



Instituto Tecnológico de Tuxtla Gutiérrez

**Ingeniería Electrónica
Con Especialidad Comunicaciones**

**Nombre del Proyecto:
Monitoreo de los Equipos de Comunicaciones Utilizando
Protocolo de SNMP.**

**Nombre del Alumno:
Alondra Isabel Gómez Rodas**

**Asesor interno: Ing. Arnulfo Cabrera Gómez.
Asesor externo: Ing. Alejandro Morales Aguilar.**

Agosto 2016, TUXTLA GTZ CHIAPAS



Índice de contenido

Capítulo I

1.1 caracterización de el área en que se participo	6
1.1.1 Antecedentes de la empresa.....	6
1.1.2 Localización.....	9
1.1.3 Organigrama de la empresa	10
1.1.4 Misión, Visión	11
1.1.4.1 Misión	11
1.1.4.2 Visión	11

Capítulo II

2.1 Introducción	12
2.2 Objetivos	13
2.2.1 objetivos Generales.....	13
2.2.2 Objetivos Específicos	13
2.3 Justificación	13
2.4 Planteamiento.....	14
2.5 Limitaciones	14

Capítulo III

3.1 fundamento teórico.....	15
3.1.1 SNMP.....	15
3.1.2 Versiones	19
3.1.2.1 SNMPv1	19
3.1.2.2 SNMPv2	20
3.1.2.3 SNMPv3	20
3.2 Autenticación.....	21
3.2.1 Mecanismo de autenticación	21
3.3 Privacidad	23
3.3.1 Mecanismo de privacidad.....	24
3.4 Elemento de la Arquitectura.....	24



3.4.1 NMS (<i>Network Management Station</i> –Estación de Gestión de Red.....	24
3.4.2 Agente	25
3.4.3 MIB (<i>Management Information Base</i> – Base de información de Gestión).	25
3.4.4ASN.1 (<i>Abstract Syntax Notation.1</i> – Notación de Sintaxis Abstracta.1)....	28
3.4.5 SMI (<i>Structure of Management Informacion</i> – Estructura de Información de Gestión)	28
3.5 Mensajes	30
3.6 Redes de información	30
3.6.1 Redes de área local.....	31
3.6.2 Redes de área metropolitana	32
3.6.3 Redes de área amplia	32
3.6.4 Redes virtuales privadas	33
3.6.4.1 Fundamento General de una Red Virtual	34
3.7 Elementos de red	35
3.7.1 Routers.....	35
3.7.2 Equipos de comunicación a monitorear	36
3.8 ICMP (<i>Internet Control Message Protocol</i> – Protocolo de Mensajes de Control de Internet)	41
3.9 ZABBIX	41

Capítulo IV

Desarrollo	43
4.1 Investigación	43
4.2 Instalación de software.....	44
4.2.1 Instalación de centos.....	44
4.2.2 instalación de ZABBIX.....	45
4.2.2.1 Descarga de repositorios ZABBIX	45
4.2.2.2 Instalación de requisitos de paquetes de ZABBIX.....	45
4.2.2.3 configuración de base de datos.....	46
4.2.2.4 Configuración de puertos	46



4.2.2.5 configuración del ZABBIX.....	47
4.2.2.6 Configuración de Scripts de inicio	47
4.2.2.7 Instalación de interfaz web	47
4.2.2.8 Comprobación y pasos de instalación	48
4.2.3 Pruebas	51
4.2.3.1 Agente ZABBIX.	51
4.3.4 Configuración de parámetros	53
4.3.5 Configuración de monitorización del trafico.....	55
4.3.6 Monitorización de la CPU	56
4.3.7 Configuración de alarma	60
4.3.8 Creación de graficas.....	63
4.4 Pruebas de Funcionamiento	64
4.4.1 Envió de alarmas.....	64
 Capitulo V	
5.1 Resultados	65
5.2 instalación inicial	65
5.3 configuración de parámetros	65
5.4 Pruebas locales de funcionamiento	66
5.4.1 pruebas con paquetes ICMP	66
5.5 instalación del servidor	67
5.6 conclusión	68
Anexo I	69
Anexo II	70
Referencias	110

CAPITULO I

1.1 CARACTERIZACIÓN DE LA ÁREA EN QUE SE PARTICIPO

1.1.1 ANTECEDENTES DE LA EMPRESA

La generación de energía eléctrica inició en México a fines del siglo XIX. La primera planta generadora que se instaló en el país (1879) estuvo en León, Guanajuato, y era utilizada por la fábrica textil “La Americana”. Casi inmediatamente se extendió esta forma de generar electricidad dentro de la producción minera y, marginalmente, para la iluminación residencial y pública.

En 1889 operaba la primera planta hidroeléctrica en Batopilas (Chihuahua) y extendió sus redes de distribución hacia mercados urbanos y comerciales donde la población era de mayor capacidad económica.

No obstante, durante el régimen de Porfirio Díaz se otorgó al sector eléctrico el carácter de servicio público, colocándose las primeras 40 lámparas "de arco" en la Plaza de la Constitución, cien más en la Alameda Central y comenzó la iluminación de la entonces calle de Reforma y de algunas otras vías de la Ciudad de México.

Algunas compañías internacionales con gran capacidad vinieron a crear filiales, como The Mexican Light and Power Company, de origen canadiense, en el centro del país; el consorcio The American and Foreign Power Company, con tres sistemas interconectados en el norte de México, y la Compañía Eléctrica de Chapala, en el occidente.

A inicios del siglo XX México contaba con una capacidad de 31 MW, propiedad de empresas privadas. Para 1910 eran 50 MW, de los cuales 80% los generaba The Mexican Light and Power Company, con el primer gran proyecto hidroeléctrico: la planta Necaxa, en Puebla. Las tres compañías eléctricas tenían las concesiones e instalaciones de la mayor parte de las pequeñas plantas que sólo funcionaban en sus regiones.

En ese período se dio el primer esfuerzo para ordenar la industria eléctrica con la creación de la Comisión Nacional para el Fomento y Control de la Industria de Generación y Fuerza, conocida posteriormente como Comisión Nacional de Fuerza Motriz.

Fue el 2 de diciembre de 1933 cuando se decretó que la generación y distribución de electricidad son actividades de utilidad pública.

En 1937 México tenía 18.3 millones de habitantes, de los cuales únicamente siete millones contaban con electricidad, proporcionada con serias dificultades por tres empresas privadas.

En ese momento las interrupciones de luz eran constantes y las tarifas muy elevadas, debido a que esas empresas se enfocaban a los mercados urbanos más reductibles, sin contemplar a las poblaciones rurales, donde habitaba más de 62% de la población. La capacidad instalada de generación eléctrica en el país era de 629.0 MW.

Para dar respuesta a esa situación que no permitía el desarrollo del país, el gobierno federal creó, el 14 de agosto de 1937, la Comisión Federal de Electricidad (CFE), que tendría por objeto organizar y dirigir un sistema nacional de generación, transmisión y distribución de energía eléctrica, basado en principios técnicos y económicos, sin propósitos de lucro y con la finalidad de obtener con un costo mínimo, el mayor rendimiento posible en beneficio de los intereses generales. (Ley promulgada en la Ciudad de Mérida, Yucatán el 14 de agosto de 1937 y publicada en el Diario Oficial de la Federación el 24 de agosto de 1937).

La CFE comenzó a construir plantas generadoras y ampliar las redes de transmisión y distribución, beneficiando a más mexicanos al posibilitar el bombeo de agua de riego y la molienda, así como mayor alumbrado público y electrificación de comunidades.

Los primeros proyectos de generación de energía eléctrica de CFE se realizaron en Teloloapan (Guerrero), Pátzcuaro (Michoacán), Suchiate y Xía (Oaxaca), y Ures y Altar (Sonora).

El primer gran proyecto hidroeléctrico se inició en 1938 con la construcción de los canales, caminos y carreteras de lo que después se convirtió en el Sistema Hidroeléctrico Ixtapantongo, en el Estado de México, que posteriormente fue nombrado Sistema Hidroeléctrico Miguel Alemán.

En 1938 CFE tenía apenas una capacidad de 64 kW, misma que, en ocho años, aumentó hasta alcanzar 45,594 kW. Entonces, las compañías privadas dejaron de invertir y CFE se vio obligada a generar energía para que éstas la distribuyeran en sus redes, mediante la reventa.

Hacia 1960 la CFE aportaba ya el 54% de los 2,308 MW de capacidad instalada, la empresa Mexican Light el 25%, la American and Foreign el 12%, y el resto de las compañías 9%.

Sin embargo, a pesar de los esfuerzos de generación y electrificación, para esas fechas apenas 44% de la población contaba con electricidad. Por eso el



presidente Adolfo López Mateos decidió nacionalizar la industria eléctrica, el 27 de septiembre de 1960.

A partir de entonces se comenzó a integrar el Sistema Eléctrico Nacional, extendiendo la cobertura del suministro y acelerando la industrialización. El Estado mexicano adquirió los bienes e instalaciones de las compañías privadas, las cuales operaban con serias deficiencias por la falta de inversión y los problemas laborales.

Para 1961 la capacidad total instalada en el país ascendía a 3,250 MW. CFE vendía 25% de la energía que producía y su participación en la propiedad de centrales generadoras de electricidad pasó de cero a 54%.

En esa década la inversión pública se destinó en más de 50% a obras de infraestructura. Se construyeron importantes centros generadores, entre ellos los de Infiernillo y Temascal, y se instalaron otras plantas generadoras alcanzando, en 1971, una capacidad instalada de 7,874 MW.

Al finalizar esa década se superó el reto de sostener el ritmo de crecimiento al instalarse, entre 1970 y 1980, centrales generadoras que dieron una capacidad instalada de 17,360 MW.

Cabe mencionar que en los inicios de la industria eléctrica mexicana operaban varios sistemas aislados, con características técnicas diferentes, llegando a coexistir casi 30 voltajes de distribución, siete de alta tensión para líneas de transmisión y dos frecuencias eléctricas de 50 y 60 Hertz.

Esta situación dificultaba el suministro de electricidad, por lo que CFE definió y unificó los criterios técnicos y económicos del Sistema Eléctrico Nacional, normalizando los voltajes de operación, con la finalidad de estandarizar los equipos, reducir sus costos y los tiempos de fabricación, almacenaje e inventariado. Posteriormente se unificaron las frecuencias a 60 Hertz y CFE integró los sistemas de transmisión en el Sistema Interconectado Nacional.

En los años 80 el crecimiento de la infraestructura eléctrica fue menor que en la década anterior, principalmente por la disminución en la asignación de recursos a la CFE. No obstante, en 1991 la capacidad instalada ascendió a 26,797 MW.

A inicios del año 2000 se tenía ya una capacidad instalada de generación de 35,385 MW, cobertura del servicio eléctrico del 94.70% a nivel nacional, una red de transmisión y distribución de 614,653 kms, lo que equivale a más de 15 vueltas completas a la Tierra y más de 18.6 millones de usuarios, incorporando casi un millón cada año.

A partir octubre de 2009, CFE es la encargada de brindar el servicio eléctrico en todo el país.

El servicio al cliente es prioridad para la empresa, por lo que se utiliza la tecnología para ser más eficiente, y se continúa la expansión del servicio, aprovechando las mejores tecnologías para brindar el servicio aún en zonas remotas y comunidades dispersas.

CFE es reconocida como una de las mayores empresas eléctricas del mundo, y aún mantiene integrados todos los procesos del servicio eléctrico.

1.1.2 Localización

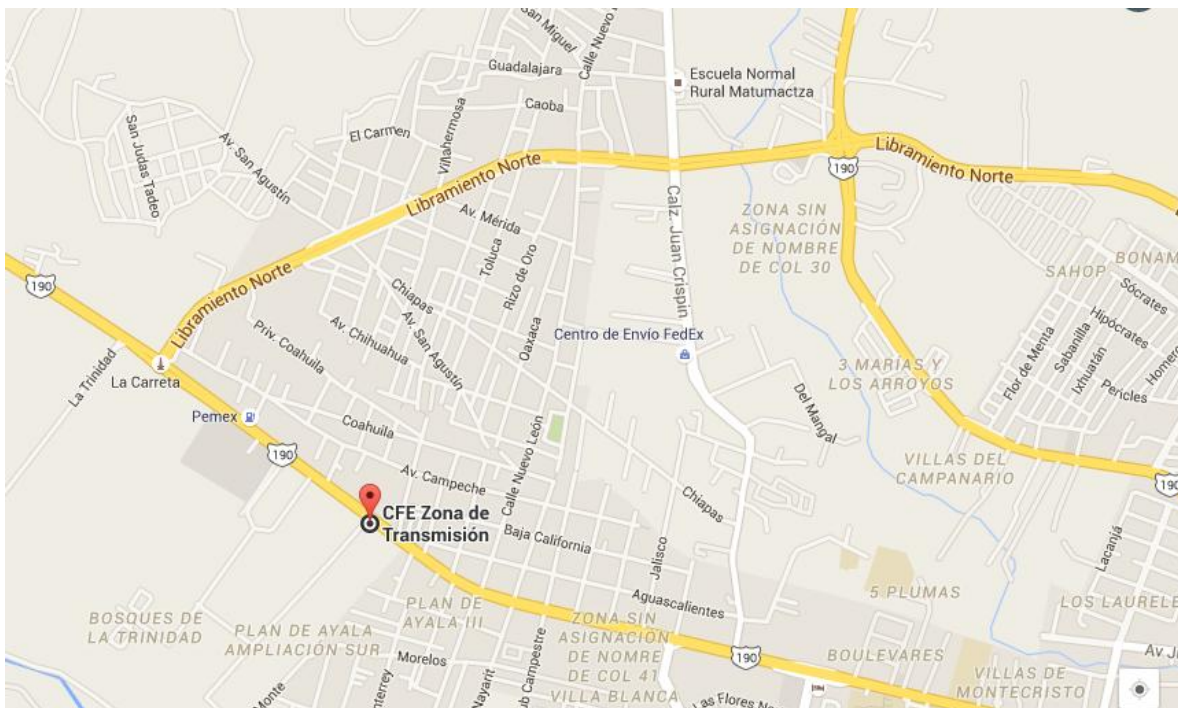
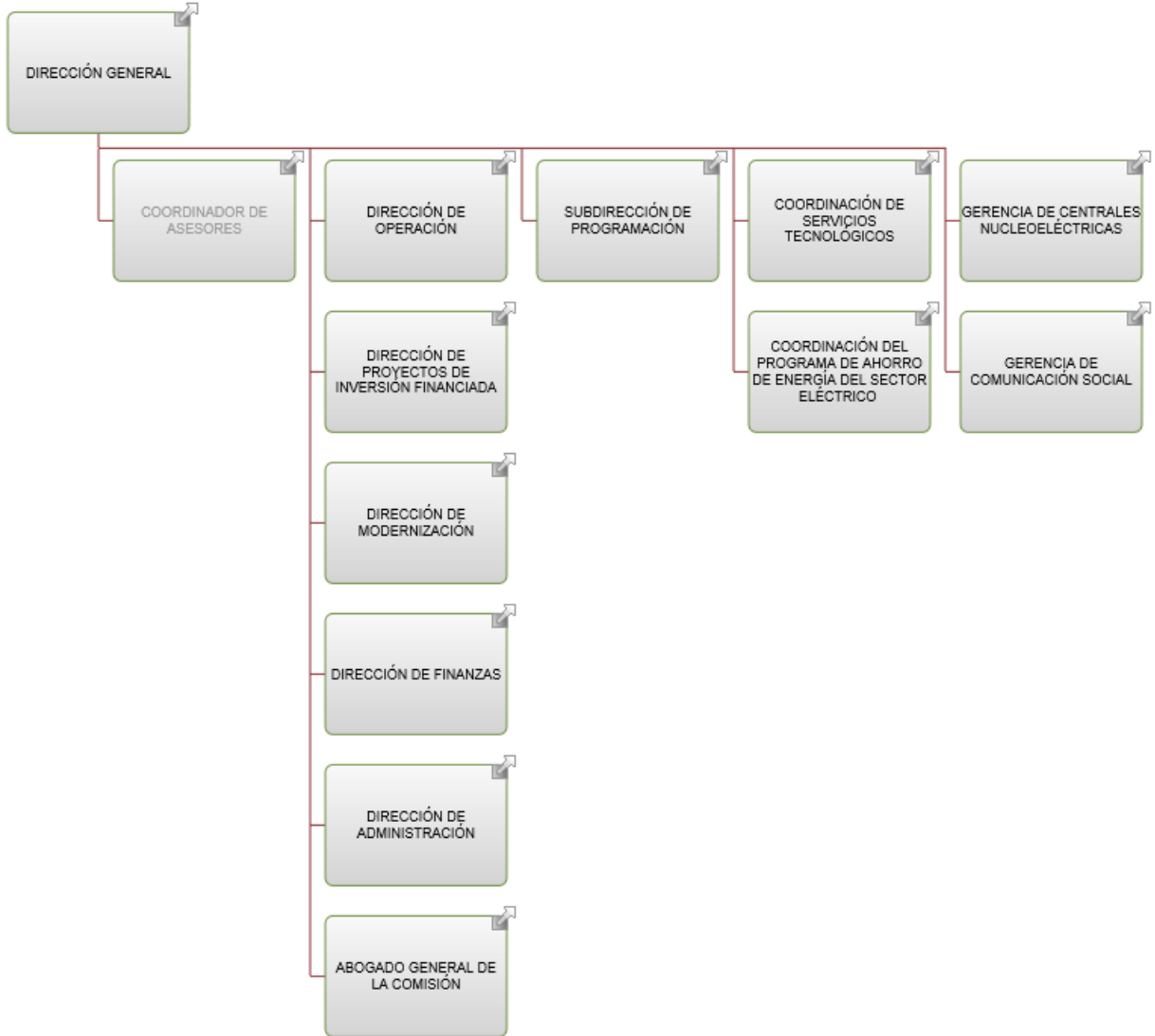


Figura 1.1 ubicación de la empresa

Comisión federal de electricidad (CFE) se encuentra ubicado en carretera panamericana Km. 1077, Int. 300M. colonia plan de Ayala.

1.1.3 Organigrama de la Empresa





1.1.4 Misión, Visión

1.1.4.1 MISIÓN

Prestar el servicio público de energía eléctrica con criterios de suficiencia, competitividad y sustentabilidad, comprometidos con la satisfacción de los clientes, con el desarrollo del país y con la preservación del medio ambiente.

1.1.4.2 VISIÓN AL 2030

Ser una empresa de energía, de las mejores en el sector eléctrico a nivel mundial, con presencia internacional, fortaleza financiera e ingresos adicionales por servicios relacionados con su capital intelectual e infraestructura física y comercial.

Una empresa reconocida por su atención al cliente, competitividad, transparencia, calidad en el servicio, capacidad de su personal, vanguardia tecnológica y aplicación de criterios de desarrollo sustentable.

CAPITULO II

2.1 Introducción

A lo largo de la historia han existido las comunicaciones, pero en la medida que ha evolucionado la raza humana, también han evolucionado los medios y métodos de comunicación. En los últimos años, la internet, las redes se han vuelto sumamente importantes, estas permiten intercambio de cualquier tipo de información a corta y larga distancia. Para que esto sea posible, se utiliza una serie de protocolos y especificaciones estándar, de manera que exista compatibilidad entre las redes.

Un tema importante para el buen funcionamiento de las redes de comunicación, es conocer las condiciones de la misma, monitoreo de los equipos, con el fin de detectar condiciones anormales que permitirán análisis y solución de fallas.

Un protocolo que se utiliza en esta área es SNMP, es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. ya que permite la obtención de información referente a los estados de la conexión, recursos, entre otros. Ellos conectan a la red los dispositivos administrados y permiten recopilar información sobre los diferentes objetos. Así como configurar comunicaciones más seguras.

2.2 Objetivos

2.2.1 Objetivo General

Implementar un sistema de monitoreo basado en el software libre ZABBIX el cual es capaz de informar el estado de los equipos con la adquisición de datos en tiempo real para garantizar la estabilidad y confiabilidad de los sistemas de comunicación.

2.2.2 Objetivos específicos

- Implementar un sistema capaz de monitorear la fiabilidad de los equipos.
- Poner en funcionamiento un sistema de gestión capaz de informar en tiempo real el estado de los es quipos.

2.3 Justificación

Debido a que personas y empresas necesitan estar constantemente comunicadas, es necesario crear estrategias en el ámbito de la seguridad y eficiencia de las redes que comunican a los individuos dependientes de los distintos servicios prestados por empresas de telecomunicaciones, a su vez, esta empresa depende de otras que les facilitan el trabajo en el área, tanto de proyecto como prestaciones de servicio técnico por lo anterior la empresa requiere de una herramienta eficaz en la administración de redes, propuesta del presente trabajo.

Hoy en día, disponer de sistemas adecuados para verificar el estado de los servicios prestados a terceros es vital tanto en el aspecto técnico como en el económico, ya que incluiría a su carpeta de presentación soporte de los diversos dispositivos necesarios para una red.

Es por ello que surgió la necesidad de realizar las investigaciones necesarias para obtener una buena base teórica y realizar el trabajo práctico con la mayor precisión y simplicidad posible, ya que todo sistema simple y con un buen rendimiento acarrea menores costos de implementación y mantenimiento, beneficiando así a las partes involucradas en los contratos de servicio.

Desde el punto de la ingeniería de telecomunicaciones se obtiene un beneficio igualmente importante, ya que la posibilidad de conocer el estado de los equipos y enlaces que conforman una red es vital para ofrecer la máxima calidad de servicio al cliente, independientemente del área en que se desempeñe el mismo

2.4 Planteamiento del problema

Comisión federal de electricidad es una empresa de servicios profesionales que brinda soporte de primer, segundo y tercer nivel a terceros sobre la plataforma de comunicaciones y transporte de datos. Se encarga del despliegue y mantenimiento de redes, y cuenta con personal disponible para responder en caso de reportes de falla.

Debido que la empresa carecía de un sistema de gestión y monitoreo de casos que permitiese brindar soporte a sus clientes en caso de fallas de manera proactiva y realizar los mecanismos acuerdo a los contratos, se implemento un sistema de monitoreo, mediante la adaptación de herramientas existentes a las necesidades del cliente, de manera que quedasen satisfechas las necesidades de todas las partes involucradas.

2.5 Limitaciones

- Los equipos no se puedan librar (sacar de operación) ya que se encuentra en funcionamiento y con servicios hacia los clientes externos e internos. Las modificaciones a las configuraciones de estos equipos, deben hacerse en vivo y sin afectación a usuarios.
- La autorización de las ventanas de mantenimiento a los equipos de los clientes externos, es un proceso tardado, y no hay garantía de que sean autorizados para una implementación de un sistema como el del presente trabajo.

Capítulo III

3.1 Fundamento teórico

En este capítulo se tratara de los enfoques teóricos, estudios y antecedentes sobre los protocolos, tipo de mensajes, arquitectura de red para su debida monitorización.

3.1.1 SNMP (Simple Network Management protocol – Protocolo simple de gestión de red)

Al tener una red es necesario poder monitorear lo que ocurre con ella, desde el punto de vista de la administración. Uno de los factores más importantes que se deben considerar es el control y corrección de errores para poder ofrecer fidelidad. SNMP es un protocolo que permite de una manera muy simple para realizar esto.

Este es un protocolo de capa de aplicación (modelo OSI), está diseñado para facilitar el intercambio de información entre los equipos de la red y su administrador, a fin de que este pueda supervisar su funcionamiento y sea posible tomar acciones en caso de fallas o de eventos indeseados. Como todos los protocolos, esta estandarizado y tiene un lenguaje común, se conoce ampliamente que esto se hace para que los equipos puedan comunicarse entre sí, siempre y cuando sean compatible, sin importar quienes sean el fabricante y el usuario.

Es un protocolo que se usa para administrar redes TCP/IP y funciona sobre UDP, los comandos son fáciles de entender y utilizar. La forma en que trabaja SNMP es a través del sondeo, el cual consiste en preguntar como gestor a un agente, esto significa enviar una solicitud pidiendo información sobre su estado físico, o bien pedir una actualización de su estado de trabajo, tras una solicitud, el gestor espera una respuesta del agente, lo cual puede ser tanto una respuesta como una confirmación de cambio de estado. SNMP hace uso de los mensajes de interrupción, comúnmente llamados *trap*, en este tipo de mensaje los agentes pueden enviar información o alarmas a un gestor o nodo administrativo ante una eventual anomalía en la red.

SNMP facilita el intercambio de información entre dispositivos de red.

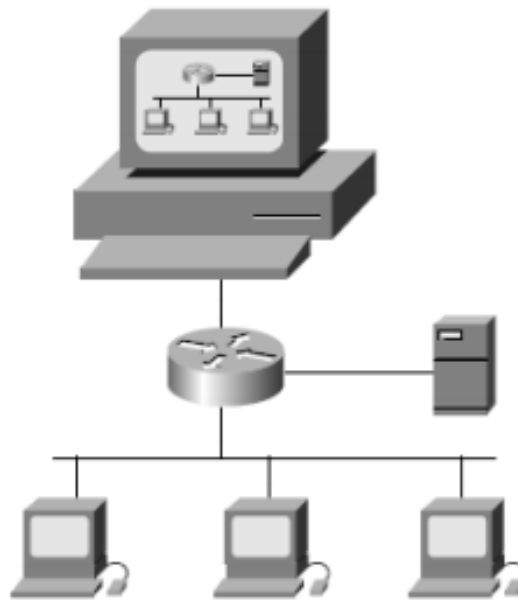


Figura 3.1 Red básica SNMP

Componentes básicos de SNMP:

Una red administrada con SNMP consiste de tres componentes fundamentales:

1. Dispositivos administrados (Managed Devices (MD):

Es un nodo de red que contiene un agente SNMP y que reside en una red administrada. Los dispositivos administrados coleccionan y almacenan información y hacen que esta información esté disponible al NMS's utilizando SNMP.

2. Agentes (Agent):

Es un modulo de SW de gestión de red que reside en un Manage Device. Un Agente tiene conocimiento local de información (sobre su memoria, numero de paquetes recibidos-enviados, dirección IP, rutas,etc.) y traduce esa información en una forma de formato compatible con SNMP.

3. Sistemas administrados de red (NMS);

Ejecuta aplicaciones que monitorean y controlan Managed Devices. Los NMS's proporcionan la mayor parte de recursos de procesamiento y memoria requeridos para la gestión de red.

Una red gestionada con SNMP, se compone de dispositivos gestionados, los agentes y los SMN

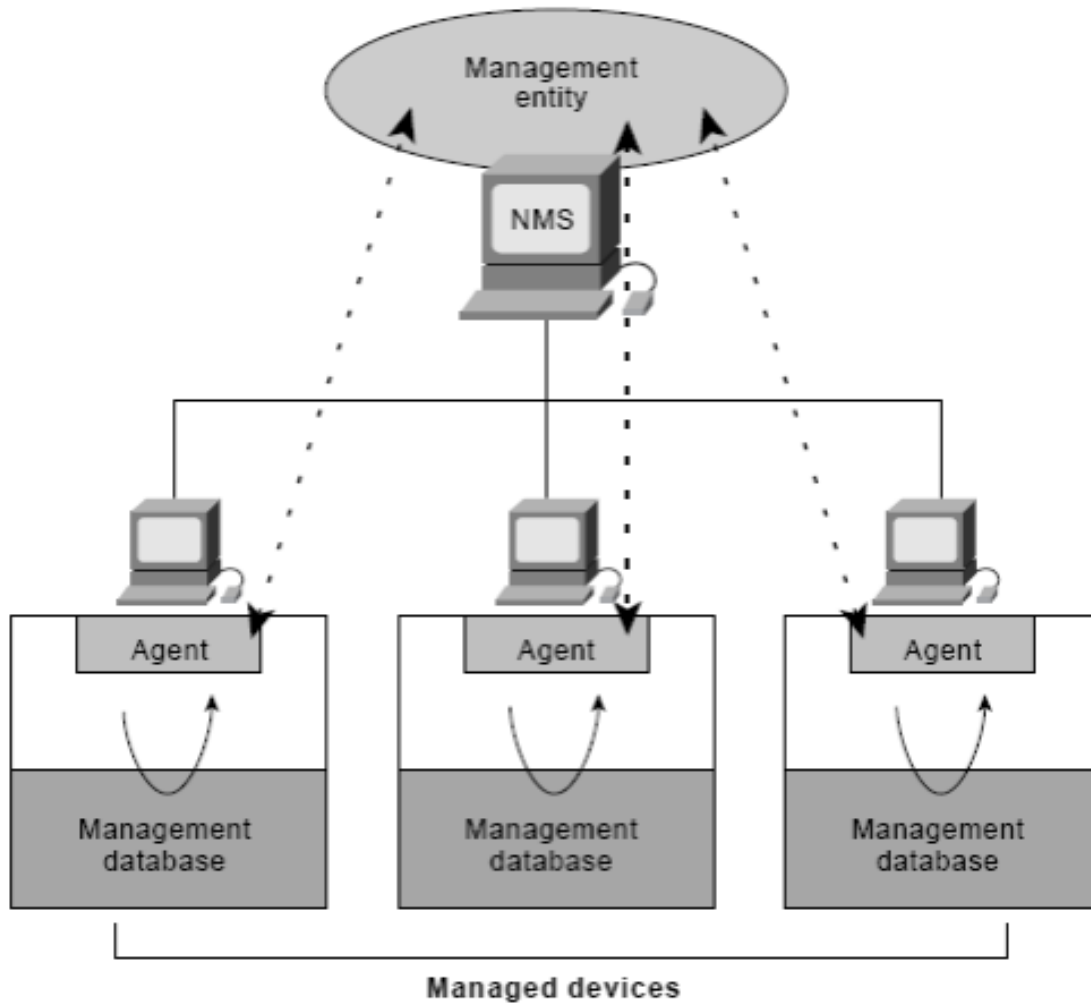


Figura 3.2 Relación entre MD, Agent y NMS



Comandos básicos:

Los dispositivos administrados (MD) son supervisados y controlados utilizando cuatro comandos:

- **Lectura**

Es usado por un NMS para supervisar elementos de red. El NMS examina diferentes variables que son mantenidas por los dispositivos administrados

- **.Escritura**

Es usado por un NMS para controlar elementos de red. El NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrados.

- **Trap**

Usado por los dispositivos administrados para reportar eventos en forma asíncrona a un NMS. Cuando cierto tipo de evento ocurre, un dispositivo administrado envía una notificación al NMS.

- **Transversales**

Usadas por el NMS para determinar que variables soporta un dispositivo administrado y para recoger secuencialmente información en tablas de variables, como por ej. Una tabla de rutas.

Operaciones del protocolo SNMP

La **operación Get** es utilizada por el NMS para recuperar el valor de una o mas instancias de un objeto desde un agente. Si el agente responde a la operación Get y no puede proporcionar valores para todas las instancias del objeto en una lista, no proporcionara entonces ningún valor.

La **operación GetNext** es utilizada por el NMS para recuperar el valor de la siguiente instancia del objeto en una tabla de una lista dentro de un agente.

La **operación Set** es usada por el NMS para colocar los valores de los objetos dentro de un agente.

La **operación Trap** es utilizada por los agentes para informar asíncronamente al NMS sobre un evento importante.

La versión SNMP V2 define 2 nuevas operaciones de protocolo: **GetBulk e inform.**

La **operación GetBulk** es utilizada por el NMS para recuperar de manera eficiente grandes bloques de datos, tales como múltiples filas de una tabla.



La operación GetBulk llena un mensaje de respuesta con la mayor cantidad de datos solicitados.

La **operación Inform** permite que un NMS envíe Traps hacia otro NMS y luego reciba una respuesta.

3.2.2 versiones

Actualmente existen tres versiones SNMP V1, SNMP v2 y SNMP v3, las tres versiones tienen un número de características en común, pero SNMP v2 ofrece mejoras en las operaciones del protocolo; otra versión de SNMP V3 ofrece mejoras sobre los aspectos de seguridad. Se empezó a desarrollar el protocolo en la década de 1980, en vista de la necesidad de una herramienta que permitiera la administración y gestión de las redes. Así nacieron HEMP y HEMS (High-level entity-management system), que es una generalización del que fue quizás el primer protocolo de gestión usado en Internet (HMP), así como otros protocolos que se publicaron antes de que la IETF (Internet Engineering Task Force) decidiese que era necesario estandarizar, por lo que publicó un RFC, donde se especificó como debía desarrollarse el estándar, además de resaltar la importancia del mismo. En sus inicios, se definió que SNMP debía implementarse sobre SGMP, actualmente no es así. A continuación se describen las versiones que posteriormente se desarrollaron e implementaron. Los cambios relevantes en la evolución del protocolo han sido en el área de seguridad.

3.2.2.1 SNMP v1

Fue la primera versión, descrita en el RFC 1067, que posteriormente fue reemplazado por los RFC 1098 y 1157, respectivamente. La seguridad de esta versión se basó en comunidades con contraseñas simples sobre texto plano, lo cual significa que mientras se conoce la clave, se puede utilizar el equipo. Luego se creó una versión SNMPsec, con la intención de incrementar la seguridad en SNMPv1, “en esta versión se incluyeron algunos mecanismos de criptografía y se proponía el uso de parties, que son entidades lógicas que pueden iniciar o recibir una comunicación SNMP.”

Los comandos (PDUs) utilizados son los siguientes:

Transmitidos por el NMS y recibidos por el agente:

- *Get Request*, para solicitar atributos a un objeto.
- *Get Next Request*, solicita el siguiente atributo del objeto.
- *Set Request*, para actualizar uno o más atributos de algún objeto.
- *Set Next Request*, para actualizar el siguiente atributo del mismo objeto.

Transmitidos por los agentes y recibidos por los NMS:

- *Get Response*, devuelve los atributos solicitados con los comandos *GET* transmitidos por el *NMS*.
- *Trap*, información de fallas en el agente.

3.2.2.2 SNMP v2

Se tomo como punto de partida SNMPsec, fue publicada por primera vez en 1992.

En esta versión se añadieron tres comandos:

- *Get bulk Request*, solo en SNMPv2, solicita un conjunto de valores en lugar de solicitarlos uno a uno.
- *Inform Request*, descripción de la base local de información de gestión para intercambiar información de nodos administradores entre ellos.
- *Report*, para intercambio de información de control.

Además, se incluyeron algunos tipos de datos adicionales. “Sobre su arquitectura puede construirse aplicaciones de gestión como alarmas y monitores de desempeño que hasta ahora quedaban fuera del estándar.”(Arazo, 2011)

Las versiones SNMPv2c, SNMPv2u y SNMPv2* aparecieron como mejoras de SNMPv2, SNMPv2c se utilizó mucho y su seguridad estaba basada en comunidades, donde se puede asociar un nombre a un perfil de la base de datos SNMP, junto con los derechos de acceso a dicho perfil. SNMPv2u tenía un modelo de acceso con usuarios y contraseñas. SNMPv2* se desarrolló como un protocolo distinto. No es compatible con el resto.

3.2.2.3 SNMPv3

Es la versión actual, en esta existe distintos módulos que tienen distintas tareas, independizando así los mecanismos de control de acceso, seguridad y gestión.

Se introdujeron el USM y el VACM, lo cual incremento de manera notable la seguridad del protocolo ya que definiciones mucho más específicas de los objetos accesibles.

Además se incluyeron mecanismos de autenticación y privacidad, así como una estructura sobre la cual se pueden configurar nombres de usuario, derechos de acceso y claves asociados a estos, para mayor seguridad.

3.2 Autenticación

Autenticar es autorizar o legalizar algo. La autenticación en este caso es precisamente eso, aplicado a la rama de seguridad información, así como también se puede verificar los usuarios, de manera confiable. Aplicándolo específicamente al tema de SNMP, los agentes y gestores necesitan poder autenticar las solicitudes y respuestas de los otros equipos de la red para evitar amenazas, o para poder evadirlas en caso de que se introdujesen en la red.

Las amenazas más importantes que se pueden mencionar son, por ejemplo, la suplantación, que es simplemente cuando se reemplaza un equipo autorizado por un equipo intruso haciéndose pasar por este. También se debe tener cuidado especial con la posibilidad de que exista modificación de información, esto puede ocurrir si un equipo ajeno a la red interviene en la comunicación entre dos equipos de la red y modifica alguna solicitud o alguna respuesta, puede suceder sin que exista suplantación.

3.2.1 Mecanismos de autenticación

3.2.1.1 HMAC (Hash-based Message Authentication Code- código de Autenticación de Mensajes basado en Hash)

Es un mecanismo que, mediante el uso de algoritmo, calculando un MAC incluyendo una función *hash* y una clave secreta asociada.

MAC es el nombre que típicamente se le da a los mecanismos que sirve para verificar la integridad de la información transmitida en un enlace o red, o de la información almacenada en un medio poco confiable. Se usa dos entidades lógicas que comparten una clave que sirve para validar la información que transmiten entre ellas.

Una función almacenada en un medio poco confiable. Se usan entre dos entidades lógicas que comparten una clave que sirve para validar la información que transmiten entre ellas.

Una función *hash* es una función criptográfica que indexa datos grandes en datos pequeños. Se conocen en español como funciones resumen, ya que lo que hacen es resumir la información original.

El cálculo del HMAC ocurre de la siguiente manera:

El emisor calcula un resumen del mensaje basado en el contenido de la solicitud de respuesta y lo incluye en la cabecera de este. El receptor calcula el resumen del mensaje recibido y verifica que concuerda con el enviado por el emisor. La

clave solo es conocida por emisor y receptor, por lo que cualquier modificación puede ser idéntica.”(Arazo,2011)

Las funciones *bash* que se pueden utilizar son MD5 y SHA-1.

3.2.1.2 MD5 (Message-Digest algorithm 5 – Algoritmo de Digestión de Mensaje 5)

Ronald Rivest (MIT) lo desarrolló, basándose en MD2 y MD4. No tiene mejor rendimiento que MD4 en cuanto a velocidad; pero es mucho más seguro. Produce un número de 128 bits (32 dígitos hexadecimal) partiendo de un texto de cualquier longitud, y lo hace siguiendo una serie de pasos que se enumeran a continuación, obtenidos de Arazo,(2011):

1. **Adición de bit.** El algoritmo inicia añadiendo un relleno al mensaje que sea congruente con $448 \bmod 512$. El relleno está formado por 1 bit “1” seguido por la cantidad necesaria de bits “0”. Se puede añadir entre 1 y 512 bits. El relleno se añade aunque el mensaje original ya sea congruente con $448 \bmod 512$.
2. **Longitud del mensaje.** Se almacena la longitud original del mensaje en los últimos 64 bits del relleno. Si el tamaño fuese mayor a 2^{64} solo se utilizan los 64 bits menos significativos.
3. **Inicialización del búfer MD (*Message Digest*).** Cuatro registros forman el búfer, estos se denominan A,B,C y D y se inicializan siempre con los siguientes valores hexadecimales:

$$A = 67\ 45\ 23\ 01$$

$$B = EF\ CD\ AB\ 89$$

$$C = 98\ BA\ DC\ FE$$

$$D = 10\ 32\ 54\ 76$$

4. **Procesado de mensaje en bloque de 16 palabras.** Cada bloque de 512 bits se divide en 16 palabras 32 bits. El algoritmo opera en cada una de estas por turnos, haciendo 64 operaciones que consisten de 4 etapas llamadas rondas, cada ronda tiene una función asociada y en cada ronda se utiliza una distinta. Las funciones son las siguientes:
5. $f(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$
6. $G(X, Y, Z) = (X \wedge Y) \vee (X \wedge \neg Z)$
7. $H(X, Y, Z) = X \oplus Y \oplus Z$
8. $J(X, Y, Z) = Y \oplus (X \vee \neg Z)$

Los símbolos \oplus , \wedge , \vee , \neg denotan las funciones lógicas: XOR, AND, OR y NOT, respectivamente.

5. **Salida.** El resumen del mensaje es el valor que contienen los registros A, B, C y D después de las operaciones. Empieza en el bit menos significativo de A y termina en el más significativo de D.

3.2.1.3 SHA-1 (*secure Hash Algorithm-1* – Algoritmo Seguro de Hash-1)

Es un algoritmo de la familia de los SHA, que es una familia de funciones *hash* creadas por la Agencia de Seguridad de EEUU. Es el algoritmo más usado de la familia a pesar de que se han encontrado fallas de seguridad, y a pesar de que no se han encontrado ataques exitosos a ninguna de las SHA-2, y la más reciente SHA-3 que fue seleccionada en una competición de funciones *hash* celebrada por el NIST en 2012. Esta última versión se caracteriza por ser la que más difiere de sus predecesoras.

Esta función produce un resumen de 160 bits, su funcionamiento está basado en MD5. Tienen el mismo número de pasos y los 2 primeros son idénticos, las modificaciones se muestran a continuación:

1. **Inicialización del búfer SHA.** En lugar de los 4 registros que existen en MD5, hay registros A, B, C, D y E. A, B, C y D se inicializan igual que en MD5, el registro E se inicializa con el siguiente valor hexadecimal:

$$E=C3\ D2\ E1\ F0$$

2. **Procesado del mensaje de bloques de 16 palabras.** También se utilizan 4 funciones no lineales, una para cada etapa. Cada una de las etapas está compuesta por 20 operaciones que incluyen una de las 4 funciones (la segunda y la última etapa usan la misma función). Se define también una tabla de constantes compuesta por 4 valores diferentes que se mantienen a lo largo de las operaciones. Dichas operaciones modifican los valores de los registros.

El mensaje se divide en bloques de 16 palabras de 32 bits cada una, a partir de estas palabras se hace una extensión, obteniendo 80 palabras.

3. **Salida.** El resumen del mensaje es el valor que contienen los registros A, B, C, D y E.

3.3 Privacidad

Se puede definir como “Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.” Nos referimos a la habilidad de mantener información en secreto o poder seleccionar a quien es revelada, la que se maneja

entre el gestor y el resto de los equipos de la red. Para lograr esto se utilizan herramientas de encriptación para que la información no viaje en texto plano y no sea fácil acceder a ella sin tener autorización significa también conocer el mecanismo de privacidad utilizado para poder hacer la operación necesaria para ver el mensaje completo. Para lograr el proceso de encriptación, los algoritmos que se utilizan son AES, DES y 3-DES. A continuación se da una breve explicación de los mismos.

3.3.1 Mecanismos de privacidad

3.3.1.1 DES (*Data Encryption Standard* – Estándar de Cifrado de Dato)

Es un sistema de cifrado por bloques, es simétrico, los bloques son de 64 bits. La clave que se utiliza es de la misma longitud, pero como un byte se utiliza como control de paridad, solo son efectivos 56 bits de dicha clave.

3.3.1.2 3-DES (*Triple Data Encryption Standard* – Estándar de cifrado de datos tripe)

Es suplemente el algoritmo que resulta de aplicar 3 veces consecutivas el algoritmo DES.

3.3.1.3 AES (*Advanced Encryption Standard* – Estándar de Cifrado Avanzado)

Al igual que los 2 anteriores, es un algoritmo de cifrado por bloques, en este caso son bloques de 128 bits. (Arazo, 2011)

3.4 Elementos de la Arquitectura

Ya que el protocolo SNMP es parte de un modelo de gestión de redes tipo TCP/IP se deben conocer con anticipación varios elementos de dicho modelo para una mejor comprensión de los componentes básicos en una estructura de administración de redes.

3.4.1 NMS (*Network Management Station* – Estación de Gestión de Red)

Son las estaciones de Gestión (hardware), son las interfaces entre el operador humano (administrador de red) y el sistema de gestión de la red, cuenta con una base de datos que contiene toda la información necesaria para la gestión y que se obtiene de todas las bases de datos de las entidades a gestionar.



Un NMS “Suele ser un equipo potente con un CPU veloz, mucha memoria y gran espacio de disco. Generalmente, un solo equipo se encarga de monitorizar todos los elemento de la red.”

La función de los NMS es ejecutar las aplicaciones que controlan y supervisan los dispositivos que se administran en la red. En cualquier red debe existir por lo menos un equipo gestor. La supervisión y el control se logran utilizando comandos básicos de lectura, escritura, notificación y las llamadas operaciones transversales, estas son utilizadas para determinar que variables puede o no soportar un equipo, así como para recolectar información de cualquiera de las tablas variables.

3.4.2 Agente

Es un componente de software que reside en los nodos administrados (elementos de la red, routers, switches, módems, computadores, impresoras....). Su trabajo consiste en responder las solicitudes que recibe, dependiendo del tipo de solicitud, debe devolver un valor o modificarlo (en el dispositivo sobre el que actúa).

3.4.3 MIB (Management information Base – Base de Información de Gestión)

Es una base de datos en la que están contenidos todos los objetos que se van a administrar es la red junto con sus características. La información se almacena en forma de árbol de manera jerárquica.

Tiene 8 niveles de registro:

Grupo	Variable	Significado
<i>System (sys)</i>	<i>sysUpTime</i>	Tiempo desde el ultimo arranque
<i>Interfaces (intf)</i>	<i>ifNumber</i>	Número de Interfaces.
<i>Interfaces (intf)</i>	<i>ifInErrors</i>	Número de paquetes entrantes en los que el agente ha encontrado error.
<i>Address Traslation (add trs)</i>		
<i>Internet Protocol (ip)</i>	<i>ipInReceives</i>	Numero de paquetes recibidos
<i>Internet Control Message (icmp)</i>	<i>icmpInEchos</i>	Número de solicitudes ICMP recibidas.
<i>Transmision Control Protocol (tcp)</i>	<i>tcpInSegs</i>	Número de paquetes TCP recibidos.
<i>User Datagram Protocol (udp)</i>	<i>udpInDatagrams</i>	Número de datagramas UDP recibidos.

Figura 3.1 Niveles de registro del MIB

Fuente: Arazo, 2001

“Para que un dispositivo pueda ser manejado a través de SNMP debe incorporar una MIB que incluya todo los objetos que van a ser accesibles desde un manager instalado en un NMS. La MIB contiene la forma en cómo pueden ser accedidos estos objetos, definiendo la relación existente entre ellos, su estructura y el tipo de dato al que pertenecen.” (Arazon, 2011)

Existen MIBs estándar que tienen una carga predeterminada de objetos que están en todas las redes comúnmente, pueden extenderse añadiendo los objetos que se consideren necesarios. Las MIBs se deben guardar en un lugar determinado, de manera que puedan ser encontradas por el gestor y los agentes cuando arrancan.

También existen MIBs con interfaces graficas, lo cual hace mucho mas sencilla su utilización, ya que se puede acceder a los objetos como en una estructura común de directorios. Cuando no tiene interfaz grafica, deben accederse con comandos. Si se tiene la MIB de un objeto, no es necesario solicitar los objetos con los comandos get ya que se pueden acceder y visualizar de forma sencilla, esto también disminuye el tráfico y mejora el rendimiento del sistema.

3.4.3.1 Árbol MIB

La estructura de las MIBs es un árbol, una estructura en cascada, donde los nodos, que contienen distintos objetos, están ordenados por niveles, según la tarea que deben desempeñar. Se conoce como “el árbol MIB”.

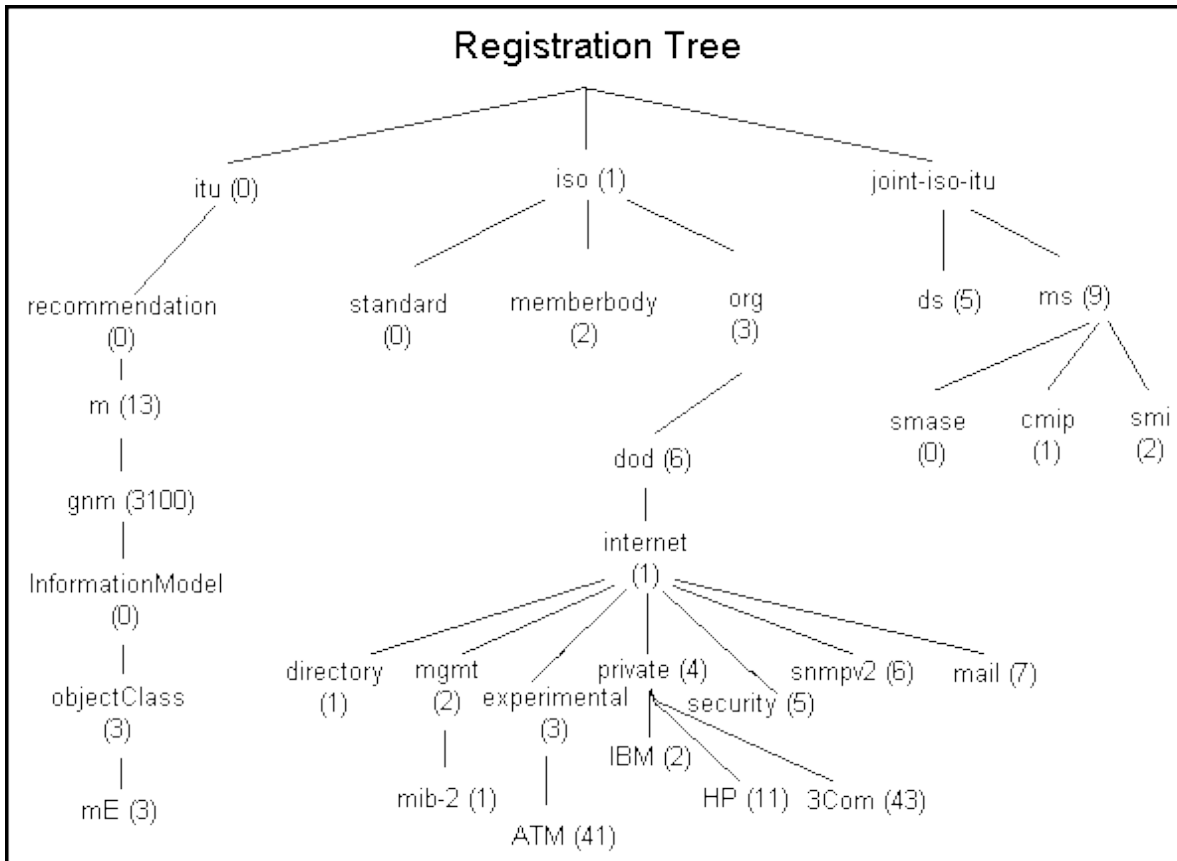


Figura 3.2. Árbol MIB

En la figura se puede observar claramente la división en nodos. La zona superior está reservada para las organizaciones estándares. La rama principal del árbol es el nodo ISO, dentro de esta hay una rama que incluye el resto de las organizaciones (org). El resto de las ramas dentro del nodo ISO son para su propio uso; la misma lógica aplica para los demás nodos y sus ramas.

Ya que el internet es una herramienta extremadamente importante en la actualidad para todos, se describe a continuación este nodo.

- *Directory*, reservada para memorias futuras que discutan sobre la organización de la estructura OSI usada en internet.

- *Mgmt*, identifica los objetos definidos en documentos aprobados por IAB. aquí se almacena las MIBs estándar.
- *Experimental*, almacena las MIBs que están en fase de pruebas.
- *Private*, almacena las MIBs definidas forma unilateral. Dentro de este existe el nodo Enterprise donde hay un espacio reservado para que cada fabricante conocido almacene sus MIBs.
- *Security*, almacena objetos relacionados con seguridad del protocolo.
- *Snmpv2*, para los nuevos objetos de SNMPv2.
- *Mail*, para los objetos de correo electrónico.

Los niveles definidos como superiores van desde el root, el cual es la raíz de todos los demás, hasta las ramas mib-2 y Enterprise.

En la rama mib-2 se describen los grupos de objetos.

3.4.4 ASN.1 (*Abstract Syntax Notation.1* – Notación de sintaxis Abstracta.1)

Notación de sintaxis abstracta1, es un estándar de notación que se desarrollo como parte del modelo OSI, como todos los estándares, describe normas, en este caso, son normas para representar, codificar, decodificar y transmitir datos, también describe tipo de alto nivel, lo cual lo hace sencillo de usar. Es comúnmente utilizado para describir protocolos, en este caso se menciona su existencia debido a que la sintaxis utilizada en SNMP es un subconjunto de esta.

3.4.5 SMI (*Structure of Management Information* – Estructura de Información de Gestión)

Definida dentro del ASN.1, es donde se especifican todas las normas sintácticas para describir los objetos administrables dentro de la MIB, así como los tipos de datos y notaciones permitidos.

Garantiza que los distintos objetos que se van a administrar comparten un lenguaje común y se pueden comunicar exitosamente. Está diseñada para:

“Definir las características generales asociadas a los objetos de un MIB, como deben ser descritos. Definir los tipos de datos que se pueden utilizar al crear los objetos en la MIB. Describir la estructura jerárquica para identificar los objetos. Definir la información de administración asociada a cada objeto de la MIB.”

SIMBOLO	SIGNIFICADO
::=	Asignación
	Alternativa
{ }	Inicio y final de una lista
[]	Inicio y final de una etiqueta
()	Inicio y final de un subtipo
-	Numero con signo
--	Comentario
..	Rango

Figura 3.3 símbolos ASN.1

ELEMENTO	CONVENCIÓN
Tipo	Inicial en mayúscula
Valor	Inicial en minúscula
Macro	Todas mayúsculas
Modelo	Inicial en mayúsculas
Palabra clave	Todas mayúsculas

Figura 3.4 convenciones ASN.1 para escritura de nombres de los tipos de elementos en una MIB.

Fuente: Arazo, 2011.

3.5 Mensajes

Los mensajes SNMP están conformados por tres campos:

1. **Versión.** Donde se indica la versión del protocolo que se esta utilizando.
2. **Comunidad:** indica la comunidad que se utiliza.
3. **PDU:** contiene la información específica del comando que género el mensaje. Este campo puede tener configuraciones distintas según el comando enviado.

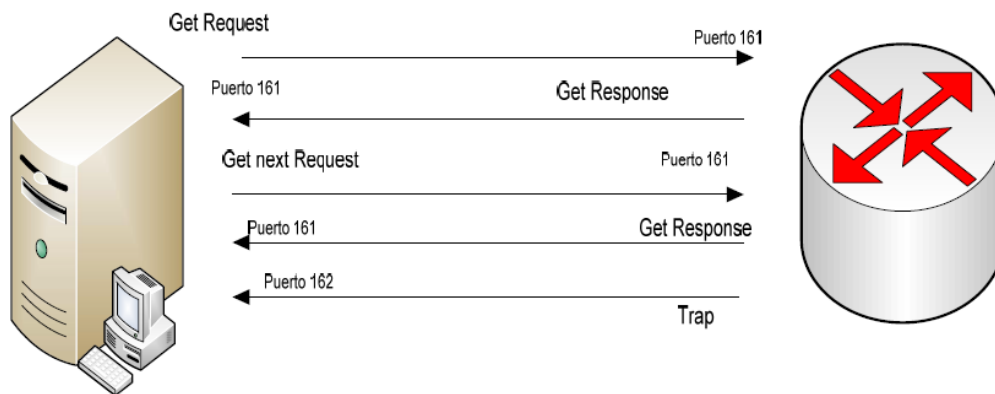


Figura 3.5 Intercambio de Mensajes

3.6 Redes de Información

Una red se puede definir como una tela de araña, en este caso, los hilos son cables y los puntos de agarre computadoras o dispositivos, teniendo esto en cuenta, una red es la interconexión de múltiples equipos (computadoras, router, switches...), debido a la necesidad de un intercambio de información constante, ya que hoy en día dependemos de ellos como nunca antes en la historia. Como ya se ha mencionado, en internet existen diversos protocolos, los cuales tienen una o varias tareas específicas en distintas áreas, para que se lleve a cabo un buen traslado de información (efectivo y seguro) a través de los distintos medios físicos a utilizar, lógicamente podemos imaginar que existen redes de distintos tamaños, lo cual es cierto y cada una tiene características y funciones distintas, éstas se definirán a continuación.

3.6.1 Redes de área local

Comúnmente llamadas redes LAN (Local Área Network), son redes de datos de alta velocidad y, como su nombre lo indica, son locales, lo cual se refiere que están geográficamente limitadas, frecuentemente se implementan en oficinas o edificios. Al igual que cualquier otra red, su función es interconectar los equipos que se desea que la conformen, bien sea para que intercambien información o para poder acceder unos a otros de manera remota y utilizar los servicios que ofrece cada uno sin necesidad de que se implementen varios equipos iguales, un ejemplo de ello es una impresora de uso común en una oficina, todos los agentes pueden imprimir los documentos que generan en sus equipos, sin necesidad de cada uno tenga una impresora en su puesto de trabajo ya que la impresora está conectada a la red y se puede utilizar de manera remota. Este tipo de redes tienen protocolos y tecnologías de transmisión diferentes a las demás, así mismo, pueden utilizar distintas topologías, dependiendo de las necesidades que se desean cubrir.

“Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red.”

3.6.1.1 Ethernet

Se puede considerar este como el estándar mas usado en las redes de área local para la conexión de sus equipos, esta definido por el estándar IEEE 802.3 publicado en 1983, es compatible con las capas 1 y 2 del modelo referencial OSI, este estándar funciona con modulaciones banda base o banda ancha, existen diversas tecnologías que han evolucionado a partir de esta, las cuales solo presentan ligeras modificaciones, ya sea en cuanto a velocidad o medio físico que utilizan.

Las velocidades de transmisión en Ethernet son las siguientes:

- Ethernet: 10Mbps.
- FastEthernet: 100Mbps.
- GigabitEthernet: 1000Mbps.
- 10GigabitEthernet: 10000Mbps.

Los medios físicos de transmisión usados en este protocolo son los siguientes:

- Cable coaxial grueso o delgado.
- Cable UTP categoría de la 3 a la 6.
- Fibra óptica, multimodo o monomodo.

En la siguiente tabla se describe la relación entre las velocidades de transmisión y los medios físicos a usar.

VELOCIDADES Mbps	MODULACIÓN	MEDIO	DESCRIPCION
10	BASE	2	Coaxial delgado
		5	Coaxial grueso
		T	Cable UTP
100	BASE	T	Cable UTP
		F	Fibra óptica
1000	BASE	T	Cable UTP
		S,L	Fibra óptica

Figura 3.6 Tecnologías Ethernet

Fuente: <http://www.ie.itcr.ac.cr/Faustino/Redes/Clase8/4.2Ethernet.pdf>

3.6.2 Redes de área metropolitana

Son las denominadas redes MAN (Metropolitana Área Network), son una versión extendida a nivel de geográfico de las redes LAN, lo que se quiso hacer con este tipo de red fue usar una arquitectura muy similar a las redes de área local pero con conexiones privadas de larga distancias, este tipo de red fue la base de la evolución de lo que actualmente se conoce como tecnología 4G como WiMAX y LTE, las cuales tienen como características principal el alcance de altas velocidades a larga distancias.

3.6.3 Redes de área amplia

Son aquellas redes que operen mas allá de las distancias geográficas en las que puede operar una red LAN, este tipo de red es necesario para conectar distintas redes privadas, comúnmente el acceso a esta se hace a través de un router, pueden tener una extensión que abarque una ciudad o ciudades, incluso continentes, por lo general, las empresas no pueden crear enlaces directos con otras sucursales en su misma ciudad o alrededor del mundo, por lo que se ven en la necesidad de pagar a un proveedor de servicios de redes de área local, para poder conectarse a otras sucursales o otros hosts alrededor del planeta.

“Las tecnologías LAN proporcionan velocidad y rentabilidad para la transmisión de datos de organizaciones, a través de áreas geográficas relativamente pequeñas. Sin embargo, hay otras necesidades empresariales que requieren la comunicación entre sitios remotos, incluidas las siguientes:

- Los empleados de las oficinas regionales o las sucursales de una organización necesitan comunicarse y compartir datos con la sede central.
- Con frecuencia, las organizaciones desean compartir información con otras organizaciones que se encuentran a grande distancias. Por ejemplo, los fabricantes de software comunican periódicamente información sobre productos y promociones a los distribuidores que venden sus productos a los usuarios finales.
- Con frecuencia, los empleados que viajan por temas relacionados con la empresa necesitan acceder a la información que se encuentra en las redes corporativas.”

A continuación se presenta una representación gráfica de una red WAN.

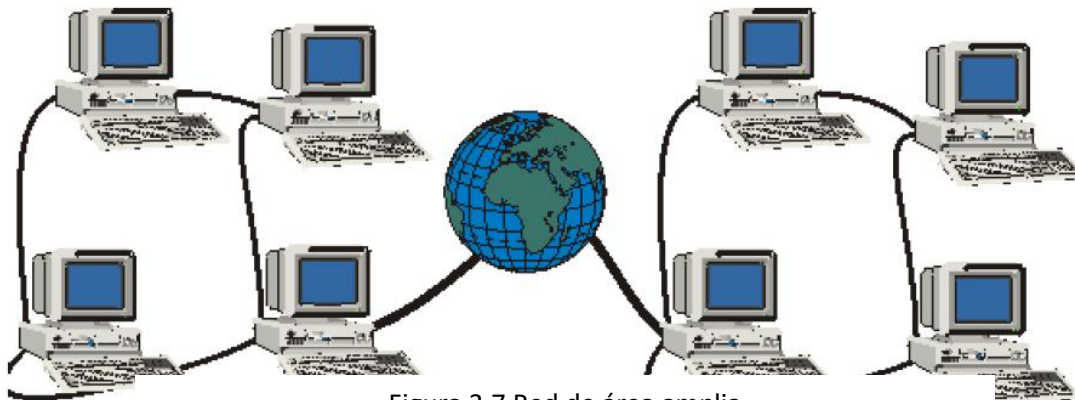


Figura 3.7 Red de área amplia

3.6.4 Redes virtuales privadas.

En los últimos años, el costo de implementación de un enlace físico dedicado ha incrementado considerablemente, por lo que en muchos casos se han visto afectadas las empresas que requieren, por ejemplo, empresas con distintas sedes o sucursales en el territorio nacional. Como solución a este problema se han implementado redes privadas virtuales, estas establecen conexiones punto a punto sin necesidad de la arquitectura que requiere un enlace dedicado, esta conexión se puede lograr a través de una red WAN.

Concretamente, una VPN (virtual Private Network) es una red virtual que se puede implementar sobre una red física, que bien puede ser internet o WAN, independientemente del protocolo de enlace de datos que esté utilizando, por ello,

representa un bajo costo para las empresas comparados con un enlace dedicado de un proveedor de servicios.

3.6.4.1 Funcionamiento general de una red virtual privada

Su funcionamiento general es simple, dado que estas crean una especie de túnel privado donde ambas partes negocian el tipo de autenticación y encriptación de datos a utilizar ya que es una conexión privada usando un medio de transmisión público, como el internet.

Por lo general, las empresas necesitan implementar servidores VPN en su red para aplicar este servicio, el mismo podría tener la operatividad como Gateway de la LAN que se desea conectar con su par a distancia, o puede ser simplemente un computador más de la red. También se debe instalar un cliente VPN, software que sirve para comunicar los equipos de la red con el servidor VPN y, una vez efectuado este proceso, poder acceder al túnel privado entre los dos puntos de interés.

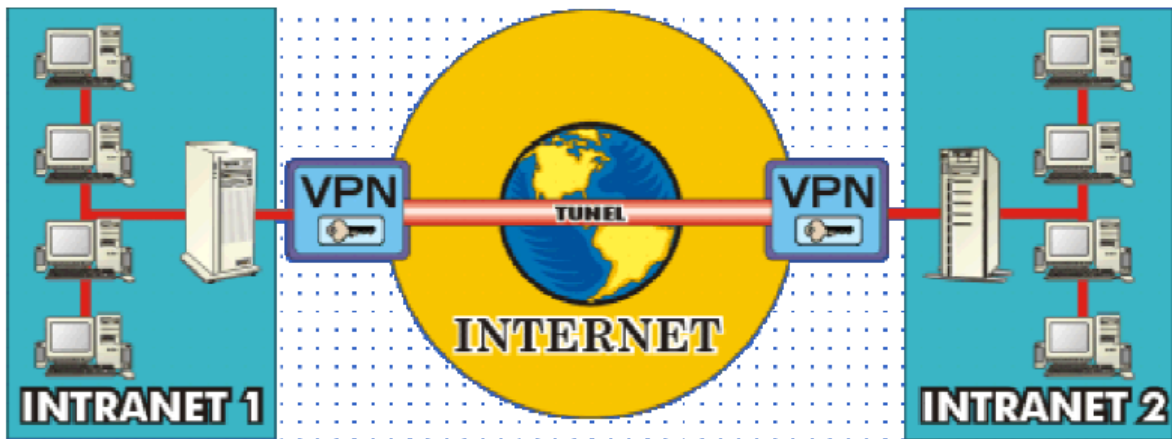


Figura 3.8 Esquema de una VPN

Fuente: http://www.redes-linux.com/manuales/vpn/Estudios_VPN.pdf

3.7 Elementos de red

3.7.1 Routers

Los *routers* son equipo que se utilizan para “enrutar” la información , se encarga de marcar o determinar la vía por la cual debe viajar dicha información, mediante una serie de reglas y estándares, y tras una serie de configuraciones; lo hacen de forma automatizada, haciendo el trabajo del administrador de la red increíblemente más sencillo. Mediante el uso de estos equipos se pueden interconectar redes, bien sea LANs, WANs, o cualquier tipo de red, con otro tipo, por ejemplo, la red local de una casa a la internet. Debido a las características antes mencionadas (interconectar y enrutar), los *routers* son los responsables de que los paquetes sean entregados a través de las redes en las que estos trabajan de manera inequívoca. Para lograr esto, son capaces de crear rutas alternas en caso de que falle la ruta principal, de esta manera garantizan el servicio. Así mismo, proveen servicios integrados de datos, voz y video, y dan prioridad a los paquetes, por lo que se pueden utilizar para transmisiones en tiempo real sin ningún problema, ya que tienen la capacidad de permitir o denegar el acceso de paquetes a la red colabora con la seguridad de la misma.

Estos equipos son extremadamente similares a los computadores, tienen CPU (Central Processing Unit – Unidad de Proceso Central), memorias ROM (*Read-Only Memory* – Memoria de solo lectura) y RAM (*Random Access Memory* – Memoria de Acceso Aleatorio), y cuenta con un sistema operativo, mediante el cual se puede programar y configurar.

Los *routers*, en general, son invisibles para el usuario. Entre el computador que una persona opera y el servidor al que ingresa puede haber cualquier cantidad de routers que se encargan de que la conexión pueda realizarse. Debido a que conectan muchas redes, tienen varias interfaces, cada una de las cuales está identificada con una dirección IP correspondiente con la red en la que se encuentre. Es común que tengan interfaces para WAN e interfaces para redes LAN.

Para lograr hacer su trabajo y determinar las rutas para los paquetes, la herramienta que utiliza es la tabla de enrutamiento, en esta tabla están contenidos una serie de detalles que permiten al *router*, utilizando distintos algoritmos, decidir cuál es la ruta más conveniente en cada caso, también incluye la dirección de la interfaz por la cual es la que saldrá el paquete. Dependiendo de los protocolos que utilicen los enlaces a los que se conectan estas interfaces, los paquetes pueden tener formatos diferentes (Ethernet, PPP...) cada uno de los protocolos tiene sus propios estándares de encapsulado de paquetes, por lo que el *router* puede hacer el proceso de desencapsulado y re-encapsulado dependiendo de los medios a los cuales está conectado.

Para aprender sobre las redes remotas y poder hacer el direccionamiento, los *routers* utilizan rutas estáticas y enrutamiento dinámico, las rutas estáticas suelen utilizarse cuando se trabaja con una red de pocos equipos, cuando la red tiene un único punto de salida a internet o en situaciones que no requieran de enrutamiento dinámico; por otra parte, el enrutamiento dinámico es una herramienta extremadamente útil cuando se desea acceder a redes remotas, este tipo de enrutamiento también actualiza las tablas de enrutamiento cada cierto tiempo, y, de haber cambios en la topología, los refleja modificando la misma.

Los *routers* cuentan con una serie de interfaces físicas mediante las cuales se pueden administrar, se les conoce como puertos de administración, estos puertos no se utilizan para el envío de paquetes. Entre estos el más popular es el llamado puerto de consola, allí se puede conectar un computador donde se ejecute un software que emule el terminal que se necesita para configurar el *router* sin necesidad de acceder a la red, o bien se puede conectar un terminal. La razón por la que es necesario un terminal es que los *routers* tienen un sistema operativo que administra sus recursos (asignación de memoria, procesos, seguridad, sistemas de archivos y cualquier otro recurso de software además de los recursos de hardware). Además de las interfaces de administración previamente mencionadas, los enrutadores tienen interfaces de conexión, a través de estas se conectan a las redes, pueden ser de distintos tipos, para conectar a distintos tipos de red, todas las interfaces que se mencionan en este párrafo son físicas y se encuentran en la parte externa del *router*. Al igual que un sinfín de equipos electrónicos, los *routers* cuentan con indicadores LED destinados a cumplir distintas funciones, generalmente se cuenta con un LED que indica si el equipo está encendido o no, uno por cada interfaz física que indica si existe una conexión y con uno por cada interfaz física que indica que se está enviando/recibiendo información, esto no es una condición sine qua non, dependiendo del tipo de *router* (marca, modelo) estas características pueden variar.

Entre las interfaces para conexión de red comúnmente se observan LAN y WAN, las cuales se utilizan, como es de suponerse, para conectar el router a una LAN o una WAN, respectivamente.

3.7.2 Equipos de comunicación a Configurar

Matrix 5000

El UPS es un mejorado sistema de alimentación ininterrumpida de línea interactiva de alta potencia que proporciona, de alimentación de CA limpia y confiable a la computadora, manejo de datos y cargas de telecomunicaciones. Normalmente, el UPS funciona en línea y proporciona la energía derivada de la entrada de red fuente, regulando continuamente la tensión de carga para compensar las fluctuaciones de tensión en la red eléctrica. Un circuito de cambio de toma del

transformador multinivel ofrece esta regulación, mientras que el logro de altos niveles de eficiencia en línea. Para ajustar la tensión de carga, el UPS hace funcionar temporalmente la carga de la batería mientras se realiza un cambio de toma del transformador adecuado. Si las condiciones son inaceptables, el UPS se transfiere la carga de energía de la red eléctrica a la (funcionamiento con batería) inversor de forma sincrónica y prácticamente sin problemas en todas las condiciones. La forma de onda de tensión durante el funcionamiento a batería es una onda sinusoidal de baja distorsión. Resincronización y la transferencia de poder de nuevo carga a la red es automática cuando el voltaje de la línea es de nuevo dentro de los límites normales.

Un sistema UPS completo se compone de tres tipos de módulos: una unidad electrónica (UE) montado en la parte superior de una unidad de aislamiento (IU), y unidades de alimentación, que puede ser añadido para aumentar el tiempo de ejecución de batería. La UE sí se conecta a la IU cuando se monta, y contiene controles de microprocesador del UPSs, inversor, cargador de batería, transferencia y circuitos de derivación cambiando, las interfaces remotas, y el control de usuario y panel de visualización.

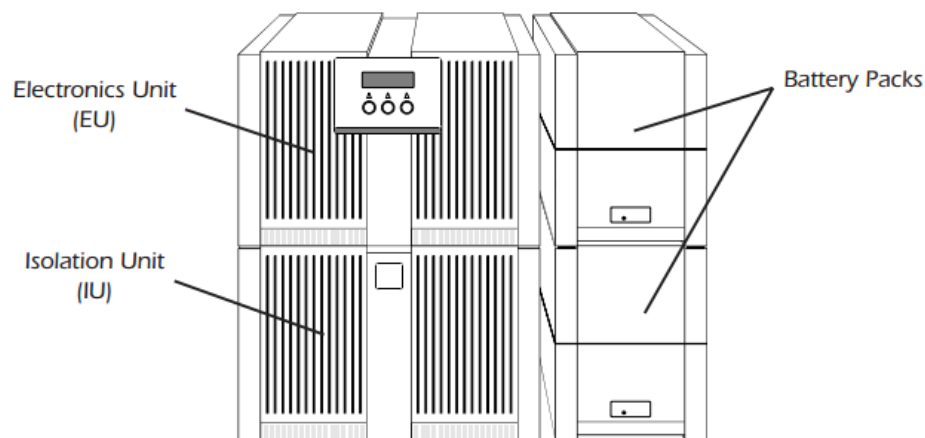


Figura 3.9 Matrix5000

Motorola pidu:

El PIDU Plus genera la tensión de alimentación de la ODU de la red eléctrica (o de una fuente externa de CC) e inyecta esta tensión de alimentación en la ODU. El PIDU Plus está conectado a la ODU y equipos de red mediante un cable CAT5e con conectores RJ45.

INTERFACES	FUNCIONES
100-240V 47-63Hz 1.8 ^a DC in	Red de entrada (figura 1.8) Entrada de alimentación de CC alternativa. Se refieren a configuraciones de redundancia y alimentación alternativa.
DC Out	Salida de potencia DC a una segunda PIDU Plus. Se utiliza para proporcionar redundancia de suministro de energía.
ODU	enchufe RJ45 para conectar el cable CAT5e para ODU.
LAN	Enchufe RJ45 para conectar el cable CAT5e de la red.
Recovery	Se utiliza para recuperar la unidad de errores de configuración o la corrupción de imágenes de software.

Tabla 1-3. Interfaces de PIDU Plus.

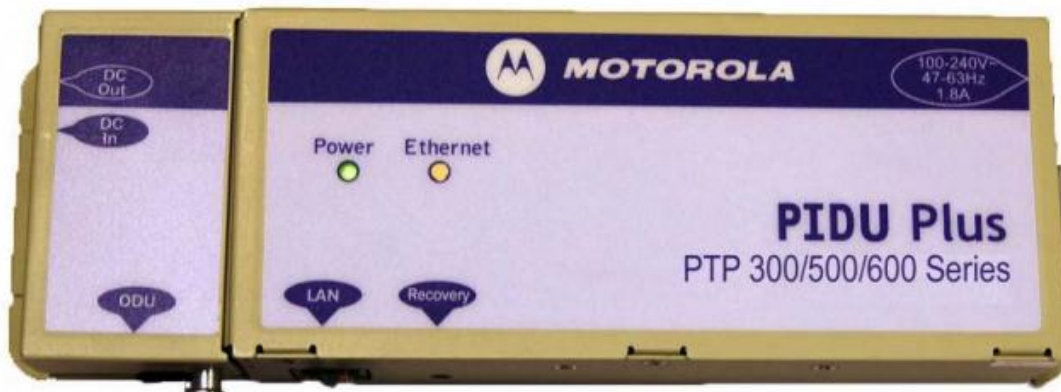


Figura 3.10 Motorola PIDU Plus

RAD205A:

El dispositivo de demarcación ETX-205A Carrier Ethernet ofrece la funcionalidad de demarcación Ethernet para servicios empresariales, así como la funcionalidad de puerta de enlace del sitio celular para aplicaciones de backhaul móviles. Proporciona control de servicio de extremo a extremo y la gestión del rendimiento a través de redes de paquetes.

El dispositivo ofrece servicios de negocios basados en SLA a las instalaciones del cliente a través de conexiones Ethernet nativas, que termina por encima de cualquier tipo de red de paquetes.

ETX-205A transporta hasta cinco Gbps de rendimiento para el usuario al tiempo que garantiza la SDH / SONET rendimiento similar y confiabilidad de cinco nueves.

ETX-205A puede entregar VPN IP, VoIP y acceso dedicado a Internet sobre el mismo enlace físico como un servicio de LAN-to-LAN de capa 2, todos con calidad diferenciada del servicio y la supervisión de extremo a extremo.



Figura 3.11 ETX-205A

SWT3000:

Con el SWT 3000 pueden utilizarse vías analógicas y digitales de transmisión en la misma red. Además, las conexiones de comunicaciones analógicas y digitales pueden equiparse con interfaces ópticas, incluso después de la instalación de los sistemas.

El SWT 3000 puede equiparse con una segunda fuente de alimentación redundante “Hot-Standby” para mejorar su seguridad. Si falla la fuente de alimentación principal, la segunda continuará operando sin que se produzcan interrupciones, procurando un servicio continuo del SWT 3000. Además, las dos fuentes de alimentación eléctrica pueden tomar la energía de fuentes diferentes (por ejemplo, la alimentación primaria, 230 V AC, y la alimentación secundaria, 110 V DC).

En el SWT 3000 se reúnen distintas técnicas nuevas que contribuyen a una mejora del rendimiento del sistema en los siguientes campos:

- Siemens desarrolló la tecnología INC (Impulse Noise Compression) para asegurar que los impulsos de ruido, hasta ahora, la mayor fuente de errores en redes analógicas no se interpreten como comandos, evitando que lleven a activaciones erróneas.
- El direccionamiento de los dispositivos impide que se produzcan conexiones involuntarias entre dos de ellos debido a un routing incorrecto

en redes digitales, al tiempo que garantiza que las señales de protección correctas alcancen el destino deseado.

- La conmutación a una ruta alternativa permite una redundancia completa de la vía de transmisión.
- Fuente de alimentación redundante con la función “Hot-Standby”.
- Varias conexiones directas por cables de fibra óptica entre dos SWT 3000, conexión por fibra óptica a un multiplexor o a un equipo de onda portadora PLC.
- Modo de activación codificada para cuatro órdenes independientes a través de líneas de transmisión analógicas.

Cargadores EMEISA:

En conjunto con su correspondiente baterías conforman un sistema estacionario utilizado para garantizar la alimentación de los servicios en Corriente Directa (CD) en caso de ausencia del suministro de Corriente Alterna (CA), en esta situación la batería es la que se encarga de entregar la corriente necesaria a los consumidores hasta que se restablezca el servidor de energía (CA), se ponga en marcha un grupo electrógeno o para dar tiempo a realizar las maniobras necesarias antes de quedarse definitivamente sin energía.

Adicionalmente incorporan protecciones contra sobrecargas, sobretensiones y cortocircuito, y además de limitar electrónicamente la corriente máxima de salida asignada, también son capaces de limitar la corriente de carga de las baterías en función del tipo y modelo, con el propósito de protegerlas y alargar al máximo su vida útil.

Cada Cargador tiene programado dos niveles de carga (Flotación e Igualación ó carga rápida) los cuales son ajustados en fábrica dependiendo de las características de las baterías, estos valores pueden ser modificados posteriormente por el usuario si a lo largo del tiempo de operación del equipo cambian las circunstancias de uso. Habitualmente los Cargadores trabajan en flotación, esto es, alimentan a los servicios a la vez que mantienen cargadas las baterías. Cuando se presenta una falla en la red que suministra corriente alterna (CA), la batería se descarga hasta que la alimentación se restablezca, momento en el cual el rectificador entra automáticamente en igualación (carga rápida) para recargar la batería lo antes posible en previsión de otra eventualidad.



Figura 3.12 cargadores EMEISA

3.8 ICMP (*Internet Control Message Protocol* – *Protocolo de Mensaje de Control de Internet*)

El protocolo ICMP es uno de los protocolos del grupo de protocolos de internet, del cual forman parte todos los protocolos usando para internet y redes similares, envían mensajes con características similares a las de un datagrama UDP, pero con un formato más simple, ya que en vez de contener los datos enviados con información de usuario, se basa en controlar si el paquete no puede alcanzar un destino o si su vida a expirado. Se puede decir que es un protocolo orientado al manejo de errores, es una herramienta de gran valor para los administradores de red, ya que de esta forma se puede confirmar o no la conexión entre varios hosts y al mismo tiempo muestra información del problema.

Existen distintos tipos de mensajes ICMP, entre los cuales destacan los mensajes echo request (8) y echo reply (0), los cuales son utilizados para hacer el comúnmente conocido “ping”, bien sea para comprobar el estado de un enlace local, un enlace remoto o el estado de la tarjeta de red del propio dispositivo. (El protocolo ICMP, 2012).

3.9 ZABBIX

ZABBIX es un software de fuente abierta, esto se refiere que está basado en software libre. Esta herramienta permite controlar numerosos parámetros de red, así como la salud e integridad de los distintos servicios o dispositivos. ZABBIX utiliza distintos mecanismos de notificaciones, como SMS y correos electrónicos.

ZABBIX utiliza un mecanismo flexible de la notificación que permita que los usuarios configurar e-mail para cualquier acontecimiento. Esto permite una reacción rápida a los problemas del servidor, tiene una buena presentación de



informes y características de visualización de datos basados en los datos almacenados.

Todos los informes y estadísticas, así como los parámetros de configuración se acceden a través de un interfaz basado en web final. Basado en la web asegura que el estado de la red y de los servidores pueden ser evaluados desde cualquier ubicación, esto si se configura correctamente.

ZABBIX es libre de costo, esto significa que su código fuente se distribuye gratuitamente y está disponible para el público en general. bbix ofrece:

- La detección automática de servidores y dispositivos de red
- Monitorización con administración centralizada WEB
- Soporte para los mecanismos de captura
- Software de servidor para Linux, Solaris, HP-UX, AIX, BSD libres, BSD Open OS X
- Agentes de alto rendimiento (software de cliente para Linux, Solaris, HP-UX, AIX, BSD libres, BSD Open, OS x, Tru64/OSF1, Windows NT 4.0, Windows 200, Windows 2003, Windows XP, Windows Vista)
- Autenticación de usuario segura.
- Permisos de usuarios flexibles
- Interfaz basada en web
- Notificación flexible de correo electrónico de eventos predefinidos
- Alto nivel (de negocios) vista de los recursos controlados
- Registro de auditoria

Capítulo IV

Desarrollo

En este capítulo se describe el proceso que se siguió para la realización del trabajo, las fases en las que se dividió el mismo y todos los detalles correspondientes con la implementación del software y su puesta en marcha, así como las pruebas de funcionamiento realizadas al culminarlo.

4.1 INVESTIGACION

El trabajo se inicio con una fase de investigación acerca de los temas que se tratarían y el protocolo a utilizar. La finalidad principal de esta fase fue obtener conocimientos teóricos necesarios para poder proceder con las fases de implementación del proyecto; igualmente resulta importante al ser el capítulo inicial del trabajo ya que permite al lector conocer la teoría necesaria para el desarrollo del mismo.

Se investigo el protocolo simple de gestión de red (SNMP), siendo este el más importante ya que este protocolo está incluido dentro del firmware de los equipos a monitorear, en este entorno se realizaron descripciones de las versiones existentes del protocolo, los comandos que se utilizan comúnmente en cada una de ellas, las características importantes de seguridad y privacidad disponibles al utilizarlo, entre otros. Se describió de manera detallada la arquitectura del protocolo, deteniéndose en cada uno de los elementos que la componen, y la lógica de funcionamiento del mismo.

De manera complementaria se dedico parte del capítulo a la descripción de las redes de información, los tipos de redes más comunes según su alcance, los equipos que actualmente se encuentran operando en la CFE

También se realizo la selección del software ZABBIX, la razón por la cual se tomo la decisión de utilizarlo es que, además de ser totalmente gratuito y es de configuración sencilla y capaz de obtener datos, manejar estadísticas y crear gráficos, sin necesidad de utilizar software adicional.

4.2 Instalación de software

4.2.1 Instalación de centos.

Se formateo la maquina la que se encuentra en la Site de comunicaciones ubicado de la gerencia, contaba con el sistema operativo WINDOWS 7. Se sustituyo por el sistema operativo centos 6, es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, se instalo centos ya que es un sistema estable y confiable para proceso que requieren alto consumos de recursos.

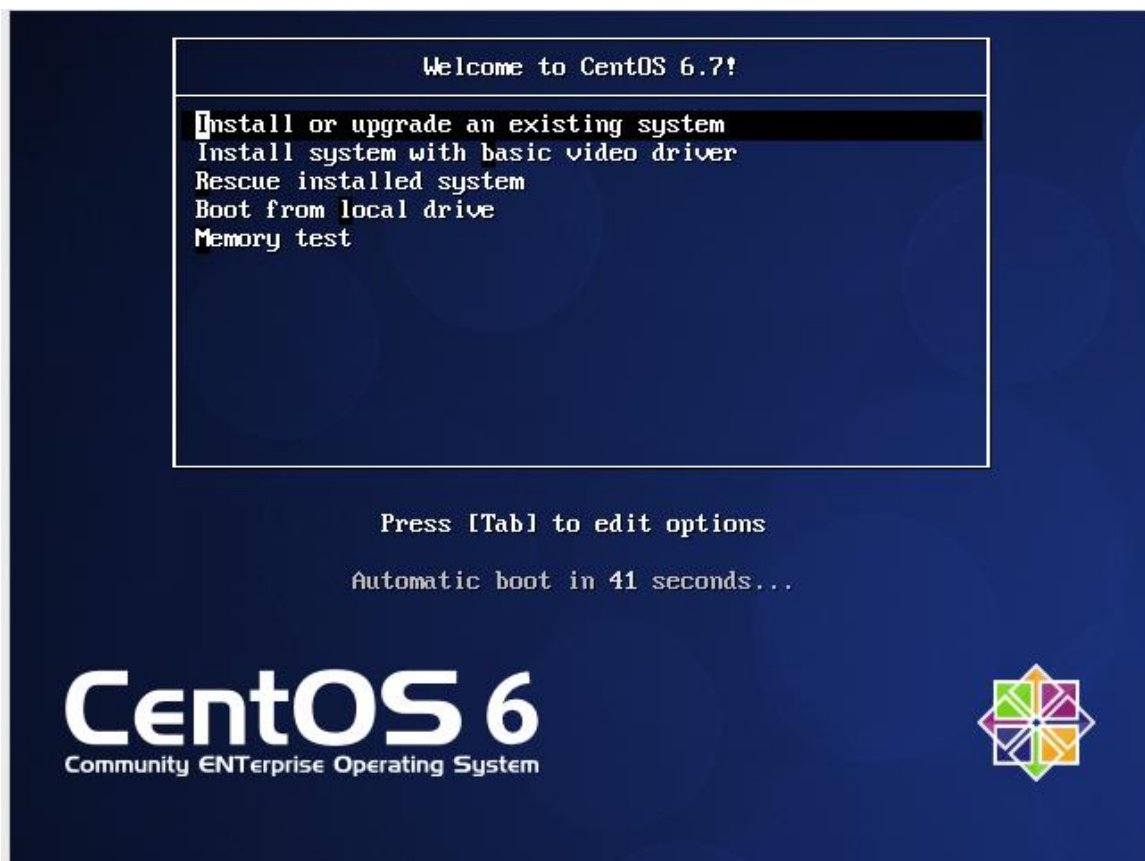


Figura 4.1 instalación de centos
Fuente: Elaboración propia.

4.2.2 Instalación de ZABBIX

ZABBIX requiere de la instalación previa de un software de base de datos y de php para su funcionamiento, para la instalación del mismo se utilizó el comando que se muestra a continuación:

Software	Versión	Comentarios
Apache	1.3.12 o posterior	
PHP	5.0 o posterior	
Módulos PHP: php-gd	GD 2.0 o posterior	Debe soportar imágenes .png
MySQL php-mysql	3.22 o posterior	Si se utilizara MySQL como base de datos para ZABBIX
Servidor: fping		Se requiere para artículos de ping ICMP
Servidor: net-snmp		Se requiere para el soporte SNMP

Tabla 1-4 Requisitos de software para la instalación de ZABBIX.

Fuente: Elaboración propia.

Por otra parte, los requisitos de hardware para un óptimo desempeño del software dependen de la cantidad de hosts a monitorear.

4.2.2.1 Descarga de repositorios ZABBIX

Se descargó el software de monitorización ZABBIX, para la descarga se utilizó la página principal www.zabbix.com, en la cual se consiguieron todas las versiones existentes, así como los manuales de funcionamiento.

Para la descarga se utilizó el comando

- `Rpm -ivh http://repo.zabbix.com/zabbix/2.4/rhel/6/x86_64/zabbix-release-2.4.1.el6.noarch.rpm`

4.2.2.2 Instalación de requisitos de paquetes del ZABBIX.

Como se mencionó anteriormente, ZABBIX requiere de la instalación previa de un software de base de datos y php para su funcionamiento, para la instalación del mismo se utilizó el comando que se muestra a continuación:

```
# yum install zabbix-server-mysql zabbix-web-mysql
```

```
root@sannet-VirtualBox:~/home/sannet# wget http://sourceforge.net/projects/zabbix/files/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz/download?use_mirror=voxel
--2012-04-12 12:24:16-- http://sourceforge.net/projects/zabbix/files/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz/download?use_mirror=voxel
Resolviendo sourceforge.net... 216.34.181.60
Conectando a sourceforge.net|216.34.181.60|:80... conectado.
PeticiÃ³n HTTP enviada, esperando respuesta... 302 Found
UbicaciÃ³n: http://downloads.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz?r=sts=1334249660&use_mirror=voxel [siguiente]
--2012-04-12 12:24:21-- http://downloads.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz?r=sts=1334249660&use_mirror=voxel
Resolviendo downloads.sourceforge.net... 216.34.181.59
Conectando a downloads.sourceforge.net|216.34.181.59|:80... conectado.
PeticiÃ³n HTTP enviada, esperando respuesta... 302 Found
UbicaciÃ³n: http://voxel.dl.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz [siguiente]
--2012-04-12 12:24:22-- http://voxel.dl.sourceforge.net/project/zabbix/ZABBIX%20Latest%20Stable/1.8.11/zabbix-1.8.11.tar.gz
Resolviendo voxel.dl.sourceforge.net... 74.63.52.163, 74.63.52.166, 74.63.52.167
...
Conectando a voxel.dl.sourceforge.net|74.63.52.163|:80... conectado.
PeticiÃ³n HTTP enviada, esperando respuesta... 200 OK
Longitud: 4224738 (4.0M) [application/x-gzip]
Guardando en: Ã¿download?use_mirror=voxelÃ¿
0% [=====>
```

Figura 4.3. Instalaci3n de la fuente ZABBIX.

Fuente: Elaboraci3n propia.

4.2.2.3 CONFIGURACION DE BASE DE DATOS

Se escogi3 utilizar como software de base de datos MySQL, debido a su popularidad para este tipo de aplicaciones, aunque este no es el 3nico software de base de datos que se puede utilizar con ZABBIX. Una vez descargados los paquetes correspondientes con el software de base de datos MySQL, resultado necesario configurar de la misma manera que pudiese gestionar los usuarios configurados en ZABBIX junto con los datos correspondientes a cada uno; para la configuraci3n, se otorgaron permisos al usuario de manera que los mismos se ajustase a las labores que este debe cumplir dentro de la red.

4.2.2.4 Configuraci3n de puertos en el FIREWALL

Se tuvo que dar d permisos para permitir que el trÃ¡fico interno salga a internet con los siguientes puertos:

- Puerto 161 (requests)
- Puerto 162 (traps)

4.2.2.5 Configuración de zabbix_server.conf

En la fase de configuración del servidor se modifico el archivo zabbix_server.conf, de manera que reconociera el usuario y contraseña correspondientes al administrador de la red, este archivo se ubica en la carpeta /etc/zabbix/zabbix_server.conf. Esto es con el fin de dar accesos al servidor ZABBIX a la base de datos MySQL.

```
GNU nano 2.0.9          Fichero: zabbix_server.conf
# DBName=
DBName=zabbix
### Option: DBSchema
#   Schema name. Used for IBM DB2 and PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=
### Option: DBUser
#   Database user. Ignored for SQLite.
#
# Mandatory: no
# Default:
# DBUser=
DBUser=zabbix
^G Ver ayuda  ^O Guardar  ^R Leer Fich ^Y Pág Ant  ^K CortarTxt ^C Pos actual
^X Salir     ^J Justificar ^W Buscar   ^U Pág Sig  ^U PegarTxt  ^T Ortografía
```

Figura 4.4 configuración de zabbix_server.conf

Fuente: Elaboración propia.

4.2.2.6 Configuración de *scripts* de inicio

Es necesario ejecutar los siguientes comandos en el Shell, para permitir un arranque automático de los servicios del servidor y agente cuando el equipo arranca.

- chkconfig ZABBIX-server on
- chkconfig ZABBIX-agent on

4.2.2.7 Instalación de interfaz web

ZABBIX trabaja por medio de una interfaz web para más comodidad al momento de hacer configuraciones desde cualquier sistema operativo en la red

con acceso al servidor y con un explorador de internet. Se configuro el PHP que se encuentra en /etc/httpd/conf.d/conf.d/zabbix.conf.

```
GNU nano 2.0.9          Fichero: zabbix.conf
#
# Zabbix monitoring system php web frontend
#
Alias /zabbix /usr/share/zabbix

<Directory "/usr/share/zabbix">
  Options FollowSymLinks
  AllowOverride None
  Order allow,deny
  Allow from all

  <IfModule mod_php5.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value date.timezone America/Mexico_City
  </IfModule>

```

[57 líneas leídas]

^G Ver ayuda	^O Guardar	^R Leer Fich	^Y Pág Ant	^K CortarTxt	^C Pos actual
^X Salir	^J Justificar	^W Buscar	^U Pág Sig	^U PegarTxt	^T Ortografía

Figura 4.5 configuraciones de PHP
Fuente: Elaboración propia.

4.2.2.8 Comprobación y últimos pasos de instalación

Una vez realizados todos los pasos anteriores se introdujo la dirección ip del servidor ZABBIX en el explorador web, la dirección por defecto de ZABBIX es “dirección_ip/ZABBIX”, esto fue modificado dentro del servidor apache para poder acceder de forma directa al colocar únicamente la dirección IP del servidor en este caso la IP es fija. Se verifico que la configuración se hubiese realizado correctamente.

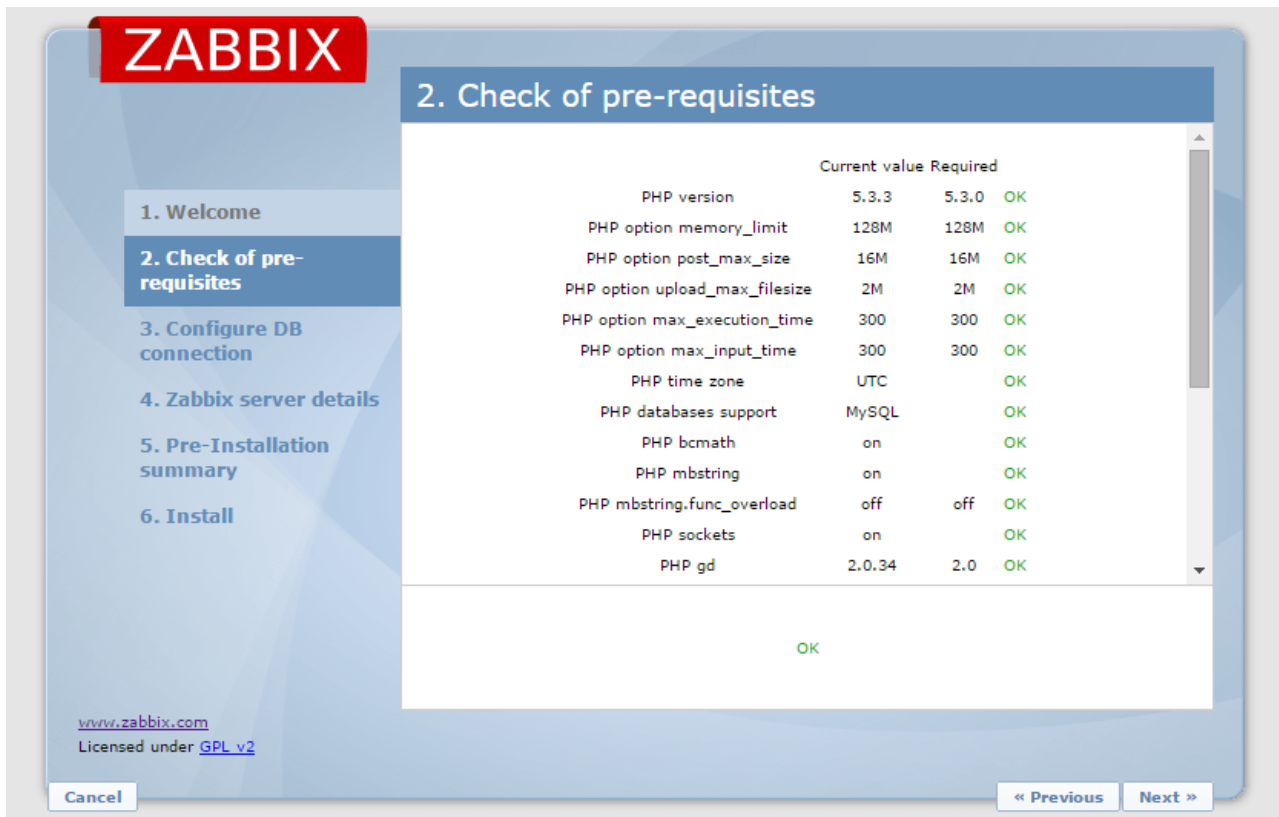


Figura 4.6 comprobaciones de PHP

Fuente: Elaboración propia.

Luego se verifico la existencia de la conexión con la base de datos, esto se muestra en la siguiente imagen:

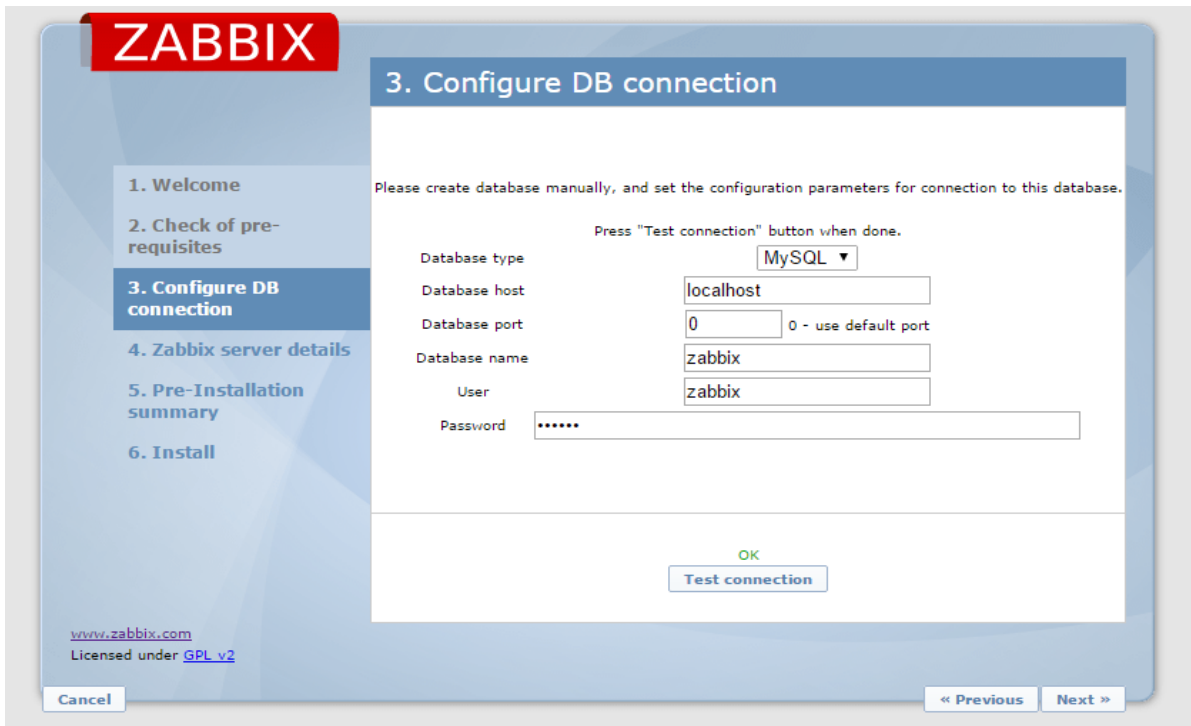
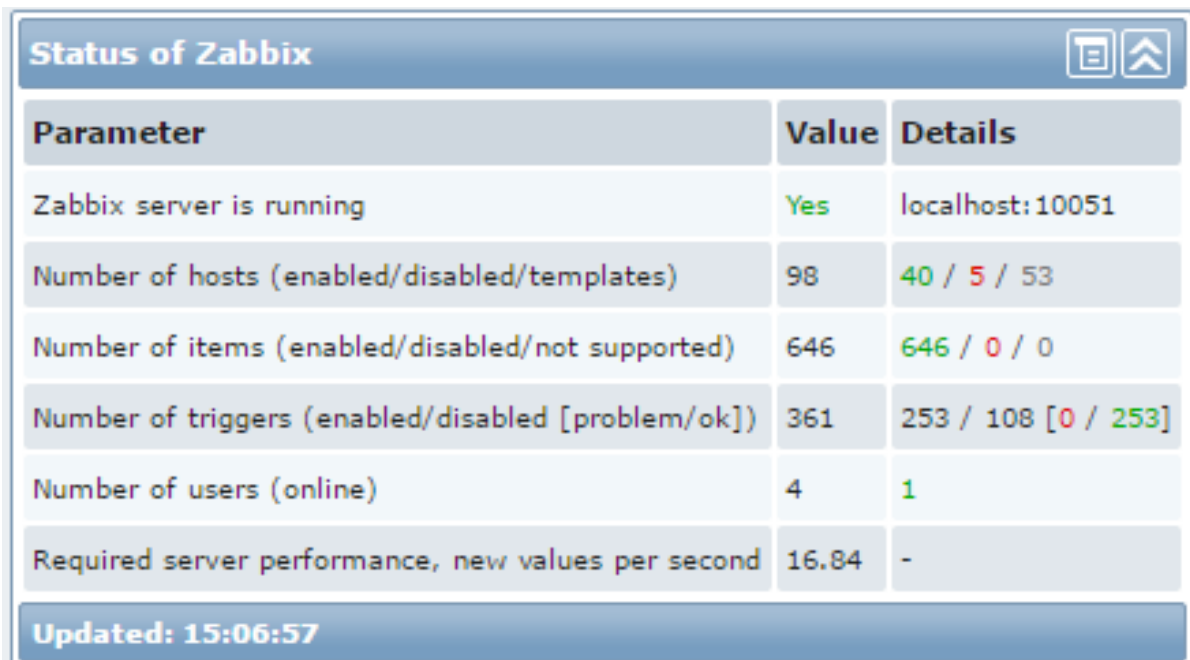


Figura 4.7 Verificación de conexión con MySQL
Fuente: Elaboración propia.

4.2.3 Pruebas

4.2.3.1 Agente ZABBIX

Para confirmar que el agente ZABBIX funcionara correctamente, se verifico su estado dentro del servidor y se confirmo la obtención de valores. Al entrar en la página principal del servidor, específicamente en la pestaña dashboard, se puede apreciar el estado del sistema:



Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	98	40 / 5 / 53
Number of items (enabled/disabled/not supported)	646	646 / 0 / 0
Number of triggers (enabled/disabled [problem/ok])	361	253 / 108 [0 / 253]
Number of users (online)	4	1
Required server performance, new values per second	16.84	-

Updated: 15:06:57

Figura 4.8 estado del ZABBIX

Fuente: Elaboración propia.

Una vez confirmado el correcto funcionamiento del servidor, se procedió a la verificación de los datos obtenidos cada 1 minuto, a continuación se pueden observar algunos de los ítems monitorizados por ZABBIX.

The screenshot shows the ZABBIX web interface. At the top, there is a navigation menu with options like Monitoring, Inventory, Reports, Configuration, and Administration. Below that, there is a breadcrumb trail: History: Dashboard » Network maps » Dashboard » Configuration of hosts » Dashboard. The main section is titled 'LATEST DATA' and 'Items'. A table displays the following data:

Host	Name	Last check	Last value	Change
SysFza_4toTribunal	Alarmas (1 Item)			
SysFza_CJFAcorzo	Alarmas (1 Item)			
SysFza_CJFCereso	Alarmas (1 Item)			
SysFza_CJFOTE32	Alarmas (1 Item)			
SysFza_4toTribunal	Analogicas (5 Items)			
SysFza_CJFAcorzo	Analogicas (5 Items)			
	Corriente_Bateria	2015-11-20 11:21:30	0 Ampers	-0.2 Ampers
	Corriente_Rectificador	2015-11-20 11:21:31	6.9 Ampers	-0.1 Ampers
	Corriente_Salida	2015-11-20 11:21:32	6.9 Ampers	+0.1 Ampers
	Voltaje_AC_F1-2	2015-11-20 11:21:34	216 Volts	-1 Volts
	Voltaje_CD_Salida	2015-11-20 11:21:36	54.14 Volts	-0.05 Volts
SysFza_CJFCereso	Analogicas (5 Items)			
	Corriente_Bateria	2015-11-20 11:21:36	0 Ampers	-

Figura 4.9 valores de los ítems monitorizados en ZABBIX servidor.

Fuente: Elaboración propia.



4.3.4 Configuración de parámetros

Una vez instalado el servidor y realizadas las modificaciones pertinentes se determinaron los diferentes parámetros y equipos a monitorear, como por ejemplo:

Router:

- Cisco serie 3000: tráfico, ping constante, monitorizar CPU.

Cargadores:

- Matrix 5000: Alta temperatura, Falla VCA, tiempo restante de batería.
- Sistema de fuerza EMI: Corriente de batería, corriente rectificador, corriente de salida, bajo voltaje AC.
- Sistema de fuerza EMEISA: Falla de rectificadores, bajo voltaje CA, alto voltaje CA, ping constante, voltajes de salida bajo y alto CD.



Radios

- Pidu Motorola: Estado de enlace, estado del puerto, ping constante.

Sistemas OPLAT

- SWT3000: ping constante, trafico.

Al mismo tiempo se pidió que las alarmas llevaran un lineamiento para la homologación de la denominación de alarmas de comunicaciones en el sistema de control supervisorio. Para el cual sería más fácil para identificar la alarma.

 	<p align="center">COMISIÓN FEDERAL DE ELECTRICIDAD SUBDIRECCIÓN DE TRANSMISIÓN</p> <p align="center">"LINEAMIENTOS PARA LA HOMOLOGACION DE LA DENOMINACION DE ALARMAS DE COMUNICACIONES EN EL SISTEMA DE CONTROL SUPERVISORIO."</p>	<p align="right">Página 6 de 14</p> <p align="right">CLAVE: I-COM-01</p> <p align="right">REVISIÓN: 0</p> <p align="right">FECHA DE ELABORACIÓN 27-ENERO-2015</p>
---	--	---

Dónde:

ALC	Indicativo de presencia de Alarma de Comunicaciones (ALC) en el equipo. 3 Caracteres fijos.
DESCRIPCION	Es la descripción breve del tipo de alarma presentada. Deberá contar con un máximo de 12 caracteres.
EQUIPO	Es el modelo de equipo que ha presentado la alarma. Máximo 8 caracteres. Ejemplo: ESB200i, ESB500.
LINEA	Es la Línea de transmisión de acuerdo a la nomenclatura de ACOR donde opera el equipo. Deberá contar con 11 caracteres. Ejemplo: ANGA3T30THP.
FX	Se refiere a la Fase de la L.T. donde opera el equipo. Únicamente 3 caracteres. Ejemplo: FA (Fase A) o FF (Fase a Fase)

A continuación se presentan los siguientes ejemplos: (Anexo 1 y 2)

ALC - GENERAL EQPO - ESB200i - ANGA3T30THP - FF
 ALC - AMP RF 100W - PLK3000 - MPDA3050MID - FF
 ALC - AMP RF 50 W - ESB500 - MMT73940MPU - FB

Alarmas mínimas que se deben de enviar al Sistema de Control Supervisorio:

- 1 GENERAL EQUIPO
- 2 FALLA TX
- 3 FALLA RX
- 4 SEÑAL / RUIDO

6.2 Sistema de Teleprotecciones.



Deberá contar con la siguiente estructura:

ALC - INDICADOR - DESCRIPCION - EQUIPO - LINEA - MEDIO



4.3.5 configuración de monitorización del tráfico

Para monitorear el tráfico de entrada y salida en los elementos de la red, se crearon grupos, ya que cada elemento que se desee monitorear debe ser registrado como un host dentro de un grupo en el software ZABBIX, los grupos se crearon en correspondencia con la ubicación geográfica de los equipos. Posterior a la creación de los grupos *hosts*. Seguidamente se crearon los ítems en cada uno de los casos, se considera un ítem cada parámetro a monitorizar en un equipo.

En caso de la lectura del tráfico de entrada y salida en los enlaces de la red se utilizo como la información proporcionada por Cisco systems, inc en su pagina web.

En la ventana de creación de ítem se rellenaron los siguientes campos:

- *Description* : descripción del ítem.
- *Type*: versión SNMP.
- *SNMP OID*: OID correspondiente
- *SNMP community*: comunidad a la que pertenece el dispositivo, se debe tomar en cuenta que el servidor debe pertenecer a la misma comunidad para poder obtener información del equipo.
- *Type of información*: tipo de dato, en este caso *Numeric(float)*.
- *Units*: unidad de medida de dato, en este caso b/s (bits por segundo).
- *Usen custom multiplier*: multiplicador, en caso de desearlo. En este caso se coloco el número 8, debido a que se deseaba obtener las medidas en Bytes por segundo.
- *Stre value*: Delta(speed per second), ya que el dato que se obtiene es una velocidad.

Item

Parent items [Template SWT3000](#)

Name

Type

Key

Host interface

SNMP OID

SNMP community

Port

Type of information

Data type

Units

Use custom multiplier

Update interval (in sec)

Flexible intervals

Interval	Period	Action
No flexible intervals defined.		

New flexible interval

Interval (in sec)	<input type="text" value="50"/>	Period	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Add"/>
-------------------	---------------------------------	--------	--	------------------------------------

History storage period (in days)

Trend storage period (in days)

Store value

Show value [show value mappings](#)

New application

Applications

- None-
- Alarmas
- ICMP

4.12 configuración de ítem de tráfico

Fuente: Elaboración propia.

4.3.6 Monitorización de la CPU

Para la monitorización del uso de CPU de los enrutadores se realizó el mismo procedimiento de creación de ítem, muy similar al descrito anterior, en este caso resulta un poco más sencillo, ya que se modifican menos parámetros que en el caso del tráfico, los campos modificados fueron los siguientes:

- *Description*: descripción del ítem.
- *Type*: se escogió como versión SNMP la versión 2.
- *NMP OID*: se colocó la cadena OID correspondiente
- *Units*: se colocó el símbolo % dado el valor obtenido es un porcentaje.

Item

Parent items: [Template App Zabbix Server](#)

Name: Zabbix \$4 \$2 processes, in %

Type: Zabbix internal

Key: zabbix[process,trapper,avg,busy]

Type of information: Numeric (float)

Units: %

Use custom multiplier: 1

Update interval (in sec): 60

Flexible intervals

Interval	Period	Action
No flexible intervals defined.		

New flexible interval: Interval (in sec) 50 Period 1-7,00:00-24:00 Add

History storage period (in days): 7

Trend storage period (in days): 365

Store value: As is

Show value: As is [show value mappings](#)

New application:

Figura 4.13 Configuración de ítem CPU.
Fuente: Elaboración propia

El mismo proceso se llevo a cabo con cada uno de los enrutadores monitorizados en la red.

4.3.6.1 configuraciones de ítems

Para comprobar la conexión entre servidor-host, en primer lugar se debe agregar el host para ser monitorizado por ZABBIX, esto se configuro haciendo clic en la pestaña configuración, luego se hizo clic en host de algunos de los grupos que ya se habían configurado y en la siguiente ventana se selecciono create host para su configuración.

Dentro de la ventana de configuración de host se debe configurar el puerto de escucha, en este caso el 161, que es el punto que usa el protocolo SNMP, y en la dirección de IP se colocó la IP del host a monitoria.

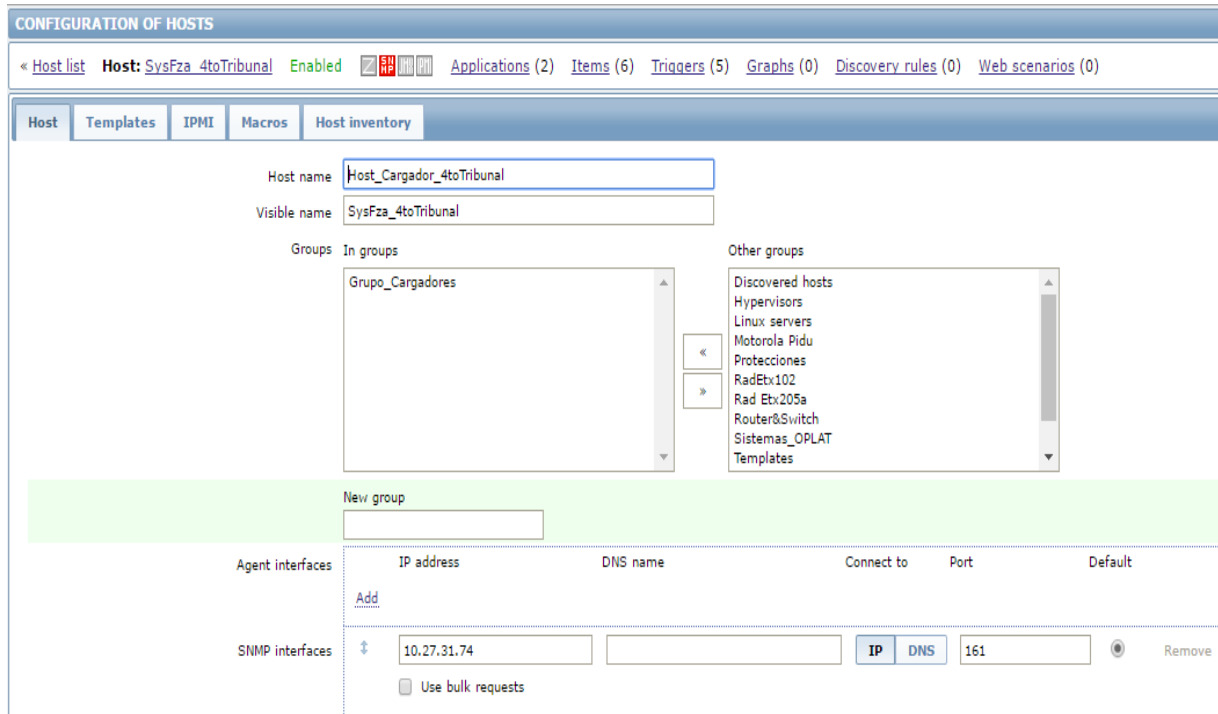


Figura 4.10 configuración de host

Fuente: Elaboración propia.

Al finalizar la creación del host, se realizó la configuración de un ítem para comprobar la conexión entre el servidor y un host. Esto se configuró en la ventana "ítem", dentro del menú host, que a su vez se encuentra dentro de la ventana configuración. En la siguiente imagen se muestra la configuración de un ítem.

Item

Name:

Type:

Key:

SNMP OID:

SNMP community:

Port:

Type of information:

Data type:

Units:

Use custom multiplier:

Update interval (in sec):

Flexible intervals

Interval	Period	Action
No flexible intervals defined.		

New flexible interval

Interval (in sec)	<input type="text" value="50"/>	Period	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Add"/>
-------------------	---------------------------------	--------	--	------------------------------------

History storage period (in days):

Trend storage period (in days):

Store value:

Show value: [show value mappings](#)

New application:

Applications:

Populates host inventory field:

Figura 4.11 configuración de ítem
Fuente: Elaboración propia.

Una vez configurados los ítems, los resultados obtenidos se pudieron observar en la ventana *latest data* ubicada en *monitoring*,

Host	Description	Last check ↓	Last value	Change	History
HOST DE PRUEBA	- other - (1 Items)				
	PRUEBA	31 May 2012 13:07:19	1	-	Graph

Figura 4.12 Prueba del ítem a host de red.
Fuente: Elaboración propia

Este proceso se realizó una vez por cada interfaz incluida en el diagrama facilitado por el administrador de la red. Una vez configurados todo el ítem se realizó a la validación de datos, y acto seguido a la configuración de alarmas.

4.3.7 Configuración de alarmas

Se determinaron los ítems que contarían con una alarma, así como el tipo de alarma, que se utilizaría (correo electrónico), también se había optado por teewter pero no tuvo el resultado esperado. Estas alertas vía correos solo ocurrirían en caso de falla, y serían enviadas a las personas encargadas de solucionar el problema.

Una vez determinados los casos de alerta se procedió a la configuración de las alarmas. Para realizar la configuración se debe ingresar a la ventana *triggers* dentro de la configuración de *host*, una vez allí, se procede a modificar los parámetros necesarios como se muestra a continuación:

The screenshot shows a configuration window for a trigger. At the top, there are two tabs: "Trigger" (selected) and "Dependencies". Below the tabs, the "Parent triggers" field is set to "TemplateCisco_3750". The "Name" field contains "Estado_Port01". The "Expression" field contains the code "{Cisco3750_GRTSE:ifOperStatus.Port01.min(120)}<>1" and has an "Add" button to its right. Below the expression field is a link for "Expression constructor". The "Multiple PROBLEM events generation" checkbox is unchecked. The "Description" field is empty. The "URL" field is empty. At the bottom, the "Severity" is set to "High" from a list of options: "Not classified", "Information", "Warning", "Average", "High", and "Disaster".

Figura 4.13 Configuración de alarma.

Fuente: Elaboración propia.

El campo *expression* se completa de manera automática al rellenar los campos de la ventana que se genera al presionar el botón *add*. Esto se puede observar en la imagen:

The screenshot shows a dialog box titled "Trigger expression condition". It contains the following fields and controls:

- Item:** A text box containing "TemplateCisco_3750: ifOperStatus.Port01" and a "Select" button.
- Function:** A text box containing "Last (most recent) T value is = N".
- Last of (T):** A text box with a dropdown menu set to "Time".
- Time shift:** A text box with the label "Time" next to it.
- N:** A text box containing the value "0".
- Buttons:** "Insert" and "Cancel" buttons at the bottom.

Figura 4.14 Generación de expresión de alarma ICMP.
Fuentes: Elaboración propia.

4.3.7.1 configuraciones de envío de alarmas

Para realizar el envío de alarmas, se debe realizar la configuración correspondiente al protocolo SMTP, ya que es mediante este que ZABBIX realiza el envío de correos electrónicos. Para esto se configuro desde la terminal por medio de comandos y se accedió a la opción *media types*, donde aparece una ventana de configuración como la que se observa en la imagen. En los campos censurados se ingreso la información correspondiente con el servidor SMTP y la dirección de correo desde la cual serian enviadas las alertas.

The screenshot shows a dialog box titled "Media type" with the following configuration:

- Name:** Email
- Type:** Email (dropdown menu)
- SMTP server:** [Redacted]
- SMTP helo:** [Redacted]
- SMTP email:** [Redacted]
- Enabled:**

Figura 4.15 Configuración de e-mail.
Fuente: Elaboración propia.

Una vez configurado el servidor SMTP, para envío de correos electrónicos, se otorgaron los permisos correspondientes y se agregaron las direcciones de correo de los destinatarios; esto se realizó ingresando en la ventana *users* ubicada en *administration*; en el menú principal.

Para que el envío del correo electrónico ocurriera automáticamente al ocurrir un error se configuró acciones. Para hacer esta configuración se ingresó en el menú *actions* dentro de *configuration*; allí se procedió a configurar el tipo de acción a tomar, en este caso: enviar un correo electrónico, por ende se seleccionó *e-mail* y se configuró finalmente el tipo de alarma a ser enviada, así como las características de la falla.

CONFIGURATION OF ACTIONS

Action | Conditions | Operations

Name: Reportar Problemas a Comunicaciones

Default subject: {TRIGGER.STATUS}: {TRIGGER.NAME};{HOST.NAME1}

Default message: Evento: {TRIGGER.NAME}
Estatus: {TRIGGER.STATUS}
Gravedad: {TRIGGER.SEVERITY}
Hora de Falla: {EVENT.TIME}

Valores:

Recovery message:

Recovery subject: {TRIGGER.STATUS}: {TRIGGER.NAME};{HOST.NAME1}

Recovery message: Evento: {TRIGGER.NAME}
Estado: {TRIGGER.STATUS}
Gravedad: {TRIGGER.SEVERITY}
Hora de Recuperacion: {EVENT.RECOVERY.TIME}
Estado Actual: {EVENT.RECOVERY.STATUS}

Valores:

Enabled:

Figura 4.16 Configuración de una acción.

Fuente: Elaboración propia.

4.3.8 creación de gráficos

El paso final en el proceso de implementación consistió en la creación de gráficos de comparación entre el tráfico de entrada y salida de cada una de las interfaces monitoreadas.

Para la creación de dicho grafico se siguió la ruta *configuración-host-graphs*; al estar dentro del área de configuración de gráficos se hizo clic en el botón *create graph*, y en la ventana que aparece a continuación se añadieron los ítem que formarían parte del grafico, en este caso estos fueron tráficos de entrada y tráficos de salida. También se selecciono el tipo de línea a utilizar en los gráficos así como los colores para cada uno de los ítems.

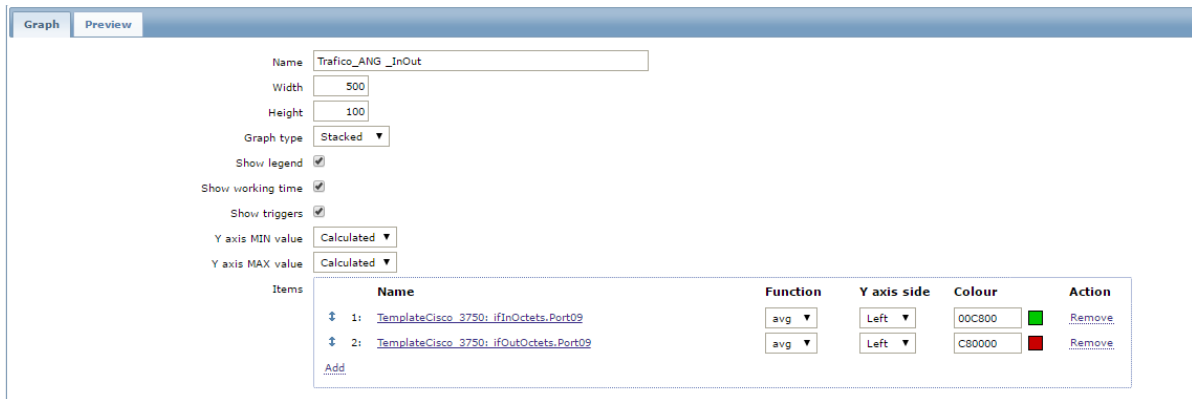


Figura 4.17 Creación de grafica de tráfico.

Fuente: Elaboración propia.

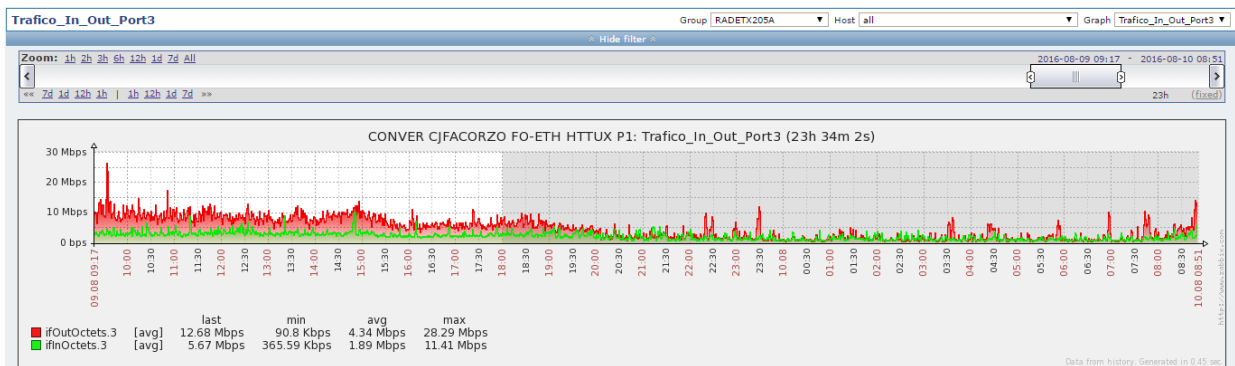


Figura 4.18 Grafica de trafico de un equipo

Fuente: Elaboración propia

4.4 pruebas de funcionamiento

Las pruebas de funcionamiento del sistema de gestión consistieron en validar los datos recolectados por ZABBIX, para luego ser comparados con los valores mostrados por el sistema operativo de los enrutadores.

4.4.1 envió de alarmas

Una vez conformes con la validación de los datos obtenidos, se procedió a la configuración de envío de alarmas, para comprobar esto se interrumpieron conexiones de manera controlada, a fin de comprobar que las alarmas respondieran adecuadamente, incluidos los casos en los que se debía enviar un correo electrónico.

Host	Issue	Last change	Age	Info	Ack	Action
SWT3000_MMT_A3130_SAB	SWT3000 MMT A3130 SAB is unavailable by ICMP	2016-07-26 13:56:45	18h 17m 41s		No	
Cisco3750_GRTSE	C		7m 47s		No	
RAD_HTTUX_4toTribunal	R	2016-07-26 13:56:45	18h 17m 41s		No	
RAD_HTTUX_CJFAcorzo	R	2016-04-30 15:08:45	2m 26d 22h		No	
SWT3000_SAB_A3T60_MMT	S	2016-04-30 13:43:45	1h 25m		No	
ServidorPMU_400	ServidorPMU_400 No responde Ping	2016-07-26 13:56:39	18h 17m 47s		No	
SWT3000_SAB_A3130_MMT	SWT3000_SAB_A3130_MMT No responde Ping	2016-07-26 13:56:39	18h 17m 47s		No	
Pidu_GrtseMactumat	Pidu_GrtseMactumat No responde Ping	2016-07-26 13:56:33	18h 17m 53s		No	
Matrix5000_GRTSE	Matrix5000_GRTSE No responde Ping	2016-07-26 13:56:33	18h 17m 53s		No	

Time	Status	Duration	Age	Ack
2016-07-26 13:56:45	PROBLEM	18h 17m 41s	18h 17m 41s	No
2016-04-30 15:08:45	OK	2m 26d 22h	2m 27d 17h	No
2016-04-30 13:43:45	PROBLEM	1h 25m	2m 27d 18h	No

Figura 4.18 Activación de una alarma.

Fuente: Elaboración propia

Al realizar la desconexión del enlace se observó que las alarmas correctas aparecen en el registro de eventos del sistema. Acto seguido, se confirmó que la recepción de correos electrónicos ocurriese acorde a la configuración.

Capítulo V

5.1 Resultados

Con el fin de mostrar la relación entre las labores llevadas a cabo a lo largo de la realización de este trabajo especial de grado y los objetivos planteados al principio del mismo, se hizo una recolección de resultados basados en cada una de las fases descritas en el marco metodológico.

Ya que gran parte de la realización del trabajo consistió en la implementación del sistema de monitorización presentado en el capítulo cuatro, a continuación se presentaran los resultados, deseados o no, y los procesos utilizados para las resolución de problemas.

5.2 instalación inicial

Utilizando el apoyo de los manuales de usuario, disponibles de manera gratuita en la página web del software de gestión ZABBIX, se logro la exitosa instalación, además se logro manejar un nivel de dominio del software suficientemente profundo para brindar un servicio de monitorización confiable. Parte importante del uso del soporte brindado por los creadores del software, fue la utilización de sus tablas de recomendaciones como guías al momento de determinar la mejor combinación de características de hardware que permitiese obtener los mejores resultados a partir de ZABBIX, tomando en cuenta factores como el numero de *hosts* en la red, y las capacidades de procesamiento de los equipos, entre otros.

Utilizando estos mismos manuales, junto con un poco de práctica, se aprendió la sintaxis y la lógica a ser utilizada para la correcta configuración de las características que se deseaba monitorizar de manera que se obtuviesen resultados fiables, ya que esto no depende únicamente de que la instalación sea adecuada, sino de una combinación optima entre recursos, instalación y configuración que se adapte a la necesidades de la red.

5.3 configuración de parámetros básicos

Una vez se logro la instalación de manera satisfactoria, se procedió a la configuración de una serie de parámetros básicos locales que se utilizarían para la realización de pruebas de funcionamiento iniciales. Para esto se configuro un agente local, que tuvo como objetivo emular un equipo conectado a la red del servidor. En este agente se configuro el envío de paquetes ICMP correspondiente.

5.4 pruebas locales de funcionamiento

Al contar con el software en estado funcional y sin problemas aparentes se decidió seguir adelante con las pruebas de configuración. Como se menciono anteriormente, se llevo a cabo un proceso de configuración de parámetros básicos a fin de comprender la forma correcta de ingresar los parámetros que componen cada ítem en el software y así obtener los resultados deseados.

El siguiente paso fue realizar pruebas básicas de funcionamiento con los parámetros configurados.

5.4.1 pruebas con paquetes ICMP

Al estar configurado los ítem necesarios para realizar pruebas, a fin de detectar el estado, activo o inactivo, de los *hosts* de la red pruebas, se accedió a la sección *latest data*, en la cual se encuentra toda la información reciente con la que cuenta el sistema, y allí se observaron los resultados correspondientes con las respuestas a los mensajes ICMP enviados por el sistema.

Host	Description	Last check	Last value
HOST DE PRUEBA	- other - (1 Items)		
	PRUEBA	03 Jun 2012 16:23:19	Up (1)

Figura 45. Host de prueba en estado activo.

Fuente: Elaboración propia

Como se puede observar en la figura anterior, los resultados obtenidos en este caso fueron correspondiente con los deseados, ya que el host se encontraba activo; posteriormente, a fin de obtener comprobación total del funcionamiento, se desactivo el host, lo cual arrojó un resultado de *host* inactivo, tal como era deseado.

HOST DE PRUEBA	- other - (1 Items)				
	PRUEBA	03 Jun 2012 19:03:37	Down (0)	-	Graph

Figura 46. Host de prueba en estado inactivo.

Fuente: Elaboración propia.

5.5 Instalación en el servidor

En lo referente a la instalación en el servidor que se encontraba en el Site de comunicaciones fue un proceso simple, ya que consistió en realizar lo mismo que se hizo en la maquina virtual que se había instalado previamente para realizar los ensayos, se hizo pequeñas modificaciones en cuanto a las contraseñas y nombres de usuario.

Posterior a esto se realizaron las configuraciones correspondientes con todos los parámetros que se debían monitorizar.

5.5.1 Pruebas de funcionamiento de alertas

Una vez finalizada la configuración completa del sistema, en la cual se incluye la configuración de todos los ítems, así como el envío de correos electrónicos, se realizaron pruebas para verificar que estos fueran recibidos según lo planificado. Tal como se describió en el capítulo anterior, la metodología utilizada para la comprobación del funcionamiento de las alertas de correo electrónico consistió en la desconexión de algunos de los enlaces de la red del cliente; al realizar la desconexión, se pudo comprobar que se activaran las alarmas correspondientes con el enlace desconectado, entre las cuales debía estar la falla del envío y recepción de respuestas correspondientes con los paquetes *fping* (ICMP), y enviarle la falla a los usuarios correspondientes a su correo.

Last 20 issues						
Host	Issue	Last change	Age	Info	Ack	Actions
Zabbix server	Zabbix unreachable poller processes more than 75% busy	2016-08-12 09:38:50	3h 46m 54s		No	1
CONVER SETGU FO-ETH SAEQRTSE P1	No responde Ping ICMP	2016-08-12 09:33:32	3h 52m 12s		No	10
RADIO MIO SETGU PTP500 PEDRE 01	No responde Ping ICMP			User	Details	Status
RADIO MIO PEDRERA PTP500 SETGU 01	No responde Ping ICMP			Admin (Zabbix Administrator)	Email	Sent
RADIO MIO SCTSMAYO PTP500 PEDRE 01	No responde Ping ICMP			comunicaciones (comunicaciones)	Email	Sent
RADIO MIO PEDRERA PTP500 SCTSM 01	No responde Ping ICMP			comunicaciones (comunicaciones)	Email	Sent
CONVER SAEQRTSE FO-ETH SETGU P1	PUERTO1 F.O.			comunicaciones (comunicaciones)	Email	Sent
CONVER SAEQRTSE FO-ETH SETGU P1	Estado_Lag1			comunicaciones (comunicaciones)	Email	Sent
CONVER HTTUX FO-ETH SAGARPA P1	ALC_ENLACE_FO_PRINCIPAL			comunicaciones (comunicaciones)	Email	Sent
CONVER SAGARPA FO-ETH DIRHTTUX P1	ALC_ENLACE_FO_PRINCIPAL			comunicaciones (comunicaciones)	Email	Sent
CONVER SAEQRTSE FO-ETH SETGU P1	Interface Ethernet1 is down			comunicaciones (comunicaciones)	Email	Sent
Zabbix server	Zabbix icmp pinger processes more than 75% busy			comunicaciones (comunicaciones)	Email	Sent
				comunicaciones (comunicaciones)	Email	Sent

Figura 5.4 Activación de las alarmas.

Fuente: Elaboración propia



alexis.sol01@cfe.gob.mx [Agregar a contactos](#) 11/06/2016 ▶

Para: isabel_93@live.com.mx ✕

Evento: No responde Ping ICMP

Estatus: PROBLEM

Gravedad: Average

Hora de Falla: 21:26:26

Valores:

1. ICMP ping (CONVER AGCINTALA FO-ETH CJFOTE32 P1:icmpping): Down (0)

Figura 5.5 visualización del mensaje.

Fuente: Elaboración propia.

5.6 Conclusión

En general se considera que los objetivos fueron alcanzados, ya que se realizó la implementación de un sistema de monitorización en la red.

El instrumento ZABBIX cumplió con todas las expectativas y demostró ser una herramienta eficaz al momento de detectar fallas en los distintos dispositivos de red. Los logros obtenidos al utilizar esta herramienta de software libre, demuestran que, correctamente implementadas, las soluciones de software libre son tan eficientes como el resto de las soluciones existentes.

El éxito en la implementación del sistema se debe principalmente a que se trabajó bajo los esquemas en el cual se definieron de manera clara las necesidades presentes, y toda la labor se realizó en función de satisfacerlas.

Las herramientas de monitorización son vitales para prevención y anticipación de problemas en una red, hoy en día, a medida que las redes se expanden, los costos de mantenimiento aumentan, por ello es necesario hallar las fallas en el menor tiempo posible.

Anexo I

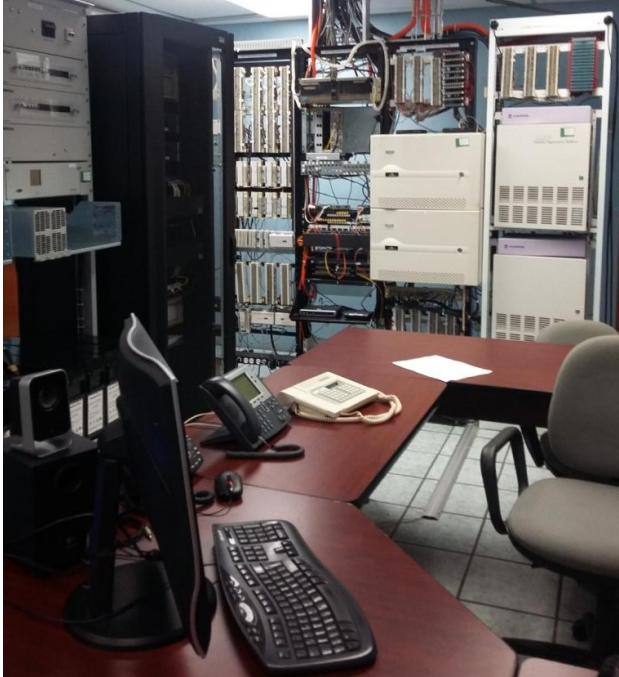


Figura 1. Site de comunicaciones

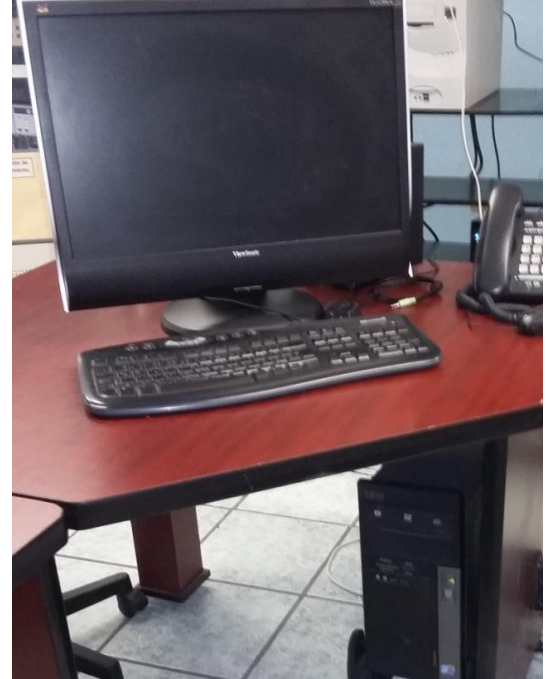


Figura 2. Servidor

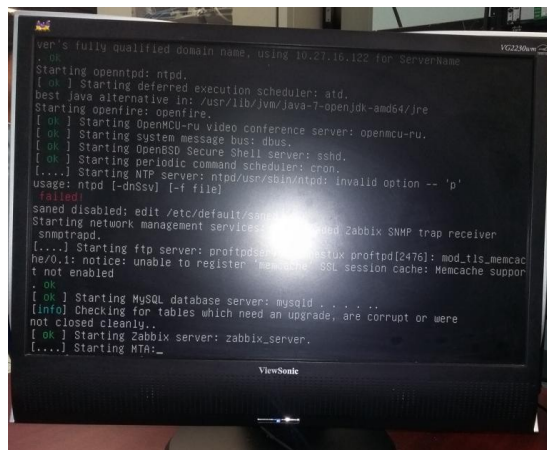


Figura 3. Instalación en el servidor

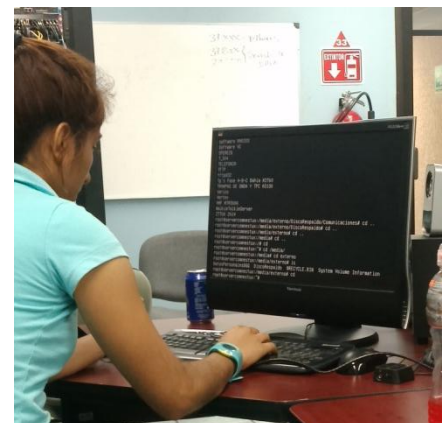


Figura 4. Configuraciones en el servidor



Figura 5. Cargadores



Figura 5. Equipos que opera el ZABBIX

Anexo II

2.4GHZ Bluetooth 2.0 baja Tensión



TRW-24BUC1 es Módulo de audio Bluetooth 2.0V. Especializar a construir-en el receptor de cabeza. La frecuencia es de 2,4 GHz; voltaje de funcionamiento:

- bajo es 1.9V.
- Tamaño: 17,5 * 13.46 * 3,3 mm.

Cualquier dispositivo con Bluetooth como lengua de comunicación PC o teléfono móvil son capaces de conectar con este módulo por radio, y será fácil de hacer que el producto final.

Características

Ventaja Bluetooth

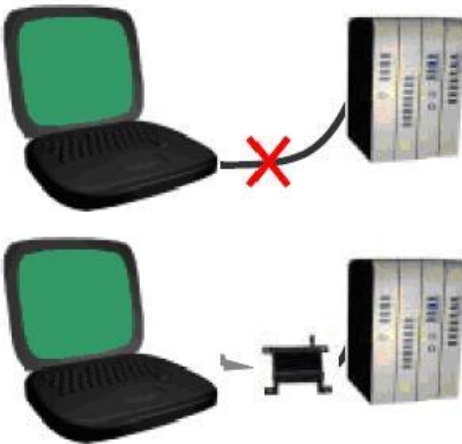
1. Vuelva a colocar el cable de alambre de cadena: Conexión inalámbrica con Bluetooth puede reemplazar el cable de alambre cuerda.

2. unifica el Bluetooth y la tecnología de Internet. Usos La capacidad de administración de la CPU que ofrece Bluetooth, aumenta de múltiples funciones para el equipo, como la etapa de interfaz humana acumulación en Web.

3. Industria punto de acceso. A través de un punto de acceso conecta varios equipos Bluetooth con la red cableada tradicional, por ejemplo, la red IP (por ejemplo: Ethernet) o una red de bus de campo escena industria. (Por ejemplo: Controlnet y Profibus ... etc.)

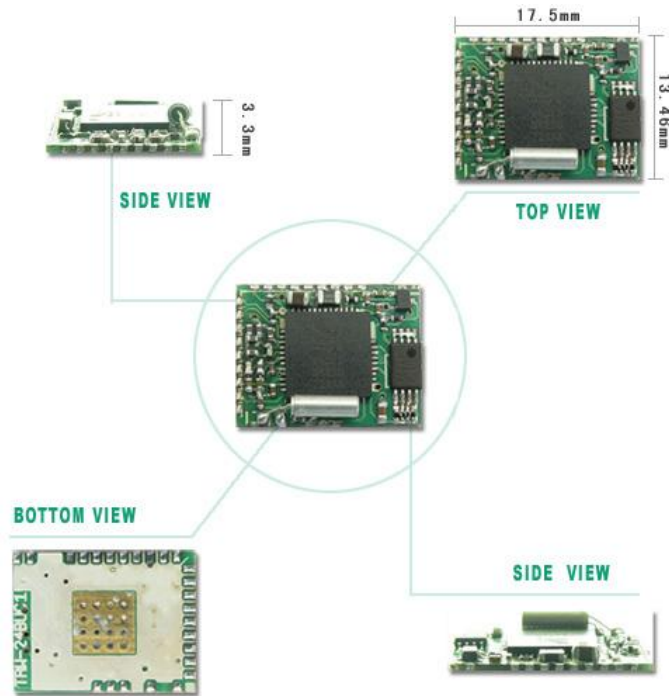
4. Un sensor inalámbrico y el arrancador. Utilizar Bluetooth para venir a relacionar el equipo más cercano a la regulación física del sistema (sensor, motor de arranque y la simple analogía / varios equipos IO) se conecta al sistema de control.

En la actualidad muchos equipos industriales todo el uso de la interfaz tradicional

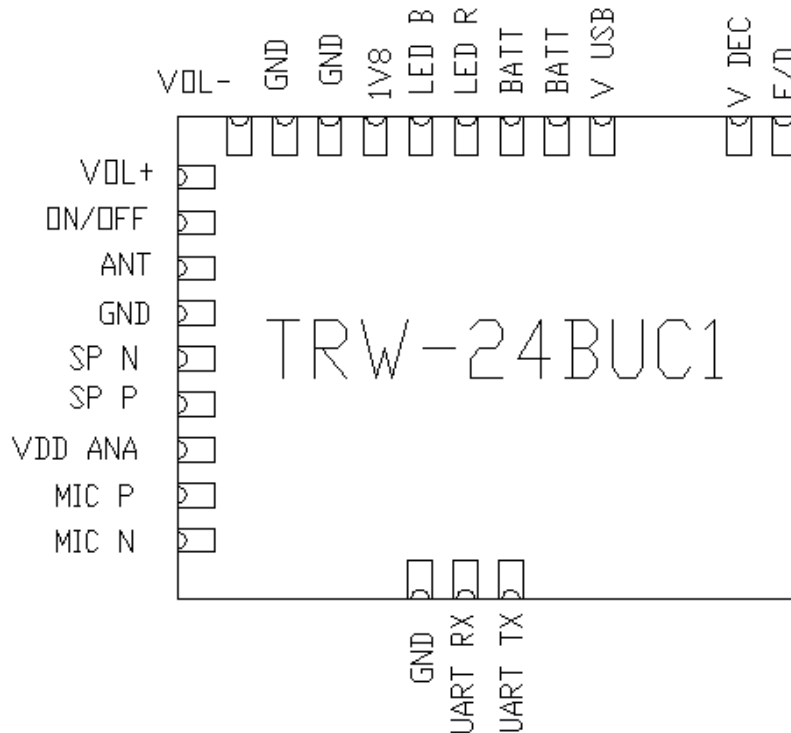


de serie (ex.RS232, RS422 o RS485) para conectar la herramienta de programación o desechar. Esas herramientas especialmente necesitan redistribuir o para programar cuando el equipo con él de conexión, por lo general todo funciona en el equipo estándar, y generalmente utiliza algún método independiente o el equipo de la correspondencia de propósito especial llega a un acuerdo viene y el equipo lleva a cabo la conexión. Todos estos factores hacen que este campo se convierta en una muy buena oportunidad de Bluetooth.

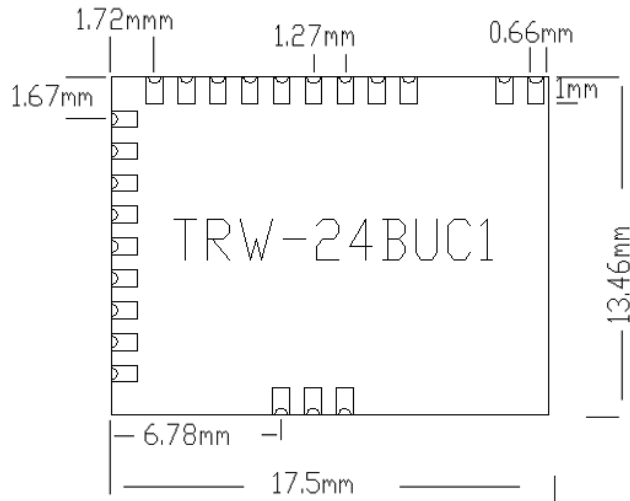
Apariencia del circuito



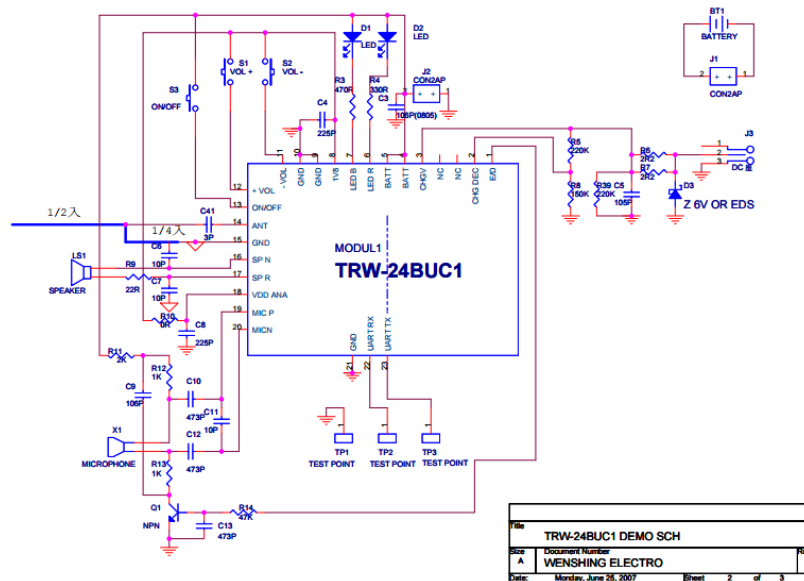
Asignación de PIN



Tamaño vista superior



Circuito



Bluetooth de 2,4 GHz 2.0OR Baja Tensión de trabajo Datos de los módulos

TRW-24BUL es el módulo de datos Bluetooth 2.0V. Se especializan en la construcción-Ratón inalámbrico Bluetooth, y también se puede utilizar con el inductor ligera de ratón Bluetooth y la comunicación con la consola Wii. La frecuencia es de 2,4 GHz; diseño de bajo voltaje de trabajo. Más baja que 1.9V.

WENSHING módulo Bluetooth TRW-24BUL es un módulo Bluetooth con controlador de Broadcom BCM2042 Bluetooth. Este módulo es ideal para la aplicación en el ratón inalámbrico, teclado, joystick y gamepad. Construir-en el firmware se adhiere al perfil Bluetooth HID. Este módulo está integrado con antena PCB, cristal, EEPROM y reguladores de conmutación para reducir el costo BOM externo. Ha sido diseñado para proporcionar potencia ultra baja, bajo costo y comunicaciones robustas y totalmente compatibles con la especificación de radio Bluetooth V 2.0.

Característica

Especificación Bluetooth V2.0 compatible.

- Perfil HID de Bluetooth V1.0 compatible.
- Proporcionar 3.0V y potencia de salida de 1,8 V DC.
- Ajustarse a 2 Potencia de salida Bluetooth clase.
- Diseño de energía extremadamente bajo. (Por ejemplo: ratón óptico inalámbrico: below10mA en funcionamiento).
- Soporta AFH (Adaptive Frequency Hopping).
- Incorporado un regulador de conmutación para reducir la lista de materiales externa y proporcionar alta potencia eficiente para sensor externo.
- En la EEPROM del módulo y cristal y PCB de la antena.
- Excelente sensibilidad del receptor.
- Dimensiones: 25.6mm (L) x 11.7mm (W) x 4 mm (H) con Crystal
- Dimensiones: 25.6mm (L) x 11.7mm (W) x 2,3 mm (H) sin cristal
- Pad: 28
- Soporta interfaz HID general.
- Puede proporcionar el firmware a la medida de aplicación HID.

Aplicaciones

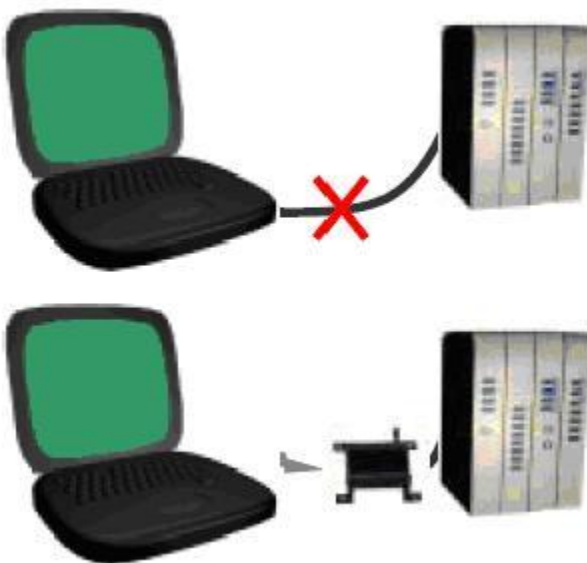
- ratón inalámbrico, bola de seguimiento, el dispositivo de puntero.
- teclado inalámbrico, teclado.
- Mando a distancia RF.
- Sensor remoto de RF para uso médico o de seguridad.

Modelo: TRW-24BUL

Ventaja Bluetooth

1. Vuelva a colocar el cable de alambre de cadena: Conexión inalámbrica con Bluetooth puede reemplazar el cable de alambre cuerda.
2. unifica el Bluetooth y la tecnología de Internet. Usos La capacidad de administración de la CPU que ofrece Bluetooth, aumenta de múltiples funciones para el equipo, como la etapa de interfaz humana acumulación en Web.
3. Industria punto de acceso. A través de un punto de acceso conecta varios equipos Bluetooth con la red cableada tradicional, por ejemplo, la red IP (por ejemplo: Ethernet) o una red de bus de campo escena industria. (Por ejemplo: Controlnet y Profibus ... etc.)
4. Un sensor inalámbrico y el arrancador. Utilizar Bluetooth para venir a relacionar el equipo más cercano a la regulación física del sistema (sensor, motor de arranque y la simple analogía / varios equipos IO) se conecta al sistema de control.

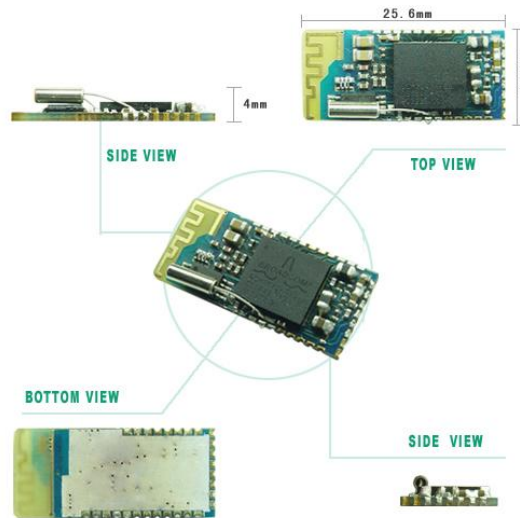
Reemplazar cable serie



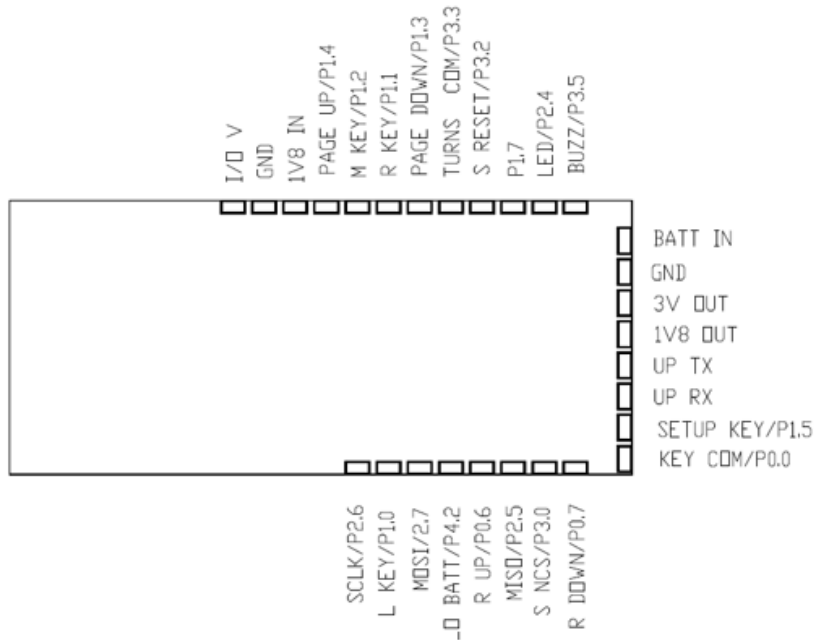
En la actualidad muchos equipos industriales todo el uso de la interfaz tradicional de serie (ex.RS232, RS422 o RS485) para conectar la herramienta herramienta de programación o desechar. Esas herramientas especialmente necesitan redistribuir o para programar cuando el equipo con él de conexión, por lo general todo funciona en el equipo estándar, y generalmente utiliza algún método independiente o el equipo de la correspondencia de propósito especial llega a un acuerdo viene y el equipo lleva a cabo la conexión. Todos estos

factores hacen que este campo se convierta en una muy buena oportunidad de Bluetooth.

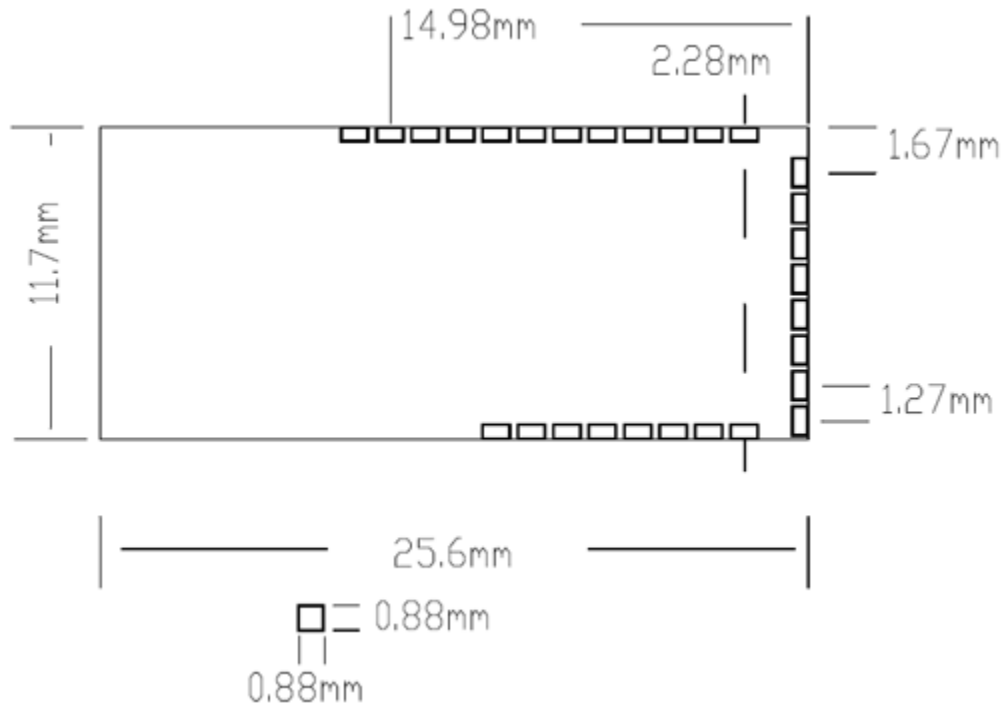
Apariencia



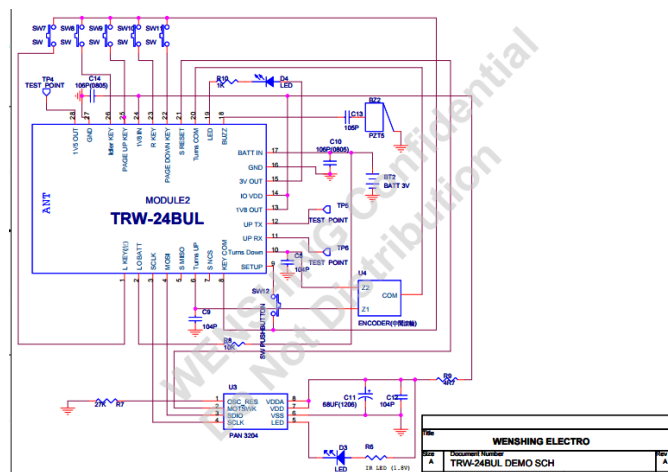
Pines



Tamaño



Circuito



Aplicación



TRW-24BUL es el módulo de datos Bluetooth 2.0V. Se especializan en la construcción-Ratón inalámbrico Bluetooth, y también se puede utilizar con el inductor ligero de ratón Bluetooth y la comunicación con la consola Wii. La frecuencia es de 2,4 GHz; diseño de bajo voltaje de trabajo. Menor que 1.9V.Size: 25,6 * 11,7 * 4 mm.

Amplificadores de bajo nivel de ruido LNA

Es un amplificador electrónico utilizado para amplificar señales débiles por ejemplo, aquellas capturadas por una antena. Por lo general se encuentran muy cerca del dispositivo de detección para reducir las pérdidas en la línea de alimentación. Este arreglo activo de antenas es de uso frecuente en sistemas de microondas como el GPS, ya que el cable coaxial de línea de transmisión es de mucha pérdida en frecuencias de microondas, (una pérdida del 10% procedente de unos pocos metros de cable podría causar una degradación del 10% de la señal-ruido- (SNR)).

El uso de una LNA, el efecto de ruido de las etapas posteriores de la cadena que recibe, se reduce por el aumento de la LNA, mientras su propio ruido se inyecta directamente a la señal recibida. Por tanto, es necesario que la LNA para aumentar la potencia de la señal deseada al tiempo que añade el menor ruido y la distorsión posible, de manera que la recuperación de esta señal sea posible en las etapas posteriores del sistema. Una buena LNA tiene una figura de ruido baja, como de 1 dB, una ganancia lo suficientemente grande, como de 20 dB y debe tener intermodulación lo suficientemente grande así como el punto de compresión. Otros criterios de operación, como el ancho de banda de funcionamiento, la ganancia, la estabilidad y la VSWR de entrada y de salida.

HD30538 modulo de amplificador de bajo nivel de ruido

El HD30538 es un módulo de amplificador de clase A, perfecto como un 59, o como una fase piloto en los sistemas militares, comerciales, industriales, médicos o científicos exhibe excelente potencia y la linealidad de back-off, y utiliza una combinación de tecnologías para el MOSFET rendimiento óptimo.



Specifications				
$V_{sup} = +28VDC, I_{DQ} = 3.30A, P_{out} = 20W, T_{base} = 25^{\circ}C$				
Parameter	Min	Typ	Max	Units
Freq. Range	1		525	MHz
P_{1dB}	20	See Figure 4		W
Input Power		-3	0	dBm
Gain	43	46		dB
Gain Flatness		+/-1.0	+/-1.5	dB
Drain Current		3.30	3.50	A
Efficiency		22	20	%
IRL		-20	-14	dB
f_2		-35	-23	dBc
f_3		-40	-25	dBc
IMD_3 20W PEP, $\Delta f = 10kHz$		-37	-30	dBc
Dimensions	2.40 X 4.60 X 1.31 (60.96 X 116.84 X 33.27)			inch (mm)

Maximum Ratings	
Operation beyond these ratings will void warranty	
Parameter	Value
V_{sup}	24-28VDC
Bias Current	3.30A
Drain Current	3.50A
Load Mismatch*	5:1
Housing Base Temp.	65°C
Storage Temp.	-40°C to 85°C

*All phase angles, 20W forward power, current limited to 3.5A for 3 seconds max.

Option Ordering Info

Disable (TTL, active high)	HD30538-DIS
Heatsink and fan	HD30538-HSF
Enclosure with DC supply and fan	HD30538

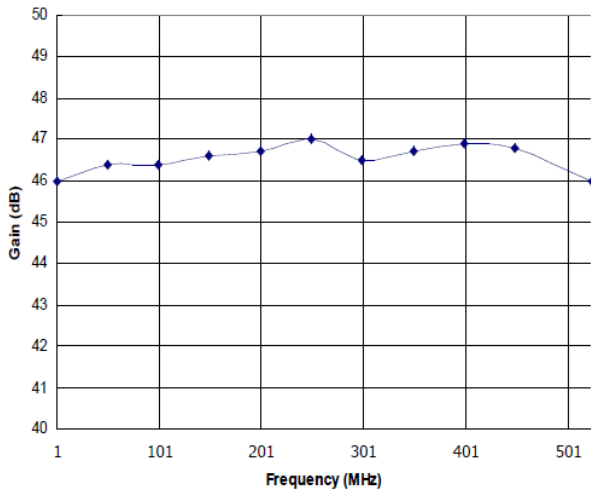


Figure 1: HD30538 Typical Gain vs. Frequency @ $P_{out} = 20W$

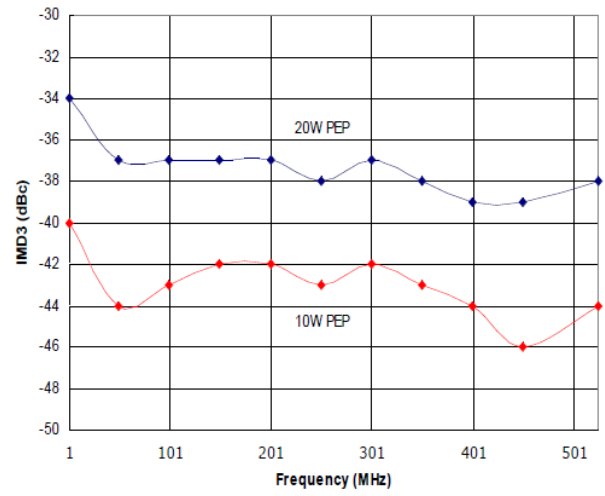


Figure 2: HD30538 Typical IMD_{3r} $\Delta f=10kHz$, @ $P_{out} = 10W$ and $20W$ PEP

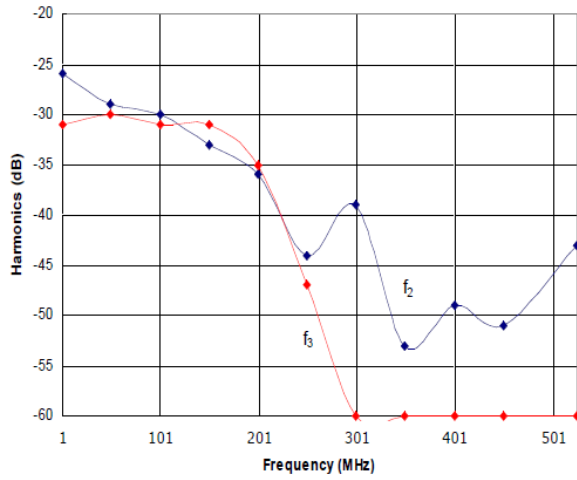


Figure 3: HD30538 Typical f_2 and f_3 vs. Frequency @ $P_{out} = 20W$

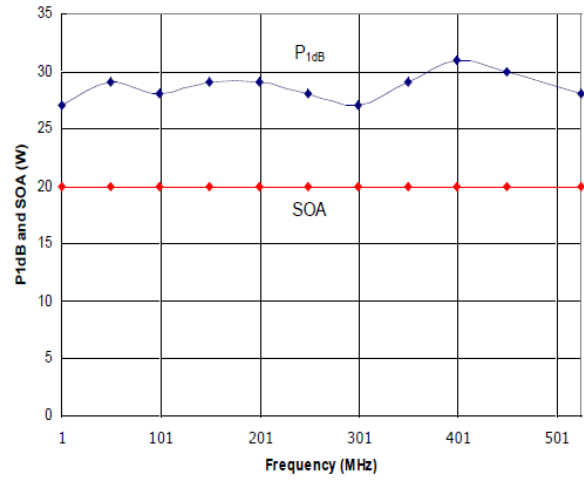
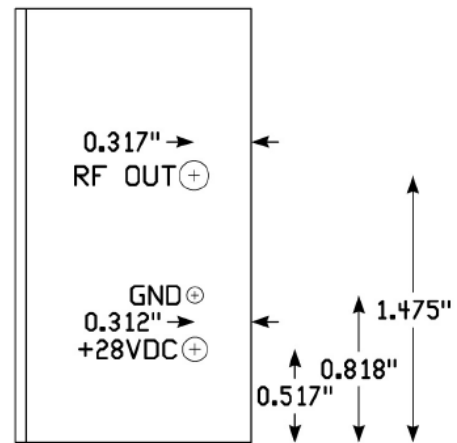
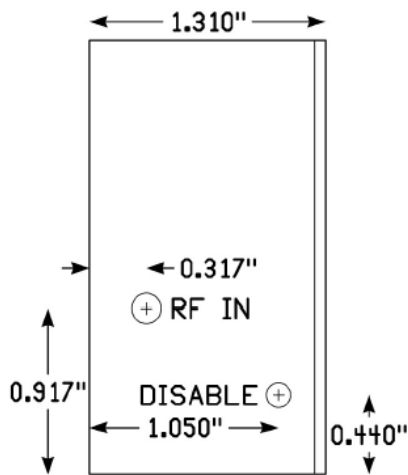
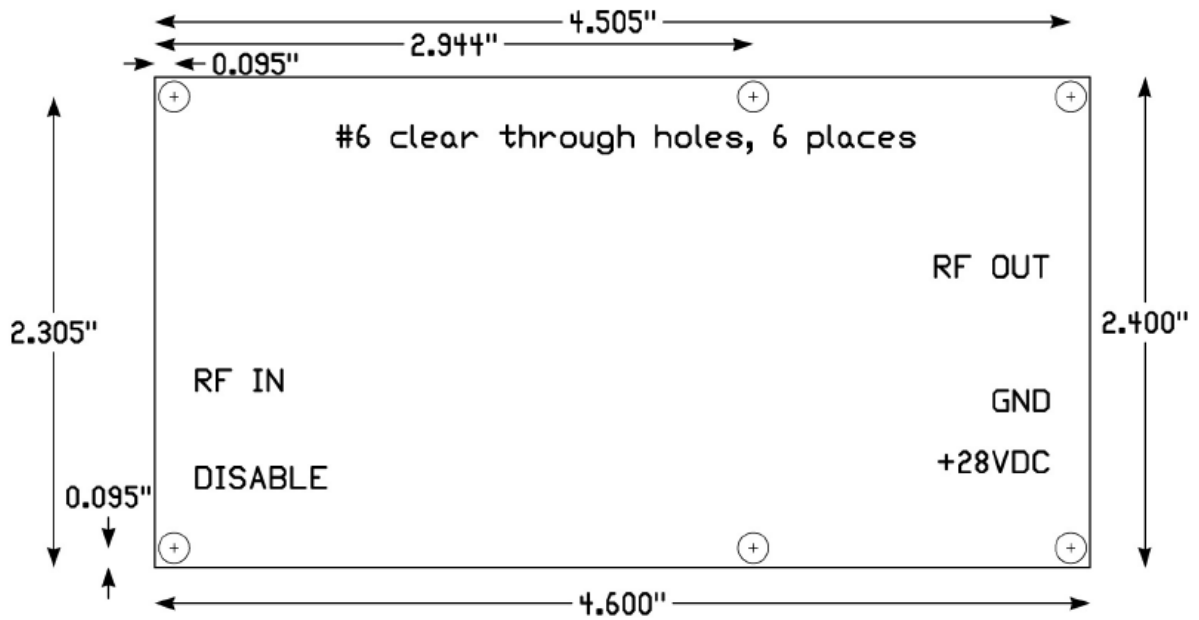


Figure 4: HD30538 Typical P_{1dB} and Safe Operating Area (SOA)

Dimensiones del amplificador





Instrucciones de uso Amplificador

1) Si no se suministra con un disipador de calor, aplicar una capa de pasta térmica de alta calidad a la parte inferior de la carcasa del amplificador. Más delgado es mejor, pero hay que asegurarse de que cuando se monta el disipador de calor, se puso en contacto en toda la base de la carcasa. Las lagunas y las burbujas de aire reducir significativamente el enfriamiento, dando lugar a posibles daños amplificador.

2) Garantizar suficiente flujo de aire a través de las aletas del disipador térmico para mantener la base máxima temperatura igual o inferior a la especificada en la sección máxima de calificaciones.

3) Conectar la fuente correcta de conector RF IN, y la carga deseada al conector RF OUT. Conectores de par a estándares de la industria para el tipo suministrado con el amplificador.

4) Conectar DC Vsup y cables de tierra a los terminales suministrados. Asegúrese de que las conexiones son de polaridad adecuada.

5) Aplicar alimentación de CC y la unidad de RF suficiente para alcanzar el nivel de salida deseado. Asegúrese de que el nivel de potencia de seguridad Área de servicio (SOA) se indica en la figura 4 no se supere, o amplificador daño puede ocurrir, y anulará la garantía.

6) Para desconectar el amplificador, primero retire la unidad de RF, a continuación, la corriente continua.

Característica y beneficios

- Single-ended or Balanced Output
- High Output IP3: +27 dBm
- Low Noise Figure: 3.5 dB
- Single Positive Supply: +5V
- 75 Ohm Input

El HMC549MS8G (E) es una GaAs MMIC PHEMT amplificador de bajo ruido que son pre-amplificador ideal para CATV Set Top Box, puerta de enlace doméstica, y los receptores de televisión digital que funcionan entre 40 y 960 MHz. Este alto rango dinámico LNA ha sido optimizado para proporcionar 3,5 dB figura de ruido y de salida 27 dBm IP3 a partir de una sola fuente de alimentación de +5 V @ 120 mA.

Las salidas de este LNA son extremadamente bien equilibrado, y se pueden utilizar para conducir un sintonizador de entrada diferencial con requisitos muy alta de entrada IP2. Este LNA de doble propósito también se puede utilizar como una conducción de entrada de dos sintonizadores de terminación única divisor activo. Este LNA está alojado en un paquete compatible con RoHS MSOP8G SMT con la paleta de tierra expuesta.

Aplicaciones

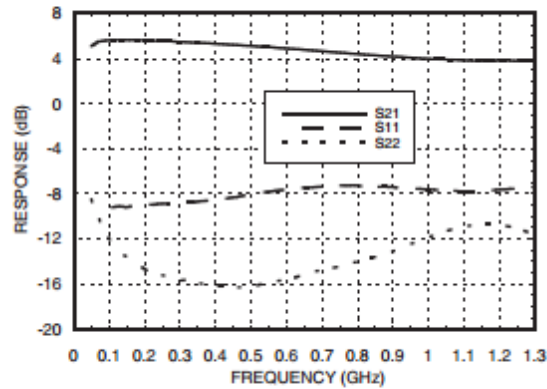
- Los receptores de televisión digital
- Multisintonizador Set Top Boxes
- PVR y Home Gateways

Electrical Specifications, 75 Ohm System, $T_A = +25^\circ\text{C}$, $V_{dd} = +5\text{V}$

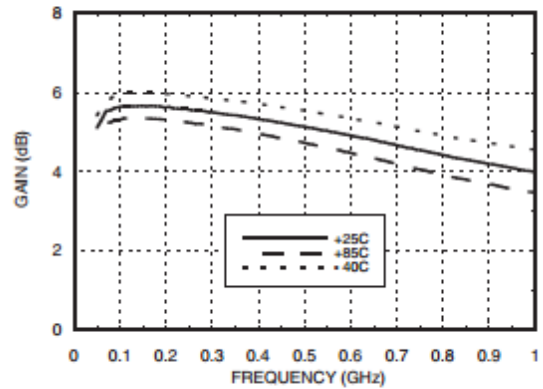
Parameter*	Min.	Typ.	Max.	Units
Frequency Range	0.04 - 0.96			GHz
Gain	2	5		dB
Gain Variation over Temperature		0.01	0.02	dB/°C
Noise Figure		3.5	5.2	dB
Input Return Loss		8		dB
Output Return Loss		15		dB
Output Power for 1 dB Compression (P1dB)		12.5		dBm
Output Third Order Intercept (OIP3)		27		dBm
Output Second Order Intercept (OIP2)		52		dBm
Amplitude Balance		0.3		dB
Phase Balance		2		deg
Supply Current (I _{dd})		120		mA

* Unless otherwise noted, all measurements performed with balun on the output.

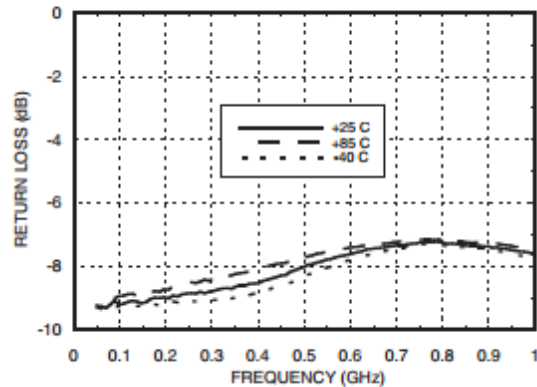
Broadband Gain & Return Loss



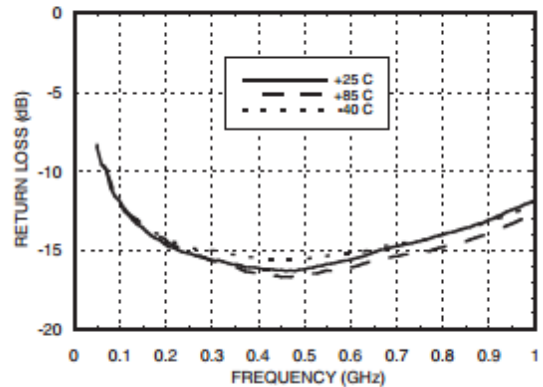
Gain vs. Temperature



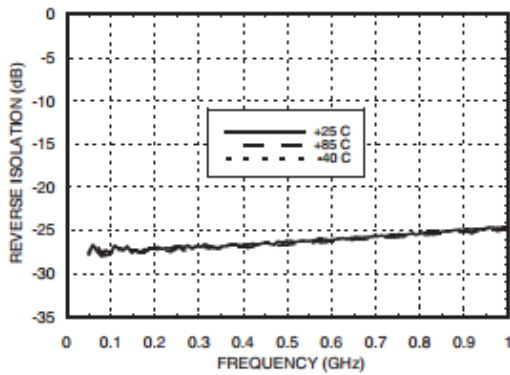
Input Return Loss vs. Temperature



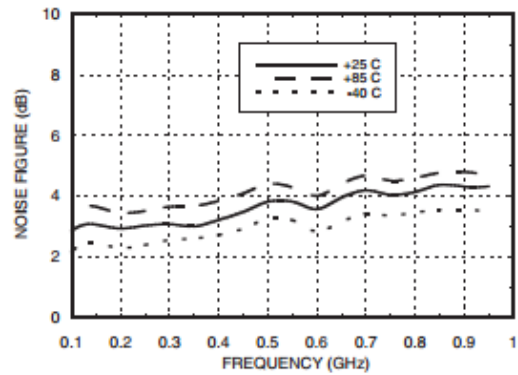
Output Return Loss vs. Temperature



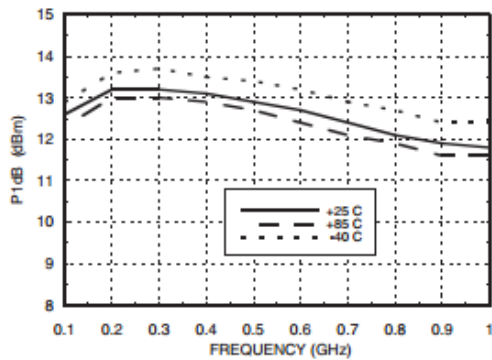
Reverse Isolation vs. Temperature



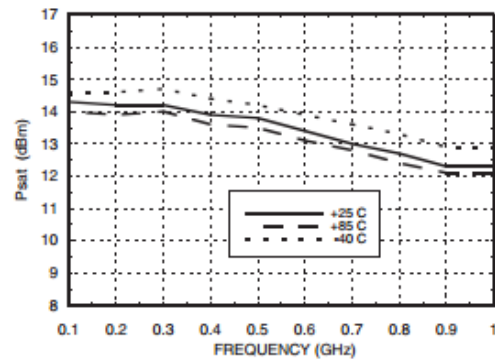
Noise Figure vs. Temperature



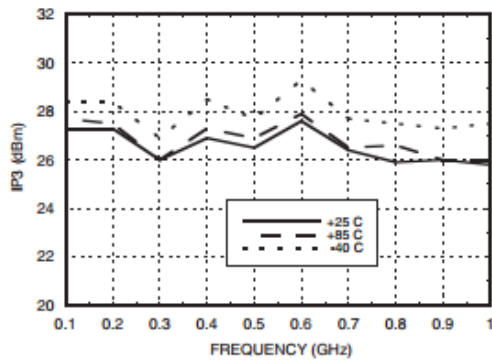
P1dB vs. Temperature



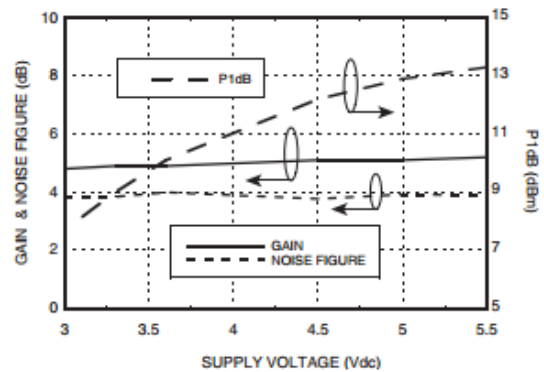
Psat vs. Temperature



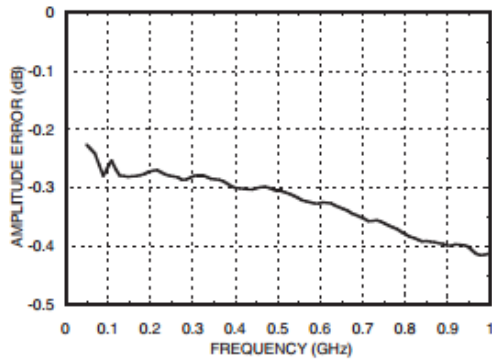
Output IP3 vs. Temperature



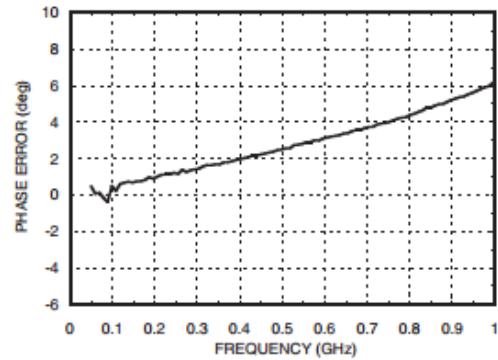
Gain, Noise Figure & P1dB vs. Supply Voltage @ 500 MHz



Amplitude Balance *



Phase Balance *



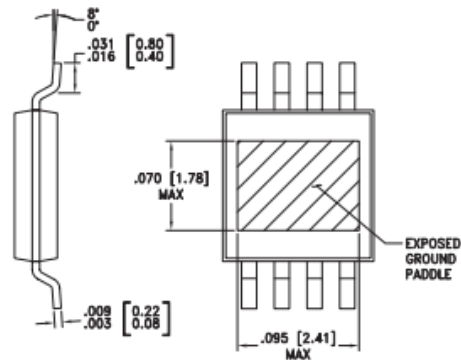
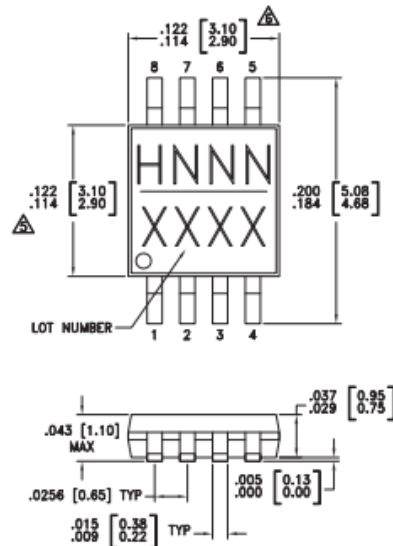
Absolute Maximum Ratings

Drain Bias Voltage (Vdd)	+7V
RF Input Power (RFIN)(Vdd = +3 Vdc)	0 dBm
Channel Temperature	150 °C
Continuous P _{diss} (T = 85 °C) (derate 20 mW/°C above 85 °C)	1.32 W
Thermal Resistance (channel to ground paddle)	49 °C/W
Storage Temperature	-65 to +150 °C
Operating Temperature	-40 to +85 °C
ESD Sensitivity (HBM)	Class 1A

Typical Supply Current vs. Vdd

Vdd (Vdc)	I _{dd} (mA)
3.0	117.1
3.3	117.5
3.6	117.9
4.5	118.5
5.0	119.0
5.5	119.3

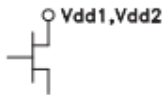
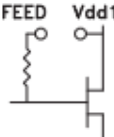
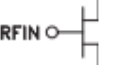
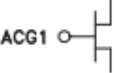
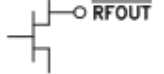
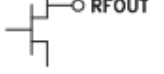
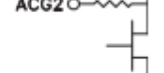
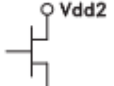
Outline Drawing



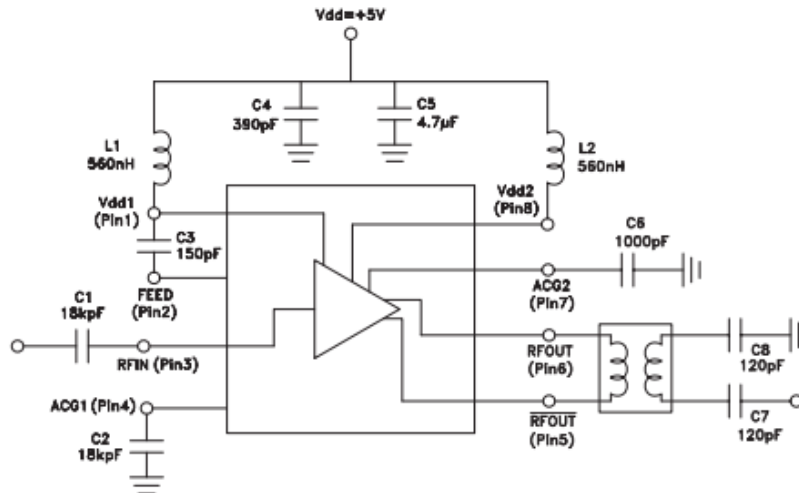
NOTES:

1. PACKAGE BODY MATERIAL: LOW STRESS INJECTION MOLDED PLASTIC, SILICA AND SILICON IMPREGNATED.
2. LEAD AND GROUND PADDLE MATERIAL: COPPER ALLOY
3. LEAD AND GROUND PADDLE PLATING: 100% MATTE TIN.
4. DIMENSIONS ARE IN INCHES [MILLIMETERS]
- △ DIMENSION DOES NOT INCLUDE MOLDFLASH OF 0.15mm PER SIDE.
- △ DIMENSION DOES NOT INCLUDE MOLDFLASH OF 0.25mm PER SIDE.
7. ALL GROUND LEADS AND GROUND PADDLE MUST BE SOLDERED

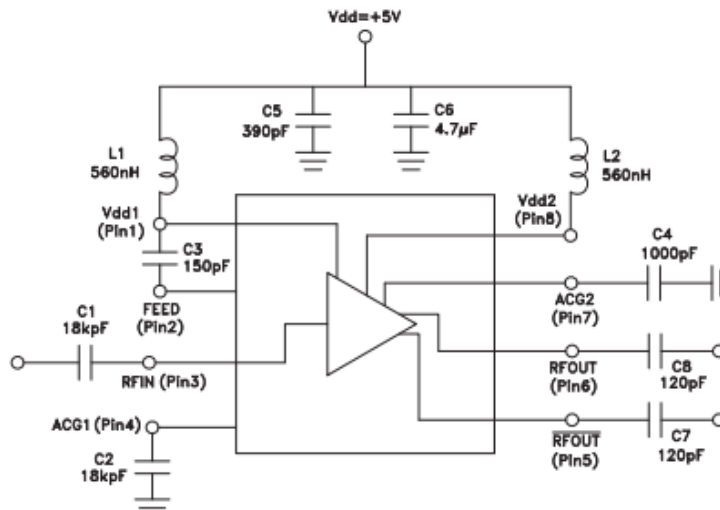
Pin Descriptions

Pin Number	Function	Description	Interface Schematic
1, 8	Vdd1, Vdd2	Power supply voltage for the first stage. An external choke inductor is required. See application circuit.	
2	FEED	Feedback capacitor for the first stage.	
3	RFIN	This pin is DC coupled and requires a DC blocking cap. See application circuit.	
4	ACG1	This pin has to be terminated by an external capacitor. See application circuit.	
5	$\overline{\text{RFOUT}}$	RF differential output 2. This port is DC coupled.	
6	RFOUT	RF differential output 1. This port is DC coupled.	
7	ACG2	This pin has to be terminated by an external capacitor. See application circuit.	
8	Vdd2	Power supply voltage for second stage. An external choke inductor is required. See application circuit.	

Application Circuit for 109236 - HMC549MS8G(E) (2-port)



Application Circuit for 113184 - HMC549MS8G(E) (3-port)



HMC-C045 Amplificador de bajo ruido del módulo, 1.8 - 4.2 GHz

Características y Beneficios



- Noise Figure: 0.7 dB @ 2.4 GHz
- Gain: 26 dB
- OIP3: +26 dBm
- P1dB Output Power: +15.5 dBm
- 50 Ohm Matched Input/Output
- Hermetically Sealed Module
- Field Replaceable SMA Connectors
- -55 to +85°C Operating Temperature

La HMC-C045 es un amplificador de bajo ruido GaAs MMIC PHEMT en una miniatura, módulo hermético que opera entre 1,8 y 4,2 GHz. Este módulo alto rango dinámico amplificador de bajo ruido proporciona 26 dB de ganancia, sub-1 factor de ruido dB y hasta 26 dBm de la producción de IP3 mientras se opera desde una sola fuente de alimentación positiva entre 8 V y + 15V. El amplificador de E / S se corresponden internamente a los 50 ohmios y DC bloqueada para un rendimiento robusto. El módulo dispone de conectores coaxiales desmontables que se pueden soltar para permitir la conexión directa de los pines de E / S a un circuito microstrip o coplanar.

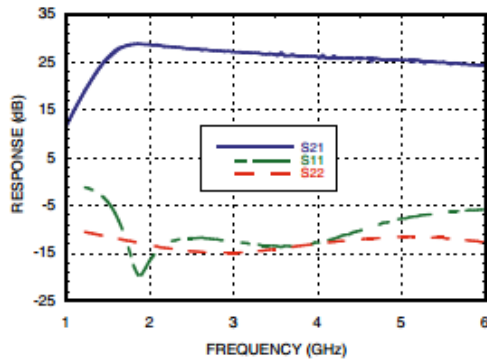
Aplicaciones

- Infraestructura de telecomunicaciones
- Microondas Radio y VSAT
- Militar y Espacio
- Equipo de prueba

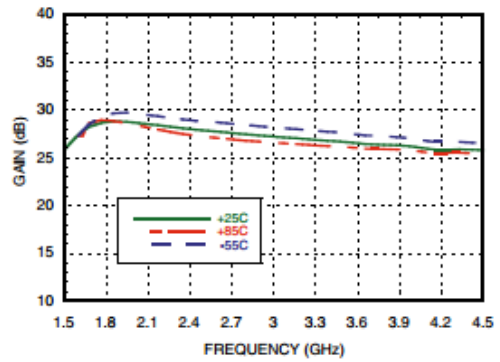
Electrical Specifications, $T_A = +25^\circ C$, $V_{dc} = +12V$

Parameter	Min.	Typ.	Max.	Min.	Typ.	Max.	Units
Frequency Range	1.8 - 4.2			2.0 - 3.8			GHz
Gain	23	26		23	26		dB
Gain Variation Over Temperature		0.03	0.05		0.03	0.05	dB/ °C
Noise Figure		1.2	2.5		1.2	2.0	dB
Input Return Loss		13			13		dB
Output Return Loss		13			13		dB
Output Power for 1 dB Compression (P1dB)	12.5	15.5		12.5	15.5		dBm
Saturated Output Power (Psat)		17.5			17.5		dBm
Output Third Order Intercept (IP3)		26			26		dBm
Supply Current		105	140		105	140	mA

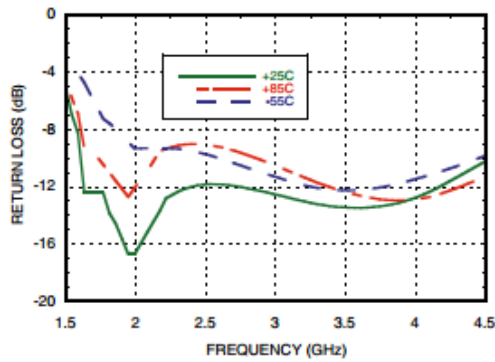
Broadband Gain & Return Loss



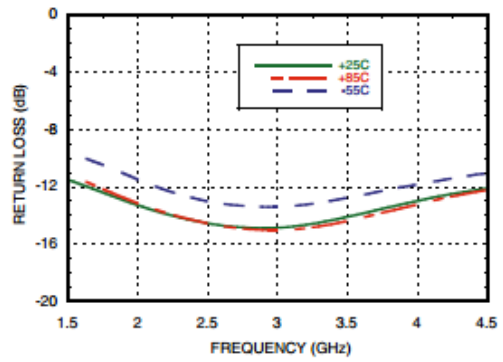
Gain vs. Temperature



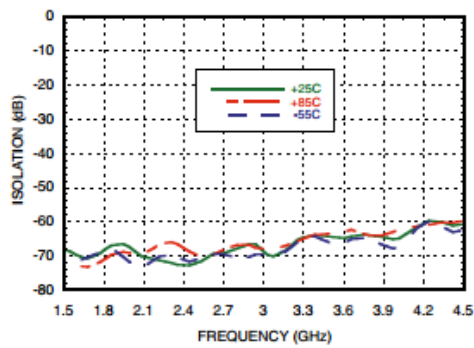
Input Return Loss vs. Temperature



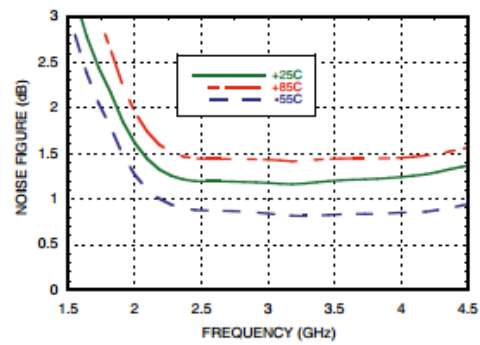
Output Return Loss vs. Temperature



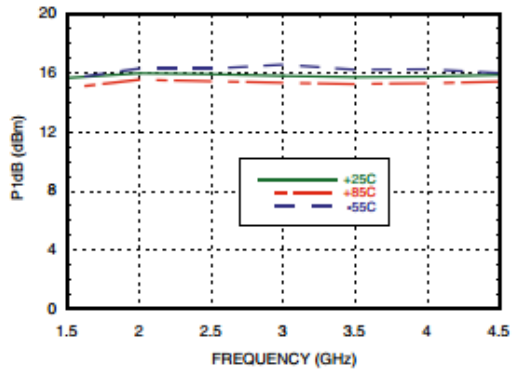
Reverse Isolation vs. Temperature



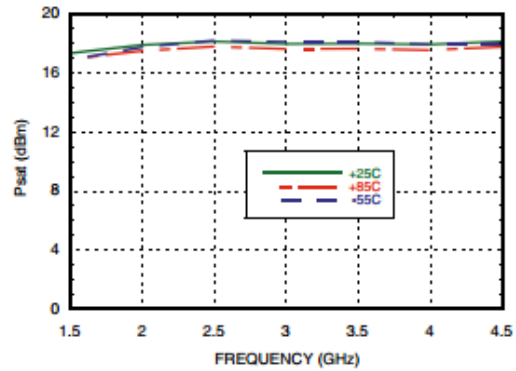
Noise Figure vs. Temperature



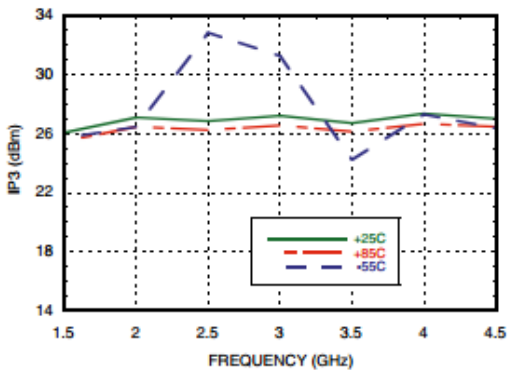
Output P1dB vs. Temperature



Output Psat vs. Temperature



Output IP3 vs. Temperature



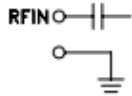

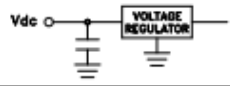
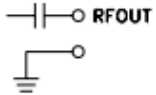
Absolute Maximum Ratings

Bias Supply Voltage (Vdc)	+15 Vdc
RF Input Power (RFIN)	+0 dBm
Storage Temperature	-65 to +150 °C
Operating Temperature	-55 to +85 °C

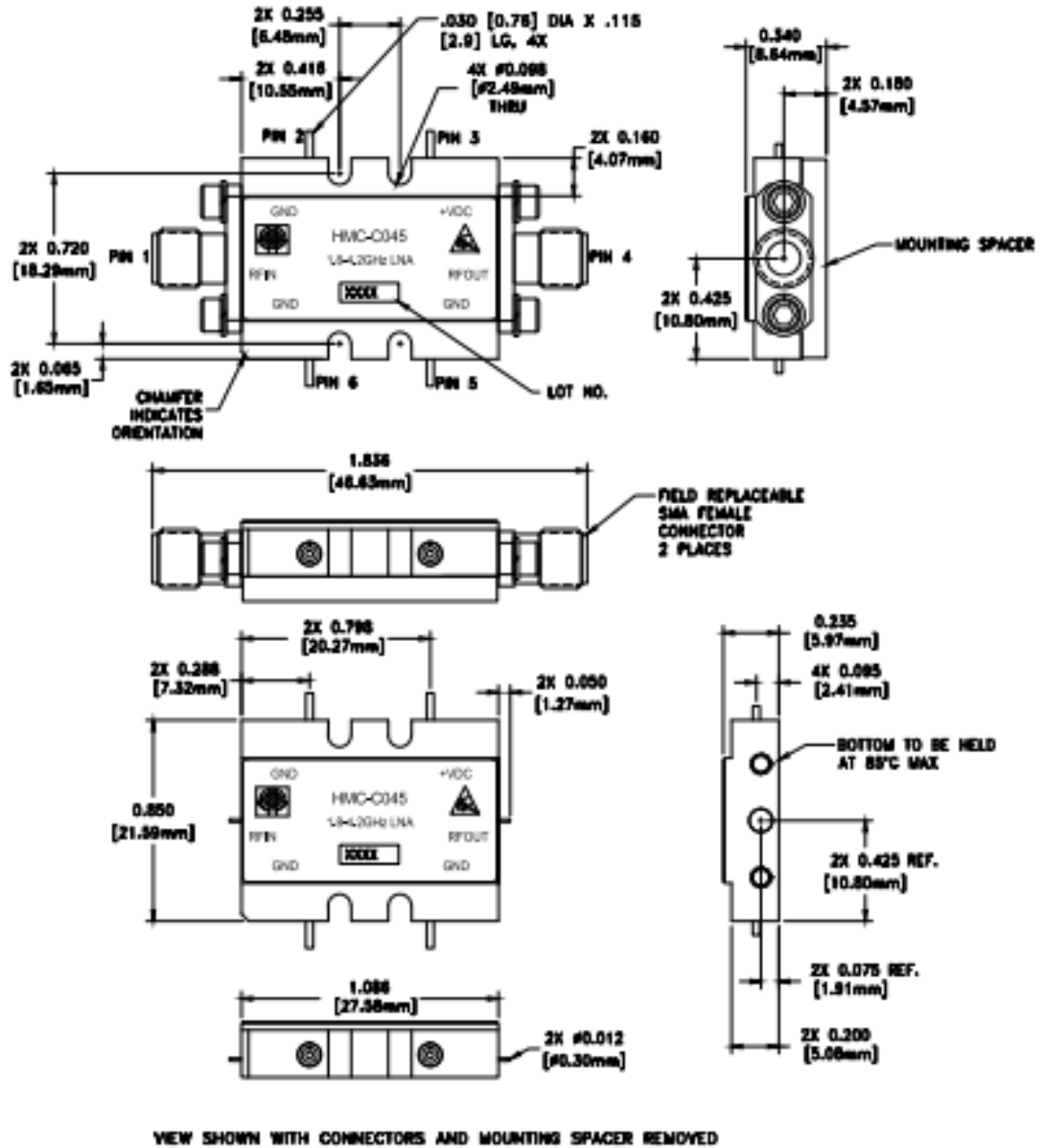


**ELECTROSTATIC SENSITIVE DEVICE
OBSERVE HANDLING PRECAUTIONS**

Pin Descriptions

Pin Number	Function	Description	Interface Schematic
1	RFIN & RF Ground	RF input connector, coaxial female, field replaceable. This pin is AC coupled and matched to 50 Ohms.	
2, 5, 6	GND	One of these pins must be connected to power supply ground.	
3	Vdc	Power supply voltage for the amplifier.	
4	RFOUT & RF Ground	RF output connector, coaxial female, field replaceable. This pin is AC coupled and matched to 50 Ohms.	

Outline Drawing



Package Information

Package Type	C-10
Package Weight [1]	18.7 gms [2]
Spacer Weight	3.3 gms [2]

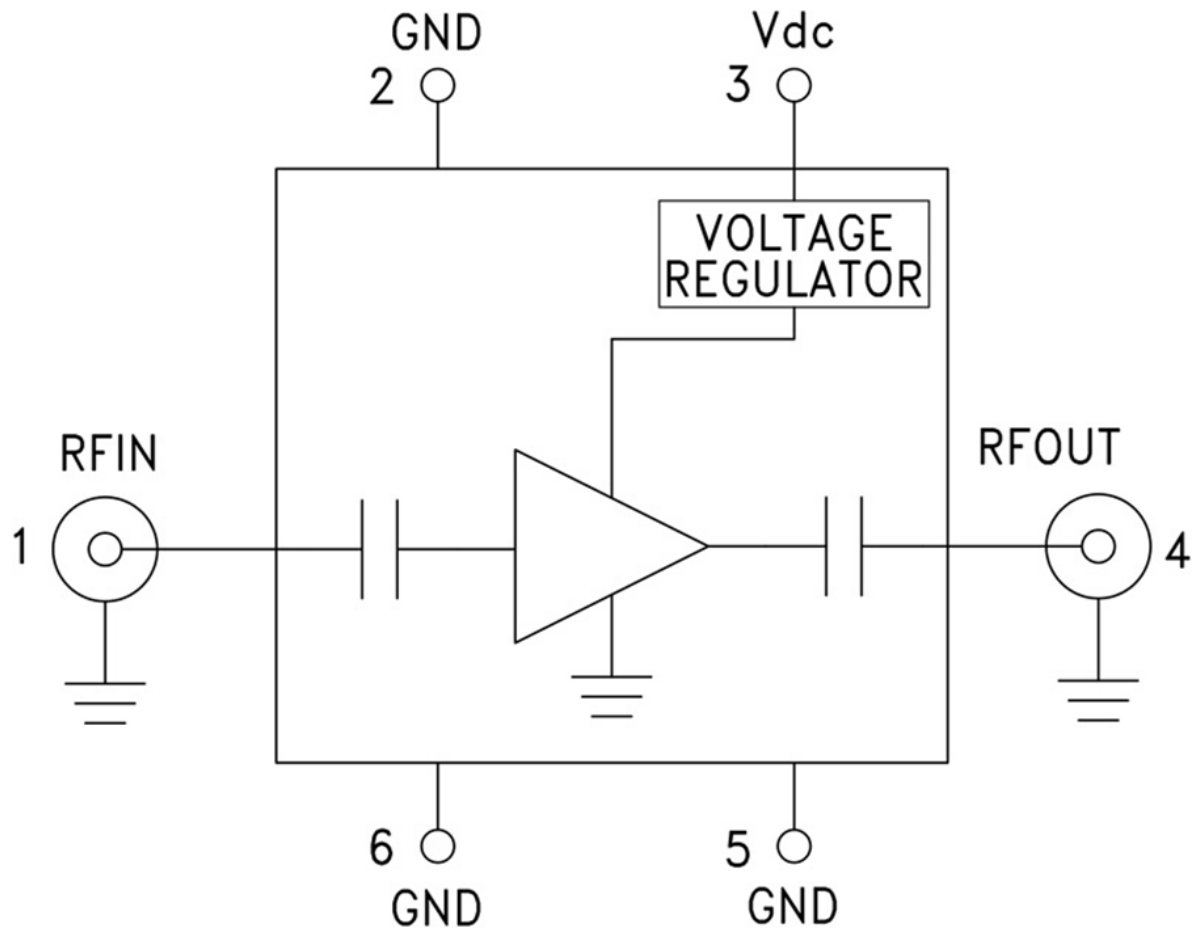
[1] Includes the connectors

[2] ±1 gms Tolerance

NOTES:

1. PACKAGE, LEADS, COVER MATERIAL: KOVAR™
2. FINISH: GOLD PLATE OVER NICKEL PLATE
3. ALL DIMENSIONS ARE IN INCHES (MILLIMETERS)
4. TOLERANCES:
 - 4.1 .XX ±0.02
 - 4.2 .XXX ±0.010
5. FIELD REPLACEABLE SMA CONNECTORS

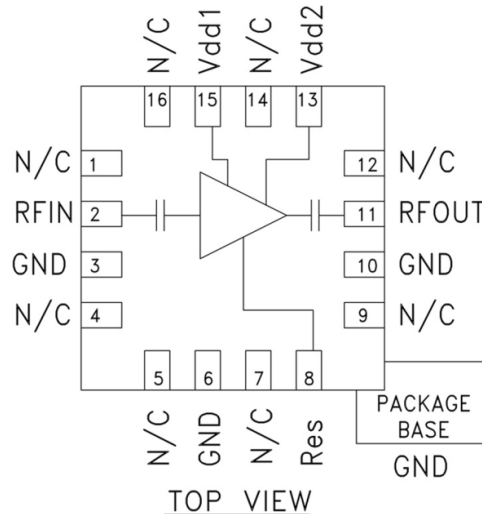
Función del diagrama



HMC382LP3 / HMC382LP3E Amplificador de bajo ruido SMD, 1.7 - 2.2 GHz

Características y Beneficios:

- La figura de ruido: 1 dB
- IP3 de salida: 30 dBm
- Ganancia: 17 dB
- Corriente de suministro ajustable externamente
- alimentación única positivo: + 5V
- 50 Ohm entrada coincidente / salida



El HMC382LP3 (E) es un alto rango dinámico de GaAs MMIC PHEMT bajo ruido Amplifier ideal para GSM y CDMA receptores de estación base de front-end celular que operan entre 1,7 y 2,2 GHz. Este LNA ha sido optimizado para proporcionar 1 figura de ruido dB, 17 dB de ganancia y +30 dBm IP3 de salida a partir de una sola fuente de alimentación de +5 V. El HMC382LP3 (E) cuentan con un suministro ajustable desde el exterior actual, que permite al diseñador para adaptar el rendimiento de linealidad del LNA para cada aplicación.

Aplicaciones

- Infraestructura celular / 3G
- Estaciones Base y Repetidores
- CDMA, W-CDMA, y TD-SCDMA
- GSM / GPRS y EDGE

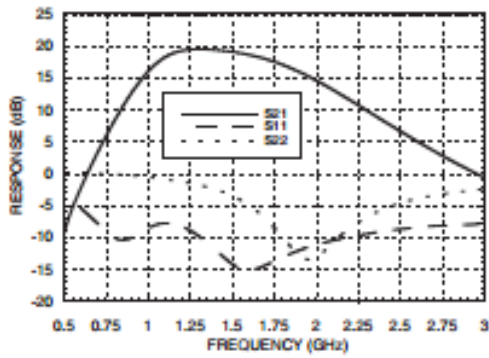


Electrical Specifications, $T_A = +25^\circ C$, $V_{dd1}, V_{dd2} = +5V$, $R_{bias} = 16\ Ohms^*$

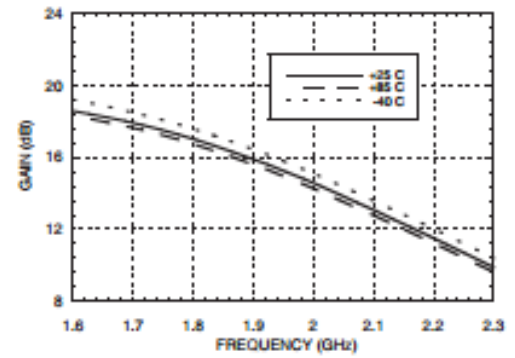
Parameter	Min.	Typ.	Max.	Min.	Typ.	Max.	Min.	Typ.	Max.	Min.	Typ.	Max.	Units
Frequency Range		1.7 - 1.9		1.9 - 2.0			2.0 - 2.1			2.1 - 2.2			GHz
Gain	14	17		12	15		11	14		9	12		dB
Gain Variation Over Temperature		0.01	0.015		0.01	0.015		0.01	0.015		0.01	0.015	dB/°C
Noise Figure		1.0	1.3		1.05	1.35		1.15	1.45		1.2	1.5	dB
Input Return Loss		13			12			11			10		dB
Output Return Loss		10			13			12			9		dB
Reverse Isolation		37			36			35			35		dB
Output Power for 1dB Compression (P1dB)		16			16			15.5			14		dBm
Output Third Order Intercept (IP3) (-20 dBm Input Power per tone, 1 MHz tone spacing)		29.5			30			30			29.5		dBm
Supply Current ($I_{dd1} + I_{dd2}$)		67			67			67			67		mA

* R_{bias} resistor value sets current. See application circuit herein.

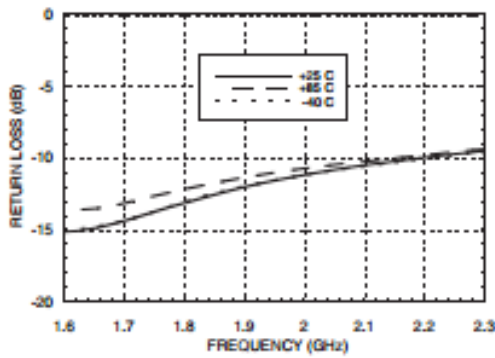
Broadband Gain & Return Loss



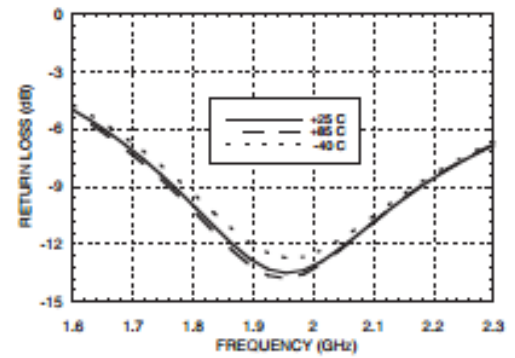
Gain vs. Temperature



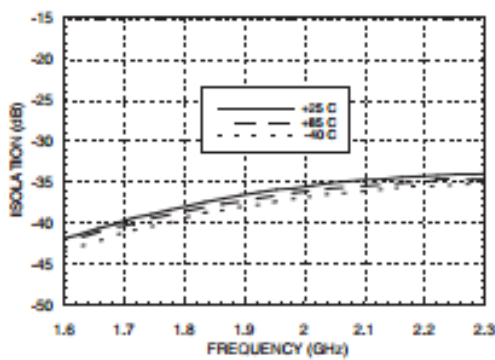
Input Return Loss vs. Temperature



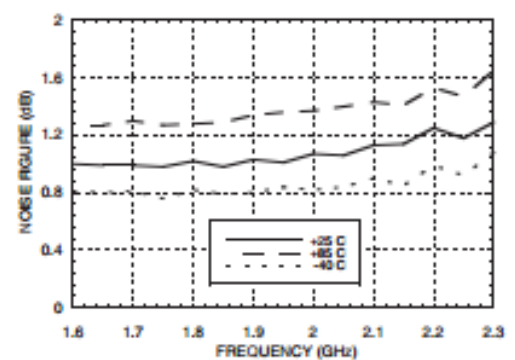
Output Return Loss vs. Temperature



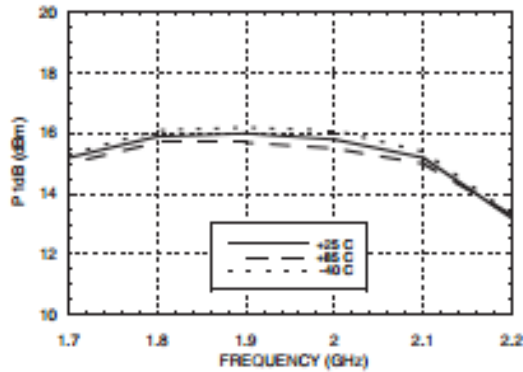
Reverse Isolation vs. Temperature



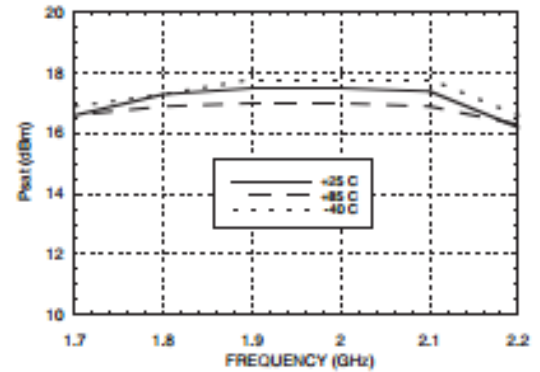
Noise Figure vs. Temperature



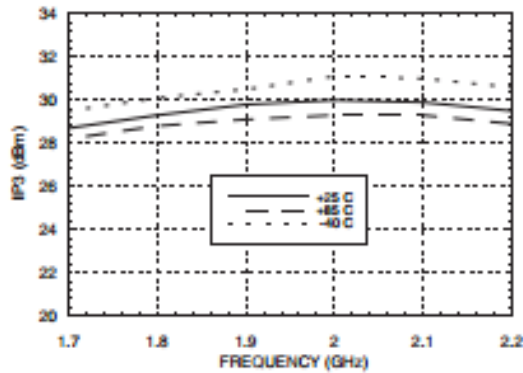
P1dB vs. Temperature @ I_{dd} = 67 mA



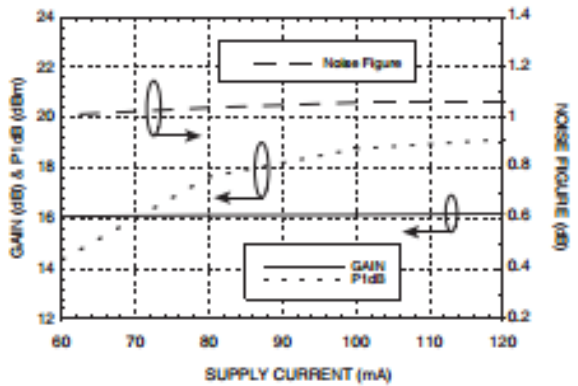
Psat vs. Temperature @ I_{dd} = 67 mA



Output IP3 vs. Temperature I_{dd} = @ 67 mA



Gain, Noise Figure & P1dB vs. Supply Current @ 1900 MHz



Absolute Maximum Ratings

Drain Bias Voltage (V _{dd1} , V _{dd2})	+8.0 Vdc
RF Input Power (RFIN)(V _s = +5.0 Vdc)	+10 dBm
Channel Temperature	150 °C
Continuous P _{diss} (T = 85 °C) (derate 6.94 mW/°C above 85 °C)	0.451 W
Thermal Resistance (channel to ground paddle)	144 °C/W
Storage Temperature	-65 to +150 °C
Operating Temperature	-40 to +85 °C

Typical Supply Current vs. V_{dd1} & V_{dd2}

V _{dd} (Vdc)	I _{dd} (mA)
+4.5	67.2
+5.0	67.4
+5.5	67.6

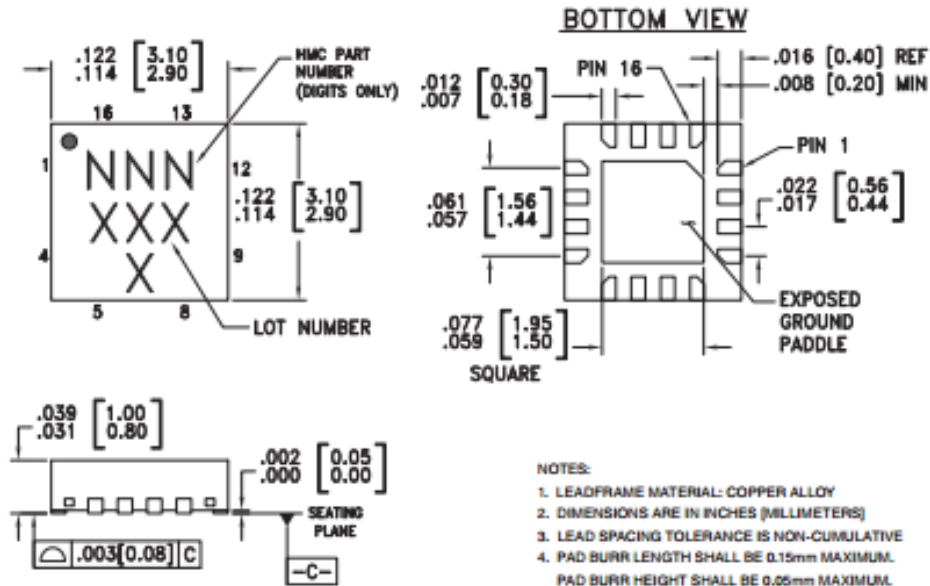
Recommended Bias Resistor Values for Various I_{dd1} & I_{dd2}

I _{dd1} + I _{dd2} (mA)	R _{bias} (Ohms)
60	27
70	16
80	13
100	8.2
120	3.9



ELECTROSTATIC SENSITIVE DEVICE
OBSERVE HANDLING PRECAUTIONS

Outline Drawing



NOTES:

1. LEADFRAME MATERIAL: COPPER ALLOY
2. DIMENSIONS ARE IN INCHES (MILLIMETERS)
3. LEAD SPACING TOLERANCE IS NON-CUMULATIVE
4. PAD BURR LENGTH SHALL BE 0.15mm MAXIMUM.
PAD BURR HEIGHT SHALL BE 0.05mm MAXIMUM.
5. PACKAGE WARP SHALL NOT EXCEED 0.05mm.
6. ALL GROUND LEADS AND GROUND PADDLE MUST BE SOLDERED TO PCB RF GROUND.
7. REFER TO HITTITE APPLICATION NOTE FOR SUGGESTED LAND PATTERN.

Package Information

Part Number	Package Body Material	Lead Finish	MSL Rating	Package Marking ^[2]
HMC382LP3	Low Stress Injection Molded Plastic	Sr/Pb Solder	MSL1 ^[1]	382 XXXX
HMC382LP3E	RoHS-compliant Low Stress Injection Molded Plastic	100% matte Sn	MSL1 ^[2]	382 XXXX

[1] Max peak reflow temperature of 235 °C

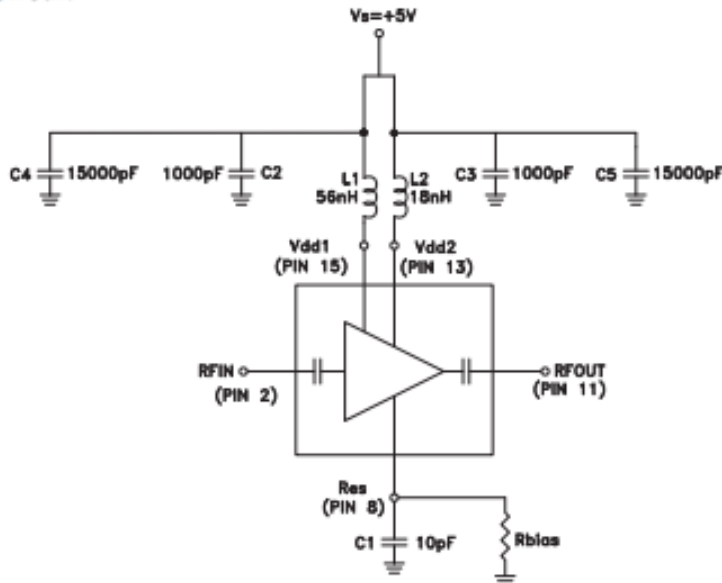
[2] Max peak reflow temperature of 260 °C

[3] 4-Digit lot number XXXX

Pin Descriptions

Pin Number	Function	Description	Interface Schematic
1, 4, 5, 7, 9, 12, 14, 16	NC	No connection necessary. These pins may be connected to RF/DC ground. Performance will not be affected.	
2	RFIN	This pin is AC coupled and matched to 50 Ohms.	RFIN
3, 6, 10	GND	These pins and package bottom must be connected to RF/DC ground.	
8	Res	This pin is used to set the DC current of the amplifier by selection of external bias resistor. See application circuit.	
11	RFOUT	This pin is AC coupled and matched to 50 Ohms.	RFOUT
13,15	Vdd2, Vdd1	Power supply voltage. Choke inductor and bypass capacitors are required. See application circuit.	

Application Circuit



Amplificadores de potencia (HPA) para RF

Es una parte importante del circuito de transmisión. Por lo general, está constituido por un amplificador de varias etapas, cuya salida es el punto más alto del transmisor de enlace, y la comunicará a través de la impresión a doble cara antenna está conectada. HPA es el papel importante en la frecuencia de transmisión a la amplificación de la señal de bajo nivel requerido para la transmisión a larga distancia de los niveles de alta potencia. Bandas debido a la distancia de transmisión, ganancia de la antenna, la modulación de la señal y otros factores, la potencia de salida del transmisor diferente varía mucho HPA. Puede variar desde decenas de vatios a decenas de milivatios en una banda de microondas convencional (800MHz ~ 28GHz). Características del amplificador de alta potencia:

De gran capacidad (o vehículo) sistema de comunicaciones digital, diseño de circuitos HPA, sobre todo en el circuito de etapa tardía, la contradicción entre la producción de energía y los requisitos de linealidad a menudo ocurre. A menudo utilizando tres soluciones * circuito amplificador equilibrado, su potencia de salida combinada de un solo tubo doble y mantienen una sola línea de. A menudo se utiliza en un circuito convencional de banda de microondas en cuadratura híbrido se muestra a continuación (o 3 dB puente) para lograr la síntesis del poder. Antena de transmisión MIX RF MOD BPF HPA MUL BB en la figura HPA 1a ubicación del transmisor RF...

KHPA0206 Módulos amplificadores de 2-6 GHz RF de alta potencia

La familia KHPA0206 SSPA es una serie de amplificadores de banda ancha que cubren 2-6 GHz que son adecuados para el montaje en bastidor. Estos amplificadores son capaces de dar salida hasta 300W de potencia de RF continua. Un número de opciones están disponibles dependiendo de las necesidades del cliente, tales como TTL de conmutación remoto local. versiones de 100W y 300W están disponibles. modelos de menor potencia están disponibles bajo petición.

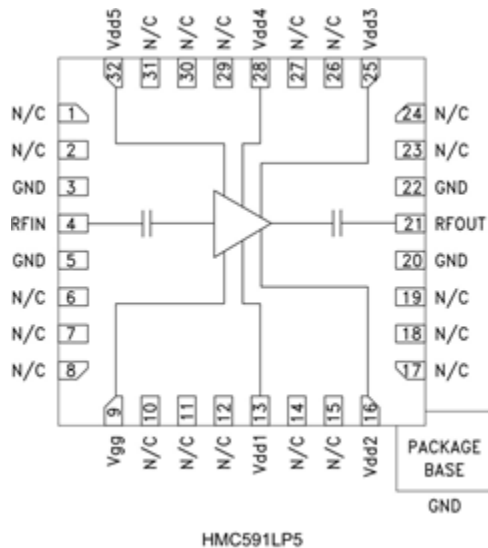
Aplicaciones

- Radar comercial
- Radar militar
- Guerra electrónica
- Equipo de prueba

Table 1. Specifications

Input Power	
AC Power	110/240VAC
Frequency	50/60 Hz
Output Specifications [@ 25° C]	
Frequency Range	2-6 GHz
Saturated Power Output	300W TYP
Gain	60 dB Min
Noise Figure	5 dB TYP
In/Out VSWR	<2:1 TYP
In/Out Impedance	50 Ω
Local/ Remote	TTL
Connectors	
RF In / Out	"N" Female
Mechanical	
5U Aluminum Chassis (19" rack mount) 19" wide, 10.5" High, 17.7" Depth Chassis Grounded	
Environmental	
Operating Temperature	-40° to 50° C
Storage Temperature	-40° to 50° C
Relative Humidity	5 to 95% non-condensing
MTBF	
200,000 hours	

El HMC591LP5 (E) 2 vatios amplificador de energía de SMT, 6,0 - 9.5 GHz



Características y beneficios

- Saturated Output Power: +33 dBm @ 20% PAE
- Output IP3: +41 dBm
- Gain: 18 dB
- DC Supply: +7V @ 1340 mA
- 50 Ohm Matched Input/Output
- QFN Leadless SMT Packages, 25 mm²

El HMC591LP5 (E) es un alto rango dinámico de GaAs MMIC PHEMT 2 vatios amplificador de potencia que opera 6-9,5 GHz. El amplificador proporciona 18 dB de ganancia, 33 dBm de potencia saturada, y 19% PAE desde un suministro de +7V. Este 50 Ohm corresponde amplificador no requiere componentes externos y la RF I / Os se bloquean DC para el funcionamiento robusto. Para aplicaciones que requieren OIP3 óptima, Idd deberá ser ajustado a 940 mA, para producir +41 dBm OIP3. Para aplicaciones que requieren un rendimiento óptimo P1dB, Idd deberá ser ajustado a 1340 mA, para dar salida +33 dBm P1dB.

Aplicaciones

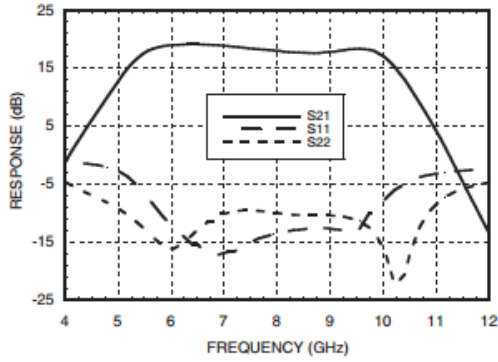
- Punto-a-Punto radios
- Punto a Multipunto-radios
- Equipos y sensores de prueba
- Militares del uso final
- Espacio

Electrical Specifications, $T_A = +25^\circ \text{C}$, $V_{dd} = +7\text{V}$, $I_{dd} = 1340 \text{mA}$ ^[1]

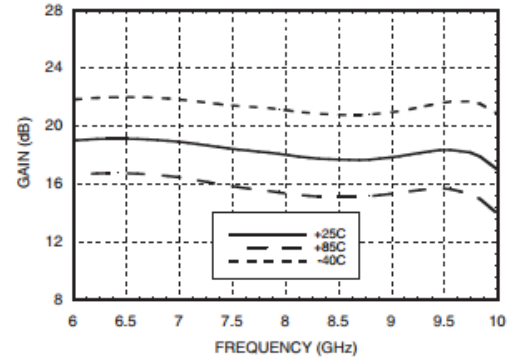
Parameter	Min.	Typ.	Max.	Min.	Typ.	Max.	Units
Frequency Range	6 - 8			6 - 9.5			GHz
Gain	16	19		15	18		dB
Gain Variation Over Temperature		0.05			0.05		dB/ °C
Input Return Loss		14			12		dB
Output Return Loss		12			10		dB
Output Power for 1 dB Compression (P1dB)	30	32		30	33		dBm
Saturated Output Power (Psat)		32.5			33		dBm
Output Third Order Intercept (IP3) ^[2]		41			41		dBm
Supply Current (Idd)		1340			1340		mA

[1] Adjust Vgg between -2 to 0V to achieve Idd= 1340 mA typical.

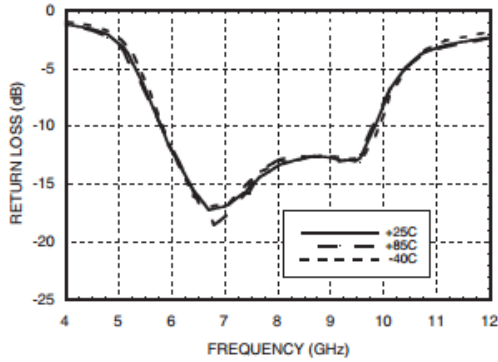
Broadband Gain & Return Loss



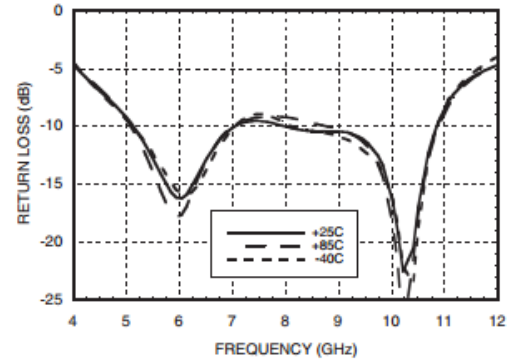
Gain vs. Temperature



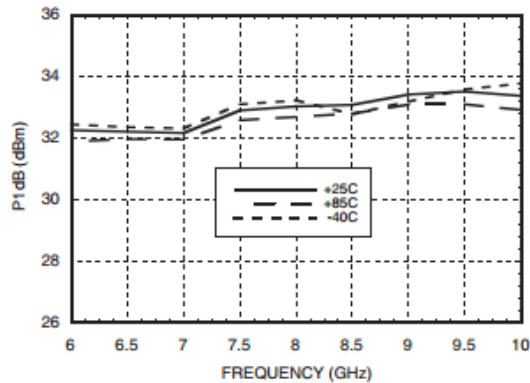
Input Return Loss vs. Temperature



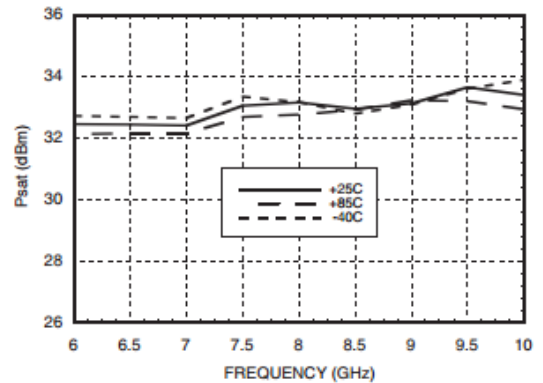
Output Return Loss vs. Temperature



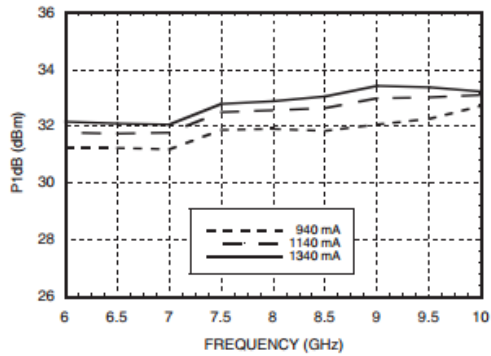
P1dB vs. Temperature



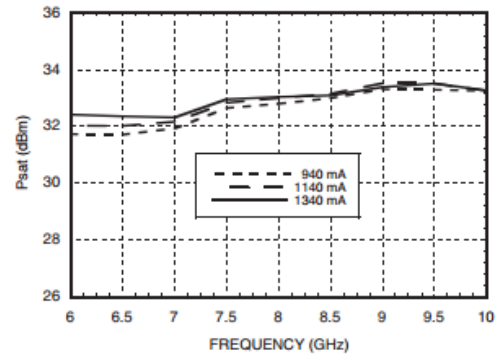
Psat vs. Temperature



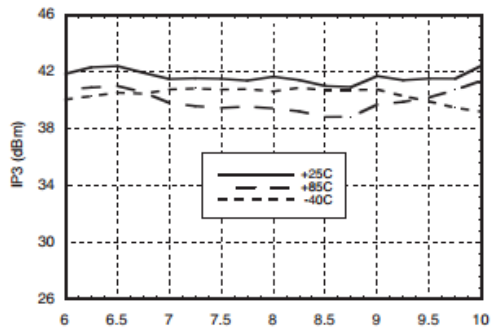
P1dB vs. Current



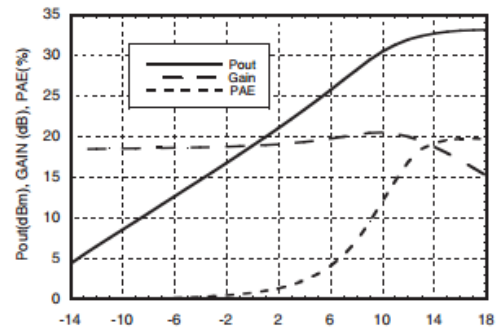
Psat vs. Current



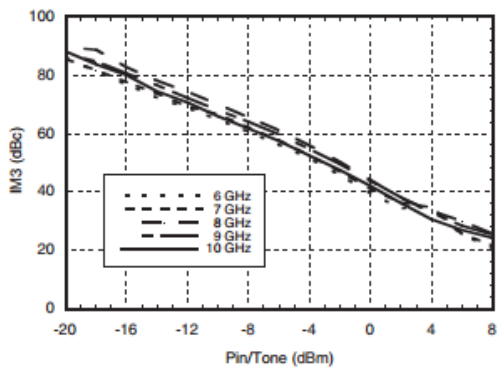
Output IP3 vs. Temperature
7V @ 940 mA, Pin/Tone = -15 dBm



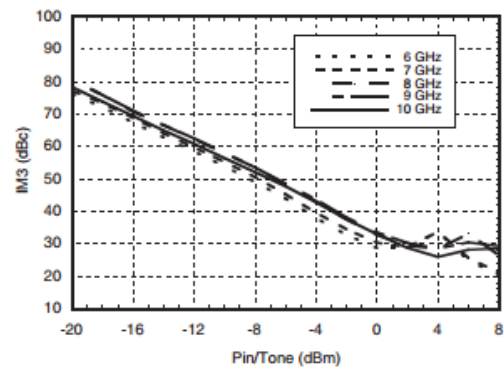
Power Compression @ 8 GHz,
7V @ 1340 mA



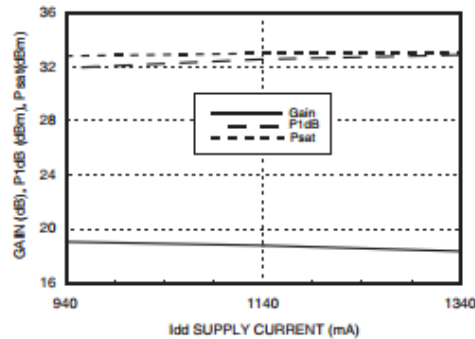
Output IM3, 7V @ 940 mA



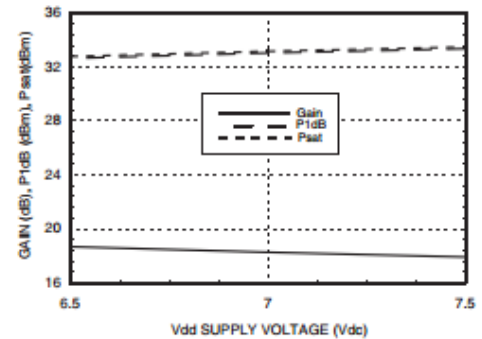
Output IM3, 7V @ 1340 mA



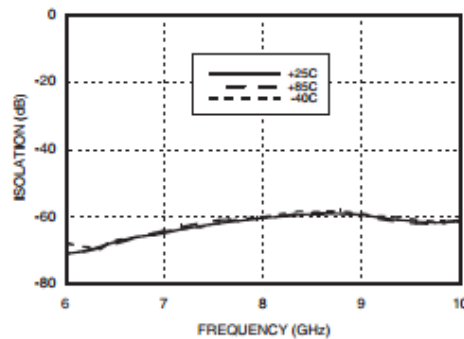
Gain & Power vs. Supply Current @ 8 GHz



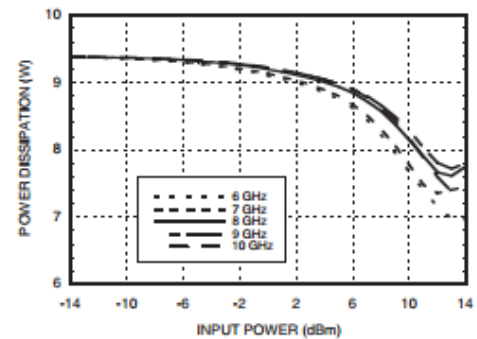
Gain & Power vs. Supply Voltage @ 8 GHz



Reverse Isolation vs. Temperature, 7V @ 1340 mA



Power Dissipation



Absolute Maximum Ratings

Drain Bias Voltage (Vdd)	+8 Vdc
Gate Bias Voltage (Vgg)	-2.0 to 0 Vdc
RF Input Power (RFIN)(Vdd = +7.0 Vdc)	+15 dBm
Channel Temperature	175 °C
Continuous P _{diss} (T _a = 75 °C) (derate 104.3 mW/°C above 75 °C)	10.43 W
Thermal Resistance (channel to package bottom)	9.59 °C/W
Storage Temperature	-65 to +150 °C
Operating Temperature	-40 to +85 °C

Typical Supply Current vs. Vdd

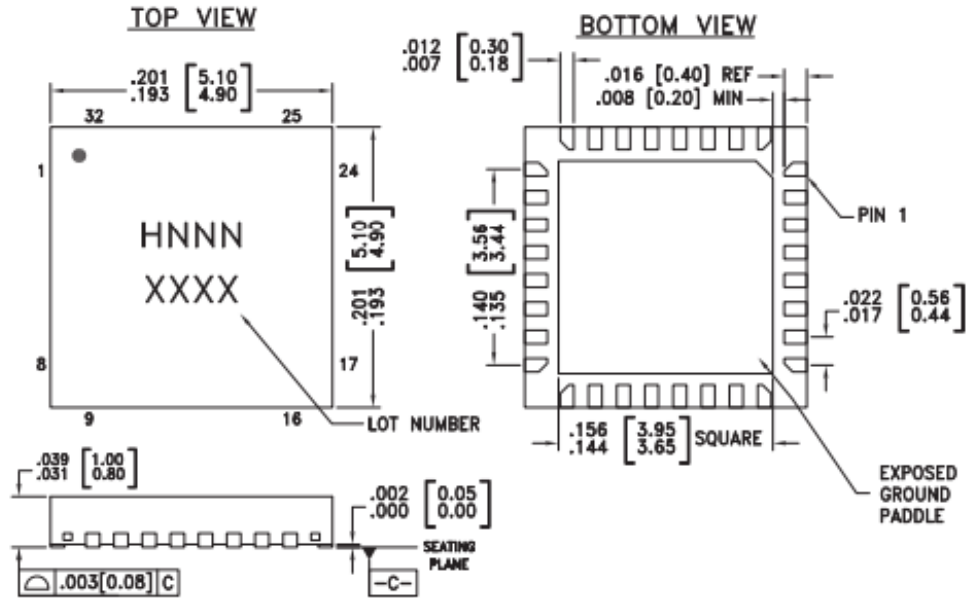
Vdd (V)	I _{dd} (mA)
+6.5	1350
+7.0	1340
+7.5	1330

Note: Amplifier will operate over full voltage ranges shown above V_{gg} adjusted to achieve I_{dd} = 1340 mA at +7.0V



ELECTROSTATIC SENSITIVE DEVICE
OBSERVE HANDLING PRECAUTIONS

Outline Drawing



NOTES:

1. LEADFRAME MATERIAL: COPPER ALLOY
2. DIMENSIONS ARE IN INCHES (MILLIMETERS)
3. LEAD SPACING TOLERANCE IS NON-CUMULATIVE
4. PAD BURR LENGTH SHALL BE 0.15mm MAXIMUM.
PAD BURR HEIGHT SHALL BE 0.05mm MAXIMUM.
5. PACKAGE WARP SHALL NOT EXCEED 0.05mm.
6. ALL GROUND LEADS AND GROUND PADDLE MUST BE SOLDERED TO PCB RF GROUND.
7. REFER TO HITTITE APPLICATION NOTE FOR SUGGESTED LAND PATTERN.

Package Information

Part Number	Package Body Material	Lead Finish	MSL Rating	Package Marking ^[3]
HMC591LP5	Low Stress Injection Molded Plastic	Sn/Pb Solder	MSL1 ^[1]	H591 XXXX
HMC591LP5E	RoHS-compliant Low Stress Injection Molded Plastic	100% matte Sn	MSL1 ^[2]	H591 XXXX

[1] Max peak reflow temperature of 235 °C

[2] Max peak reflow temperature of 260 °C

[3] 4-Digit lot number XXXX

Pad Descriptions

Pad Number	Function	Description	Interface Schematic
1, 2, 6 - 8, 10 - 12, 14, 15, 17 - 19, 23, 24, 26, 27, 29 - 31	N/C	Not connected.	
3, 5, 20, 22	GND	Package bottom has an exposed metal paddle that must be connected to RF/DC ground.	
4	RFIN	This pad is AC coupled and matched to 50 Ohms.	
9	Vgg	Gate control for amplifier. Adjust to achieve I _{dd} of 1340 mA. Please follow "MMIC Amplifier Biasing Procedure" Application Note. External bypass capacitors of 100 pF and 2.2 μF are required.	
13, 16, 25, 28, 32	Vdd 1-5	Power Supply Voltage for the amplifier. External bypass capacitors of 100 pF and 2.2 μF are required.	
21	RFOUT	This pad is AC coupled and matched to 50 Ohms.	

Application Circuit

Component	Value
C1 - C6	100pF
C7 - C12	2.2μF

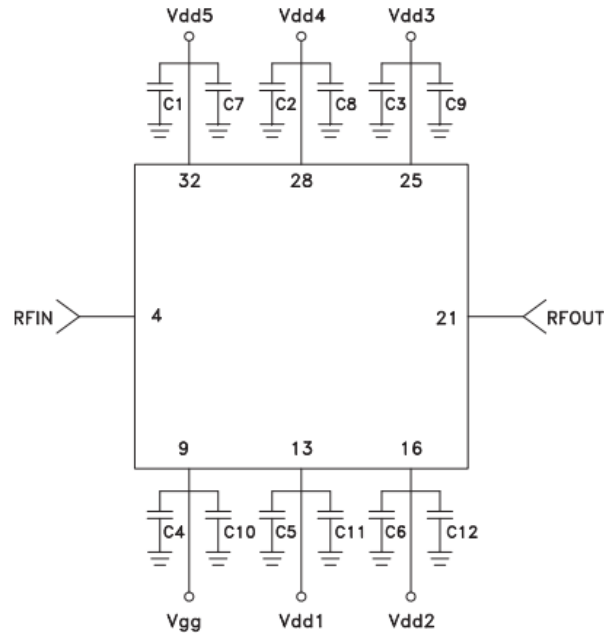




Tabla de los diferentes amplificadores de bajo nivel de ruido

Amplificador de bajo consumo (-40C a + 85C)

HD P/N	Frequency (MHz)	NF (dB)	Gain (dB)	P1 (dBm)	IP3 (dBm)	VSWR (Input/Output)	DC Power	
							Volt	mA
HD24410	10-1500	3.6	40	+20	+32	1.3/1.4	12	135
HD24649	100-1000	3.5	45	+20	+34	1.5/1.5	12	135
HD23458	10-3000	3.3	18	+20	+33	1.7/1.9	12	115
HD24838	50-3000	4.5	24	+14	+24	1.4/1.5	12	95
HD24839	30-3500	6.0	27	+23	+35	1.5/1.5	5	160
HD23414	10-4000	3.5	18	+20	+34	1.5/2.0	12	80
HD24840	100-5000	4.5	15	+19	+35	1.5/1.5	12	85
HD24841	60-4000	4.2	20	+20	+35	1.5/1.5	5	75
HD24842	70-5500	4.5	15	+19	+35	1.5/1.5	5	80
HD24221	100-6000	4.0	15	+12.5	+26	2.0/2.3	12	40
HD24222	100-6000	4.2	34	+19	+32	2.0/2.0	12	125
HD24223	100-10000	4.0	16	+13	+28	1.7/1.7	12	50
HD26005	1-3000	4.0	20	+22	+35	1.5/2.0	15	110
HD26183	0.01-3000	4.0	13	+13	+27	1.2/1.5	15	47
HD26399	50-1000	3.6	20	+20	+36	1.2/1.3	12	85
HD26418	50-2500	4.0	17	+18.5	+32.5	1.5/1.5	12	85
HD26419	50-3000	4.4	11.5	+17.5	+32.5	1.2/1.3	12	80
HD26905	0.3-6500	4.5	37	+17	+32	1.4/1.6	12	120

Amplificador de baja potencia (-54 C a 85 C)

HD P/N	Frequency (MHz)	NF (dB)	Gain (dB)	P1 (dBm)	IP3 (dBm)	VSWR (Input/Output)	DC Power	
							Volt	mA
HD24052	10-300	2.8	25	+20	+31	1.5/1.6	15	50
HD24053	10-1000	4.0	25	+20	+33	1.3/1.5	15	125
HD24843	5-600	4.0	16	+18	+32	1.5/1.4	15	56
HD24844	3-600	4.5	13	+22	+34	1.5/1.5	15	85

Para ponerse en contacto con la empresa

Department	E-mail
Customer Service	custsvc@hdcom.com
Human Resources	hr@hdcom.com
Orders	orders@hdcom.com
Sales+ (see note below)	sales@hdcom.com
Technical Support+ (see note below)	rfcomponents@hdcom.com
Technical Sales (pricing, availability, & product info) dial (631) 588-3877 ext. 112 Our phone hours are Monday - Friday; 9:00 am (ET) - 5:00 pm (ET)	
Request For Quote (RFQ) Form	



REFERENCIAS BIBLIOGRAFICAS

Arazo, M, (2011). *Diseño e implementación de una sistema de monitorización y control para un modem satélite a través del protocolo SNMP*. Proyecto final de carrera, Escola Tecnica superior d'Enginyeria de Telecomunicacion de Barcelona, Universitat politécnica de Catalunya, Barcelona, España.

Arquitectura de administración OSI. Recuperado el 03 de septiembre de 2016, de <http://www.arcesio.net/osinm/osinminformacion.html>

Cisco systems, Inc. (2007). *CCNA Exploration 4.0 Conceptos y protocolos de enrutamiento*

Castells, M (2006). *La sociedad red: una visión global*. Madrid, España Aliana Editorial.

El *protocolo ICMP*. Recuperado el 16 de julio de 2016 de, <http://es.kioskea.net/contents/internet/icmp.php3>

El *protocolo ICMP*. Recuperado el 16 de julio de 2016 de, <http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html>

Case, fedor, Schoffstall, & Davin. (05/1990). *RFC1157*. Recuperado el 27 de julio de 2016, de <http://www.ietf.org/rfc/rfc1157.txt>

Comandos. Recuperado el 25 de julio de 2016 de, <https://es.scribd.com/doc/45378946/02-CentOS-Comandos-basicos>

MIB browser. Recuperada el 29 de julio de 2016, de <http://www.oidview.com/images/mibbrowser-full.gif>

Martinez, Navaez. (2010). *Implementación de ZABBIX como herramienta de monitorización de infraestructura informática de la compañía santini System Group Ltda*. Proyecto final de carrera, facultad de ingeniería Electronica, Universidad Santo Tomás, Bogotá, Colombia.

La empresa. Recuperada el 20 de julio de 2016 de, http://www.cfe.gob.mx/ConoceCFE/Paginas/Conoce_CFE.aspx

MySQL. Recuperado el 14 de julio de 2016 de, <http://isyskernel.blogspot.mx/2014/01/instalar-configurar>

SNMPv2. Recuperado el 03 de julio de 2016, de <http://www4.ujaen.es/~mdmolina/grr/Tema%203.pdf>

Tanenbaum, A. (2003). *Redes de computadoras*. Mexico. Editorial McGraw-Hill.



ZABBIX manual. Recuperado el 27 de julio de 2016 de, <http://www.ZABBIX.com>

EMEISA. Recuperado el 25 de julio de 2016, de <http://www.emeisa.com.mx/cargadoresrecti.php>.

Red de Área Extensa (WAN). Recuperada el 14 de julio de 2016, de <http://profecarolinaquinodoz.com/principal/wpcontent/uploads/2009/04/wan1.gif>