



ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

CARRERA DE SISTEMAS E INFORMÁTICA

TEMA: ELABORAR EL MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE MONITOREO Y GESTIÓN WHATSUP GOLD.

PROYECTO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN COMPUTACIÓN

**ELABORADO POR:
USCA PATIÑO DANIEL ERNESTO
LEMA MONTALUISA SEGUNDO SERGIO**

**DIRECTOR:
ING. SANTIAGO JÁCOME**

**CODIRECTOR:
ING. CÉSAR NARANJO**

LATACUNGA, AGOSTO DEL 2009

ESCUELA POLITÉCNICA DEL EJÉRCITO

SEDE LATACUNGA

CARRERA DE SISTEMAS E INFORMÁTICA

CERTIFICADO

Los suscritos Ing. Santiago Jácome e Ing. César Naranjo certifican que el presente trabajo titulado: **“ELABORAR EL MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE MONITOREO Y GESTIÓN WHATSUP GOLD”** Fue desarrollado íntegramente por los señores: Usca Patiño Daniel Ernesto y Lema Montaluisa Segundo Sergio, bajo nuestra supervisión.

Ing. Santiago Jácome
DIRECTOR DE TESIS

Ing. César Naranjo
CODIRECTOR DE TESIS

AGRADECIMIENTO

Son muchas las personas que debería nombrar en estas líneas, pero me quedaré con las más trascendentales... con aquellas que no han bajado la guardia y siempre me han apoyado, tanto a lo largo del desarrollo de esta Tesis como a lo largo de mi vida.

Primero y antes que nada, dar gracias a **Dios**, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Al Ing. Santiago Jácome por asesorarme a lo largo de la tesis y acompañarme en este camino que hoy culmina en el presente proyecto, por compartir su conocimiento conmigo e inspirar en mi mucha admiración.

Al Ing. César Naranjo por ayudarme a lo largo de la tesis desinteresadamente y brindarme su amistad.

A mis padres y hermanos por ser los mejores y estar conmigo incondicionalmente, gracias porque sin ellos y sus enseñanzas no estaría aquí ni sería quien soy ahora, a ellos les dedico esta tesis.

No puedo dejar de nombrar a la mujer que alegro mi vida al darme mis dos amados hijos Brian y Brithany, y que ha sido un pilar fundamental en esta etapa de mi carrera. Gracias Kathy por ser mi compañera, mi amiga, mi confidente....

Gracias por aguantar las noches de desvelo y trabajo, en donde siempre me acompañaste. Gracias por el apoyo constante y los consejos que siempre tuviste en los momentos difíciles. Gracias mi querida esposa. Por estar conmigo... Tú abriste mi alma y dejaste salir lo mejor de mí.

Mi más amplio agradecimiento a la Fuerza Terrestre, la cual después de abrigarme en sus filas me brindo la oportunidad de superarme profesional y académicamente.

Finalmente quiero expresar un fraternal agradecimiento a la Escuela Superior Politécnica Del Ejército en especial a la carrera de Sistemas e Informática y a sus docentes, por sus conocimientos brindados a lo largo de nuestra vida estudiantil.

A todos mi mayor reconocimiento y gratitud.

AGRADECIMIENTO

Mi profundo agradecimiento a mi Dios todo poderoso por darme la vida, cuidarme y ayudarme a culminar mis estudios superiores con éxito.

A mí querida esposa por su confianza incondicional su cariño, comprensión, apoyo constante estímulo brindada no solamente durante todo mi periodo de estudio sino durante ya más de cinco años de vidas compartidas.

A mi hija querida que diariamente me daba este aliento que yo necesitaba por su paciencia y por enseñarme a enfrentar los obstáculos con alegría y sencillez.

A mis padres y hermanos por brindarme un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos.

A mi Director de Tesis, por su generosidad al brindarme la oportunidad de recurrir a su capacidad y experiencia científica en un marco de confianza, afecto y amistad, fundamentales para la concreción de este trabajo.

Quiero también dar un profundo agradecimiento a mi institución por abrirme las puertas y darme la oportunidad de seguir estudiando.

Un agradecimiento a la Escuela Politécnica del Ejército por hacer de mí un hombre útil a la patria.

DEDICATORIA

Durante estos escasos tres años de lucha constante, de gratas vivencias, de momentos de éxitos y también de angustias y desesperanza para poder cumplir mis objetivos y así poder alcanzar uno de mis mas grandes anhelos, culminar mi carrera, los deseos de superarme y de lograr mi meta eran tan grandes que logre vencer todos los obstáculos y es por ello que debo dedicar este triunfo a quienes en todo momento me llenaron de amor y apoyo, y por sobre todo me brindaron su amistad:

A Dios Todopoderoso por iluminarme el camino a seguir y que siempre está conmigo en los buenos y sobre todo en los malos momentos.

A mi esposa e hijos con los cuales he compartido tantos momentos de mi vida, por darme aliento para continuar luchando en esta vida que a veces parece terrible, sin su apoyo y compañía estos tres años no hubiesen sido lo mismo ustedes hacen que mi vida sea siempre hermosa. Este triunfo lo comparto con ustedes.

A mis Padres: Daniel y Margarita, pilares fundamentales en mi vida, dignos de ejemplo de trabajo y constancia, quienes han brindado todo el apoyo necesario para alcanzar mis metas y sueños, y han estado allí cada día de mi vida, compartiendo los buenos y los malos ratos desde el día en que nací....Los quiero mucho y gracias.

Especialmente a mi persona, pues fue una meta que me trace y con la que siempre soñé y ahora es una realidad.

Daniel

DEDICATORIA

Esta tesis la dedico con todo mi amor y cariño A ti dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

Con mucho cariño principalmente a mis padres que gracias a sus consejos y palabras de aliento crecí como persona ya que me dieron la vida y supieron confiar en mí.

También a mi querida esposa e hija que son el motor fundamental para este logro porque siempre han estado conmigo en todo momento apoyándome y brindándome todo su amor. A mis maestros por compartir generosamente sus conocimientos.

Al personal Directivo y Administrativo de la facultad por brindarme todas las facilidades a lo largo de estos años de formación académica; y a mis compañeros de estudio, por brindarme su amistad y apoyo moral.

Sergio

CONTENIDO

CAPÍTULO I: MARCO TEÓRICO	- 1 -
1.1.- CONCEPTOS QUE SE MANEJA EN LA GESTIÓN DE RED DE DATOS	- 1 -
1.1.1.- PAQUETE DE DATOS	- 1 -
1.1.1.1.- Dirección fuente o “Source” y dirección destino o “destination”	- 2 -
1.1.1.2.- Tamaño de los paquetes.....	- 3 -
1.1.2.- PROTOCOLO DE LOS PAQUETES	- 3 -
1.1.2.1.- Protocolo TCP/IP.....	- 4 -
1.1.2.2.- Protocolo UDP.....	- 4 -
1.1.2.3.- Protocolo ARP	- 5 -
1.1.2.4.- Protocolo FTP	- 6 -
1.1.2.5.- Protocolo DNS.....	- 7 -
1.1.2.6.- Protocolo IGMP.....	- 7 -
1.1.2.7.- Protocolo ICMP	- 7 -
1.1.2.8.- Protocolo SNMP.....	- 9 -
1.1.2.9.- Protocolo SMTP	- 10 -
1.2.- PARÁMETROS QUE DEFINEN UNA RED.....	- 11 -
1.2.1.- ÁREA DE DISEÑO	- 11 -
1.2.1.1.- Topologías de redes.....	- 12 -
1.2.1.2.- Topología en estrella	- 12 -
1.2.1.3.- Topología en estrella extendida.....	- 13 -
1.2.1.4.- Topología en bus	- 14 -
1.2.1.5.- Topología en anillo.....	- 15 -
1.2.1.6.- Topología en árbol.....	- 16 -
1.2.1.7.- Topología de malla completa	- 17 -
1.2.2.- ÁREA FÍSICA	- 18 -
1.2.2.1.- Servidor	- 19 -
1.2.2.2.- Estación de Trabajo	- 19 -
1.2.2.3.- Hub	- 20 -
1.2.2.4.- Switch	- 20 -
1.2.2.5.- Router	- 21 -
1.2.2.6.- Sistema Operativo	- 21 -
1.2.3.- ÁREA DE INTERCONECTIVIDAD.....	- 22 -
1.2.4.- ÁREA DE SEGURIDAD	- 23 -
1.3.- MONITOREO DE REDES DE COMPUTADORAS	- 25 -
1.3.1.- LA NUEVA REALIDAD DE LA GESTION DE RED.....	- 27 -
1.3.2.- MEJOR CONOCIMIENTO CONDUCE A UN MEJOR RENDIMIENTO DE LA RED	- 28 -
1.4.- IMPORTANCIA DEL PROYECTO PARA LA RED DE DATOS DEL EJÉRCITO	- 28 -
1.5.- DESARROLLO	- 30 -
CAPÍTULO II: ANÁLISIS DEL SISTEMA	- 31 -
2.1.- IPSWITCH.....	- 31 -
2.2.- DEFINICIÓN DE WHATSUP GOLD.....	- 32 -
2.3.- FUNCIONES DE WHATSUP GOLD	- 33 -
2.3.1.- IDENTIFICACIÓN Y MAPEO DINÁMICO DE LA RED.....	- 33 -
2.3.2.- RÁPIDA RESOLUCIÓN DE PROBLEMAS	- 33 -

2.3.3.-	PROFUNDO MONITOREO DE SNMP Y WMI	- 34 -
2.3.4.-	MONITOREO DE RENDIMIENTO Y REPORTES	- 34 -
2.3.5.-	INFORMES COMPLETOS	- 35 -
2.4.-	PROPIEDADES DE WHATSUP GOLD	- 35 -
2.4.1.-	CARTOGRAFIA DE LA RED	- 35 -
2.4.1.1.-	Métodos de exploración con WhatsUp Gold	- 35 -
2.4.2.-	CONTROL DE LA RED	- 36 -
2.4.3.-	OBTENER INFORMACIÓN DEL MAPA DE RED	- 37 -
2.4.4.-	OBTENER LA CONDICIÓN DE UN DISPOSITIVO	- 38 -
2.4.5.-	PRESENTACIÓN DE INFORMES	- 39 -
2.4.5.1.-	Gráficos de rendimiento	- 39 -
2.4.5.2.-	Informes de eventos	- 39 -
2.4.5.3.-	Informes de estadísticas	- 39 -
2.5.-	CAPACIDADES DE WHATSUP GOLD	- 40 -
2.6.-	BENEFICIOS DE WHATSUP GOLD	- 40 -
2.6.1.-	LIVIANA ACCIONABLE Y CENTRALIZADA	- 40 -
2.6.2.-	LISTA PARA EL NOC	- 41 -
2.6.3.-	LA ARQUITECTURA WHATSUP GOLD COMPROBADA	- 41 -
2.6.4.-	EXTENSIBILIDAD	- 41 -
2.6.5.-	DISPONIBILIDAD	- 42 -
2.7.-	REQUISITOS DEL SISTEMA	- 42 -
2.7.1.-	OTROS REQUISITOS	- 42 -
2.7.1.1.-	Espacio libre	- 43 -
2.7.1.2.-	Uso del programa de desinstalación	- 43 -

CAPÍTULO III: WHATSUP GOLD Y SU UTILIZACIÓN COMO SISTEMA DE MONITOREO

3.1.-	CREACIÓN DE UN MAPA DE RED	- 44 -
3.1.1.-	DESCUBRIR Y MAPEAR DISPOSITIVOS DE RED	- 49 -
3.1.2.-	USO DE SNMP SMARTSCAM	- 51 -
3.1.2.1.-	Resultados de SmartScan	- 54 -
3.1.3.-	CARTOGRAFÍA DE UNA RED PLANA	- 55 -
3.1.3.1.-	Resultados de la Exploración	- 57 -
3.1.4.-	DESCUBRIR DISPOSITIVOS DE ENTORNO DE RED	- 57 -
3.2.-	PROPIEDADES GENERALES DE UN DISPOSITIVO	- 58 -
3.2.1.-	CONFIGURACIÓN DE VIGILANCIA	- 62 -
3.2.2.-	USO DEL MENÚ EN EL BOTON DERECHO DEL RATON	- 65 -
3.3.-	CREACIÓN DE UNA SUBRED	- 66 -
3.4.-	CONFIGURACIÓN DE PROPIEDADES DEL MAPA	- 68 -
3.4.1.-	AJUSTE DE MAPA DE COLORES	- 69 -
3.4.1.1.-	Estado de los dispositivos	- 70 -
3.5.-	EDICIÓN DE UN MAPA DE RED	- 72 -
3.5.1.-	COMO ENTRAR Y SALIR DEL MODO DE EDICIÓN	- 72 -
3.5.1.1.-	Líneas Adjunto	- 73 -
3.5.1.2.-	Creación de títulos de texto	- 74 -
3.6.-	CONFIGURACIÓN DE NOTIFICACIONES	- 74 -
3.6.1.-	DEFINIENDO EL SONIDO DE NOTIFICACIÓN	- 74 -
3.6.2.-	DEFINIENDO LA NOTIFICACIÓN WINPOPUP	- 76 -
3.7.-	SERVICIOS DE VIGILANCIA	- 78 -

3.8.-	TRABAJO DE LA CONSOLA	- 78 -
3.8.1.-	INICIAR AUTOMATING POLLING	- 78 -
3.8.2.-	PARAR AUTOMATING POLLING	- 79 -
3.8.3.-	LECTURA DEL MAPA DE RED.....	- 79 -
3.8.4.-	RECEPCIÓN DE ALARMAS.....	- 80 -
3.8.5.-	UTILIZANDO QUICK ESTADO	- 81 -
3.8.6.-	USO DE LA VENTANA DE ESTADO.....	- 82 -
3.9.-	REGISTROS Y REPORTES.....	- 83 -
3.9.1.-	CREACIÓN DE UN INFORME DE EVENTO.....	- 84 -
3.9.1.1.-	Depuración de los registros de información	- 86 -
3.9.2.-	CREACIÓN DE UN INFORME DE ESTADISTICAS	- 87 -
3.9.2.1.-	Exportación de datos en bruto	- 90 -
CAPÍTULO IV: RESULTADOS DEL SISTEMA		- 91 -
4.1.-	RESULTADOS DE LA INTERACCIÓN DEL USUARIO CON EL SISTEMA.....	- 91 -
4.2.-	CARACTERÍSTICAS EN MATERIA DE SEGURIDAD A TOMAR EN CUENTA	- 91 -
4.3.-	RED UTILIZADA PARA EL USO DE LA APLICACIÓN	- 92 -
4.3.1.-	PRUEBAS DE USO	- 93 -
4.3.1.1.-	Dependencias que existen en la red monitoreada.....	- 94 -
4.3.1.2.-	Estadísticas de la red monitoreada	- 94 -
4.3.1.3.-	Estado de la red monitoreada	- 95 -
4.3.1.4.-	Dispositivo caído	- 96 -
4.3.1.5.-	Respuestas de un dispositivo	- 97 -
4.3.1.6.-	Porcentaje de respuestas de un dispositivo.....	- 98 -
4.3.1.7.-	Reportes de la red	- 99 -
4.3.1.8.-	Exportación de Reportes de la red del ejército.....	- 101 -
4.4.-	ESCALABILIDAD	- 102 -
4.5.-	MANUAL DE USUARIO DEL SISTEMA DE GESTIÓN Y MONITOREO WHATSUP GOLD	- 102 -
4.5.1.-	PASOS PARA LA INSTALACIÓN	- 102 -
4.5.2.-	CONFIGURACIÓN SNMP EN WINDOWS SERVER	- 109 -
4.5.2.1.-	Agregar SNMP como un servicio de Windows	- 109 -
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES		- 118 -
5.1.-	CONCLUSIONES	- 118 -
5.2.-	RECOMENDACIONES.....	- 118 -

TABLA DE ILUSTRACIONES

Figura 1-1. Trama de datos simple	- 2 -
Figura 1-2. Campos del datagrama.....	- 5 -
Figura 1-3. Transferencia de datos por FTP	- 6 -
Figura 1-4. Encapsulación del protocolo ICMP	- 8 -
Figura 1-5. Protocolo SNMP	- 9 -
Figura 1-6. Protocolo SMTP.....	- 11 -
Figura 1-7. Topología en estrella.	- 13 -
Figura 1-8. Topología en estrella extendida.....	- 14 -
Figura 1-9. Topología en bus.	- 15 -
Figura 1-10. Topología en anillo.	- 16 -
Figura 1-11. Topología en árbol.....	- 17 -
Figura 1-12. Topología en malla completa.....	- 18 -
Figura 1-13 Servidor.	- 19 -
Figura 1-14 Estación de trabajo.	- 20 -
Figura 1-15 Hub.	- 20 -
Figura 1-16 Switch.	- 21 -
Figura 1-17 Router.....	- 21 -
Figura 1-18 Sistemas operativos.....	- 22 -
Figura 1-19. Capas del modelo OSI.....	- 23 -
Figura 1-20. Área de seguridad.	- 24 -
Figura 2-1. Control de la red.	- 37 -
Figura 2-2. Información del mapa de red.	- 38 -
Figura 2-1. Información de estado de la red.	- 39 -
Figura 3-1. Típico mapa de red.....	- 44 -
Figura 3-2. Crear nuevo mapa de red	- 45 -
Figura 3-3. Opción crear mapa en blanco.....	- 45 -
Figura 3-4. Boton de modo de edición	- 46 -
Figura 3-5. Barra de herramientas en modo de edición	- 46 -
Figura 3-6. Propiedades de un dispositivo	- 47 -
Figura 3-7. Cuadro de dialogo general.....	- 47 -
Figura 3-8. Seleccionar supervisar este dispositivo	- 48 -
Figura 3-9. Seleccionar sonido de alerta.....	- 48 -
Figura 3-10. Descubra y trace los dispositivos de la red.....	- 49 -
Figura 3-11. Parámetros para descubrir dispositivos de una red.....	- 50 -
Figura 3-12. Descubre la red con SNMP SmartScan.....	- 52 -
Figura 3-13. SNMP SmartScan.....	- 52 -
Figura 3-14. Servicios que desee analizar con SNMP SmartScan	- 53 -
Figura 3-15. Inicio de la exploración de dispositivos	- 53 -
Figura 3-16. Dispositivos encontrados	- 54 -
Figura 3-16. Resultados de SmartScan	- 54 -
Figura 3-18. Descubre la red usando ICMP	- 55 -
Figura 3-19. Servicios que desee analizar utilizando ICMP	- 56 -
Figura 3-20. Rango de las direcciones a monitorear.....	- 56 -
Figura 3-21. Resultados de la exploración utilizando ICMP	- 57 -
Figura 3-22. Cuadro general de propiedades de un dispositivo	- 59 -

Figura 3-23. Nombre del dispositivo.....	- 59 -
Figura 3-24. Tipo de dispositivo	- 60 -
Figura 3-25. Método de búsqueda para un dispositivo	- 60 -
Figura 3-25. Introducción de la dirección IP	- 61 -
Figura 3-26. Agregar información de un dispositivo	- 62 -
Figura 3-27. Configuración de vigilancia	- 63 -
Figura 3-27. Tiempo de respuesta para un dispositivo monitoreado	- 64 -
Figura 3-28. Establecer horarios de monitoreo para cada dispositivo.....	- 64 -
Figura 3-29. Menú del botón derecho del ratón	- 65 -
Figura 3-30. Icono subred.....	- 67 -
Figura 3-31. Configuración de propiedades del mapa	- 68 -
Figura 3-32. Mapa de colores	- 70 -
Figura 3-33. Estado de los dispositivos.....	- 71 -
Figura 3-34. Botón para modo de edición	- 72 -
Figura 3-35. Líneas de adjunto	- 73 -
Figura 3-36. Botón de texto.....	- 74 -
Figura 3-37. Definiendo el sonido de notificación	- 75 -
Figura 3-38. Alarmas WAV	- 76 -
Figura 3-39. Reproducción de alarmas WAV.....	- 76 -
Figura 3-40. Definiendo notificación WinPopup	- 77 -
Figura 3-40. Agregar nombre a la notificación	- 77 -
Figura 3-41. Botón para monitoreo automático.....	- 79 -
Figura 3-42. Botón para silenciar una alarma	- 80 -
Figura 3-43. Ventana de estado de un dispositivo	- 81 -
Figura 3-44. Selección para ver estado de un dispositivo.....	- 82 -
Figura 3-45. Ventana de dispositivos activos utilizando colores	- 83 -
Figura 3-46. Configuración de reporte de eventos.....	- 84 -
Figura 3-47. Configuración de reporte de eventos.....	- 85 -
Figura 3-48. Reporte de eventos.....	- 86 -
Figura 3-49. Configuración reporte de estadísticas	- 87 -
Figura 3-50. Ruta de informe	- 88 -
Figura 3-51. Tipo de informe.....	- 88 -
Figura 3-52. Informe generado por WhatsUp Gold	- 89 -
Figura 3-53. Exportar un informe a otro formato	- 90 -
Figura 3-54. Datos exportados a Excel.....	- 90 -
Figura 4-1. Red de Datos del Ejército	- 93 -
Figura 4-2. Dependencias de la red de Datos del Ejército	- 94 -
Figura 4-3. Estadísticas de la red de Datos del Ejército.....	- 95 -
Figura 4-4. Estado de la red de Datos del Ejército.....	- 96 -
Figura 4-5. Propiedades dependencia caída	- 97 -
Figura 4-6. Respuestas de un dispositivo	- 98 -
Figura 4-7. Porcentaje de respuestas de un dispositivo.....	- 99 -
Figura 4-8. Reporte de Windows.....	- 100 -
Figura 4-7. Reporte de texto	- 100 -
Figura 4-10. Reporte exportado a Excel	- 101 -
Figura 4-11. Reporte exportado a PDF	- 101 -
Figura 4-12. Instalación WhatsUp Gold Paso 1	- 103 -
Figura 4-13. Instalación WhatsUp Gold Paso 2	- 103 -

Figura 4-14. Instalación WhatsUp Gold Paso 3	- 104 -
Figura 4-15. Instalación WhatsUp Gold Paso 4	- 104 -
Figura 4-16. Instalación WhatsUp Gold Paso 5	- 105 -
Figura 4-17. Instalación WhatsUp Gold Paso 6	- 106 -
Figura 4-18. Instalación WhatsUp Gold Paso 7	- 106 -
Figura 4-19. Instalación WhatsUp Gold Paso 8	- 107 -
Figura 4-20. Instalación WhatsUp Gold Paso 9	- 107 -
Figura 4-21. Instalación WhatsUp Gold Paso 10	- 108 -
Figura 4-22. Instalación WhatsUp Gold Paso 11	- 108 -
Figura 4-23. Configuración SNMP Paso 1	- 109 -
Figura 4-24. Configuración SNMP Paso 2	- 110 -
Figura 4-25. Configuración SNMP Paso 3	- 110 -
Figura 4-26. Configuración SNMP Paso 4	- 111 -
Figura 4-27. Configuración SNMP Paso 5	- 111 -
Figura 4-28. Configuración SNMP Paso 6	- 112 -
Figura 4-29. Configuración SNMP Paso 7	- 112 -
Figura 4-30. Configuración SNMP Paso 8	- 113 -
Figura 4-31. Configuración SNMP Paso 9	- 113 -
Figura 4-32. Configuración SNMP Paso 10	- 114 -
Figura 4-33. Configuración SNMP Paso 11	- 115 -
Figura 4-34. Configuración SNMP Paso 12	- 115 -
Figura 4-35. Configuración SNMP Paso 13	- 116 -
Figura 4-36. Configuración SNMP Paso 14	- 116 -
Figura 4-37. Configuración SNMP Paso 15	- 117 -

CAPÍTULO I

MARCO TEÓRICO

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de la operación es cada vez más demandante. Las redes, soportan aplicaciones y servicios estratégicos de las organizaciones. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez mas importante y de carácter pro-activo para evitar problemas.

En este capítulo, revisaremos fundamentos teóricos que se manejan en la gestión de redes de datos y que serán utilizados a lo largo del estudio del monitoreo de redes como, funcionalidad y características que ayudaran a fortalecer nuestros conocimientos.

1.1.- CONCEPTOS QUE SE MANEJA EN LA GESTIÓN DE RED DE DATOS

Para conocer lo que está pasando realmente en una red LAN/WAN, el usuario o administrador debe tener pleno conocimiento de los términos que se manejan en el área de redes, al momento de presentarle algún reporte o un conjunto de datos.

Por lo tanto a continuación se muestran los datos que el administrador podrá observar al momento de realizar el análisis pertinente.

1.1.1.- PAQUETE DE DATOS

Los paquetes de datos son “un conjunto de mensajes de tamaño predefinido, donde cada fracción contiene la información tanto de procedencia como de destino e información requerida para el re-ensamblaje del mensaje”.

A continuación se muestra una gráfica de la composición de un paquete datos



Figura 1-1. Trama de datos simple

En ella se observa que las partes principales del paquete son el identificador o dirección destino, el identificador o dirección origen, el control de trama el cual “indica si en el paquete enviado o recibido hay datos o solo información para fines de control”.

A continuación siguen los datos enviados y por último se encuentra el CRC el cual “es un campo para la detección de errores tanto en los paquetes enviados como en los recibidos”, se recuerda que todos estos paquetes son representados por bits.

Para el caso que se está analizando en los reportes generados por el Sistema de Monitoreo de Redes WhatsUp Gold se tienen las siguientes características que se nos muestran como parte del paquete rastreado.

1.1.1.1.- Dirección fuente o “Source” y dirección destino o “destination”

En estos campos se muestran las direcciones IP (Internet Protocol), las cuales están conformadas por cuatro octetos de bits, estas direcciones son del tipo denominado IP.v4 y en las cuales tanto se manda un paquete hacia otro equipo en la misma subred (dirección fuente) y se recibe un paquete de otro equipo en la misma subred (dirección destino).

Por ejemplo: se manda un paquete desde la dirección 140.148.26.86 que es una dirección clase B (dirección fuente) a la dirección 140.148.63.92 que también es

una dirección clase B (dirección destino), se observa que las dos direcciones pertenecen a la misma subred (con máscara 255.255.0.0).

El tipo de error que se puede tener en este campo es que la computadora mande o reciba un paquete que no le corresponde, o en todo caso, puede ser generado por el error del router al que se encuentran conectados ya que es el que decide el direccionamiento de los paquetes que pasan a través de él, en resumen, el posible error en este caso es la configuración del router.

1.1.1.2.- Tamaño de los paquetes

En este campo se analiza el tamaño de cada uno de los paquetes que se mandan en nuestra red LAN, entre los valores que se pueden detectar con respecto al tamaño de los paquetes, están los siguientes rangos.

- Paquetes de menos de 64 bytes.
- Paquetes entre 65 y 127 bytes.
- Paquetes entre 128 y 255 bytes.
- Paquetes entre 256 y 511 bytes.
- Paquetes entre 512 y 1023 bytes.
- Paquetes entre 1024 y 1517 bytes.
- Paquetes mayores de 1518 bytes.

1.1.2.- PROTOCOLO DE LOS PAQUETES

En este campo se muestra el tipo de protocolos de cada uno de los paquetes. Un protocolo “es un método para intercambiar información entre computadoras y que se encuentran regidos por un conjunto de reglas”.

Esto permite que dos computadoras que tengan un sistema operativo o protocolo de comunicación distinto puedan transmitir datos entre ellos. Los protocolos de mayor importancia que WhatsUp Gold detecta en la comunicación entre una dirección fuente y una dirección destino son los siguientes:

1.1.2.1.- Protocolo TCP/IP

Se considera el protocolo más importante en Internet en donde se juntan los protocolos Transfer Control Protocol (TCP) e Internet Protocol (IP), la función principal de este protocolo es un procedimiento de comunicación general que garantiza la transmisión de datos entre los equipos.

El error más común que se puede encontrar en este protocolo, es realizar la comunicación en el envío de paquetes y recibir una negativa de que no pudo completarse la transferencia de datos al equipo emisor, para que nuevamente se realice la comunicación; en caso de que no exista ninguna comunicación, debe revisarse el equipo el cual cuenta con este protocolo para saber si se encuentra bien configurado.

1.1.2.2.- Protocolo UDP

Las siglas UDP quieren decir User Datagram Protocol y se considera como un protocolo no orientado a la conexión y en lugar de entregar paquetes entrega datagramas, en donde la diferencia entre estos dos es que en el paquete hay un control de flujo de errores y en el datagrama no.

Aunque en el datagrama sí se llegan a utilizar funciones de detección de errores, por lo tanto “no proporciona ningún tipo de control de errores ni de flujo, aunque sí que utiliza mecanismos de detección de errores”. Cuando se detecta un error en un datagrama en lugar de entregarlo a la aplicación se descarta y no se toma en cuenta.

Las características principales de este protocolo es que no garantiza la fiabilidad al momento de entregar información y entrega la información desordenada y sin ninguna secuencia y por lo tanto es un protocolo más propenso a errores al momento de la transferencia de datos, ya que no se tiene ninguna respuesta de si se recibió la información correctamente.

A continuación en la figura, se muestra la composición de un datagrama.

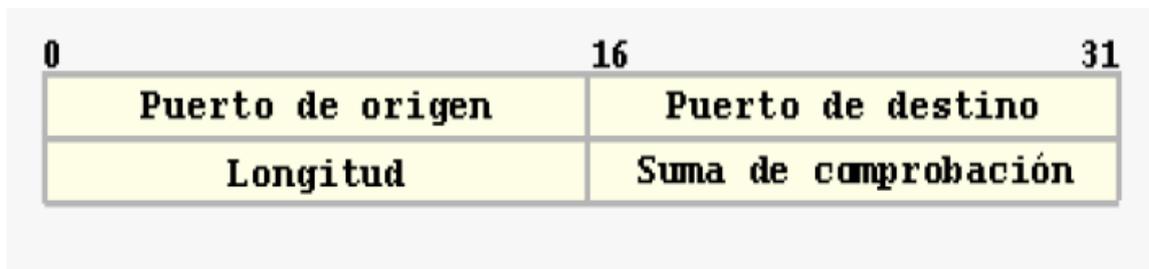


Figura 1-2. Campos del datagrama.

1.1.2.3.- Protocolo ARP

El protocolo ARP se denomina como Address Resolution Protocol y se encarga de utilizar un mecanismo de resolución dinámico el cual crea una tabla de equivalencias entre las direcciones MAC (Media Access Control) o sea la dirección física de la computadora y las direcciones IP (Internet Protocol) que son las direcciones lógicas de la computadora.

El ejemplo más común a este protocolo es cuando una máquina necesita la dirección MAC de otra máquina a partir de una dirección IP, entonces la máquina manda lo que se llama un Broadcast ARP Request, que consiste en mandar la dirección IP a todos los equipos con los que se puede comunicar y la computadora que tenga esa dirección IP responderá con ARP Reply el cual contiene su dirección MAC.

El error más común en este protocolo es que exista duplicidad de direcciones IP, no puede existir duplicidad en direcciones MAC ya que es única, pero en las direcciones IP, puede existir la posibilidad que dos máquinas compartan la misma dirección IP y por lo tanto existir un error en la comunicación, con otros equipos en la red.

Esto propicia que los equipos pueden mandar información a cualquiera de las dos direcciones lo cual en su momento, puede interpretarse como inconsistencia y pérdida en el envío y recepción de datos.

1.1.2.4.- Protocolo FTP

El protocolo de transferencia de hipertexto (Hypertext Transfer Protocol) en donde el hipertexto es toda la información y contenido que se maneja en las páginas Web y es el más usado. El funcionamiento de este protocolo consiste en que “se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla, es decir, se basa en sencillas operaciones de solicitud/respuesta”.

Se basa en el modelo cliente-servidor y que articula los intercambios de información que existen entre los clientes Web y los servidores HTTP. Cabe mencionar además, que este protocolo se encuentra soportado sobre los servicios de conexión del protocolo TCP/IP.

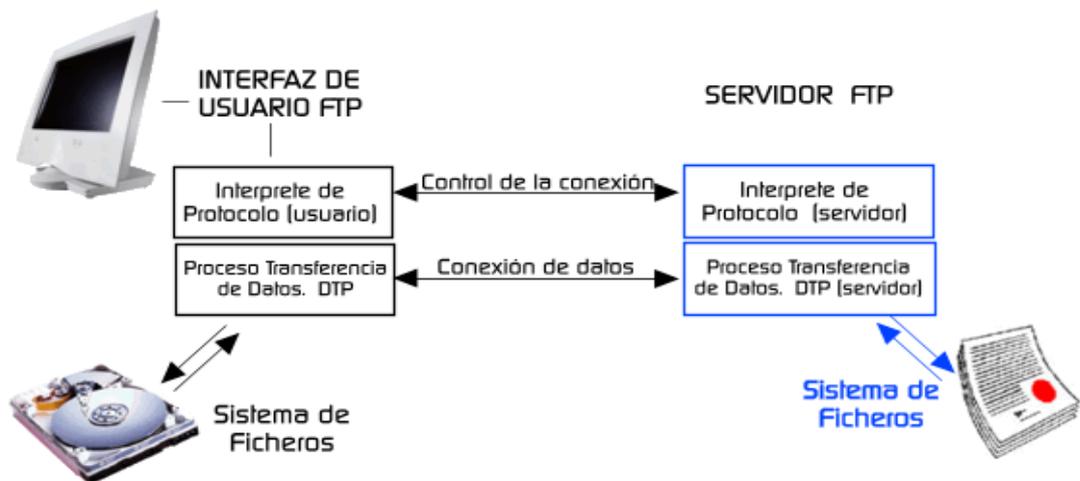


Figura 1-3. Transferencia de datos por FTP

1.1.2.5.- Protocolo DNS

Aunque no es un protocolo en sí, tiene su propia especificación en un paquete de datos, DNS que quiere decir “Domain Name Server” está basado en la estructura cliente-servidor el cual basa su mayor actividad en el servidor o bien llamado “revolvedor”, la función principal del servidor es proporcionar la información sobre la relación dirección IP-dominio, este protocolo se basa principalmente en un sistema jerárquico de dominios y sub-dominios.

Esto quiere decir que una vez “que se haya configurado el servidor para usar los servidores DNS raíz se puede utilizar recursivamente con otros servidores del mismo tipo y así llegar a conocer cualquier dominio asociado a cualquier dirección IP”.

Este protocolo es muy útil ya que el usuario no memoriza las páginas mediante una dirección IP sino mediante un dominio que está conformado por un nombre único en la red.

1.1.2.6.- Protocolo IGMP

El protocolo IGMP (Internet Group Management Protocol), “es usado para la suscripción o anulación de suscripción de/desde grupos de multidifusión”. Este protocolo solo se puede llegar a utilizar en redes que requieran de tecnologías de multidifusión (transmisión de archivos de video y audio).

1.1.2.7.- Protocolo ICMP

Es considerado a nivel IP, ya que es empleado por éste para notificar mensajes de error o situaciones que requieren cierta atención. Debido a que la información ICMP viaja en paquetes IP es considerado a veces un nivel por encima. Existen numerosos tipos de mensajes que permiten tanto notificar situaciones de error, como realizar peticiones de información. Asimismo, un mensaje ICMP siempre contiene los 8 primeros bytes del paquete IP que dio lugar a su generación, así, el

sistema receptor al extraerlo de la red sabrá a qué módulo asociárselo: TCP o UDP.

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (Internet Control Message Protocol, protocolo de mensajes de control de error), se encarga de informar al origen si se ha producido algún error durante la entrega de un mensaje. Pero no solo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa las incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP, como se puede apreciar en el siguiente esquema.

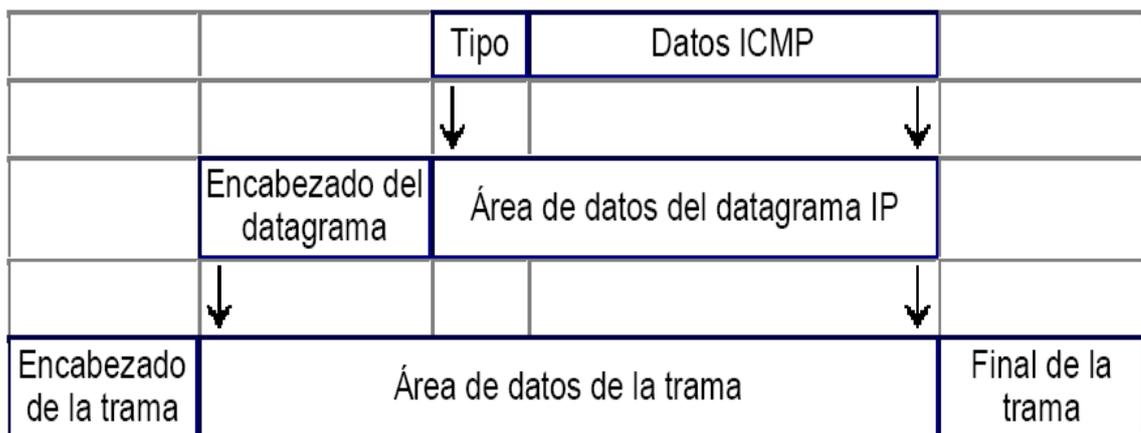


Figura 1-4. Encapsulación del protocolo ICMP

Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se crea un nuevo mensaje ICMP sino que el primero se descartara sin más.

1.1.2.8.- Protocolo SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

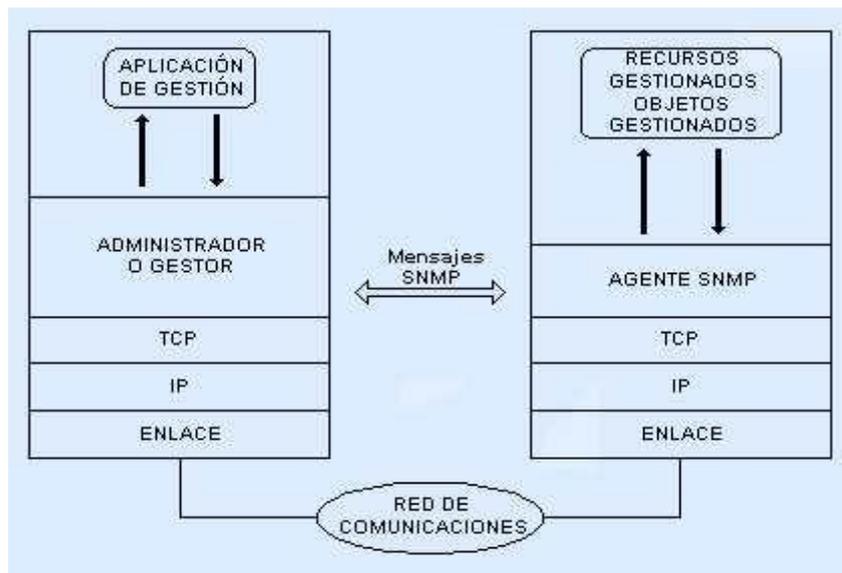


Figura 1-5. Protocolo SNMP.

El objetivo del sistema operativo es gestionar y administrar eficientemente los recursos hardware de la computadora, permitiendo ejecutar concurrentemente varios programas sin que haya conflictos en el acceso de cada uno de ellos a cada uno de los recursos que necesita y sin que ningún programa monopolice un recurso determinado, se subdivide en dos:

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados
- Agentes
- Sistemas administradores de red (NMS's)

Un dispositivo administrado es un nodo de red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's usando SNMP. Los dispositivos administrados, a veces llamados elementos de red, pueden ser routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías.

Un NMS ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

1.1.2.9.- Protocolo SMTP

El protocolo SMTP (Protocolo simple de transferencia de correo) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

Éste es un protocolo que funciona en línea, encapsulado en una trama TCP/IP. El correo se envía directamente al servidor de correo del destinatario. El protocolo SMTP funciona con comandos de textos enviados al servidor SMTP (al puerto 25 de manera predeterminada). A cada comando enviado por el cliente (validado por la cadena de caracteres ASCII CR/LF, que equivale a presionar la tecla Enter) le sigue una respuesta del servidor SMTP compuesta por un número y un mensaje descriptivo.

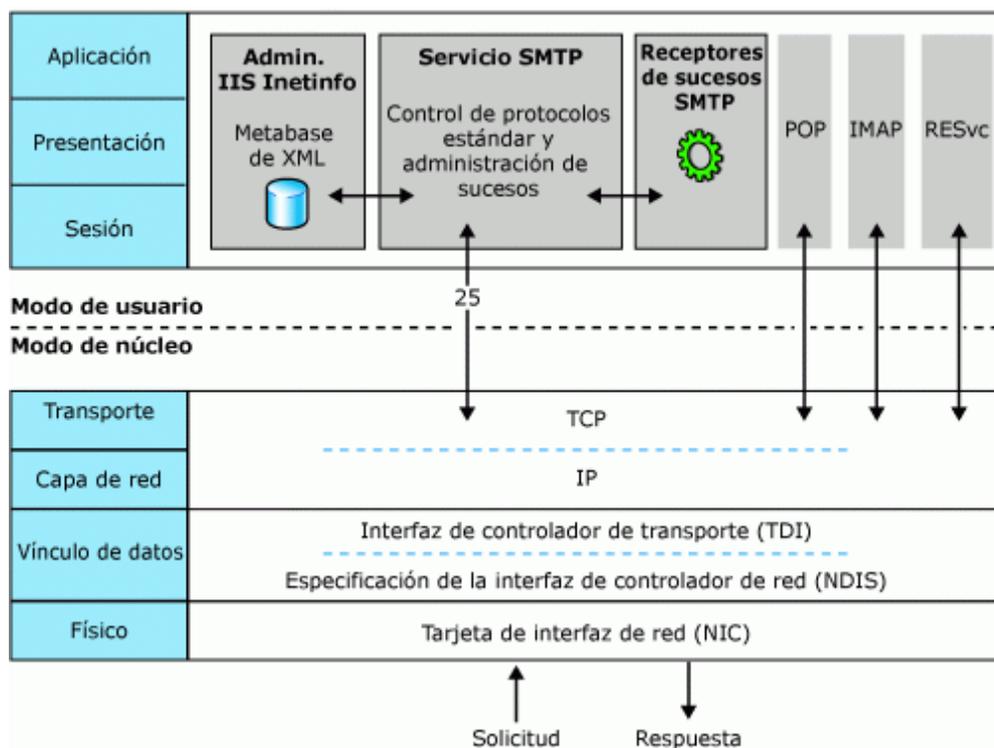


Figura 1-6. Protocolo SMTP.

1.2.- PARÁMETROS QUE DEFINEN UNA RED

Los parámetros que definen a una red de computadoras (LAN/WAN), se pueden describir en cuatro áreas principales, que se complementan unas con otras:

- Área de diseño.
- Área física.
- Área de Interconectividad.
- Área de seguridad.

1.2.1.- ÁREA DE DISEÑO

En el área de diseño así como en las demás se debe tener un especial cuidado, ya que en el diseño se encuentra depositada la posibilidad de expandir y hacer mucho más rentable nuestra RED, si no hay un buen diseño, el administrador se

encontrará en serias dificultades para encontrar las posibles fallas que puedan aquejar a nuestro sistema.

Un ejemplo que es crucial en el diseño, son las topologías de red, las cuales nos van a indicar la colocación de nuestro equipo para que no existan futuros problemas, de aquí se pasa a otra área importante que es la física.

1.2.1.1.- Topologías de redes

Entre las topologías más importantes se tienen: la topología de bus, topología de anillo, topología de árbol o jerárquica y topología de estrella (estrella sencilla, estrella extendida). Las redes de computadoras surgieron como una necesidad de interconectar los diferentes host de una empresa o institución para poder así compartir recursos y equipos específicos. Pero los diferentes componentes que van a formar una red se pueden interconectar o unir de diferentes formas, siendo la forma elegida un factor fundamental que va a determinar el rendimiento y la funcionalidad de la red.

La disposición de los diferentes componentes de una red se conoce con el nombre de topología de la red. La topología idónea para una red concreta va a depender de diferentes factores, como el número de máquinas a interconectar, el tipo de acceso al medio físico que se desea.

1.2.1.2.- Topología en estrella

En este esquema todas las estaciones están conectadas a un concentrador o HUB con cable por computadora. Para futuras ampliaciones pueden colocarse otros hubs en cascada dando lugar a la estrella jerárquica.

Por ejemplo en la estructura CLIENTE-SERVIDOR: el servidor está conectado al HUB activo, de este a los pasivos y finalmente a las estaciones de trabajo.

Ventajas:

- La ausencia de colisiones en la transmisión y dialogo directo de cada estación con el servidor.
- La caída de una estación no anula la red.

Desventajas:

- Baja transmisión de datos.

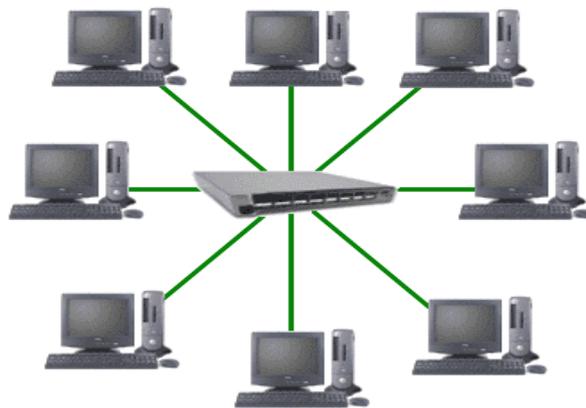


Figura 1-7. Topología en estrella.

1.2.1.3.- Topología en estrella extendida

La topología en estrella extendida es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. Generalmente el nodo central está ocupado por un hub o un switch, y los nodos secundarios por hubs.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central. La topología en estrella extendida es sumamente jerárquica, y busca que la información se

mantenga local. Esta es la forma de conexión utilizada actualmente por el sistema telefónico

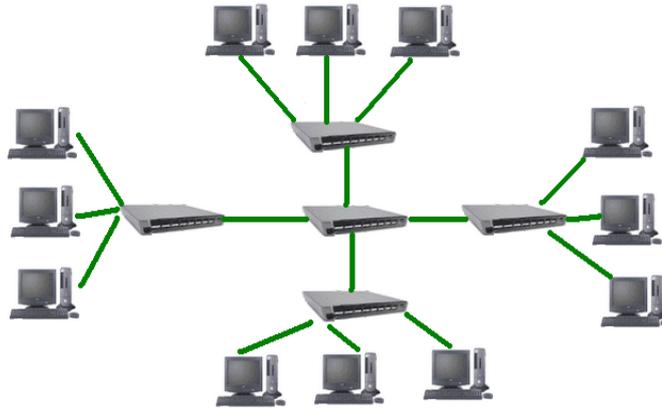


Figura 1-8. Topología en estrella extendida.

1.2.1.4.- Topología en bus

Consiste en un solo cable al cual se le conectan todas las estaciones de trabajo. En este sistema una sola computadora a la vez puede mandar datos los cuales son escuchados por todas las computadoras que integran el bus, pero solo el receptor designado los utiliza.

Ventajas:

- Es la más barata. Apta para oficinas medianas y chicas.

Desventajas:

- Si se tienen demasiadas computadoras conectadas a la vez, la eficiencia baja notablemente.
- Es posible que dos computadoras intenten transmitir al mismo tiempo provocando lo que se denomina “colisión”, y por lo tanto se produce un reintento de transmisión.

- Un corte en cualquier punto del cable interrumpe la red.

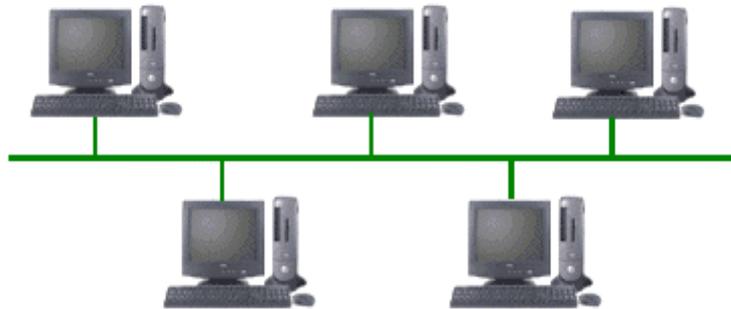


Figura 1-9. Topología en bus.

1.2.1.5.- Topología en anillo

Es un desarrollo de IBM que consiste en conectar cada estación con otra dos formando un anillo. Los servidores pueden estar en cualquier lugar del anillo y la información es pasada en un único sentido de una a otra estación hasta que alcanza su destino.

Cada estación que recibe el TOKEN regenera la señal y la transmite a la siguiente, por ejemplo en esta topología, esta envía una señal por toda la red.

Si la terminal quiere transmitir pide el TOKEN y hasta que lo tiene puede transmitir.

Si no está la señal la pasa a la siguiente en el anillo y sigue circulando hasta que alguna pide permiso para transmitir.

Ventajas:

- No existen colisiones, pues cada paquete tiene una cabecera o TOKEN que identifica al destino.

Desventajas:

- La caída de una estación interrumpe toda la red. Actualmente no hay conexiones físicas entre estaciones, sino que existen centrales de cableado o MAU que implementa la lógica de anillo sin que estén conectadas entre sí evitando las caídas.
- Es cara, llegando a costar una placa de red lo que una estación de trabajo.

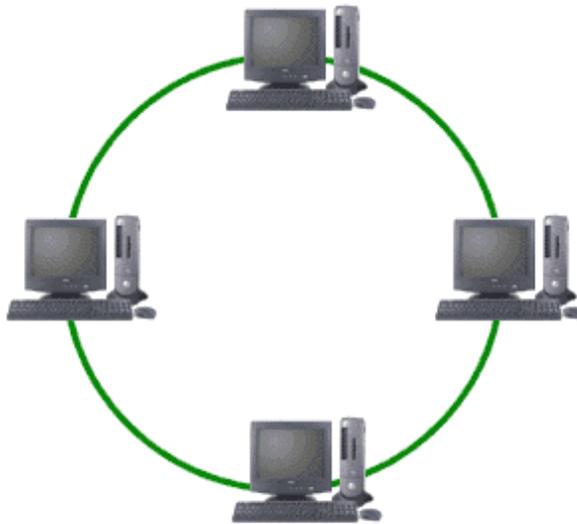


Figura 1-10. Topología en anillo.

1.2.1.6.- Topología en árbol

En esta topología que es una generalización del tipo bus, el árbol tiene su primer nodo en la raíz y se expande hacia fuera utilizando ramas, en donde se conectan las demás terminales.

Esta topología permite que la red se expanda y al mismo tiempo asegura que nada más existe una ruta de datos entre dos terminales cualesquiera.

Ventajas:

- La falla de un nodo no implica interrupción en las comunicaciones.
- La topología en árbol puede verse como una combinación de varias topologías en estrella.

Desventajas:

- La información se propaga hacia todas las estaciones.

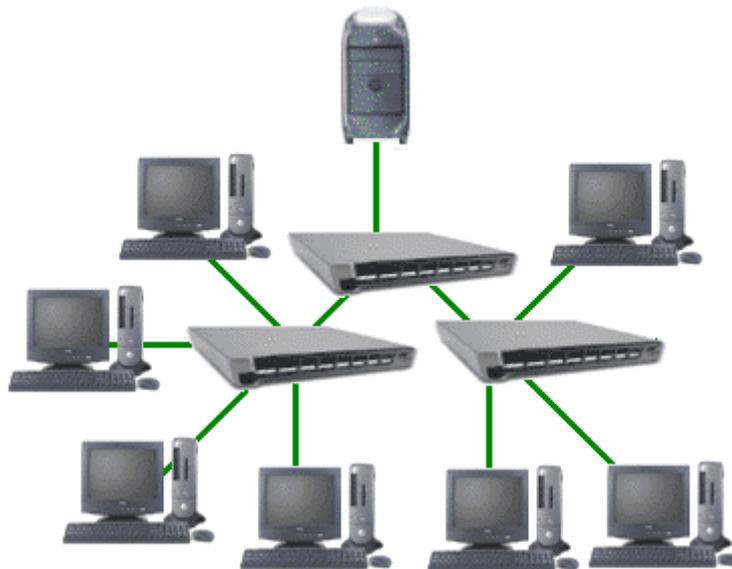


Figura 1-11. Topología en árbol.

1.2.1.7.- Topología de malla completa

En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta llegar

a destino. Además, esta topología permite que la información circule por varias rutas a través de la red.

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

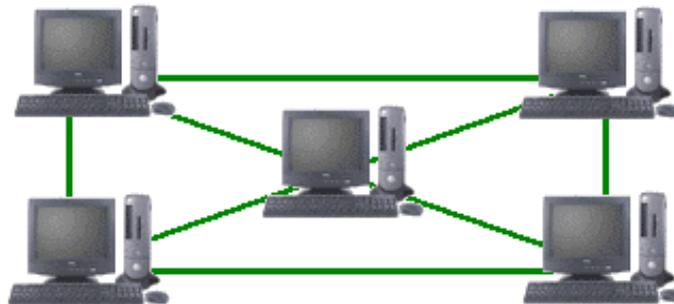


Figura 1-12. Topología en malla completa.

1.2.2.- ÁREA FÍSICA

El área física tiene que ver con todo lo relacionado al material que se utiliza para construir una red, entre los cuales están: los cables, las computadoras, servidores, switches, routers y hubs. Esta área se complementa con la de diseño, también se debe tener especial cuidado en los equipos que se adquieren, porque en ocasiones la calidad entre un equipo y otro puede llegar a ser considerable.

Lo que se busca es tener una mayor rentabilidad en nuestra red basado en el mejor costo, esto se hace con la finalidad de no tener que invertir en gastos innecesarios como son las reparaciones y revisiones a lo largo de nuestra red LAN/WAN que a la larga en lugar de obtener beneficios se obtienen pérdidas económicas considerables.

A continuación se hace referencia a algunos de los equipos utilizados en la red del Ejército.

1.2.2.1.- Servidor

El servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red.

Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.



Figura 1-13 Servidor.

1.2.2.2.- Estación de Trabajo

Los ordenadores que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los Servidores a los cuales pueden acceder.

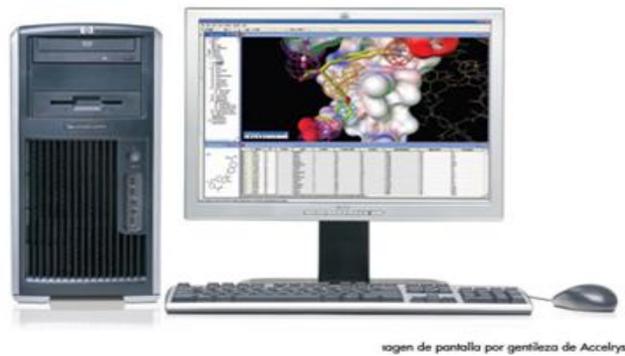


Figura 1-14 Estación de trabajo.

1.2.2.3.- Hub

O concentrador. Dispositivo que permite conectar entre sí a los equipos y que reenvía la señal recibida desde uno de los equipos de la red a todos los demás. Dependiendo de sus funciones se clasifican en Hubs activos, Hubs pasivos y Hubs híbridos.



Figura 1-15 Hub.

1.2.2.4.- Switch

O conmutador. Es un dispositivo que permite la interconexión de dos o más segmentos de una red. Tiene una función similar a la de los puentes. Se utilizan para conectar varias redes consiguiendo una red única, también funcionan como filtros de seguridad.



Figura 1-16 Switch.

1.2.2.5.- Router

O enrutador. Dispositivo que envía paquetes de datos entre redes, permite la conexión de una Red Local LAN con una red extensa WAN. Dispone de dos direcciones de IP una local para la LAN y otra pública para la WAN.

Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.



Figura 1-17 Router.

1.2.2.6.- Sistema Operativo

Es el conjunto de aplicaciones que permiten la comunicación con el ordenador, Existen sistemas operativos especializados para trabajar en red como Windows 2003 Server.



Figura 1-18 Sistemas operativos.

1.2.3.- ÁREA DE INTERCONECTIVIDAD

En el área de Interconectividad intervienen las dos áreas anteriores, además del establecimiento de los estándares para la conexión y el entendimiento entre los distintos equipos, esto ha existido desde los inicios del desarrollo de redes de área local con grupos que buscan establecer sus propios estándares de interconexión para los equipos.

Los principales grupos que han sobresalido en esta área son “The Consultative Comité for Telecommunications (CCITT) y la “The Institute of Electrical and Electronic Engineers” (IEEE), así como la “Internacional Organization of Standarization” (ISO) y se basan en el modelo “Open Systems Interconnection” (OSI) con sus 7 capas (Capa física, Capa de enlace de datos, Capa de Red, Capa de transporte, Capa de sesión, Capa de presentación y Capa de aplicación).

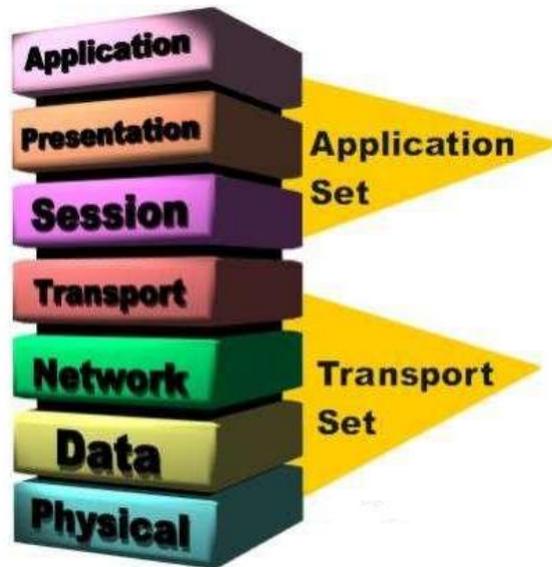


Figura 1-19. Capas del modelo OSI.

También se deben asignar los protocolos de comunicación, que si bien entre algunos se tienen diferencias, “deben de comunicarse en base a los estándares establecidos a partir de las capas más bajas (Física y enlace de datos), por lo tanto por la diferencia entre protocolos no es necesario que se tengan similitudes en las capas superiores del modelo OSI”.

Otra parte esencial del área de Interconectividad es el direccionamiento para cada uno de los equipos, para que no exista pérdida de información y de traspaso de datos, para poder realizar esta tarea se puede almacenar la dirección del equipo manualmente o teniendo un servidor DNS (Domain Name Server) para asignar una dirección lógica de manera dinámica.

1.2.4.- ÁREA DE SEGURIDAD

La seguridad es parte primordial en el diseño de una red, ya que “tener una política de seguridad en la red, puede proteger la inversión y sus recursos de información”, también del grado de la política de seguridad va a depender de gran manera “a qué tipo de servicios de trabajo y recursos de Internet se va a permitir que tengan acceso los usuarios”.

Ya que si estos disfrutan de un “acceso irrestricto, podrá ser difícil adoptar una política que restrinja su acceso”, con esto cualquier persona podría tener acceso a los recursos más importantes que tiene nuestra red y por lo tanto pueden ser vulnerables a cualquier ataque por parte de un usuario desconocido.

A continuación se muestra un esquema en el cual, para los intereses y finalidades que se tienen en el diseño de nuestra red, se puede tomar para evitar posibles ataques por parte de usuarios indeseables y que es parte primordial para la protección de la misma.

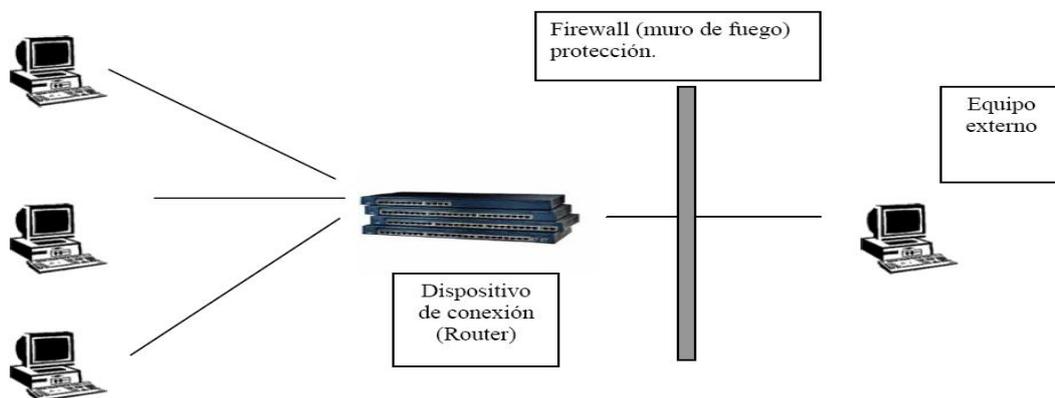


Figura 1-20. Área de seguridad.

En el esquema se observa, que la manera de proteger nuestra red es poniendo una barrera de seguridad o “firewall”, el cual evita que cualquier equipo que se encuentra afuera de los límites de nuestra red LAN/WAN, pueda enviar o recibir información concerniente a la comunicación de nuestros equipos.

Aunque se puede ingresar desde afuera siempre y cuando se tenga una clave de autenticación o “password” para poder ingresar y que sea proporcionado por parte del administrador de la red.

Mencionados los puntos anteriores la administración de redes toma una parte esencial en nuestro trabajo ya que se puede decir que “la administración de redes es un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada”.

También se deben realizar algunas preguntas que nos determinarán la política de seguridad en la red, todo esto para realizar un conjunto de objetivos para que posteriormente se tomen las medidas necesarias y proteger nuestra información. Para realizarlo se debe saber que “definir una política de seguridad de red significa desarrollar procedimientos y planes que salvaguarden los recursos de la red”, para desarrollar una política de seguridad se puede tomar en cuenta el siguiente análisis, con las siguientes preguntas:

¿Qué recursos se quieren proteger?

¿De qué personas necesita proteger los recursos?

¿Qué tan reales son las amenazas?

¿Qué tan importante es el recurso?

¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Es de vital importancia que se “examine con frecuencia su política de seguridad de red para verificar si sus objetivos y circunstancias en la red han cambiado”. Para el planteamiento de este trabajo, los recursos se tomarán en cuenta a partir del equipo con el que se cuenta así como su información almacenada y además de lo que se transfiere y se intercambia en nuestra red.

1.3.- MONITOREO DE REDES DE COMPUTADORAS

También se deben realizar algunas preguntas que nos determinarán la política de seguridad en la red, todo esto para realizar un conjunto de objetivos para que posteriormente se tomen las medidas necesarias y proteger nuestra información.

La palabra monitoreo no tiene una definición exacta, pero en el contexto computacional ha adquirido un auge muy grande, de manera más específica en el área de redes y de seguridad. Se ha discutido mucho sobre la definición de la palabra monitoreo se han hecho estudios sobre la mejor definición y se enfocará en uno muy particular que es “una función que busca conocer cómo se están realizando las tareas definidas en el plan operativo y de presupuesto”.

Aunque la definición anterior, no aplica exactamente en el área estudiada, nos proporciona un panorama en donde se puede extender más en una definición concreta para nuestra investigación.

En el área tecnológica el concepto de monitoreo debe tener un enfoque más práctico, en materia de redes, por ejemplo, todas las acciones que proporciona un control completo sobre los enlaces, visualización, disponibilidad, desempeño y la administración de fallos necesitando tener constante acción con el equipo involucrado, conexiones y es el caso de este tema a desarrollar, supervisar todas las funciones que implica el trabajo de una red de computadoras.

El monitoreo se encuentra muy ligado con el concepto de Inteligencia Competitiva la cual se define como: “conocimiento generado a partir del análisis resultante de la integración de información sobre el entorno de la organización, que está disponible lícitamente”.

En base a este conocimiento generado, se pueden realizar acciones específicas en el caso de que una infraestructura de redes pueda tener algún tipo de problema, esta sería la diferencia entre el simple análisis de datos y monitorear una red.

En caso del monitoreo además de realizar un análisis detallado acerca de las acciones que se suceden en la red, también se realizan las acciones de supervisar y reaccionar ante algún imprevisto.

Estos imprevistos se pueden traducir en eventos como es el caso de “problemas de ruido en la línea de transmisión y que crean situaciones que no existen tales como direcciones de computadoras que no pertenecen a ninguno de los nodos, errores de tipo hardware y software detectados en los servidores o estaciones conectadas en red, performance de la red porcentaje de utilización del Ancho de banda de la red en sus niveles promedio, máximos y mínimos los cuales se comparan con valores recomendados por normas, por mencionar algunos”.

A grandes rasgos lo que se pretende en el proyecto de tesis es “Conocer a profundidad cómo es el desempeño de una red, lo que permitirá recopilar información, a continuación analizar e informar sobre los patrones de tráfico y utilización de ancho de banda en tiempo real. WhatsUp Gold no sólo pone de relieve la utilización general de la LAN o WAN o para un dispositivo o interfaz, también indica a los usuarios, las aplicaciones y los protocolos que están consumiendo valioso ancho de banda de red.

1.3.1.- LA NUEVA REALIDAD DE LA GESTION DE RED

El mantenimiento de la red ejecutando 24 horas al día por 365 días al año no es suficiente. Ahora también hay que entender cómo, la red está siendo utilizada con el fin de garantizar un rendimiento óptimo. Una red lenta tiene efectos adversos sobre el conjunto, la red es el negocio (mapa), y sin las herramientas adecuadas no siempre se puede identificar rápidamente problemas de rendimiento o eficiencia.

Si no puede encontrar el problema en la red de tráfico o determinar los destinos, tanto dentro como fuera de su red, cómo puede saber si las descargas de vídeos de YouTube están afectando el rendimiento general de las aplicaciones de ancho de banda. Cuando hay un problema de rendimiento de la red, los gestores de la red necesitan al ingresar, analizar la información para comprender la cuestión, y a continuación resolver rápidamente el problema.

1.3.2.- MEJOR CONOCIMIENTO CONDUCE A UN MEJOR RENDIMIENTO DE LA RED

El análisis de patrones de tráfico de la red y la comprensión del monitoreo, identifica problemas de red como los usuarios que están afectando el desempeño general o las aplicaciones que necesitan más ancho de banda, así se puede tomar medidas para garantizar que la red está dentro de los parámetros.

Lo que ocurre en todo caso es que si esto sucede con cada una de las computadoras conectadas a la red que se encuentra bajo análisis “se llevará un conteo de los errores que están ocurriendo en la red, de tal forma que si una computadora se da cuenta de que el número de errores excedió a la cuenta permitida, le informa a la computadora que está "monitoreando" a la red, a fin de que pueda declararse una condición de error y mostrarla en el servidor de toda la red”.

Vistos todos los aspectos anteriormente mencionados se puede dar una definición de monitoreo en el área de redes y es: “Análisis detallado que surge a partir del estudio sobre la red supervisada y que da un conocimiento de su funcionamiento y en caso de tener algún error dar la acción inmediata para su restablecimiento”.

En esta parte se puede concluir que el tema de monitoreo de redes es apenas un desarrollo que no se ha explotado del todo y que puede tener muchas variantes, para cuestiones de nuestro proyecto de monitoreo de redes y disponiendo de la tecnología de punta y la facilidad que nos brinda el Internet de obtener Software open source se realizará mediante la herramienta WhatsUp Gold.

1.4.- IMPORTANCIA DEL PROYECTO PARA LA RED DE DATOS DEL EJÉRCITO

Actualmente la Dirección de Sistemas y Comunicaciones de la Fuerza Terrestre (DISICOM) en su Centro Principal de Comunicaciones cuenta con los nodos

centrales de diversas Redes de Área Amplia, para la integración de los mandos territoriales distribuidos a lo largo y ancho de la República Ecuatoriana. Dichas redes proporcionan servicios como voz, datos y video, y están soportados sobre múltiples protocolos como Ethernet e IP los mismos que corren sobre infraestructuras de fibra óptica y satelitales con accesos FDMA y TDMA1.

Al implementar una interfaz estándar de monitoreo y administración de las alarmas generadas en las redes IP de la Dirección de Sistemas y Comunicaciones de la Fuerza Terrestre (DISICOM), que además permita efectuar la pronta detección y diagnóstico de las fallas generadas así como su almacenamiento cronológico, conducirá a tomar acciones correspondientes en menores tiempos encaminadas a la restauración y a la buena operación de los servicios proporcionados, sin necesidad de contar con conocimientos avanzados de las herramientas de análisis de redes para la detección de los eventos.

Las Tecnologías de monitoreo serán una herramienta fundamental en la operación y desarrollo del Ejército Ecuatoriano, no obstante los beneficios que traen consigo los avances tecnológicos, sobre todo, representan grandes retos para las áreas encargadas de la administración de redes, es un motivo por el cual es necesario que dentro del Ejército Ecuatoriano se implemente un servicio que se encargara de la gestión y monitoreo de las redes.

En consecuencia es de mucha importancia efectuar una investigación encaminada a implementar una interfaz de monitoreo, administración, detección y diagnóstico de alarmas, fallas y análisis de tráfico de redes IP, integrando en una sola aplicación las herramientas dedicadas para tales fines en forma aislada e independiente e interactuándola a su vez a una base de datos dinámica para su almacenamiento y consulta, todo ello sobre una plataforma abierta y con acceso vía Intranet.

1.5.- DESARROLLO

Como primer paso, se realiza la investigación sobre las herramientas necesarias para el monitoreo de redes y el manejo de las mismas, en este caso se lleva a cabo la búsqueda de un software open source, que para nuestro caso será el sistema de monitoreo de redes WhatsUp Gold, ya que los datos que este deduce se pueden utilizar para los objetivos establecidos, y se instala en la computadora encargada del monitoreo.

Después se procede a hacer un estudio sobre el sistema de monitoreo WhatsUp Gold, que es el familiarizarse con la herramienta, aprender a manejarla, los fines para los que se utiliza y la relación que puede tener para con otras herramientas, como los servicios Web.

A continuación se hace el levantamiento del sistema de monitoreo de redes WhatsUp Gold, con sus análisis correspondientes y que tenga las utilidades que el administrador necesita, después se pasará a la parte en donde se configurara nuestro software con la finalidad de obtener las variables que contienen los datos que nos interesan y finalmente presentarlas de una manera fácil.

De manera simultánea, se redacta la parte correspondiente al desarrollo de nuestra aplicación, se procede a realizar las pruebas necesarias para evaluar y garantizar la capacidad de trabajo y los niveles de servicio de WhatsUp Gold

CAPÍTULO II

ANÁLISIS DEL SISTEMA

Este capítulo se enfoca al estudio de las características, propiedades y cada uno de los elementos que involucran el Sistema de Gestión y Monitoreo, esto implica hablar de la herramienta WhatsUp Gold, su origen, descripción, funcionamiento y los elementos de la información que se pretende manejar para que el usuario finalmente pueda mantener una red operativa, eficiente, segura, constantemente monitoreada y con una planeación adecuada y propiamente documentada.

Anteriormente, cuando no se disponía de las herramientas que hoy existen, era necesario contratar a una empresa especializada para esta labor, con un costo muy elevado. El sistema de Monitoreo y Gestión WhatsUp Gold permitirá realizar esta importante labor, y contar con un sistema experto como aliado que ayudara en la interpretación de los resultados obtenidos todo el tiempo.

2.1.- IPSWITCH

Fundada en 1991, Ipswitch, Inc. es una empresa que desarrolla y comercializa soluciones de software que es fácil de aprender y utilizar. Más de 100 millones de personas en todo el mundo utilizan el software Ipswitch para vigilar sus redes. Siempre que lanza un producto en el mercado se identifica por este nombre seguido de la herramienta creada.

Ipswitch ofrece soluciones de monitoreo de red, gerencia de datos y transferencia de archivos (con elementos de seguridad dentro de cada solución) y tiene presencia en el país desde hace más de cinco años. Representa una alternativa para las empresas que requieren soluciones funcionales de alto valor pero de poco costo de administración e inversión monetaria, ese es el principal atractivo de estos productos.

La creciente necesidad de reportar las condiciones de la red. El último aporte de Ipswitch al mercado llega en un momento en el que los profesionales TI de empresas de todos los tamaños están preocupados por mantener las redes y las aplicaciones de servicio a través de los múltiples puntos geográficos del negocio.

Estas compañías necesitan mantener sus Centros de Operaciones de Redes (NOC -Network Operations Centers) y equilibrar la cantidad de datos que son enviados de nuevo al NOC desde las locaciones remotas con la necesidad de una rápida y fácil identificación del problema y la solución.

Con la edición distribuida de WhatsUp Gold, las organizaciones de todos los tamaños pueden beneficiarse con la productividad de un panel de control central o NOC. La pantalla administradora de utilidades que posee WhatsUp Gold le permite a las compañías de todos los tamaños crear un panel de control inteligente que centralice la visualización de los sitios y resúmenes de status de los dispositivos por sitio en una sola pantalla o grupo de pantallas en el NOC.

2.2.- DEFINICIÓN DE WHATSUP GOLD

El WhatsUp Gold es la solución de GESTIÓN Y MONITOREO DE REDES líder del mercado mundial, es un sistema que mapea, monitorea, alerta y proporciona reportes acerca de los cambios en los estados de todo el equipo crítico de la red y en los estados de las aplicaciones y servidores Windows es profundo y fácil de utilizar, permitiendo la conversión de datos de la red a información.

Al monitorear proactivamente todos los servicios y dispositivos críticos, el WhatsUp Gold reduce el tiempo caído de red, Con su totalmente renovada interfaz Web, el WhatsUp Gold permite el control total de la infraestructura y de las aplicaciones de la red, para que el trabajo estratégico, táctico y que trae resultados no sea interrumpido, el WhatsUp Gold provee fácil configuración, escalabilidad robusta, simplicidad de utilización y rápido retorno de inversión.

2.3.- FUNCIONES DE WHATSUP GOLD

En general, WhatsUp Gold tiene distintas funciones las cuales ayudan al administrador a realizar toma de decisiones, es decir, las acciones a tomar en base a los diagnósticos y análisis de lo que está sucediendo en la red.

El funcionamiento principal de WhatsUp Gold se basa en cinco consideraciones, las cuales obtienen las principales funciones de WhatsUp Gold de manera general:

2.3.1.- IDENTIFICACIÓN Y MAPEO DINÁMICO DE LA RED

Descubra la red en minutos utilizando ayudantes de instalación intuitivos para rastrear en búsqueda de routers, switches, servidores, impresoras y otros dispositivos. Toda esta información es almacenada en una base de datos relacional, para posibilitar fácil gestión de dispositivos y reportes.

Grupos Dinámicos permiten la unificación de dispositivos de acuerdo a sus específicas características; por ejemplo, todos los dispositivos que han fallado o todos los dispositivos de un tipo particular.

Identificación y mapeo de direcciones MAC hasta direcciones IP, para poder ilustrar la conectividad entre los puertos y dispositivos específicos de un switch, permitiendo la mejor localización de recursos.

2.3.2.- RÁPIDA RESOLUCIÓN DE PROBLEMAS

Acompañe las fallas de su red y envíe alertas cuando surgen problemas, reinicie un servicio detenido o inicie un programa automáticamente. El WhatsUp Gold puede:

- Enviar alertas vía correo electrónico, teléfono celular, SMS, audio y alertas en la bandeja de tareas del Sistema.
- Re direccionar SNMP

- Reiniciar servicios que son críticos al negocio.

2.3.3.- PROFUNDO MONITOREO DE SNMP Y WMI

Controle la disponibilidad y el desempeño de los sistemas fundamentales para la empresa. WhatsUp Gold ofrece el control en tiempo real de los servicios de la red, los servicios de Windows NT, el registro de eventos, los eventos diarios del sistema y la utilización de recursos del sistema. WhatsUp Gold también puede determinar la disponibilidad de páginas HTTP y monitorear octetos para identificar asuntos de ancho de banda.

2.3.4.- MONITOREO DE RENDIMIENTO Y REPORTE

Los monitores de rendimiento de WhatsUp Gold obtienen importante información sobre dispositivos que se están utilizando en la red, luego utilizan tales datos para crear reportes de tendencias de utilización y disponibilidad de diferentes aspectos de tales dispositivos.

WhatsUp Gold es instalado con cinco monitores de rendimiento que monitorean tipos de datos específicos de los dispositivos de la red:

- Utilización CPU
- Utilización de Disco
- Utilización de Interfaz/Ancho de Banda
- Utilización de Memoria
- Latencia y Disponibilidad vía Ping

WhatsUp Gold también tiene la capacidad de crear monitores personalizados pueden ser creados para cualquier contador de rendimiento WMI o SNMP. Una vez que tal monitor sea configurado, un reporte de rendimiento puede ser generado para que se vean los resultados de las investigaciones de rendimiento.

Estos reportes pueden ser utilizados para solucionar problemas de la red.

2.3.5.- INFORMES COMPLETOS

Uno de los aspectos clave de administrar redes distribuidas es la comunicación y uno de los factores críticos en las empresas es la responsabilidad. WhatsUp Gold ofrece informes detallados que se pueden enviar automáticamente o en forma programada.

Estos informes les permiten a los gerentes de TI conocer el estado los motivos de la disponibilidad y los cortes de la red. Con los informes de WhatsUp Gold, el usuario siempre sabe qué, cuándo y por qué ocurren las cosas en toda la red.

2.4.- PROPIEDADES DE WHATSUP GOLD

Las propiedades más importantes de WhatsUp Gold en la cual el administrador tendrá la posibilidad de conocer el estado de la red en forma remota y de la misma forma poder detectar posibles problemas en la comunicación son las siguientes:

2.4.1.- CARTOGRAFIA DE LA RED

La herramienta WhatsUp Gold puede crear el mapa de su red de varias maneras, incluyendo un sistema automático "descubrir y mapa" con la capacidad que puede explorar los archivos y la red Windows.

También puede crear un mapa de red mediante el análisis de información SNMP, escaneo de un rango de direcciones IP, cargando un archivo de hosts, la exploración de un entorno de red, o el dibujo mismo.

2.4.1.1.- Métodos de exploración con WhatsUp Gold

Sondeo sobre los dispositivos de la red a la que el ordenador está conectado
Identificar cualquier TCP / IP, NetBIOS, IPX o dispositivos.

Crear un mapa de red con un icono para cada dispositivo (de trabajo, servidores, hosts, puentes, encaminadores, subredes, contenedores, cajas de LAN, hubs, impresoras). Cada dispositivo está asociado con una dirección específica.

2.4.2.- CONTROL DE LA RED

Una vez que haya creado o cargado un mapa de red, puede configurar WhatsUp Gold para un seguimiento continuo de la red, o puede iniciar un "sondeo" de la red.

Un sondeo de la red implica un seguimiento de cada dispositivo en el mapa de red. Cada "chequeo" de WhatsUp Gold consiste en el envío una encuesta petición a un dispositivo y el seguimiento de la respuesta.

Para cada dispositivo de seguimiento, puede elegir entre un conjunto de opciones en las propiedades del dispositivo para determinar cómo se controla el dispositivo y definir qué medidas tomar si el dispositivo no responde a un chequeo.

En cada dispositivo TCP / IP en el mapa de red, puede determinar qué servicios se están ejecutando en ese dispositivo (como HTTP, SMTP, DNS) y usted puede seleccionar los servicios que desea controlar.

Cuando se abre la ventana del mapa de red, WhatsUp Gold comienza automáticamente el seguimiento de la red.

Cuando usted coloca el cursor sobre el icono de un dispositivo, la barra de estado muestra el nombre de dispositivo, la dirección, y la breve descripción de estado, incluyendo el estado de cualquier dispositivo que este siendo supervisado.

La barra de estado muestra el tiempo que un dispositivo está bajo sondeo.

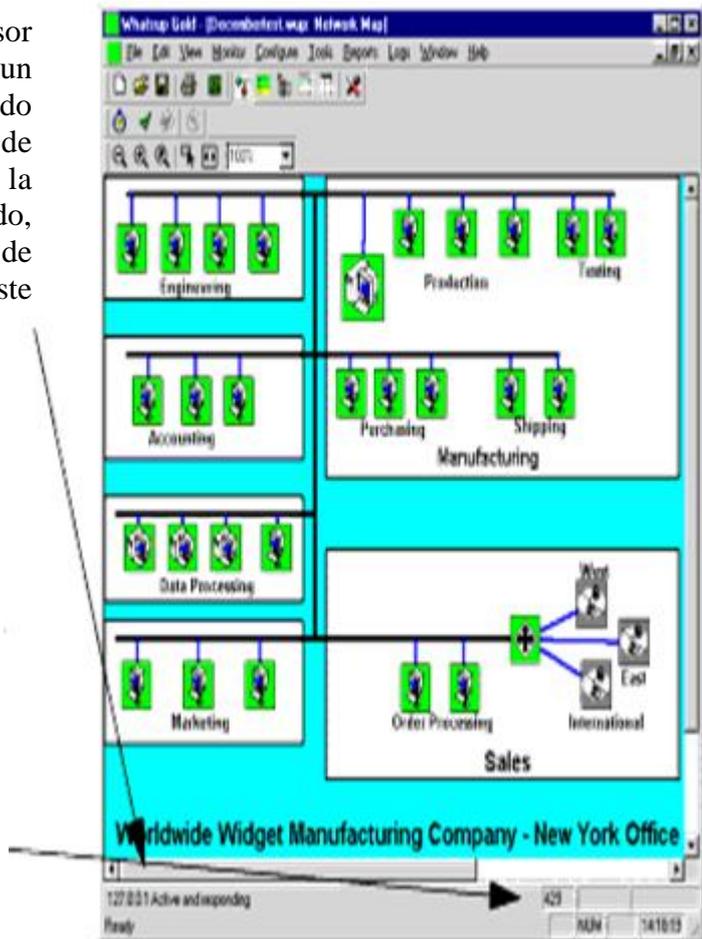


Figura 2-1. Control de la red.

WhatsUp Gold se encuentra en modo monitor o bien el modo de edición. El modo monitor es el modo en el cual el WhatsUp Gold sondea la red. Modo de edición es el modo en el que se puede realizar cambios en el mapa, puede utilizar el modo de edición para refinar el mapa de red, añadir dispositivos, establecer líneas de conexión, y convertir iconos a un icono de diferente tipo.

2.4.3.- OBTENER INFORMACIÓN DEL MAPA DE RED

En modo monitor, el mapa da la indicación gráfica de los problemas potenciales y reales de la red. Si un evento ocurre, como la falla de un dispositivo el nombre del dispositivo se convierte en relieve en el mapa.

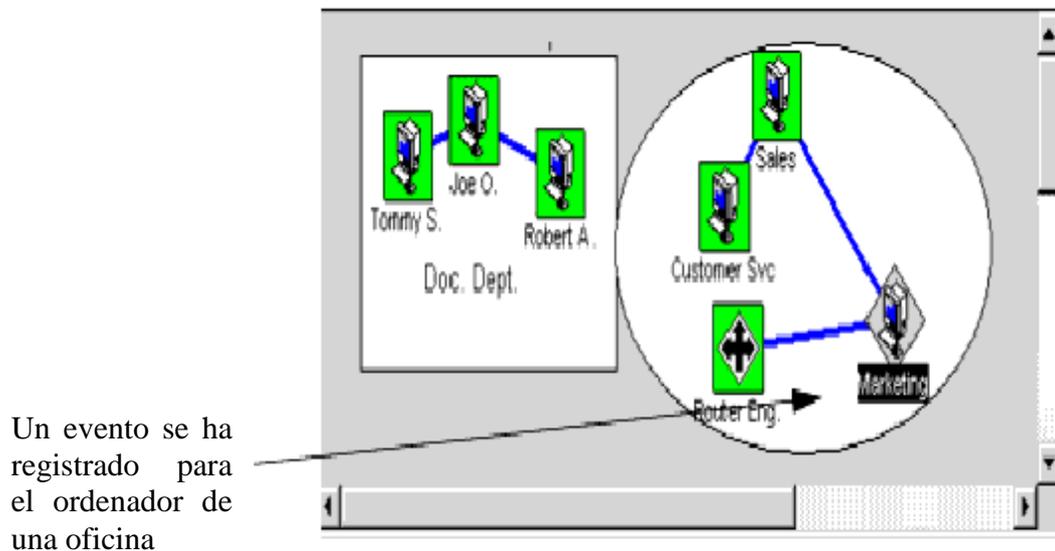


Figura 2-2. Información del mapa de red.

Además, los colores y formas indican el estado de los diversos dispositivos. De forma predeterminada, los dispositivos que responden a las encuestas se muestran en verde, los que han perdido una encuesta son de color verde claro, los que han perdido dos encuestas son de color amarillo, y los que no son accesibles (o no han respondido a las encuestas de cuatro) son de color rojo. Puede cambiar el valor por defecto de colores y formas.

2.4.4.- OBTENER LA CONDICIÓN DE UN DISPOSITIVO

En modo de monitor, puede mostrar al minuto la información de estado acerca de un dispositivo haciendo clic derecho en el icono del dispositivo, seleccionar **Quick Estado** y a continuación, clic en Estado.

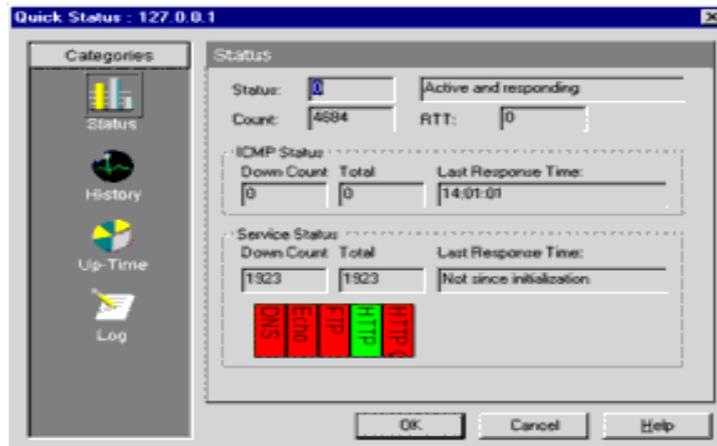


Figura 2-1. Información de estado de la red.

2.4.5.- PRESENTACIÓN DE INFORMES

WhatsUp Gold registra dos tipos de datos: cambios de estado de red (acontecimientos llamados), como la baja de un dispositivo y las estadísticas de sondeo para cada uno de ellos.

De estos datos registrados, WhatsUp Gold puede crear varios informes y gráficos que muestran el estado de su red de diferentes maneras. Desde el menú de **informes**, puede crear los siguientes:

2.4.5.1.- Gráficos de rendimiento

Muestra dispositivos con el mejor o peor funcionamiento basado en estadística agregada que sondea.

2.4.5.2.- Informes de eventos

Muestra eventos de dispositivo activos y caídos, servicio de subir y bajar los eventos, y abrir y cerrar el mapa.

2.4.5.3.- Informes de estadísticas

Muestra las estadísticas de sondeo acumuladas por dispositivo.

2.5.- CAPACIDADES DE WHATSUP GOLD

El sistema de gestión y monitoreo de redes WhatsUp Gold ofrece muchas nuevas capacidades:

- Interfaz Web permite ahora la seguridad Web por mapa.
- Interfaz de usuario actualizada barras de herramientas, iconos y cuadros de diálogo de uso fácil e intuitivo.
- Modificado diseño de menú y menús contextuales.
- Mejoras en el mapa: Los mapas son ahora basados en gráficos vectoriales que permiten ajustar a redes, ampliar y reducir, y la habilidad de cambiar el tamaño de los mapas independiente. Los mapas de propiedades tienen ahora ilimitadas opciones de color.
- Mejora de la visualización del archivo de registro para permitir el filtrado, la impresión, el ahorro y la copia. También mejoró la gestión del tamaño del archivo de registro.
- SNMP agregó una herramienta Visor que te permite ver rápidamente el estado de las interfaces de un dispositivo SNMP.
- Informes de rendimiento permite ahora una carta de presentación de informes, y la capacidad de generar un informe sobre la ejecución por hora.
- Se ha añadido una herramienta para recibir mensajes Syslog.

2.6.- BENEFICIOS DE WHATSUP GOLD

En este punto se explicará a breves rasgos los beneficios que nos brinda el sistema de gestión y monitoreo WhatsUp Gold en la administración de redes.

2.6.1.- LIVIANA ACCIONABLE Y CENTRALIZADA

WhatsUp Gold reporta a un sitio central el estado de todos los dispositivos por sitio. A diferencia de otras soluciones que requieren grandes cantidades de datos transferidos a la instalación central, WhatsUp Gold fue diseñado con la eficiencia

de la red en mente, eliminando los potenciales cuellos de botella en la red provocados por la sobrecarga de datos.

2.6.2.- LISTA PARA EL NOC

Organizaciones de todos los tamaños pueden beneficiarse con la productividad de un panel de control central o NOC. La Pantalla Administradora de WhatsUp Gold le permite a las compañías crear un panel de control inteligente que centralice las visualizaciones de todos los sitios y los resúmenes de status de los dispositivos por sitio en una sola pantalla en el sitio central.

Los administradores no necesitan estar presentes físicamente en las dispares locaciones físicas. A su vez, los administradores pueden enfocarse en un trabajo estratégico sabiendo que WhatsUp está trabajando 24 horas al día, 7 días a la semana, alerta a cualquier cambio de importancia que se produzca basado en las reglas seeteadas previamente por el administrador.

2.6.3.- LA ARQUITECTURA WHATSUP GOLD COMPROBADA

WhatsUp Gold es una herramienta creada sobre una plataforma comprobada, ganadora de premios, escalable, que lidera el mercado debido a su funcionalidad y uso. Representa todas las características positivas de la plataforma WhatsUp extendida a entornos distribuidos.

2.6.4.- EXTENSIBILIDAD

WhatsUp Gold permite un fácil intercambio de marca de servidor (construido después de Microsoft IIS) a IIS y el intercambio de la base MSDE a una SQL completamente funcional. WhatsUp Gold puede extenderse a entornos que utilizan Linux y UNÍX con agentes SNMP capaces de proveer monitoreo de disponibilidad, memoria y utilización del CPU. WhatsUp Gold también tiene un módulo de escritura incorporado que le permite a los administradores extender la colaboración de WhatsUp con soluciones de mesa de ayuda como Remedy u otras aplicaciones de monitoreo de sistemas.

2.6.5.- DISPONIBILIDAD

WhatsUp Gold está disponible en Ipswitch y su red mundial de distribuidores y canales. Las instalaciones centrales y remotas están disponibles para 100, 300, 500 o ilimitados dispositivos. Los usuarios de WhatsUp Gold con acuerdos de servicio activo pueden actualizar su software para una instalación central de la edición Distribuida.

2.7.- REQUISITOS DEL SISTEMA

La herramienta de gestión y monitoreo de redes WhatsUp Gold requiere los siguientes recursos del sistema:

- Un procesador Intel 486, o la familia del procesador Pentium o equivalente.
- Windows NT 4.0 o superior, Windows XP, Windows 2000 o Windows 98.
- Un protocolo TCP / IP.
- Si desea instalar la capacidad de rendimiento de gráficos, es necesario instalar primero Microsoft Open Data base Connectivity (ODBC) y la interfaz de controlador ODBC de texto.
- WhatsUp Gold establece estadísticas de datos, a partir de la cual se crean los gráficos, como una base de datos ODBC.
- ODBC está instalado como parte de Microsoft Office 2003 o posterior, o bien puede obtener los archivos de ODBC de Microsoft en el sitio web: www.microsoft.com/data/download_250rtm.htm. No es necesario crear la fuente de datos ODBC. Si el procedimiento de instalación WhatsUp Gold de ODBC se encuentra en su ordenador, automáticamente se crea la fuente de datos (DNS) de la ejecución de gráficos. La fuente de datos es wugstats.log (en el directorio whatsup) y utiliza Microsoft.

2.7.1.- OTROS REQUISITOS

Los siguientes requisitos adicionales se deben cumplir para poder instalar el software de WhatsUp Gold.

2.7.1.1.- Espacio libre

El directorio temporal debe tener un mínimo de 250 MB libres para la instalación de WhatsUp Gold.

2.7.1.2.- Uso del programa de desinstalación

Si necesita eliminar WhatsUp Gold del sistema, es fundamental que utilice el programa de desinstalación que se incluye con el software. Si intenta utilizar cualquier otro método, surgirán problemas cuando intente reiniciar la misma versión o cuando desee instalar una versión nueva.

CAPÍTULO III

WHATSUP GOLD Y SU UTILIZACIÓN COMO SISTEMA DE MONITOREO

En esta instancia del proyecto se describe el funcionamiento básico de la herramienta, así como los procedimientos que se deben utilizar para probar WhatsUp Gold como un sistema de monitoreo de redes.

3.1.- CREACIÓN DE UN MAPA DE RED

El mapa de red es una representación gráfica de los dispositivos en una red. A continuación se muestra un típico mapa de red.

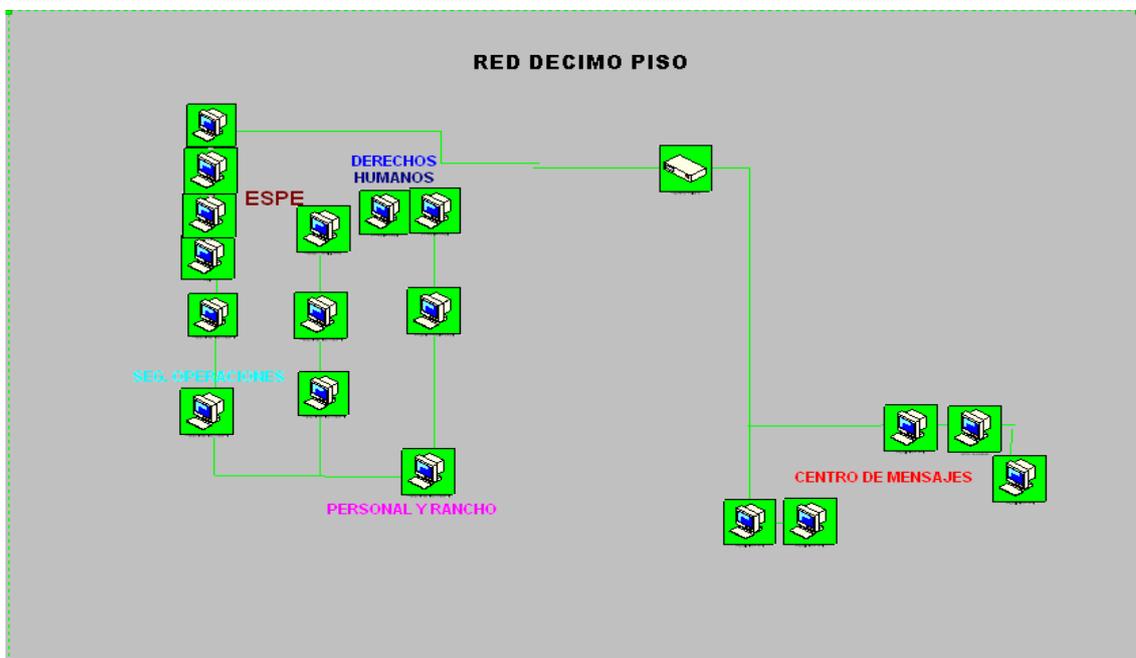


Figura 3-1. Típico mapa de red.

Los dispositivos de red pueden ser, estaciones de trabajo, servidores, routers, bridges, hubs, cajas LAN, impresoras, subredes, o cualquier tipo de host personalizado.

WhatsUp Gold ofrece varios métodos y herramientas para crear un mapa de red y añadir dispositivos a la misma:

Pasos para crear un nuevo mapa de red:

1. En el menú **File**, seleccione **New Map Wizard**.



Figura 3-2. Crear nuevo mapa de red

2. Seleccione **Create a blank map** y haga clic en **Finish**. WhatsUp Gold muestra un mapa en blanco.

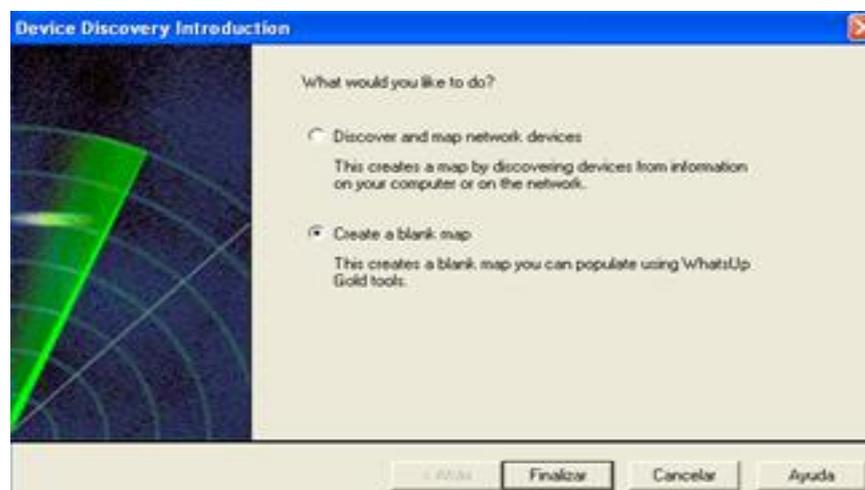


Figura 3-3. Opción crear mapa en blanco

- Haga clic en el botón **Edit Mode** en la barra de herramientas principal, y WhatsUp Gold muestra la barra de herramientas **del modo de edición**.

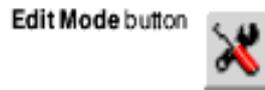


Figura 3-4. Boton de modo de edición

- Haga clic en el dispositivo de trabajo que desea utilizar en la ventana de dispositivos y a continuación, arrástrelo hasta el mapa para crear un icono de la estación de trabajo.

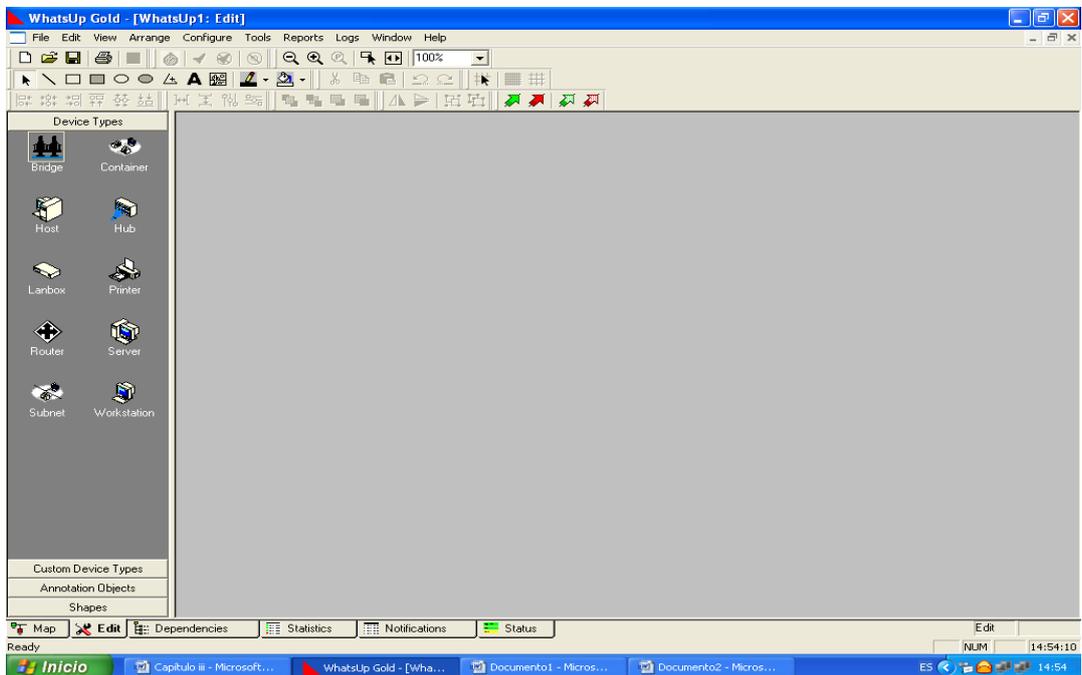


Figura 3-5. Barra de herramientas en modo de edición

- Haga doble clic en el icono que acaba de crear para ver propiedades del dispositivo.

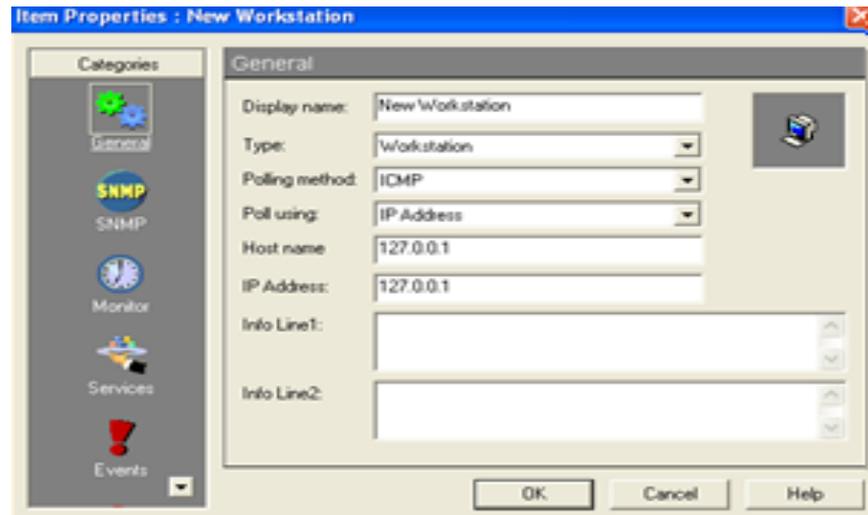


Figura 3-6. Propiedades de un dispositivo

6. En el cuadro de diálogo General, escriba la información como se muestra. Establezca un nombre en la pestaña **Display Name** en nuestro caso será consola Tesis WhatsUp Gold o cualquier nombre que desee para la consola WhatsUp Gold.

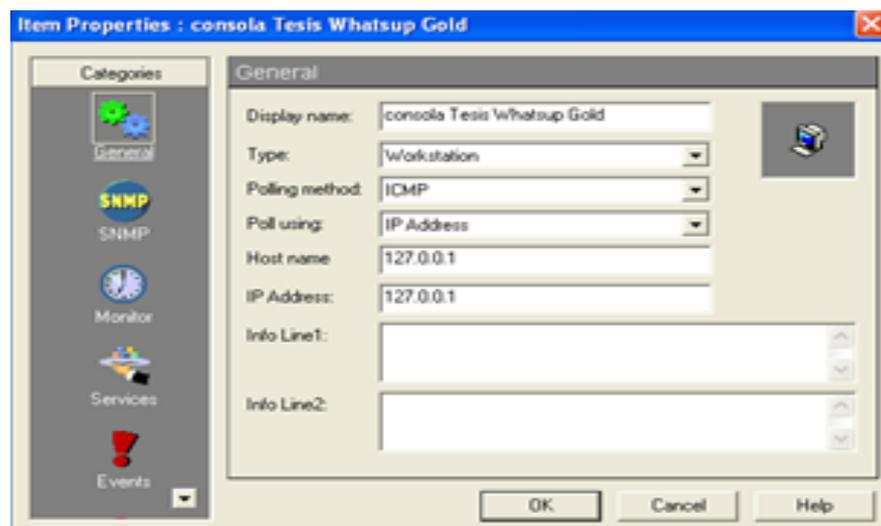


Figura 3-7. Cuadro de dialogo general

7. La dirección IP es 127.0.0.1, que es el valor por defecto. (Este es el local de "loopback" de direcciones de red, que es la dirección que se utiliza para

controlar su propio sistema.). Puede introducir la dirección IP de cualquier dispositivo que desee controlar.

8. Haga clic en monitor, asegúrese de que **Monitor This Device** este seleccionado.

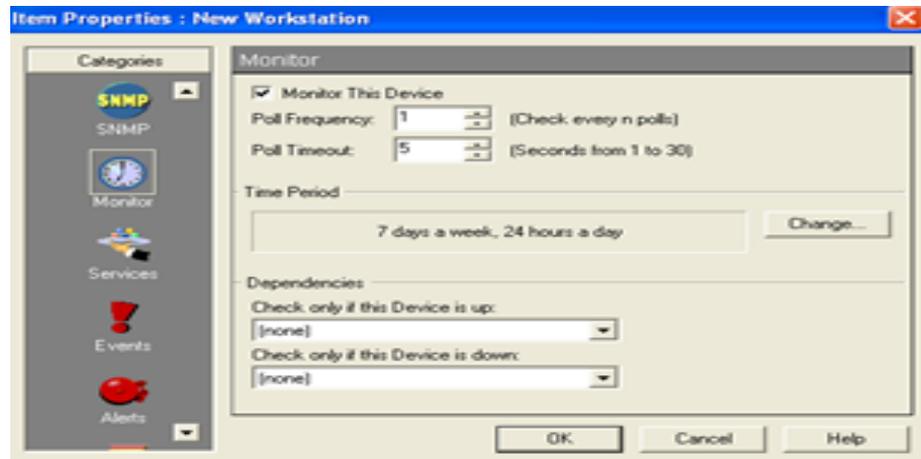


Figura 3-8. Seleccionar supervisar este dispositivo

9. Haga clic en **Alerts**, seleccione **Enable alerts** y haga clic en **Add**. Desde el cuadro de lista, seleccione "Sonido" y, a continuación, seleccione "Default". Haga clic en Aceptar y Aceptar de nuevo. Este establece el valor por defecto de sonido de alerta cuando este dispositivo se va.

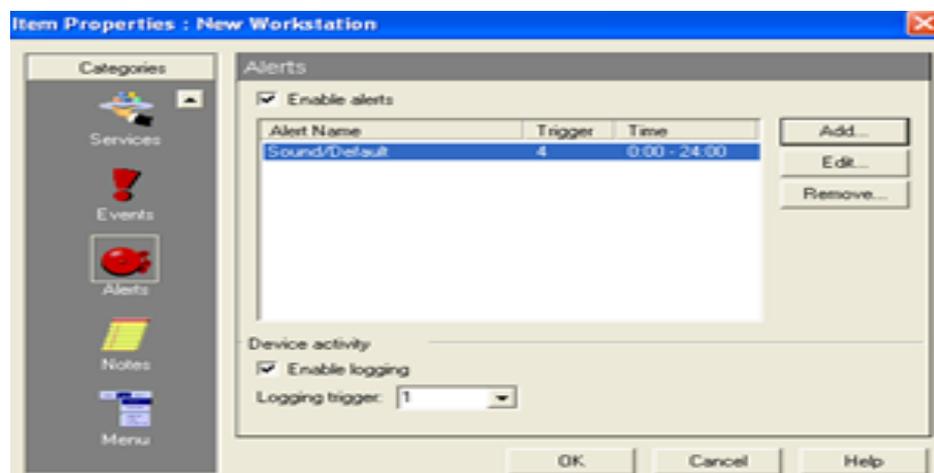


Figura 3-9. Seleccionar sonido de alerta

3.1.1.- DESCUBRIR Y MAPEAR DISPOSITIVOS DE RED

Descubra dispositivos de la red y cree un mapa de la información en su computadora o en la red a la que el ordenador está conectado mediante la lectura de archivos de red e identificar dispositivos que figuran en los archivos.

Para utilizar la capacidad de descubrir Mapas:

1. En el menú Archivo, seleccione **New Map Wizard** para ver el siguiente cuadro de diálogo.

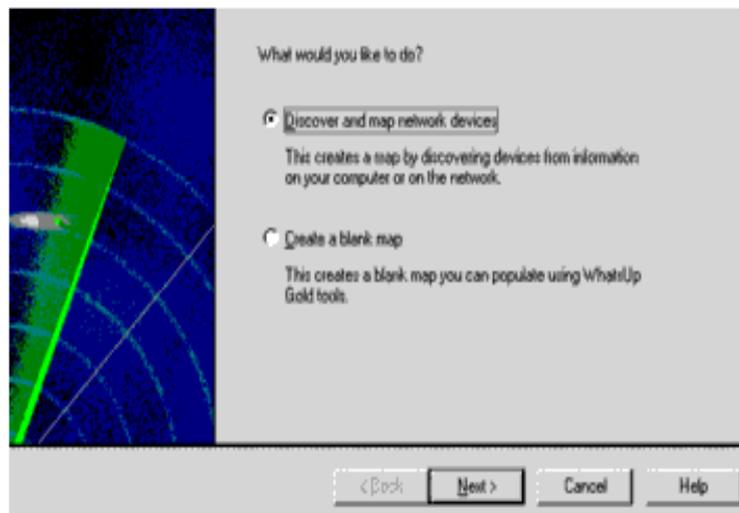


Figura 3-10. Descubra y trace los dispositivos de la red

2. Seleccione **Discover and map network devices**, y a continuación, haga clic en siguiente. Descubra los dispositivos de la pantalla.

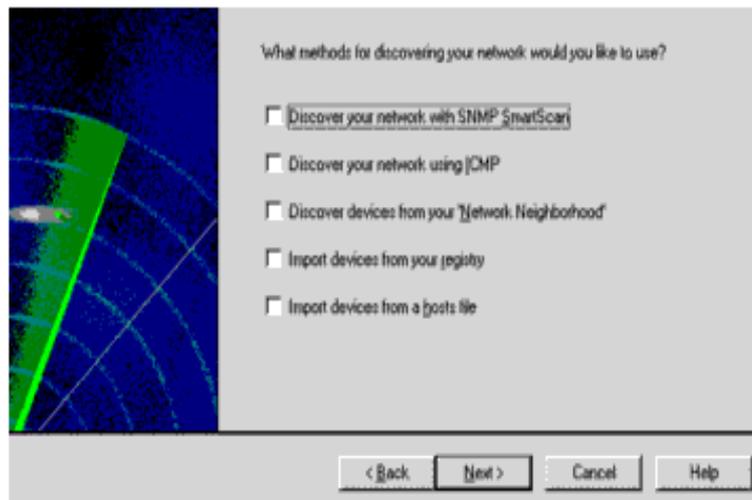


Figura 3-11. Parámetros para descubrir dispositivos de una red

3. Seleccione los parámetros que desea utilizar para crear el mapa.

Descubre tu red con SNMP SmartScan. Lee la información de SNMP en su router por defecto para identificar los dispositivos en su red y también identifica subredes dentro de su red.

Descubre tu red utilizando ICMP. Escanea un rango de direcciones IP y los mapas de los dispositivos que responder a un mensaje enviado a través de Internet Control Message Protocol (ICMP).

Discover devices from your Network Neighborhood. (Descubra los dispositivos de su entorno de red). Si su ordenador está conectado a una red de Microsoft Windows, WhatsUp Gold escanea la red y crea un icono para cada dispositivo que encuentre. (Esto puede tardar unos minutos, dependiendo del tamaño de su red.)

Import devices from your registry. (Importación de dispositivos de su registro). Lee el registro de Windows para encontrar los dispositivos que se hace referencia en el protocolo TCP/IP, Microsoft Internet Explorer o

Netscape Navigator configuraciones y, a continuación, agrega automáticamente los dispositivos para el mapa.

Import devices from a hosts file. (Importación de dispositivos de un archivo hosts). Lee el archivo hosts en el sistema local y crea un icono para cada dispositivo de red.

4. Haga clic en el botón **Next**. Dependiendo de las opciones seleccionadas WhatsUp Gold lee los archivos de red, localiza los dispositivos y los muestra en el cuadro de diálogo los "Resultados de exploración". Solicita que hacer con estos dispositivos que desea que aparezca en el mapa. Haga clic en **Finish** y el mapa se crea.
5. En el menú **File**, seleccione **Save o Save As** para guardar el mapa.

3.1.2.- USO DE SNMP SMARTSCAM

Descubra los dispositivos en su red utilizando SmartScan:

1. Si no está ya en el cuadro de diálogo "SNMP SmartScan", puede iniciar su análisis en cualquiera de las siguientes formas:

Para crear un nuevo mapa, en el menú **File**, seleccione **New Map Wizard**. Seleccione **Discover and map network devices** en la primera pantalla, y a continuación, haga clic en siguiente, seleccione **Descubre tu red con SNMP SmartScan** en la siguiente pantalla.

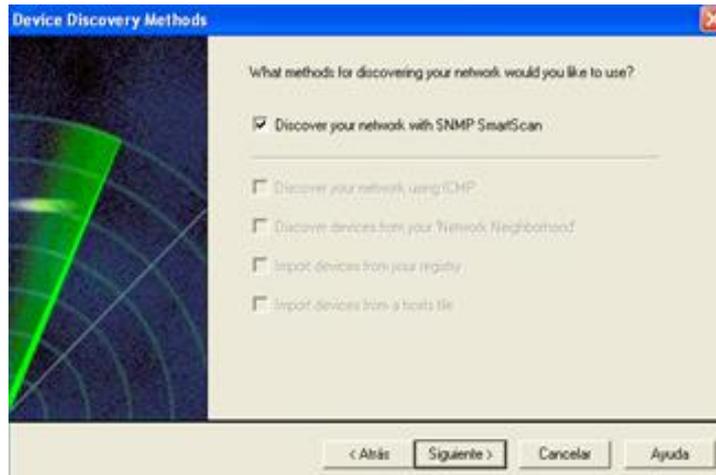


Figura 3-12. Descubre la red con SNMP SmartScan

Para añadir dispositivos a un mapa o un mapa en blanco, seleccione el mapa y, a continuación, en el menú Herramientas, seleccione descubrir dispositivos, seleccione **descubre tu red SNMP con SmartScan** en la pantalla que se muestra a continuación.

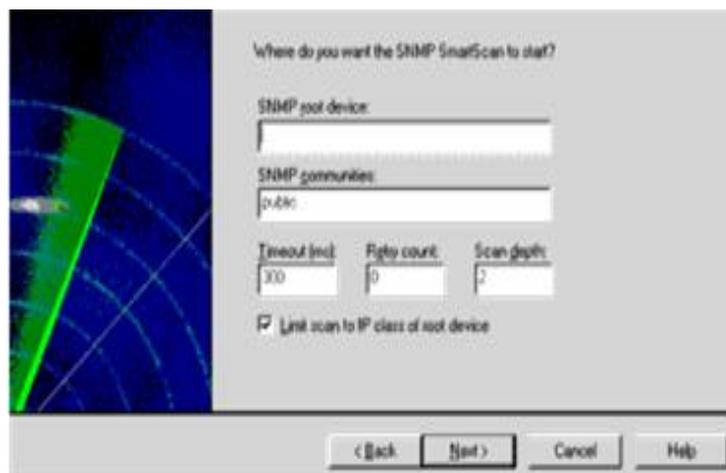


Figura 3-13. SNMP SmartScan

2. Modificar cualquiera de las opciones SmartScan. Haga clic en Ayuda para una definición de cada opción. Haga clic en **Next** para continuar.

3. Seleccione los servicios que desea analizar, y haga clic en **Next**.

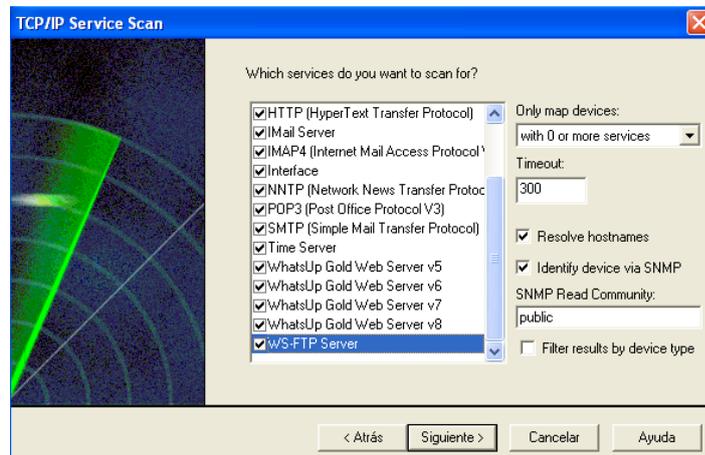


Figura 3-14. Servicios que desee analizar con SNMP SmartScan

4. La exploración se inicia.

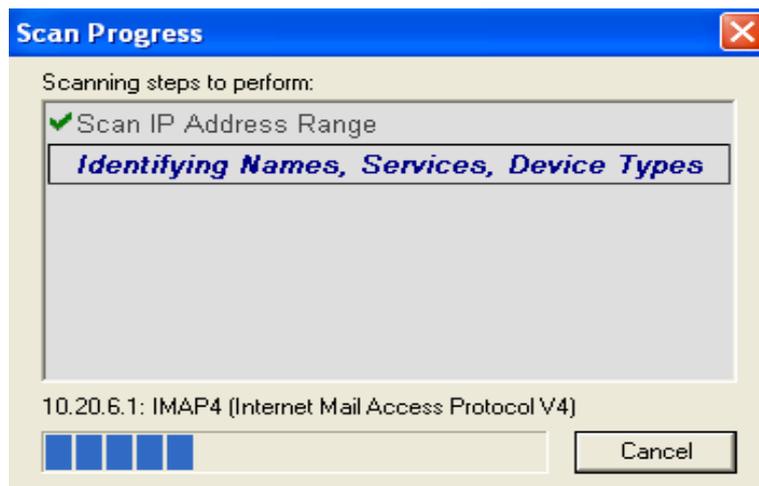


Figura 3-15. Inicio de la exploración de dispositivos

5. Cuando haya completado, se le ofrece la oportunidad de concluir que los dispositivos que desea que aparezca en el mapa. Haga clic en **Finalizar** para completar el asistente.

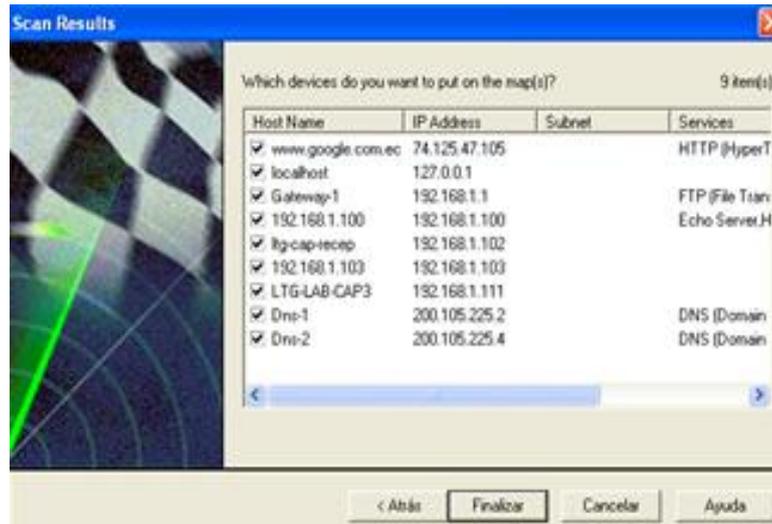


Figura 3-16. Dispositivos encontrados

6. En el menú **File**, seleccione **Save** o **Save As** para guardar el mapa.

3.1.2.1.- Resultados de SmartScan

SmartScan crea un mapa que refleja la jerarquía de su red y sus subredes. Crea un mapa separado para cada subred y crea una matriz mapa con enlaces a las subredes.

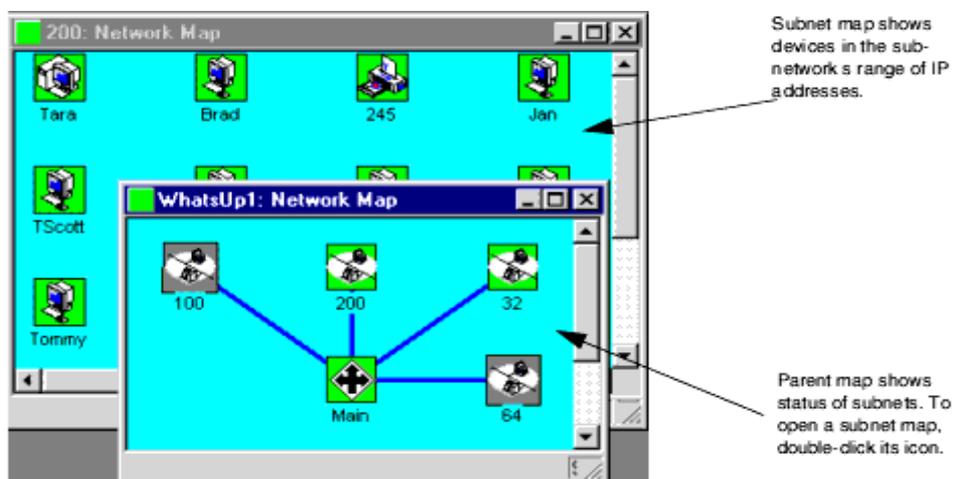


Figura 3-16. Resultados de SmartScan

Nota: Un mapa creado por SmartScan puede mostrar otras redes conectadas a la red como un icono de color gris subred. Esto significa que la exploración no ha podido trazar un mapa de los dispositivos de la subred, ya que los valores de escaneo no lo permiten.

3.1.3.- CARTOGRAFÍA DE UNA RED PLANA

Para iniciar una exploración utilizando ICMP:

1. Seleccione un mapa existente o crear una nueva ventana de mapa.
Para crear un nuevo mapa, en el menú **File**, seleccione **New Map Wizard**. En el Nuevo Mapa, seleccione la opción **Discover and map network devices** en la primera pantalla y seleccione **Descubre tu red mediante ICMP** en la siguiente pantalla.

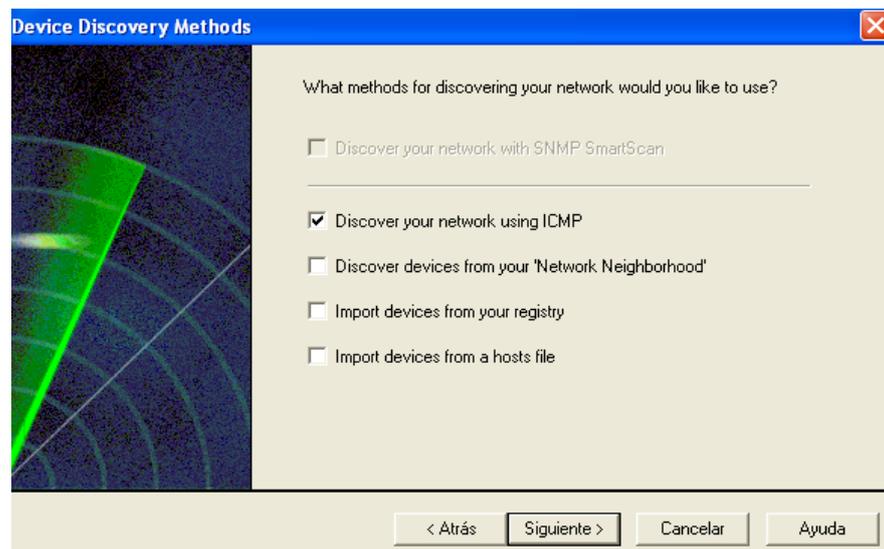


Figura 3-18. Descubre la red usando ICMP

Para añadir dispositivos a un mapa, seleccione el mapa y, a continuación, en el menú Herramientas, seleccione Descubrir Dispositivos y seleccione Descubre tu red mediante ICMP en la siguiente pantalla.

2. Haga clic en **Help** para una definición de cada opción. Haga clic en **Next** para continuar.

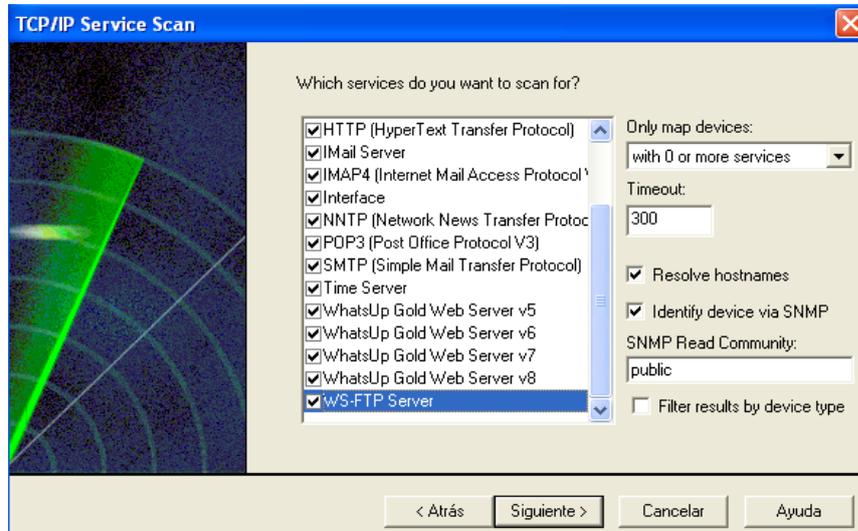


Figura 3-19. Servicios que desee analizar utilizando ICMP

3. Por defecto se muestra la dirección donde inicia y termina el monitoreo de la red.

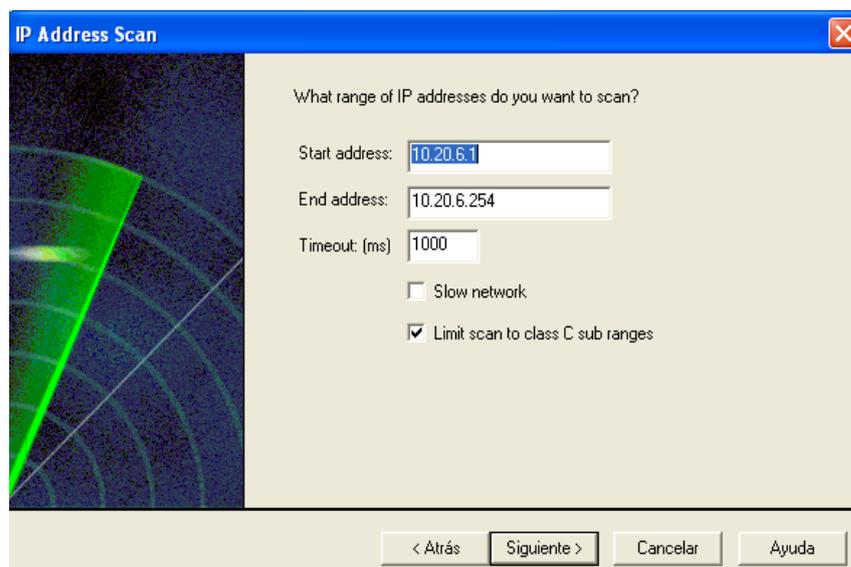


Figura 3-20. Rango de las direcciones a monitorear

4. Seleccione los servicios que desea analizar, y haga clic en **Next**.
5. En el menú Archivo, seleccione **Save o Save As** para guardar el mapa.

3.1.3.1.- Resultados de la Exploración

Cuando utiliza la herramienta de análisis como se describe anteriormente, WhatsUp Gold explora el rango de direcciones. Para cada host activo se encuentra la dirección IP.

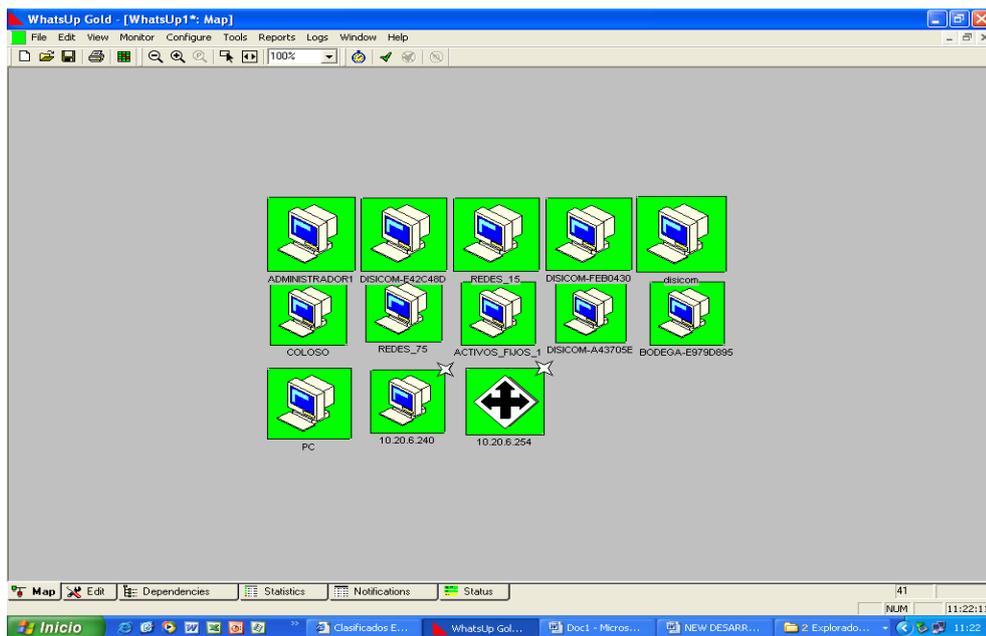


Figura 3-21. Resultados de la exploración utilizando ICMP

En las condiciones adecuadas, la exploración puede también reconocer los tipos de dispositivos personalizados.

3.1.4.- DESCUBRIR DISPOSITIVOS DE ENTORNO DE RED

Descubra los dispositivos de su Entorno de red y cree un mapa mediante el análisis de red de Windows a la que el ordenador está conectado, y realice la búsqueda de otros dispositivos en la red. Cree un icono para cada dispositivo que se encuentra en la red.

Para iniciar una exploración de Entorno de red:

1. Seleccione un mapa existente o crear una nueva ventana de mapa.
Para crear un nuevo mapa, en el menú Archivo, seleccione **New Map Wizard**. En el Nuevo Mapa, seleccione la opción **Discover and map network devices** en la primera pantalla y seleccione **Discover devices from your Network Neighborhood** en la siguiente pantalla.

Para añadir dispositivos en un mapa, seleccione el mapa y, a continuación, en el menú Herramientas, seleccione Descubrir Dispositivos y seleccione Descubra los dispositivos de su Entorno de red en la siguiente pantalla.

2. Haga clic en **Next** para continuar. WhatsUp muestra los posibles ámbitos para que pueda incluir en su red de exploración.
3. Seleccione dominios y haga clic en **Next**.
4. WhatsUp Gold explora su red Windows y crea un icono en el mapa para cada dispositivo que encuentre. Tenga en cuenta que esta exploración puede tomar unos minutos para completar dependiendo del tamaño de su red.
5. En el menú **File**, seleccione **Save o Save As** para guardar el mapa.

3.2.- PROPIEDADES GENERALES DE UN DISPOSITIVO

En el cuadro de diálogo General, puede realizar cambios en las propiedades generales, cambie el tipo de icono para un dispositivo, y establezca el método de rastreo que utiliza WhatsUp Gold para cada dispositivo.

Para ver o cambiar propiedades del dispositivo:

1. Haga clic derecho en el dispositivo y seleccione **Properties** en el menú emergente. Haga clic en **General**.

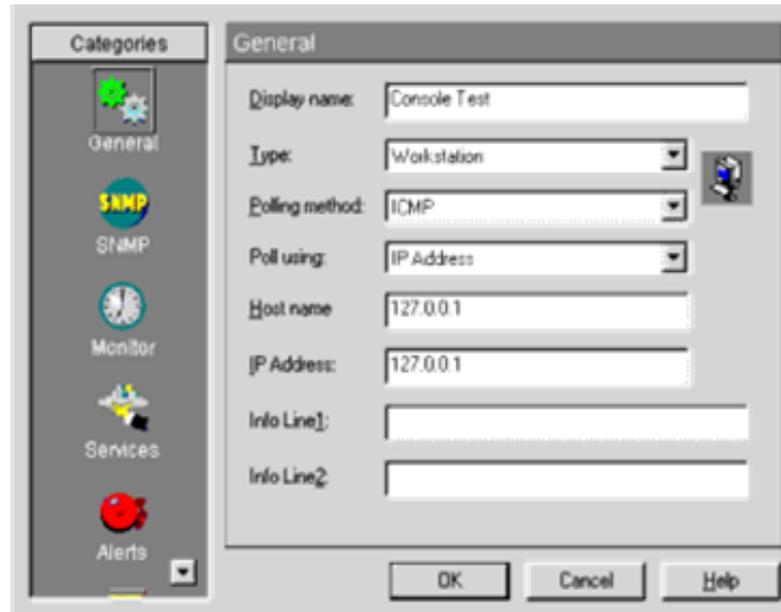


Figura 3-22. Cuadro general de propiedades de un dispositivo

2. En el cuadro **Display Name**, escriba un nombre. Este es el nombre que aparece en el mapa de red.

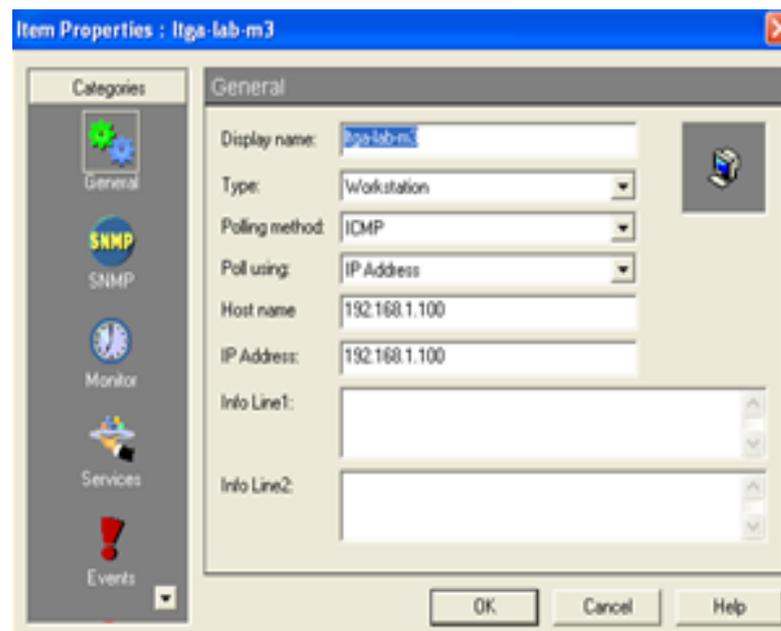


Figura 3-23. Nombre del dispositivo

3. En el cuadro **Type**, seleccione el tipo de dispositivo. Esta selección determina el icono que aparece en el mapa de red.

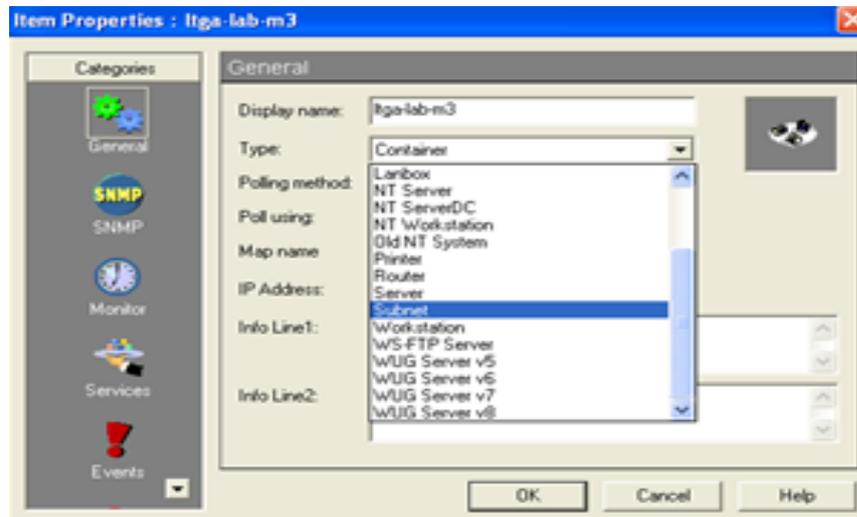


Figura 3-24. Tipo de dispositivo

4. En el cuadro de texto **Polling Method**, seleccione el método de búsqueda a utilizar para este dispositivo.
5. La búsqueda serán o dirección IP o nombre de host.
Nota: Puede alternar entre el nombre de host y dirección IP.

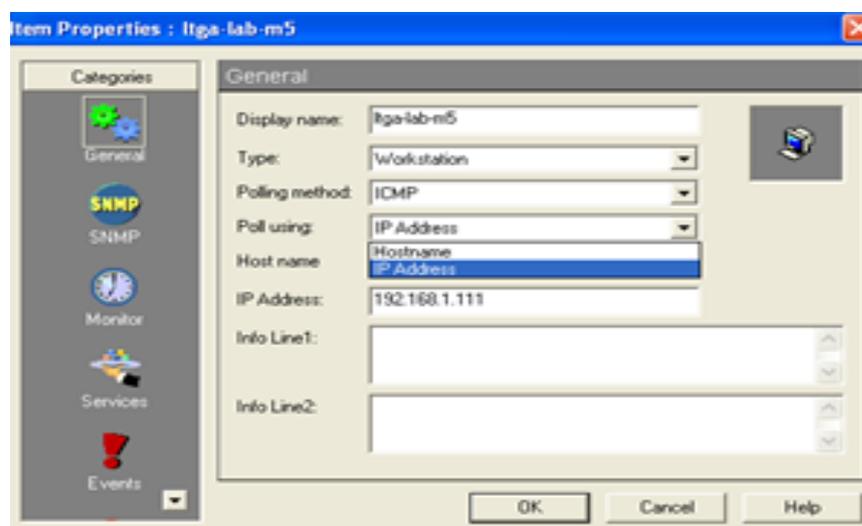


Figura 3-25. Método de búsqueda para un dispositivo

6. **Host Name.** Si el método de búsqueda es ICMP o TCP / IP, escriba el nombre de host, ya sea aquí o la dirección IP en el paso 5. Si introduce un nombre de host, debe ser un nombre que puede ser resuelto a una dirección IP. En otras palabras, el nombre de host deben estar en su sistema de archivo de host en su red o del servidor de DNS.
7. En el cuadro de texto **IP Address**, introduzca una dirección IP válida. Si el método de selección es ICMP o TCP / IP y ha introducido un nombre de host en el **Paso 5**, usted puede dejar en blanco y WhatsUp Gold utilizará el nombre de host para buscar la dirección IP.

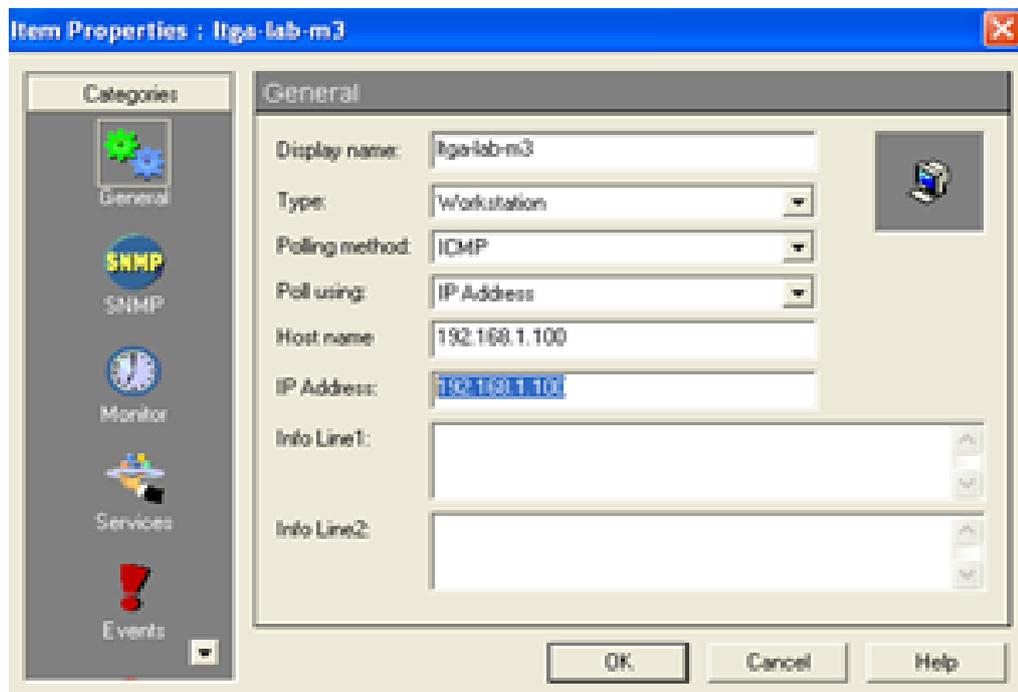


Figura 3-25. Introducción de la dirección IP

Si el método de votación es de NetBIOS o IPX, deje en blanco la dirección; WhatsUp Gold muestra la dirección Ethernet del hardware del dispositivo después de que complete una encuesta.

8. En los cuadros de texto **Info Line 1 and Info Line 2**, escriba cualquier información adicional acerca de este dispositivo.

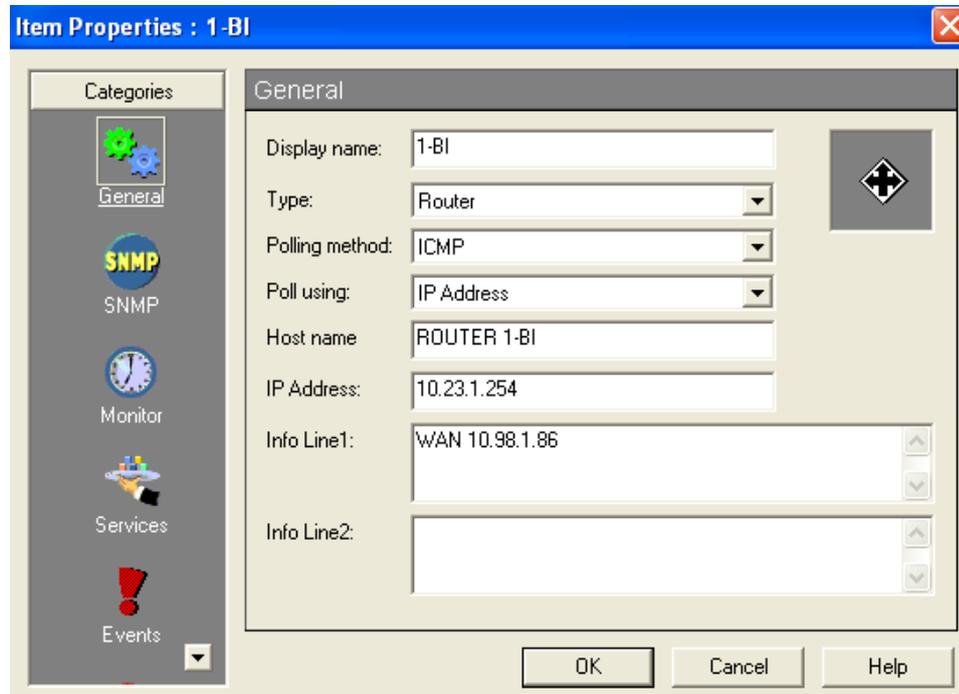


Figura 3-26. Agregar información de un dispositivo

9. Haga clic en **Aceptar** para aplicar los cambios y salir del cuadro de diálogo.

3.2.1.- CONFIGURACIÓN DE VIGILANCIA

Puede utilizar **Monitor** de vigilancia para activar o desactivar un dispositivo, para especificar con qué frecuencia, para comprobar el dispositivo, el número de segundos a esperar para una respuesta de los dispositivos de una dependencia.

1. En las propiedades del dispositivo, haga clic en **Monitor**.

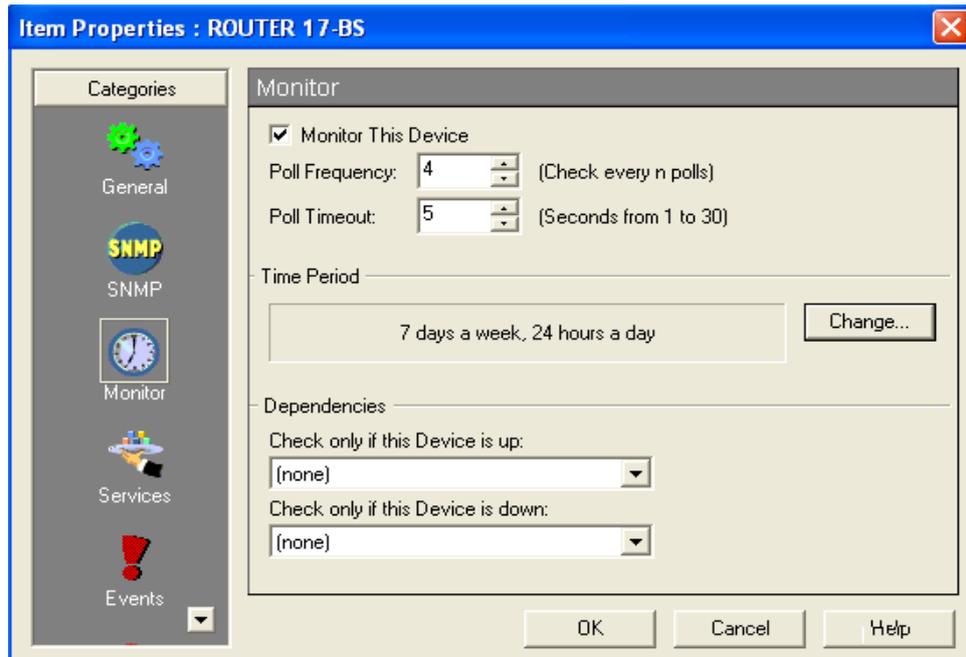


Figura 3-27. Configuración de vigilancia

2. Asegúrese de que Monitor de este dispositivo es seleccionado.
3. En el cuadro de texto **Poll Frequency**, introduzca un valor para determinar la frecuencia con que este dispositivo se debe comprobar. **Poll Frequency** determina si este dispositivo se verificará en cada búsqueda (valor = 1), cada segundo sondeo (valor = 2), cada tercer sondeo (valor = 3), y así sucesivamente. El valor por defecto en cada búsqueda es (1), pero puede utilizar esta propiedad para buscar un dispositivo con menos frecuencia.
4. En el cuadro de texto **Poll Timeout**, introduzca el número de segundos a esperar para una respuesta de un dispositivo de seguimiento. El valor por defecto es 5 segundos. Este tiempo debe ser fijado a la menor utilidad práctica. Para una red local, un tiempo de 2 segundos es generalmente suficiente. Para una larga distancia (o de lento camino), el tiempo de búsqueda puede ser tan alto como 10 segundos.

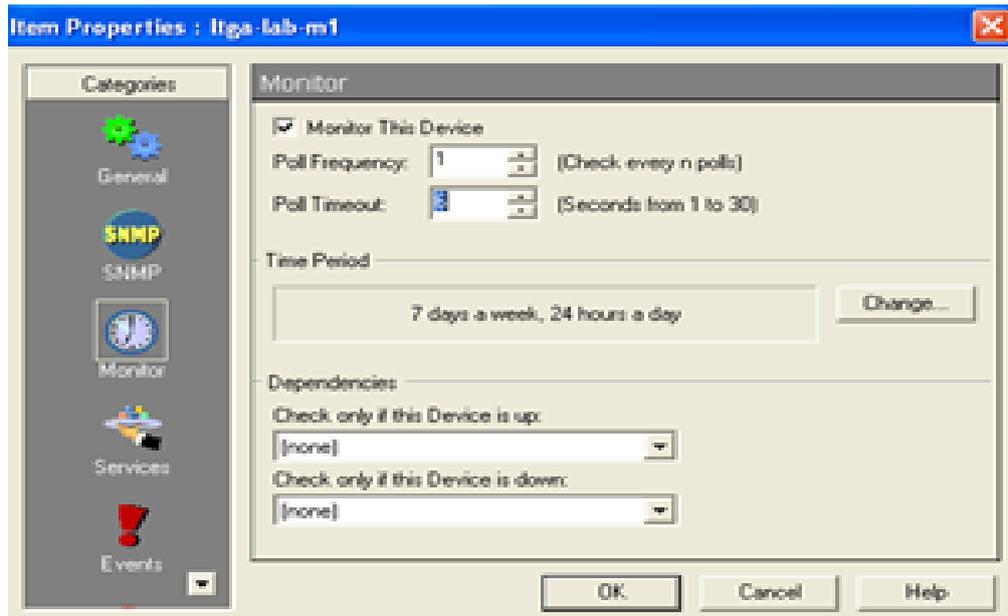


Figura 3-27. Tiempo de respuesta para un dispositivo monitoreado

5. En el cuadro **Time Period** puede establecer opciones para especificar si desea controlar este dispositivo. Haga clic en el botón **Change** para cambiar la configuración por defecto de 7 días a la semana, las 24 horas del día.

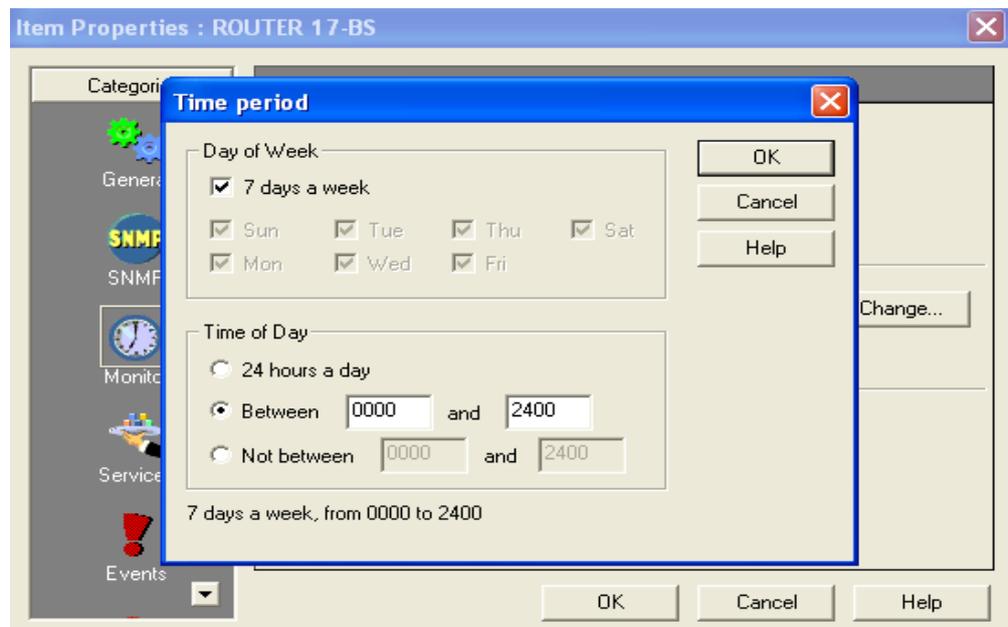


Figura 3-28. Establecer horarios de monitoreo para cada dispositivo

6. Seleccione la opción **days a week**: 7 días a la semana es el valor por defecto. Puede borrar los 7 días de la semana y luego seleccione los días de la semana que desea controlar este dispositivo.
7. Seleccione una de las opciones Hora del día: Utilice las 24 horas del día para supervisar todo el día. Use **Between** para definir el tiempo de principio y fin del seguimiento. Utilice **Not between** para establecer las horas que el control estará apagado.
8. Haga clic en Aceptar para guardar los cambios y salir del cuadro de diálogo "**TimePeriod**".
9. Haga clic en **Aceptar** para aplicar los cambios y salir del cuadro de diálogo.

3.2.2.- USO DEL MENÚ EN EL BOTON DERECHO DEL RATON

Seleccione un dispositivo y, a continuación, haga clic en el botón derecho del ratón para mostrar el dispositivo de menú emergente. Cuando esté en el modo de edición, el menú es similar a la imagen que se muestra aquí, en modo monitor, el menú tiene un menor número de comandos. Puede añadir comandos de menú que se inician las aplicaciones.



Figura 3-29. Menú del botón derecho del ratón

Los comandos de menú por defecto en el menú derecho del ratón (en modo de edición) son los siguientes:

Cut, Copy, Paste, Delete le permite cortar, copiar, pegar o borrar el dispositivo seleccionado.

New Device (Nuevo dispositivo) permite agregar dispositivos a la ruta.

Attach (Adjuntar) señala una línea del dispositivo seleccionado para el próximo objeto que haga clic.

Bring to Front. (Traer al frente). Si el elemento seleccionado es una forma de preparado, como un rectángulo o un círculo, este comando se mueve en frente de todos los demás dibujados.

Send to Back. (Enviar al fondo). Si el elemento seleccionado es una forma de extraer, por ejemplo, como un rectángulo o un círculo, este comando se mueve detrás de todos los demás dibujados.

Quick Status. Donde se puede ver el Estado, la Historia, el tiempo de registro y de Historia para este dispositivo.

Properties (Propiedades). Muestra las propiedades del dispositivo.

3.3.- CREACIÓN DE UNA SUBRED

La característica de subred WhatsUp Gold le permite crear mapas separados para los diferentes segmentos de su red, sin embargo, se mantiene una conexión entre los mapas. Si ya tiene un mapa de red matriz, puede crear un segundo mapa de red para un determinado segmento de la red y, a continuación, vincular a los padres mapa.

Para crear un mapa de subred (suponiendo que usted ya tiene un mapa padre):

1. Crear un mapa nuevo y agregar los dispositivos de la subred. Puede utilizar cualquiera de los métodos para la creación de un mapa de red se describe

en la sección anterior. También puede copiar y pegar los dispositivos existentes de un mapa.

2. Guarde el nuevo mapa.
3. Abra el mapa de los padres si aún no está activo o abierto.
4. Haga clic en el botón **Edit Mode** para ver las barras de herramientas de edición.



Figura 3-30. Icono subred

5. Haga clic en el icono **Subnet** y arrástrelo en la red que desea crear el icono de la subred.
6. Haga clic derecho en el icono de subred, seleccione **Properties** y haga clic en **General**.
7. En el cuadro de texto **Display Name**, escriba el nombre de archivo de la subred, no el mapa titular o padre. Este debe ser el nombre del archivo. WUP archivo sin la extensión del archivo. Por ejemplo, si la subred se denomina archivo de mapa SubnetA.wup, introduzca SubnetA aquí.
8. Haga clic en **Monitor**, asegúrese de que este ítem del monitor está seleccionado.
9. Haga clic en **Aceptar**.
10. Haga clic en el botón **Edit Mode** para regresar a modo de monitor.
11. Cuando se abre un mapa de red, WhatsUp Gold también puede abrir cualquier mapa asociado o subred y empezar el control. (Desde el menú **Configurar**, seleccione **Programa Opciones -> General** y, a continuación, seleccione **cargar automáticamente subredes al abrir los mapas**.)

Si una subred mapa ventana no se abre, puede hacer clic derecho en la subred y seleccione el icono de carga de subred en el menú para abrirlo.

Si una subred mapa está abierta, pero se oculta detrás de otras ventanas, puede hacer clic derecho en el icono de subred y seleccione **View Subnet**.

3.4.- CONFIGURACIÓN DE PROPIEDADES DEL MAPA

Abra la ventana de mapa para el mapa de red. Haga clic derecho en un área vacía del mapa para visualizar el menú derecho del ratón y seleccione **Propiedades**. Haga clic en **General**.

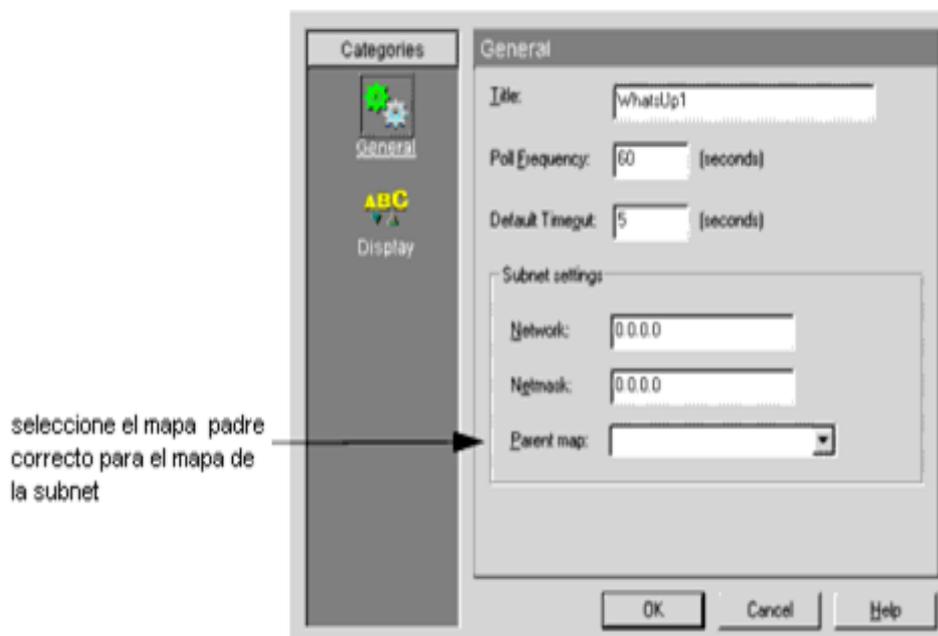


Figura 3-31. Configuración de propiedades del mapa

Title. (Título). Este título se utiliza para identificar un mapa de red en el mapa de la ventana y cuando se accede desde un navegador web. Usted debe tener cuidado acerca de cómo cambiar el título, ya que también se utiliza para comunicar información en caso de Estadística y los registros. Votaciones estadísticas se guardan en el [título. Wui] archivo. El Estado, sus dependencias,

Estadísticas y Notificaciones de Windows mostrar información por mapa y utilizar el título.

Poll Frequency. (Encuesta de frecuencia). Este es el número de segundos entre el comienzo de una encuesta del mapa. Puede introducir un valor en el rango 10 a 3600. La línea de estado de cada ventana de Mapa muestra un temporizador de cuenta regresiva que de este número a cero antes de comenzar cada encuesta. El temporizador de cuenta regresiva continúa durante las encuestas: si la anterior encuesta no está completa cuando el cronómetro llega a cero, una nueva encuesta no se ha iniciado.

Default timeout (Tiempo de espera predeterminado). Este es el número de segundos a esperar para una respuesta de un dispositivo buscado. Este valor por defecto se asigna a los nuevos dispositivos que se añaden al mapa.

Subnet Settings (Configuración de subred). El principal objetivo de estas opciones es establecer un mapa de los Padres para el mapa actual. Si ha creado el mapa utilizando SmartScan, cada subred mapa ya dispone de una entrada para el mapa padre. Para cambiar el mapa de los Padres, seleccione cualquiera de los mapas se muestra en el cuadro de lista. Esta lista muestra todos los mapas abiertos

Netmask. (Máscara de red). Muestra la máscara de red para este segmento de la red. La máscara de red define la forma de leer la dirección IP para identificar los dispositivos y subredes.

3.4.1.- AJUSTE DE MAPA DE COLORES

Para cambiar el mapa de colores:

Para establecer los colores por defecto para cada mapa, desde el menú **Configure**, seleccione **Program Options** y haga clic en **Map Colors**.

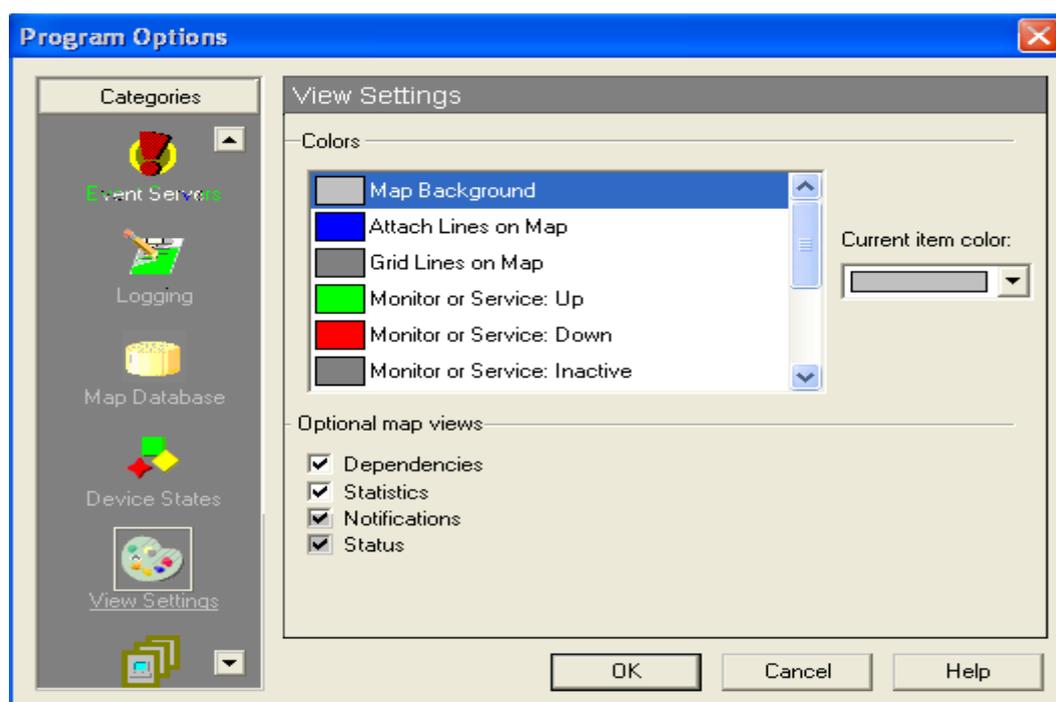


Figura 3-32. Mapa de colores

Para cambiar el color de un elemento, seleccione **Map Colors** en la casilla. En el cuadro de texto **Current Item Color** seleccione el color que desee. La configuración actual de un nombre se muestra en el cuadro de lista.

3.4.1.1.- Estado de los dispositivos.

Para ver las formas y colores por defecto para los dispositivos a medida que pierda las búsquedas, desde el menú **Configure**, seleccione **Program Options** y haga clic en **Device States**.

Si desea cambiar la configuración por defecto, en el Conjunto de color para la columna, seleccione el estado del dispositivo que desea cambiar. Después de seleccionar, puede cambiar el color de la línea, de relleno de color, o forma para satisfacer sus necesidades.

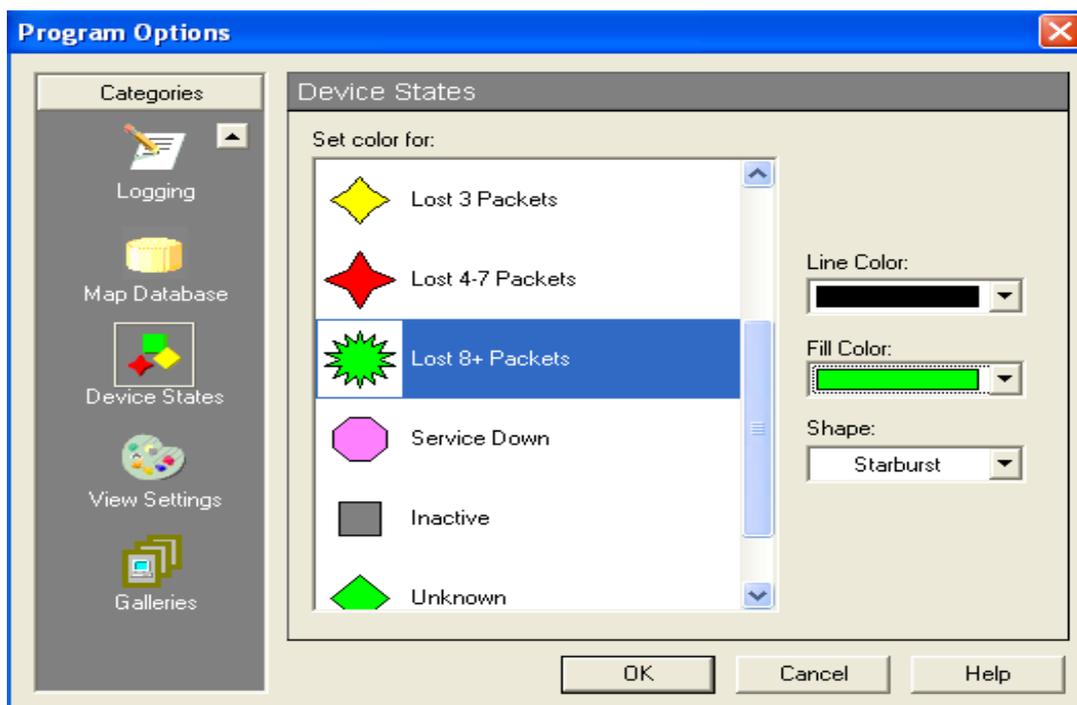


Figura 3-33. Estado de los dispositivos

Responding. (Responder). Este es el color que indica que un dispositivo está respondiendo a las encuestas. El valor por defecto es sólido verde brillante.

Lost 1 pkt. (Perdió 1 pkts). El color que indica que un dispositivo no ha respondido a una encuesta. El valor por defecto es sólido de color verde claro.

Lost 2 pkts (Perdió a 2 pkts). El color que indica que un dispositivo no ha respondido en dos encuestas consecutivas. El valor por defecto es sólido amarillo.

Lost 3 pkts. (Perdió 3 pkts). El color que indica que un dispositivo no ha respondido en tres encuestas consecutivas. El valor por defecto es sólido amarillo.

Lost 4-7 pkts (Perdió 4ta-7ma pkts). El color que indica que un dispositivo no ha respondido en los sondeos de cuatro a siete. El valor por defecto es sólida luz roja.

Lost 8+ pkts. (Perdió 8 + pkts). El color que indica que un dispositivo no ha respondido en ocho o más encuestas o tiene un error de red. El valor por defecto es sólido de color rojo oscuro.

Service down. (Servicio abajo). El color que indica que un servicio se ha reducido en un dispositivo. El valor por defecto es sólido púrpura.

Inactive. (Inactivo). El color que indica que un dispositivo que no se supervisa. El valor por defecto es sólido gris oscuro.

3.5.- EDICIÓN DE UN MAPA DE RED

Puede utilizar el modo de edición para mover el dispositivo en torno a los iconos en la ventana del mapa. Cuando esté en modo de edición, puede utilizar herramientas para:

- Añadir y eliminar iconos de dispositivo
- Cortar, copiar y pegar dispositivo iconos y objetos dibujados
- Dibujar, el color, tamaño y formas gráficas para organizar visualmente elementos de la red.

3.5.1.- COMO ENTRAR Y SALIR DEL MODO DE EDICIÓN

Para acceder a modo de edición, asegúrese de que el mapa que desea editar está activo, haga clic en el botón de modo de edición en la barra de herramientas principal. La edición de las barras de herramientas aparece.

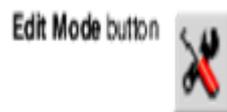


Figura 3-34. Botón para modo de edición

Cuando está en modo de edición WhatsUp Gold detiene el monitoreo de los dispositivos.

Para salir del modo de edición y volver al modo de monitor, haga clic de nuevo el botón **Edit Mode** .Las barras de herramientas desaparecen.

3.5.1.1.- Líneas Adjunto

Además de las líneas de mano que se comportan como cualquier otro objeto dibujado, también puede utilizar las líneas adjunta.

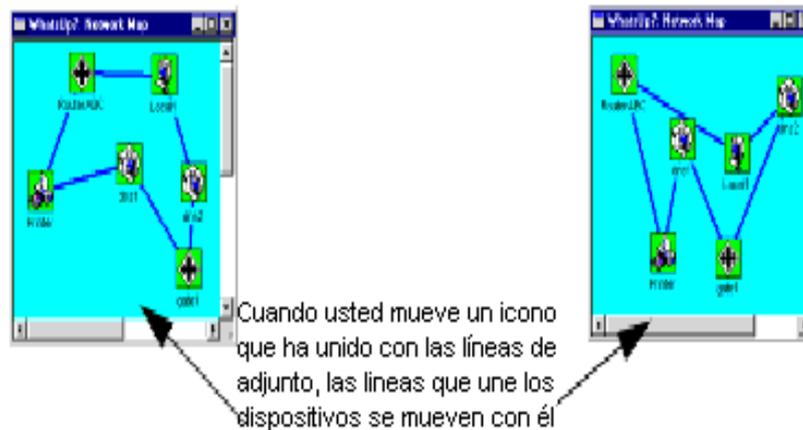


Figura 3-35. Líneas de adjunto

Se puede conectar un dispositivo a un máximo de otros cinco aparatos u objetos dibujados. Para conectar de un dispositivo a otro debes estar en modo de edición.

1. Haga clic derecho en el icono del dispositivo que desea dibujar una línea adjunta.
2. Seleccione **Attach to**, el cursor se convierte en una línea de caracteres.
3. Haga clic en el elemento al que desea conectar el dispositivo.

Para desconectar cualquier línea adjunta que tienen su origen en el dispositivo seleccionado:

1. Haga clic derecho en el dispositivo.
2. Seleccione **Disconnect** en el menú derecho del ratón.

3.5.1.2.- Creación de títulos de texto

Puede utilizar títulos de texto para identificar un mapa de red o segmentos de un mapa. Está disponible en muchos tipos de letra, tamaño, efectos de texto, y colores.

Para agregar texto al mapa de red:

1. Haga clic en el botón de **Edit Mode**.
2. Seleccione el botón **Text** y haga clic en el mapa en el que desea el texto.



Figura 3-36. Botón de texto

3. Aparece el cuadro de diálogo de **Text Properties**. En el cuadro de texto, sustituir la muestra de texto con el texto deseado.
4. Ajuste el color del texto, el color de fondo, grados de rotación, y Estilo de la fuente, según proceda.
5. Haga clic en **Aceptar**.

3.6.- CONFIGURACIÓN DE NOTIFICACIONES

Se puede definir los diferentes tipos de notificaciones utilizando el Editor de Notificaciones. Para acceder al Editor de Notificaciones realice lo siguiente:

Desde el menú **Configurar**, seleccione **Notifications Library**.

3.6.1.- DEFINIENDO EL SONIDO DE NOTIFICACIÓN

En la notificación de sonido suena una alarma cuando un dispositivo o servicio se cae.

Para definir un sonido de notificación:

1. Desde el menú **Configurar**, seleccione **Notifications Library** y, a continuación, seleccionar Sonido.

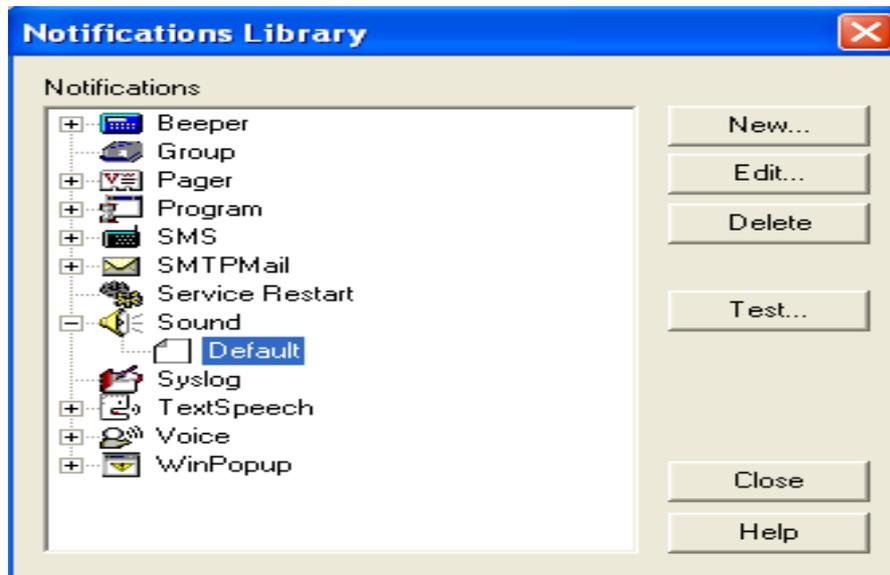


Figura 3-37. Definiendo el sonido de notificación

2. Haga clic en **Add** y escriba un nombre único para la notificación.
3. En el cuadro de texto **Filename**, vaya a la **Browse** deseada. Hay una "Grabadora de sonidos" puedes hacer clic en el botón para escuchar el sonido que acaba de seleccionar.



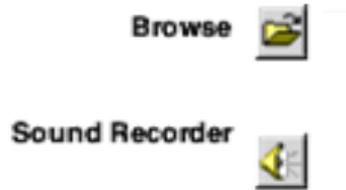


Figura 3-38. Alarmas WAV

4. Opcionalmente, seleccione la casilla de verificación **Continuos Play** para reproducir el sonido continuamente, hasta que se apaga manualmente (haciendo clic en el botón Silencio en la barra de herramientas principal).



Figura 3-39. Reproducción de alarmas WAV

5. Haga clic en **Aceptar**.

3.6.2.- DEFINIENDO LA NOTIFICACIÓN WINPOPUP

Para definir una notificación WinPopup:

1. Desde el menú **Configurar**, seleccione **Biblioteca de Notificaciones** y, a continuación, seleccione **WinPopup**.

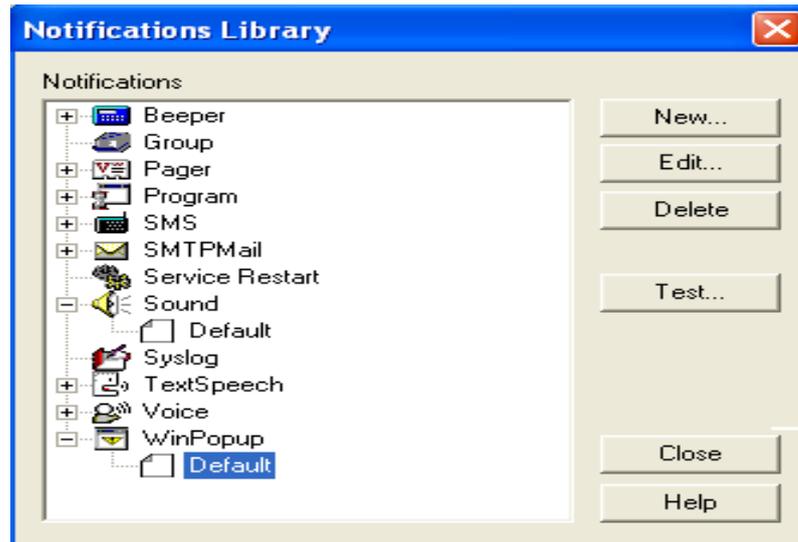


Figura 3-40. Definiendo notificación WinPopup

2. Haga clic en **Agregar** y escriba un **nombre** único para la notificación en el cuadro de texto **Display Name**.

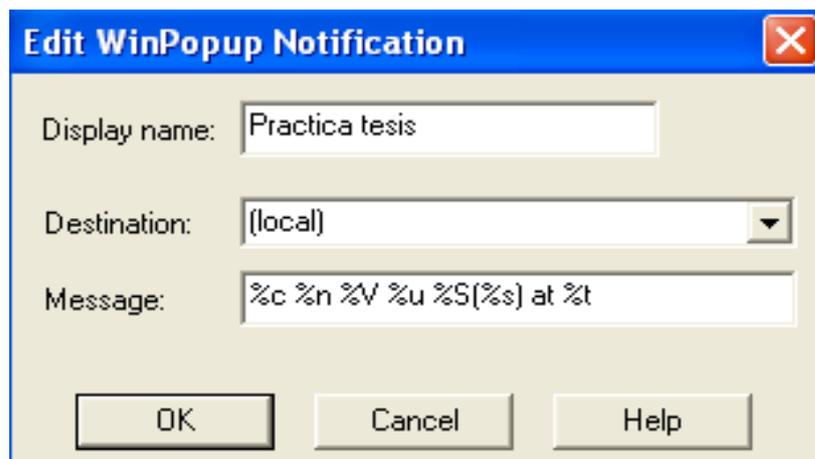


Figura 3-40. Agregar nombre a la notificación

3. En el cuadro de lista **Destination**, especifique el host de Windows NT o el dominio que desea recibir esta notificación. Tenga en cuenta que un dominio está marcado con un asterisco (*).

4. En el cuadro de texto **Message**, escriba un mensaje de texto más las variables de la notificación.
5. Haga clic en **Aceptar**.

3.7.- SERVICIOS DE VIGILANCIA

Cuando desee controlar los servicios (ya sea estándar o personalizado), es necesario realizar los siguientes cambios a las propiedades del dispositivo:

1. En el cuadro de diálogo **Monitor** de las propiedades del dispositivo, seleccione **Monitor This Device**.
2. Utilice el cuadro de diálogo **Services** de las propiedades del dispositivo para seleccionar **Services to Monitor** en el dispositivo.

3.8.- TRABAJO DE LA CONSOLA

La consola WhatsUp Gold es el sistema en el que está instalado la herramienta. Este capítulo describe cómo utilizar la consola para iniciar y detener la votación de los dispositivos en su red y el mapa de cómo mostrar el estado de la red.

3.8.1.- INICIAR AUTOMATING POLLING

Cuando se abre un mapa de red, WhatsUp Gold inmediatamente lo monitorea con sus correspondientes mapas de subred.

Para cambiar la configuración predeterminada de monitoreo automático, haga clic derecho en un espacio en blanco en el mapa y seleccione **Propiedades**.

En el mapa de propiedades que aparece haga clic en **General** y fijar el número de segundos que desea entre los controles (**Poll Frequency**), el número de segundos a esperar antes de una respuesta (**Default Timeout**), y cualquier otra opción es posible que desee cambiar.

Stopwatch button



Figura 3-41. Botón para monitoreo automático

En caso de que el monitoreo se detenga, se puede reiniciar automáticamente haciendo clic en el botón **Cronómetro** en la barra de herramientas principal.

WhatsUp Gold controla cada dispositivo y pide respuestas. Después de esperar el plazo establecido, en **Poll Frequency** se hace un segundo monitoreo a través de los dispositivos y continúa sucesivamente hasta que deje de monitorear haciendo clic en el botón **Stopwatch** o cerrando la ventana del mapa.

WhatsUp Gold busca los dispositivos en el orden en que fueron creados en el mapa de red.

3.8.2.- PARAR AUTOMATING POLLING

Para detener temporalmente el monitoreo automático, haga clic en el botón **Stopwatch** (Cronómetro) en la barra principal de herramientas. Para reanudar el monitoreo, haga clic de nuevo **Stopwatch**.

3.8.3.- LECTURA DEL MAPA DE RED

De forma predeterminada, las siguientes convenciones se usan en la ventana del mapa para indicar el estado de un producto o servicio:

Relieve en el nombre del dispositivo.- Un caso se ha registrado para el dispositivo

Icono de dispositivo de color verde (en forma de un cuadrado de fondo).- El dispositivo está "arriba" (en respuesta al monitoreo).

Icono de luz verde (en forma de diamante de fondo).- El dispositivo ha perdido al menos una solicitud de monitoreo.

Icono de color amarillo (en forma de diamante de fondo).- El dispositivo ha perdido dos peticiones de monitoreo.

Icono rojo (en forma alargada diamante de fondo).- el dispositivo está "abajo" (que no es accesible o no ha respondido a las cuatro solicitudes de monitoreo). Después de que un dispositivo falla a 8 solicitudes de monitoreo, el fondo se convierte en una forma Starburst.

Icono Morado (con un fondo en forma de octágono).- un servicio estándar en el dispositivo está inactivo.

3.8.4.- RECEPCIÓN DE ALARMAS

Si Activado Alertas (Alertas sobre el cuadro de diálogo de propiedades del dispositivo), ha seleccionado, y ha añadido un aviso, se produce una alerta cuando un dispositivo no responde a cuatro (por defecto) solicitudes consecutivas, Para reproducir una alerta sonora, debe tener una tarjeta de sonido instalada en su sistema.



Figura 3-42. Botón para silenciar una alarma

Para silenciar una alerta sonora, haga clic en el botón **Quiet** en la barra de herramientas principal, o desde el menú del monitor, seleccione. **Stop Alarm.**

3.8.5.- UTILIZANDO QUICK ESTADO

Para mostrar la información de estado asociados con cualquiera de los dispositivos de muestra (activo o inactivo), haga clic derecho en el dispositivo, seleccione **Quick Estado**, y haga clic en Condición **Status** para mostrar información de estado actual.

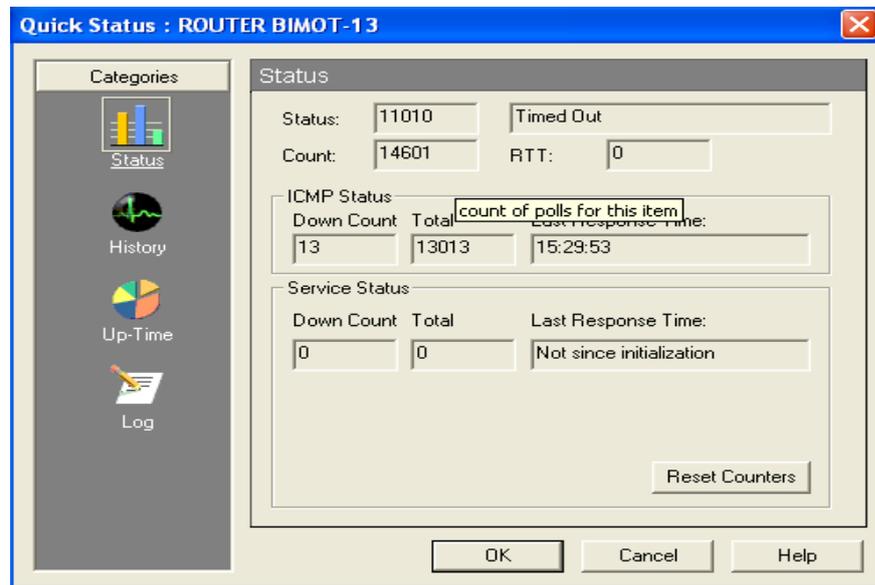


Figura 3-43. Ventana de estado de un dispositivo

El cuadro de diálogo **Status** muestra el estado de los paquetes enviados por WhatsUp Gold a la búsqueda de este dispositivo y un mensaje de estado actual.

Status.- Estado actual del dispositivo. Un cero código de estado indica que el dispositivo está en marcha. Un código numérico de estado por encima de 10000 es un código de error Winsock. El texto para el mensaje de error también se muestra.

Count.- Número total de veces que este dispositivo se encuestados.

RTT.- Tiempo ida y vuelta (RTT) es el tiempo (en milisegundos) que tomó el último paquete enviado para llegar a el dispositivo y volver.

ICMP Status.- Muestra los siguientes tres puntos para el estado del dispositivo y el Estado del Servicio:

Down Count.- Cuántas encuestas han pasado desde el dispositivo o servicio última respondió.

Total.- Recuento total del número de encuestas se produjeron cuando el producto o servicio no ha respondido desde el mostrado la última vez.

Last Response Time.- Hora del día (en horas: minutos: segundos) de la última respuesta.

3.8.6.- USO DE LA VENTANA DE ESTADO

La ventana de estado muestra una lista de los dispositivos activos que están actualmente en el mapa y muestra el estado utilizando los mismos colores utilizados en el mapa. También se indica la situación de los servicios objeto de un seguimiento.

En el menú Ver, seleccione **Status**.

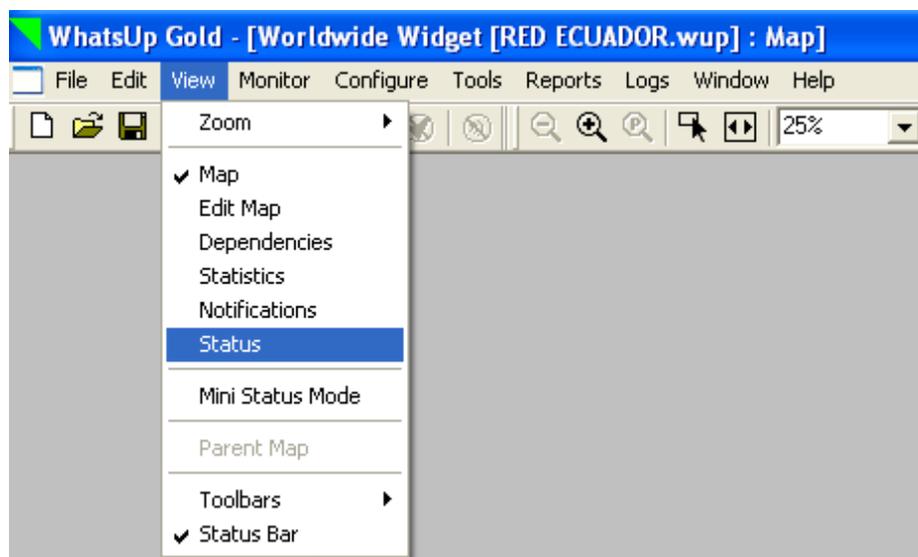


Figura 3-44. Selección para ver estado de un dispositivo

Usted puede controlar la red a través de la ventana de estado. Usted necesita ampliar la ventana de **Status**, a fin de leer el servicio de información de estado.



Figura 3-45. Ventana de dispositivos activos utilizando colores

En la barra de herramientas principal, haga clic en el botón **Poll** para iniciar la búsqueda, un solo control para cada dispositivo en la ventana de estado. Haga clic en el botón **Stopwatch** para iniciar el monitoreo automático de cada dispositivo.



3.9.- REGISTROS Y REPORTE

WhatsUp Gold tiene tres tipos de registros de datos:

Eventos - Los eventos son cambios en el estado de la red, como un dispositivo o bajando una copia de seguridad de dispositivo próximos. Los eventos se registran en el registro de eventos (EV-aa-mm-dd.tab), que proporciona una historia de lo

que ha ocurrido en la red. Además, el registro de depuración proporciona una ventana de vista de los acontecimientos a medida que se producen.

Estadísticas de monitoreo.- Las estadísticas de monitoreo son los tiempos acumulados de ida y vuelta (RTT), de encuestas enviadas a un dispositivo. Estas estadísticas miden la disponibilidad y el desempeño de un dispositivo. Estadísticas electorales se registran en el Registro de Estadística (ST-aaaa-mm-dd.tab).

SNMP Traps.- Muestra todos los registros SNMP que se han recibido. Al utilizar este asistente, todas las trampas se pueden ver (a diferencia de utilizar "Quick estatus" en un dispositivo). Para habilitar SNMP, vaya a **Configuración > Opciones de Programa > SNMP Traps** y seleccione Habilitar trampa SNMP.

De estos datos registrados, WhatsUp Gold puede crear varios informes y gráficos que muestran el estado de su red de diferentes maneras.

3.9.1.- CREACIÓN DE UN INFORME DE EVENTO

Para crear un Informe del evento:

1. Desde el menú **Reports** seleccione **Event Report**, en el cuadro de diálogo de Event Report aparece.

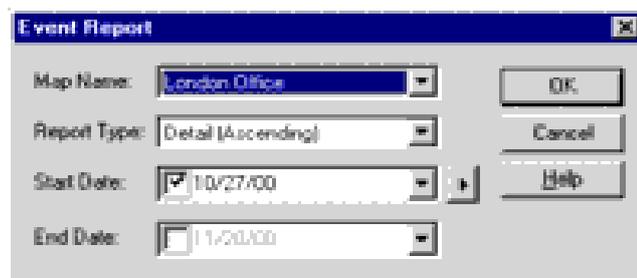


Figura 3-46. Configuración de reporte de eventos

2. En el cuadro de texto **Map Name** Seleccione la ruta para la cual desea un informe.
3. Seleccione **Report Type**.

Summary (Resumen). Total de informes de servicio caído para cada dispositivo, tiempo para cada tipo de dispositivo y el nombre del dispositivo por clase en orden ascendente o descendente.

Detail. (Detalle). Informes de todos los eventos de rendimiento para cada dispositivo, informa el tiempo de inactividad transcurrido. El informe ordena los dispositivos por nombre en orden **ascendente** o **descendente**.

También puede ordenarlos en orden **Worst First**, lo que significa que el dispositivo con más tiempo de inactividad se presenta en primer lugar.

Raw Data (datos en bruto). Los datos están ordenados por fecha y hora en orden ascendente.

4. Seleccione el intervalo de fechas para el informe.
Cuando se selecciona una opción, se muestran la **fecha de inicio** y **finalización**.

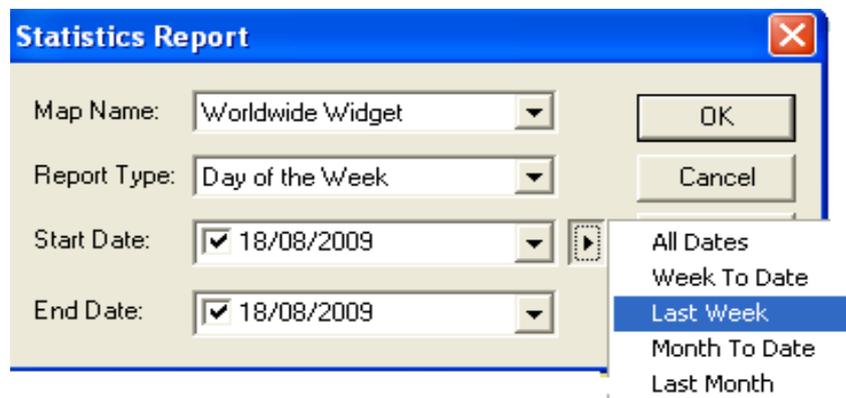


Figura 3-47. Configuración de reporte de eventos

El valor por defecto incluye todos los días desde que empezó el seguimiento de la ruta, haciendo clic en **Borrar Clear** se borra datos en el registro de sucesos desde el último.

5. Haga clic en **Aceptar** para generar el informe.

WhatsUp Gold genera el informe especificado y lo muestra en la ventana **From the Report Window**, puede guardar los datos a un archivo, imprimir o copiar los datos a otra aplicación.

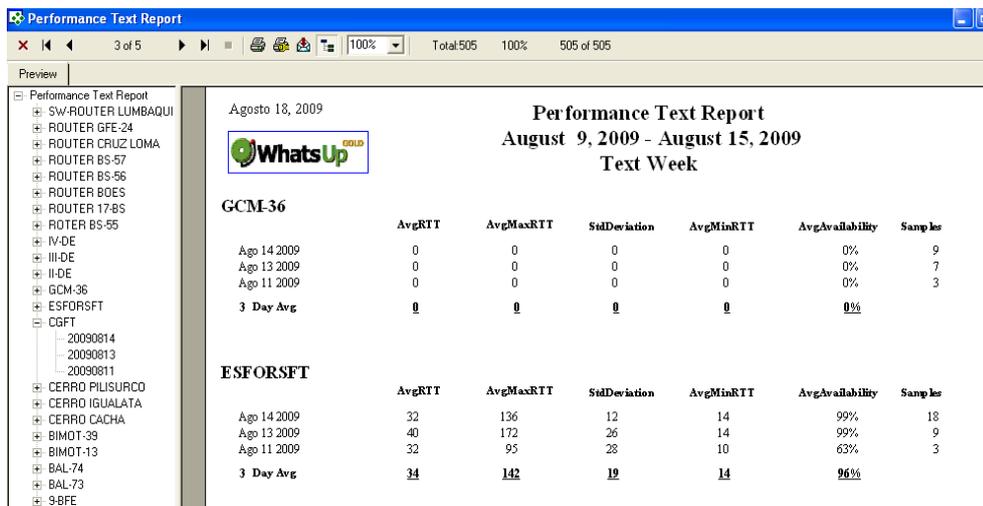


Figura 3-48. Reporte de eventos

Si recibe el mensaje de "datos insuficientes", es posible que usted no haya supervisado el mapa durante el tiempo suficiente para generar datos de eventos.

3.9.1.1.- Depuración de los registros de información

Todas las acciones, como la búsqueda de las solicitudes de servicio y los controles efectuados por WhatsUp Gold, se muestran en la ventana de registro de depuración. Depurar el registro en un tiempo real muestra como se producen los

acontecimientos. Para ver el registro, desde el menú, **Logs** seleccione, **Debug Log**.

3.9.2.- CREACIÓN DE UN INFORME DE ESTADÍSTICAS

Después de que WhatsUp Gold ha supervisado un mapa durante el tiempo suficiente para generar estadísticas, puede crear informes basados en las estadísticas.

Para crear un informe de las estadísticas:

1. Desde el menú **Reports**, seleccione **Statistics Report**.

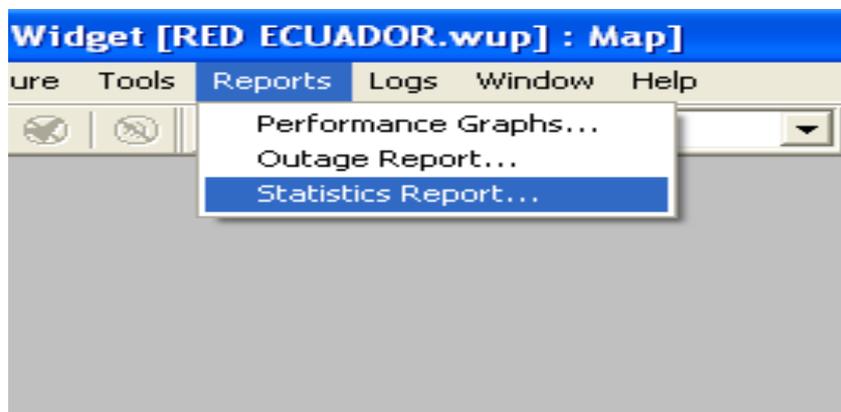


Figura 3-49. Configuración reporte de estadísticas

2. En el cuadro de texto **Map Name** Seleccione la ruta para la cual desea hacer un informe.

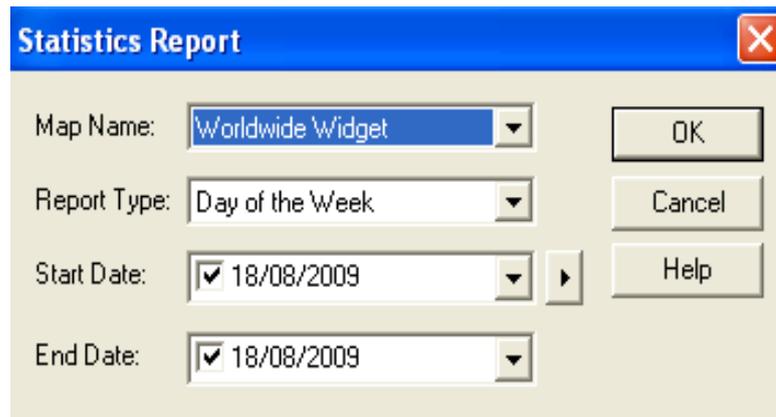


Figura 3-50. Ruta de informe

3. Seleccione el tipo de informe.

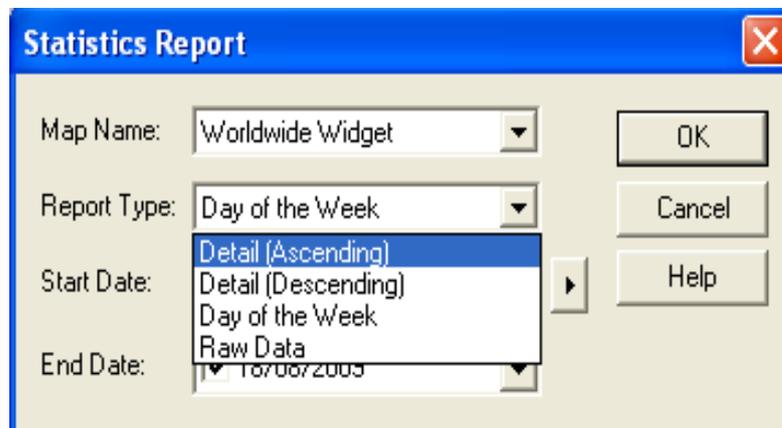


Figura 3-51. Tipo de informe

Detail. (Detalle).- Informe de estadísticas de votación para cada tipo de dispositivo y el nombre del dispositivo en orden ascendente o descendente. Las estadísticas se calculan a partir de los datos en el Registro de Estadísticas.

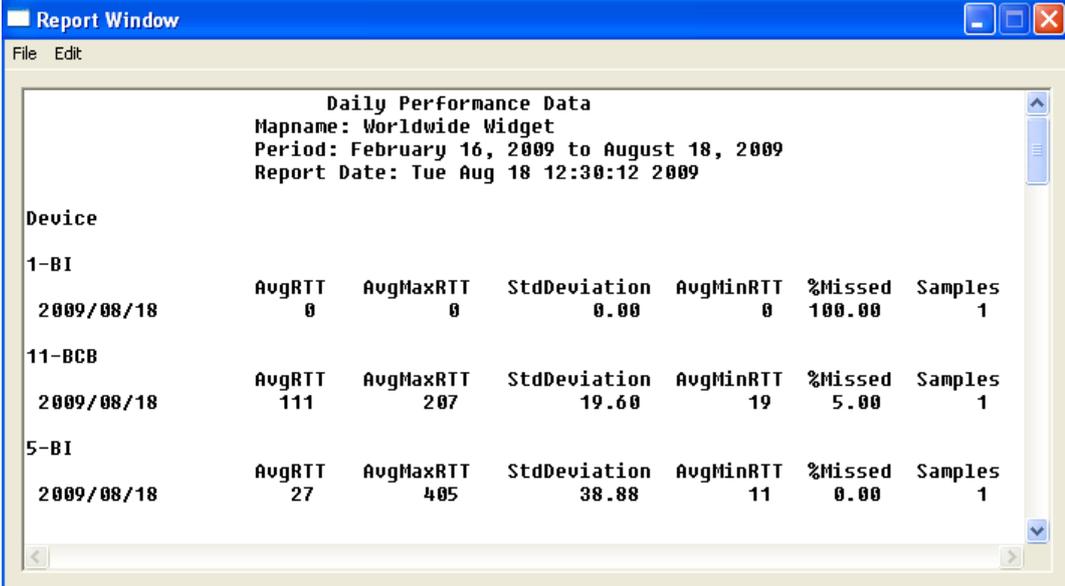
Raw Data. (Datos en bruto). Guardar los datos de las Estadísticas del Registro a un formato delimitado por tabuladores que pueden importarse

por otra aplicación. Los datos están ordenados por orden dispositivo monitoreado.

Day of the Week. (Día de la semana). Por cada día de la semana, se informa los eventos de rendimiento para cada dispositivo, informa el tiempo de inactividad transcurrido. Seleccione el intervalo de fechas para el informe. Cuando se selecciona una opción, la fecha de inicio y finalización se muestran.

4. Haga clic en **Aceptar** para generar el informe.

WhatsUp Gold genera el informe especificado y lo muestra en la ventana **From the Report Window**, puede guardar los datos a un archivo, imprimir o copiar los datos a otra aplicación.



Daily Performance Data
Mapname: Worldwide Widget
Period: February 16, 2009 to August 18, 2009
Report Date: Tue Aug 18 12:30:12 2009

Device	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	%Missed	Samples
1-BI 2009/08/18	0	0	0.00	0	100.00	1
11-BCB 2009/08/18	111	207	19.60	19	5.00	1
5-BI 2009/08/18	27	405	38.88	11	0.00	1

Figura 3-52. Informe generado por WhatsUp Gold

Si recibe el mensaje de "datos insuficientes", es posible que usted no ha supervisado el mapa durante el tiempo suficiente para generar las estadísticas de votación.

3.9.2.1.- Exportación de datos en bruto

Como se ha mencionado anteriormente, puede crear un archivo de datos en bruto de la Estadística Informe. El archivo de datos en bruto puede ser importado por otra aplicación.

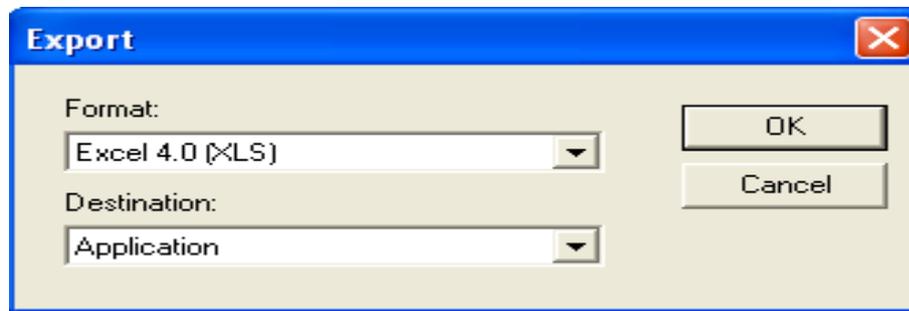
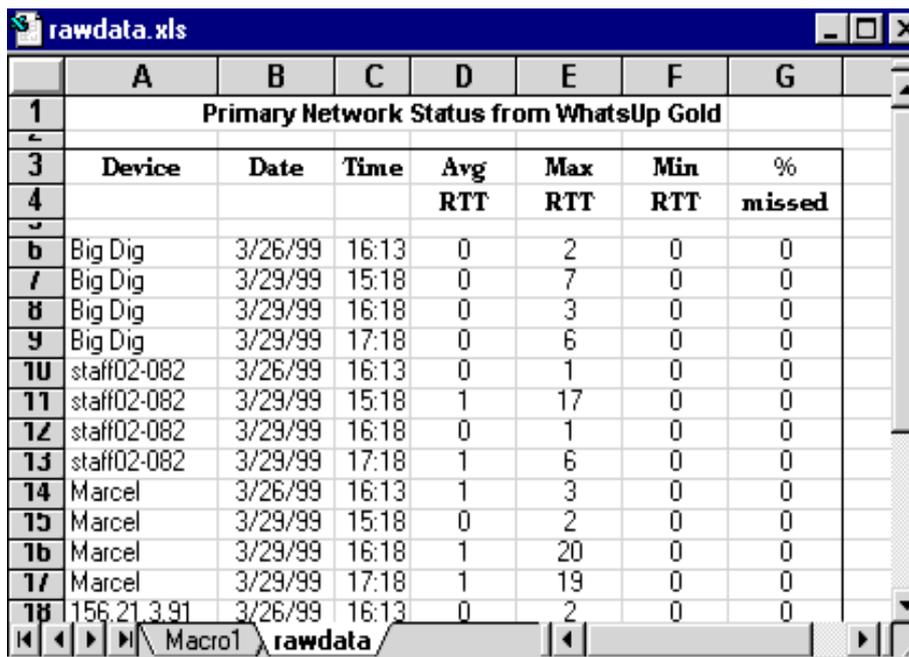


Figura 3-53. Exportar un informe a otro formato

Por ejemplo, una aplicación de hoja de cálculo.



	A	B	C	D	E	F	G
1	Primary Network Status from WhatsUp Gold						
3	Device	Date	Time	Avg RTT	Max RTT	Min RTT	% missed
4							
6	Big Dig	3/26/99	16:13	0	2	0	0
7	Big Dig	3/29/99	15:18	0	7	0	0
8	Big Dig	3/29/99	16:18	0	3	0	0
9	Big Dig	3/29/99	17:18	0	6	0	0
10	staff02-082	3/26/99	16:13	0	1	0	0
11	staff02-082	3/29/99	15:18	1	17	0	0
12	staff02-082	3/29/99	16:18	0	1	0	0
13	staff02-082	3/29/99	17:18	1	6	0	0
14	Marcel	3/26/99	16:13	1	3	0	0
15	Marcel	3/29/99	15:18	0	2	0	0
16	Marcel	3/29/99	16:18	1	20	0	0
17	Marcel	3/29/99	17:18	1	19	0	0
18	156.21.3.91	3/26/99	16:13	0	2	0	0

Figura 3-54. Datos exportados a Excel

CAPÍTULO IV

RESULTADOS DEL SISTEMA

En este capítulo se conocen los resultados y las pruebas finales de la aplicación del sistema WhatsUp Gold para el monitoreo de redes. Por lo tanto se mencionan entre otros puntos, los resultados de la interacción por parte del usuario, las características en materia de seguridad, el esquema de la red de área local que se monitorea, las pruebas generales de la aplicación y por último el manual de usuario del sistema.

4.1.- RESULTADOS DE LA INTERACCIÓN DEL USUARIO CON EL SISTEMA

La aplicación tuvo como objetivo principal facilitar la elaboración del manual de configuración y uso de la misma para el monitoreo de redes, se puede decir que se cumplieron todas las características del sistema de monitoreo de redes WhatsUp Gold mencionadas en el Capítulo II y en general se resumen en los siguientes puntos:

El usuario interactúa con la tecnología de WhatsUp Gold gracias a su sencilla interfaz gráfica, por lo tanto se siente más seguro al momento de usar este tipo de aplicaciones.

Las interfaces para el usuario son muy amigables y hace que se sienta con libertad de interactuar por completo con el sistema, siempre y cuando se realicen las tareas para las cuales fue creada WhatsUp Gold.

4.2.- CARACTERÍSTICAS EN MATERIA DE SEGURIDAD A TOMAR EN CUENTA

El servidor que nos proporciona el acceso a los servicios que nos brinda WhatsUp Gold, debe tener características en materia de seguridad que nos permita estar tranquilos y saber que el acceso a la información se encuentra limitada a ciertos

usuarios y los cuales se encuentran identificados por el administrador del sistema y por el sistema mismo.

Se debe tener especial cuidado en los puntos faltantes los cuales son: Equipos indebidamente configurados (puede haber un punto de acceso por parte de usuarios indebidos), aunque esto se considera difícil ya que se necesita conocer a detalle cómo y de qué manera se configuró en este caso el servidor y el sistema en general.

Otro punto importante es tener una revisión constante de la base de datos, realizar su debido backup y respaldo de la información.

Seguridad en el equipo: El equipo debe encontrarse protegido principalmente por un anti-virus actualizado para evitar problemas y fallas en la parte de Hardware.

4.3.- RED UTILIZADA PARA EL USO DE LA APLICACIÓN

En esta parte se describe a grandes rasgos la red utilizada para la aplicación, la cual nos sirve para obtener los reportes y estadísticas necesarias para saber qué es lo que está sucediendo en la red.

A continuación se muestra un esquema por el cual se conoce cada uno de los nodos que forman parte de nuestra red a analizar y la cual pertenece a la red de las unidades del Ejército Ecuatoriano, cabe destacar que se monitorea el total de las computadoras que existen en el Ejército.

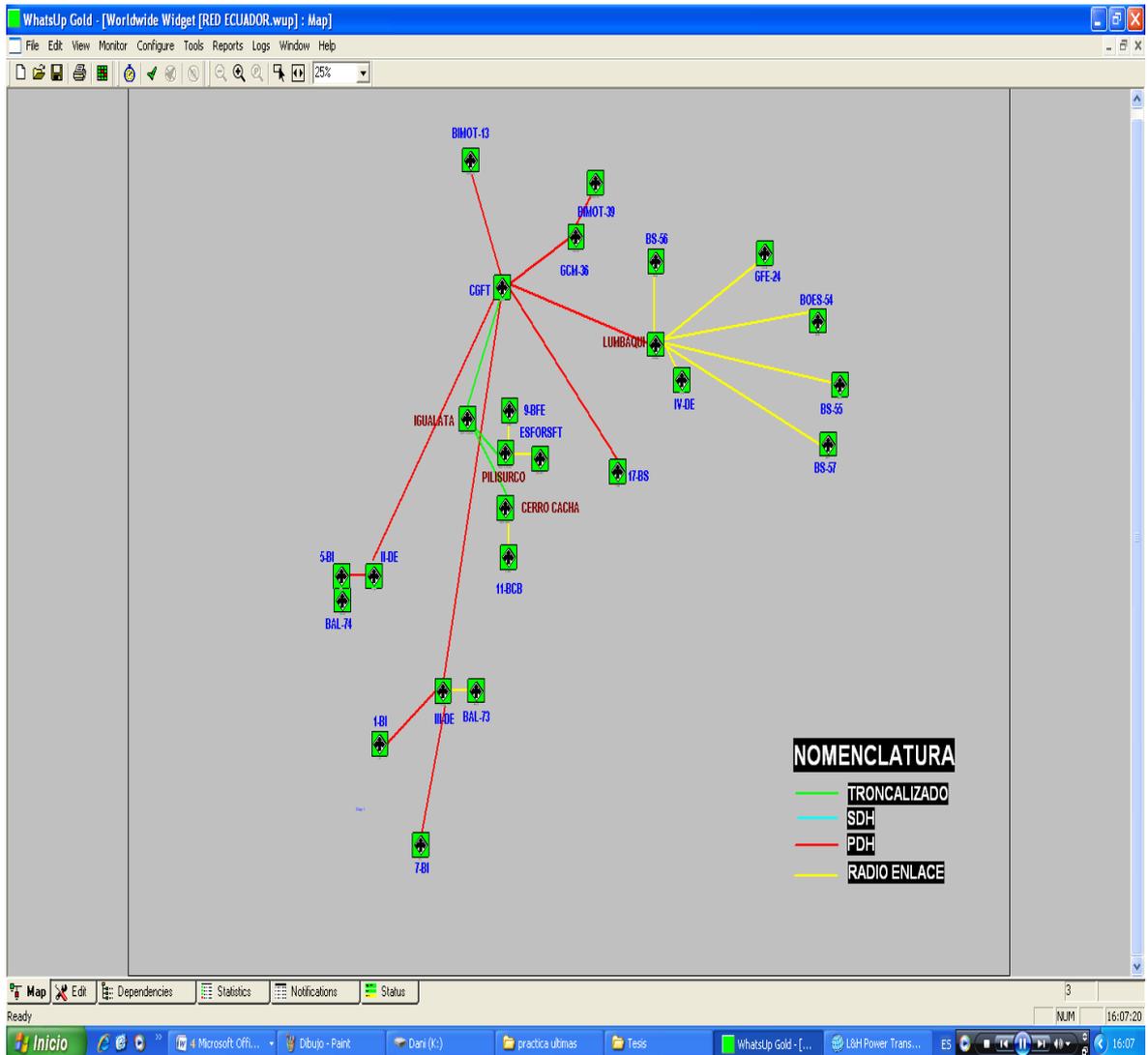


Figura 4-1. Red de Datos del Ejército

El sistema de gestión y monitoreo de redes WhatsUp Gold además de detectar las direcciones IP, también detecta las direcciones físicas de los equipos, por lo cual es más fácil diferenciar un equipo de otro.

4.3.1.- PRUEBAS DE USO

En esta sección se explica las pruebas de uso que se le realizaron con el sistema de gestión y monitoreo WhatsUp Gold, la cual se detalla por pasos, para lo cual se utilizó la WAN descrita en el punto anterior.

4.3.1.1.- Dependencias que existen en la red monitoreada

Aquí podemos observar las dependencias y tipo de dispositivos, para esto se hizo referencia al mapa que proyecta WhatsUp Gold, a continuación se muestran cada uno de ellos en la ventana de dependencias monitoreadas.

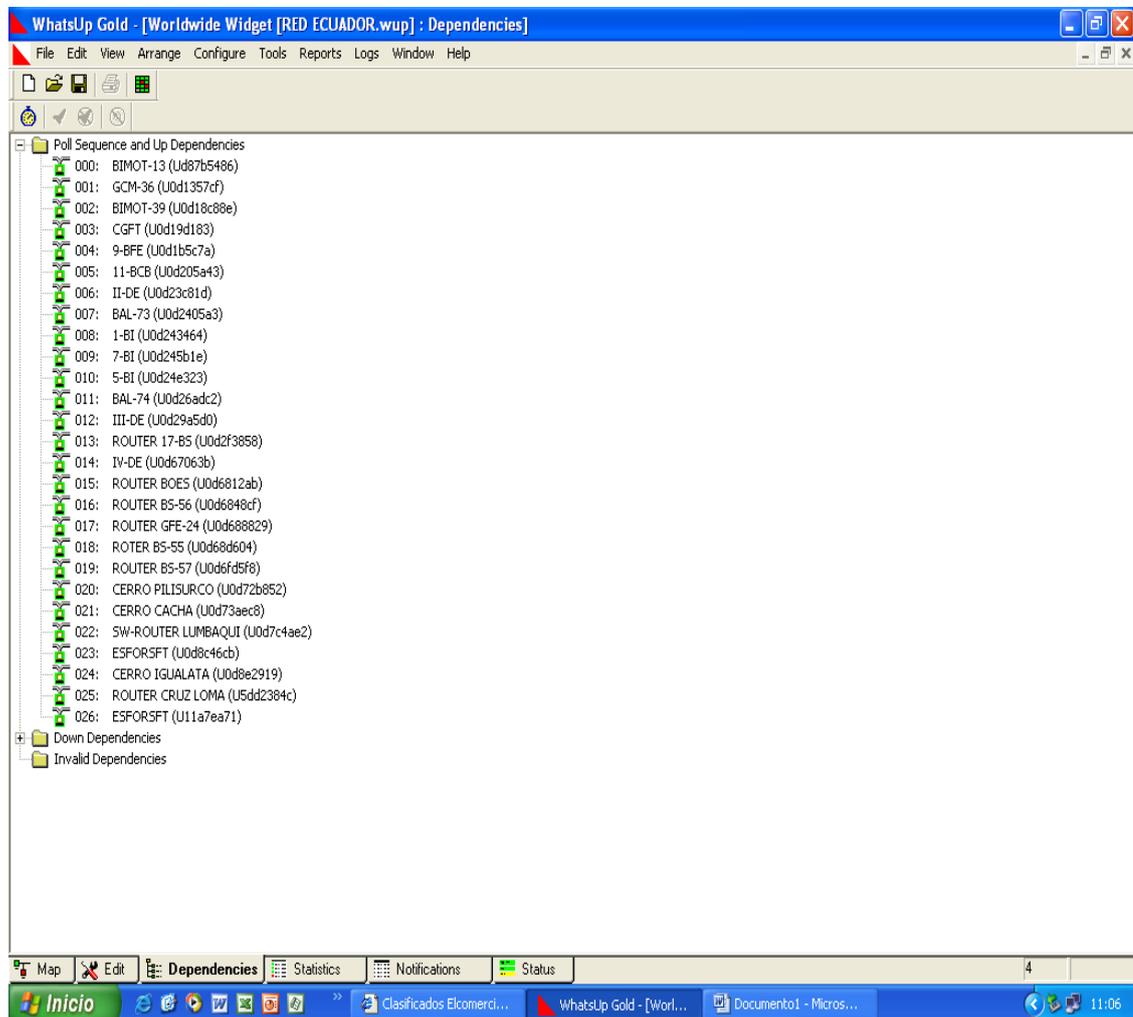


Figura 4-2. Dependencias de la red de Datos del Ejército

4.3.1.2.- Estadísticas de la red monitoreada

En esta ventana se muestra direcciones IP para cada dependencia, además se observa el tipo de monitoreo el estado y el periodo de frecuencia con el cual fue monitoreado el dispositivo de cada dependencia.

Device	Address	Type	Status	Period	Count	% Resp...	% Missed	Down T...	# Alerts	AvgRTT	MinRTT	MaxRTT
BIMOT-13	10.21.5.254	ICMP	11010	4725:25	14606	10.87	89.13	216:58	0	14	11	463
GCM-36	10.21.65.254	ICMP	11010	4725:25	14607	38.57	61.43	149:33	0	28	5	2219
BIMOT-39	10.21.68.254	ICMP	11010	4725:25	14606	9.00	91.00	221:31	0	16	7	565
CGFT	10.20.5.254	ICMP	0	4725:25	14607	93.43	6.57	16:00	0	0	0	33
9-BFE	10.21.1.254	ICMP	0	4725:25	14606	43.26	56.74	138:07	0	36	16	353
11-BCB	10.21.32.254	ICMP	0	4725:25	14606	49.21	50.79	123:39	0	38	18	256
II-DE	10.22.0.254	ICMP	0	4725:25	14606	85.88	14.12	34:23	0	6	0	235
BAL-73	10.23.73.254	ICMP	0	4725:25	14606	88.62	11.38	27:42	0	15	8	459
1-BI	10.23.1.254	ICMP	11010	4725:25	14606	81.30	18.70	45:32	0	11	6	432
7-BI	10.23.32.254	ICMP	0	4725:25	14606	90.59	9.41	22:54	0	35	11	869
5-BI	10.22.1.254	ICMP	0	4725:25	14606	90.39	9.61	23:24	0	34	10	866
BAL-74	10.22.161.254	ICMP	0	4725:25	14606	90.39	9.61	23:24	0	26	10	819
III-DE	10.23.0.254	ICMP	0	4725:25	14606	87.03	12.97	31:34	0	17	9	2568
ROUTER 17-B5	10.24.32.254	ICMP	0	4725:25	14606	84.81	15.19	36:59	0	18	6	724
IV-DE	10.24.0.254	ICMP	0	4725:25	14606	86.25	13.75	33:28	0	13	4	463
ROUTER BOE5	10.24.2.254	ICMP	0	4725:25	14606	90.25	9.75	23:44	0	26	18	5018
ROUTER BS-56	10.24.1.254	ICMP	0	4725:25	14606	90.61	9.39	22:51	0	16	10	5016
ROUTER GFE-24	10.24.11.254	ICMP	0	4725:25	14605	90.67	9.33	22:42	0	13	8	5018
ROUTER BS-55	10.24.5.254	ICMP	0	4725:25	14605	89.51	10.49	25:32	0	29	18	4518
ROUTER BS-57	10.24.8.254	ICMP	0	4725:25	14605	79.14	20.86	50:47	0	47	24	4518
CERRO PILLISURCO	10.60.1.6	ICMP	0	4725:25	14605	59.26	40.74	99:10	0	22	6	242
CERRO CACHA	10.60.1.14	ICMP	0	4725:25	14605	59.28	40.72	99:07	0	23	8	255
SW-ROUTER LU...	10.24.9.254	ICMP	0	4725:25	14605	90.74	9.26	22:33	0	8	5	4956
ESFORSFT	10.60.1.75	ICMP	0	4725:25	14605	40.27	59.73	145:23	0	31	12	231
CERRO IGUALATA	10.60.1.2	ICMP	0	4725:25	14605	88.83	11.17	27:11	0	19	5	251
ROUTER CRUZ L...	10.60.1.1	ICMP	0	935:20	1940	89.59	10.41	3:22	0	39	4	221
ESFORSFT	10.21.227.254	ICMP	0	116:53	953	89.09	10.91	1:44	0	49	12	229

Figura 4-3. Estadísticas de la red de Datos del Ejército

4.3.1.3.- Estado de la red monitoreada

En la ventana de estado se puede observar fácilmente las dependencias que tienen sus dispositivos caídos, como se puede observar en la siguiente ventana existen cuatro unidades del ejército que no están respondiendo al monitoreo.

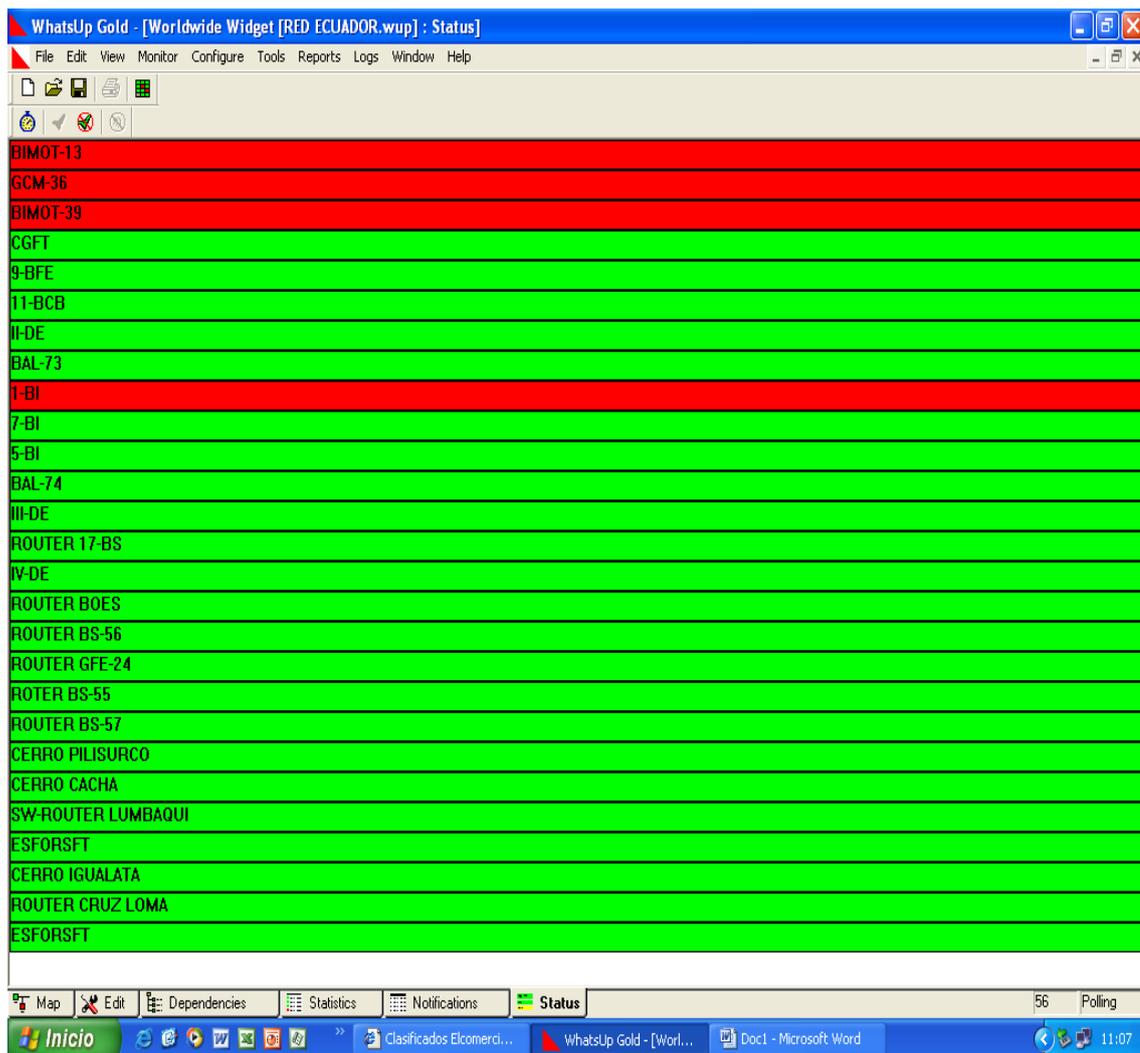


Figura 4-4. Estado de la red de Datos del Ejército

4.3.1.4.- Dispositivo caído

Para saber de una mejor forma porque no responden los dispositivos al monitoreo, verificamos las propiedades de la dependencia caída, como se puede observar en la ventana anterior se reportan cuatro dependencias que están fuera de servicio, vamos a verificar la dependencia I-BI para saber de qué dispositivo se trata y sus diferentes propiedades.

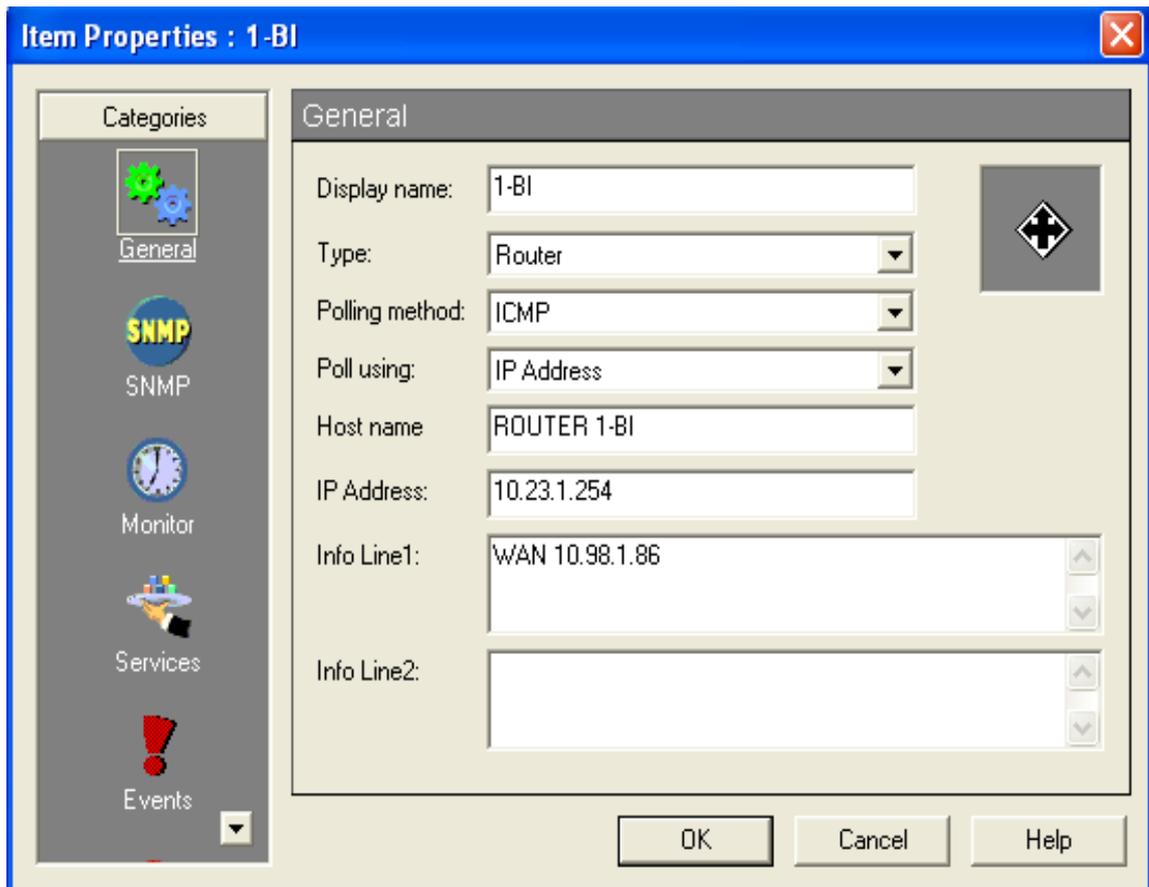


Figura 4-5. Propiedades dependencia caída

4.3.1.5.- Respuestas de un dispositivo

Más adelante se tiene una opción importante a seleccionar, la cual es revisar la cantidad de las respuestas de un dispositivo, para que el administrador tenga una visión sobre el rendimiento de la red, como ejemplo vamos a ver la dependencia BIMOT-13 que es otra dependencia que no responde al monitoreo.

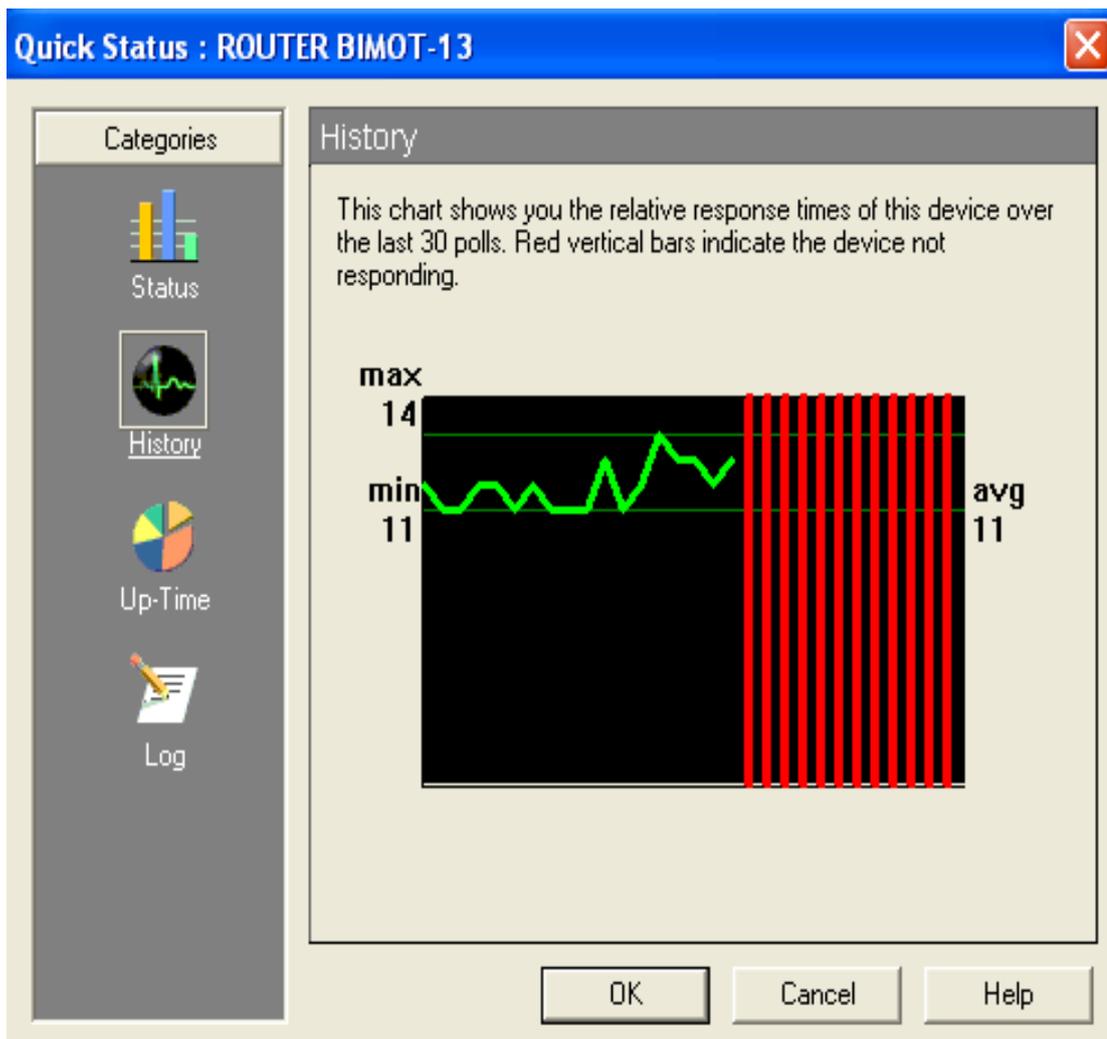


Figura 4-6. Respuestas de un dispositivo

4.3.1.6.- Porcentaje de respuestas de un dispositivo

Teniendo en cuenta los elementos antes mostrados se puede obtener un porcentaje exacto de las respuestas de monitoreo sobre un dispositivo.

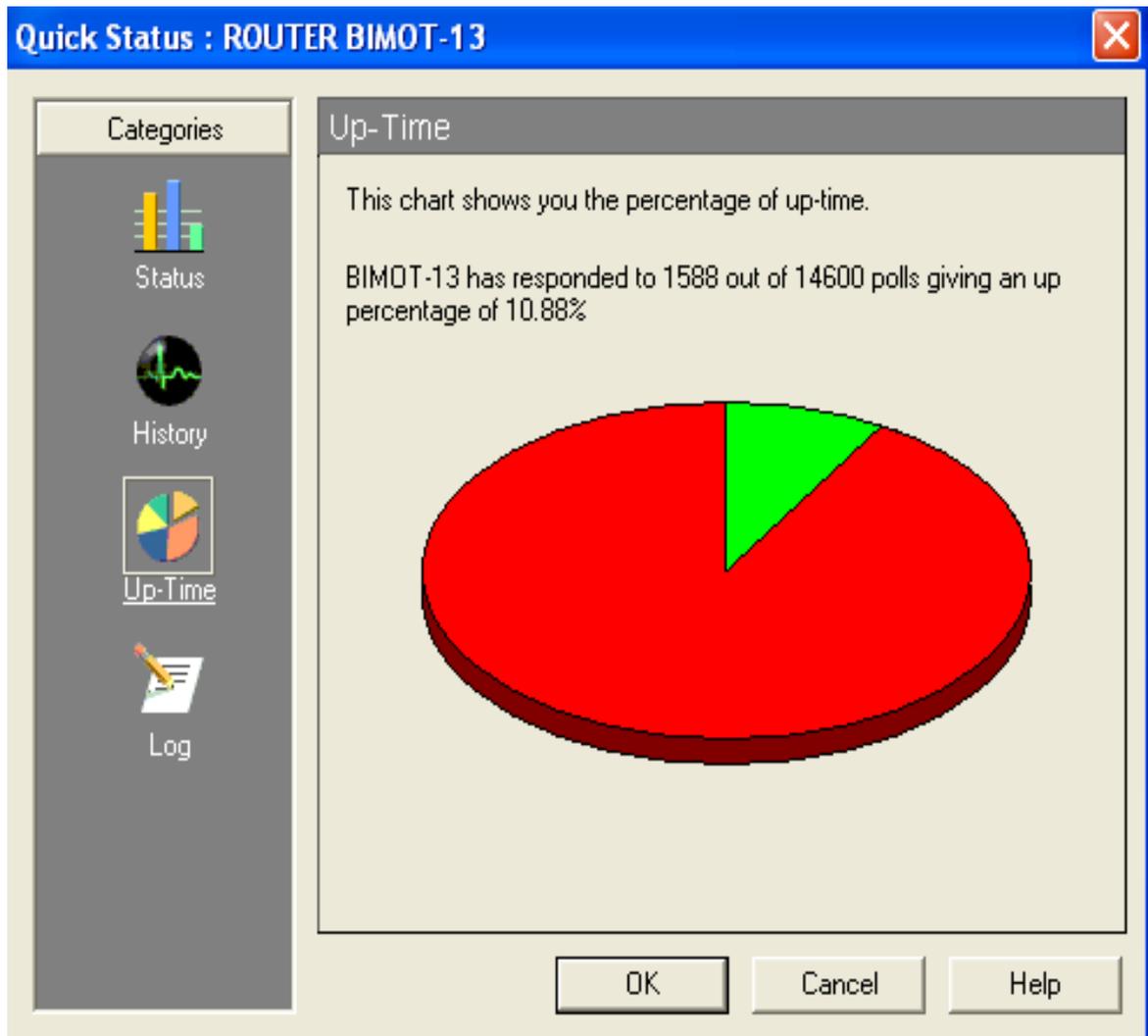


Figura 4-7. Porcentaje de respuestas de un dispositivo

4.3.1.7.- Reportes de la red

Esta herramienta también nos da la libertad de escoger o crear un tipo de reporte para cada red monitoreada, crear una carpeta para almacenar estos reportes y desde ahí extraerlos para su almacenamiento. A continuación se muestran algunas ventanas con distintos tipos de reportes.

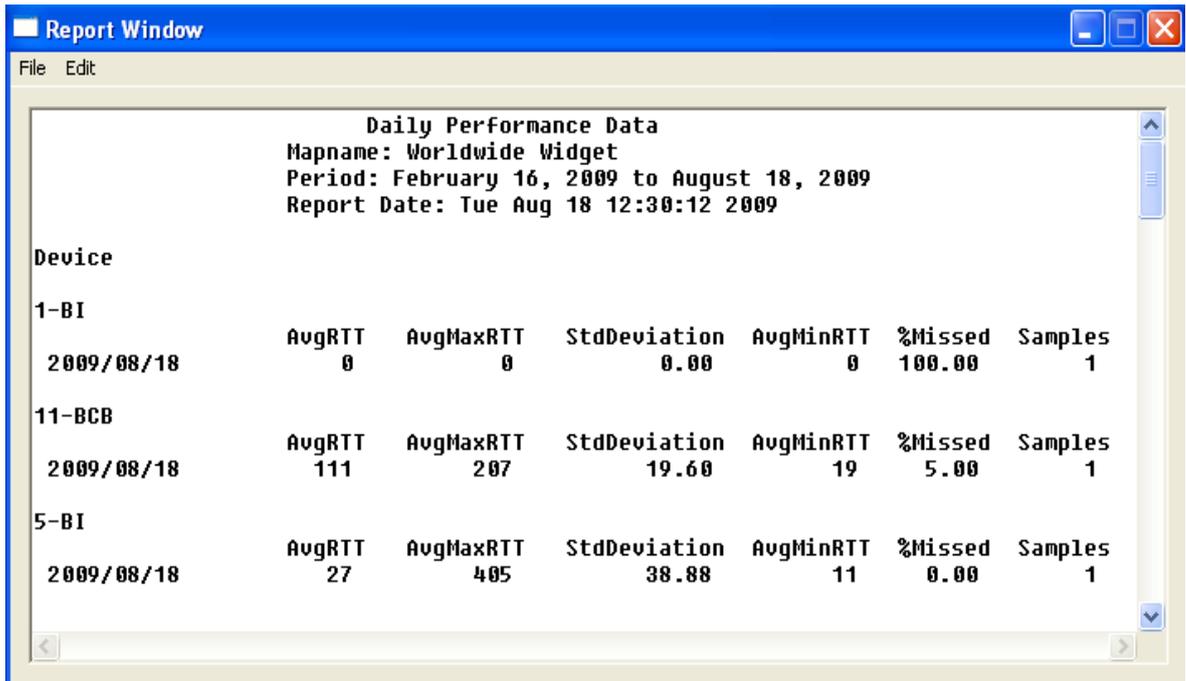


Figura 4-8. Reporte de Windows

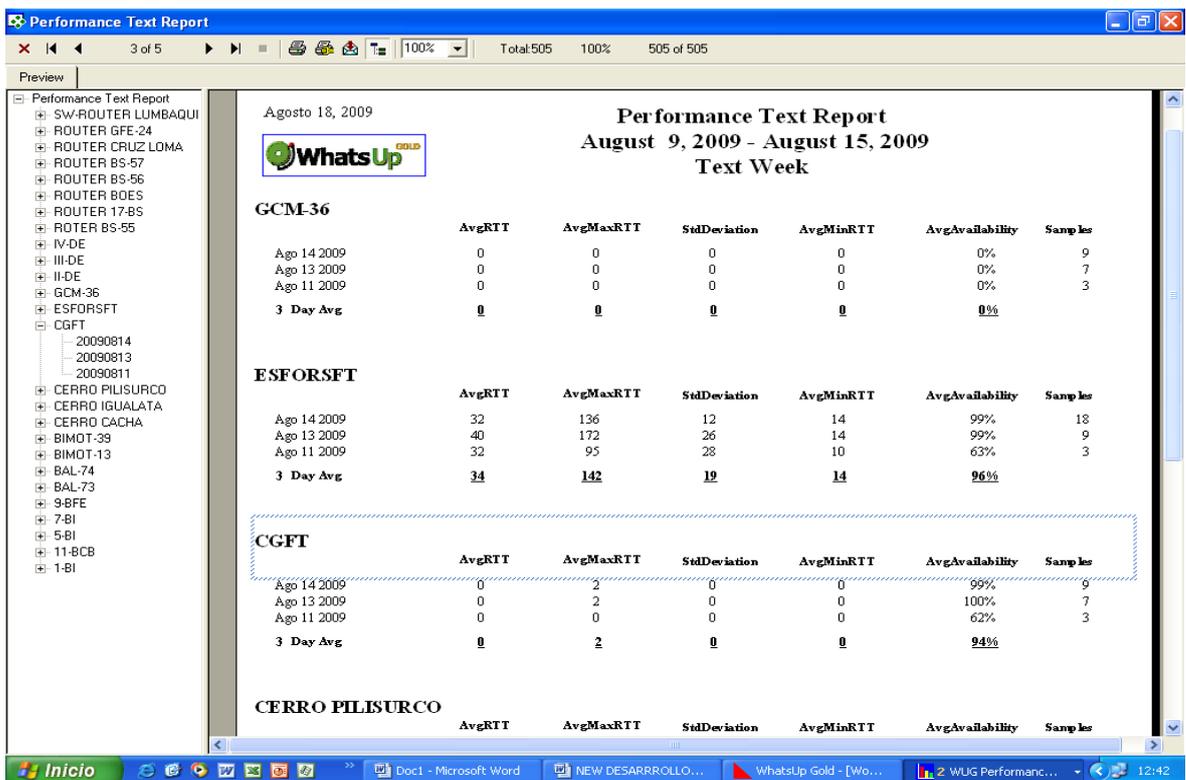


Figura 4-7. Reporte de texto

4.3.1.8.- Exportación de Reportes de la red del ejército

Este reporte detalla en general todos los elementos involucrados en el monitoreo. Enseguida se muestra una hoja de ejemplo exportada a Excel y otra exportada a PDF de todas las dependencias pertenecientes a la red de datos del ejército.

Performance Text Report August 9, 2009 - August 15, 2009 Text Week						
SW-ROUTER LUMBAQUI						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	8	91	2	5	99%	9
Ago 13 2009	8	77	2	5	100%	7
Ago 11 2009	5	57	4	3	63%	3
3 Day Avg	7	80	3	5	94%	
ROUTER GFE-24						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	13	92	2	9	99%	9
Ago 13 2009	11	57	2	9	100%	7
Ago 11 2009	9	89	8	6	62%	3
3 Day Avg	11	79	3	9	94%	
ROUTER CRUZ LOMA						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	20	123	13	4	99%	9
Ago 13 2009	33	155	30	4	99%	7
Ago 11 2009	26	89	22	3	63%	3
3 Day Avg	26	130	22	4	93%	
ROUTER BS-57						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	40	139	5	27	99%	9
Ago 13 2009	31	97	14	22	99%	7

Figura 4-10. Reporte exportado a Excel

Performance Text Report August 9, 2009 - August 15, 2009 Text Week						
SW-ROUTER LUMBAQUI						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	8	91	2	5	99%	9
Ago 13 2009	8	77	2	5	100%	7
Ago 11 2009	5	57	4	3	63%	3
3 Day Avg	7	80	3	5	94%	
ROUTER GFE-24						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	13	92	2	9	99%	9
Ago 13 2009	11	57	2	9	100%	7
Ago 11 2009	9	89	8	6	62%	3
3 Day Avg	11	79	3	9	94%	
ROUTER CRUZ LOMA						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	20	123	13	4	99%	9
Ago 13 2009	33	155	30	4	99%	7
Ago 11 2009	26	89	22	3	63%	3
3 Day Avg	26	130	22	4	93%	
ROUTER BS-57						
	AvgRTT	AvgMaxRTT	StdDeviation	AvgMinRTT	AvgAvailability	Samples
Ago 14 2009	40	139	5	27	99%	9
Ago 13 2009	31	97	14	22	99%	7

Figura 4-11. Reporte exportado a PDF

4.4.- ESCALABILIDAD

El sistema de gestión y monitoreo de redes WhatsUp Gold puede ser lo más eficiente posible dependiendo de la velocidad del servidor que estemos utilizando ya que, si se tiene un servidor con un procesador reciente se trabaja mejor, de esto depende que WhatsUp Gold labore de manera eficiente y que al momento de realizar una consulta o una inserción de los reportes no exista ningún problema, con esto, se puede monitorear cualquier red a la que esté conectado nuestro servidor, la clave de la escalabilidad de la aplicación es el funcionamiento paralelo velocidad servidor- WhatsUp Gold

4.5.- MANUAL DE USUARIO DEL SISTEMA DE GESTIÓN Y MONITOREO WHATSUP GOLD

El objetivo principal de este manual es mostrar al usuario administrador la forma correcta de instalar y configurar WhatsUp Gold así como el funcionamiento, con los datos que debe ingresar, además de interactuar de manera correcta con el sistema (inserción correcta de datos, configuración SNMP en Windows server).

4.5.1.- PASOS PARA LA INSTALACIÓN

Para empezar, lo primero que tenemos que hacer, es descargar “WhatsUp Gold” desde la página oficial, eligiendo ahí, la versión más reciente o a su vez adquirir el software con licencia. Si ha adquirido una versión WhatsUp Gold en CD-ROM, inserte el CD-ROM en la unidad.

Si el programa de instalación no se ejecuta automáticamente, haga clic en Iniciar, seleccione Ejecutar y, a continuación, introduzca el CD seguido por Autorun.exe por Ejemplo: d: **Autorun.exe**.

1. Si ha descargado WhatsUp Gold de Internet, ejecute la aplicación descargada, **wugoldec.exe**.

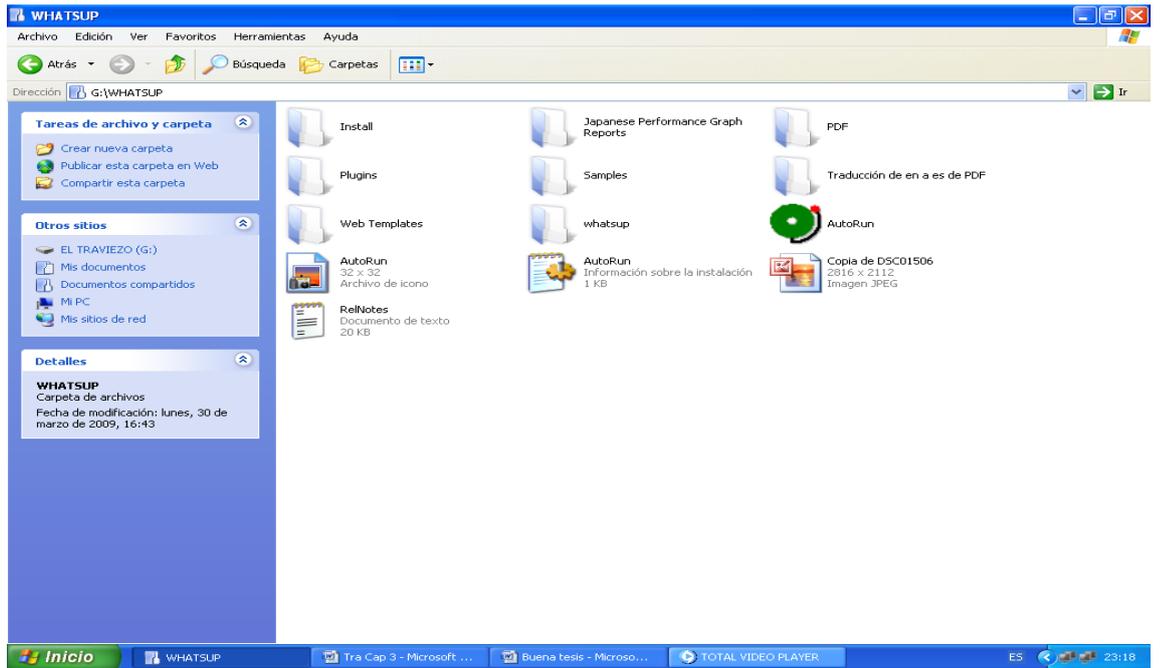


Figura 4-12. Instalación WhatsUp Gold Paso 1

2. En la siguiente ventana nos muestra cuatro cajas de dialogo para continuar con la instalacion hacemos clic en **Install whatsUpGold**.



Figura 4-13. Instalación WhatsUp Gold Paso 2

3. Enseguida se mostrara la pantalla de bienvenida del sistema, hacemos clic en **Next** para seguir con la instalación.

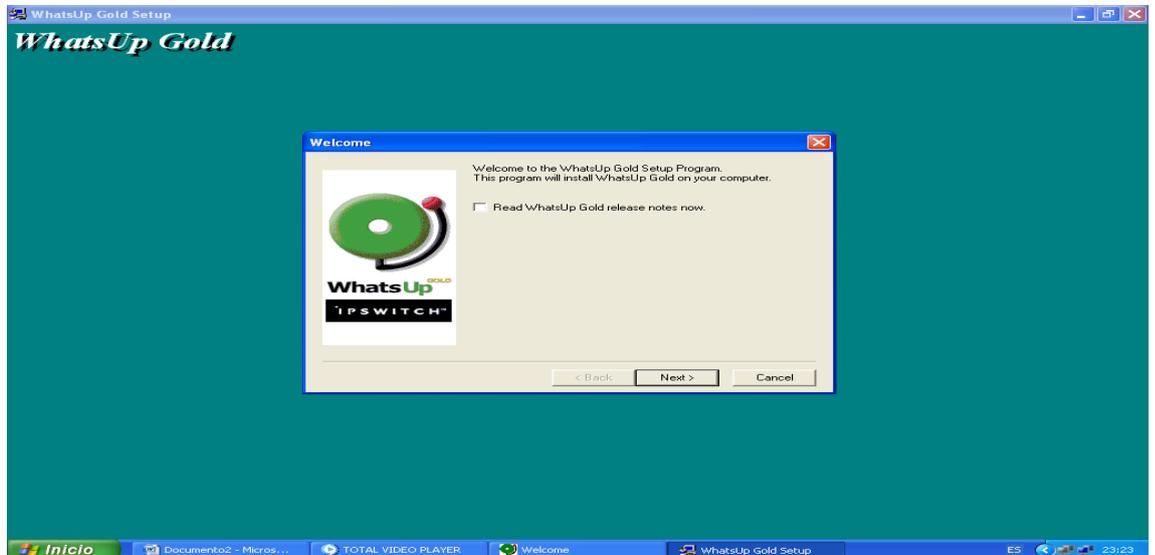


Figura 4-14. Instalación WhatsUp Gold Paso 3

4. Esta ventana muestra la ubicación donde se guardaran los archivos del sistema **C:\ Archivo de programa\WhatsUp**.



Figura 4-15. Instalación WhatsUp Gold Paso 4

5. Si no queremos guardar los archivos en esta ubicación, escogemos la ubicación en la que queremos que se guarden los archivos de WhatsUp Gold **.d:\Archivos Whatsup.**

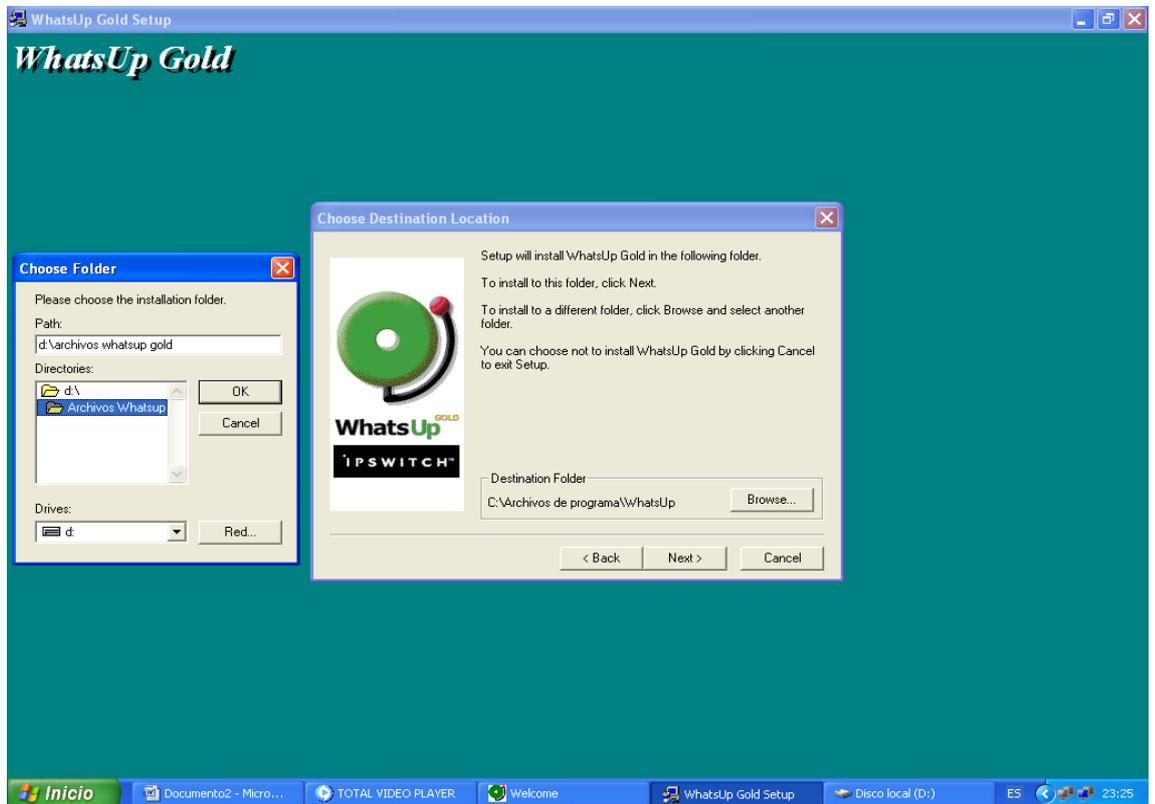


Figura 4-16. Instalación WhatsUp Gold Paso 5

6. A continuación se muestra la ventana **Select Monitor Plugins**. Plugins amplían la funcionalidad de WhatsUp y le permiten adaptar el uso a sus propias necesidades. El monitor plugins le permite escoger recursos de red específicos a monitorear.
Escoja el plugins que usted quiere instalar. **NT services** identifica y supervisa todos sus servicios NT y automáticamente los comienza de nuevo de ser no disponible.

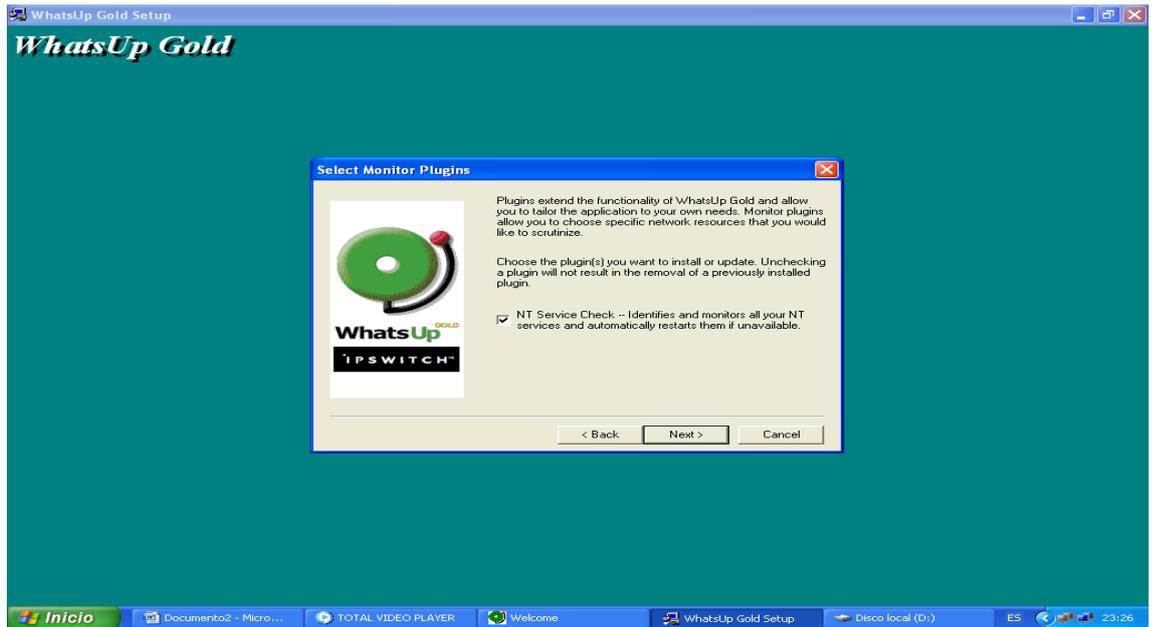


Figura 4-17. Instalación WhatsUp Gold Paso 6

7. En la siguiente pantalla escogemos **Syslog Notifications** este le permite enviar mensajes a un servidor Syslog. **Text to Speech** Provee la Notificación hablada vía sonidos del sistema.

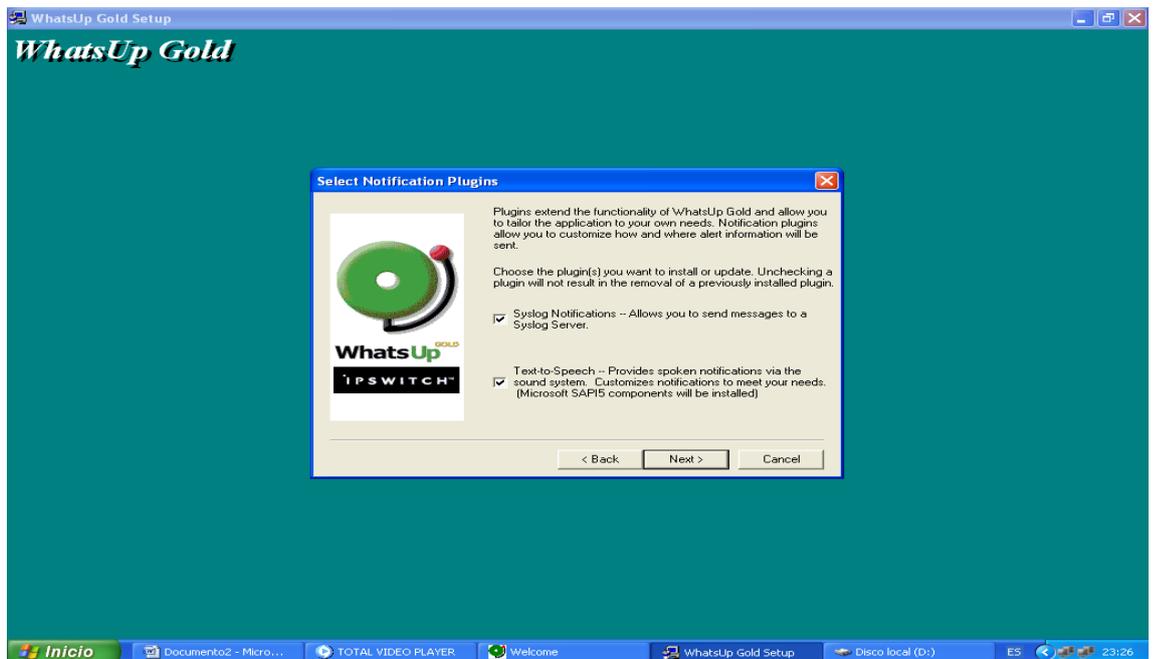


Figura 4-18. Instalación WhatsUp Gold Paso 7

8. En la ventana **Select Program Folder** muestra la Carpeta del Programa selecta para guardar los archivos WhatsUp, para continuar hacemos clic en **Next**.

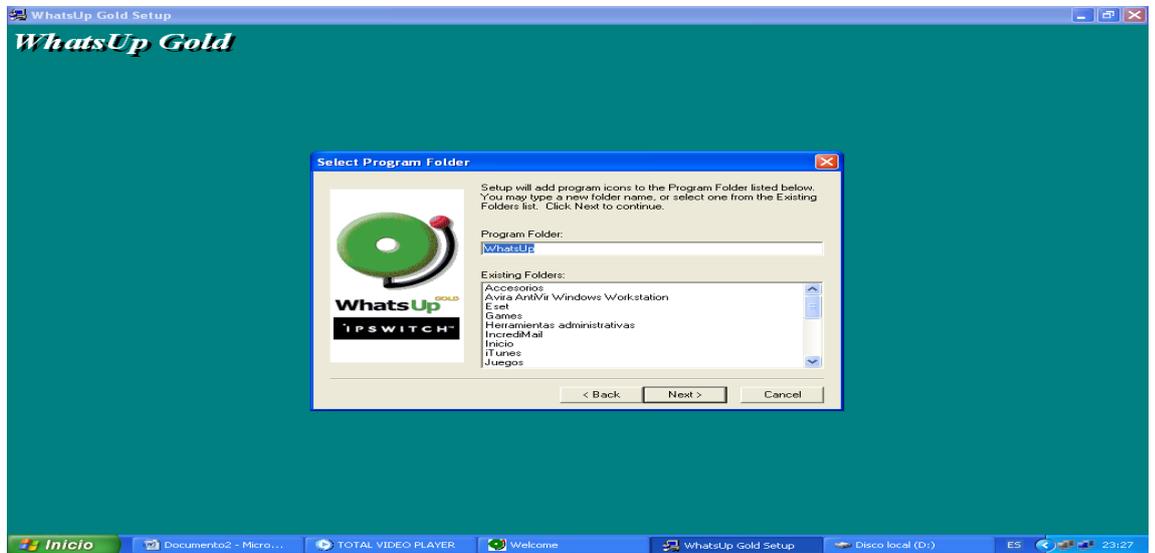


Figura 4-19. Instalación WhatsUp Gold Paso 8

9. En este momento empezara la instalacion de todas las herramientas del sistema de monitoreo WhatsUp Gold.

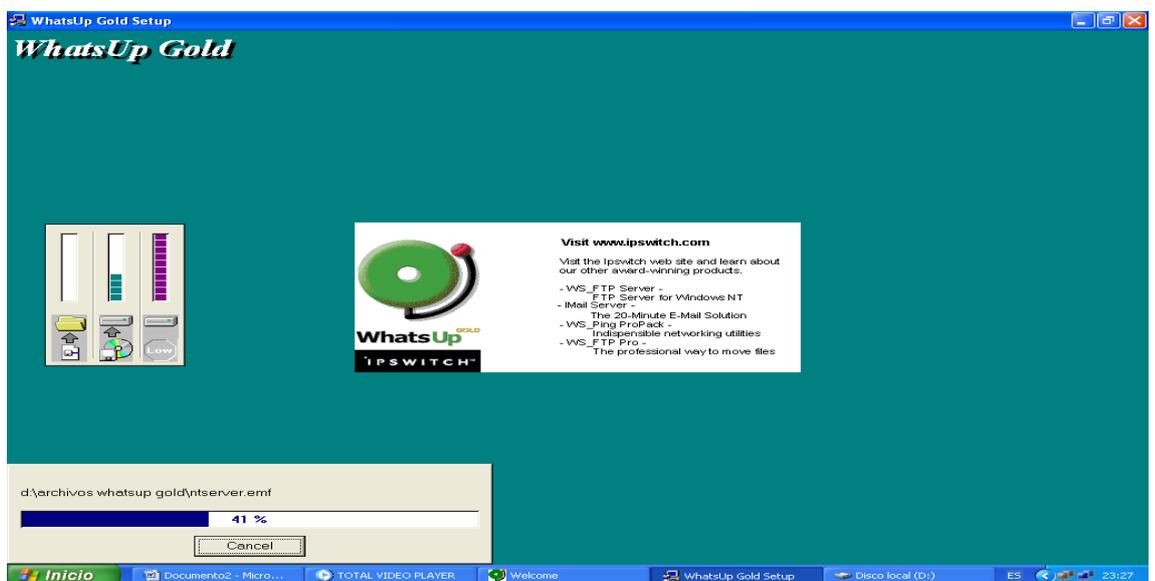


Figura 4-20. Instalación WhatsUp Gold Paso 9

10. Para concluir con la instalación señalamos la pestaña **Setup Examples Maps** para ver un mapa demo de WhatsUp Gold y hacemos clic en **Finish**.

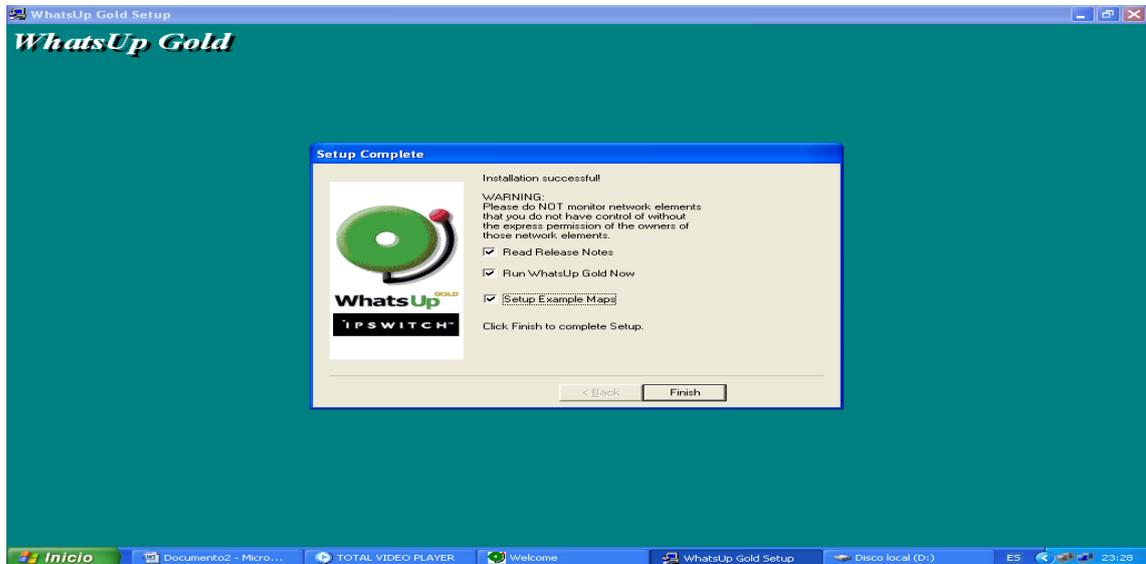


Figura 4-21. Instalación WhatsUp Gold Paso 10

11. Una vez concluida la instalación WhatsUp Gold abre el mapa de demostración llamado **World.wup**.

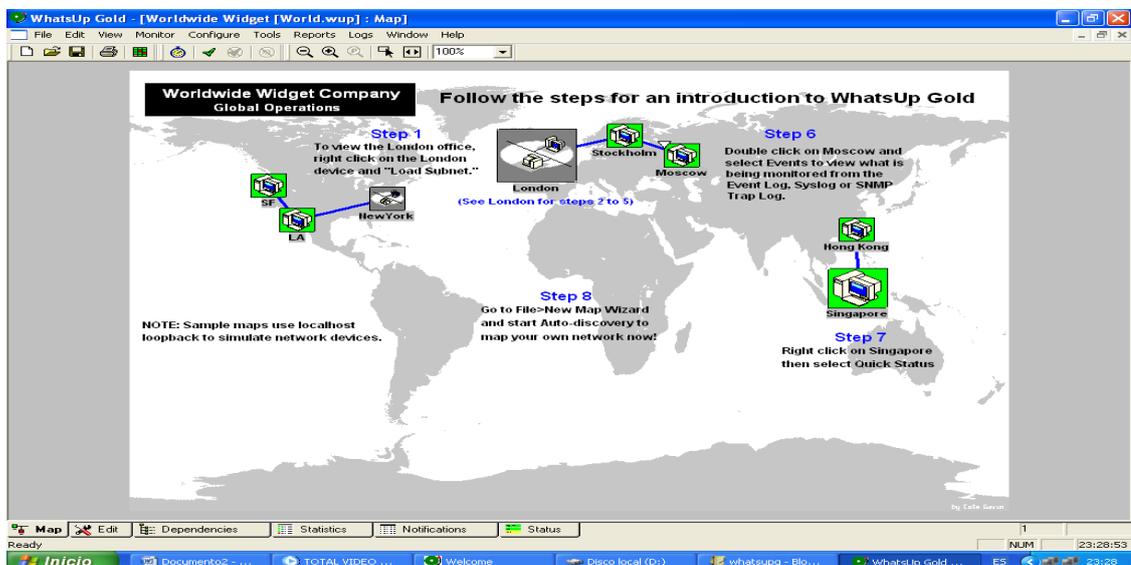


Figura 4-22. Instalación WhatsUp Gold Paso 11

4.5.2.- CONFIGURACIÓN SNMP EN WINDOWS SERVER

En esta parte se va a mostrar como levantar el servicio de SNMP para todo lo que es monitoreo de redes, esto permite el acceso del sistema de gestión y monitoreo de redes WhatsUp Gold a la información de nuestro procesador, con el fin de mantener una red operativa, eficiente y segura, constantemente monitoreada.

4.5.2.1.- Agregar SNMP como un servicio de Windows

Es importante que se agregue SNMP como un servicio de Windows para permitir la perfecta funcionalidad de los software de monitoreo. Para agregar por primera vez SNMP sobre la máquina en la cual queremos trabajar se le pedirá al usuario que siga los siguientes pasos:

1. En primer lugar vamos hacer clic en inicio, panel de control, agregar o quitar programas.

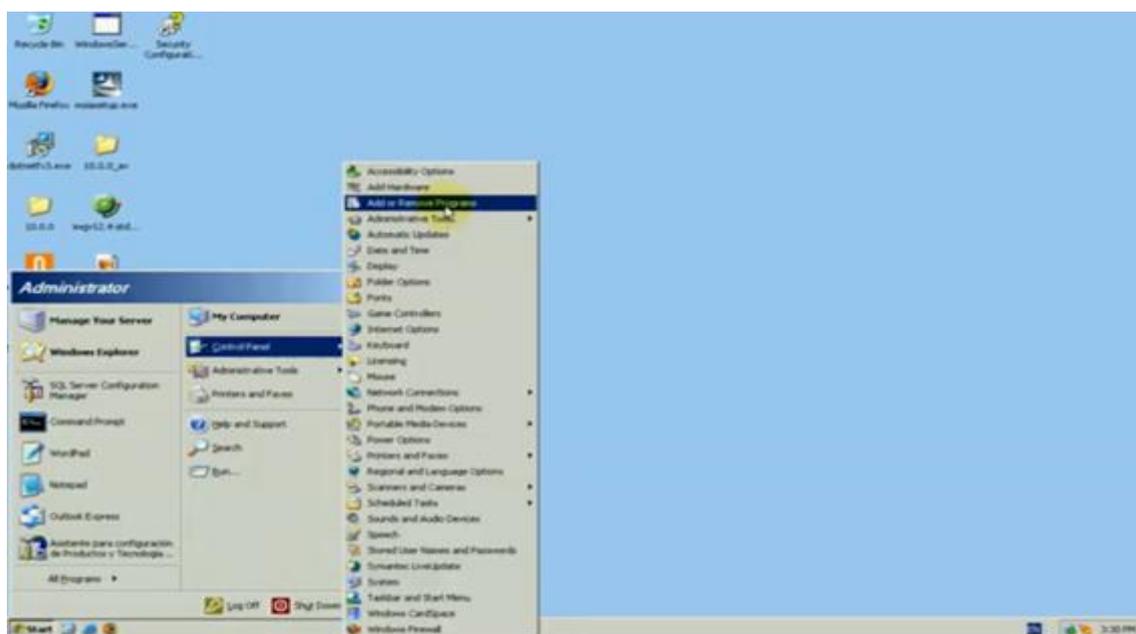


Figura 4-23. Configuración SNMP Paso 1

2. Seleccionamos agregar o quitar componentes de Windows y esperamos que se cargue la pantalla.

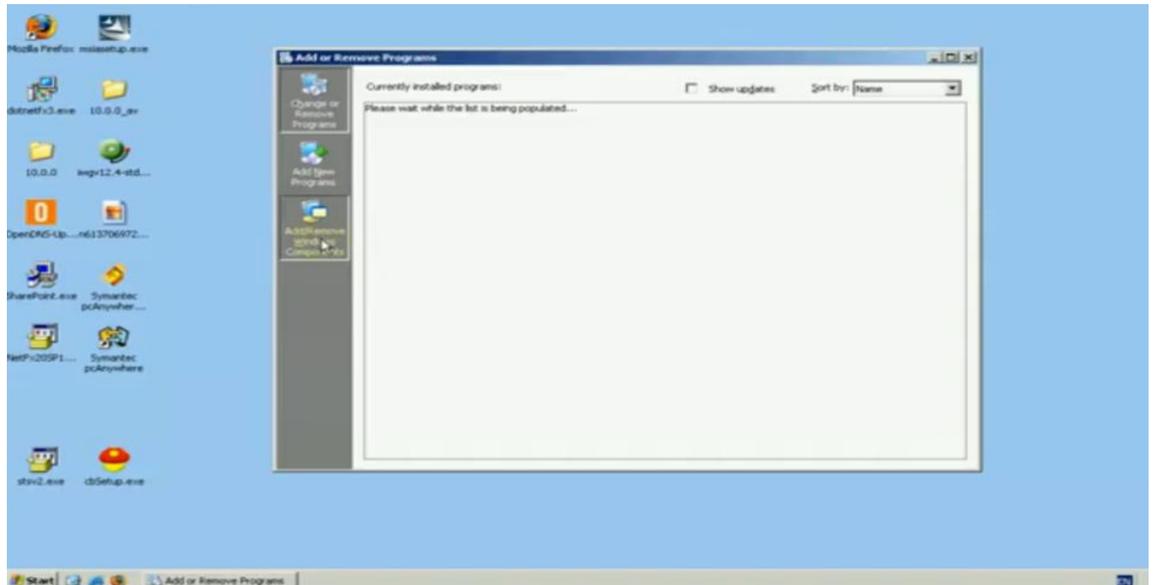


Figura 4-24. Configuración SNMP Paso 2

3. En la pantalla que aparece buscamos herramientas de administracion y monitoreo hacemos doble clic.

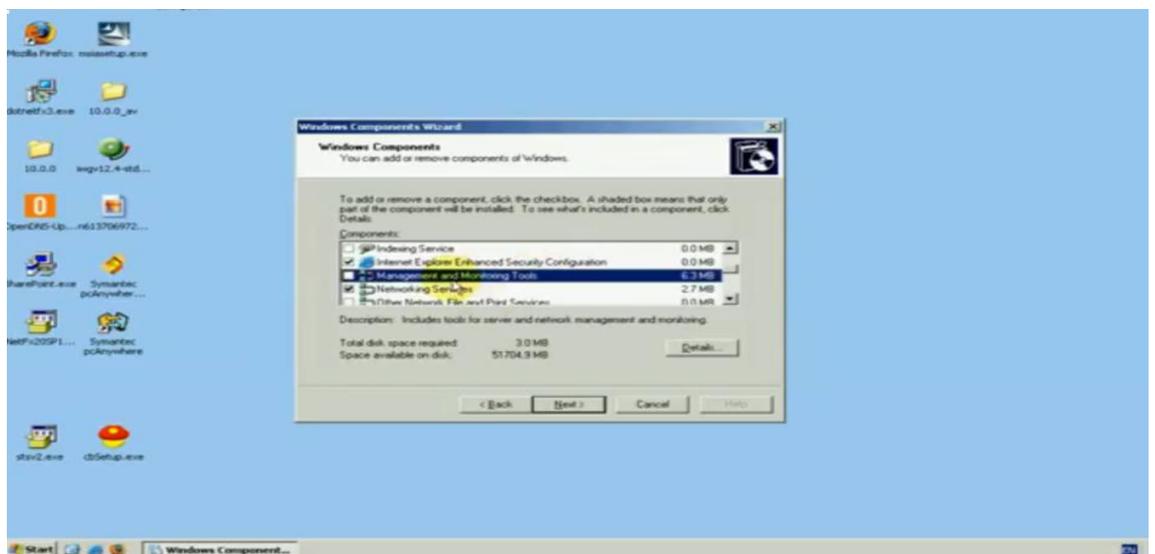


Figura 4-25. Configuración SNMP Paso 3

4. En la siguiente pantalla seleccionamos Simple Network Management Protocol y WMI SNMP properties, este servicio nos va a permitir acceder a todo lo que es la instrumentación de Windows.

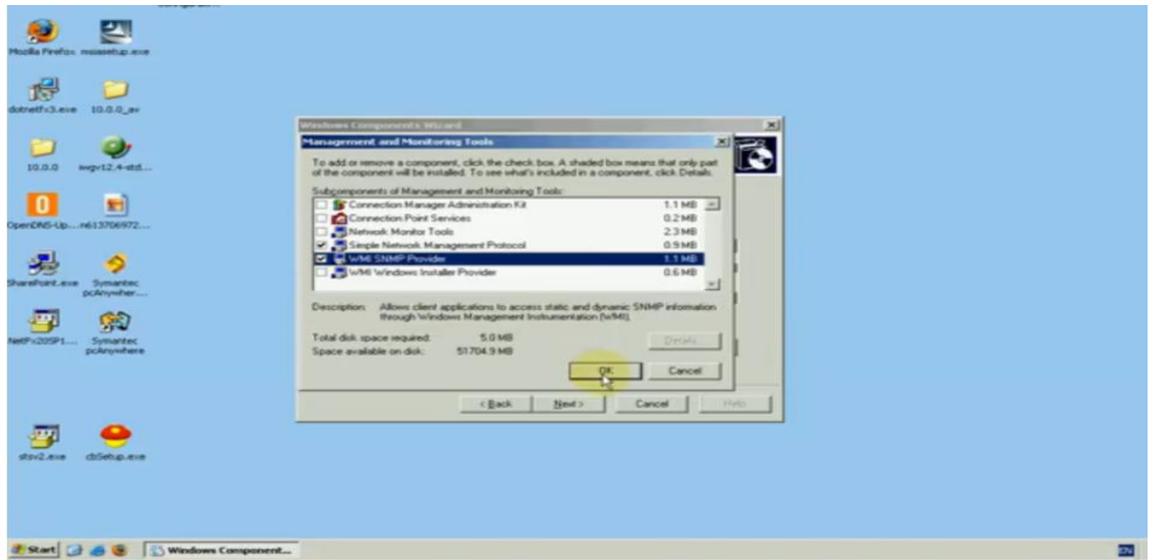


Figura 4-26. Configuración SNMP Paso 4

5. Hacemos clic en aceptar, siguiente y va a comenzar la instalación.

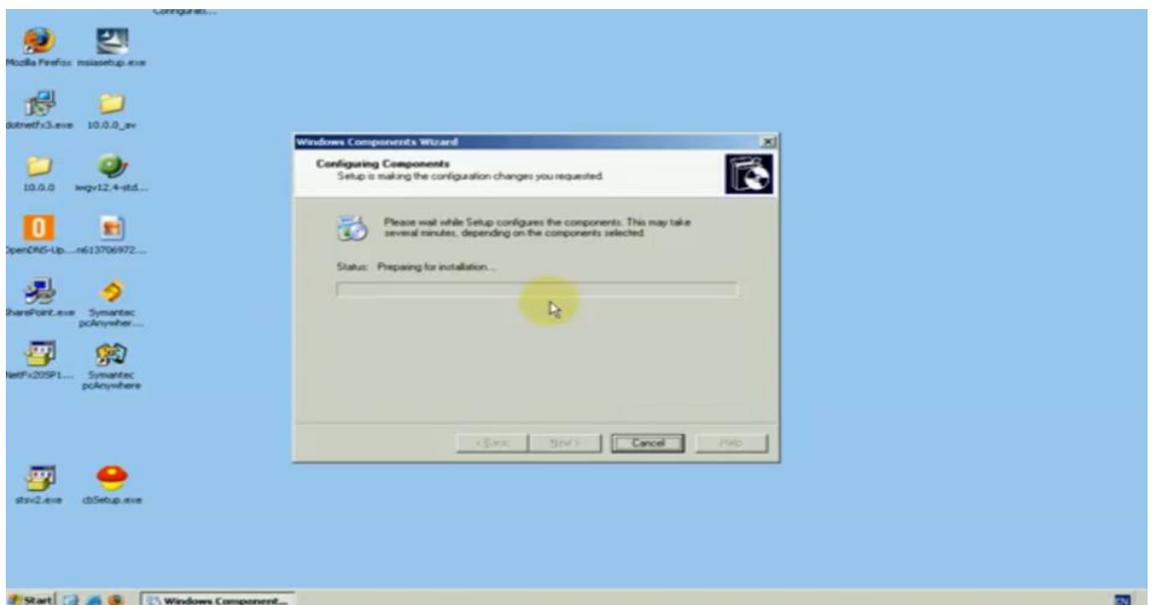


Figura 4-27. Configuración SNMP Paso 5

6. Terminada la instalación hacemos clic en finish.



Figura 4-28. Configuración SNMP Paso 6

7. Como siguiente paso abrimos el menú >Inicio>Mi PC y hacemos clic en administrar.

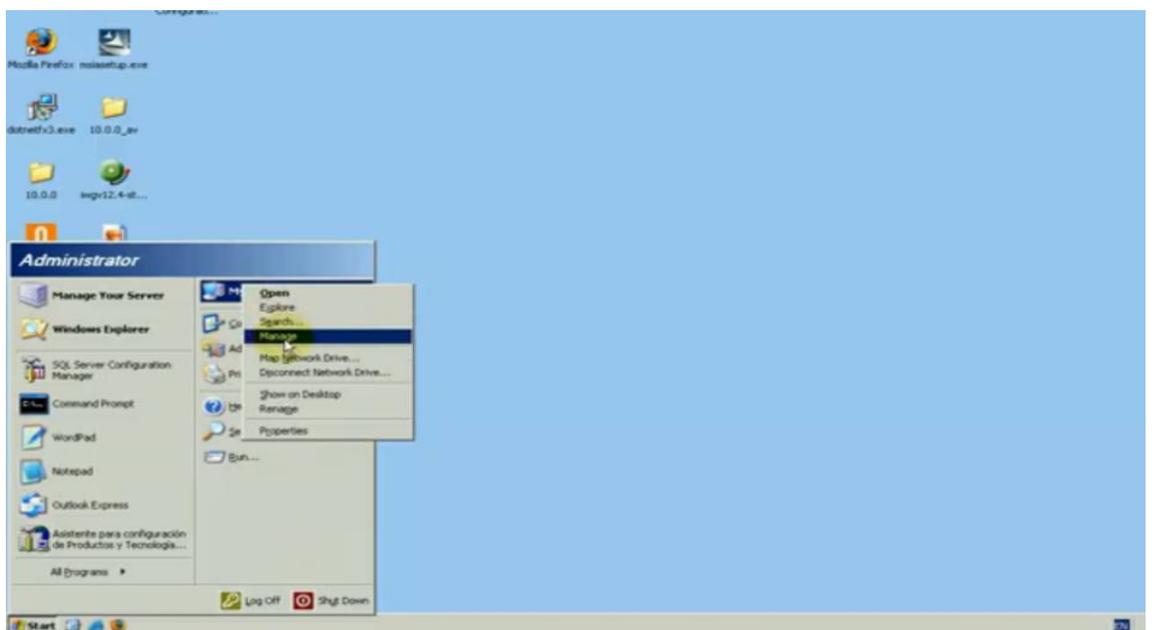


Figura 4-29. Configuración SNMP Paso 7

8. En la pantalla que se muestra buscamos Services and Applications.

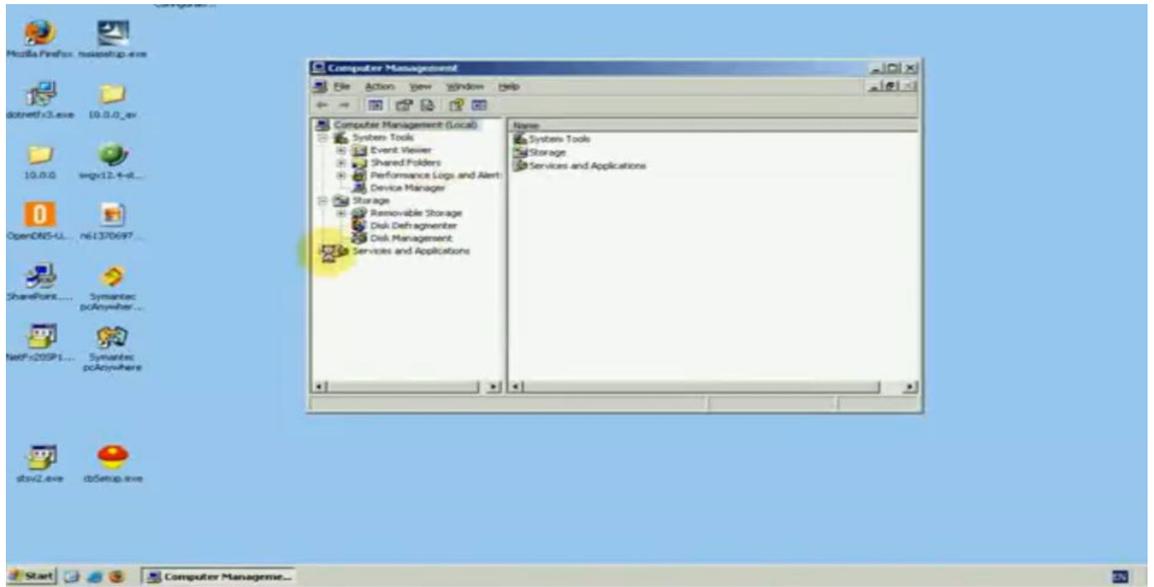


Figura 4-30. Configuración SNMP Paso 8

9. Buscamos al lado izquierdo de la pantalla services, hacemos clic y esperamos que cargue.

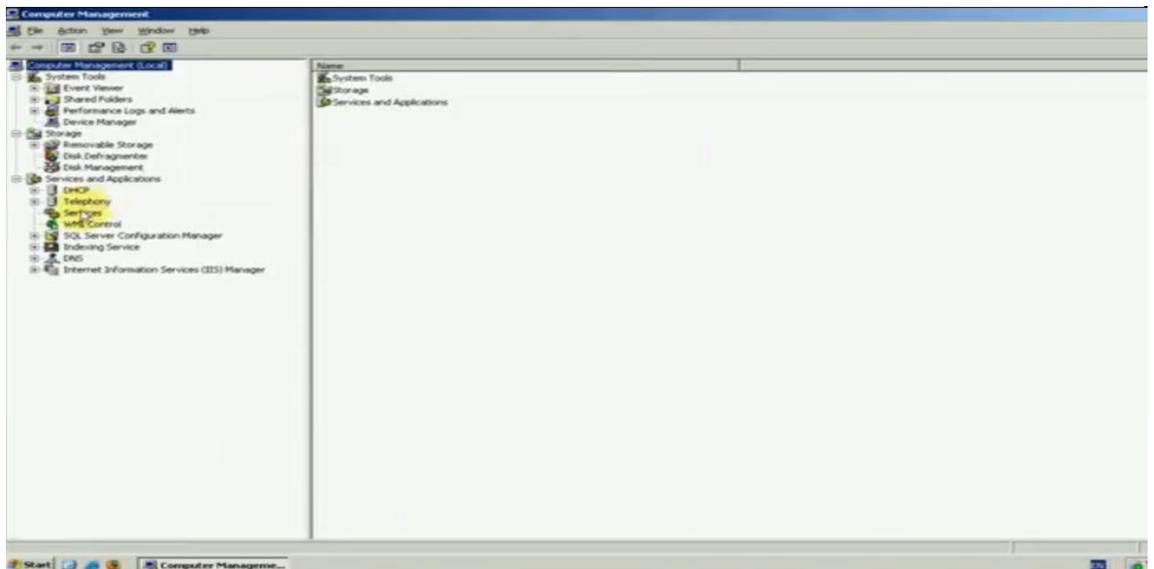


Figura 4-31. Configuración SNMP Paso 9

10. Una vez cargada la siguiente pantalla seleccionamos SNMP services y hacemos doble clic.

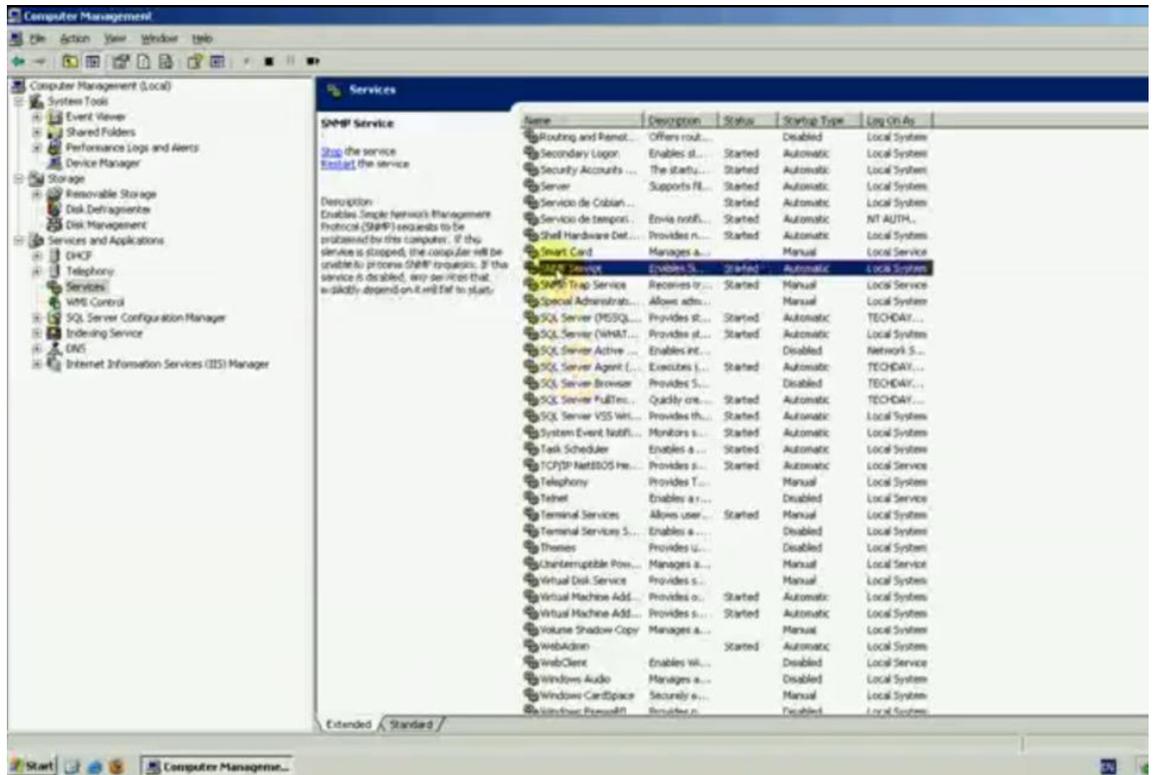


Figura 4-32. Configuración SNMP Paso 10

11. Enseguida se nos mostrara una nueva pantalla, en la ventana **Community name** asignaremos un nombre de comunidad, este nombre es un identificador que usara nuestro sistema de monitoreo para poder monitorear los equipos por SNMP.

Para cuestiones de estudio nuestro nombre de comunidad será Espel, agregamos nuestro nombre a la lista.

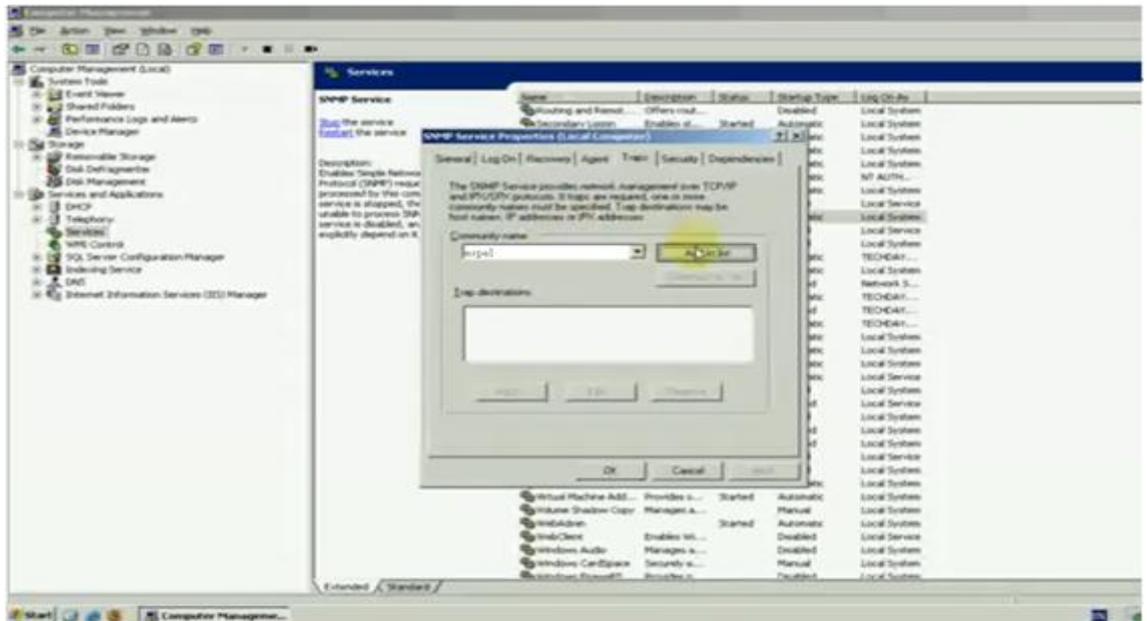


Figura 4-33. Configuración SNMP Paso 11

12. Hacemos clic en la pestaña security y se nos muestra dos opciones **Accept packets from my host**, si queremos monitorear solo desde nuestro host y **Accept packets from any host**, si queremos monitorear desde cualquier host.

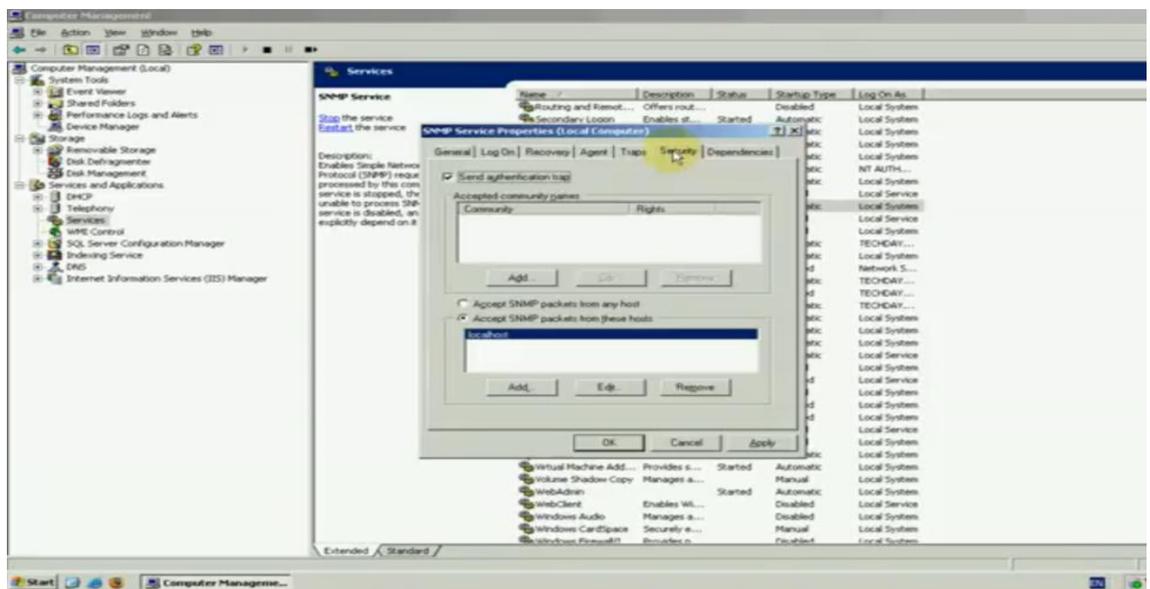


Figura 4-34. Configuración SNMP Paso 12

13. En la pantalla que se muestra a continuación seleccionamos monitorear desde cualquier host y hacemos clic en **Add**.

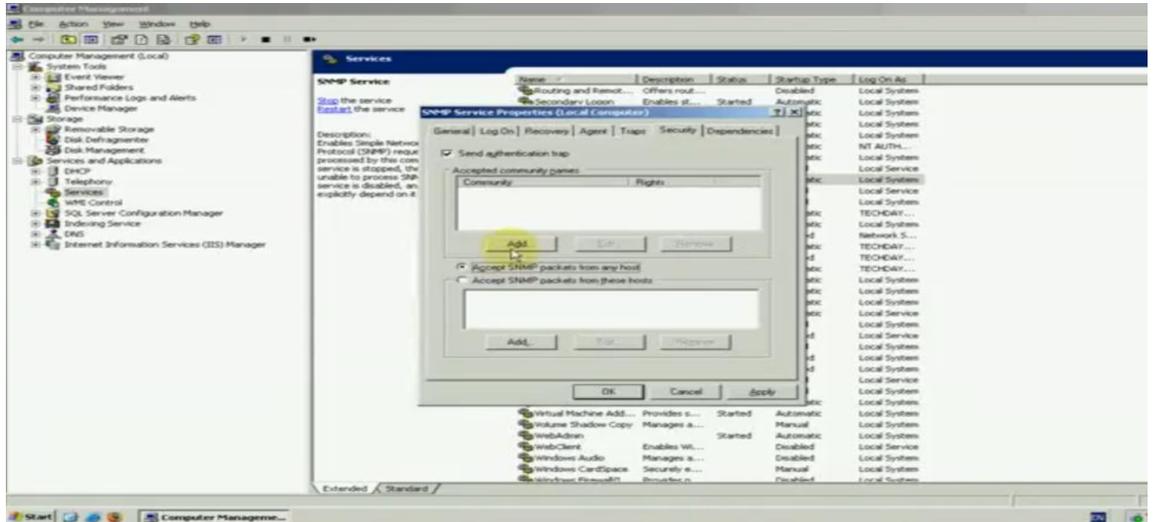


Figura 4-35. Configuración SNMP Paso 13

14. En la siguiente ventana seleccionamos Read Only y Espel que es el nombre de comunidad que colocamos anteriormente hacemos clic en agregar, aplicar y aceptar.

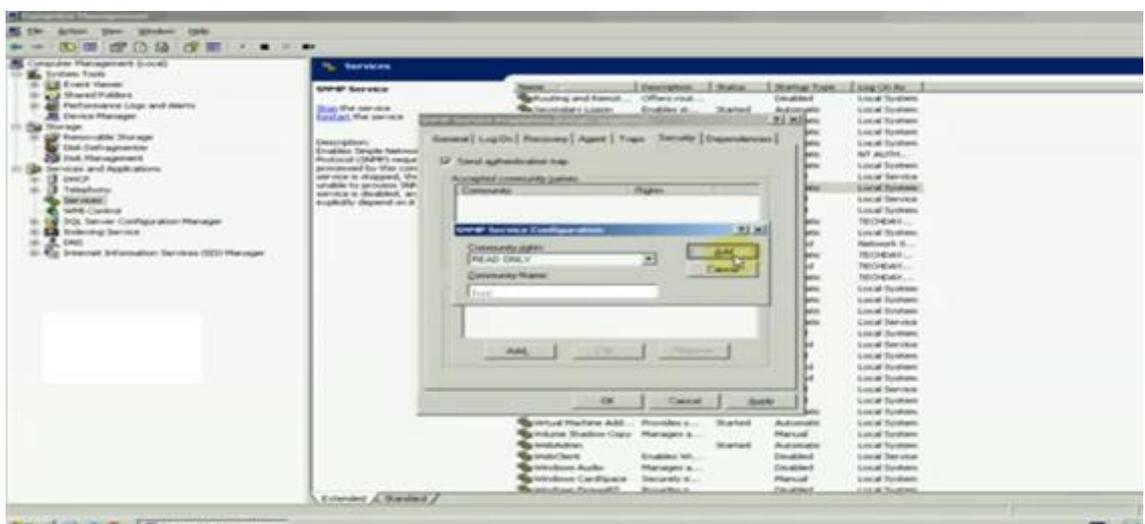


Figura 4-36. Configuración SNMP Paso 14

15. Para terminar con la configuración de SNMP seleccionamos **SNMP services** clic derecho y hacemos clic en **restart**.

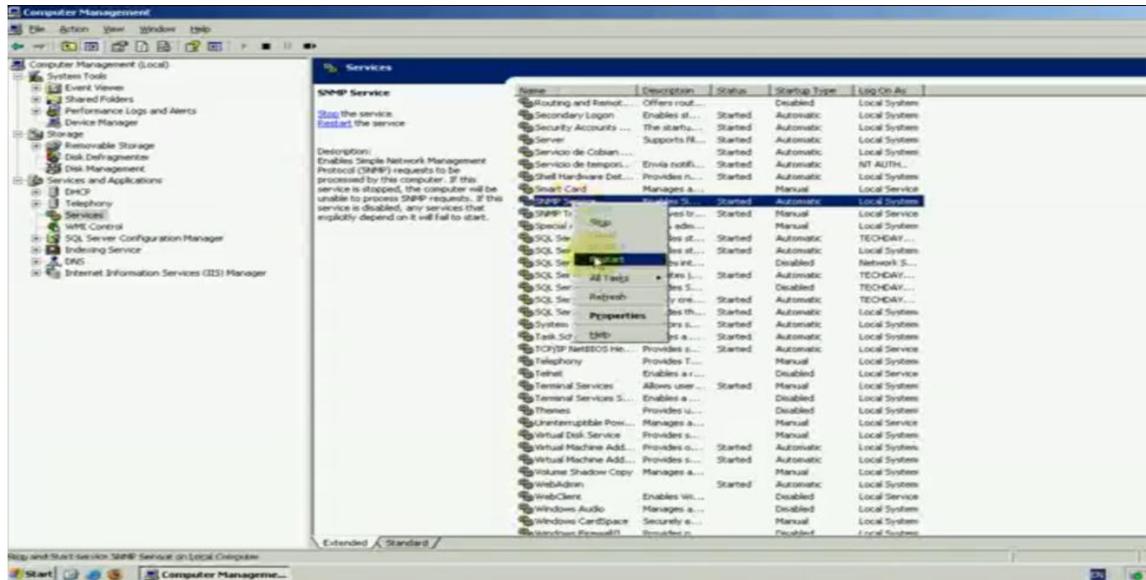


Figura 4-37. Configuración SNMP Paso 15

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Finalmente en este capítulo se resumen las conclusiones y recomendaciones clave que se obtienen después del análisis del sistema de gestión y monitoreo WhatsUp Gold.

5.1.- CONCLUSIONES

- El usuario mediante el sistema de gestión y monitoreo de redes WhatsUp Gold, puede realizar el análisis y monitoreo de redes, permitiéndole conocer el estado actual de cualquier dispositivo conectado a la red.
- El funcionamiento de sistema en general es bueno, pues no se presentan errores durante el momento de monitorear una red, lo que genera un grado de confianza en el desempeño de WhatsUp Gold.
- El usuario tiene la posibilidad de almacenar, recuperar y analizar la información, esto es debido a que el sistema permite realizar este tipo de cosas.

5.2.- RECOMENDACIONES

- Dado que la red de una institución como el Ejército Ecuatoriano está sujeta a constantes cambios (físicos y lógicos), se recomienda realizar estudios periódicos sobre el comportamiento de la misma, a fin de establecer las adecuaciones pertinentes para mantener su óptimo rendimiento.
- El monitoreo de redes es la suma de todas las actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad. Dentro de estas actividades, se tiene diferentes responsabilidades fundamentales como, la atención a fallas, configuración, y seguridad. Por ello se recomienda una planificación en cuanto a la delegación de estas funciones a los técnicos encargados de la red del Ejército Ecuatoriano, con lo cual se conseguirá un buen desempeño de la

red, ayudando a mantener la operatividad de los recursos y el buen estado de los mismos.

- Los lineamientos desarrollados proporcionan una guía que permite obtener claramente información relevante de la red operante, así como proporciona una secuencia ordenada y lógica de los dispositivos existentes en la red, por lo que se recomienda aplicarlo en la Dirección de Sistemas de Información y Comunicaciones del Ejército (DISICOM).

FUENTES DE INFORMACIÓN:

- <http://www.ipswitch.com/support/whatsup/>
- http://es.whatsupgold.com/products/whatsup_gold_msp/system_requirements.asp
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/monitoreo.html
- [http://mx.geocities.com/quartzzan.html.](http://mx.geocities.com/quartzzan.html)
- [http://www.cisco.com.](http://www.cisco.com)
- [http://www.rad.com/Article.html.](http://www.rad.com/Article.html)
- [http://www.monografias.com/tesis/tesis/Erlang-b.htm.](http://www.monografias.com/tesis/tesis/Erlang-b.htm)
- [http://www.monografias.com/tesis/tesis/Erlang B.htm.](http://www.monografias.com/tesis/tesis/Erlang B.htm)
- http://www.rad.com/RADCnt/MediaServer/6062_asmi-51.pdf
- <http://www.interlan.com.co/pimm.htm>
- [http://revista.ecua.net.ec/sept2002/vanguardia.html.](http://revista.ecua.net.ec/sept2002/vanguardia.html)
- <http://www.cisco.com/web/learning/netacad/index.html>
- <http://snmp.westhawk.co.uk/index.html>
- <http://www.ipswitch.ca/whatsup.htm>
- <http://www.ietf.org/html.charters/bridge-charter.html>
- <http://www.solotutoriales.com/directory/default.aspx?fid=132&all=1>
- <http://w3.mor.itesm.mx/~lssalced/remota.html>

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD EXPRESADA

Quien suscribe CBOP. DE COM. Usca Patiño Daniel Ernesto, portador de la C.I. 060292591-9, libre y voluntariamente declaro que el presente tema de investigación: **“ELABORAR EL MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE MONITOREO Y GESTIÓN WHATSUP GOLD”**, su contenido, ideas, análisis, conclusiones, y propuestas son auténticos y personales.

En tal virtud son para efectos legales y académicos que se desprenden de la presente tesis es y será de mi exclusiva responsabilidad legal y académica, como autor de esta tesis de grado.

Para el derecho intelectual del autor, de la información obtenida y utilizada a manera de bibliografía se muestra en el documento la referencia de donde fue obtenida.

El resto de la información de este documento es soporte intelectual adquirido mediante las prácticas realizadas y lo aprendido en el transcurso de mi carrera universitaria.

Atentamente;

Daniel E. Usca P.

EL AUTOR

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD EXPRESADA

Quien suscribe CBOP. DE COM. Lema Montaluisa Segundo Sergio, portador de la C.I. 050241031-9, libre y voluntariamente declaro que el presente tema de investigación: **“ELABORAR EL MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DEL SISTEMA DE MONITOREO Y GESTIÓN WHATSUP GOLD”**, su contenido, ideas, análisis, conclusiones, y propuestas son auténticos y personales.

En tal virtud son para efectos legales y académicos que se desprenden de la presente tesis es y será de mi exclusiva responsabilidad legal y académica, como autor de esta tesis de grado.

Para el derecho intelectual del autor, de la información obtenida y utilizada a manera de bibliografía se muestra en el documento la referencia de donde fue obtenida.

El resto de la información de este documento es soporte intelectual adquirido mediante las prácticas realizadas y lo aprendido en el transcurso de mi carrera universitaria.

Atentamente;

Segundo S. Lema M.

EL AUTOR

ESCUELA POLITÉCNICA DEL EJÉRCITO SEDE LATACUNGA

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

Este proyecto fue elaborado por:

Daniel E. Usca P.
CI: 0602925919

Segundo S. Lema M.
CI: 0502410319

El Coordinador de Carrera

El Secretario Académico

Ing. Edison Espinoza

Dr. Rodrigo Vaca

Latacunga, Agosto del 2009