráfico 1.9. VPN de acceso remoto.



Fuente: (Cisco System, 2001),

Los pasos siguientes describen el proceso de comunicación entre el equipo portátil y el firewall de la organización:

- El usuario con el equipo portátil marca a su PSI local y establece una conexión PPP.
- El equipo portátil solicita las claves del dispositivo del firewall.
- El firewall responde con la clave apropiada.
- El software VPN instalado en el equipo portátil ve la solicitud hecha por el

¹² Cisco System, 2001

usuario del equipo portátil, cifra el paquete y lo envía a la dirección IP pública del Firewall.

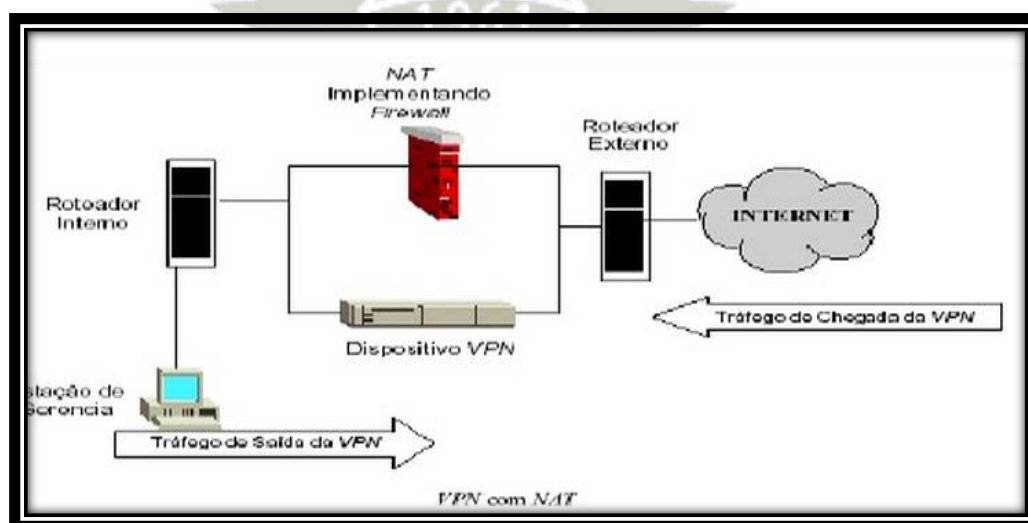
- El firewall le quita la dirección IP, descifra el paquete y lo envía al servidor al que ha sido direccionado dentro de la LAN local.
- El servidor interno procesa la información recibida, responde a la solicitud y envía el documento de regreso.
- El firewall examina el tráfico y reconoce que es información de túnel VPN así que toma el paquete, lo cifra y lo envía al equipo portátil.
- La pila de VPN en el equipo portátil ve el flujo de datos, reconoce que viene del dispositivo firewall, descifra el paquete y lo maneja en aplicaciones de niveles.

TOPOLOGIA DE VPN UTILIZANDO NAT

(Network Address Translation) Traducción de Direcciones de Nombres es el proceso de cambiar una dirección IP de una organización (una dirección privada de la organización) por una dirección IP pública enrutable, es decir poseen la capacidad para esconder las direcciones privadas de una organización.

Entretanto, el NAT interfiere directamente en la implementación de la VPN, pues cambia la dirección IP a la hora que el paquete de datos sale de la red interna. La utilización de NAT no resulta complicada, pero la ubicación del dispositivo VPN es importante. La figura inferior ilustra el proceso.

Gráfico 1.10. Diagrama VPN con Nat



Fuente: (Cisco System, 2001),

Los pasos siguientes describen el proceso de comunicación de entrada y salida con un dispositivo NAT

- Cuando un paquete precisa salir de la red interna, este es enviado hacia el Firewall implementado con NAT. Este por primera vez, cambia la dirección IP enrutable.
- El firewall implementado con NAT reenvía el paquete al dispositivo VPN que realiza el proceso de cifrado del paquete.
- El paquete es enviado hacia el enrutador externo que sea transmitido a su destino.
- Cuando un paquete quiere entrar a una red interna debe primero dirigirse hacia el dispositivo VPN que verifica su autenticidad. Luego este paquete es ruteado hacia el firewall implementado con NAT que cambia la dirección IP por el número original, este es enviado hacia el ruteador interno para ser dirigido hacia su destino.

1.2.7. Protocolos de la VPN

Los conocimientos que fundamentan a una VPN son una criptografía y un tunelamiento. Una criptografía se utilizada para garantizar la autenticación, confidencialidad e integridad de las conexiones y es la base para la seguridad de las redes; mas el tunelamiento es el responsable por el encapsulamiento y transmisión de los datos sobre una red pública entre dos puntos distintos. Dentro del mercado existen diversos protocolos que nos proporcionan este servicio y que difieren entre si dependiendo del nivel del modelo ISO/OSI donde actúan, de la criptografía utilizada y de cómo influye directamente el nivel de seguridad en el acceso remoto VPN.

Características básicas de un análisis de seguridad:

Las características básicas de un análisis de seguridad de los principales protocolos utilizados actualmente para acceso remoto VPN en plataformas ya sea Windows Linux o Unix son las siguientes:

POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

Point-to-Point Tunneling Protocol, es un protocolo que fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3 Com Corporation, Microsoft, y ECI Telematics para proveer una red privada virtual entre usuarios de acceso remoto y servidores de red.

Como protocolo de túnel, PPTP encapsula data gramas de cualquier protocolo de red en data gramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

La idea básica de PPTP es la de dividir las funciones de acceso remoto de tal modo que las personas de las empresas pudiesen utilizar una infraestructura de Internet para proveer una conectividad segura entre clientes remotos y redes privadas, es por eso que PPTP provee un mecanismo para tunelamiento de trafico PPP (Point to Point Protocol) sobre redes IP.

Gráfico 1.11. Diagrama del protocolo PPTP



Fuente: (Cisco System, 2001),

El PPTP es un protocolo de red que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una Red Privada Virtual (VPN) basada en TCP/IP. PPTP soporta múltiples protocolos de red (IP, IPX y NetBEUI) y puede ser utilizado para establecer dichas redes virtuales a través de otras redes públicas o privadas como líneas telefónicas, redes de área local o extensa (LAN's y WAN's) e Internet u otras redes públicas basadas en TCP/IP.

Una red privada virtual consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el Point-to-Point protocolo (PPP), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa también remota, LAN o WAN, por un dispositivo PPTP. La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing

Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión. El paquete PPTP está compuesto por un header (encabezamiento) de envío, un header IP, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como es, direcciones de origen y destino, longitud del data grama enviado, etc.¹³

El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. El paquete de carga es el paquete encapsulado, que en el caso de PPP, el data grama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros.

La siguiente figura ilustra las capas del encapsulamiento PPTP. Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y acepta cualquier tipo, inclusive texto plano. Si se utiliza CHAP (protocolo de autenticación por reto), standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Authentication Protocol), que no encripta las contraseñas. Para la encriptación, PPTP utiliza el sistema RC4.

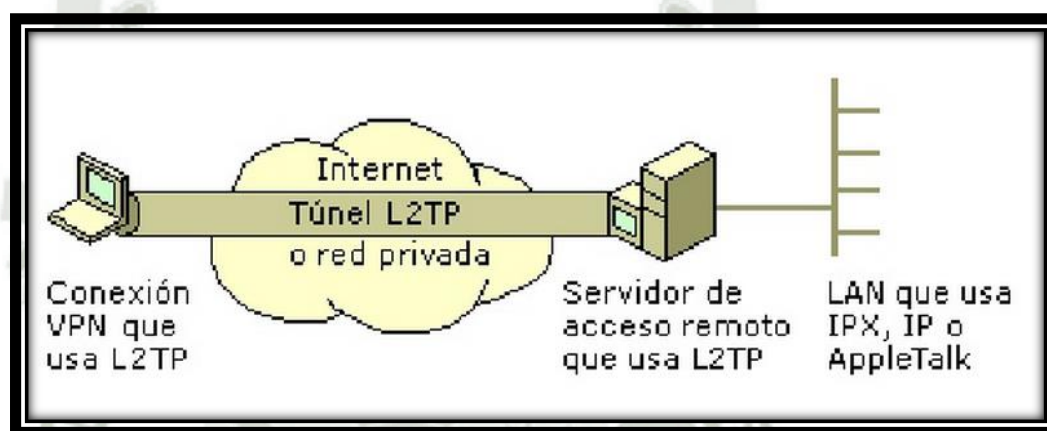
LAYER TWO TUNNELING PROTOCOL (L2TP)

Layer Two Tunneling Protocol es una extensión del PPTP (Point-to-Point Protocol), que mezcla lo mejor de los protocolos PPTP de Microsoft y L2F de Cisco. Los dos componentes principales del L2TP son: El LAC (L2TP Access Concentrator), que es el dispositivo que físicamente termina una llamada; y el LNS (L2TP Network Server), que es el dispositivo que autentifica y termina el enlace PPP. L2TP utiliza

¹³ Cisco System, 2001

redes conmutadas de paquetes para hacer posible que los extremos de la conexión estén ubicados en distintas computadoras. El usuario tiene una conexión L2 al LAC, el cual crea el túnel de paquetes PPP. Así, los paquetes pueden ser procesados en el otro extremo de la conexión, o bien, terminar la conexión desde un extremo. L2TP soporta cualquier protocolo incluyendo IP, IPX y AppleTalk, así como también cualquier tecnología de backbone WAN, incluyendo Frame Relay, modos de transferencia asíncrono ATM, X.25 y SONET.

Gráfico 1.12. Diagrama del protocolo L2TP



Fuente: (Cisco System, 2001)

IP SECURITY IPSec (Internet Protocol Security)

IPSec es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.¹⁴,

¹⁴ (Cisco System, 2001)

1.2.8. Ventajas e Inconvenientes

VENTAJAS

- Una VPN permite disponer de una conexión a red con todas las características de la red privada a la que se quiere acceder. El cliente VPN adquiere totalmente la condición de miembro de esa red, con lo cual se le aplican todas las directivas de seguridad y permisos de un ordenador en esa red privada, pudiendo acceder a la información publicada para esa red privada a través de un acceso público. Al mismo tiempo, todas las conexiones de acceso a Internet desde el ordenador cliente VPN se realizarán usando los recursos y conexiones que tenga la red privada.
- Representa una gran solución en cuanto a seguridad, confidencialidad e integridad de los datos y reduce significativamente el costo de la transferencia de datos de un lugar a otro.
- Simplifica la integración y crecimiento de una Red ya que la VPN provee una solución propietaria flexible y escalable para su implementación y crecimiento.
- Permite la integración de diversos ambientes computacionales en una sola red de información cohesiva. Esto se debe fundamentalmente a estar basado en estándares abiertos.
- Minimiza el costo de administración y soporte de la red. Las VPN ayudan a aumentar la productividad del personal de soporte y administración de la red.
- Provee un punto central para la distribución de software y updates, manuales, etc. El browser al ser único, reduce los costos de entrenamiento de personal, pues emplea aplicaciones existentes o nuevas manteniendo la misma apariencia a través de todas las aplicaciones.

INCONVENIENTES

- Mayor carga en el cliente VPN puesto que debe realizar la tarea adicional de encapsular los paquetes de datos, situación que se agrava cuando además se realiza encriptación de los datos; lo cual origina que las conexiones sean mucho más lentas.
- Mayor complejidad en el tráfico de datos que puede producir

- Redes Virtuales Privadas efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o numero IP)
- Las VPN primero deben establecer correctamente las políticas de seguridad y de acceso.¹⁵

1.3. SERVIDOR RADIUS

Cuadro 1.3. Cuadro Comparativo TACAS vs RADIUS

	Tacacs+	Radius
funcionalidad	Separa las funciones AAA en elementos distintos. Authentication está separado de authorization, y ambos son separados de Accounting	Combina algunas de las funciones de authentication y authorization. Se puede detallar la capacidad de accounting a la hora de configurar.
Estándar	Propietario Cisco,	Estándar abierto y soportado por muchos vendedores
confidencialidad	Todos los paquetes son encriptados entre los servidores ACS y los clientes.	sólo la contraseña se encripta con respecto a los paquetes enviados de ida y vuelta entre el servidor ACS y el cliente
Granular command por autorización de comandos	Esto es un soporte con lo cual podemos permitir mediante reglas en el servidor cual o cuales comandos son habilitados o deshabilitados	No tiene dicha función
Accounting	Tiene soporte para accountig	Proporciona mayor soporte para accountng que TACACS+

Comentario: Como se puede observar en la tabla anterior una de las decisiones porque se eligió Radius, es que es un estándar completamente abierto además de que hoy en día existe un sinnúmero de proveedores de aplicaciones y equipos que trabajan con el estándar de Radius en cambio TACACS+ es un estándar propio de CISCO por consiguiente si queremos trabajar con dicho estándar se tiene que trabajar forzosamente con equipos y aplicaciones de CISCO y esto supone una gran inversión económica.

¹⁵ Cisco System, 2005

1.3.1. Introducción

Radius es un protocolo de control de acceso que autentica usuarios a través de un método muy común denominado genéricamente desafío/respuesta. El proceso que lleva a cabo se denomina AAA.

El proceso de AAA se puede sintetizar en las siguientes preguntas que realiza el servidor de acceso al cliente:

- ¿Quién eres?
- ¿Qué servicios estoy autorizado a darte?
- ¿Qué hiciste con los servicios mientras los usabas?

La Autenticación es el proceso de verificar la identidad que ha declarado un cliente (máquina o persona). Uno de los métodos más comunes para realizar esta tarea es utilizar un nombre de usuario y una contraseña.

El objetivo principal de este proceso es formar una relación de confianza entre el cliente y el servidor. El proceso de Autorización consta de un conjunto de reglas para decidir qué puede hacer un usuario autenticado en el sistema. Las reglas son definidas por los administradores del sistema.

El Registro es el proceso que documenta el uso de los recursos hecho por los usuarios que acceden al sistema. Los datos recabados por el proceso de Registro se pueden utilizar para controlar autorizaciones realizadas, cobrar la utilización de recursos, medir tendencias en el uso de recursos, y para realizar actividades relacionadas con la planificación del crecimiento.

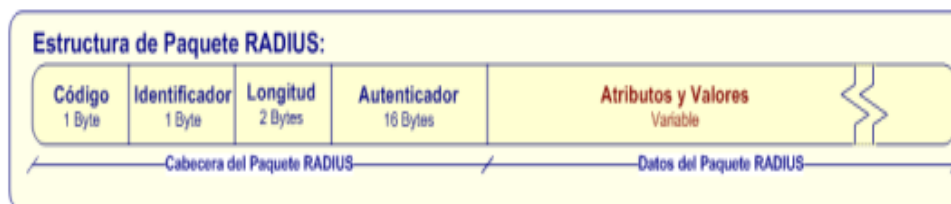
1.3.2. Características de Radius:

Las características generales del protocolo, definidas en la RFC2865, son:

- Usa un modelo Cliente/Servidor, donde el modelo de seguridad que se utiliza se denomina hop-by-hop, y se basa en un secreto compartido entre el NAS1 y el Servidor que no se transmite en la red.
- Utiliza UDP/IP para las conexiones.
- Es un protocolo stateless, es decir sin estado
- Soporta una gran variedad de métodos de autenticación, que otorgan una gran flexibilidad. Soporta PAP, CHAP, EAP, Unix, entre otros.

- El protocolo es extensible. Todas las transacciones utilizan un trío de valores Atributo-Longitud-Valor, y permite agregar definiciones de valores sin comprometer el funcionamiento de las implementaciones existentes.¹⁶⁾

Gráfico 1.13. Estructura del paquete Radius



Fuente: (Cisco System, 2001)

El protocolo se comunica a través de los puertos UDP/1812 y UDP/1813. En el gráfico se puede apreciar la estructura del paquete Radius. En el Cuadro 1.2 se puede observar el significado de los campos del paquete Radius. (Yago Fernández Hansen, 2001)

Cuadro 1.4. Significado de los campos del paquete Radius (radius, 2015)

Campo	Descripción
Código	Este campo es el que distingue el tipo de mensaje Radius. Los paquetes con código inválido se descartan. Los códigos permitidos son: Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, Access-Challenge, Status-Server, Status-Client, Reservado.
Identificador	Este valor se utiliza para relacionar una respuesta a una solicitud. También permite que el servidor Radius detecte las solicitudes duplicadas que se realizan en un corto período de tiempo, comparando la dirección IP y el puerto UDP origen, junto con el identificador.
Longitud	Indica la longitud (incluye Código, Identificador, Longitud, Autenticador y Datos) y si el paquete es más largo se descarta el excedente y si el paquete es más corto se descarta. Las longitudes válidas oscilan entre 20 bytes y 4096 bytes
Autenticador	Con este valor se verifica la integridad de los datos. Existen dos tipos diferentes de valores: Solicitud y Respuesta. El primer valor se calcula de forma aleatoria. El segundo valor se calcula con el algoritmo MD5 en función de los siguientes parámetros: Código, Identificador, Longitud, Autenticador de la solicitud, Datos, Secreto).
Atributos y Valores	Este campo de longitud variable es el contiene los pares, atributo valor que intercambia el servidor con el NAS.

¹⁶ Yago Fernández Hansen, 2001

En los procesos de Autenticación y Autorización son relevantes cuatro tipos de paquetes: Access-Request, Access-Accept, Access-Reject, y Access-Challenge. El primer paso del proceso de autenticación lo ejecuta el usuario. El cliente solicita acceso a un servicio particular al enviar al Servidor Radius un paquete del tipo Access-Request. El paquete debe contener ciertos atributos que son significativos para el proceso de autenticación. Por ejemplo, debe contener atributos que identifiquen al NAS (NAS-IPAddress y/o NAS-Identifier), la contraseña del usuario (User-Password o CHAP-Password) y debería contener nombre de usuario (User-Name) y el puerto de conexión (NAS-Port y/o NAS-Port-Type). El paquete AccessRequest puede contener atributos adicionales. Si el atributo UserPassword está presente, no debe transmitirse en texto plano, sino utilizando un hash MD5. Al recibir el paquete, el servidor debe determinar y comunicar si el usuario tiene permitido el acceso a través del NAS y al tipo de servicio que ha solicitado. Todos los paquetes válidos de este tipo deben ser contestados por el servidor, ya sea con un paquete del tipo Access-Accept, del tipo Access-Reject o del tipo Access-Challenge.

Una vez que el servidor ha procesado un paquete tipo AccessRequest y ha determinado que todos los atributos son aceptables y se puede conceder acceso al usuario, envía un paquete del tipo AccessAccept. Este paquete debe proveer la información necesaria para realizar configuración específica a fin de comenzar con la utilización del servicio. El campo Autenticador debe contener la respuesta correcta para el campo Autenticador de paquete tipo Access-Request que ha recibido previamente. El servidor puede enviar al usuario un desafío que requiera de una respuesta para disminuir el riesgo de una autenticación fraudulenta.

Si este es el caso se envía al cliente un paquete del tipo Access-Challenge al que el cliente debe responder con un paquete del tipo Access-Request que incluya los atributos apropiados. En el paquete Access-Challenge se pueden incluir uno o más atributos Reply-Message y un atributo State. Adicionalmente sólo se puede incluir alguno de los siguientes atributos: Específicos-del-Fabricante, Idle-Timeout, Session-Timeout o Proxy-State. Si el servidor determina, al procesar el paquete Access-Request, que debe negar el acceso porque alguno de los atributos recibidos no es aceptable (por política de sistema, privilegios insuficientes u otro criterio), debe enviar un paquete del tipo Access-Reject.

Este tipo de paquete puede incluir uno o más atributos Reply-Message con el texto que el NAS debe mostrar al usuario y uno o más atributos Proxy-State.

No se permiten otro tipo de atributos. Los paquetes del tipo Access-Reject pueden ser enviados en cualquier instancia de una sesión, por lo que son muy útiles para aplicar límites de tiempo en la duración de la sesión. Una vez que se lleva a cabo el proceso de autenticación puede empezar el proceso de Accounting o Registro, para esto usa el puerto 1813/UDP. El cliente (NAS o Proxy Server) envía un paquete del tipo Accounting-Request al Servidor de Accounting Radius. Este servidor puede ser el mismo servidor Radius utilizado para los procesos de Autenticación y Autorización u otro servidor configurado para tal propósito. Este paquete de tipo Accounting-Request, denominado AccountingStart, transmite la información que se registrará como utilización del servicio por parte del usuario. Al recibir este paquete el servidor debe transmitir un paquete del tipo Accounting-Response si puede almacenar satisfactoriamente el contenido del paquete y no debe transmitir ninguna respuesta si existe algún tipo de falla en el proceso de almacenamiento. A excepción de los atributos User-Password, CHAP-Password, ReplyMessage y State, se pueden enviar todos los atributos que pueden estar en un paquete Access-Request o Access-Accept. El paquete AccountingRequest debe contener el atributo NAS-IP-Address y/o NAS-Identifier. Si está presente en el paquete o si estuvo presente en el paquete Access Accept, el atributo Framed-IP-Address debe contener la dirección IP realmente asignada al usuario. Cuando el cliente finaliza una sesión envía un paquete Accounting Request, denominado Accounting-Stop, que incluye las estadísticas de uso (duración de la sesión, volumen de datos transferidos, etc.). El servidor debe confirmar que pudo almacenar esta información con éxito enviando un paquete tipo Accounting-Response.

El cliente debería reenviar el paquete Accounting-Response hasta que el servidor confirme la operación de almacenamiento. Como se puede apreciar en los procesos AAA, Radius transporta toda la información necesaria para llevar a cabo estos procesos en Atributos (Yago Fernández Hansen, 2001).

1.4. APLICACIÓN NAGIOS

1.4.1. ¿Cómo Funciona?

Nagios es un sistema de supervisión de red y aplicación. Este nos permite observar Hosts y servicios que nosotros especifiquemos, además de alertar cuando sucesos inesperados ocurren en los Host y cuando estos están en buen estado.

Nagios fue originalmente diseñado para correr bajo LINUX, aunque también debería funcionar en la mayoría de otros UNIX.

Algunas de las muchas características de Nagios incluyen:

Seguimiento de los servicios de red (SMTP, POP3, HTTP, FTP, PING, etc.)

Seguimiento de los recursos de Host (carga del procesador, uso de disco, etc.)

Diseño simple de plug-ins que permite a los usuarios desarrollar fácilmente sus propios chequeos de servicios. Chequeo de Servicios de red y/o Recursos de Host en paralelo Servicio de notificaciones a contactos cuando se producen problemas en los Hosts a través del correo electrónico, mensajes a celular vía SMS, o un método definido por el usuario. Rotación automática del archivo de registro (Nagios almacena un historial de los eventos en un archivo con extensión .log y para no hacer de este archivo muy grande Nagios elimina los historiales que son muy viejos). Soporte para la implementación de la supervisión redundante de Hosts. Interfaz Web Opcional para ver el estado de los dispositivos de la red desde cualquier punto de la red, así como las alertas y el historial de los sucesos, etc.

El único requisito para el funcionamiento de Nagios es una máquina con sistema operativo Linux (o UNIX variante) y un compilador de C. Probablemente también quieren tener TCP / IP se configura, ya que la mayoría de los controles del servicio se llevará a cabo a través de la red.

Nagios es un sistema de supervisión de red y aplicación. Este nos permite observar Hosts y servicios que nosotros especifiquemos, además de alertar cuando sucesos inesperados ocurren en los Host y cuando estos están en buen estado.

Nagios fue originalmente diseñado para correr bajo LINUX, aunque también

debería funcionar en la mayoría de otros UNIX.

Algunas de las muchas características de Nagios incluyen:

1. Un servidor Web de preferencia Apache.
2. La librería GD necesaria para crear las imágenes en formato PNG utilizadas en las gráficas de estadísticas en la interfaz web de Nagios.
3. El compilador de lenguaje C GCC para la compilación e instalación de Nagios

Campos del PDU TRAP de Nagios

Cuadro 1.5. Significado de los campos del paquete Nagios

Enterprise	Agent address	Generic trap type	Specific trap code	Time stamp	Object 1 Value 1	Object 2 Value 2	Object x Value x
------------	---------------	-------------------	--------------------	------------	------------------	------------------	------------------

Enterprise:	Identifica el tipo de subsistema de gestión u objeto administrado que ha emitido el trap.
Generic Trap Type:	Indica uno de una serie de tipos de trap genéricos:
Generic Trap Type:	Indica uno de una serie de tipos de trap genéricos: Cold start (0): Indica que el agente ha sido inicializado o reinicializado; Warm start (1): Indica que la configuración del agente ha cambiado; Link down (2): Indica que una interfaz de comunicación se encuentra fuera de servicio (inactiva); o Link up (3): Indica que una interfaz de comunicación se encuentra en servicio (activa); o Authentication failure (4): Indica que el agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad); EGP neighbor loss (5): Indica que en sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio; Enterprise (6): En esta categoría se encuentran todos los nuevos traps incluidos por los vendedores 10 Specific Trap Code: Es usado para traps privados (de fabricantes), así como para precisar la información de un determinado trap genérico
Time Stamp:	Indica la cantidad de tiempo que ha transcurrido entre la última re inicialización de la red o el agente y la generación del TRAP.
Variables binding:	Se utiliza para proporcionar información adicional sobre la causa del mensaje

Cuadro 1.6. Cuadro comparativo software de monitoreo de redes y servicios (aplicaciones para monitoreo de red, 2015)

Nombre	Gráficas	Informes SLA	Grupos lógicos	Estadísticas	Predicción de estadísticas	Autodescubrimiento	Agentes	SNMP	Alertas	Monitorización distribuida	Método de almacenaje de datos	Licencia
Nimsoft	Sí	Sí	Sí	Sí	Sí	Sí	Con agente y sin agente	Sí	Sí	Sí	SQL	Comercial
Netscope	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	SQL	Comercial
Zyrion	Sí	En tiempo real o programados	Sí	Sí	Sí	Sí	Con agente o sin agente	Sí	Sí	Sí	SQL	Comercial
PacketTrapper	Sí	No	Sí	Sí	Desconocido	Sí	Sí	Sí	Sí	Sí	SQL	Comercial
doppler VUE	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	SQL	Comercial
CA eHealth	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Oracle	Comercial
Nagios	Sí	Sí	Sí	Sí	Sí	Sí	Sí	A través de plugin	Sí	Sí	MYSQL	GPL

Comentario: Como se pudo observar en la tabla anterior de comparaciones de aplicaciones de monitoreo una de las decisiones más importantes que se tomo es que la aplicación Nagios maneja una licencia libre, además de contar con una base de datos también libre. En cambio las otras aplicaciones trabajan con licencias comerciales lo cual supone una inversión económica, muy fuerte.

Fuente: <http://infotelecommil.webcindario.com/librostelecom/SNMP.pdf>

1.4.2. Guía de instalación de Nagios

En la página oficial de Nagios se puede obtener la documentación necesaria para poder configurar Nagios según nuestras necesidades. Esta documentación la podemos obtener del sitio oficial de Nagios la cual incluye guías rápidas de instalación las cuales están destinadas a proporcionar instrucciones sencillas de cómo instalar Nagios desde el código fuente y tener un seguimiento de una máquina local dentro de 20 minutos. En el Apéndice A se explicaran estas guías de instalación. Estas guías de instalación están disponibles para las siguientes distribuciones de Linux:

- Fedora
- Open SUSE
- Ubuntu

Las cuales son la base para la mayoría de la mayoría de las distribuciones de Linux. Si se quiere instalar Nagios en un sistema operativo o distribución de Linux diferente, es recomendable leer la guía rápida para Fedora para tener una visión general de lo que se necesita hacer ya que nombres de comandos, rutas, etc. pueden variar ampliamente a través de las diferentes distribuciones, de

modo que, lo más probable es que sea necesario modificar los pasos de la instalación y trabajar un poco más para un caso particular. Sin embargo, también se pueden encontrar guías sobre Distribuciones en particular en la página (Nagios System and Network Monitoring, por Wolfgang Barth)

1.4.3. Modificaciones después de la instalación

Una vez que Nagios se ha instalado es necesario hacer algunas modificaciones para no solo tener un seguimiento de la máquina local, en este trabajo solo se describirán los pasos para poder monitorear enrutadores y switches además de máquinas con Windows ya que es lo que más le interesa, los pasos para monitorear:

- Vigilancia de la máquina Windows
- Vigilancia de Linux / Unix máquinas
- Vigilancia Enrutadores y/o Switches
- Disponibilidad de servicios públicos (HTTP, FTP, SSH, etc.).

1.4.4. Configuración general

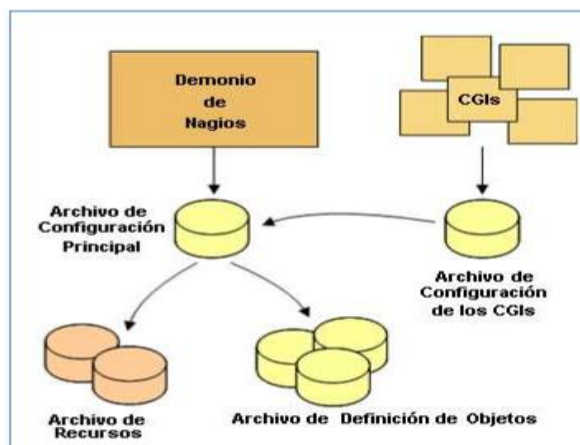
Para llevar a cabo la supervisión de los dispositivos y/o servicios mencionados anteriormente existen diferentes tipos de archivos de configuración que se necesitan crear o editar antes de iniciar el seguimiento nada. La configuración de Nagios puede tomar un buen tiempo, especialmente si es la primera vez para los usuarios. Una vez que se averigua cómo funcionan las cosas, es más fácil y vale la pena el tiempo invertido en leer la documentación.

Los archivos de configuración se instalan en el directorio:

/usr/local/Nagios/etc/

Cuando se sigue la guía de instalación rápida del Apéndice A.

Gráfico 1.14. Interacción de Nagios con los archivos de configuración



Fuente: (Nagios System and Network Monitoring, por Wolfgang Barth)

1.4.5. Archivo de configuración principal

Este archivo de configuración se instala con el nombre de *nagios*. *Cfgy* contiene una serie de directivas que afectan a la forma en que el demonio de Nagios funciona. Este archivo de configuración es leído por el demonio de Nagios y los CGIs. A partir de este archivo también se tienen acceso otros archivos de configuración como son archivos de recursos, archivos de definición de objetos y archivo de configuración CGI.

1.4.6. Archivo de recursos

Archivos de recursos pueden ser utilizados para almacenar Host definidos por el usuario. El principal punto de tener archivos de recursos es utilizarlos para almacenar la información de configuración sensible (como contraseñas), sin ponerlos a disposición de los CGIs.

La directiva *resource_file* en el archivo de configuración principal *nagios.cfges* usada para especificar uno o más archivos de recursos opcionales.

De forma predeterminada se crea un archivo de recursos con el nombre *resource.cfg* en el mismo directorio que *nagios.cfg*. Este archivo contiene la(s) contraseña(s) de cada usuario creado para entrar en la interfaz web de Nagios, por defecto el usuario debe ser “*nagiosadmin*” y la contraseña puede ser cualquiera.

1.4.7. Archivos de definición de objetos

Los archivos de definición de objetos se utilizan para definir los Hosts, servicios, grupo de Host, contactos, grupo de contactos, comandos, etc. Aquí es donde se definen todas las cosas que se desean vigilar y como se quieren controlar los mismos.

cfg_filecfg_dir: es una directiva en donde se pueden especificar uno o más archivos de definición de objetos mediante el uso de las directivas *cfg_file/ocfg_diren* el archivo principal de configuración.

El directorio por defecto dónde están estos archivos es el directorio `/usr/local/nagios/etc/objects/` y entre los archivos de ejemplo que se instalan por defecto tenemos:

- `Localhost.cfg`: en este archivo se definen todos los aspectos que queramos monitorear de la máquina donde se está ejecutando Nagios.
- `Switch.cfg`: en este archivo se especifican los aspectos que se desean monitorear de un Switch o un enrutador como puede ser interfaces Ethernet levantadas y/o caídas, el tiempo que llevan encendidos, su localización, etc.

1.4.8. Archivo de configuración CGI

El archivo de configuración CGI contiene una serie de directivas que afectan el funcionamiento de los CGIs. También contiene una referencia al archivo de configuración principal, por lo que el CGI puede saber cómo se ha configurado Nagios y por lo tanto también tiene acceso a los archivos `resources.cfg`, `localhost.cfg`, `switch.cfg`, etc.

Un CGI (*Common Gateway Interface*) o interfaz de entrada común, es una importante tecnología de la World Wide Web que permite a un cliente solicitar datos de un programa ejecutado en un servidor web.

En este caso el cliente es un explorador web por el cual entraremos a la interfaz Web de Nagios pudiendo hacerlo desde cualquier punto de la red y el servidor Web sería el equipo donde está instalado Nagios. De esta forma cuando a través de la interfaz web de Nagios observamos el estado de algún dispositivo de la red o queremos ver el historial de los sucesos que han ocurrido, los CGIs obtienen esa información de los plug-ins de Nagios y los muestra en pantalla.

En el archivo `cgi.cfg` que está en `/usr/local/nagios/etc/` instalando Nagios y creamos un usuario para la interfaz Web de Nagios se establece como “*nagiosadmin*” el nombre de usuario en este archivo. Aun cuando pongamos otro nombre de usuario se establecerá como “*nagiosadmin*”, es por ello que si ponemos otro nombre de usuario, es necesario cambiarlo manualmente, de lo contrario al entrar en la interfaz web de Nagios e ingresar el usuario y contraseña

no se podrá tener acceso. Esto debido a que los CGIs leerán el archivo cgi.cfg que tiene otro nombre de usuario registrado, entonces la página web de Nagios se nos mostrará que no tenemos permisos para observar los datos obtenidos por los CGIs.

1.4.9. Definición de Objetos

1.4.9.1. ¿Cuáles son los objetos?

Los objetos son todos los elementos que intervienen en la lógica del seguimiento y la notificación. Los tipos de objetos incluyen:

- Servicios y Grupos de servicio
- Host y Grupos de Host
- Contactos y Grupos de Contacto
- Comandos
- Períodos de tiempo
- Notificación escalada
- Notificación y ejecución de las dependencias

1.4.9.2. ¿Dónde están los objetos definidos?

Como vimos anteriormente los objetos pueden ser definidos en uno o más archivos de configuración y/o directorios que se especifique en las directivas `cfg_file`/o `cfg_dir` en el archivo principal de configuración.

Cuando se ha seguido la guía rápida de instalación, un conjunto de varios archivos de configuración de objetos se encuentran en `/usr/local/nagios/etc/objects/`. Se pueden utilizar estos archivos de ejemplo para ver cómo funciona la definición de objetos y aprender a definir su propia definición de objetos.

1.4.9.3. Explicación de los objetos

Algunos de los principales tipos de objetos se explican a continuación:

Host: uno de los objetos en la supervisión. Los atributos importantes de los Hosts son los siguientes:

- Los Hosts son generalmente dispositivos físicos de la red (servidores, estaciones de trabajo, enrutadores, interruptores, impresoras, etc.)
- Los Hosts tienen una dirección de algún tipo (por ejemplo, un IP o dirección MAC).
- Los Hosts tienen uno o más servicios asociados con ellos.

Grupos de Hosts (Host groups): Son grupos de uno o más hosts lo pueden hacer más fácil ver el estado de las máquinas relacionadas mediante ese grupo en la interfaz web de Nagios y simplificar su configuración.

Servicio (Services): Los servicios están relacionados con anfitriones y pueden ser:

- Atributos de un host (la carga de la CPU, uso de disco, tiempo de actividad, etc.)
- Los servicios prestados por el Host (HTTP, POP3, FTP, SSH, etc.)
- Otras cosas asociadas con el host (registros DNS, etc.)

Grupos de servicios (Service Groups): Son grupos de uno o más servicios. Como en el caso de los grupos de Host pueden hacer que sea más fácil ver el estado de los servicios relacionados con Nagios en la interfaz web y simplificar su configuración.

Contactos (Contacts): Son las personas a las cuales se les notificara en caso de que algún suceso anormal pase algún dispositivo de la red y tienen dos características:

- Los Contactos deben tener uno o más métodos de comunicación (mensajes SMS a celulares, correo electrónico, etc.)
- Los Contactos deben recibir las notificaciones de las máquinas y de servicios de los cuales son responsables.

Grupos de contactos (Contact groups): Son grupos de uno o más contactos.

Periodos de tiempo (Time periods): Se utilizan para el control de:

- Cuando los hosts y servicios pueden ser monitoreados
- Cuando los contactos pueden recibir notificaciones

Comandos (*Commands*): Se usan para decirle a Nagios qué programas, scripts o plug-ins se deben ejecutar para llevar a cabo:

- Chequeo de Host y Servicios
- Notificaciones
- Eventos
- Y más.

1.4.10. Plug-ins de Nagios

A diferencia de muchos otros instrumentos de supervisión, Nagios no incluyen los mecanismos internos para el control de la situación de los Hosts y servicios de la red. En lugar de ello, Nagios se basa en programas externos llamados plug-ins para hacer todo el trabajo.

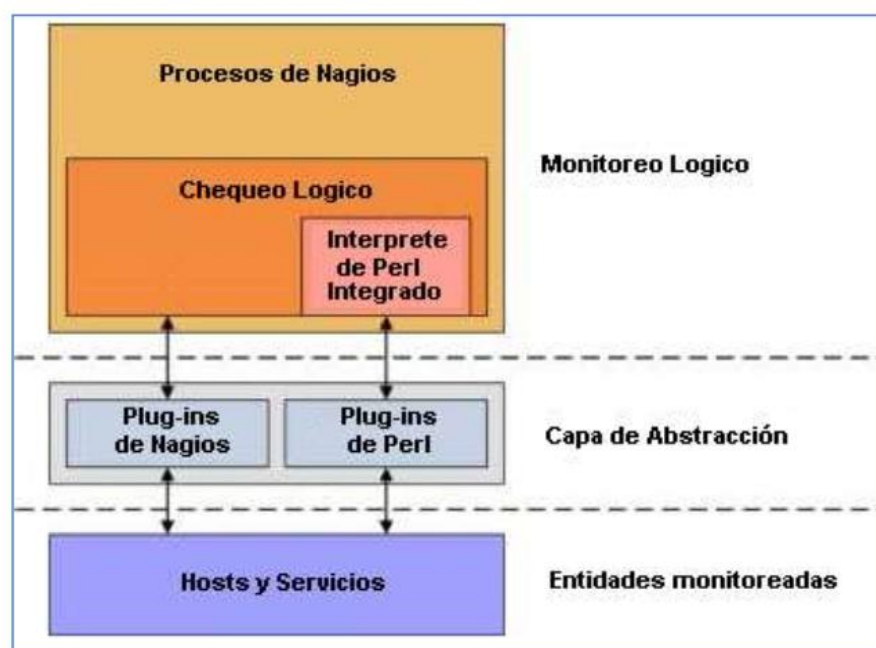
1.4.10.1. ¿Qué son los Plug-ins?

Los plug-ins son compilados ejecutables o secuencias de comandos (scripts de Perl, scripts en Shell, etc.) que se puede ejecutar desde una línea de comandos para comprobar el estado o un host o servicio. Nagios utiliza los resultados de plug-ins para determinar la situación actual de los anfitriones y los servicios en su red. Nagios ejecutará un plug-in cada vez que hay una necesidad de comprobar el estado de un servicio o de un Host. El plug-in hace algo para realizar el control y, a continuación, simplemente devuelve los resultados a Nagios este a su vez procesará los resultados que se recibe desde el plug-in y adopta las medidas necesarias (en ejecución de eventos, envío de notificaciones, etc.).

Plug-ins como una capa de abstracción

La arquitectura que utiliza Nagios en conjunto con los plug-ins ya que son estos prácticamente los que están monitoreando los dispositivos de red.

Gráfico 1.15. Arquitectura de Nagios y plug-ins (Nagios Core Documentation)



Fuente: Disponible en: <http://nagios.sourceforge.net/docs/nagioscore/4/en/>
[Consulta: 22 abril 2015].

Los plug-ins actúan como una capa de abstracción entre la lógica de vigilancia presente en el demonio de Nagios y la realidad de los servicios y hosts que se están vigilando.

La ventaja de este tipo de arquitectura de plug-in es que se puede controlar casi cualquier cosa que se pueda imaginar. Si se pudiera automatizar el proceso de control de algo, también se podría controlar con Nagios. Ya hay una gran cantidad de plug-ins que se han creado con el fin de controlar los recursos básicos, como carga del procesador, uso de disco, comprobación de conectividad mediante ping, etc.

El inconveniente de este tipo de arquitectura de plug-ins es el hecho de que Nagios no tiene absolutamente ninguna idea de qué es lo que se está monitoreando. Puede ser el monitoreo de estadísticas de tráfico de red, las tasas de error de datos, voltaje de CPU, la velocidad del ventilador, la carga del procesador, espacio en disco, o cualquier otra cosa, Nagios no entiende los detalles de esos recursos monitoreados sólo sigue pistas de los cambios en el estado de esos recursos. Sólo los plug-ins saben exactamente lo que se está monitoreando y saben cómo realizar el control real.¹⁷

¹⁷ (Nagios Core Documentation [Consulta: 22 abril 2015]. Disponible en:

1.4. TÉCNICAS Y HERRAMIENTAS

1.4.1. Técnicas

Se utilizó como técnica la información documental y trabajo en equipo

1.4.2. Herramientas

Material

- Libros de consulta de la especialidad
- Páginas web

Medios de aplicación

- Estándar IEEE802.16
- Servidor Radius
- VPN
- OLSR

1.5. ASPECTOS RELEVANTES DEL DESARROLLO.

El presente trabajo es un tema de actualidad, en razón al existente crecimiento de la población en diferentes distritos de la ciudad y el aumento de la inseguridad de Arequipa, en vista a esto es de suma importancia la cooperación de las distintas Municipalidad para poder garantizar el bienestar de los ciudadanos y comodidad que las distintas Municipalidades tiene que cooperar entre ellas, para poder realizar obras que beneficiaran a las Municipalidades involucradas, pero para ello es necesario establecer una comunicación segura para poder intercambiar datos de suma importancia entre ellas.

Es un tema de importancia, debido a que en situaciones de emergencias como: accidentes de tránsito, incendios, atenciones médicas de urgencia, etc., es necesario comunicar a las Municipalidades y Comisarías para que ellas tomen las mediciones del caso.

La motivación personal es lograr un esquema de arquitectura de seguridad de acuerdo al uso de la red y al grado de participación de los nodos en la misma, para mejorar la capacidad del protocolo de obtener “Disponibilidad, Integridad, Confidencialidad y Autenticación”.

<http://nagios.sourceforge.net/docs/nagioscore/4/en/>

2.1 PLAN DEL PROYECTO INFORMÁTICO.

	Nombre de la tarea	Fecha de inicio	Fecha de finalizac ión	Duración	Predecesoras	P2			P3		P4		
						Abr	May	Jun	Jul	Agosto	Sep	Oct	Nov
1	Definición del Plan de Tesis	12/05/15	30/06/15	38d					36d				
2	Reuniones #1	12/05/15	14/05/15	3d			3d						
3	Recolección de información	15/05/15	10/06/15	19d	2			19d					
4	Reuniones #2	11/06/15	15/06/15	3d	3			3d					
5	Planteamiento del Plan de Tesis	16/06/15	30/06/15	11d	4				11d				
6	Revisión y Aprobación del Plan de Tesis	02/07/15	04/08/15	24d					24d				
7	Primer Entregable	02/07/15	02/07/15	1d					1d				
8	Corrección del Primer Entregable	03/07/15	06/07/15	2d	7				2d				
9	Reuniones #3	03/07/15	03/07/15	1d					1d				
10	Reuniones #4	06/07/15	06/07/15	1d	9				1d				
11	Aprobación del Plan de Tesis	07/07/15	04/08/15	21d	8					21d			
12	Elaboración del Diseño	03/08/15	13/10/15	52d						52d			
13	Estudio de Viabilidad del proyecto	03/08/15	21/08/15	15d						15d			
14	Discusión de la viabilidad del proyecto												
15	Reuniones #5												
16	Especificación de requisitos del proyecto	24/08/15	23/09/15	23d	13						23d		
17	Especificación de Diseño	24/09/15	13/10/15	14d								14d	
18	Identificación de los Puntos o Nodos	24/09/15	25/09/15	2d								2d	
19	Reuniones #6	24/09/15	24/09/15	1d								1d	
20	Comprobación de Puntos o Nodos	25/09/15	25/09/15	1d								1d	
21	Diseño Logico	28/09/15	30/09/15	3d	18							3d	
22	Reuniones #7	28/09/15	30/09/15	3d								3d	
23	Comprobación del Diseño Lógico	28/09/15	30/09/15	3d								3d	
24	Diseño Fisico	01/10/15	13/10/15	9d	21							9d	
25	Reuniones #8	01/10/15	05/10/15	3d								3d	
26	Comprobación del diseño Físico	01/10/15	13/10/15	9d								9d	
27	Instalación	02/11/15	20/11/15	15d									15d
28	Implementación de OLSR	02/11/15	03/11/15	2d									2d
29	Instalación de DALORADIUS	04/11/15	06/11/15	3d	28								3d
30	Instalación de servicio de Nagios	09/11/15	11/11/15	3d	29								3d
31	Configuración de la VPN	12/11/15	17/11/15	4d	30								4d
32	Pruebas	12/11/15	20/11/15	7d									7d
33	Pruebas de conectividad	12/11/15	14/11/15	2d									2d
34	análisis de resultados	12/11/15	12/11/15	1d									1d
35	Reunion #9	14/11/15	14/11/15	1d									1d
36	Pruebas de ejecución	16/11/15	20/11/15	5d	33								5d
37	Análisis de Resultados	16/11/15	18/11/15	3d									3d
38	Reunión #10	16/11/15	20/11/15	5d									5d
39	Informe Final de Tesis	20/11/15	03/12/15	10d									10d

- **Determinación de la viabilidad.**

Se realizó una entrevista a los representantes de los grifos con mayor demanda en el Distrito de José Luis Bustamante y Rivero para conocer si se contaba con algún sistema de seguridad ante algún evento delictivo, comprobándose que sólo se

cuenta con cámaras de vigilancia, pero no tienen comunicación, ni interconexión con las autoridades policiales.

- **Viabilidad Técnica**

✓ Requerimientos:

- Antena
- Computadora
- Servidor
- Routers
- Acces Point

- **Viabilidad Económica**

Los recursos básicos que se consideraron fueron:

- ✓ El tiempo es corto, en cuanto a la instalación y puesta en funcionamiento da la propuesta.
- ✓ El costo del estudio será menor, ya que la Municipalidad ya cuenta con el servicio del Protocolo VPN
- ✓ El costo del tiempo, será asumido por los Investigadores

- **Equipos, materiales, bienes y servicios.**

DENOMINACIÓN	CANTIDAD	COSTO TOTAL
Materiales de Escritorio	1	668.00
Movilidad		120.00
Antena Ubiquiti M5	1	450.00
Servidor Radius, Nagios	1	1250.00
Router Cisco 2811 Wired Router	1	1250.00
Operador Serenazgo	1	750.00
Operador Comisaria	1	750.00
Cable de Red Cat 6 Caja AMP	1	350.00
Access Point TP LINK w8901g	3	450.00
Switch CISCO 2940	1	120.00
TOTAL		S/. 6144.00

Cabe señalar, que la investigación es un presupuesto a prueba que va ser presentado posteriormente al alcalde del distrito de José Luis Bustamante y Ribero.

Viabilidad Operativa:

✓ **Recursos Humanos:**

Moisés Vladimir Cárdenas Torreblanca
Fredy Emigdio Quispe Ruelas

✓ **Operatividad del Proyecto:**

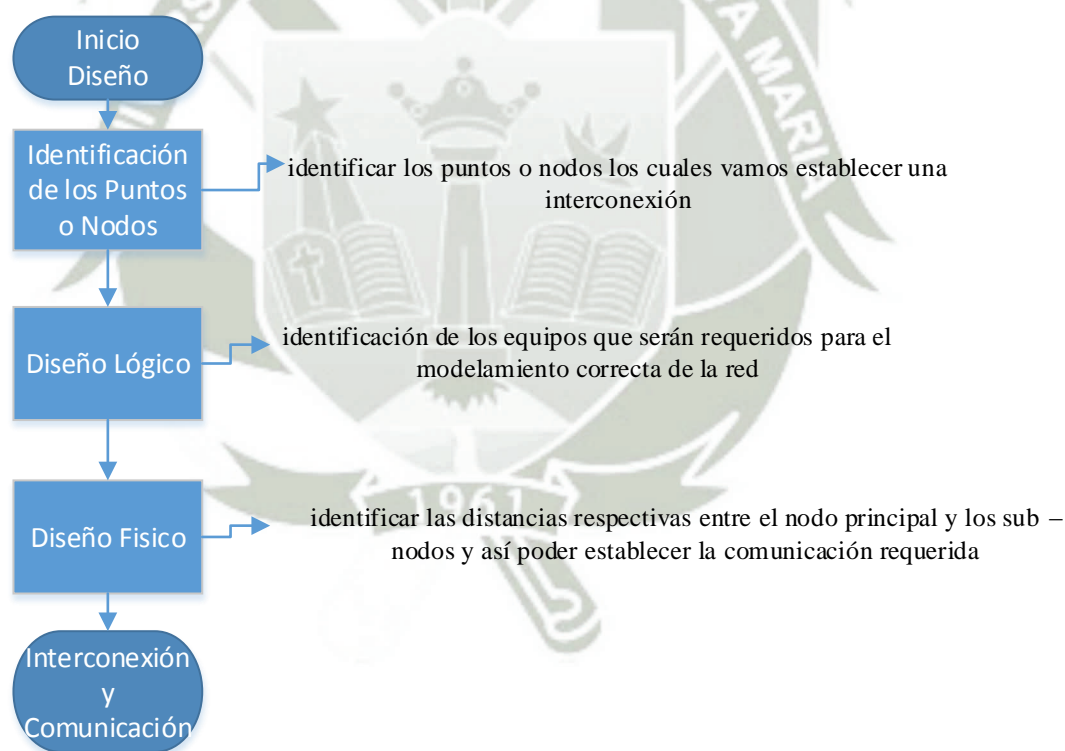
La propuesta será desarrollada e implementada en los diferentes establecimientos distribuidos de combustibles del distrito de José Luis Bustamante y Rivero y con proyección a otras empresas en otros rubros comerciales.

El servidor Radius y monitoreo Nagios, será implementado en el Municipalidad de José Luis Bustamante y Rivero.

2.2. ESPECIFICACIÓN DE REQUISITOS DEL PROYECTO

El beneficiario (grifos) deberá contar un AP y una computadora, para poder comunicarse con la Municipalidad Distrital de José Luis Bustamante y Rivero.

2.3. ESPECIFICACIÓN DE DISEÑO



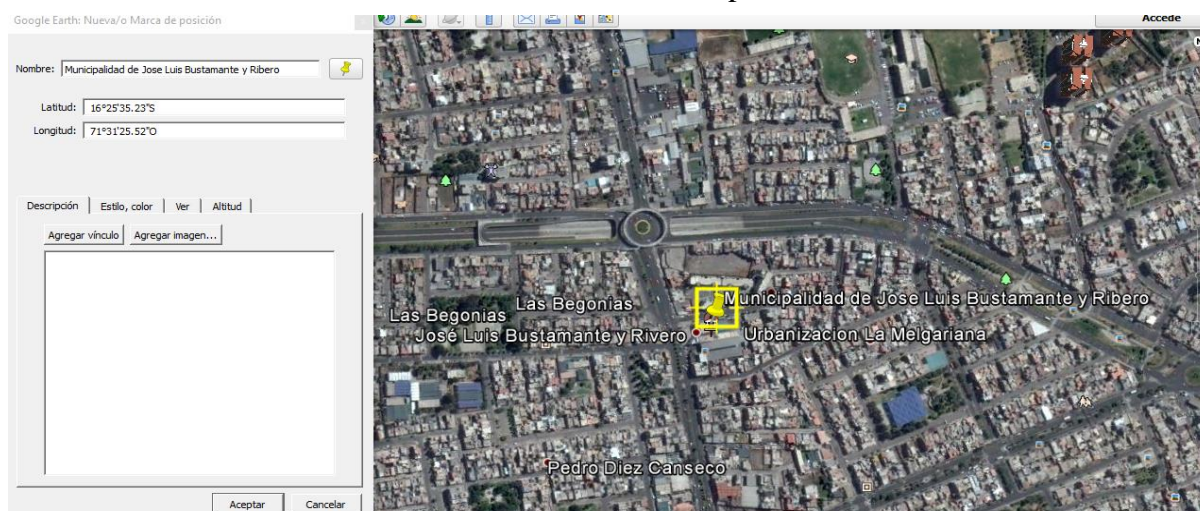
2.3.1. Diseño e Implementación de la Red

Es una metodología que proponemos se desarrolla en cinco Fases, para el diseño de redes:

I. FASE: IDENTIFICACIÓN DE LOS PUNTOS O NODOS

El primer lugar es identificar los puntos o nodos los cuales vamos establecer una interconexión para ello nos dirigimos a la aplicación de google Earth y buscamos la municipalidad de José Luís Bustamante y Ribero y anotamos las respectivas coordenadas que aparecerán en google Earth.

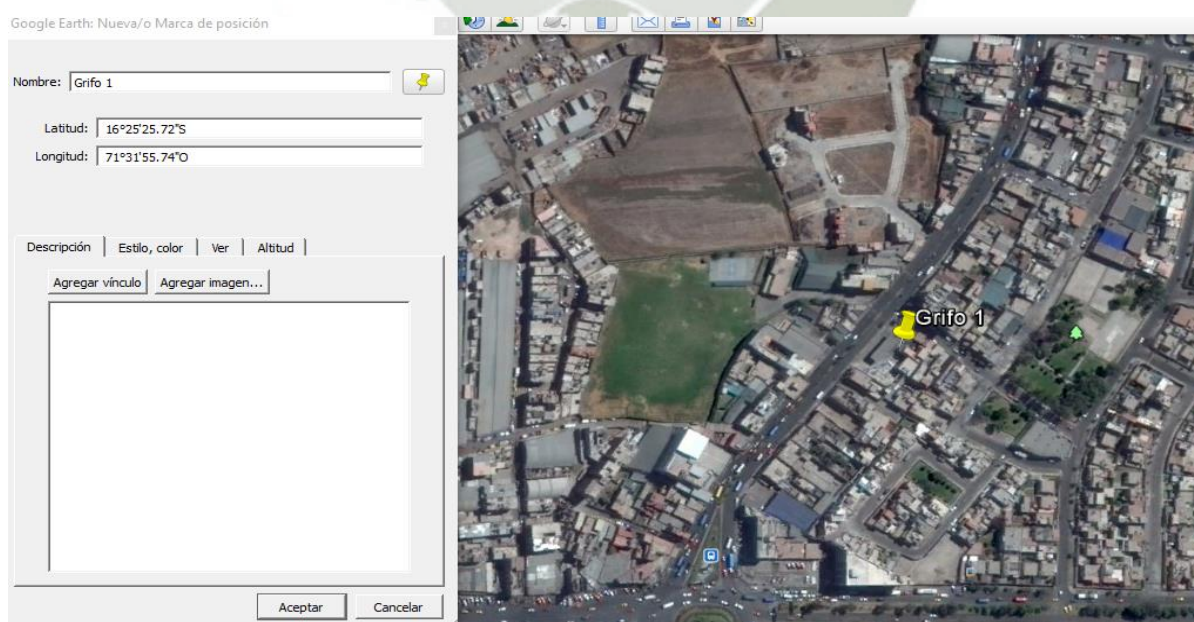
Gráfico 2.1. Identificación de puntos o nodos



Fuente: Elaboración propia

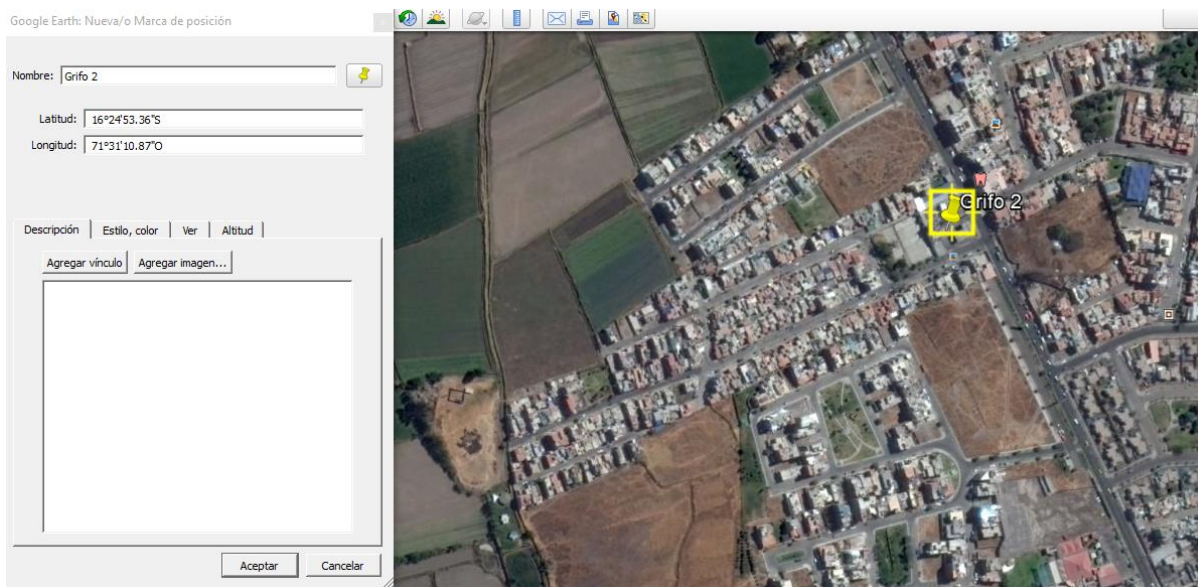
En el gráfico 2.2. Podemos observar en primer punto en este caso es el punto principal y del mismo modo identificaremos los siguiente puntos.

Gráfico 2.2. Identificación Grifo 1



Fuente: Elaboración Propia

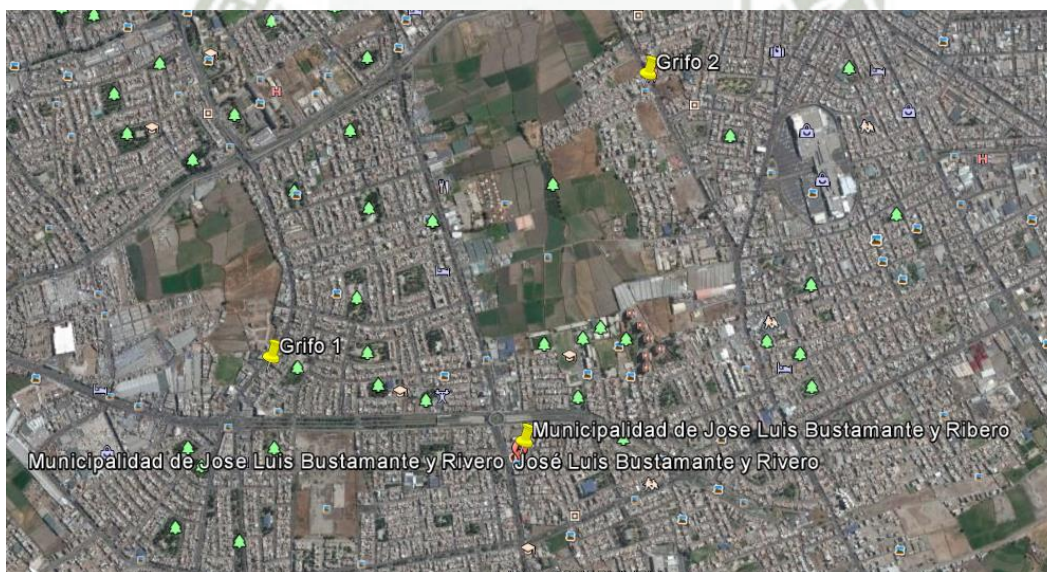
Gráfico 2.3. Identificación Grifo 2



Fuente: Elaboración Propia

Y final mente una vista global de las estaciones que deseamos comunicar.

Gráfico 2.4. Vista Global de Estaciones



Fuente: Elaboración Propia

Una vez obtenido los siguientes datos podremos trazar si la antena puesta en la Municipalidad tiene el alcance correcto para poder establecer la Red inalámbrica para ello en la Municipalidad se creara un Red temporal y mediante un testeo y la utilización del protocolo Ping comprobaremos la conectividad.

II. FASE: DISEÑO LÓGICO

En esta base lo primordial es la identificación de los equipos que serán requeridos para el modelamiento correcta de la red.

Como primer punto explicaremos el uso de cada uno de los siguientes equipos

Router: Este equipo es el que establecerá la comunicación entre dos o más Municipalidades, en este modelo comunicara a dos Municipalidades y con la ayuda del protocolo VPN podremos comunicar ambas Municipalidades encriptado los mensajes. La Municipalidad ya cuenta con dicho equipo.

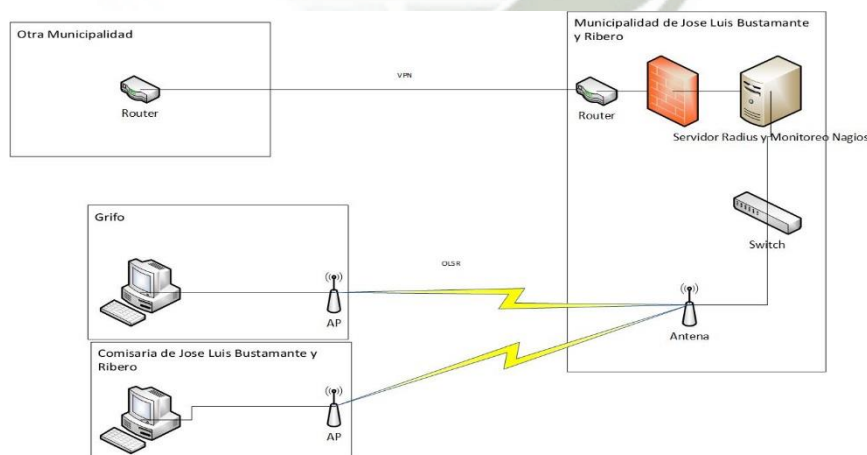
Firewall: Este dispositivo de red es el encargado de filtrar los paquetes y protocolos de comunicación que lleguen a la red privada de la Municipal de José Luis Bustamante y Rivero, tener en cuenta que dicho dispositivo es administrado por el área de Tecnología de la Información. La Municipalidad cuenta con dicho equipo.

Este dispositivo en el cual se va configurar el servicio Radius y el monitoreo Nagios para ello no es necesario que se a un equipo robusto ya que la aplicación que instalaremos y configuraremos está diseñado para el sistema operativo LINUX. Por ello no es muy necesario requerimientos de hardware muy robustos.

Switch: Dicho dispositivo de red actuara como un intercomunicador para con la cual podremos llegar a la antena respectiva.

AP: Este dispositivo de red estará ubicado en las estaciones (grifos) los cuales captaran la señal que transmite la antena ubicada en la Municipalidad de José Luis Bustamante y Rivero.

Gráfico 2.5. Proceso de Transmisión



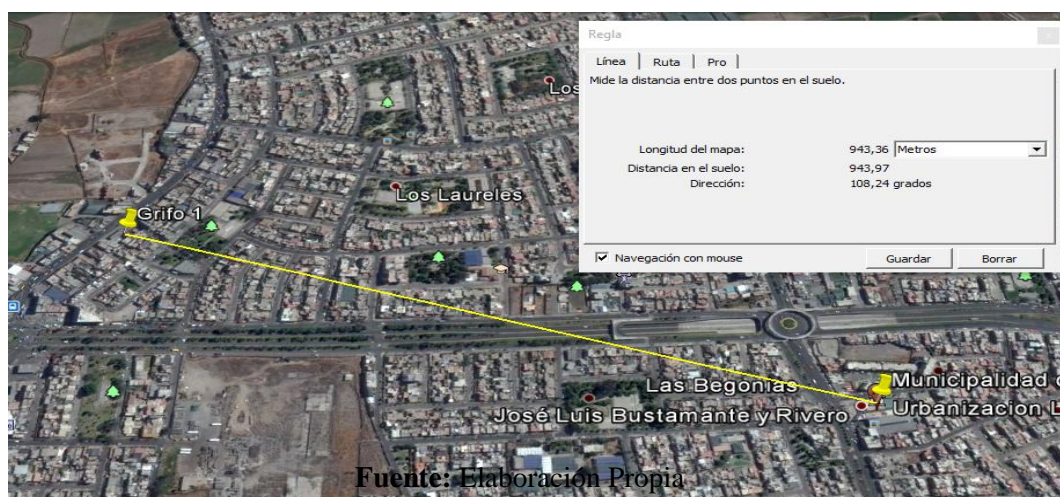
Fuente: Elaboración Propia

III. FASE: DISEÑO FÍSICO

En esta fase lo primordial es identificar las distancias respectivas entre el nodo principal y los sub – nodos y así poder establecer la comunicación requerida

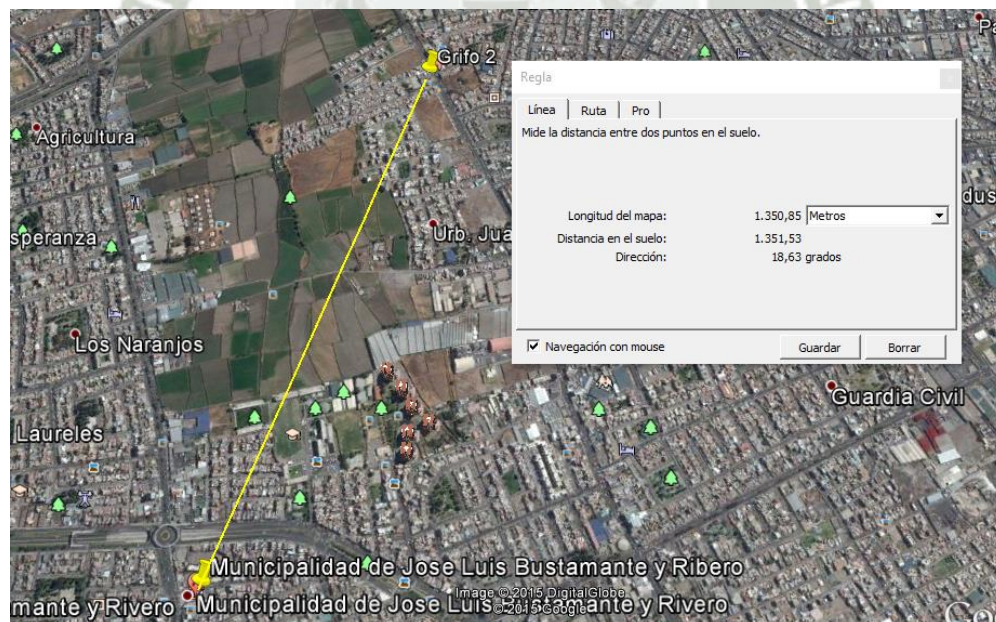
Ahora estableceremos la distancia de dichas redes y del mismo caso con la ayuda de google Earth podremos hacer dicha medida.

Gráfico 2.6. Distancia de Redes Grifo 1



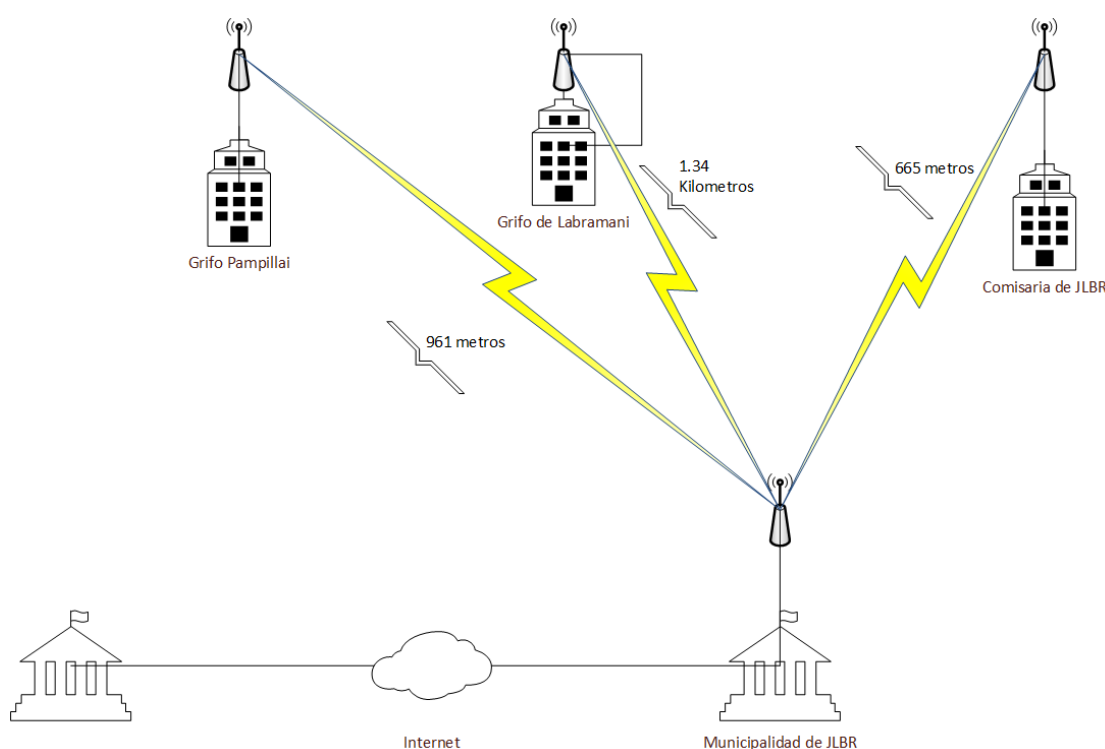
Identificamos que el primer punto tiene una distancia de 943.36 metros

Gráfico 2.7. Distancia de Redes Grifo 2



El siguiente punto tiene una distancia de 1350.85 metros

Gráfico 2.8. Interconexión y Comunicación



Fuente: Elaboración Propia

IV. INSTALACIÓN:

Una vez comprobada la señal de la antena la cual irradiara hasta los sub-nodos se comenzara con la configuración de los quipos.

Implementación de OLSR

Posteriormente se requerirá de una maquina con las siguientes características como mínimo:

- Procesador x 86 a 1 GHz.
- Memoria RAM de 1 GB.
- Disco Duro de 15 GB (swap incluida).
- Tarjeta gráfica y monitor capaz de soportar una resolución de 800x600.
- Lector de CD-ROM, puerto USB o tarjeta de red Inalámbrica.
- Conexión a Internet puede ser útil.
- Sistema operativo Ubuntu.

Se descargara el código fuente:

<http://www.olsr.org/releases/0.6/olsr-0.6.0.tar.gz>

Un vez descargado el paquete se procede a instalarlo para ello se dirige donde se descargó el paquete y se procede compilarlo e instalarlo.

`make`

`make install`

Después de la instalación es necesario modificar el archivo de configuración:

`nano /etc/olsrd/olsrd.conf`

En el archivo se indica la red a la que pertenece el host, interfaz que formara parte de la red e implementara OLSR y el modo de “debug” para ver información del protocolo.

Antes de iniciar el protocolo, es necesario que se una a la red inalámbrica creada sobre la cual actuara OLSR, para ello se realiza la siguiente configuración.

`ifconfig wlan0 down`

`iwconfig wlan 0 mode ad-hoc channel 2 essid “mesh”`

`ifconfig wlan0 192.168.10.3 up`

Es recomendable deshabilitar cualquier software de gestor de red que se utilice en la PC para que no se re-configura la interfaz Wlan0

Luego se verifica la conexión mediante el comando

`iwconfig wlan0`

Todos los nodos en la red debe tener el mismo número de celda para iniciar el protocolo para ello se utiliza el comando:

`olsrd -f /etc/olsrd/olsrd.conf`

El parámetro `-f` indica la ruta al archivo de configuración

Luego de iniciar el protocolo, se dirige a ver en pantalla para así observar todo lo aprendido por OLSR

El resultado final de OLSR se muestra en las tablas de ruteo del sistema operativo:

route-n

Implementación de Servidor Radius

Para la instalación y configuración del servidor Radius se debe ingresar al terminal e instalar los siguientes paquetes y librerías:

- apt-get install mysql-client mysql-server
- apt-get install phpmyadmin
- apt-get install php5 php-pear php5-gd php-DB

Para el servicio:

- apt-get install freeradius freeradius-mysql

Como siguiente paso se testeara al servidor con un usuario local del Sistema, usando el commando radtest(cliente para un servidor Radius).

- radtest + usuario + contraseña + 127.0.0.1 0 testing123

NOTA: Si todo está bien deberá aparecer un mensaje

- rad_recv:Access-Accept

Hasta este punto ya está instalado el servidor Radius con autenticación para usuarios del sistema LINUX definidos en /etc/passwd.

Se ingresa al directorio de Radius cd /etc/freeradius, ahí se editara el archivo de configuración radius.conf con el editor nano.

En este archivo se quitara el comentario de la línea \$ INCLUDED sql.conf (Ctrl + W), seguidamente se saldrá y guardara los cambios realizados.

Estando en dicho directorio, se va al archivo de configuración del módulo mysql

- cd sql/mysql/

Aquí hay varios archivos en los cuales se almacenan instrucciones sql y las diferentes tablas que requiere el sistema.

Ahora se procede a crear la base de datos Radius, utilizando el cliente mysql

- `Mysql -u root -p`

Se especifica el password que se ingresa cuando se hace la instalación.

Se muestra como se crea la base de datos y el usuario dándole todos los privilegios, una contraseña y demás características; “quit” para salir.

Se ingresa a las tablas de la base de datos mysql-Radius a través de:

- `mysql -u root -p radius < schema.sql`

NOTA: Con esto se insertan en la base de datos Radius las sentencias sql contenidas en el archivo schema.sql (tablas necesarias para la autenticación de usuarios con mysql).

Si no muestra ningún error significa que el INSERT Fue exitoso.

Luego se edita el archivo sql.conf (habilitar autenticación de usuarios myql)

En el directorio principal de freeradius con el editor nano se ingresa al archivo,

Aquí se cambiara el password “radiuspass” guardar y salir

Ahora se editara el archivo **sites-available**, se quita los comentarios que contengan la línea **sql (Ctrl+W)** en las secciones **authorize** y **accounting**. Opcionalmente se puede hacer lo mismo para las sesiones **sesión y post-auth**.

Creación de usuarios en la base de datos.

Se puede usar phpmyadmin o comandos sql.

NOTA: la tabla que almacena los usuarios es **radcheck**.

Se ingresa al explorador para proceder a crear los usuarios, con la URL

- `http://localhost/phpmyadmin/`

Se abre la página principal y escribimos el usuario y la contraseña, cuando se ingresa se dirige a la base de datos de **Radius** y se va a la tabla **radcheck**.

Al insertar un usuario se dirige a la pestaña “insertar”.

En este caso el usuario se llamara “la red”, el atributo será el password y el valor del password será “red administrativa” y continua.

Posteriormente se dirige a la pestaña examinar ahí se ver cada uno de los elementos en la tabla.

Se sigue haciendo una prueba de freeradius con mysql, se procede a testear el servidor con un usuario de la base de datos:

- **radtest + usuario + contraseña + el mismo servidor (127.0.0.1)+ puerto (1812) testing123**

Instalación de DALORADIUS

DALORADIUS, es una aplicación avanzada de gestión de Radius web destinada a la gestión de puntos de acceso y a las implementaciones de proveedor de internet para fines generales. Es una interfaz web que permite configurar y administrar un servidor freeradius. Se procede a descargar la aplicación, se descomprime y se le renombra como “daloradius”

Enlace de descarga:

- **<http://sourceforge.net/projects/daloradius/files>**

Se ingresa al directorio `cd /var/www/daloradius/library/` y se lista todos los archivos y se procede a editar con nano el archivo `daloradius.conf.php`; aquí se almacena toda la información acerca de las tablas y acerca del usuario de la base de datos. Por defecto viene el usuario “root”, se modifica la contraseña, y la tabla de usuarios (por defecto aparece “usergroup”), se agrega al inicio “rad” que es la tabla existente.

Estando allí se devolverá un directorio (`cd ..`) y se va a `acdcontrib/db/`, allí se encontrara algunas sentencias; en este caso solamente se necesita las sentencias contenidas en el archivo

`mysql-daloradius.sql` y se ejecuta el comando:

- **`mysql -u root -p radius < mysql-daloradius.conf`**

Y se digita el password.

Posteriormente se dirige al explorador y se coloca en la barra de direcciones:

- **`http://localhost/daloradius/`**

Por defecto aparece el usuario administrador y se ingresa la contraseña “radius”, aparece toda una consola de administración. Se puede ver el estado de los servicios (si está

habilitado), se agregara y listara los usuarios, entre otros.

Instalación del servicio de Nagios

Configure las PC's y el Router las interfaces respectivas para conseguir conectividad total.

Habilite el servicio SNMP utilizando los siguientes comandos:

```
Router(config)#snmp-server community public ro 60
Router(config)#snmp-server community private rw 60
"Creamos la comunidad pública y damos permisos de lectura y
escritura".
Router(config)#access-list 60 permit 192.168.10.142
router(config)#snmp-server enable traps
router(config)#interface f0/0
router(config-if)#ip address 192.168.10.143 255.255.255.0
router(config-if)#no shutdown
"Permitimos el acceso al equipo que va a monitorear el dispositivo".
```

En el cliente Linux se instalara el servicio de NAGIOS con ayuda del comando yum:

```
#yum install nagios nagios-plugins nagios-plugins-nrpe nagios-
devel
```

“Se procede a instalar Nagios”

Gráfico 2.9. Instalación de Nagios

```
[root@server101 yum.repos.d]# yum install nagios nagios-plugins nagios-plugins-nrpe nagios-devel
base 100% |=====| 951 B 00:00
Setting up Install Process
Parsing package install arguments
Resolving Dependencies
--> Running transaction check
--> Package nagios-plugins-nrpe.i386 0:2.14-1.el5.rf set to be updated
--> Package nagios.i386 0:3.2.3-3.el5.rf set to be updated
--> Package nagios-devel.i386 0:3.2.3-3.el5.rf set to be updated
--> Package nagios-plugins.i386 0:1.4.16-1.el5.rf set to be updated
--> Processing Dependency: fping for package: nagios-plugins
--> Processing Dependency: perl(Net::SNMP) for package: nagios-plugins
--> Running transaction check
--> Package fping.i386 0:3.4-1.el5.rf set to be updated
--> Package perl-Net-SNMP.noarch 0:5.2.0-1.2.el5.rf set to be updated
--> Processing Dependency: perl(Crypt::DES) for package: perl-Net-SNMP
--> Running transaction check
--> Package perl-Crypt-DES.i386 0:2.05-3.2.el5.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
nagios-devel i386 3.2.3-3.el5.rf base 42 k
```

Fuente: Elaboración Propia

El archivo donde almacena los usuarios y contraseñas que accederán a Nagios es htpasswd. users, por defecto no se encuentra creado, se utilizara el parámetro - c para

crear el archivo con el usuario respectivo. Cabe resaltar que la primera vez se utiliza este parámetro para crear el archivo en los posterior tendrá que omitirlo.

Configurare password del usuario nagiosadmin para acceder al administrador web de nagios.

- **#htpasswd -c /etc/nagios/htpasswd.users nagiosadmin**

“Se inserta un password al usuario nagiosadmin para poder acceder al administrador web, luego se inicia el servicio web”

Gráfico 2.10. Configuración Password del usuario nagios admin

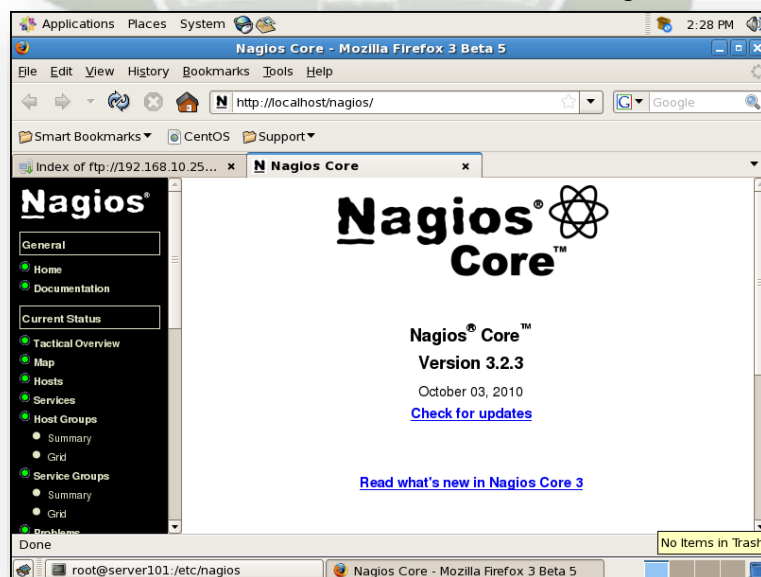
```
[root@server101 nagios]# htpasswd -c /etc/nagios/htpasswd.users nagiosadmin
New password:
Re-type new password:
htpasswd: password verification error
[root@server101 nagios]# htpasswd -c /etc/nagios/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
[root@server101 nagios]# service httpd status
httpd is stopped
[root@server101 nagios]# service httpd start
Usage: httpd {start|stop|restart|condrestart|reload|status|fullstatus|graceful|help|configtest}
[root@server101 nagios]# service httpd start
Starting httpd: httpd: Could not reliably determine the server's fully qualified domain name, u
ing 127.0.0.1 for ServerName
[ OK ]
```

Fuente: Elaboración Propia

El inicio al servicio HTTP y al servicio Nagios, se prueba el servicio desde el browser ingresando en la URL la dirección <http://localhost/nagios>. Se utiliza el usuario y contraseña antes creado para acceder al sistema

“Se ingresa al administrador web de Nagios”

Gráfico 2.11. Administrador Web Nagios

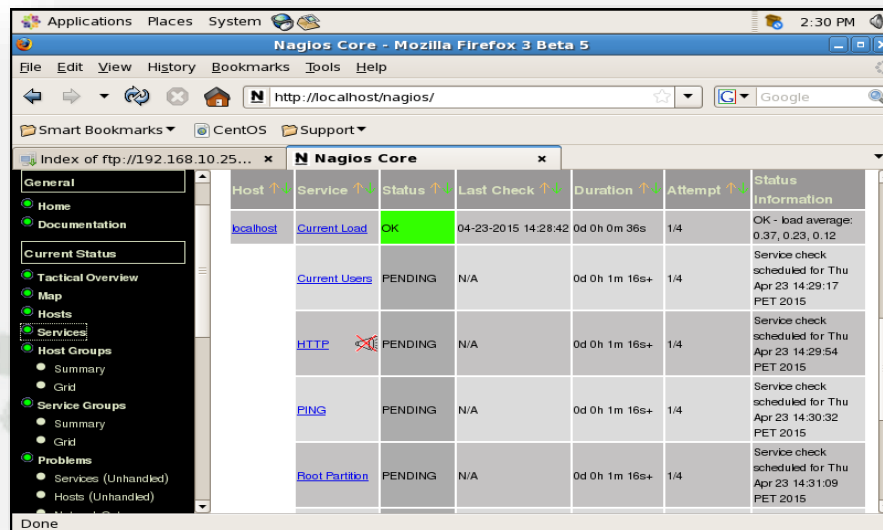


Fuente: Elaboración Propia

Qué equipo y servicios está monitoreando el servidor.

“En este caso el Nagios se encuentra monitoreando solo al equipo local, se observa el estado de los servicios, duración del tiempo en el que corre el servicio e información sobre estos”

Gráfico 2.12. Monitorización de equipo local



Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	04-23-2015 14:28:42	0d 0h 0m 36s	1/4	OK - load average: 0.37, 0.23, 0.12
	Current Users	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:29:17 PET 2015
	HTTP	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:29:54 PET 2015
	PING	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:30:32 PET 2015
	Root Partition	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:31:09 PET 2015

Fuente: Elaboración Propia

Nagios utiliza el comando snmpwalk para mostrar información en su sistema.

Lo implementa vía plugins pre instalados en su máquina respectiva.

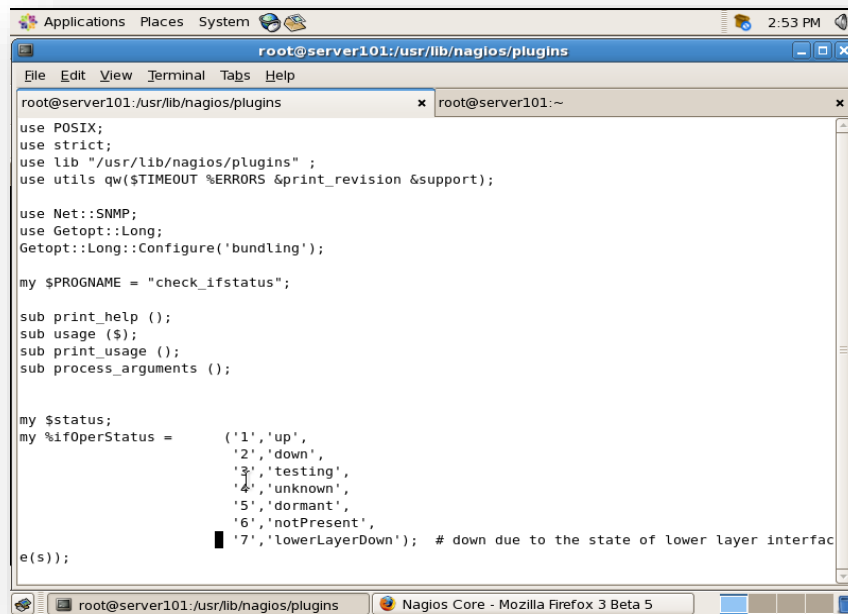
El repositorio plugins es:

- `/usr/lib/nagios/plugins/`

Edite un plugin con el comando vi y verifique el contenido. Que información puede observar.

“Este archivo devuelve valores de las librerías de plugins, muestra información sobre los errores de sistema que se puedan registrar” en plugin a registrar tiene de nombre “check_ifstatus”.

Gráfico 2.13. Repositorio plugin



```

root@server101:/usr/lib/nagios/plugins
File Edit View Terminal Tabs Help

root@server101:/usr/lib/nagios/plugins x root@server101:~ x

use POSIX;
use strict;
use lib "/usr/lib/nagios/plugins" ;
use utils qw($TIMEOUT $ERRORS &print_revision &support);

use Net::SNMP;
use Getopt::Long;
Getopt::Long::Configure('bundling');

my $PROGNAME = "check_ifstatus";

sub print_help ();
sub usage ($);
sub print_usage ();
sub process_arguments ();

my $status;
my %ifOperStatus = (
    '1','up',
    '2','down',
    '3','testing',
    '4','unknown',
    '5','dormant',
    '6','notPresent',
    '7','lowerLayerDown'); # down due to the state of lower layer interfac
e(s));
    
```

Fuente: Elaboración Propia

Para ejecutar el plugins se utiliza el siguiente comando:

- **`#!/usr/lib/nagios/plugins/./check_ifstatus -C public -H <IP Router> -x1`**

Nagios utiliza los dispositivos a monitorear como objetos, estos objetos contienen servicios que son los parámetros que serán monitoreados.

Se puede adicionar una imagen de referencia que simbolizara el equipo de comunicación, descargue el repositorio de imágenes Satrapa de la página:

<http://exchange.nagios.org/directory/Images-and-Logos>

Descargue y descomprima la imagen en la carpeta `/usr/share/nagios/images/logos`

Cree el archivo `/etc/nagios/objects/routers.cfg`, e ingrese el siguiente contenido.

```

define host{
use          generic-switch
host_name    cisco2600
alias        cisco router
address      <IP del router>
icon_image   my_router.gif
statusmap_image my_router.gd2
}

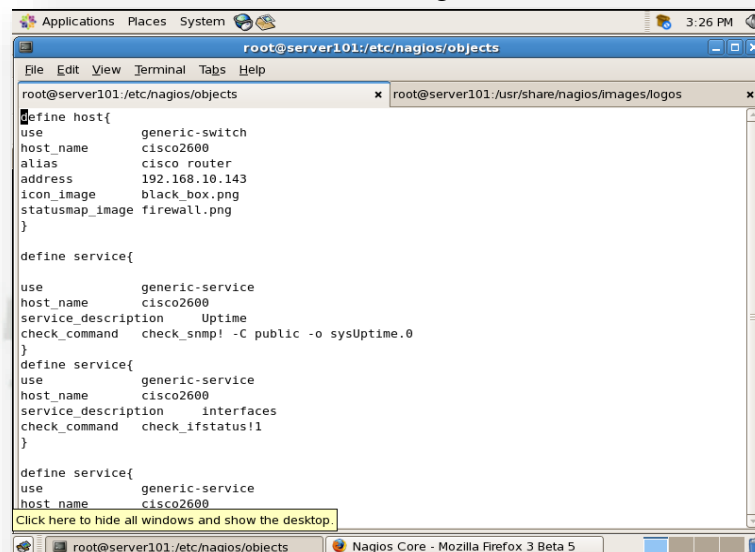
define service{
use          generic-service
host_name    cisco2600
service_description Uptime
check_command check_snmp!-C public -o sysUpTime.0
}

define service{
use          generic-service
host_name    cisco2600
service_description interfaces
check_command check_ifstatus!1
    
```

```
}
define service{
use          generic-service
host_name    cisco2600
service_description    PING
check_command    check_ping!200.0,20%!600.0,60%
normal_check_interval    5
retry_check_interval    1
}
}
```

“Se ingresa los comandos al archivo creado”

Gráfico 2.14. Ingreso de Comandos



Fuente: Elaboración Propia

Se registra la configuración del objeto en Nagios, edite el archivo /etc/nagios/nagios.cfg e ingrese el registro del Router debajo del Switch

- `cfg_file=/etc/nagios/objects/routers.cfg`

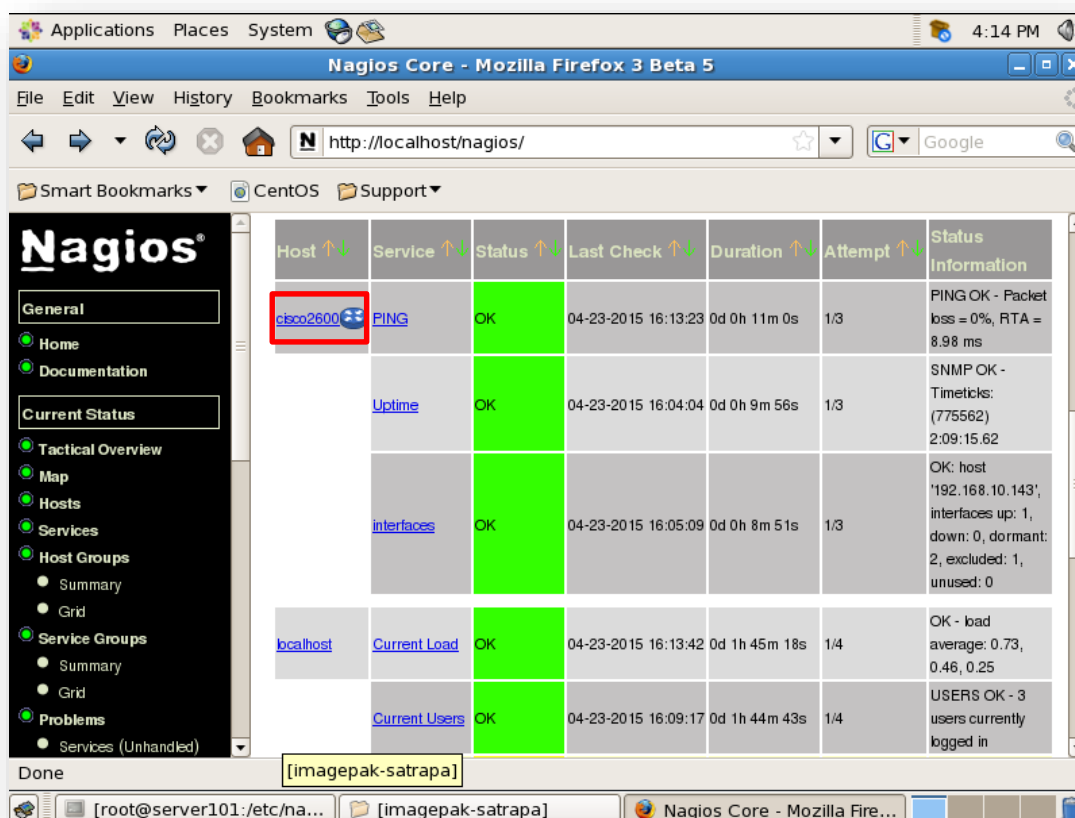
Se registra los comandos para que se utilice Nagios, en commands.cfg.

```
# snmp Commands
define command{
command_name    check_ifstatus
command_line    $USER1$/check_ifstatus -H $HOSTADDRESS$ -C public -x
$ARG1$
}
```

Se reinicia el servicio Nagios y se prueba el objeto creado. Que información se puede encontrar sobre este objeto.

“Se Ingresa a la pagina web de la administracion de Nagios, en la opcion services, muestra el objeto que se adiciono, en este caso es el servicio de nuestro Access point” (González, 2015)

Gráfico 2.15. Ingreso de página web de administración de Nagios



Fuente: Elaboración Propia

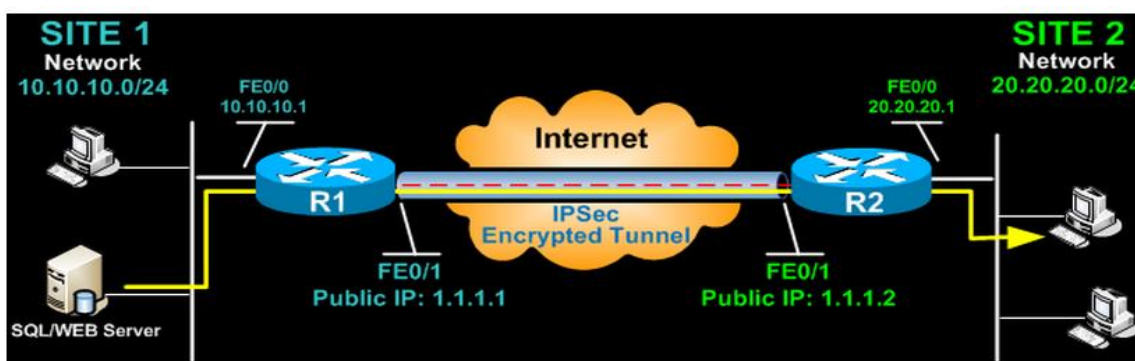
REQUISITOS IPSEC VPN

Estos pasos son los siguientes:

- (1) Configure ISAKMP (ISAKMP Fase 1)
- (2) Configurar IPSec (ISAKMP Fase 2, ACL, Crypto MAP)

Nuestro ejemplo de instalación es entre dos ramas de una pequeña empresa, se trata de Sitio 1 y Sitio 2. Tanto los Routers de sucursales conectarse a Internet y tener una dirección IP estática asignada por su ISP como se muestra en el diagrama:

Gráfico 2.16. Routers de Sucursales conectadas a Internet



Fuente: Elaboración Propia

Sitio 1 está configurado con una red interna de 10.10.10.0/24, mientras Sitio 2 está configurado con la red 20.20.20.0/24. El objetivo es conectar de forma segura tanto en redes LAN y permitir la plena comunicación entre ellos, sin ninguna restricción.¹⁸

CONFIGURAR ISAKMP (IKE) - (ISAKMP FASE 1)

IKE sólo existe para establecer las SA (Security Association) para IPsec. Antes de que pueda hacer esto, IKE debe negociar una SA (una SA ISAKMP) la relación con los pares.

Para empezar, vamos a empezar a trabajar en el Sitio 1 del Router (R1)

El primer paso es configurar una Fase 1 de ISAKMP política:

```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# encrytion 3des
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# lifetime 86400
```

Los comandos anteriores definen los siguientes (en orden):

- **3DES - El método de cifrado.**
- **MD5 - El algoritmo de hash.**

Utilice la tecla Pre - compartida como método de autenticación - Pre -share

Grupo 2 - El grupo Diffie - Hellman que se utilizará.

86400 - Sesión duración de la clave. Expresado en kilobytes (después de x - cantidad de tráfico, cambiar la clave) o segundos. Establecer valor es el valor predeterminado.

Debemos tener en cuenta que ISAKMP Fase 1 se define la política a nivel mundial. Esto significa que si tenemos cinco sitios remotos diferentes y configurados cinco políticas ISAKMP Fase 1 diferentes (uno para cada Router remoto), cuando nuestro Router intenta negociar un túnel VPN con cada sitio que enviará las cinco políticas y utilizar el primer partido que es aceptado por ambos extremos.

A continuación vamos a definir una clave compartida previamente para la autenticación con nuestro peer (Router R2) utilizando el siguiente comando:

¹⁸ Nagios Core Documentation [Consulta: 22 abril 2015]. Disponible en: <http://nagios.sourceforge.net/docs/nagioscore/4/en/>

R1(config)#crypto isakmp key firewallcx address 1.1.1.2

Clave compartida previamente de los pares se establece en firewallcx y su dirección IP pública es 1.1.1.2. Cada vez que R1 trata de establecer un túnel VPN con R2 (1.1.1.2) , se utilizará esta clave previamente compartida.

Configurar IPSec

Para configurar IPSec necesitamos configurar el siguiente orden:

- Crear ACL extendida.
- Crear IPSec Transform.
- Crear Crypto Mapa.
- Aplicar mapa criptográfico para la interfaz pública.

Examinemos cada uno de los pasos anteriores.

CREACIÓN ACL extendida

El siguiente paso es crear una lista de acceso y definir el tráfico que nos gustaría que el Router pase por el túnel VPN. En este ejemplo, sería el tráfico de una red a la otra, 10.10.10.0/24 a 20.20.20.0/24.

Listas de acceso que definen el tráfico VPN a veces se llaman cripto lista de acceso o interesante tráfico de acceso - lista.

R1(config)# ip access-list extended VPN-TRAFFIC

R1(config-ext-nacl)# permit ip 10.10.10.0 0.0.0.255 20.20.20.0 0.0.0.255

CREAR IPSEC TRANSFORMAR (ISAKMP FASE 2 POLÍTICA)

El siguiente paso es crear el conjunto de “transformar” utilizado para proteger nuestros datos. Hemos llamado a este TS:

R1(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac

El comando anterior define lo siguiente:

- ESP- 3DES - Método de cifrado.
- MD5 - algoritmo de hash.

CREAR CRYPTO MAPA

El mapa Crypto es el último paso de nuestra instalación y conecta el ISAKMP

previamente definido y configuración IPsec juntos:

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
R1(config-crypto-map)# set peer 1.1.1.2
R1(config-crypto-map)# set transform-set TS
R1(config-crypto-map)# match address VPN-TRAFFIC
```

Hemos llamado a nuestra mapa criptográfico CMAP . La etiqueta ipsec - isakmp le dice al Router que este mapa cripto es un mapa de cifrado IPsec. Aunque sólo un pares declarada en este mapa crypto (1.1.1.2) , es posible tener múltiples compañeros dentro de un mapa criptográfico dado.

APLICAR CRYPTO MAPA a la interfaz pública

El último paso es aplicar el mapa de cifrado a la interfaz de salida del Router. En este caso, la interfaz de salida es FastEthernet 0/1.

```
R1(config)# interface FastEthernet0/1
R1(config-if)# crypto map CMAP
```

Tenga en cuenta que puede asignar un único mapa criptográfico a una interfaz.

Tan pronto como aplicamos mapa cripto en la interfaz , recibimos un mensaje del Router que confirma isakmp está en : " ISAKMP es ON" .

En este punto, hemos completado la configuración de IPsec VPN en el Router Sitio 1.

Pasamos ahora al Router Sitio 2 para completar la configuración VPN. La configuración de Router 2 son idénticos, con la única diferencia de las direcciones IP de pares y listas de acceso:

```
R2(config)# crypto isakmp policy 1
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 86400

R2(config)# crypto isakmp key firewallcx address 1.1.1.1
R2(config)# ip Access-list extended VPN-TRAFFIC
R2(config-ext-nacl)# permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255

R2(config)# crypto ipsec transform-set TS esp-3des esp-md5-hmac
R2(config)# crypto map CMAP 10 ipsec-isakmp
R2(config-crypto-map)# set peer 1.1.1.1
R2(config-crypto-map)# set transform-set TS
R2(config-crypto-map)# match address VPN-TRAFFIC
R2(config-crypto-map)# match address VPN-TRAFFIC

R2(config)# interface FastEthernet0/1
```


R2(config-if)# **crypto map CMAP**

Network Address Translation (NAT) e IPSec VPN TÚNELES

La traducción de direcciones de Red (NAT) es más probable que ser configurado para proporcionar acceso a Internet a los hosts internos . Al configurar un túnel VPN de site to site, es imperativo para instruir el Router no realizar NAT (negar NAT) en los paquetes destinados a la red VPN remoto (s) .

Esto se hace fácilmente mediante la inserción de una declaración negar al comienzo de las listas de acceso NAT como se muestra a continuación:

Para el Router del Sitio 1:

```
R1(config)# ip nat inside source list 100 interface fastethernet0/1 overload
R1(config)# access-list 100 remark = [Define NAT Service]=
R1(config)# access-list 100 deny ip 10.10.10.0. 0.0.0.255 20.20.20.0 0.0.0.255
R1(config)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
R1(config)# access-list 100 remark
```

Y el Router del sitio 2

```
R2(config)# ip nat inside source list 100 interface fastethernet0/1 overload
R2(config)# access-list 100 remark = [Define NAT Service]=
R2(config)# access-list 100 deny ip 10.10.10.0. 0.0.0.255 20.20.20.0 0.0.0.255
R2(config)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
R2(config)# access-list 100 remark
```

Para poder establecer la red de comunicación segura con la implementación del protocolo OLSR Para realizar una conexión entre dos o más puntos es necesario que los dispositivos de red inalámbricos estén operando en la misma porción del espectro de radio, esto significa que los radios 802.11a se comunican con los de la misma frecuencia de 5GHz por ejemplo con otro radio 802.11a o 802.11n, sin embargo un dispositivo 802.11b con frecuencia de 2.4GHz no puede comunicarse con un 802.11a, es decir las tarjetas inalámbricas deben coincidir en el mismo canal para realizar una comunicación; este canal es una fracción del espectro donde se evita solapamientos entre ellos realizando una canalización que depende de la frecuencia de radio y regulación propia de cada país. (<http://www.nosolounix.com/2010/04/instalar-nagios-en-ubuntu.html>)

VERIFICAR EL TÚNEL VPN SITE TO SITE

En este punto, hemos completado nuestra configuración y el túnel VPN está listo. Para iniciar el túnel VPN, tenemos que forzar un paquete para atravesar el VPN y esto se puede lograr haciendo ping desde un router a otro:

R1# ping 20.20.20.1 source fastetherne0/0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:

Packet sent with a source address of 10.10.10.1

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 44/47/48 ms

V. FASE: PRUEBAS

Prueba de conectividad

Uno de los primeros puntos es establecer la comunicación respectiva entre el nodo principal y los sub nodos para ello con la ayuda del protocolo ping probaremos la comunicación entre los dispositivos.

```
Pinging 172.16.64.7 with 32 bytes of data:

Reply from 172.16.64.7: bytes=32 time=32ms TTL=128
Reply from 172.16.64.7: bytes=32 time=0ms TTL=128
Reply from 172.16.64.7: bytes=32 time=15ms TTL=128
Reply from 172.16.64.7: bytes=32 time=0ms TTL=128

Ping statistics for 172.16.64.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 32ms, Average = 11ms
```

```
Pinging 172.16.64.3 with 32 bytes of data:

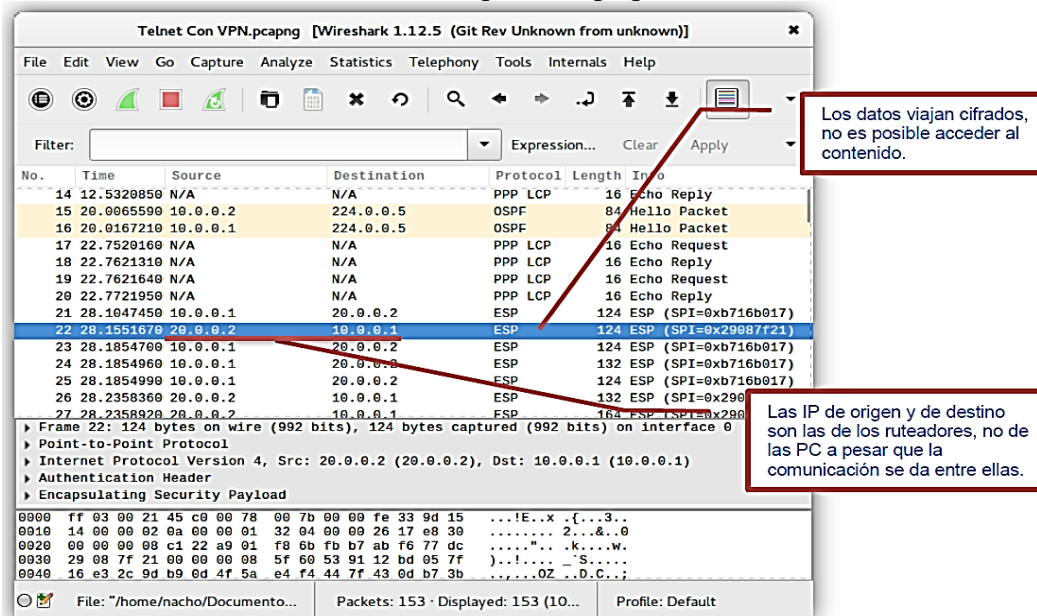
Reply from 172.16.64.3: bytes=32 time=38ms TTL=128
Reply from 172.16.64.3: bytes=32 time=0ms TTL=128
Reply from 172.16.64.3: bytes=32 time=0ms TTL=128
Reply from 172.16.64.3: bytes=32 time=0ms TTL=128

Ping statistics for 172.16.64.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 38ms, Average = 9ms

PC>
```

Prueba de captura de paquetes: En siguiente imagen que se muestra a continuación es una captura de paquete realizado mediante el programa wireshark, referenciado al cifrado que realiza la VPN.

Grafico 2.17. Captura de paquetes con wireshark



Fuente: Elaboración Propia

Comentario: en la siguiente imagen mediante la captura de paquetes realizado con el programa wireshark, se puede observar que los datos van hacer reempaquetados y esto conlleva a que sean cifrados, por consiguiente su contenido no va hacer visible hasta que sean desempaquetados en el destino.

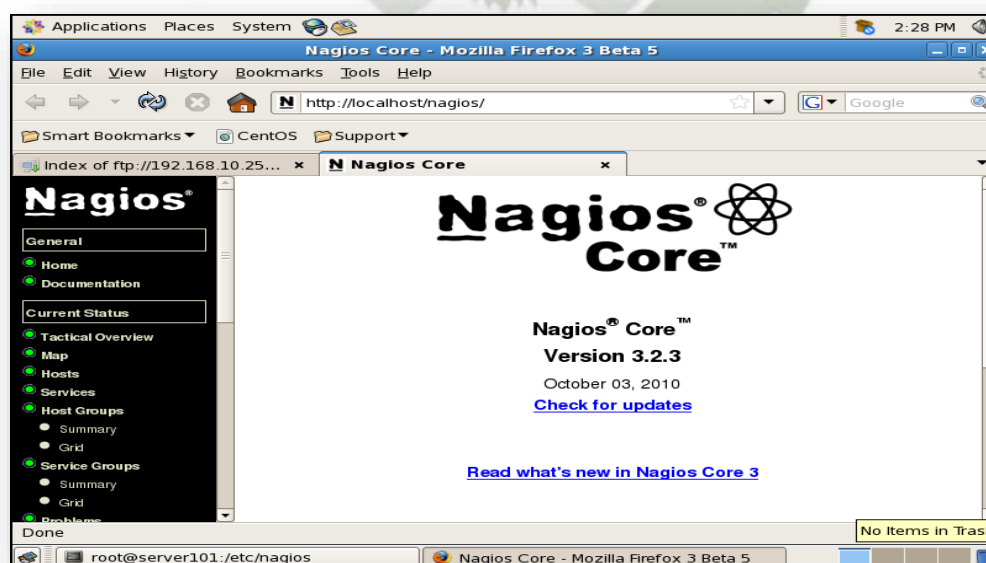
2.4. DOCUMENTACIÓN TÉCNICA DE PROGRAMACIÓN.

Validación de datos, Control de acceso y Protección de la información

2.5. PRUEBAS DE EJECUCIÓN.

2.5.1. Software de Monitoreo

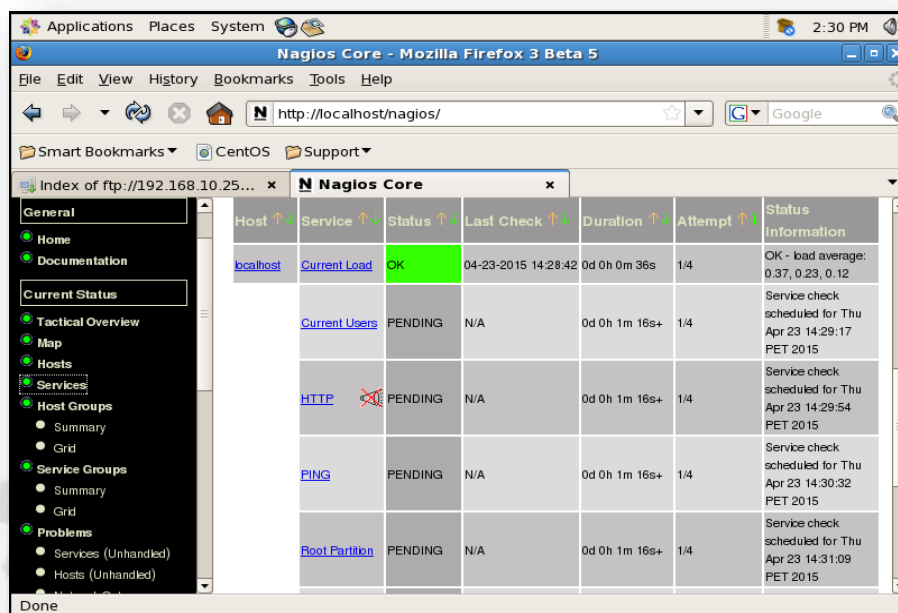
Gráfico 2.18. Monitorización de equipo local



Fuente: Elaboración Propia

Es la pantalla con la cual él se puede conectar mediante web al servicio de monitoreo de Nagios y en la imagen.

Gráfico 2.19. Software de Monitoreo (continuación)



Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	04-23-2015 14:28:42	0d 0h 0m 36s	1/4	OK - load average: 0.37, 0.23, 0.12
	Current Users	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:29:17 PET 2015
	HTTP	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:29:54 PET 2015
	PING	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:30:32 PET 2015
	Root Partition	PENDING	N/A	0d 0h 1m 16s+	1/4	Service check scheduled for Thu Apr 23 14:31:09 PET 2015

Fuente: Elaboración Propia

Podemos observar como el servicio de Nagios está monitoreando en este caso al mismo servidor en lo cual observamos, que en este caso está monitoreando el protocolo ping y los servicios HTTP, SSH y usuarios conectados el color verde muestra que el servidor está respondiendo correctamente sin percance alguno en caso que se ponga de color rojo es que el equipo dejo de responder por algún percance o problema con la red.

2.5.2. Sin interconexión

En el caso de realizar un asalto en el Grifo 1, su comunicación es casi inmediata con el 105, donde la policía tiene un tiempo de respuesta de 2 minutos con 40 segundos, según lo establecido en sus protocolos, pero todo depende del tiempo de interconexión y comunicación y de los recursos necesarios para la respuesta ante el acto delictivo.

A modo de prueba, se presenta el siguiente esquema:

Gráfico 2.20. Grifo sin interconexión



Fuente: Elaboración propia

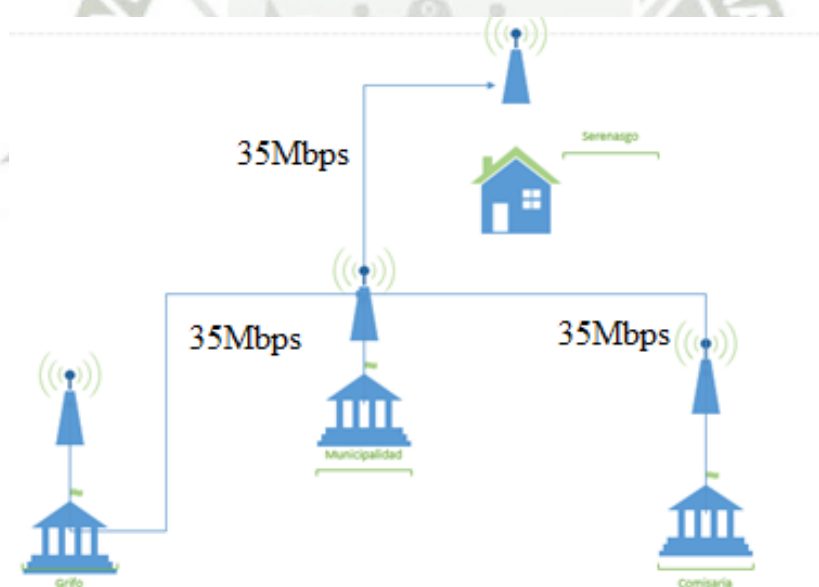
Tiempo de comunicación:

- Grifo con Central Telefónica de la Policía Nacional del Perú: 2 a 3 minutos
- Respuesta de la Policía: 5 a 7 minutos

2.5.3. Interconexión y Comunicación Segura

En el este caso, ya existe la interconexión y comunicación entre municipalidad y comisaria.

Gráfico 2.21. Grifo con interconexión



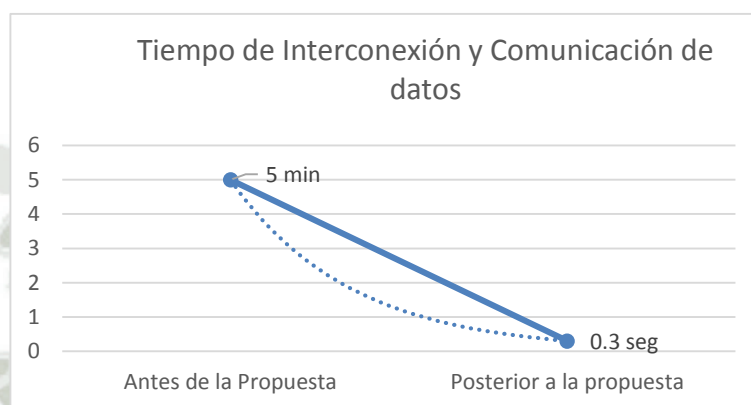
Fuente: Elaboración propia

Tiempo de comunicación:

- Grifo con Municipalidad: 0,3 segundos
- Municipalidad con Comisaria y Serenazgo: 0,3 segundos
- Respuesta de Policía: 5 a 7 minutos

2.5.4. Reporte de Tiempo

Gráfico 2.22. Tiempo de Interconexión y Comunicación de datos



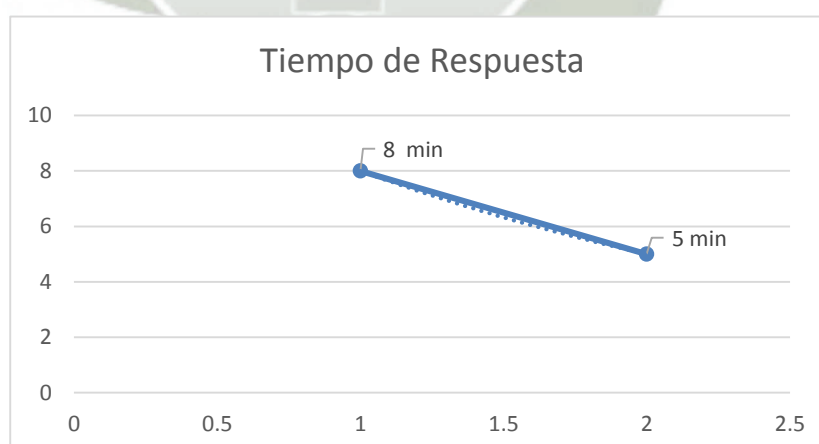
Fuente: Elaboración Propia

Comentario: el tiempo de antes de la Propuesta es de 5Min una vez propuesta la interconexión el tiempo ha disminuido.

Tiempo Sin Interconexión: 8 minutos en promedio

Tiempo con Interconexión y Comunicación: 5 minutos en promedio

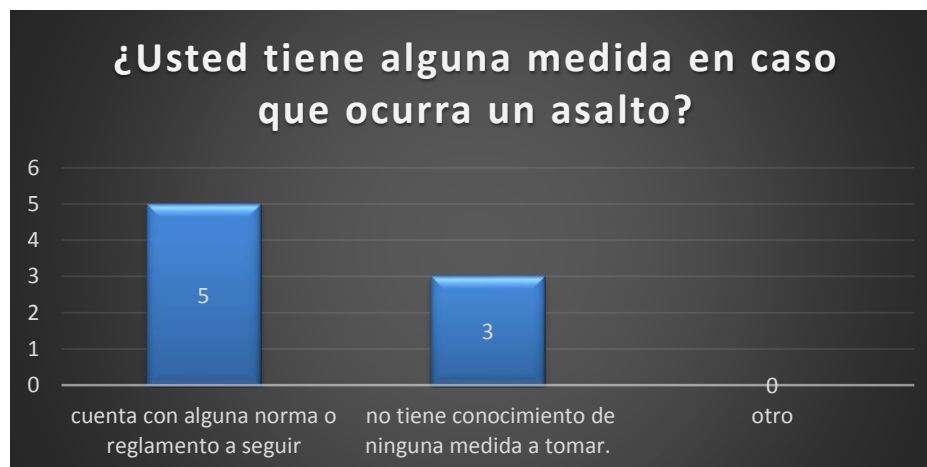
Gráfico 2.23. Reporte de Tiempo de Respuesta



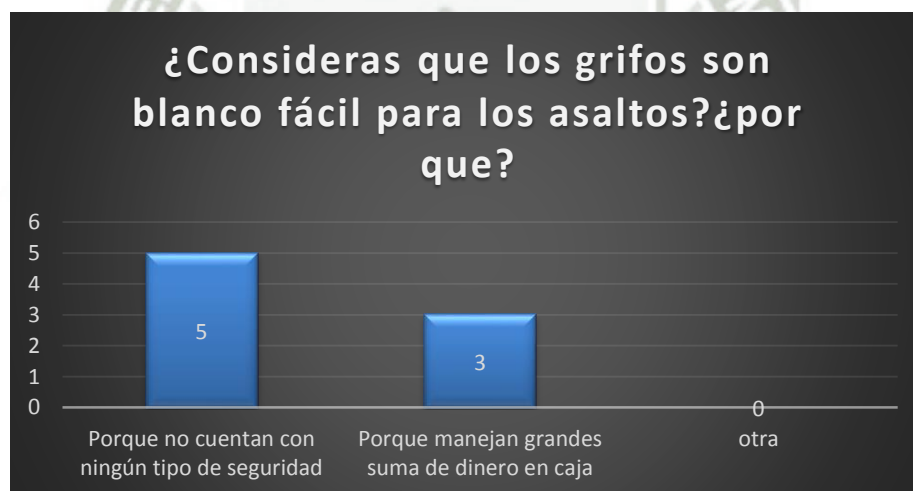
Fuente: Elaboración Propia

Comentario: El tiempo de respuesta antes de la propuesta era de 8min después de la propuesta este tiempo se logró disminuir de 8min a 5min.

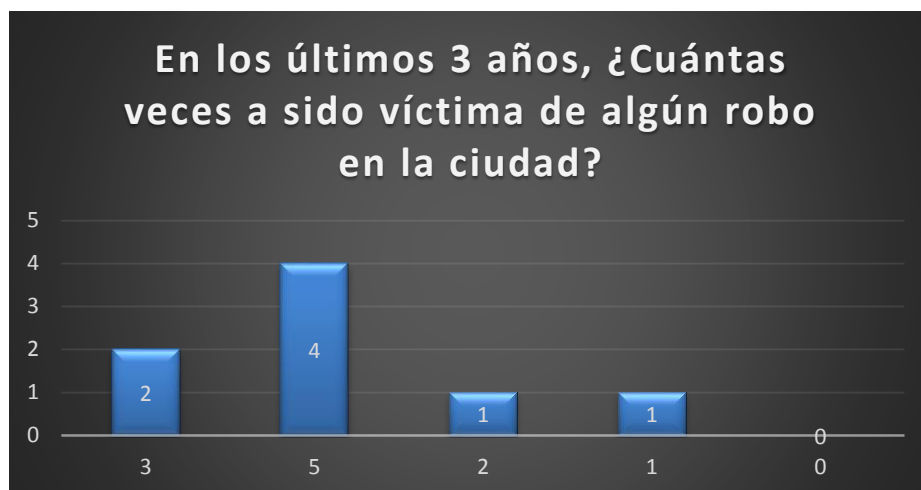
Resultados de las encuesta



En la presente encuesta realizada se pudo comprender que los empleados de los centros de distribución de combustible en un número considerable no cuentan con alguna medida o en peor de los casos son indiferentes a ello. Esto nos llega a poder concluir que los centros de distribución de combustible en un número considerado no tiene una norma o medida en caso que ocurra un asalto a dicho establecimiento.



En la gráfica podemos obtener datos muy alarmantes en un número considerable los empleados afirmaron que los centros de distribución de combustible no son blanco fácil porque dichos centros no cuentan con algún sistema de seguridad que contrarreste o disminuya los asaltos de estos centros de distribución de combustible.

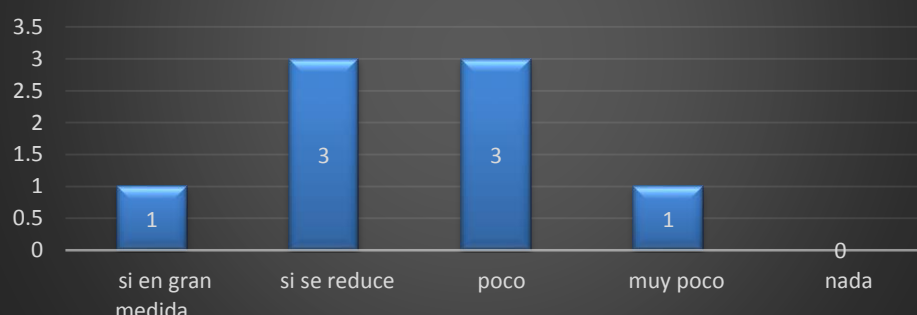


En la gráfica se concluyó que en la ciudad de Arequipa el índice de delincuencia es un problema muy serio a tomar en cuenta ya que podemos observar que a todos los encuestados han sido asaltados alguna vez y en el peor de los casos hasta 5 veces con este resultado se comprueba que la delincuencia está aumentando considerablemente en la ciudad de Arequipa.



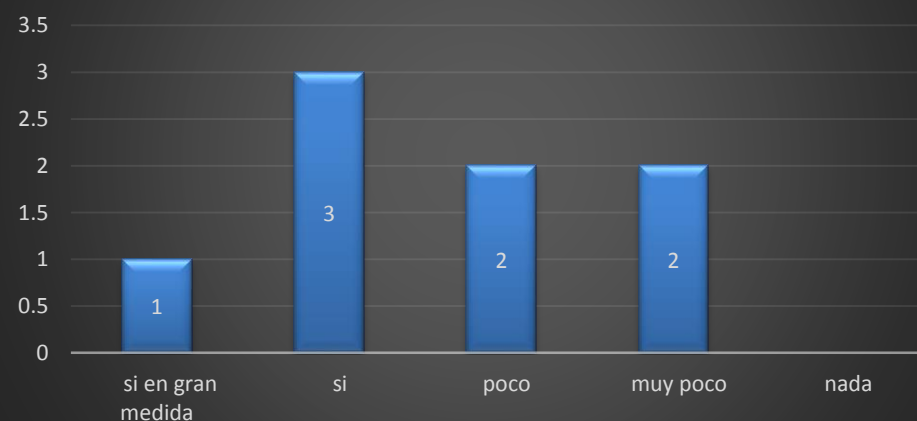
En la presente encuesta se pudo demostrar que un número considerable está de acuerdo que las entidades competentes que velan por el bienestar de la sociedad tienen que comunicarse y cooperar para así poder salvaguardar el bienestar de la sociedad de hoy en día.

Usted cree que con una mejor cooperación entre las entidades: municipalidad y comisaria se reduciría la delincuencia o saltos

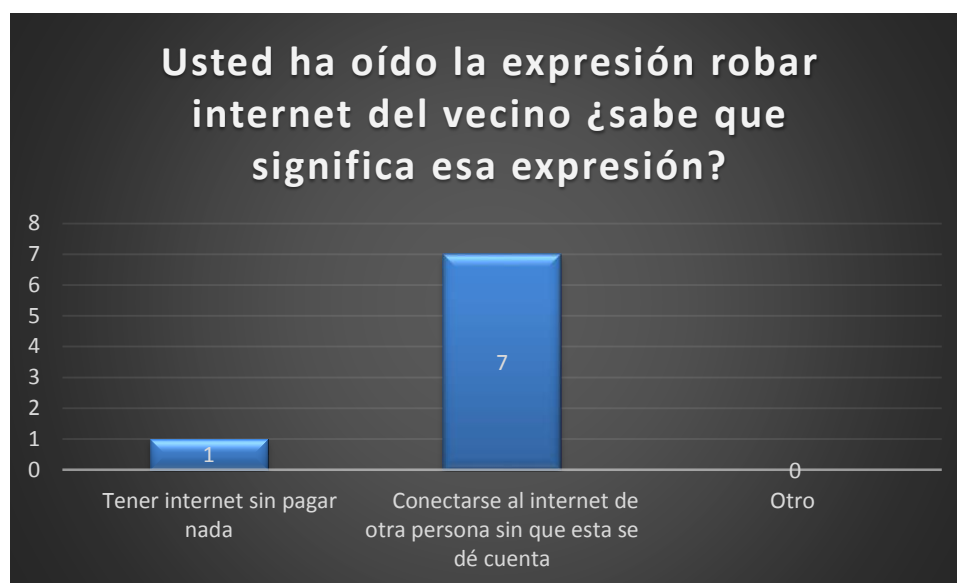


Los empleados de los centros de distribución de combustible están de acuerdo que si las entidades que velan por el bienestar de los ciudadanos cooperan y puedan comunicarse de manera rápida y confiable se puede reducir la delincuencia. Esto afirma aún más la necesidad de que las entidades que velan por el bienestar de los ciudadanos tienen que comunicarse de manera rápida y segura para reducir el índice de delincuencia.

¿Usted piensa que las tecnologías de redes inalámbricas es segura?



De comprobó que los empleados de los centros de establecimiento de combustible tiene conocimiento de las redes inalámbricas por consiguiente tienen noción de cómo funcionan esto hace que los empleados se puedan familiarizar de manera más rápida con la arquitectura que se propone implementar. Además de ello también un número considerable de ellos no confía en las redes inalámbricas por su inseguridad.



Se concluyó que el personal de los centros de distribución de combustible tienen conocimiento que las redes inalámbricas no son muy seguras porque un número considerable sabe que si se puede piratear la línea sin que el dueño de esta se dé cuenta de ello. Esto afirma aún más nuestra propuesta de crear una arquitectura con la cual se pueda implementar una medida con el fin de hacer las redes inalámbricas más seguras



CONCLUSIONES

- 1^{ra}** : Se comprobó la efectividad que brindó el protocolo VPN y servidor Radius mediante las pruebas de ejecución para intercomunicar las Municipalidades y Comisarías de la ciudad de Arequipa, en la encriptación de datos y la autenticación de puntos de conexión servidor y cliente.
- 2^{da}** : La seguridad de la red ha sido comprobada mediante la captura de los paquetes, con lo que pudo demostrar que la información está encriptada.
- 3^{ra}** : Mediante el programa Nagios se identificó las fallas más frecuentes y problemas en la arquitectura de la Red a firmando que uno de los problemas más frecuentes es la mala manipulación a los equipos de interconexión.
- 4^{ta}** : Que la propuesta de una red segura para la interconexión y cooperación de las Comisarias y Municipalidades de Arequipa utilizando los protocolos VPN y OLSR con servidor Radius y monitoreo Nagios, ha sido efectiva en el sentido de la Seguridad de la Red, ya que no cualquier individuo se puede contactarse a la red, sin previa autenticación.
- 5^{ta}** : Se concluye que con esta arquitectura de Red se podrá reducir el índice de la inseguridad ciudadana teniendo un mejor apoyo y cooperación entre las distintas entidades.

RECOMENDACIONES

En base a las evidencias encontradas en la presente investigación, se hace necesario recomendar lo siguiente:

- 1^{ra} : Se recomienda hacer un estudio más detallado para realizar la interconexión de toda la ciudad de Arequipa. Involucrando a todas las entidades con el fin de que se coopere eficientemente para el beneficio de la sociedad.
- 2^{da} : Se recomienda la implementación de radio enlaces en toda la ciudad de Arequipa especialmente en los puntos más críticos en inseguridad con el fin de que las entidades competentes se comuniquen eficientemente.
- 3^{ra} : Se recomienda en el futuro mejorar y optimizar la seguridad ya que la tecnología va cambiando constantemente, por consiguiente los ataques a la arquitectura planteada va evolucionando.
- 4^{ta} : Se recomienda realizar a futuro la implantación de aplicaciones puedan con las cuales se pueda mejorar el modo en que se envían las alertas a las entidades competentes.

BIBLIOGRAFIA

1. Charles Perkins, E. Belding-Royer, S. Das. Ad hoc On-demand Distance Vector (AODV) Routing, RFC 3561, 2003
2. Charles E. Perkins, Pravin Bhagwat. Highly Dynamic Desditation-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM 94, pp 234-244, 1994.
3. Cisco, David W; Fox, Andy. Firewalls PIX de Cisco Secure. Pearson Education. España, 2002
4. Cisco System. Guía del Segundo Año 2 Edición. Pearson Education España, 2002
5. Kauffman, Elizabeth; Newman, Andrew | Implementing IPSec, Wiley. Estado Unidos, 1999
6. Schmidt, Jeff seguridad en Microsoft Windows 2003 Prentice Hall. España, 2010
7. D. Bertsekas, R. Gallager. Data Networks, Prentice-Hall, pp 297-333, 1987.
8. D. Dhillon, T. S. Randhawa, M. Wang L. Lamont. Implementing a Fully Distributed Certificate Authority in an OLSR MANET, IEEE Communication Society, WCNC 2004 pp 682-688
9. Sallings, Willian. Comunicación de redes de computadora. Prentice-Hall Mexico, 2008
10. D. Johnson, D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC, 2007
11. David B. Johnson, David A. Maltz, Josh Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, 2004
12. Tannembaun, Andrew. Redes de Computadora 4 Edición. Prentice Hall. México 2008
13. Shneyderman, Alex. Mobile VPN. Wiley. Estados Unidos, 2003
14. Nagios System and Network Monitoring, por Wolfgang Barth 2005

INFORMATOGRAFÍA

15. http://computerhoy.com/noticias/internet/que-es-wifi-80211ac-que-hace-tan-rapido-8789_20-11-2015
16. https://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes_22-11-2015
17. http://infotelecommil.webcindario.com/librostelecom/SNMP.pdf_25-11-2015
18. https://es.wikipedia.org/wiki/Anexo:Comparaci%C3%B3n_de_sistemas_de_monitorizaci%C3%B3n_de_redes_28-11-2015





APÉNDICE(S)



APÉNDICE A PLAN DE PROYECTO

UNIVERSIDAD CATÓLICA DE SANTA MARÍA

FACULTAD DE CIENCIAS E INGENIERIAS FÍSICAS Y FORMALES

PROGRAMA PROFESIONAL DE INGENIERÍA DE SISTEMAS



PROPUESTA DE UNA RED SEGURA PARA LA INTERCONEXIÓN Y COOPERACION DE LAS COMISARIAS Y MUNICIPALIDADES DE AREQUIPA UTILIZANDO LOS PROTOCOLOS VPN Y OLSR CON SERVIDOR RADIUS Y MONITOREO NAGIOS.

Proyecto de tesis presentado por los
Bachilleres:

MOISÉS VLADIMIR CÁRDENAS TORREBLANCA
FREDY EMIGDIO QUISPE RUELAS

Para optar por el Título Profesional:
INGENIERO DE SISTEMAS

Asesor:

**AREQUIPA-PERÚ
2015**

1. PLANTEAMIENTO DEL PROBLEMA

PROPUESTA DE UNA RED SEGURA PARA LA INTERCONEXIÓN Y COOPERACION DE LAS COMISARIAS Y MUNICIPALIDADES DE AREQUIPA UTILIZANDO LOS PROTOCOLOS VPN Y OLSR CON SERVIDOR RADIUS Y MONITOREO NAGIOS.

1.1. Caracterización del Problema

Por intermedio de los diferentes medios de comunicación, se tiene conocimiento de que existe un incremento de asaltos en las empresas distribuidoras de combustible, muchas veces causan pérdidas humanas y materiales.

Se hace necesario la realización de la presente propuesta por la inexistencia de métodos que garanticen una respuesta inmediata de las autoridades policiales o de seguridad ciudadana (Serenazgo) que actúen de forma eficaz en la toma de acciones para la captura de los autores de una infracción, como lo es el robo a mano armada, el cual se ha evidenciado que se da con mayor frecuencia en empresas distribuidoras de combustibles en diversos distritos nuestro país y nuestra región Arequipa.

Se ha considerado el distritos José Luis Bustamante y Rivero, por ser una población en crecimiento económico, que atienden a un considerable parque automotor.

1.2. Palabras Clave

Palabras claves: Interconexión – Comunicación – VPN – Radius – Nagios

2. OBJETIVOS DEL PROYECTO

2.1. General

Determinar la efectividad del uso de protocolos VPN, OLSR y Radius en la interconexión y cooperación entre la municipalidad y comisaria José Luis Bustamante y Rivero.

2.2. Específicos

- Precisar la efectividad que brindara el protocolo VPN para intercomunicar las municipalidades de la ciudad de Arequipa.
- Comprobar la seguridad inalámbrica que brinda el protocolo OLSR y servidor Radius.
- Identificar mediante el programa Nagios las posibles fallas y problemas que se suscitan en el diseño de la RED.

3. FUNDAMENTOS TEÓRICOS

3.1. Antecedentes del proyecto

El primer paso fue profundizar la problemática que vive hoy en día la ciudad de Arequipa por el crecimiento de la población de manera rápida, y en vista de los últimos acontecimientos de violencia que ponen en riesgo a los ciudadanos de diferentes distritos, como también la dificultad que tienen las municipalidades y sus respectivas comisarias para poder cooperar entre ellas y así para poder ejecutar obras, en las cuales puede beneficiar a más de un distrito de la ciudad de Arequipa.

El siguiente paso fue profundizar sobre el funcionamiento de protocolos de comunicación que puedan garantizar la seguridad de la información en vista que para la ejecución de obras o difundir información esta no se vea alterado en el camino o sea robada por terceras personas u organizaciones.

Esto fue lo necesario para poder comenzar la investigación a fin de poder garantizar la información y proponer una arquitectura de red en la cual beneficiara en gran medida a la ciudad de Arequipa.

Con el conocimiento técnico del funcionamiento y vulnerabilidades de los protocolos investigados se decidió por los protocolos OLSR para una Red Móvil Urbana y VPN para una red WAN que comunicara las municipalidades y sus respectivas comisarias además de proponer un servidor Radius para garantizar la Autenticación de los usuarios y para la disponibilidad y la aplicación Nagios.

3.2. Bases Teóricas del proyecto

1. REDES MÓVILES

1.1. Redes inalámbricas

1.2. Estándar IEEE 802.16

1.3. IEEE 802.16

1.3.1. Modelo de referencia

1.4. Especificación PHY WIRELESSMAN-OFDMA

1.5. Alcance (Ranging) y Entrada de Red

2. PROTOCOLO VPN

2.1. Definición de una VPN

2.2. Características Funcionales

2.3. Elementos principales de una VPN

2.4. Requerimientos Básicos de las VPN

2.5. Tipos de VPN

2.6. Topologías de VPN

2.7. Protocolos de la VPN

2.8. Ventajas e Inconvenientes

3. SERVIDOR RADIUS

3.1. Introducción

3.2. Características de Radius

4. APLICACIÓN NAGIOS

1.1. ¿Cómo Funciona?

1.2. Guía de instalación de Nagios

1.3. Modificaciones después de la instalación

1.4. Configuración general

1.5. Archivo de configuración principal

1.6. Archivo de recursos

1.7. Archivos de definición de objetos

1.8. Archivo de configuración CGI

1.9. Definición de Objetos

1.9.1. ¿Cuáles son los objetos?

1.9.2. ¿Dónde están los objetos definidos?

1.9.3. Explicación de los objetos

1.10. Plug-ins de Nagios

1.10.1. ¿Qué son los plug-ins?

1.10.2. Plug-ins como una capa de abstracción

4. PRESENTACIÓN DEL PROYECTO

4.1. Justificación

El presente trabajo es un tema de actualidad, en razón al existente crecimiento de la población en diferentes distritos de la ciudad y el aumento de la inseguridad de Arequipa, en vista a esto es de suma importancia la cooperación de las distintas municipalidad para poder garantizar el bienestar de los ciudadanos y comodidad que las distintas municipalidades tiene que cooperar entre ellas, para poder realizar obras que beneficiaran a las municipalidades involucradas, pero para ello es necesario establecer una comunicación segura para poder intercambiar datos de suma importancia entre ellas.

Es un tema de importancia, debido a que en situaciones de emergencias como: accidentes de tránsito, incendios, atenciones médicas de urgencia, etc., es necesario comunicar a las municipalidades y comisarías para que ellas tomen las mediciones del caso.

Se considera que posee relevancia social, ya que la implementación de las Redes Móviles Seguras en el Ámbito Urbano, ayudará a la población en general de la ciudad a que se mantengan constantemente informado sobre acontecimientos importantes.

La motivación personal es lograr un esquema de arquitectura de seguridad de acuerdo al uso de la red y al grado de participación de los nodos en la misma, para mejorar la capacidad del protocolo de obtener “Disponibilidad, Integridad, Confidencialidad y Autenticación”.

4.2 Resumen del Proyecto.

PROPUESTA DE UNA RED SEGURA PARA LA INTERCONEXIÓN Y COOPERACION DE LAS COMISARIAS Y MUNICIPALIDADES DE AREQUIPA UTILIZANDO LOS PROTOCOLOS VPN Y OLSR CON SERVIDOR RADIUS Y MONITOREO NAGIOS.

4.2.1 Descripción del Proyecto a medio y largo plazo.

El presente proyecto nos brindará la oportunidad de ofrecer una forma de poder accionar en conjunto con las autoridades correspondiente ante un asalto, en este caso el que se da en las empresas distribuidoras de combustibles (Grifos)

El resultado final de la aplicación del proyecto será la efectividad que le brindar la utilización del protocolo VPN, OLSR y Radius con monitoreo Nagios.

Los beneficios más cercanos, es que el usuario tendrá la seguridad de que su llamado ante un atentado será en el menor tiempo posible, que en el mejor de los casos significará la anulación del delito y/o captura de los delincuentes.

4.2.2 Usuarios del Proyecto.

Se utilizar el Protocolo VPN, OLSR y Radius con monitoreo Nagios

Los beneficiarios serán:

Grifo Petroperú Camino Real, ubicado en la Avenida Lambrani Mz D, Lt. 28 Urb. Camino Real del Distrito de José Luis Bustamante y Rivero.

Grifo Petroperú San José, ubicado en la Av. Alcides Carrión 853 La Pampilla - José Luis Bustamante y Rivero

4.2.3 Beneficios.

Como beneficios obtendrán la oportunidad de tener una herramienta a la mano que le permita comunicarse o enviar una señal de alerta en cuestión de microsegundos, en el caso preciso de la ocurrencia de algún hecho delictivo,

4.2.4 Localización.

Distrito de José Luis Bustamante y Rivero

El distrito de José Luis Bustamante y Rivero es uno de los 29 distritos que conforman la provincia de Arequipa en el Departamento de Arequipa, bajo la administración del Región de Arequipa, en el sur del Perú.

Limites:

Norte: Cercado de Arequipa

Sur : Con los distritos de Socabaya y Sabandía

Este : Paucaparta

Oeste: Con el distrito de Jacobo D. Hunter.

José Luis Bustamante y Rivero es el distrito más joven de la provincia de Arequipa. La creación del distrito de José Luis Bustamante y Rivero se gestó a raíz de la iniciativa de un grupo de vecinos que fundaron el comité Cívico TEXAO que en su última etapa fue liderada, por Raúl Osorio Riveros, quien justamente con sus integrantes luchó arduamente para conseguir el tan anhelado objetivo de crear el distrito. Se logró constituir un nuevo núcleo autónomo que pudiera individualmente velar por los intereses y necesidades de sus pobladores a fin de acabar con la pasividad de los gobiernos locales de turno, que evidenciaron poco interés por esta zona, razón por la cual José Luis Bustamante y Rivero ocupa un área geográfica que

antes correspondió a los distritos de Paucarpata y Socabaya, y el Cercado de Arequipa.

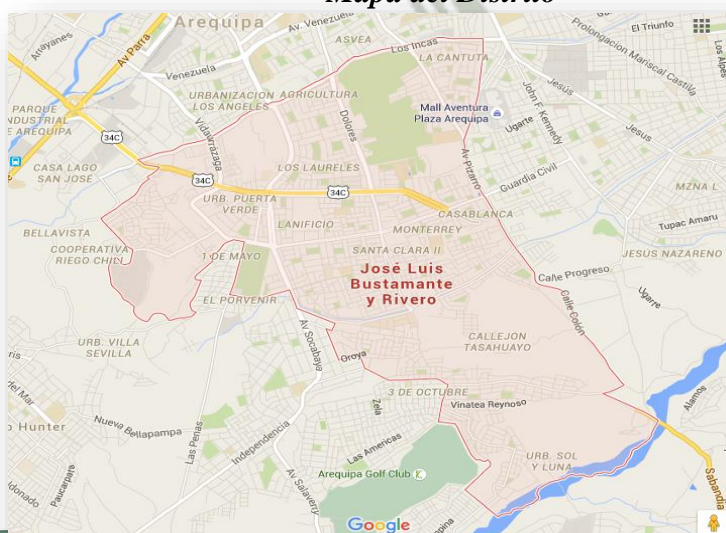
Pasaron muchos meses de esfuerzos y sacrificios, teniendo que sobrepasar innumerables obstáculos en el camino como nulidades presentadas en el congreso de la República, manejo interesado de la opinión pública, entre otras. Sin embargo gracias al amplio y decidido apoyo del congresista Arequipeño, Juan Guillermo Carpio Muñoz, logró la aprobación en el Congreso Constituyente Democrático, en el gobierno del Presidente Alberto Fujimori.

La noticia se dejó sentir en toda la jurisdicción. La celebración se dio en las calles, el júbilo de saber que desde ese momento se autogobernarían y solucionarían sus propios problemas con la guía de una Municipalidad que prioriza la participación vecinal en la toma de decisiones para el desarrollo del distrito.

El Distrito José Luis Bustamante y Rivero se encuentra ubicado en la Provincia y Región de Arequipa; situado al Sur – este del distrito de Arequipa a una distancia de 04 Km. de la plaza de Armas aproximadamente.

Se ubica a una altitud promedio de 2,363.00 m.s.n.m. entre los meridianos 16°25'04" de Latitud Sur y 71°31'48" de Longitud Oeste, posee una extensión territorial de 11.06 Km², que representa el 10% del área total de la Provincia de Arequipa.

Mapa del Distrito



Municipalidad Distrital de José Luis Bustamante y Rivero

Institución de gobierno local que tiene la función de administrar los ingresos económicos y desarrollar labores en beneficio y progreso de la comunidad local.

Máxima Autoridad: Alcalde Distrital

Dirección : Av. Dolores S/N

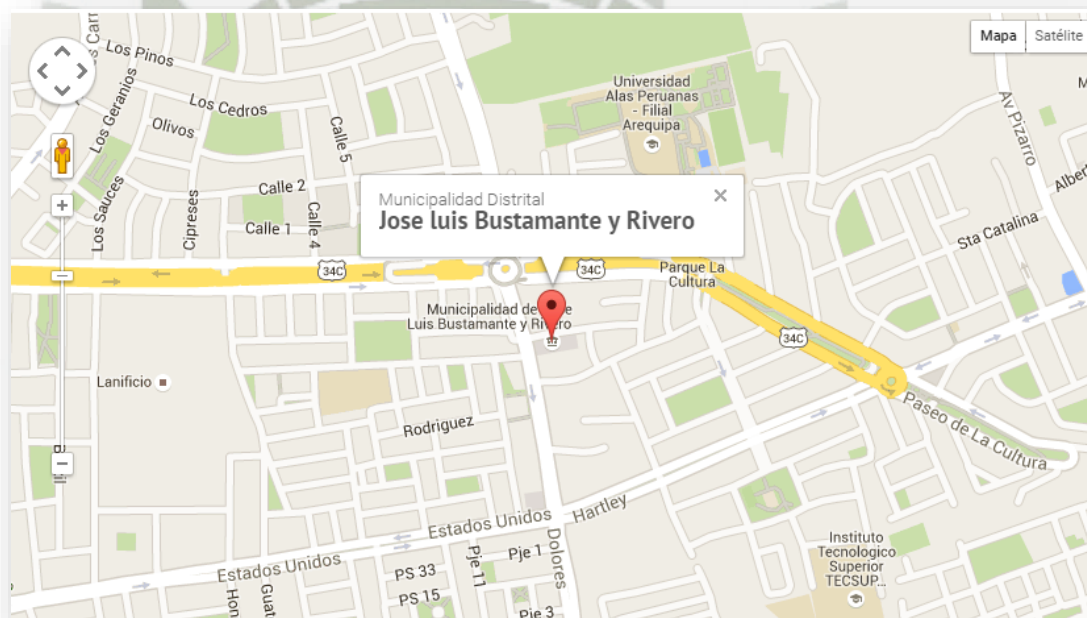
Distrito : José Luis Bustamante Y Rivero

Provincia : Arequipa

Región : Arequipa

Teléfono : (054) 430700 / 427169

Página Web : www.munibustamante.gob.pe



Comisaria de José Luis Bustamante y Rivero

Institución del Estado que tiene como función garantizar, mantener y restablecer el orden interno, prestar protección y ayuda a las personas y a la comunidad, garantizar el cumplimiento de las leyes y la seguridad del patrimonio público y privado, prevenir, investigar y combatir la delincuencia; vigilar y controlar las fronteras.

CPNP José Luis Bustamante y Rivero

Dirección : Cll. Quinta Tristan Sn Mz.Y Lt.2

Distrito : José Luis Bustamante Y Rivero

Provincia : Arequipa

Región : Arequipa

Teléfono : 427290

Web : www.pnp.gob.pe

Facebook : www.facebook.com/PoliciadelPeru

Google+ : plus.google.com/+policianacionaldelperu/posts

4.2.5 Impacto y sostenibilidad del Proyecto:

La propuesta realizada por los investigadores, se basa en la necesidad que se tienen actualmente de mayor seguridad, en cuanto al índice de criminalidad que soporta la ciudad de Arequipa, donde el blanco de los delincuentes son los negocios que manejan ingresos económicos altos y diarios, por lo que las empresas distribuidoras de combustibles, han sido víctimas de la delincuencia, lo que origina que se busque de alguna manera disminuir y porque no eliminar las cifras que actualmente maneja la Policía Nacional del Perú.

El mayor beneficio será que tendrán la oportunidad de comunicarse de manera rápida con la municipalidad, la cual coordinará con la comisaria y su servicio de seguridad ciudadana para la reacción ante el delito cometido.

La repercusión más representativa es sin lugar a dudas el sentido de seguridad y la recuperación de la confianza de los beneficiarios.

4.2.6 Riesgos que debemos afrontar.

- Competencia: buena revisión de los Antecedentes del proyecto.
- Tecnológicos: asumir que algo va a estar disponible o que por el contrario se quede obsoleto.



ANEXOS C

Encuesta

La encuesta nos permitió entrevistar a 8 trabajadores del Grifo Petroperú con la finalidad de recabar información que demuestren y validen que hoy en día es muy importante contar con una red segura para la interconexión y Cooperación de las Comisarias y Municipalidades de Arequipa utilizando la tecnología de las redes inalámbricas y cableadas que aseguren y salvaguarden la información que transita en ella.

1.- ¿Usted tiene alguna medida en caso que ocurra un asalto?

- a) cuenta con alguna norma o reglamento a seguir
- b) no tiene conocimiento de ninguna medida a tomar.
- c) que medida tomaría

.....

2.- ¿Consideras que los grifos son blanco fácil para los asaltos?¿por qué?

- a) Porque no cuentan con ningún tipo de seguridad
- b) Porque manejan grandes suma de dinero en caja
- c) otra

3.- ¿Cuánto tiempo demora en llegar después de que usted halla llamado a la Policía?

- a) 20min
- b) 10min
- c) 5min

otros.....

4.- Por favor, díganos el nivel de seguridad que tiene el Grifo.

- a) Muy inseguro
- b) Inseguro
- c) Seguro
- d) Muy seguro

5.- En los últimos 3 años, ¿Cuántas veces a sido víctima de algún robo en la ciudad?

- a) 3
- b) 5
- c) 2
- d) 1
- e) 0
- f) otro

6.- ¿Cuáles cree que serían las mejores medidas para reducir el crimen?

- a) Aumentar la presencia policial
- b) Tener cámaras de seguridad
- c) Tener una conexión directa con la policía y serenazgo

7.-Usted cree que se podría mejorar el tiempo de respuesta de la Policía al lugar de asalto

- a) Con una interconexión entre la Municipalidad y Comisaria.
- b) Con un aumento de patrulleros para la ciudad de Arequipa.
- c) Con aumento de efectivos policiales que patrullen a pie.
- d) otros

8.- Usted cree que con una mejor cooperación entre las entidades: municipalidad y comisaria se reduciría la delincuencia o saltos

- a) si en gran medida
- b) si se reduce
- c) poco
- d) muy poco
- e) nada

9.- Cree que la implementación de una red privada entre la Municipalidad y comisaria ayudaría a reducir el índice de delincuencia?

- a) si en gran medida
- b) si se reduce
- c) poco
- d) muy poco
- e) nada

10.- ¿Usted piensa que las tecnologías de redes inalámbricas es segura?

- a) si en gran medida
- b) si
- c) poco
- d) muy poco
- e) nada

11).- Usted ha oído la expresión robar internet del vecino ¿sabe que significa esa expresión?

- a) Tener internet sin pagar nada
- b) Conectarse al internet de otra persona sin que esta se dé cuenta
- c) Otro



5. REFERENCIAS BIBLIOGRÁFICAS

1. Charles Perkins, E. Belding-Royer, S. Das. Ad hoc On-demand Distance Vector (AODV) Routing, RFC 3561, 2003
2. Charles E. Perkins, Pravin Bhagwat. Highly Dynamic Desditation-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM 94, pp 234-244, 1994.
3. Cisco, David W; Fox, Andy. Firewalls PIX de Cisco Secure. Pearson Education. España, 2002
4. Cisco System. Guia del Segundo Año 2 Edicion. Pearson Education España, 2002
5. Kauffman, Elizabeth; Newman, Andrew | Implementing IPsec, Wiley. Estado Unidos, 1999
6. Schmidt, Jeff seguridad en Microsoft Windows 2003 Prentice Hall. España, 2010
7. D. Bertsekas, R. Gallager. Data Networks, Prentice-Hall, pp 297-333, 1987.
8. D. Dhillon, T. S. Randhawa, M. Wang L. Lamont. Implementing a Fully Distributed Certificate Authority in an OLSR MANET, IEEE Communication Society, WCNC 2004 pp 682-688
9. Sallings, Willian. Comunicacion de redes de computadora. Prentice-Hall Mexico, 2008
10. D. Johnson, D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC, 2007
11. David B. Johnson, David A. Maltz, Josh Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, 2004
12. Tannembaun, Andrew. Redes de Computadora 4 Edicion. Prentice Hall. Mexico 2008
13. Shneyderman, Alex. Mobile VPN. Wiley. Estados Unidos, 2003

APÉNDICE B

Glosario de Términos



Ad-hoc - comunicaciones de tipo punto a punto

AP - Access Point

DS - Distribution System

AODV - Ad hoc On Demand Distance Vector

Backbone - principales conexiones troncales de Internet

BSS - Basic Service Set

CA - Certificate Authority

CGI - Common Gateway Interface

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IPSec - Internet Protocol Security

MAC - Media access control

MANet's - Mobile ad hoc network

MPR - Relevé Multipunto

nrtPS - Non-real-time Polling Service

OFDM - Orthogonal Frequency Division Multiplexing — multiplexación por División de frecuencia ortogonal.

OFDMA - Orthogonal Frequency Division Multiple Access.

OLSR - Optimized Link State Routing

PAP - Password Authentication Protocol

PDUs - Protocol Data Unit.

PPP - Point to Point Protocol

PHY - Physical Layer— capa física

RADIUS - Remote Authentication Dial-In User Service

RAP - Remote Accesses Policies

RFC - Protocolo de resolución de direcciones

RS - estación repetidora

RTG - Receive/transmit Transition Gap

RRAS - Routing and Remote Access

rtPS - Real-time Polling Service

L2TP – Layer Two Tunneling Protocol

GRE - Generic Routing Encapsulation

SA - Security Association

SS - Subscriber Station —Estación del cliente suscriptor.

SSTG - SS Transition Gap.

STR - Simultaneous Transmit and receive relaying

THORUHGPOT - Tasa promedio de éxito en la entrega de un mensaje sobre un canal de comunicación.

HEADER - Encabezamiento

TTG - Transmit/receive Transition Gap

TTR - time-division transmit and receive relaying

TTR RS - time-division transmit and receive relaying, estación repetidora

PPTP - POINT-TO-POINT TUNNELING PROTOCOL

UGS - Unsolicited Grant Service.

UIUC - Uplink Interval Usage Code.

UL – Uplink - enlace de subida

VolP - Voice over IP

VPN - Virtual Private Network

WAN - Wide Area Network

WiBro - Tecnología de banda ancha Mobil

WiMax – Worldwide Interoperability for Microwave Access interoperabilidad mundial para acceso por microondas.

ZRP - Llamado también protocolo híbrido