

**IPN**  
**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA**  
**UNIDAD CULHUACAN**

**TESIS INDIVIDUAL**

Que como prueba escrita de su Examen Profesional para obtener el Título de **INGENIERO EN COMUNICACIONES Y ELECTRONICA** deberán desarrollar la C.:

**SONIA GUADALUPE AVILA ROJO**

**"MONITOREO DE UNA RED USANDO PROTOCOLO SNMP."**

Realizar la configuración de un router con una ip para poder monitorearlo mediante un software Solarwinds obteniendo gráficas de tráfico y disponibilidad para poder evitar saturación en la red y esté tenga un mejor rendimiento: cuando haya una caída del servicio se avisé por vía email o un SMS, con esto evitaran las pérdidas causadas por fallos en la red sin detectar. Se contará con información oportuna para conocer el estado de un enlace. Se llevará un registro histórico de la información. Y lo más importante se dará atención oportuna a la caída de la red, enterándonos rápidamente mediante el aviso que va a enviar. Con el aviso oportuno se podrán evitar pérdidas tanto económicas para el ISP y para nuestra red, también se evitarán penalizaciones y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

Ciudad de México a 17 de octubre del 2016

**CAPITULADO:**

- CAPÍTULO 1. Investigaciones previas del Monitoreo de Redes
- CAPÍTULO 2. Constructos teóricos metodológicos para el Monitoreo de Redes
- CAPÍTULO 3. Diseño de un Sistema de Alerta de Caída de una Red
- CAPÍTULO 4. Comportamiento del Sistema de Monitoreo de una Red en Fibra óptica

FIRMA DE CONFORMIDAD:

DRA. ELSA GONZÁLEZ PAREDES  
PRIMER ASESOR

Vo. Bo.

FIRMA DE CONFORMIDAD:

M. EN A. MIGUEL ÁNGEL GARCÍA LICONA  
SEGUNDO ASESOR

APROBADO:

ING. FELICIANO PRIMO ISIDRO CRUZ  
JEFE DE LA CARRERA DE I.C.E.

ING. CARLOS AQUINO RUIZ  
SUBDIRECTOR ACADÉMICO INTERINO



# **INSTITUTO POLITÉCNICO NACIONAL**

---

**ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA**

**UNIDAD CULHUACAN**

**INGENIERÍA EN COMUNICACIONES Y ELECTRÓNICA**

**ACADEMIA DE TITULACIÓN DE I.C.E.**

**TESIS PROFESIONAL**

**MONITOREO DE UNA RED USANDO EL PROTOCOLO SNMP**

**QUE PARA OBTENER EL TÍTULO DE  
INGENIERO EN COMUNICACIONES Y ELECTRÓNICA**

**PRESENTA:  
ÁVILA ROJO SONIA GUADALUPE**

**ASEORES:**

**DRA. ELSA GONZÁLEZ PAREDES  
M. EN C. MIGUEL ÁNGEL GARCÍA LICONA**



**CIUDAD DE MÉXICO. MAYO 2017**

# AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a mis padres María Luisa Rojo Téllez y Jesús Martín Ávila Ávila que, con todo su amor, esfuerzo y cuidados me impulsaron para culminar esta meta. Gracias por estar presentes en cada momento por guiarme por este camino; por superar juntos todas las adversidades, gracias por ayudarme a enfrentar la vida no hay palabras para expresar la gratitud hacia ustedes.

A mí hermano José Martín por el apoyo durante la carrera.

A mis asesores, la Doctora Elsa González Paredes y el M. C. Miguel Ángel García Licona por la paciencia y por todo el apoyo que me dieron a lo largo de este proyecto no importando las circunstancias.

A la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan por brindarme las herramientas para mi formación como profesionista, así como a toda la comunidad alumnos y profesores que en algún punto coincidimos y se presentó la ocasión de compartir vivencias que marcaron mi vida tanto personalmente como profesionalmente.

Al Glorioso Instituto Politécnico Nacional por esta grandiosa oportunidad de formar parte de la institución, es un gran orgullo poder decir que soy POLITÉCNICA.

A todos los amigos y familiares que estuvieron en el camino acompañándome durante estos años, por todas las experiencias y el aprendizaje que pude obtener de cada uno de ustedes.

## *DEDICATORIAS*

*A mis padres*

*Jesús Martín Ávila Ávila*

*Papá sé que desde donde quiera que estés, estás acompañándome y apoyándome para cumplir este sueño, sueño que iniciamos juntos y que durante todo el proceso estuviste a mi lado. Hoy no estás físicamente, pero te llevo siempre en mi mente y corazón. El que te hayas ido me hizo “Entender con el corazón en la mano que el amor no se acaba con la muerte”. Gracias Papá.*

*María Luisa Rojo Téllez*

*Mamá sin tí esto no sería posible siempre tuve y tengo tu apoyo incondicional en todo momento, solo puedo decirte Gracias Mamá. Seguiremos adelante.*

## ÍNDICE TEMÁTICO

PLANTEAMIENTO DEL PROBLEMA.....	X
JUSTIFICACIÓN.....	XI
OBJETIVOS.....	XII
Objetivo general.....	xii
Objetivos Particulares.....	xii
CAPÍTULO 1. INVESTIGACIONES PREVIAS DEL MONITOREO DE REDES.....	1
1.1 Sistemas de Monitoreo en Redes .....	2
CAPÍTULO 2. CONSTRUCTOS TEÓRICOS METODOLÓGICOS PARA EL MONITOREO DE REDES.....	4
2.1 Redes Locales (LAN) .....	5
2.2 Redes de Área Extensa (WAN) .....	6
2.3 Internet .....	6
2.4 Protocolos .....	7
2.5 MODELO OSI .....	7
2.5.1 Capa Física.....	8
2.5.2 Capa De Vínculo De Datos O Enlace .....	8
2.5.3 Capa De Red.....	8
2.5.4 Capa De Transporte .....	9
2.5.5 Capa De Sesión .....	9
2.5.6 Capa De Presentación.....	10
2.5.7 Capa De Aplicación.....	10
2.6 MODELO TCP/IP .....	10
2.6.1 Acceso a red .....	10
2.6.2 Internet .....	10
2.6.3 Transporte.....	11
2.6.4 Aplicación .....	11
2.7 COMPARACIÓN MODELO OSI & TCP/IP .....	12

2.8 PUERTOS .....	12
2.9 MEDIOS FÍSICOS .....	14
2.9.1 Fibra Óptica.....	14
2.10 ROUTER.....	17
2.11 DIRECCIONES IP.....	19
2.12 PROTOCOLO TCP .....	22
2.12.1 Significado De Los Diferentes Campos En El Modelo TCP .....	24
2.13 PROTOCOLO IP .....	24
2.14 ICMP.....	25
2.14.1 Solicitud De Eco Y Respuesta De Eco.....	26
2.15 SNMP y UDP.....	27
2.16 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) .....	27
2.16.1 ASN .....	32
2.16.2 Structure of Management Information (SMI) .....	32
2.16.2 MIB.....	33
2.16.3 OID.....	34
2.16.4 Elementos de procedimiento.....	35
2.16.5 Estructura de una PDU .....	36
2.16.6 GetRequest-PDU y GetNextRequest-PDU .....	36
2.16.7 SetRequest-PDU .....	37
2.16.8 GetResponse-PDU.....	37
2.16.9 Trap-PDU.....	38
2.17 Solarwinds Orion Network Performance Monitor.....	40
2.18 SMS.....	43
2.19 GSM. ....	43
CAPÍTULO 3. DISEÑO DE UN SISTEMA DE ALERTA DE CAÍDA DE UNA RED.....	46
3.1 Diagrama a Bloques .....	47
3.2 Diagrama de Flujo .....	48
3.3 BLOQUE I Configuración de Router .....	49
3.4 BLOQUE II Configuración Protocolo SNMP .....	58
3.5 BLOQUE III Alta en Plataforma de Monitoreo Solarwinds .....	59

3.6 BLOQUE IV Monitoreo de la Red Mediante la obtención y Análisis de Tráfico .....	63
3.7 BLOQUE V Configuración de alerta de la caída de Alguna Interfaz del Router.....	63
3.8 Bloque VI Configuración alerta vía mail y SMS.....	66
 CAPÍTULO 4 COMPORTAMIENTO DEL SISTEMA DE MONITOREO DE UNA RED EN FIBRA ÓPTICA .....	66
4.1 Configuración de router mediante cable de consola con la IP, para que tenga salida a internet.....	68
4.2 Monitoreo de la red mediante la obtención y análisis del tráfico de la misma.....	72
4.3 Configuración de alerta de la caída del sistema en la plataforma de monitoreo Solarwinds interfaz en primera instancia en la interfaz WAN.....	76
4.4 Reconexión de equipos para probar Sistema de Monitoreo.....	78
4.5 Diseño de Red de Fibra óptica en nueva ubicación.....	85
4.6 Configuración y pruebas con Equipo Huawei AR 1220 .....	86
CONCLUSIONES .....	96
REFERENCIAS .....	98
APENDICES.....	101
GLOSARIO.....	125

## ÍNDICE FIGURAS Y GRÁFICOS

Figura 1. Red LAN .....	5
Figura 2. Red WAN.....	6
Figura 3. Dispositivos conectados a Internet.....	6
Figura 4. Modelo OSI.....	7
Figura 5. Modelo TCP/IP.....	11
Figura 6. Medios Físicos de Transmisión.....	14
Figura 7. Tipos de Transmisión a través de Fibra Óptica .....	16
Figura 8. Router Cisco 2911 .....	19
Figura 9. comparación IP pública IP privada .....	21
Figura 10. IP Pública y Privada .....	22
Figura 11. Multiplexación y Demultiplexación en el Protocolo TCP.....	23
Figura 12. Esquema de datagrama Protocolo ICMP.....	25
Figura 13. Encabezado ICMP.....	26
Figura 14. Tipos de mensaje ICMP. ....	26
Figura 15. Arquitectura SNMP.....	28
Figura 16. Modelo Protocolo SNMP.....	29
Figura 17. Estructura Protocolo SNMP .....	30
Figura 18. NMS Y Elementos de la Red.....	31
Figura 19. Mensajes entre el NMS y el Agente.....	31
Figura 20. Estructura Jerárquica de la MIB-II.....	33
Figura 21. Categorías TCP/IP.....	34
Figura 22. Interfaz Gráfica Solarwinds.....	42
Figura 23. Arquitectura Básica GSM.....	44
Figura 24. Diagrama a Bloques.....	47
Figura 25. Diagrama de Flujo .....	48
Figura 26. Servicio de Internet.....	49
Figura 27. Router conectado a la corriente eléctrica.....	49
Figura 28. Se muestra el puerto de consola donde conectamos el cable.....	50
Figura 29. Se muestra el cable de consola sobre el router y esté conectado al puerto...50	50

Figura 30. Cable de consola conectado a CPU y Router.....	51
Figura 31. Conexión Hyperteminal.....	51
Figura 32. Interfaz de Conexión .....	52
Figura 33. Propiedades de la Interfaz de Conexión .....	52
Figura 34. Se logra comunicación con el router con Hyperterminal.....	53
Figura 35. Diagrama a bloques de la conexión Hyperterminal .....	53
Figura 36. Líneas que se escribieron para la configuración del router. ....	54
Figura 37. Router conectado a la red WAN.....	55
Figura 38. Ping enviado a la IP pública configurada en el router .....	55
Figura 39. Parte de la configuración del router.....	56
Figura 40. Router conectado a la PC para revisión de la configuración .....	56
Figura 41. Interfaces configuradas en el equipo router .....	56
Figura 42. Verificación de Router con salida internet con un ping hacia un DNS de Google.....	57
Figura 43. Servidor donde se encuentra alojada la aplicación Solarwinds.....	58
Figura 44. Parte trasera de servidor donde se encuentra alojada la aplicación Solarwinds.....	58
Figura 45. Aplicación Solarwinds.....	59
Figura 46. Pantalla para agregar el Nodo a Monitoreo.....	60
Figura 47. IP Pública configurada en el Sistema de Monitoreo.....	60
Figura 48. Test exitoso de la IP Pública.....	61
Figura 49. Interfaces descubiertas al momento de dar de alta en el monitoreo.....	62
Figura 50. Cambio de propiedades en el Nodo a Monitorear.....	63
Figura 51. Consola de configuración de alertas.....	64
Figura 52. Send an E-mail envía un e-mail una o más direcciones de correo electrónico.....	64
Figura 53. Definición de Alertas e Interfaces.....	65
Figura 54. Equipo ONT (Optical Network Terminal) .....	68
Figura 55. Nuevo equipo ONT que se reemplazó.....	69
Figura 56. Muestra del alcance del equipo desde la Red del proveedor.....	69
Figura 57. IP 10.207.121.82 dada de alta en sistema de monitoreo.....	70
Figura 58. Interfaces a Monitorear .....	71

Figura 59. Interfaces descubiertas del equipo Router.....	71
Figura 60. Pantalla donde se colocan las características e información sobre el Nodo... ..	72
Figura 61. Gráfica de Disponibilidad primer poleo. ....	72
Figura 62. Gráfica de Latencia & Pérdida de paquetes primer poleo.....	73
Figura 63. Interfaces Monitoreadas GigabitEthernet0/0 y GigabitEthernet0/2.....	73
Figura 64. Grafica de Disponibilidad Transcurrida una semana.....	73
Figura 65. Gráfica de Latencia & paquetes perdidos .....	74
Figura 66. Gráfica de consumo, en sistema no detecta consumo ya que aún no conectamos nada al router y por ende no hay tráfico.....	74
Figura 67. Gráficas de monitoreo durante una semana.....	75
Figura 68. IP del router dada de alta en el sistema de Monitoreo a través del Servidor donde encuentra alojada la aplicación Solar Winds.....	76
Figura 69. Configuración de texto a ser enviado .....	77
Figura 70. Pruebas realizadas sobre los diferentes mensajes que se pudieran recibir desde la aplicación Solarwinds. ....	77
Figura 71. Primer poleo después de la reconexión Disponibilidad.....	78
Figura 72. Ping extendido hacia la IP10.207.121.82.....	78
Figura 73. Maqueta de Prueba reconectada nuevamente Equipo Cisco y equipo ONT conectados a la corriente eléctrica y a la fibra óptica.....	79
Figura 74. Interfaz Gráfica del Solarwinds donde se muestra el estatus del Nodo el cual está en estado de down.....	79
Figura 75. Captura de pantalla de los SMS que llegan al celular.....	80
Figura 76. Captura de Pantalla de la llegada del mensaje en correo Gmail.....	80
Figura 77. Alertas que envía el Sistema de Monitoreo al correo de Gmail visto desde una computadora.....	81
Figura 78. a) Gráfica de Latencia y Pérdida de Paquetes durante 7 días.....	82
Figura 78. b) Gráfica de Disponibilidad durante 7 días.....	82
Figura 79. Edificio donde se realizó maqueta para hacer pruebas. ....	83
Figura 80. Caja de derivación de fibra óptica de donde dependerá el servicio.....	83
Figura 81. Fibra de 12 hilos con roseta existentes en el interior d vertical del sótano.....	84
Figura 82. Trayectoria de fibra saldrá de la roseta y se colocará en la escalerilla vertical encinchada y etiquetada .....	84

Figura 83. vertical en el piso donde se ubicará la maqueta.....	84
Figura 84. Punto llega la fibra óptica y de ahí se tendrá que realizar el tendido del cuarto de comunicaciones.....	85
Figura 85. Trayectoria que se siguió para colocar la fibra óptica .....	85
Figura 86. Este es el punto donde se realizó la instalación y donde va a estar la maqueta para realizar las pruebas .....	86
Figura 87. Router AR 1220 conectado a la PC para configuración.....	87
Figura 88. Pantalla para configuración de Router Huawei 1220 en MobaXterm.....	88
Figura 89. Equipo router AR 1220 conectado a la fibra óptica y ya encendido .....	88
Figura 90. Interfaces configuradas en el router ya con la IP asignada. ....	88
Figura 91. No se lograba salida a internet se realiza un trazado para detectar donde se estaba quedando la IP pública se observa que se queda en el Gateway de la ip pública.....	89
Figura 92. Ping hacia los DNS de Google alcanzando con éxito. ....	89
Figura 93. Trazado de la Ip Publica hacia los DNS. ....	90
Figura 94. Ping hacia la IP pública desde un servicio de Internet. ....	90
Figura 95. Trazado hacia la IP pública desde un servicio de Internet. ....	90
Figura 96. Interfaces que nos arroja el Sistema de Monitoreo para ser monitoreadas....	91
Figura 97. Equipo Router Huawei dado de alta en el sistema de monitoreo con la ip de gestión 10.253 25.212. ....	91
Figura 98. Equipo Ar Huawei 1220 en la vista de Monitoreo Solawinds.....	92
Figura 99. Gráfica de Disponibilidad Se observa que el enlace no ha tenido ninguna caída se encuentra operando de manera óptima.....	92
Figura 100. Gráfica de Latencia y pérdida de Paquetes cuando se estaban realizando las pruebas se observan conexión y desconexión de los equipos. ....	93
Figura 101 Gráfica de latencia y pérdida de paquetes cuando se estaban realizando las pruebas se observan conexión y desconexión de los equipos. ....	93
Figura 102. Alertas enviadas al correo de LOTUS durante las pruebas.....	93
Figura 103. Alertas enviadas al correo de LOTUS durante las pruebas .....	94
Figura 104. Alertas enviadas al correo GMAIL durante las pruebas .....	94
Figura 105. Alertas enviadas vía SMS durante las pruebas.....	95

## **MONITOREO DE UNA RED USANDO EL PROTOCOLO SNMP**

### **PLANTEAMIENTO DEL PROBLEMA**

Las redes de cómputo de las organizaciones, se vuelven cada vez más complejas y la exigencia de operación es cada vez más demandante. Por lo cual el análisis y monitoreo de redes se ha convertido en una labor cada vez más importante y de carácter proactivo para evitar problemas. Con un monitoreo de redes se logra entregar una velocidad óptima de red, confiabilidad y capacidad, para todos los usuarios, aplicaciones y servicios de red.

La red va a fallar en cualquier momento, eso es inevitable. Las fallas más frecuentes que ocurren son donde el medio de transmisión se daña, los más recurrentes un corte de fibra óptica, desalineación de las microondas, interferencia de frecuencias, falla de energía eléctrica en radiobase donde se encuentra el servicio, o una simple desconexión de un equipo. Lo importante es darte cuenta a tiempo sobre el problema y saber la causa para solucionarlo rápidamente. Se necesita anticipar a los problemas.

Por lo que se hace necesario tener un sistema de monitoreo de redes que permita la detección temprana de los problemas que pueda llegar a tener la red, así como el mantenimiento de los servicios que estas redes proporcionan.

La gestión se está convirtiendo en un elemento esencial para asegurar la disponibilidad tanto física como lógica de las redes metropolitanas. Ya que las empresas ofrecen un cierto SLA (Service Level Agreement) a sus clientes, el cliente va a penalizar cierta cantidad de dinero dependiendo de cuánto tiempo este fuera su servicio, esto será de acuerdo a su tiempo de facturación. La complejidad de las actuales redes impone la necesidad de utilizar sistemas de gestión capaces de controlar, administrar y monitorizar redes locales, metropolitanas y extensas, a la vez que dispositivos de interconexión, servidores y clientes.

La tendencia en la evolución de la tecnología de gestión de redes se encamina hacia el desarrollo de productos integrados capaces de gestionar conjuntamente la red en sus diferentes niveles medio físico, de transmisión, aplicaciones, etc.

Por ejemplo, la empresa ISAT se encuentra trabajando con el software de monitoreo SNMPC Management Console, SNMPC Enterprise es un sistema de gestión de seguridad distribuida de la red que proporciona monitoreo en tiempo real proactiva para toda su infraestructura de red.

La empresa GDC (General DataComm) se encuentra trabajando con un sistema de monitoreo de redes llamado PRTG el cuál proporciona una monitorización de redes concisa, potente esta

también ofrece gráficos tanto de consumo y disponibilidad para su análisis, pero el software se puede tornar un tanto difícil para el usuario final.

Para efectuar un análisis del impacto de la implementación de una solución de negocios en la infraestructura de red, sugerimos utilizar una solución de monitoreo de red, la cual permita observar el comportamiento de la red mediante gráficas, cuando se tenga una caída en la red este mande una alarma al correo electrónico y SMS. Mediante las gráficas se podrá observar cuándo se tengan tiempos altos de respuesta, cuándo este saturando el ancho de banda, y con esto se evitarán problemas futuros. Además de que podremos darnos cuenta cuando el servicio tenga caídas y atenderlo lo más rápido posible.

## **JUSTIFICACIÓN**

Realizar la configuración de un router con una IP para poder monitorearlo mediante un software Solarwinds obteniendo gráficas de tráfico y disponibilidad para poder evitar saturación en la red y esté tenga un mejor rendimiento; cuando haya una caída del servicio se avisé por vía email o un SMS, con esto se evitaran las pérdidas causadas por fallos en la red sin detectar. Se contará con información oportuna para conocer el estado de un enlace. Se llevará un registro histórico de la información. Y lo más importante se dará atención oportuna a la caída de la red, enterándonos rápidamente mediante el aviso que va a enviar.

Con el aviso oportuno se podrán evitar pérdidas tanto económicas para el ISP y para nuestra red, también se evitarán penalizaciones y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

## **OBJETIVOS**

## **OBJETIVO GENERAL**

Construcción e implementación de un sistema de monitoreo de una red que provee servicios de internet a través de fibra óptica mediante el protocolo SNMP configurado en un router, a fin de monitorear el comportamiento de la red WAN y LAN en una plataforma Solarwinds y alertar de la caída del router enviando mensajes SMS y correo electrónico al administrador.

## **OBJETIVOS PARTICULARES**

Configuración de router mediante cable de consola con la IP, para que tenga salida a internet.

Configurar el protocolo SNMP en el router.

Dar de alta el router en el sistema de monitoreo Solarwinds.

Monitoreo de la red mediante la obtención y análisis del tráfico de la misma.

Configurar alerta de la caída del sistema en la plataforma de monitoreo Solarwinds interfaz en primera instancia en la interfaz WAN.

Configurar alertas vía correo electrónico y SMS a través de los servidores donde se encuentra alojada la aplicación de Solarwinds y un servidor que se tiene para envío de mensajes SMS.

# **CAPÍTULO 1.**

# **INVESTIGACIONES PREVIAS DEL MONITOREO DE REDES**

## **1.1 SISTEMAS DE MONITOREO EN REDES**

La Unión Internacional de Telecomunicaciones en su artículo Empresa Eficiente: Metodologías, Modelación y Aplicación para fines de Regulación Tarifaria habla sobre las necesidades de información para fines regulatorios básicas para empresas de comunicaciones, en el cuál propone que las empresas que ofrecen servicios de comunicaciones como venta de servicios de internet deben tener un órgano regulatorio para que se pague de acuerdo al nivel de servicio y propone lo siguiente:

**Estadísticas de Tráficos:** Para estimar la demanda de los servicios sujetos a regulación también será necesario establecer los niveles históricos de consumo de los usuarios en función de sus relaciones relevantes con otras redes. En general, se deberán identificar los tráficos por servicios.

En la tesis llamada " Monitoreo De La Red Aplicando El Protocolo SNMP en la Empresa Superautos Universidad S.A. de C.V." (IPN ESIME). Propone una solución con la finalidad de reducir tiempos de respuesta en la detección y corrección de fallas en dispositivos o en enlaces en la red de datos, así como la centralización de la administración y mantenimiento de la red de una manera proactiva y eficiente, resumiendo sería detección de fallas, y mejoramiento del rendimiento de dicha red, documentación y reporteo.

En el artículo que publica la Universidad Tecnológica de la Mixteca, capítulo 4 "El Router Cisco" menciona lo siguiente en forma general los routers Cisco están diseñados principalmente para enrutar el tráfico de una red, y como segunda función, tienen incorporada una tecnología de filtrado de paquetes. Los routers proporcionan el hardware y el software necesarios para encaminar paquetes entre redes. Se trata de dispositivos importantes de interconexión que permiten conectar subredes LAN y establecer conexiones de redes de área amplia entre las subredes.

La conexión física entre el router y un tipo de medio físico de la red se realiza a través de una interfaz, las interfaces del router a menudo se denomina puertos y cada puerto viene designado físicamente de acuerdo con la topología de red a la que sirve.

Como se observó en el artículo que se publica en la revista de la ITU Unión Internacional de Telecomunicaciones Empresa Eficiente: Metodologías, Modelación y Aplicación para fines de Regulación Tarifaria se pretende crear regulaciones sobre el cobro de servicios de internet; en la Tesis “ Monitoreo de una Red usando el protocolo SNMP” al dar de alta el router en la plataforma Solarwinds se van a poder obtener gráficas las cuales como se menciona en el

artículo necesitan Estadísticas de Tráfico, esto lo lograremos con la configuración de SNMP en el router, ya que con esto podremos monitorear el tráfico.

Las gráficas obtenidas servirán para cobrar de acuerdo a la disponibilidad que se haya tenido ya que tendremos en la plataforma Solarwinds gráficas de hasta un año de antigüedad. Con esto se logrará que el cliente pague lo justo y esto se podrá demostrar con dichas gráficas.

En la tesis Monitoreo De La Red Aplicando El Protocolo SNMP en la Empresa Superautos Universidad S.A. de C.V. se propone el sistema de monitoreo para una red LAN, la tesis propuesta pretende ser a nivel Wan, ya que se podrá observar la disponibilidad del enlace WAN, se obtendrán reportes y se atenderán fallas rápidamente con la configuración de las alarmas que se propone.

Con base en los artículos leídos se propone esta tesis con el fin de poder mejorar el servicio que ofrece una empresa que provee servicios de Internet MPLS y VPN's, poder monitorear todos los enlaces, cobrar lo justo, observar degradación en los servicios mediante las gráficas de monitoreo, atender fallas oportunamente la alarma enviada vía e-mail y SMS.

# **CAPÍTULO 2.**

**CONSTRUCTOS  
TEÓRICOS  
METODOLÓGICOS  
PARA EL MONITOREO  
DE REDES.**

Las redes interconectan computadoras con distintos sistemas operativos, ya sea dentro de una empresa u organización (LAN's) o por todo el mundo (WAN's, Internet). Anteriormente se utilizaban básicamente para compartir los recursos de las computadoras conectadas. Hoy, las redes son medios de comunicación internacional a través de las cuales se intercambian grandes volúmenes de datos.

## 2.1 Redes Locales (LAN)

Las redes son conjuntos de ordenadores independientes que se comunican entre sí a través de un medio de red compartido. Las Local Área Network (LAN) redes de área local son aquellas que conectan una red de ordenadores normalmente confinadas en un área geográfica, como un solo edificio o un campus de la universidad. Las LAN, sin embargo, no son necesariamente simples de planificar, ya que pueden unir muchos centenares de ordenadores y pueden ser usadas por muchos miles de usuarios. El desarrollo de varias normas de protocolos de red y medios físicos han hecho posible la proliferación de LAN's en grandes organizaciones multinacionales, aplicaciones industriales y educativas.

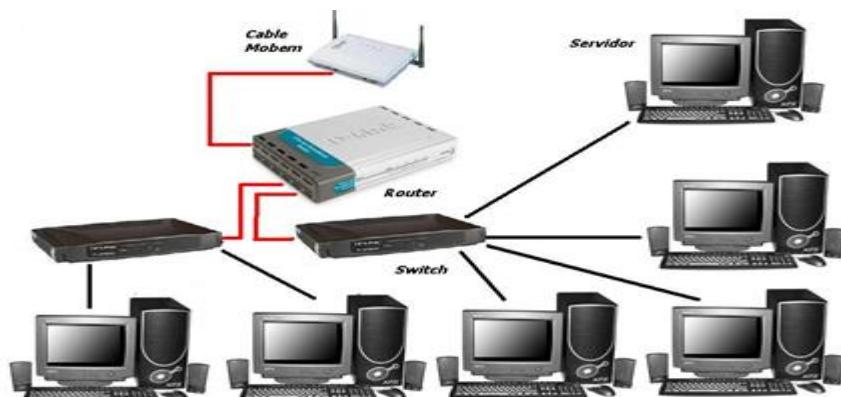


Figura 1 Red LAN

## 2.2 Redes de Área Extensa (WAN)

A menudo una red se localiza en situaciones físicas múltiples. Las redes (WAN) Wide Area Network, de área extensa conectan múltiples redes LAN que están geográficamente dispersas. Esto se realiza conectando las diferentes LAN's mediante servicios que incluyen líneas telefónicas alquiladas (punto a punto), líneas de teléfono normales con protocolos síncronos y asíncronos, enlaces vía satélite, y servicios portadores de paquetes de datos.



Figura 2 Red WAN

## 2.3 Internet

Con el meteórico auge en demanda para la conectividad, Internet se ha convertido en la autopista de comunicaciones para millones de usuarios. Internet fue usado inicialmente por el ejército y las instituciones académicas, pero ahora es un cauce de información completo para cualquiera, en todas las formas de información y comercio. Los sitios World Wide Web (WWW) de Internet proporcionan ahora recursos personales, educativos, políticos y económicos.



Figura 3 Dispositivos conectados a Internet

## **2.4 Protocolos**

Los protocolos de red son normas que permiten a los ordenadores comunicarse. Un protocolo define la forma en que los ordenadores deben identificarse entre sí en una red, la forma en que los datos deben transitar por la red, y cómo esta información debe procesarse una vez que alcanza su destino final. Los protocolos también definen procedimientos para gestionar transmisiones o "paquetes" perdidos o dañados.

Aunque cada protocolo de la red es diferente, todos pueden compartir el mismo cableado físico. Este concepto es conocido como "independencia de protocolos," lo que significa que dispositivos que son compatibles en las capas de los niveles físicos y de datos permiten al usuario ejecutar muchos protocolos diferentes sobre el mismo medio físico.

## **2.5 MODELO OSI**

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), también llamado OSI (Open System Interconnection) es el modelo de red descriptivo, que fue creado por la ISO (Organización Internacional para la Estandarización) en el año 1980. Es un marco de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones.

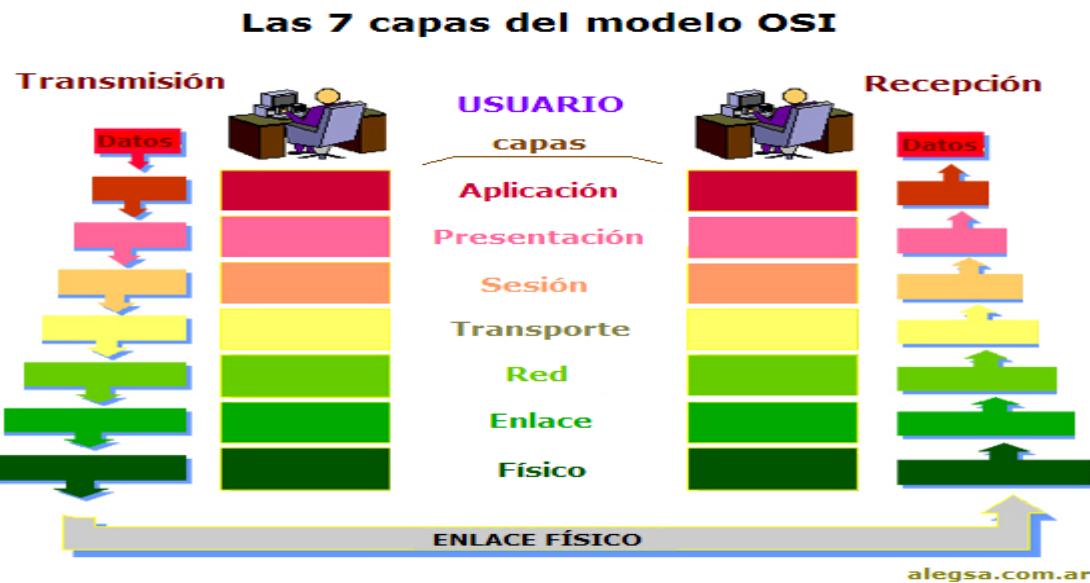


Figura 4 Modelo OSI

## 2.5.1 Capa física

La capa física, la más baja del modelo OSI, se encarga de la transmisión y recepción de una secuencia no estructurada de bits sin procesar a través de un medio físico. Describe las interfaces eléctricas/óptica, mecánica y funcional al medio físico, y lleva las señales hacia el resto de capas superiores. En la capa física las tramas procedentes de la capa de enlace de datos se convierten en una secuencia única de bits que puede transmitirse por el entorno físico de la red. La capa física también determina los aspectos físicos sobre la forma en que el cableado está enganchado a la NIC de la computadora.

## 2.5.2 Capa de vínculo de datos ó enlace

La capa de vínculo de datos ofrece una transferencia sin errores de tramas de datos desde un nodo a otro a través de la capa física, permitiendo a las capas por encima asumir virtualmente la transmisión sin errores a través del vínculo.

Cuando los paquetes de datos llegan a la capa de enlace de datos, estas pasan a ubicarse en tramas (unidades de datos), que vienen definidas por la arquitectura de red que se está utilizando. La capa de enlace de datos se encarga de desplazar los datos por el enlace físico

de comunicación hasta el nodo receptor, e identifica cada computadora incluida en la red de acuerdo con su dirección de hardware

La información de encabezamiento se añade a cada trama que contenga las direcciones de envío y recepción. La capa de enlace de datos también se asegura de que las tramas enviadas por el enlace físico se reciben sin error alguno.

### **2.5.3 Capa de red**

La capa de red controla el funcionamiento de la subred, decidiendo qué ruta de acceso física deberían tomar los datos en función de las condiciones de la red, la prioridad de servicio y otros factores. Proporciona: Enrutamiento: enruta tramas entre redes.

La capa de red encamina los paquetes además de ocuparse de entregarlos. La determinación de la ruta que deben seguir los datos se produce en esta capa, lo mismo que el intercambio efectivo de los mismos dentro de dicha ruta, La Capa 3 es donde las direcciones lógicas (como las direcciones IP de una computadora de red) pasan a convertirse en direcciones físicas (las direcciones de hardware de la NIC, la Tarjeta de Interfaz para Red, para esa computadora específica).

Los routers operan precisamente en la capa de red y utilizan los protocolos de encaminamiento de la Capa 3 para determinar la ruta que deben seguir los paquetes de datos.

### **2.5.4 Capa de transporte**

La capa de transporte garantiza que los mensajes se entregan sin errores, en secuencia y sin pérdidas o duplicaciones. Libera a los protocolos de capas superiores de cualquier cuestión relacionada con la transferencia de datos entre ellos y sus pares. El tamaño y la complejidad de un protocolo de transporte dependen del tipo de servicio que pueda obtener de la capa de transporte. Para tener una capa de transporte confiable con una capacidad de circuito virtual, se requiere una mínima capa de transporte. Si la capa de red no es confiable o solo admite datagramas, el protocolo de transporte debería incluir detección y recuperación de errores extensivos.

Encargada de controlar el flujo de datos entre los nodos que establecen una comunicación; los datos no solo deben entregarse sin errores, sino además en la secuencia que proceda. La capa de transporte se ocupa también de evaluar el tamaño de los paquetes con el fin de que estos tengan el tamaño requerido por las capas inferiores del conjunto de protocolos.

Protocolos: TCP: Los protocolos orientados a la conexión operan de forma parecida a una llamada telefónica:

UDP: El funcionamiento de los protocolos sin conexión se parece más bien a un sistema de correo regular.

### **2.5.5 Capa de sesión**

La capa de sesión permite el establecimiento de sesiones entre procesos que se ejecutan en diferentes estaciones. Proporciona: Establecimiento, mantenimiento y finalización de sesiones: permite que dos procesos de aplicación en diferentes equipos establezcan, utilicen y finalicen una conexión, que se denomina sesión.

### **2.5.6 Capa de presentación**

La capa de presentación da formato a los datos que deberán presentarse en la capa de aplicación. Se puede decir que es el traductor de la red. Esta capa puede traducir datos de un formato utilizado por la capa de la aplicación a un formato común en la estación emisora y, a continuación, traducir el formato común a un formato conocido por la capa de la aplicación en la estación receptora.

### **2.5.7 Capa de aplicación**

El nivel de aplicación actúa como ventana para los usuarios y los procesos de aplicaciones para tener acceso a servicios de red. Esta capa contiene varias funciones que se utilizan con frecuencia: Uso compartido de recursos y redirección de dispositivos.

## **2.6 Modelo TCP/IP**

La familia de protocolos TCP/IP se desarrolló antes que el modelo OSI. Por lo tanto, los niveles de Protocolo de Control de Transmisión/Protocolo de Red (TCP/IP) no coinciden exactamente con los del modelo OSI. El protocolo TCP/IP está compuesto por cuatro niveles: acceso a red, internet, transporte y aplicación.

### **2.6.1 Acceso a red**

Especifica información de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado. Los protocolos usados en este nivel son Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS -232, v.35.

### **2.6.2 Internet**

Empaque los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP. Se usan los protocolos IP, ICMP, ARP, RARP.

### **2.6.3 Transporte**

Permite administrar las sesiones de comunicación entre equipos host. Define servicio y el estado de la conexión utilizada al transportar datos. Los protocolos que se manejan en este nivel son TCP, UDP.

### **2.6.4 Aplicación**

Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red. Se usan los protocolos HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación. Microsoft, El modelo TCP/IP, 2003) MONITORIZACIÓN DE SERVICIOS DE RED Y SERVIDORES.

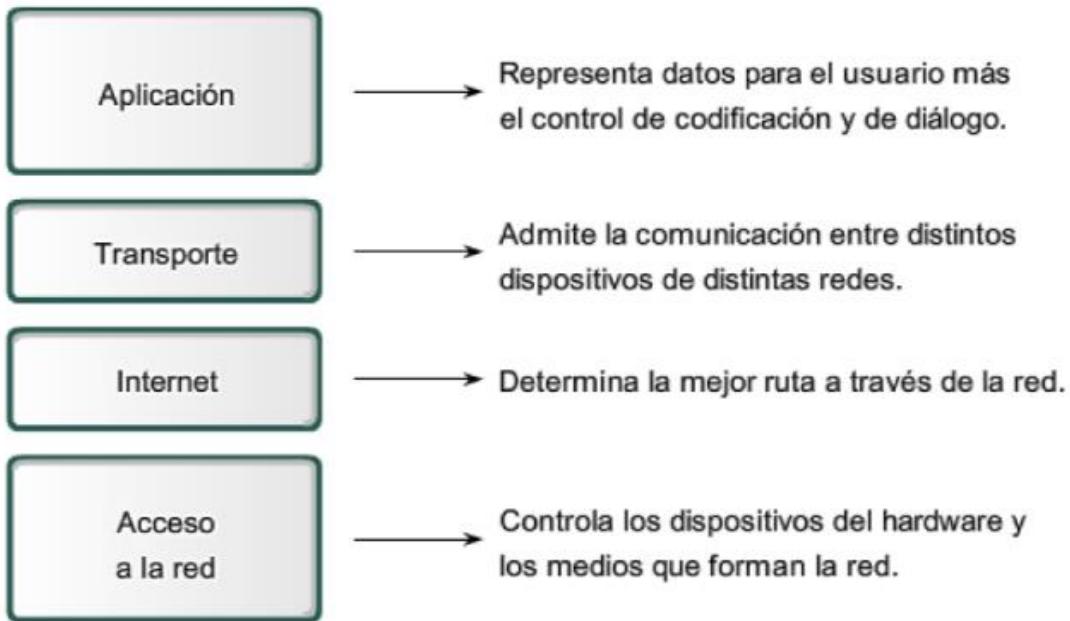


Figura 5 Modelo TCP/IP

## 2.7 Comparación modelo OSI & TCP/IP

Ambos se dividen en capas.

.Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.

Ambos tienen capas de transporte y de red similares.

Se supone que la tecnología es de conmutación por paquetes (no de conmutación por circuito).

TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.

TCP/IP combina las capas de enlace de datos y la capa física del modelo OSI en una sola capa.

TCP/IP parece ser más simple porque tiene menos capas.

Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

## 2.8 Puertos

Son canales que utiliza el subsistema de red para re direccionar la información al programa apropiado. Son una numeración lógica que se asigna a las conexiones tanto en el origen como en el destino. No tiene ninguna significación física. Están representados por un número de 16 bits usado para identificar los puntos finales de la conexión, en las cabeceras TCP o UDP. Los números de puerto oscilan entre 0 y 65,535. Se tienen tres categorías para su clasificación:

Puertos bien conocidos o reservados Son puertos del 0 al 1023. Se utilizan para servicios de red bien conocidos como son FTP<sup>4</sup> , HTTP<sup>5</sup> , SMTP<sup>6</sup> , DNS<sup>7</sup> entre otros. TCP<sup>8</sup> y UDP<sup>9</sup> utilizan estos puertos para determinar el servicio correcto ya que son puertos predeterminados para cada aplicación y están controlados por la IANA (Internet Assigned Numbers Authority) o Agencia de Asignación de Números de Internet.

Puertos registrados Oscilan entre 1024 y 49151. Pueden ser usados de manera temporal por los clientes, pero también pueden representar servicios registrados por un tercero.

Puertos dinámicos o privados Oscilan entre 49152 y 65535. Pueden también ser usados por el cliente, pero se utilizan con menos frecuencia.

20 - FTP Data - Utilizado por servidores FTP (File Transfer Protocol) para la transmisión de datos en modo pasivo.

21 - FTP - También utilizado por servidores FTP. Su mala configuración puede resultar en ataques (troyanos, hacking, etc..).

22 - SSH - Puerto utilizado por Secure Shell (SSH), el cual es un protocolo y un programa que lo utiliza para acceder a máquinas remotas a través de una red. Además, funciona como una herramienta de transmisión de datos, desde ficheros sueltos hasta una sesión de FTP cifrado.

23 - Telnet - Telnet es una herramienta que proporciona una ventana de comandos, los cuales permiten controlar una pc de forma remota.

25 - SMTP - Puerto utilizado por SMTP (Simple Mail Transfer Protocol), o en español Protocolo de transferencia simple de correo electrónico. Es el protocolo, basado en texto, que permite transferir correo electrónico entre diferentes computadoras, PDA's, celulares, etc.

53 - DNS - Este puerto lo utiliza el DNS (Domain Name System), esta base de datos distribuida o jerárquica, se encarga de traducir nombres de dominios a IP's.

59 - DCC - Utilizado principalmente en programas de comunicación para transferir ficheros.

80 - HTTP - Puerto que transmite el protocolo HTTP (Hypertext Transfer Protocol) que es el utilizado en cada transacción web (WWW).

113 - IDENT - Servicio de identificación/autorización. Los servidores de internet, como POP, IMAP, SMTP, IRC consultan este puerto en respuesta a conexiones de clientes.

443 - HTTPS - El Hypertext Transfer Protocol Secure, no es más que una versión segura, del ya mencionado HTTP.

8080 - WebProxy - Este puerto lo pueden utilizar terceros para ocultar su verdadero IP a los servidores web.

## 2.9 Medios Físicos

Una parte importante en el diseño e instalación de una red es la correcta selección del medio físico apropiado al entorno existente. Actualmente, se emplean, básicamente, cuatro tipos de cableados o medios físicos: coaxial grueso para redes 10BASE5, coaxial fino para redes 10BASE2, par trenzado no apantallado (UTP) para redes 10BASE-T o 100Base-TX y fibra óptica para redes 10BASE-FL o 100BASE-FX. Esta amplia variedad de medios físicos refleja la evolución de Ethernet y la flexibilidad de la tecnología.

Cada tipo tiene sus ventajas e inconvenientes. La adecuada selección del tipo de medio apropiado para cada caso, evitará costes de recableado, según vaya creciendo la red.



Figura 6 Medios Físicos de Transmisión

## 2.9.1 Fibra Óptica

Un Sistema de Comunicaciones es aquél que sirve para transmitir información de un lugar a otro, ya sea que estén separados por unos cuantos metros o por distancias intercontinentales. Usualmente la información es transportada por una onda electromagnética de alta frecuencia denominada onda portadora, cuya frecuencia puede variar desde algunos kilohertz hasta cientos de terahertz. Los sistemas de comunicaciones ópticas utilizan señales portadoras de altas frecuencias (alrededor de 100 THz) en la región visible o en la de infrarrojo cercano del espectro electromagnético. En ocasiones estos sistemas son llamados sistemas de ondas luminosas para distinguirlos de los sistemas de microondas, cuyas frecuencias portadoras son típicamente cinco órdenes de magnitud más pequeñas (alrededor de 1GHz). Los sistemas de comunicaciones de fibra óptica son sistemas de comunicación ópticos que utilizan fibras ópticas como líneas de transmisión.

En principio un sistema óptico de comunicaciones se diferencia de un sistema de microondas únicamente por el rango de frecuencias de sus ondas portadoras. Las frecuencias de las portadoras ópticas son típicamente de alrededor de 200 THz, en contraste con las portadoras de sistemas de microondas, con frecuencias desde 300 MHz hasta 300 GHz.

El espectro de la frecuencia electromagnética total se extiende de las frecuencias subsónicas a los rayos cósmicos;

El espectro de frecuencia de luz se puede dividir en tres zonas generales:

1. Infrarroja
2. Visible
3. Ultravioleta

La fibra óptica es un medio fino (entre 2 y 125 $\mu\text{m}$ ), transporta rayos de luz. El material con el que está construido puede ser de plástico, vidrio o silicio. Existen dos tipos: monomodo y multimodo.

Una fibra óptica multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. El hecho de que se propaguen más de un modo supone que no llegan todos a la vez al final de la fibra por lo que se usan comúnmente en aplicaciones de corta

distancia, menores a 1 km, ya que este efecto supone un problema a la hora de utilizarlas para mayores distancias. Además, son fáciles y económicas a la hora de diseñarlas.

En este tipo de fibra el diámetro del núcleo suele ser de 50 o 62.5  $\mu\text{m}$  y el diámetro del revestimiento de 125  $\mu\text{m}$ . Debido a que el tamaño del núcleo es grande, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión, es decir, que permite la utilización de electrónica de bajo costo. La propagación de los modos de este tipo de fibra es diferente según el tipo de índice de refracción del núcleo:

Salto de índice: el índice es constante en todo el núcleo, lo que da lugar a una gran dispersión modal.

Gradiente de índice: el índice es diferente ya que el núcleo está formado por diferentes materiales. En este caso la dispersión modal es menor.

Por esto que acabamos de ver, como la fibra multimodo soporta más de un modo de propagación se ve limitada por la dispersión modal.

Por otro lado, conviene señalar que las características de las fibras multimodo dependen radicalmente de las condiciones de inyección de potencia (de la excitación de modos).

En las fibras monomodo solo se propaga un modo de luz. El diámetro del revestimiento es de 125  $\mu\text{m}$ , igual que en las multimodo. Sin embargo, el diámetro del núcleo es mucho menor, de unas 9  $\mu\text{m}$ . Este hecho hace que su transmisión sea paralela al eje de la fibra y que, a diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de información. A continuación, podemos ver la comparación entre los dos tipos de propagación en la fibra multimodo así como la propagación en la fibra monomodo:

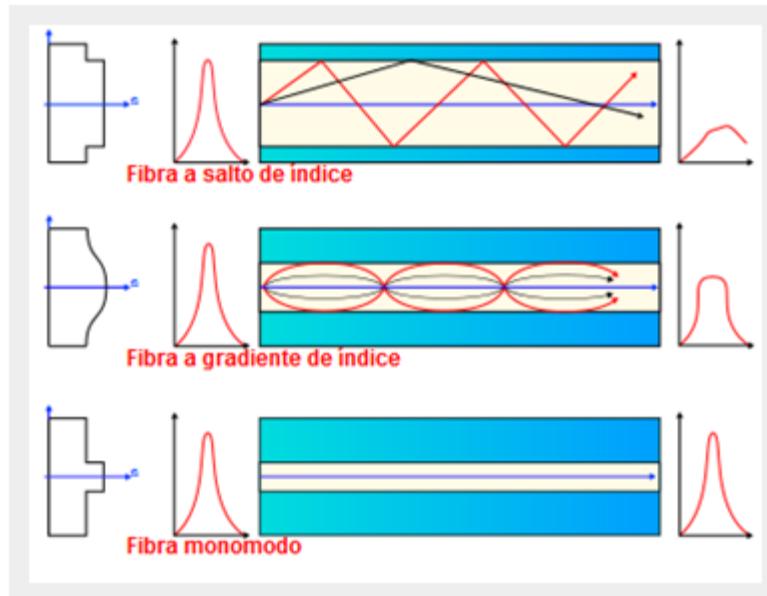


Figura 7 Tipos de Transmisión a través de Fibra Óptica

Las fibras monomodo se utilizan con mayor frecuencia en la investigación científica de alta precisión debido a que la luz se propague por un solo modo hace que sea más fácil enfocar correctamente.

Para distinguir ambos tipos de fibra se suelen utilizar ‘chaquetas de colores’. La norma TIA-598C recomienda, para aplicaciones civiles, el uso de una chaqueta amarilla para la fibra monomodo y de la naranja u otro color para la multimodo, dependiendo del tipo.

Para las aplicaciones especializadas son populares los segmentos Ethernet de fibra óptica, o 10BASE-FL. El cable de fibra óptica es más caro, pero es inestimable para las situaciones donde las emisiones electrónicas y los riesgos medioambientales son una preocupación. El cable de fibra óptica puede ser útil en áreas donde hay grandes cantidades de interferencias electromagnéticas.

La norma Ethernet permite segmentos de cable de fibra óptica de dos kilómetros de longitud, haciendo Ethernet a fibra óptica perfecto para conectar nodos y edificios que de otro modo no podrían ser conectados con cableados de cobre.

Una inversión en cableado de fibra óptica puede ser algo revalorizable, dado que según evolucionan las tecnologías de redes, y aumenta la demanda de velocidad, se puede seguir utilizando el mismo cableado, evitando nuevos gastos de instalación.

## 2.10 Router

Un router es un dispositivo de red que como su propio nombre indica se encarga de llevar por la ruta adecuada el tráfico.

Los routers funcionan utilizando direcciones IP para saber a donde tienen que ir los paquetes de datos no como ocurre en los switches. Gracias a estas direcciones, que son únicas para cada máquina, este dispositivo puede conocer por donde debe enviar el paquete.

El router es la estructura básica de las redes, que cuenta con las siguientes capacidades:

- Puede soportar simultáneamente diferentes protocolos haciendo compatible todos los equipos en la capa de red.
- Conecta a la perfección LAN a WAN.
- Filtral al exterior el tráfico no deseado aislando áreas en las que los mensajes se pueden difundir a todos los usuarios de una red.
- Actúan como puertas de seguridad comprobando el tráfico mediante listas de permisos de acceso.
- Asegura fiabilidad, ofreciendo múltiples trayectorias a través de las redes.
- Aprende automáticamente nuevas trayectorias y selecciona las mejores.

Los routers son computadoras dedicadas al procesamiento de la interconexión de redes, que no incluyen monitor, ni teclado, ni ratón, por lo que debe comunicarse con ellos de una de las siguientes formas:

Desde una terminal (PC o estación de trabajo funcionando en modo terminal) conectada a él mediante un cable.

Mediante un punto de la red. Dado que los routers son los enlaces que mantienen unidas las redes, el diseño de medidas de seguridad dentro de ellos es muy importante; la primera medida que se debe tomar en cuenta es la asignación de contraseña para no permitir el acceso al público en general.

Los puertos modulares designan sus puertos por el tipo de conexión que utilizan, seguido del número de ranura y del número de puerto. Por ejemplo, el primer puerto Ethernet en una tarjeta Ethernet instalada en la primera ranura del router se designaría como Ethernet 1/0.

Los routers construyen tablas de encaminamiento, ejecutan comandos y encaminan paquetes por las interfaces de red mediante el uso de protocolos específicos de encaminamiento. Esto significa que el router tiene que tener potencia de procesamiento, algún tipo de capacidad de almacenamiento y memoria disponible de acceso aleatorio. También requiere de un software adecuado, como un sistema operativo, que le permita configurar los protocolos de encaminamiento y los protocolos de encaminado, este sistema operativo se conoce como el IOS. (Interworking Operating System).



Figura 8 Router Cisco 2911

## 2.11 Direcciones IP

Los equipos comunican a través de Internet mediante el protocolo IP (Protocolo de Internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26 es una dirección IP en formato técnico. Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una

dirección IP exclusiva. El organismo a cargo de asignar direcciones públicas de IP, es decir, direcciones IP para los equipos conectados directamente a la red pública de Internet, es el ICANN (Internet Corporation for Assigned Names and Numbers) que remplaza el IANA desde 1998 (Internet Assigned Numbers Agency). Una dirección IP tiene dos partes diferenciadas: los números de la izquierda indican la red y se les denomina netID (identificador de red). Los números de la derecha indican los equipos dentro de esta red.

Existen dos tipos de IP, privada y pública.

IP pública: es la dirección que está visible desde Internet, suele ser la dirección que tiene el router o modem y normalmente la proporciona tu ISP, la compañía con la que accedes a Internet.

Las direcciones IP públicas son aquellas que permiten que cada dispositivo conectado a una red pueda ser identificado. Cuando un dispositivo se conecta a internet se le asigna una dirección IP de las que disponga su proveedor de acceso (ISP, Internet Service Provider). Cuándo esta persona escribe el nombre de un dominio en el navegador, este nombre es convertido en la dirección IP del servidor dónde está alojada la web con ese nombre (un servidor no es más que un ordenador conectado a internet que aloja las páginas web y las envía a los usuarios que las solicitan). La dirección IP del servidor es una dirección IP pública y el servidor utiliza la dirección IP pública del usuario para saber dónde enviar la información de vuelta.

IP privada: es la dirección de tu ordenador o dispositivo de red y está dentro de ésta, pertenece a una red privada.

Cuándo se crea una red de trabajo local en la que se conectan diversos ordenadores y dispositivos entre sí, ya sea con cables o través de WiFi, están formando una red privada. Dentro de esta red cada dispositivo conectado dispone de una dirección IP para poder ser reconocido dentro de la red y así poder compartir información y recursos. Los dispositivos de esta red no se comunican con los dispositivos de otra red directamente, por lo que varias redes pueden utilizar las mismas direcciones IP internas, estas son IP privadas. Un router, o

enrutador, se encarga de asignar la IP privada a cada dispositivo de la red y direccionar los datos y comunicación entre ellos según las IP privadas asignadas.

La red local se puede conectar a su vez a una red pública como internet. Esta conexión a internet normalmente se realiza a través del mismo router y es al router al que se le asigna una dirección IP pública por parte del proveedor de acceso a internet. De este modo la información entre la red pública (internet) y la red privada se produce entre internet y el router utilizando la dirección IP pública. El router dirige la información que recibe desde internet hacia el ordenador adecuado a través de la dirección IP privada. En otras palabras, una red local se identifica en internet con una sola dirección IP pública y los dispositivos que componen la red local se identifican entre sí mediante IP privadas. La red local más pequeña se compone de un sólo dispositivo conectado a un router.



Figura 9 comparación IP pública IP privada

La IP privada está dentro de unos **rangos reservados** para este tipo de dirección.

1. De 10.0.0.0 a 10.255.255.255
2. De 172.16.0.0 a 172.31.255.255
3. De 192.168.0.0 a 192.168.255.255

A través de la configuración de la red interna, se puede elegir la IP que se quiera dentro de estos tres rangos cumpliendo dos requisitos, no asignar la misma IP a dos equipos de la red y que todos los equipos que pertenecen a la red tengan en común los tres primeros dígitos.

La dirección IP es útil para identificar dispositivos que están conectados a una red ya que es un número único e irrepetible.

## Ventajas

Disminuye los costes de operación a las entidades proveedoras de servicios de Internet (ISP).

Minimiza el número de IP asignadas de forma fija inactivas.

## Inconvenientes

Obliga a depender de servicios que redirigen un host a una IP.

Las direcciones IP de los PCs de una red local son direcciones privadas ya que los PCs no están directamente conectados a Internet. Solamente el router dispone de conexión directa a Internet y por eso es el único que dispone de una dirección IP pública.

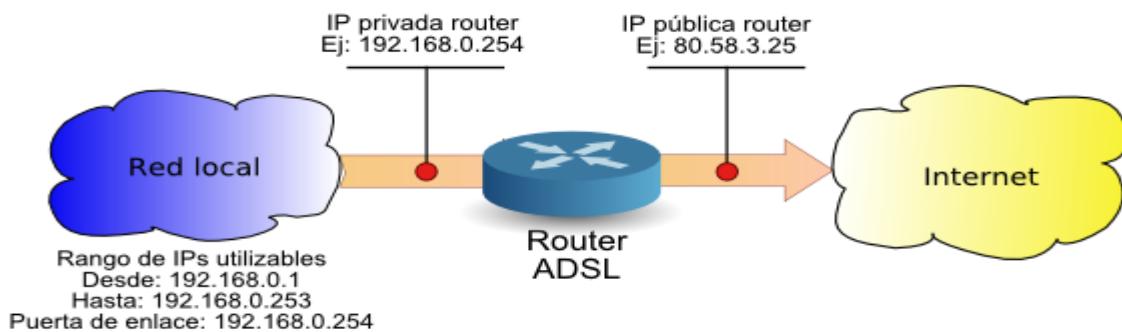


Figura 10 IP Pública y Privada

## 2.12 Protocolo TCP

TCP (Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Las principales características del protocolo TCP son las siguientes:

TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.

TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.

TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.

TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.

TCP permite comenzar y finalizar la comunicación amablemente.

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que decimos que estamos en un entorno Cliente-Servidor.

Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman segmentos.

TCP posibilita la realización de una tarea importante: multiplexar/demultiplexar; es decir transmitir datos desde diversas aplicaciones en la misma línea o, en otras palabras, ordenar la información que llega en paralelo.

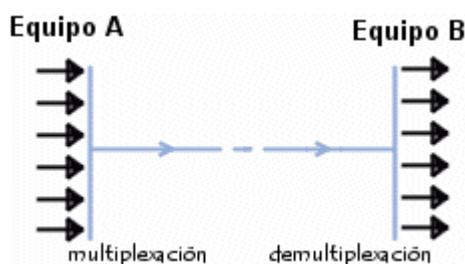


Figura 11 Multiplexación y Demultiplexación en el Protocolo TCP

Estas operaciones se realizan empleando el concepto de puertos (o conexiones), es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

### **2.12.1 Significado de los diferentes campos en el modelo TCP**

Puerto de origen: es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo representa una dirección de respuesta para el destinatario. Por lo tanto, este campo es opcional. Esto significa que si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero. En este caso, el destinatario no podrá responder (lo cual no es estrictamente necesario, en particular para mensajes unidireccionales).

Puerto de destino: este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.

Longitud: este campo especifica la longitud total del segmento, con el encabezado incluido. Sin embargo, el encabezado tiene una longitud de  $4 \times 16$  bits (que es  $8 \times 8$  bits), por lo tanto la longitud del campo es necesariamente superior o igual a 8 bytes

Suma de comprobación: es una suma de comprobación realizada de manera tal que permita controlar la integridad del segmento.

### **2.13 Protocolo IP**

El protocolo Internet Protocol IP es la base fundamental de la Internet. Porta datagramas de la fuente al destino. El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Las principales características de este protocolo son:

Protocolo NO orientado a conexión.

Fragmenta paquetes si es necesario.

Direccionamiento mediante direcciones lógicas IP de 32 bits.

Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.

## 2.14 ICMP

ICMP es un protocolo de control (Internet Control Message Protocol), que sirve para avisar de los errores en el procesamiento de los datagramas, es decir, de los paquetes IP.

La comunicación con el uso del protocolo ICMP consiste en transmitir las adecuadas informaciones sobre los errores descubiertos durante la conexión entre dos dispositivos. Las informaciones individuales tienen la forma de los paquetes correctamente formateados (en inglés llamados datagrams), que después se encapsula en una trama de protocolo IP. Contrariamente a la creencia popular el protocolo ICMP no utiliza los protocolos TCP o UDP, y por eso no usa ningunos puertos de red.

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

El ICMP únicamente informa de 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:

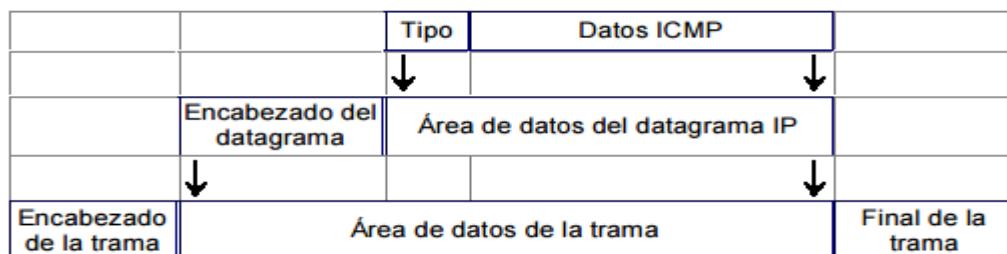


Figura 12 Esquema de datagrama Protocolo ICMP

El Servicio ICMP, se establece para el intercambio de información sobre las dificultades de ruteo con paquetes IP o intercambios simples como son las peticiones de eco y respuesta de eco.

tipo (0 u 8)	código (0)	suma de verificación (checksum)
Identificador		número de secuencia
datos opcionales		

Figura 13 Encabezado ICMP

ICMP se encapsula dentro del datagrama IP y se considera en la misma capa que IP. Soporta tráfico de difusión, es decir, se puede transmitir ICMP a varios hosts. Ping o traceroute son aplicaciones que usan ICMP.

Para la notificación de errores e incidencias ICMP tiene una serie de mensajes que se generan para cada situación.

Valor	Significado
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen
5	Redirigir
8	Eco
11	Tiempo superado
12	Problema de parámetros
13	Marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información

Figura 14 Tipos de mensaje ICMP.

#### 2.14.1 Solicitud de eco y respuesta de eco

Esto es el más utilizado para probar la conectividad IP comúnmente conocida como PING de ICMP. ICMP de solicitud de eco tendrá un campo de tipo de 8 y un campo de código de 0. Respuestas de eco con un campo de tipo de 0 y un campo de código de 0.

PING. Este comando, que permite evaluar la red, envía un datagrama a un destino y solicita que regrese.

La orden Ping envía mensajes de solicitud de Eco e informa acerca de las respuestas.

Utiliza "Echo Request" y "Echo Reply" de ICMP.

Parámetros:

- n Cantidad de peticiones Echo
- i (1-255) Especifica tiempo de vida de la solicitud.

Se utiliza para diagnosticar errores en una Red.

## 2.15 SNMP y UDP

El SNMP usa el protocolo de datagramas de usuario como protocolo de transporte para intercambiar datos entre los sistemas administradores y los agentes. UDP fue escogido sobre el protocolo TCP debido a que puede enviar mensajes sin establecer una conexión con el receptor. Esta característica de UDP lo hace poco confiable ya que no se sabe si hay pérdida de datagramas durante el envío de los mismos. Depende de la aplicación SNMP determinar si los datagramas están perdidos y volver a transmitirlos si así se requiere. Esto es normalmente acompañado con un tiempo máximo. El NMS envía una petición UDP a un agente y espera por la respuesta. La cantidad de tiempo que el NMS espera, depende de cómo esté configurado. Si se alcanza el tiempo máximo de espera y el NMS no obtiene información del agente, se asume que el paquete se perdió y retransmite nuevamente la petición.

## 2.16 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

SNMP son las siglas de “Simple Network Management Protocol”, es un protocolo que permite realizar la gestión remota de dispositivos. El predecesor de SNMP, SGMP (Simple Gateway Management Protocol) fue diseñado para administrar routers, pero SNMP puede administrar prácticamente cualquier dispositivo, utilizando para ello comandos para obtener información y para modificar la información.

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. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y etcétera. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SNMP es un componente de la suite de protocolo de Internet como se define por el IETF. La respuesta a todas las necesidades antes expuestas, es el protocolo llamado Simple Network Management Protocol (SNMP). Diseñado en los años 80, su principal objetivo fue el integrar la gestión de diferentes tipos de redes mediante un diseño sencillo y que produjera poca sobrecarga en la red.

SNMP opera en el nivel de aplicación, utilizando el protocolo de transporte TCP/IP, por lo que ignora los aspectos específicos del hardware sobre el que funciona. La gestión se lleva a cabo al nivel de IP, por lo que se pueden controlar dispositivos que estén conectados en cualquier red accesible desde la Internet, y no únicamente aquellos localizados en la propia red local. Evidentemente, si alguno de los dispositivos de encaminamiento con el dispositivo remoto a controlar no funciona correctamente, no será posible su monitorización ni reconfiguración.

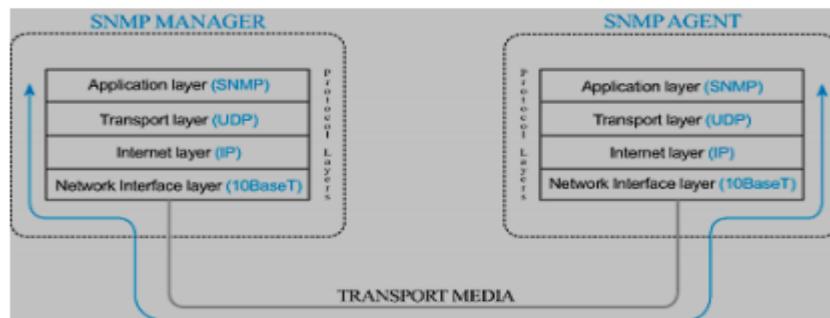


Figura 15 Arquitectura SNMP

El modelo de gestión de redes que es usado para gestión de redes TCP/IP incluye los siguientes elementos: Estación de Gestión (Manager). Agente Administrador (Agente). Base de Información de Administrada (MIB). La estación de gestión (Manager) es típicamente un dispositivo independiente, que sirve como la interfaz entre la persona administradora de la red y el sistema de gestión. Como mínimo la estación administradora (manager) tendrá: Un conjunto de aplicaciones de administración para análisis de datos, aplicaciones para recuperación de alguna falla, y demás. Una interfaz por la cual el administrador de la red pueda supervisar y controlar la red. La capacidad de traducir los requerimientos de administración de la red dentro de la supervisión actual y control de elementos remotos en la red. Una base de información extraída de la MIBs de todas las entidades en la red.

El otro elemento activo en el sistema de administración de redes es el agente administrador (agente), son elementos como: hosts, puentes, ruteadores y hubs, pueden ser equipados con agentes SNMP tal que puedan ser administrados desde una estación Administradora (manager). El agente administrador (agente) responde a peticiones, para información y acciones desde la estación de gestión (manager). Los recursos en la red pueden ser administradas representándolos como objetos. Cada objeto es, esencialmente, un dato variable pero representa un aspecto del agente administrador. La colección de objetos se refiere a una base de información administrada (MIB Management Information Base). La MIB funciona como una colección de puntos de accesos en el agente para la estación de gestión (manager), el cual es un estándar. Una estación de gestión (manager) realiza la función de supervisión tomando el valor de los objetos MIB. Una estación de gestión (manager) puede hacer una acción al recurrir en un agente o puede cambiar la configuración en un agente modificando el valor de variables específicas.

La estación de gestión (manager) y el agente administrador (agente) están ligados por un protocolo de gestión de redes. El protocolo usado para la administración de redes TCP/IP es el Simple Network Management Protocol (SNMP), la cual incluye las siguientes capacidades dominantes: get: Permite a la estación de gestión (manager) recuperar el valor de los objetos en el agente. Set: Permite a la estación de gestión (manager) alterar el valor de los objetos en el agente. Trap: Permite a un agente notificar a la estación de gestión (manager) de eventos significativos.

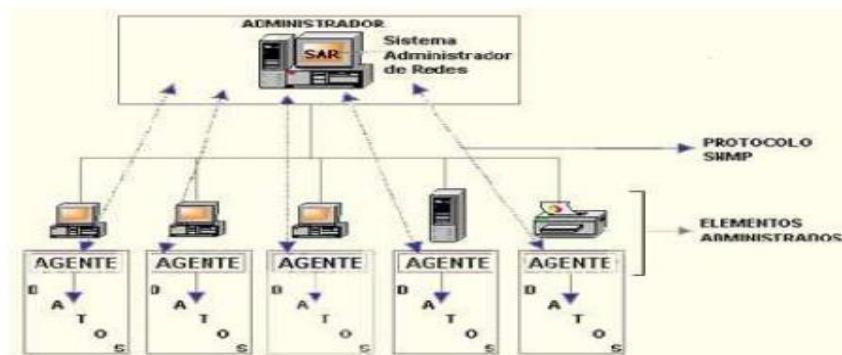


Figura 16 Modelo Protocolo SNMP

SNMP fue diseñado para ser un protocolo de la capa de aplicación que es parte de la suite del protocolo TCP/IP. Se piensa operar sobre mensajes UDP.

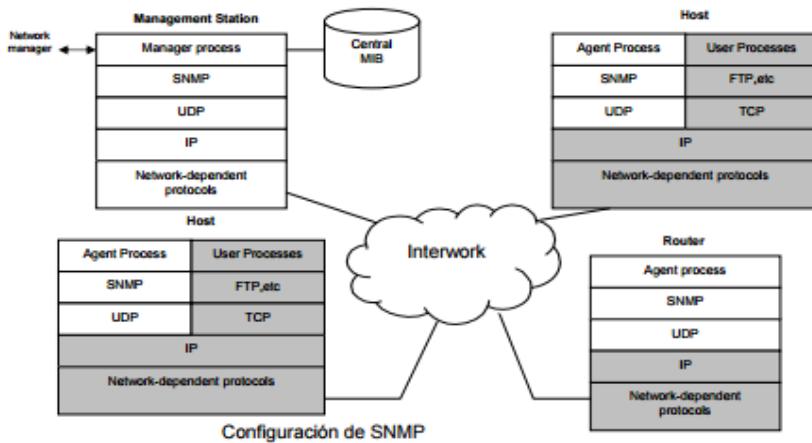


Figura 17 Estructura Protocolo SNMP

**SNMP Management Information (MIB)** Para SNMP, la MIB es, en esencia, una estructura de base de datos en forma de árbol. Cada sistema (computadoras, ruteadores, puentes, etc.) en una red o intrared mantiene una MIB que refleja el status de los recursos administrados en ese sistema. Un manager puede supervisar los recursos en ese sistema leyendo los valores de los objetos en la MIB y puede controlar el recurso en ese sistema modificando esos valores. Para que la MIB sirva a las necesidades de un sistema de administración de red, este debería conocer ciertos objetivos: El objeto u objetos utilizados para representar un recurso particular debería ser el mismo en cada sistema: Este punto se refiere a la definición de objetos y la estructura de estos objetos en la MIB. Un esquema común para la representación debería ser utilizado para soporte de interoperabilidad: Se refiere a la definición de una estructura de información administrada (SMI).

Por la forma en la que el protocolo está implementado, se distinguen dos entidades: estaciones administradoras y elementos de la red [RFC1157]. Una estación administradora es un servidor que, por medio de un programa, realiza la gestión de los dispositivos por medio de comandos y consultas SNMP. El programa que realiza la gestión es denominado NMS (Network Management System). Por otro lado en los elementos a administrar residen los

agentes, que son los que responden los mensajes y realizan las acciones indicadas por el NMS.

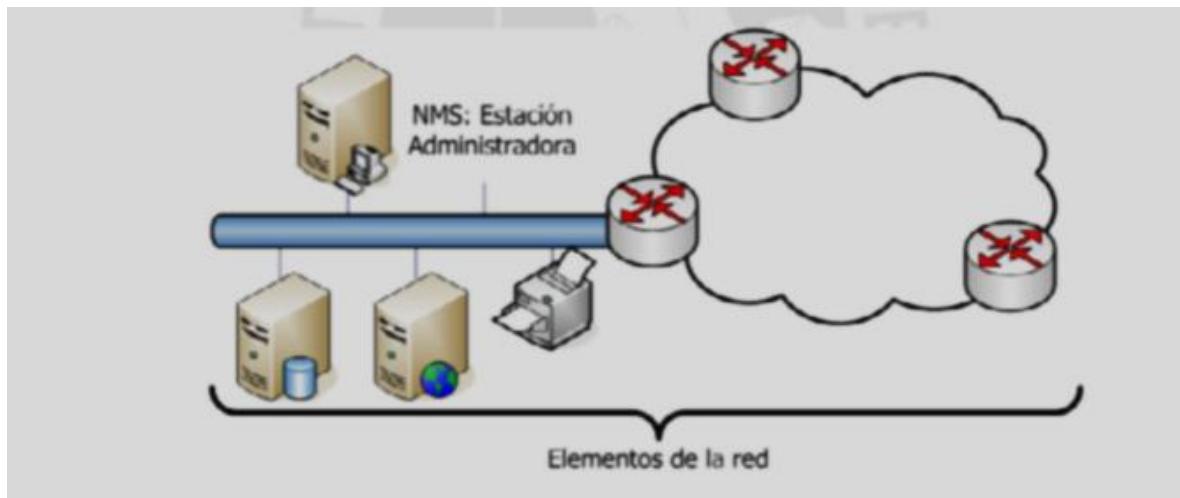


Figura 18 NMS Y Elementos de la Red

Entre el NMS y los agentes se intercambian tres tipos básicos de mensajes, mostrados en la Figura 19. La dupla query/response corresponden al pooling o sondeo que realiza el NMS de manera periódica y a la respectiva respuesta. El trap corresponde a un mensaje no solicitado por el NMS que puede mandar el agente en caso ocurra un evento determinado, por ejemplo, la desconexión de una interfaz en un router. Una cosa a considerar es que si bien el pooling es usualmente periódico, al igual que el trap es de naturaleza asíncrona, ya que no tiene un tiempo determinado de inicio y el agente debe estar preparado para responder queries o generar traps en cualquier momento.

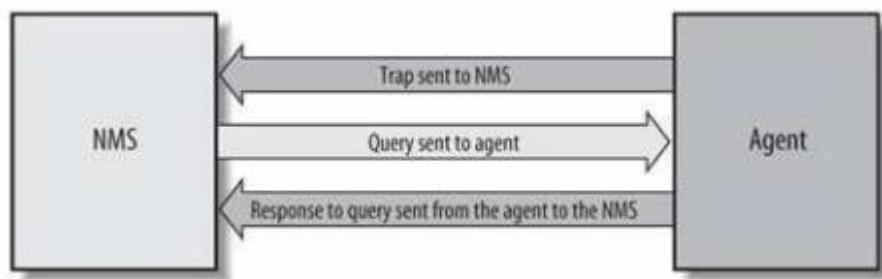


Figura 19 Mensajes entre el NMS y el Agente

## Datagrama SNMP

El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. Los datagramas correspondientes a este protocolo viajan sobre UDP utilizando normalmente el puerto 161 para mensajes y el 162 para traps. El utilizar UDP implica que no se establece una sesión entre el NMS y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido, en el caso del sondeo el NMS puede esperar un tipo por la respuesta y, en caso esta no se reciba, se puede reenviar el paquete. El problema se da en el caso de los traps, ya que el agente no espera ninguna respuesta del NMS, entonces el trap puede perderse y ninguno de los equipos es notificado.

### 2.16.1 ASN

El Abstract Syntax Notation One (ANS.1) es un estándar de la ISO y la ITU-T para describir mensajes a ser intercambiados entre aplicaciones. Provee un conjunto de reglas para describir la estructura de los objetos. SNMP utiliza un subconjunto de las reglas definidas por este estándar, para la definición de cómo se van a representar y transmitir los datos.

### 2.16.2 Structure of Management Information (SMI)

La Structure of Management Information (SMI) define el nombre y tipo de datos de los objetos gestionables. Cada objeto a gestionar tiene tres atributos:

- El nombre u OID (Object Identifier) el cual define de manera única cada objeto.
- Tipo y sintaxis: Para esto se utiliza la ASN.1, de manera que la sintaxis sea universal y no haya problema al comunicar sistemas diferentes.
- Codificación: Se define como se codifican y decodifican los objetos en una cadena de octetos, de manera que no haya problema al transmitirlos.

## 2.16.2 Management Information Base (MIB)

La Management Information Base (MIB) es la colección de objetos administrables definidos utilizando la SMI. Para estos objetos se sigue una estructura jerárquica en forma de árbol.

En la Figura 20, se muestra la estructura de la MIB-2, su posición dentro del árbol y los objetos administrables dentro de esta.

La jerarquía se inicia en la raíz, desde la cual se dividen tres ramas, una para los objetos administrados por la ITU-T, antes CCITT, la segunda para los administrados por la ISO y la tercera para los de administración conjunta.

Dentro de la rama de la ISO, la tercera subdivisión corresponde a organizaciones, como se mencionó en el Capítulo 2, la Internet nace por un proyecto del departamento de defensa de los Estados Unidos, es por ello que su OID se encuentra dentro de DOD (Department of Defense). Debajo del subárbol Internet, existen ramas relacionadas a administración de redes y SNMP, estos subárboles son administrados por la IANA.

Son de especial interés el mgmt.mib-2 y el private.enterprises, en el primero se define la MIB estándar de Internet, y el segundo es proporcionado a empresas para que puedan registrar OIDs particulares para ser utilizados en soluciones propias de hardware o software. La estructura puede ser vista en la figura

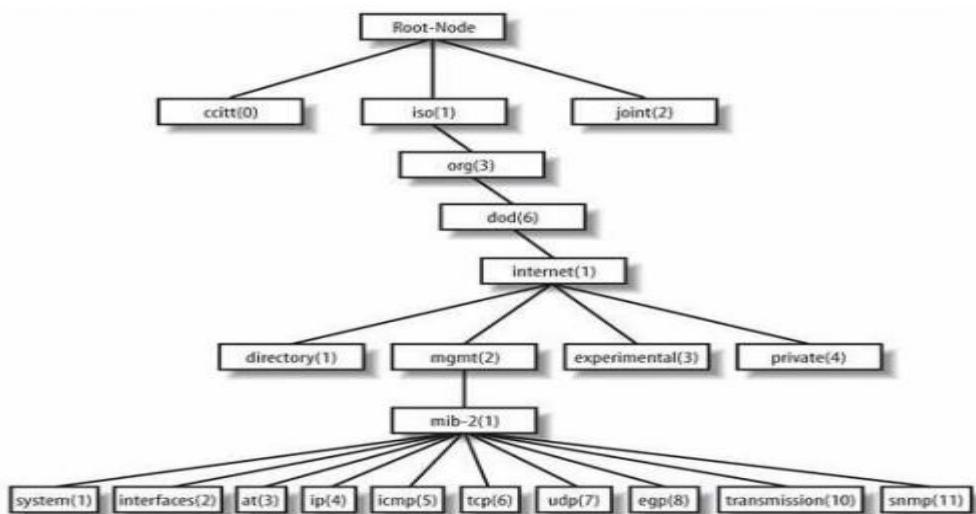


Figura 20 Estructura Jerárquica de la MIB-II

SNMP define un estándar separado para los datos gestionados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas. Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama Management Information Base (MIB) y se puede encontrar información sobre ella en varios RFC's.

La versión actual de TCP/IP MIB es la 2 (MIB-II) y se encuentra definida en el RFC-1213. En ella se divide la información que un dispositivo debe mantener en ocho categorías (Cualquier variable ha de estar en una de estas categorías).

Categoría	Información
system	Información del host del sistema de encaminamiento
interfaces	Información de los interfaces de red
addr-translation	Información de traducción de direcciones
ip	Información sobre el protocolo IP
icmp	Información sobre el protocolo ICMP
tcp	Información sobre el protocolo TCP
udp	Información sobre el protocolo UDP
egp	Información sobre el protocolo (Exterior Gateway)

Figura 21 Categorías TCP/IP

### 2.16.3 OID

Los OIDs (Object IDentifier) es la dirección de una variable o nodo dentro de la estructura de alguna MIB, está constituida por números enteros positivos separados por puntos. Por ejemplo el nodo system es: .1.3.6.1.2.1.1 Se debe notar el punto inicial que corresponde a la raíz. Además, el valor de los objetos se referencia por un sufijo, según el tipo de dato que retorna, así un valor único, como un entero o una cadena de caracteres, es referenciado por un 0 y un objeto con múltiples entradas, como una tabla, se utilizan sufijos distintos de cero para cada entrada.

El protocolo de administración de red es un protocolo de aplicación por el que las variables del MIB de un agente pueden ser inspeccionadas o alteradas. Las entidades de protocolo se comunican entre sí mediante mensajes, cada uno formado únicamente por un datagrama UDP. Cada mensaje está formado por un identificador de versión, un nombre de comunidad

SNMP y una PDU (Protocol Data Unit - Unidad de datos de protocolo). Estos datagramas no necesitan ser mayores que 484 bytes, pero es recomendable que las implementaciones de este protocolo soporten longitudes mayores. Todas las implementaciones del SNMP soportan 5 tipos de PDU:

- GetRequest-PDU
- GetNextRequest-PDU
- GetResponse-PDU
- SetRequest-PDU
- Trap-PDU

#### **2.16.4 Elementos de procedimiento**

Se describirá a continuación las acciones que realiza una entidad de protocolo en una implementación SNMP. Definiremos dirección de transporte como una dirección IP seguida de un número de puerto UDP (Si se está usando el servicio de transporte UDP).

Cuando una entidad de protocolo envía un mensaje, realiza las siguientes acciones:

1. Construye la PDU apropiada como un objeto definido con el lenguaje ASN.1.
2. Pasa esta PDU, junto con un nombre de comunidad y las direcciones de transporte de fuente y destino, a un servicio de autentificación. Este servicio generará en respuesta otro objeto en ASN.1.
3. La entidad construye ahora un mensaje en ASN.1 usando el objeto que le ha devuelto el servicio de autentificación y el nombre de comunidad.
4. Este nuevo objeto se envía a la entidad destino usando un servicio de transporte.

Cuando una entidad de protocolo recibe un mensaje, realiza las siguientes acciones:

1. Hace un pequeño análisis para ver si el datagrama recibido se corresponde con un mensaje en ASN.1. Si no lo reconoce, el datagrama es descartado y la entidad no realiza más acciones.
2. Observa el número de versión. Si no concuerda descarta el datagrama y no realiza más acciones.

3. Pasa los datos de usuario, el nombre de comunidad y las direcciones de transporte de fuente y destino al servicio de autentificación. Si es correcto, este devuelve un objeto ASN.1. Si no lo es, envía una indicación de fallo. Entonces la entidad de protocolo puede generar una trampa (trap), descarta el datagrama y no realiza más acciones.
4. La entidad intenta reconocer la PDU. Si no la reconoce, descarta el datagrama. Si la reconoce, según el nombre de comunidad adopta un perfil y procesa la PDU. Si la PDU exige respuesta, la entidad iniciará la respuesta ahora.

#### **2.16.5 Estructura de una PDU**

Los datos que incluye una PDU genérica son los siguientes:

- RequestID: Entero que indica el orden de emisión de los datagramas. Este parámetro sirve también para identificar datagramas duplicados en los servicios de datagramas poco fiables.
- ErrorStatus: Entero que indica si ha existido un error. Puede tomar los siguientes valores, que se explicarán posteriormente:

-noError (0)  
-tooBig (1)  
-noSuchName (2)  
-badValue (3)  
-readOnly (4)  
-genErr (5)

ErrorIndex: Entero que en caso de error indica qué variable de una lista ha generado ese error.

VarBindList: Lista de nombres de variables con su valor asociado. Algunas PDU quedan definidas sólo con los nombres, pero aun así deben llevar valores asociados. Se recomienda para estos casos la definición de un valor NULL.

#### **2.16.6 GetRequest-PDU y GetNextRequest-PDU**

Son PDU's que solicitan a la entidad destino los valores de ciertas variables. En el caso de GetRequest-PDU estas variables son las que se encuentran en la lista VarBindList; en el de

GetNextRequest-PDU son aquellas cuyos nombres son sucesores lexicográficos de los nombres de las variables de la lista. Como se puede observar, GetNextRequest-PDU es útil para confeccionar tablas de información sobre un MIB.

Siempre tienen cero los campos ErrorStatus y ErrorIndex. Son generadas por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP.

Estas PDU's siempre esperan como respuesta una GetResponse-PDU

### **2.16.7 SetRequest-PDU**

Ordena a la entidad destino poner a cada objeto reflejado en la lista VarBindList el valor que tiene asignado en dicha lista. Es idéntica a GetRequest-PDU, salvo por el identificador de PDU. Es generada por una entidad de protocolo sólo cuando lo requiere su entidad de aplicación SNMP. Espera siempre como respuesta una GetResponse-PDU.

### **2.16.8 GetResponse-PDU**

Es una PDU generada por la entidad de protocolo sólo como respuesta a GetRequest-PDU, GetNextRequest-PDU o SetRequest-PDU. Contiene o bien la información requerida por la entidad destino o bien una indicación de error.

Cuando una entidad de protocolo recibe una GetRequest-PDU, una SetRequest-PDU o una GetNextRequest-PDU, sigue las siguientes reglas:

1. Si algún nombre de la lista (o el sucesor lexicográfico de un nombre en el caso de GetNextRequest-PDU) no coincide con el nombre de algún objeto en la vista del MIB al que se pueda realizar el tipo de operación requerido ("set" o "get"), la entidad envía al remitente del mensaje una GetResponsePDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 2 (noSuchName), y con el campo ErrorIndex indicando el nombre de objeto en la lista recibida que ha originado el error.
2. De la misma manera actúa si algún objeto de la lista recibida es un tipo agregado (como se define en el SMI), si la PDU recibida era una GetRequest-PDU.
3. Si se ha recibido una SetRequest-PDU y el valor de alguna variable de la lista no es del tipo correcto o está fuera de rango, la entidad envía al remitente una GetResponse-PDU idéntica a

la recibida, salvo en que el campo ErrorStatus tendrá el valor 3 (badValue) y el campo ErrorIndex señalará el objeto de la lista que ha generado el error.

4. Si el tamaño de la PDU recibida excede una determinada limitación, la entidad enviará al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 1 (tooBig).

5. Si el valor de algún objeto de la lista no puede ser obtenido (o alterado, según sea el caso) por una razón no contemplada en las reglas anteriores, la entidad envía al remitente una GetResponse-PDU idéntica a la recibida, pero con el campo ErrorStatus puesto a 5 (genErr), y el campo ErrorIndex indicando el objeto de la lista que ha originado el error.

Si no se llega a aplicar alguna de estas reglas, la entidad enviará al remitente una GetResponse-PDU de las siguientes características:

- Si es una respuesta a una GetResponse-PDU, tendrá la lista varBindList recibida, pero asignando a cada nombre de objeto el valor correspondiente.
- Si es una respuesta a una GetNextResponse-PDU, tendrá una lista varBindList con todos los sucesores lexicográficos de los objetos de la lista recibida, que estén en la vista del MIB relevante y que sean susceptibles de ser objeto de la operación "get". Junto con cada nombre, aparecerá su correspondiente valor.
- Si es una respuesta a una SetResponse-PDU, será idéntica a esta, pero antes la entidad asignará a cada variable mencionada en la lista varBindList su correspondiente valor. Esta asignación se considera simultánea para todas las variables de la lista.

En cualquiera de estos casos el valor del campo ErrorStatus es 0 (noError), igual que el de ErrorIndex. El valor del campo requestID es el mismo que el de la PDU recibida.

## 2.16.9 Trap-PDU

Es una PDU que indica una excepción o trampa. Es generada por una entidad de protocolo sólo a petición de una entidad de aplicación SNMP.

Cuando una entidad de protocolo recibe una Trap-PDU [RFC 1215], presenta sus contenidos a su entidad de aplicación SNMP.

Los datos que incluye una Trap-PDU son los siguientes:

- enterprise: tipo de objeto que ha generado la trampa.
- agent-addr: dirección del objeto que ha generado la trampa.
- generic-trap: entero que indica el tipo de trampa. Puede tomar los siguientes valores:

coldStart (0)  
 warmStart (1)  
 linkDown (2)  
 linkUp (3)  
 authenticationFailure (4)  
 egpNeighborLoss (5)  
 enterpriseSpecific (6)

- specific-trap: entero con un código específico.
- time-stamp: tiempo desde la última inicialización de la entidad de red y la generación de la trampa.
- variable-bindings: lista tipo varBindList con información de posible interés.

Dependiendo del valor que tenga el campo generic-trap, se iniciarán unas u otras acciones:

- Trampa de arranque frío (coldStart): La entidad de protocolo remitente se está reinicializando de forma que la configuración del agente o la implementación de la entidad de protocolo puede ser alterada.
- Trampa de arranque caliente (warmStart): La entidad de protocolo remitente se está reinicializando de forma que ni la configuración del agente ni la implementación de la entidad de protocolo se altera.
- Trampa de conexión perdida (linkDown): La entidad de protocolo remitente reconoce un fallo en uno de los enlaces de comunicación representados en la configuración del agente. Esta Trap-PDU contiene como primer elemento de la lista variable-bindings el nombre y valor de la interfaz afectada.
- Trampa de conexión establecida (linkUp): La entidad de protocolo remitente reconoce que uno de los enlaces de comunicación de la configuración del agente se ha establecido. El primer elemento de la lista variable-bindings es el nombre y el valor de la interfaz afectada.
- Trampa de fallo de autentificación (authenticationFailure): La entidad de protocolo remitente es la destinataria de un mensaje de protocolo que no ha sido autenticado.

- Trampa de pérdida de vecino EGP (egpNeighborLoss): Un vecino EGP con el que la entidad de protocolo remitente estaba emparejado ha sido seleccionado y ya no tiene dicha relación. El primer elemento de la lista variable-bindings es el nombre y el valor de la dirección del vecino afectado.
- Trampa específica (enterpriseSpecific): La entidad remitente reconoce que ha ocurrido algún evento específico. El campo specific-trap identifica qué trampa en particular se ha generado.

## 2.17 SOLARWINDS ORION NETWORK PERFORMANCE MONITOR

Orion NMPM es una detallada aplicación basada en servidor para la administración de fallas, ancho de banda y rendimiento que permite a los usuarios ver estadísticas en tiempo real y disponibilidad de la red desde cualquier Web browser.

Para comprender mejor el propósito de un producto, muchas veces lo mejor es identificar sus funciones principales. Orion está diseñado para 1) **Monitorear** varios tipos de elementos presentes en las redes o disponibles en varios tipos de nodos de red, 2) **Alertar** cuando aspectos específicos de los elementos monitoreados atraviesen umbrales definidos, 3) **Reportar** basados en los datos actuales e históricos colectados acerca de los elementos monitoreados y los circuitos de telecomunicaciones asociados a ellos, y 4) **Escuchar** mensajes de syslog y SNMP traps enviados de red a Orion como servidor de Logs.

Módulos adicionales extienden las capacidades para también incluir el monitoreo de aplicaciones, VoIP, datos de Netflow, SLAs y direcciones IP.

### **Monitorea.**

Orion monitorea elementos de red (nodos, interfaces, y volúmenes) para obtener datos de rendimiento y fallas a través del protocolo Internet Control Messaging Protocol (ICMP), opcionalmente Simple Network Management Protocol (SNMP) Y Wondows Management Instrumentation (WMI). Una vez colectados, los datos son almacenados en una base de datos Microsoft SQL. Los datos son entonces presentados como información apropiada y utilizable a cualquier número de usuarios propiamente identificados y autenticados, por medio de una consola Web.

## **Alerta**

Orion permite a los administradores definir umbrales personalizados basados en los datos monitoreados que una vez alcanzados, colocan al o los elementos monitoreados (nodos, interfaces, volúmenes, o Universal Device Pollers) en un estado de alerta para notificar a diferentes audiencias de esta condición.

## **Reporta**

Dado que Orion almacena todos los datos colectados en una base de datos Microsoft SQL, el tomar ventaja del motor de bases de datos de SQL para generar reportes en tiempo real e históricos, es otra funcionalidad clave de Orion. Adicionalmente a un número de reportes ejemplo que vienen pre-definidos, pueden definirse reportes personalizados e incluirlos en el sitio Web de Orion para ser accedidos por usuarios o grupos de usuarios. Lo único que limita los reportes es la información que esta colectada y retenida en la base de datos. Si está en la base de datos, un reporte puede ser creado para desplegarlo.

## **Escucha**

Orion comprueba y “pregunta” a los nodos monitoreados usando ICMP y SNMP, pero también incluye servidores de Syslog y SNMP Traps totalmente funcionales. Esto permite a los administradores de redes y servidores definir uno o más polling engines (motores de sondeo) como servidores de logging en la configuración de los dispositivos de red. Todos los Traps y mensajes de Syslog son colectados y almacenados en la base de datos de Orion, poniendo a disposibilidad la opción de incluir estos datos en el Website de Orion, definir alertas (y acciones), elaborar reportes sobre los datos colectados. Históricamente este tipo de información creaba tablas que luego necesitaban ser leídas y analizadas manualmente o utilizando otras soluciones de software. Esta función está incluida “out-of-thebox”, permitiendo que esta herramienta de monitoreo poderosa se convierta en una eficiente herramienta de resolución y administración de fallas, al tomar ventaja de las alertas e información de logging generados en los nodos siendo monitoreados.

## 2.17.1 Arquitectura

Orion está construido en niveles funcionales lógicos.

El **Nivel Fundacional** (o Nivel de datos) es una base de datos Microsoft SQL. Todos los datos colectados de / acerca de los elementos monitoreados son mantenidos en la base de datos SQL.

El **Nivel de Aplicación** es el motor o motores de sondeo (polling engines) de Orion. Un motor de sondeo está constituido de varios servicios responsables de la colección y manipulación de datos de sondeo y estadísticas de los elementos monitoreados así como de almacenar los datos en la base de datos SQL designada.

El **Nivel de Presentación** consiste de uno o más web servers Microsoft Internet Information Server que hospedan el website de Orion. Cabe notar que estas capas funcionales son lógicas y pueden residir físicamente en uno o más servidores físicos o virtuales basándose en los requerimientos de recursos de cada servidor.

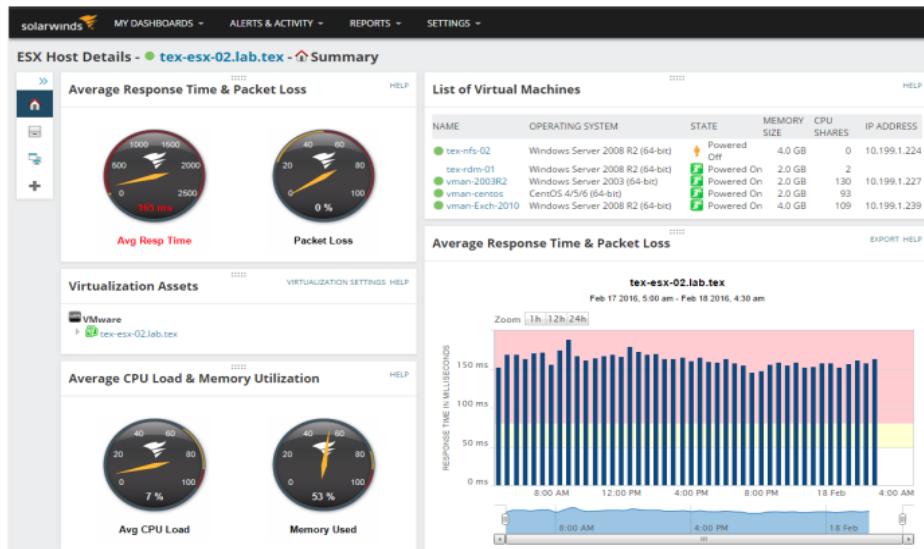


Figura 22 Interfaz Gráfica Solarwinds

## **2.18 Short Message Service (SMS)**

Servicio de mensajes cortos. Es un sistema para enviar y recibir mensajes de texto para teléfonos móviles. El texto puede estar compuesto de palabras o números o una combinación alfanumérica. SMS fue creado como una parte del estándar GSM fase 1. El primer mensaje corto, se cree que fue enviado en Diciembre de 1992 desde un ordenador personal (PC) a un teléfono móvil a través de la red GSM Vodafone del Reino Unido. Cada mensaje puede tener hasta 160 caracteres cuando se usa el alfabeto latino, y 70 caracteres si se usa otro alfabeto como el árabe o el chino.

En un principio, los mensajes (SMS) se definieron en el estándar GSM como un medio para que los operadores de red enviaran información sobre el servicio a los abonados, sin que estos pudieran responder ni enviar mensajes a otros clientes. Sin embargo la empresa Nokia desarrolló un sistema para permitir la comunicación bidireccional por SMS. Los mensajes de texto son procesados por un SMSC (Short Message Service Center) o centro de servicio de mensajes cortos, que se encarga de almacenarlos hasta que son enviados y de conectar con el resto de elementos de la red.

## **2.19 GSM.**

El servicio SMS consiste en el envío de mensajes en modo almacenamiento y reenvío a través de un centro de servicio de mensajes cortos. Se basa en los procedimientos SMS proporcionados por el subnivel de gestión de comunicación (CM).

El servicio SMS permite el envío de mensajes alfanuméricos de hasta 140 bytes (160 caracteres de 7 bits) desde una estación móvil hacia una o más estaciones móviles destinatarias. La limitación de longitud no es específica de GSM, sino que se debe a la longitud máxima de mensajes que puede transportar la red.

A diferencia de los demás servicios GSM, el servicio SMS no implica el establecimiento de un trayecto de comunicación directo entre las MS origen y destino, sino que sigue el enfoque tradicional de las redes de comutación de mensajes, basado en el empleo de nodos de almacenamiento y reenvío. En GSM, estos nodos reciben el nombre de centro de servicio de mensajes cortos (SMSC). Las especificaciones GSM consideran a los SMSC como elementos ajenos a la red, y la comunicación entre ambos se lleva a cabo a través de las pasarelas SMS (SMSG, SMS Gateway). Desde la perspectiva de GSM, el envío de un mensaje corto se limita

al encaminamiento desde la MS hasta el SMSC adecuado, y finaliza cuando este se ha entregado a la SMSG

GSM.- Sus siglas en inglés (Global System for Mobile communications) es decir sistema global para las comunicaciones móviles, es un estándar de comunicación para la telefonía móvil, que utiliza la combinación de satélites y antenas terrestres.

Una red GSM se organiza como un conjunto de células radioeléctricas continuas que proporcionan cobertura completa al área de servicio. Cada una de estas células pertenece a una estación base (BTS), que opera en un conjunto de canales de radio diferentes a los usados en las células adyacentes y que se encuentran distribuidas según un plan celular de frecuencias.

La Figura 22 indica la arquitectura básica de un sistema GSM, en la cual se puede distinguir los principales bloques que lo construyen. Un grupo de estaciones base se encuentra conectado a un controlador de estaciones base (BSC), encargado, de situaciones como traspaso del móvil de una célula a otra. El BSC se ocupa de la gestión de toda la red de radio. Una o varias BSC se conectan a una central de conmutación de móviles (MSC), verdadero núcleo de la red, responsable del inicio, enrutamiento, control y finalización de las llamadas.

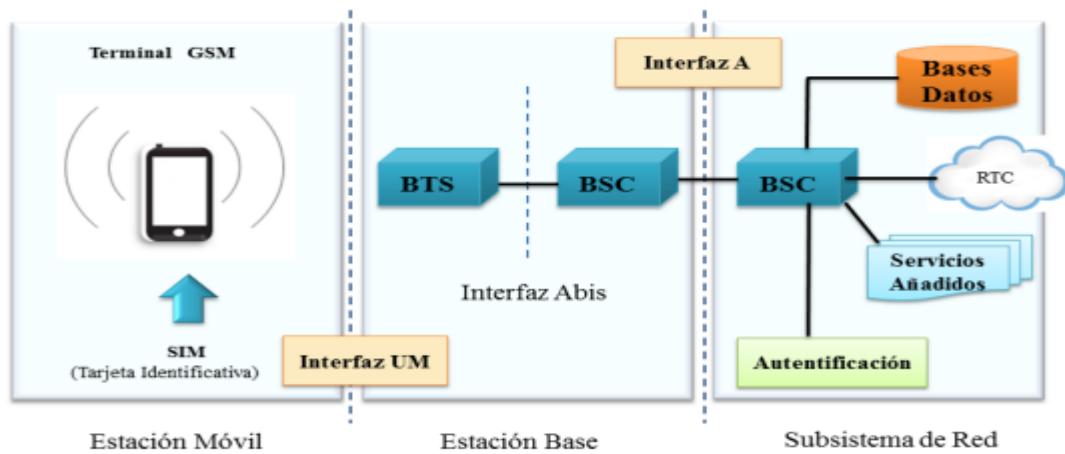


Figura 23 Arquitectura Básica GSM

El estándar de telefonía móvil GSM facilita la existencia de una serie de servicios, sin necesidad de un módem externo a través de una tarjeta para conexión con el puerto serie del ordenador. GSM posibilita la creación de redes privadas virtuales, permite la identificación de un abonado bajo dos números distintos, ofrece un servicio de mensajes alfanuméricos cortos (SMS) de hasta 160 caracteres y toda una completa gama de servicios suplementarios.

# **CAPÍTULO 3.**

## **DISEÑO DE UN SISTEMA DE ALERTA DE CAÍDA DE UNA RED**

### 3.1 Diagrama a Bloques

En el desarrollo del proyecto se diseña del diagrama a bloques para la construcción del sistema, dicho diagrama se presenta en la siguiente figura.

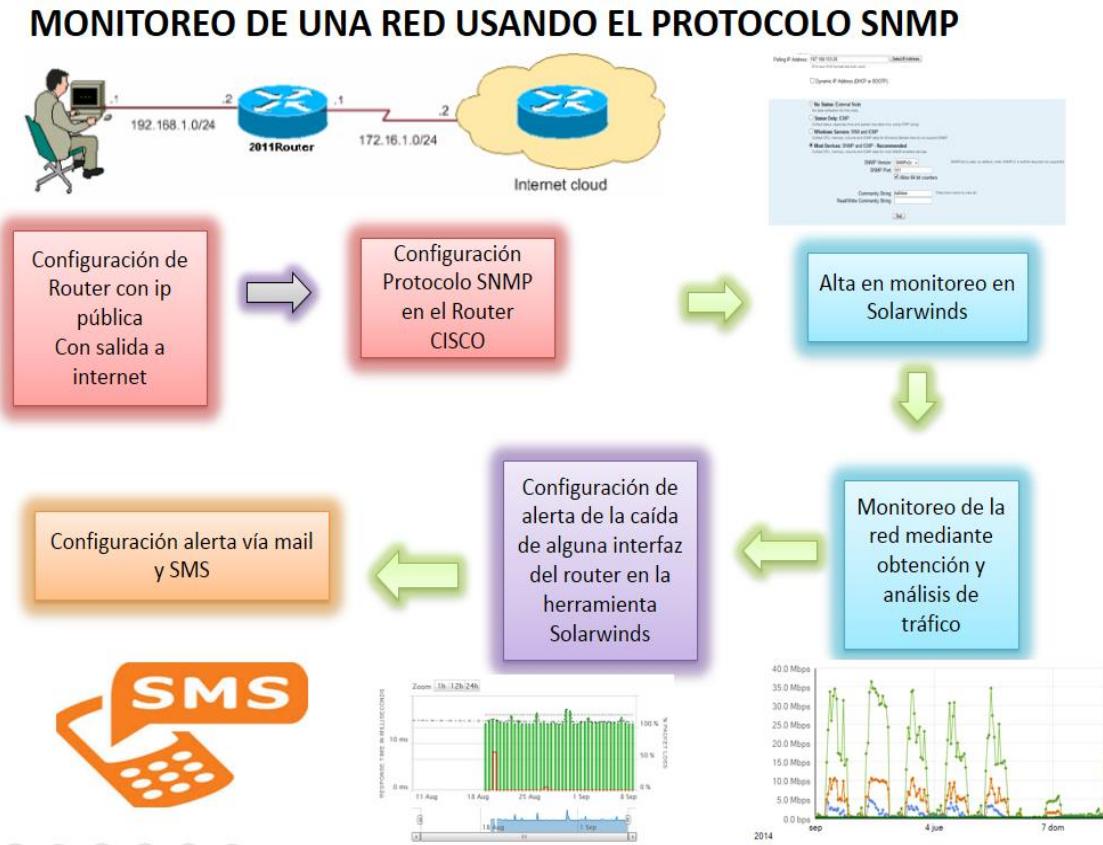


Figura 24 Diagrama a Bloques

El diagrama a bloques consta de cinco etapas las cuales se irán desarrollando en este capítulo. Se anexa una breve explicación

**BLOQUE I CONFIGURACIÓN DE ROUTER** Consiste en configurar el router para nombrarlo y dar salida a internet mediante la IP Pública que nos brinda el ISP.

## BLOQUE II CONFIGURACIÓN PROTOCOLO SNMP

En este bloque se realiza la configuración del SNMP dentro del router, previamente ya podemos acceder a este vía telnet y se agrega la línea para configurar este protocolo.

## BLOQUE III ALTA EN MONITOREO EN SOLARWINDS

Se da de alta el monitoreo del router a través la aplicación Solarwinds mediante la IP pública que se tiene configurada en el equipo.

## BLOQUE IV MONITOREO DE LA RED MEDIANTE LA OBTENCIÓN Y ANÁLISIS DE TRÁFICO

En este bloque se obtienen las gráficas de monitoreo con esto podemos analizar las y tiempos de respuesta y disponibilidad que ha tenido la red

## BLOQUE V CONFIGURACIÓN DE ALERTA DE LA CAÍDA DEL NODO O ALGUNA INTERFAZ

Se da de alta la alerta desde el servidor Solarwinds se indica que acción debe realizar al detectar que no está disponible el nodo monitoreado.

## BLOQUE VI CONFIGURACIÓN ALERTA VÍA MAIL Y SMS

Se realiza configuración de las alertas las cuáles llegarán al usuario vía Correo y SMS a través de los servidores.

### 3.2 Diagrama de Flujo

En el diagrama de flujo se describe la forma en la cual iremos desarrollando el proyecto en cada uno de los bloques.

## MONITOREO DE UNA RED USANDO EL PROTOCOLO SNMP

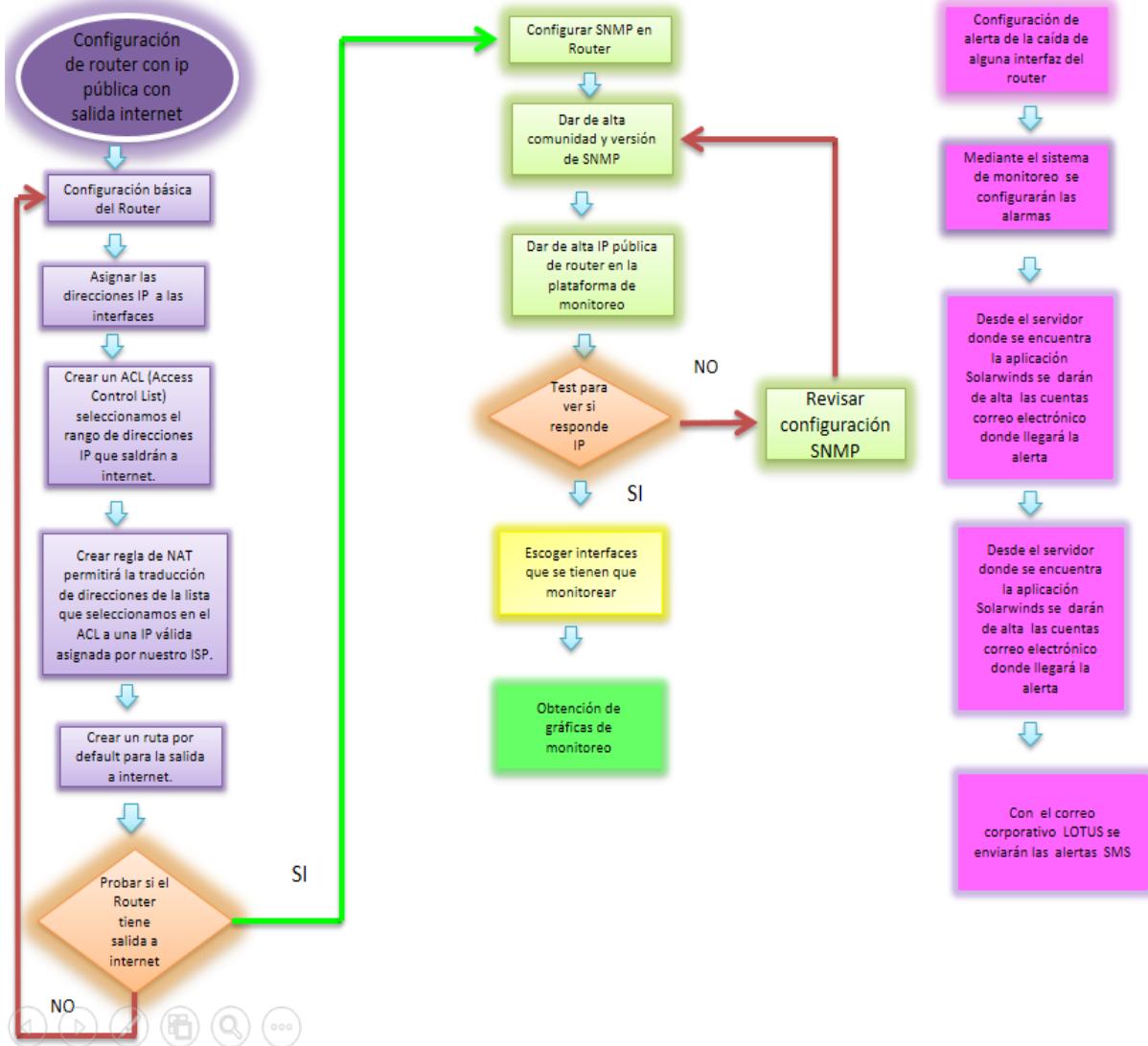


Figura 25 Diagrama de Flujo

### 3.3 BLOQUE I CONFIGURACIÓN DE ROUTER

Se tiene un proveedor de internet el cual nos brinda el servicio de la siguiente manera a través de una red de fibra óptica:

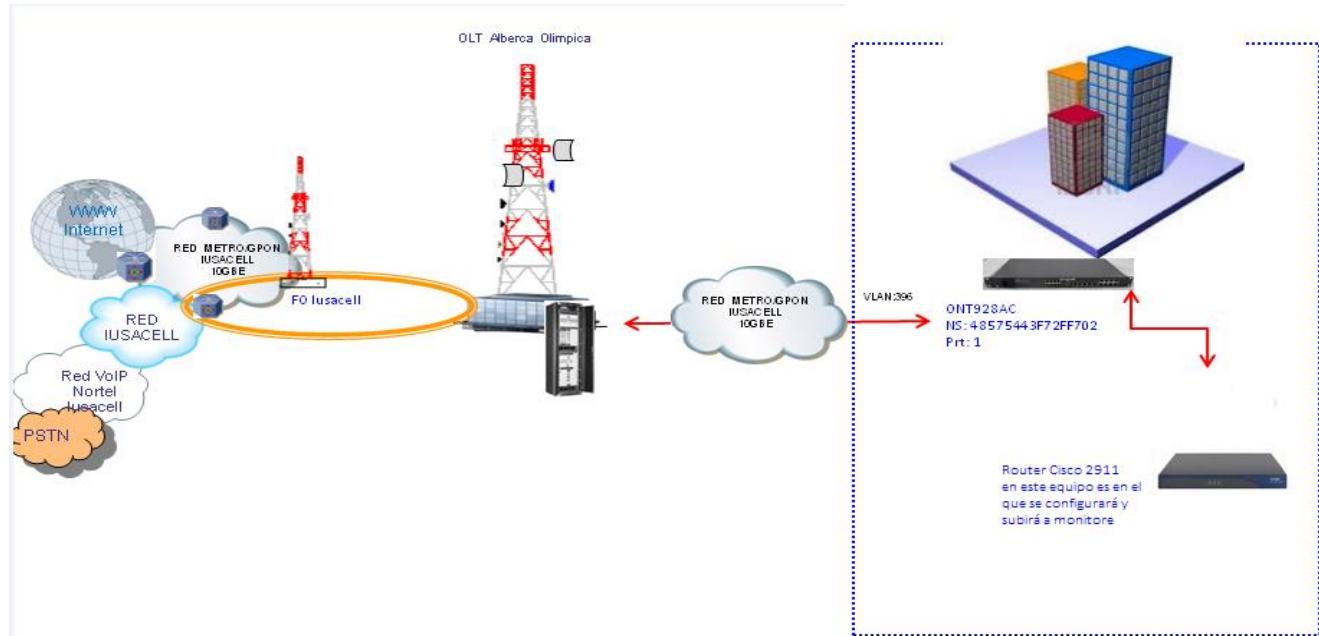


Figura 26 Servicio de Internet

Nuestro ISP Proveedor de servicios de Internet nos asignó una IP pública 187.188.103.29

Esta IP se configuró de la siguiente manera en el router:

Se conectó router Cisco 2911 a la corriente eléctrica, con el interruptor de ON / OFF se encendió.



Figura 27 Router conectado a la corriente eléctrica

Nos conectamos al puerto de consola por medio de un cable y terminal HyperTerminal. HyperTerminal es un programa sencillo de emulación de terminal basado en Windows el cual

utilizamos para conectarnos al puerto de consola del equipo router. Esto debido a que nos resultó la forma más óptima de acceder al router para verificar y cambiar su configuración.

Ocupamos una computadora con una interfaz serial e HyperTerminal instalado, el router Cisco 2911 y un cable de consola para conectar la estación de trabajo al router.



Figura 28 Se muestra el puerto de consola donde conectamos el cable

A través del puerto de consola que es un puerto específico del router el cual permite conectar físicamente la PC con el Router. Se estableció una red similar a la de la figura siguiente:



Figura 29 Se muestra el cable de consola sobre el router y esté conectado al puerto

A su vez este se conectó a la interfaz serial del CPU como se muestra en la figura 29



Figura 30 Cable de consola conectado a CPU y Router

Para la configuración lógica del router se realizó lo siguiente

Accesamos a HyperTerminal e indicamos un nombre para la sesión de HyperTerminal en este caso se eligió el nombre Cisco Console Hyperterm. En la figura 31 observamos que se está ejecutando el programa que utilizamos para comunicarnos con el router.



Figura 31 Conexión Hyperteminal

En la siguiente figura especificamos la interfaz de conexión, estos parámetros vienen definidos en el manual o bien las especificaciones del router 2911.



Figura 32 Interfaz de Conexión

En la figura 33 especificamos las propiedades de conexión de la interfaz

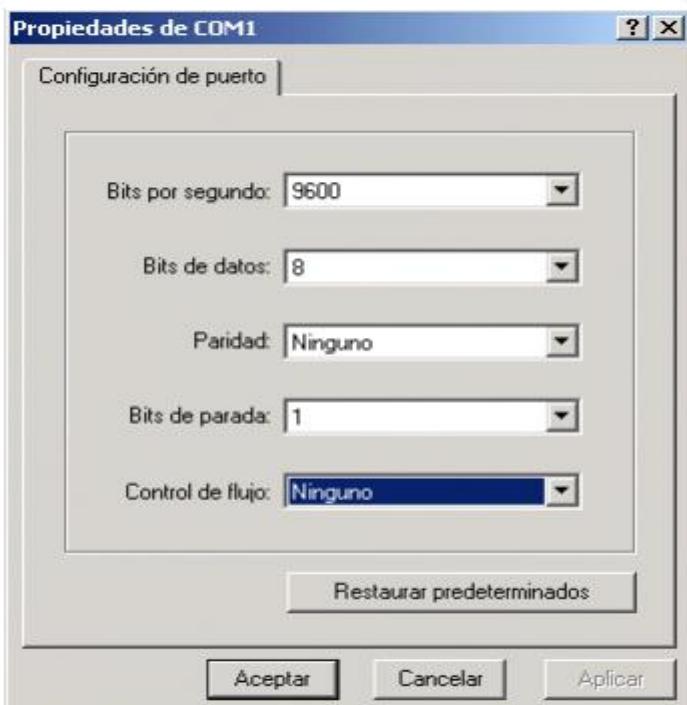


Figura 33 Propiedades de la Interfaz de Conexión

Nos logramos comunicar con el router ingresamos los comandos para asignar la IP pública a una interfaz y habilitar el protocolo telnet para poder accesar al router sin necesidad de conectarlo al cable de consola.

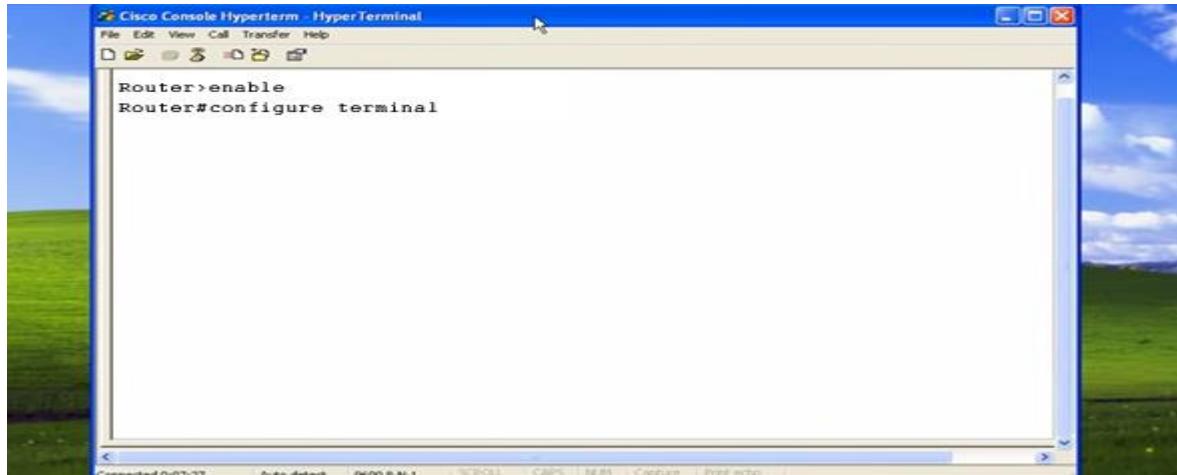


Figura 34 Se logra comunicación con el router con Hyperterminal

En la figura 35 se muestra un diagrama a bloques de como realizamos la comunicación con el router.

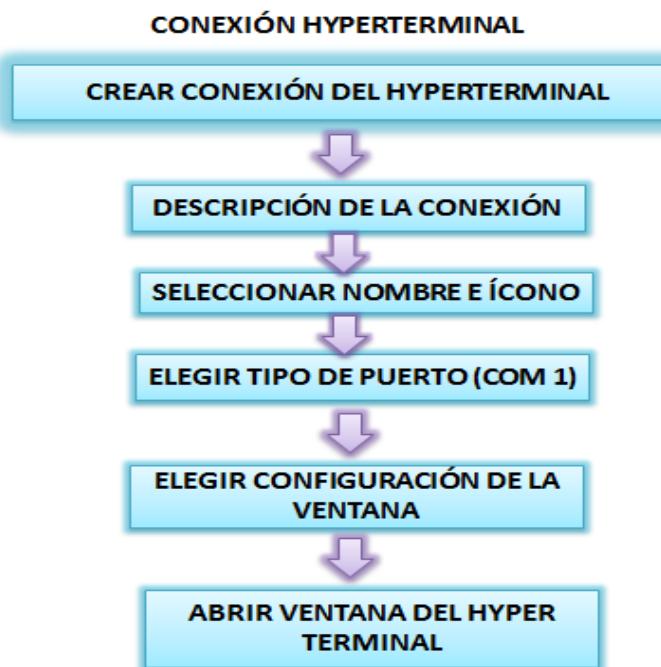
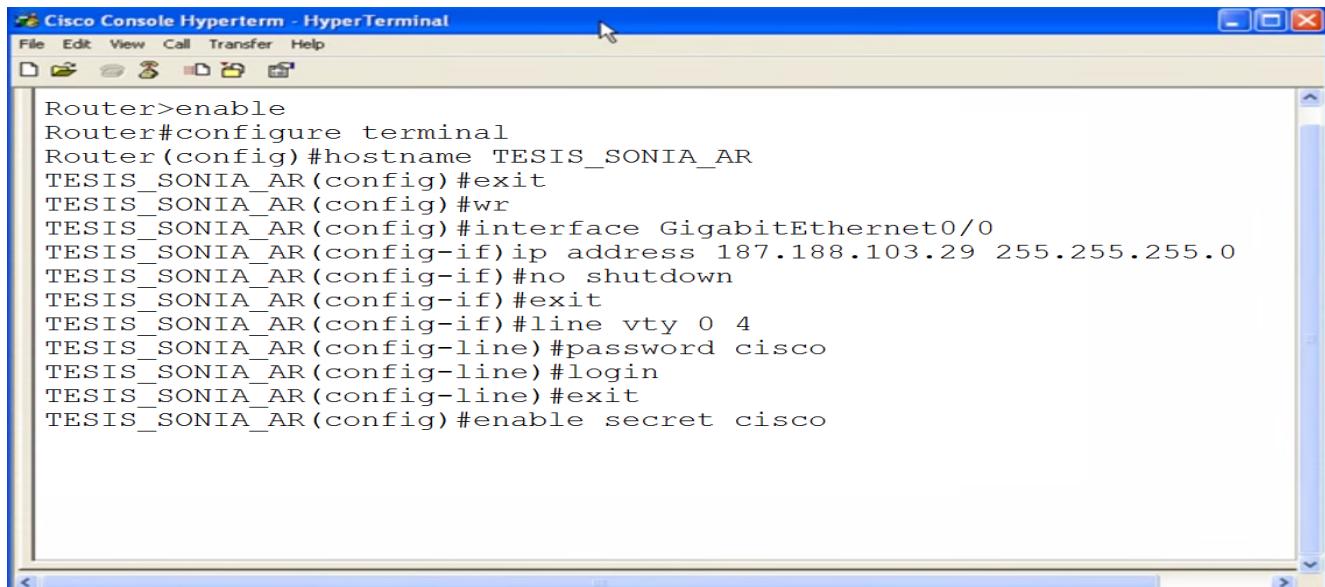


Figura 35 Diagrama a bloques de la conexión Hyperterminal

Después de tener comunicación con el equipo router especificamos el nombre de este y definimos las contraseñas de dicho equipo.



```
Router>enable
Router#configure terminal
Router(config)#hostname TESIS SONIA AR
TESIS SONIA AR(config)#exit
TESIS SONIA AR(config)#wr
TESIS SONIA AR(config)#interface GigabitEthernet0/0
TESIS SONIA AR(config-if) ip address 187.188.103.29 255.255.255.0
TESIS SONIA AR(config-if) #no shutdown
TESIS SONIA AR(config-if) #exit
TESIS SONIA AR(config-if) #line vty 0 4
TESIS SONIA AR(config-line) #password cisco
TESIS SONIA AR(config-line) #login
TESIS SONIA AR(config-line) #exit
TESIS SONIA AR(config) #enable secret cisco
```

Figura 36 Se muestra en la imagen algunas líneas que se escribieron para la configuración del router.

### Configuramos 3 contraseñas

La contraseña necesaria para entrar en el modo consola del router

La contraseña necesaria para entrar en el router mediante terminal virtual de Telnet.

La contraseña para pasar del modo usuario al modo privilegiado.

Con HyperTerminal también nos apoyamos para configurar la interfaz a la cual asignaremos la red WAN.

A partir de aquí dejamos de ocupar el cable de consola ya que configuramos lo necesario para poder accesar al router.

Lo siguiente que realizamos:

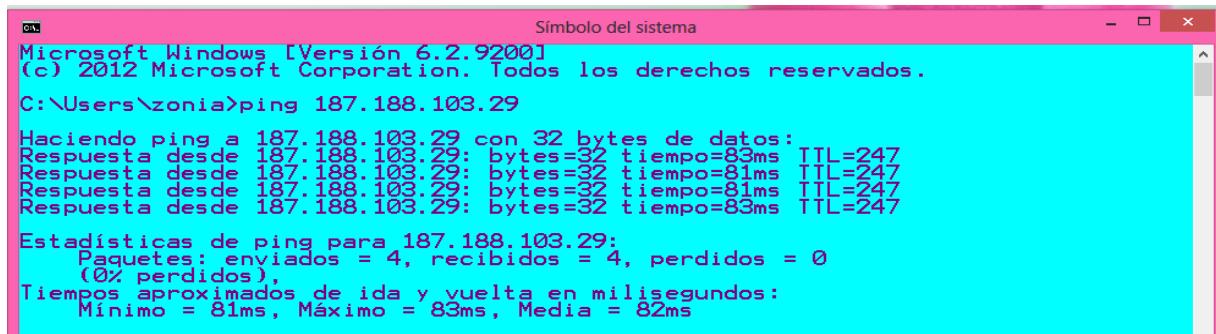
Se conecta el router a la red mediante cable Ethernet en la interfaz 0/0 ya que aquí fue donde se configuró la IP que nos asignó nuestro ISP.



Figura 37 Router conectado a la red WAN

Después de realizar esta primera configuración del Router se corroboró si responde la IP mediante un ping.

Esto se llevó a cabo desde una PC la cual tenía salida a internet y con un Command prompt



```
Símbolo del sistema
Microsoft Windows [Versión 6.2.9200]
(c) 2012 Microsoft Corporation. Todos los derechos reservados.
C:\Users\zonia>ping 187.188.103.29

Haciendo ping a 187.188.103.29 con 32 bytes de datos:
Respuesta desde 187.188.103.29: bytes=32 tiempo=83ms TTL=247
Respuesta desde 187.188.103.29: bytes=32 tiempo=81ms TTL=247
Respuesta desde 187.188.103.29: bytes=32 tiempo=81ms TTL=247
Respuesta desde 187.188.103.29: bytes=32 tiempo=83ms TTL=247

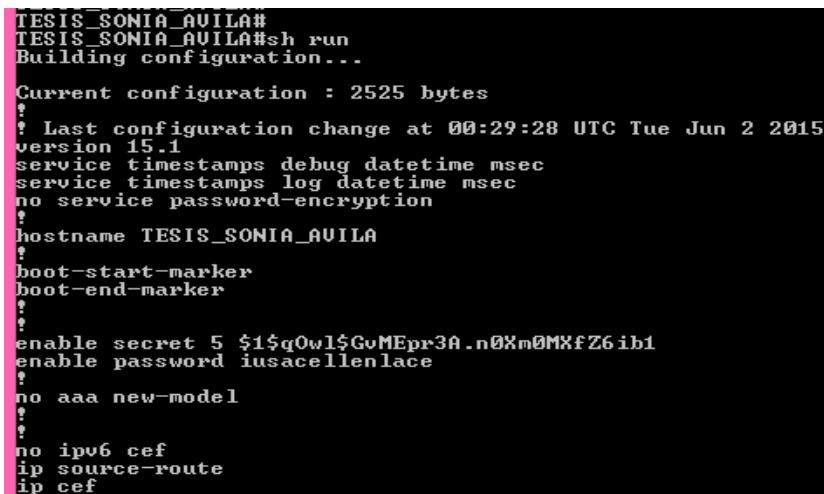
Estadísticas de ping para 187.188.103.29:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos)
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 81ms, Máximo = 83ms, Media = 82ms
```

Figura 38 Ping enviado a la IP pública configurada en el router en la cual se observa que este si responde

En la figura 38 se observa que si responde

Sin embargo la configuración no se llevó a cabo en Command prompt en se hizo en SECURE CRT. Por lo tanto ingresamos al router mediante este programa

Accesamos al router donde observamos que este ya tiene el nombre antes designado



```
TESIS SONIA_AVILA#
TESIS SONIA_AVILA#sh run
Building configuration...
Current configuration : 2525 bytes
!
! Last configuration change at 00:29:28 UTC Tue Jun 2 2015
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname TESIS SONIA_AVILA
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$g0w1$GvMEpr3A.n0Xm0MXfZ6ib1
enable password iusacellenlace
!
no aaa new-model
!
no ipv6 cef
ip source-route
ip cef
```

Figura 39 Parte de la configuración del router



Figura 40 Router conectado a la PC para revisión de la configuración

Para la Configuración del Router Cisco con salida a internet asignamos las direcciones IP a las interfaces.

Se muestra una parte del código

```
TESIS SONIA_AR# sh ip int br
TESIS SONIA_AR# sh ip int brief
Interface          IP-Address      OK? Method Status           Protocol
Embedded-Service-Engine0/0 unassigned   YES NVRAM administratively down down
GigabitEthernet0/0    187.188.103.29  YES NVRAM up               up
GigabitEthernet0/1    10.10.10.10   YES NVRAM down             down
GigabitEthernet0/2    10.203.34.55  YES NVRAM up               up
Virtual-Template2     187.188.103.29 YES unset  up               down
TESIS SONIA_AR#q
Connection to 187.188.103.29 closed by foreign host.
```

Figura 41 Interfaces configuradas en el equipo router se observa la interfaz 0/0 con la IP pública.

Creamos un ACL (Access Control List) en donde seleccionamos el rango de direcciones IP que saldrán a internet

Se creó una lista de control de acceso para definir el rango que se tendrá en cuenta para la salida a internet

Creamos reglas de NAT (Network Address Translation) que permitirá la traducción de direcciones de la lista que seleccionamos en el ACL a una IP válida asignada por nuestro ISP (internet service provider)

Se crea una ruta por default hacia el Gateway para la salida a Internet

Verificar si el router tiene salida a internet

```
TESIS SONIA_AR#ping 4.2.2.2 source 187.188.103.29
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 187.188.103.29
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/36 ms
```

Figura 42 Verificación de Router con salida internet con un ping hacia un DNS de Google.

Con esto concluimos la configuración del router con salida a internet.

### 3.4 BLOQUE II CONFIGURACIÓN PROTOCOLO SNMP

Después de configurar el router con salida a internet configuramos el protocolo SNMP dentro de este con la finalidad de tener gestión.

La aplicación de monitoreo Solarwinds se encuentra dentro de un servidor. El cuál se muestra en la figura

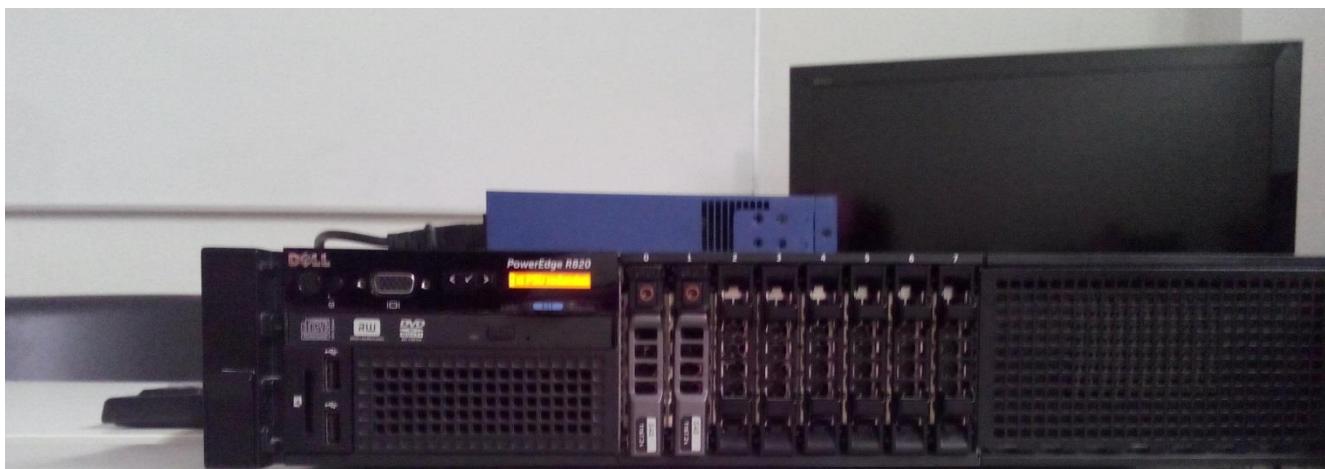


Figura 43 Servidor donde se encuentra alojada la aplicación Solarwinds



Figura 44 Parte trasera de servidor donde se encuentra alojada la aplicación Solarwinds

El sistema Solarwinds utiliza el Protocolo Simple de Administración de Red (SNMP) para recolectar información detallada acerca de los nodos y recursos asociados a los nodos como interfaces y volúmenes.

SNMP requiere un agente que reside en el cliente que monitorea y archiva información en los Identificadores de Objeto (OID) que son parte de diferentes bases de Datos de Información de Administración (MIB). El MIB reside en el nodo de red.

Orión obtiene información de los nodos monitoreados en una de dos maneras:

Orion Consulta los MIBs del nodo monitoreado y pide los valores contenidos en OIDs específicos. El nodo responde con los datos solicitados. Orion toma la respuesta y la guarda en la tabla apropiada de la base de datos de Orion.

El nodo monitoreado manda un trap de SNMP hacia el servidor de Orion. Orion recibe el trap, aplica filtros y guarda el contenido del trap en la tabla de traps en la base de datos de Orion.

### 3.5 BLOQUE III ALTA EN MONITOREO EN SOLARWINDS

Para agregar los nodos que serán monitoreados con Orion de manera manual, se realizó desde la consola web, ya que como lo mencionamos anteriormente la aplicación se encuentra en un servidor y este servidor tiene asignada una IP pública.

Se tecleo directamente la IP pública del servidor (187.188.103.17:8080) desde un navegador

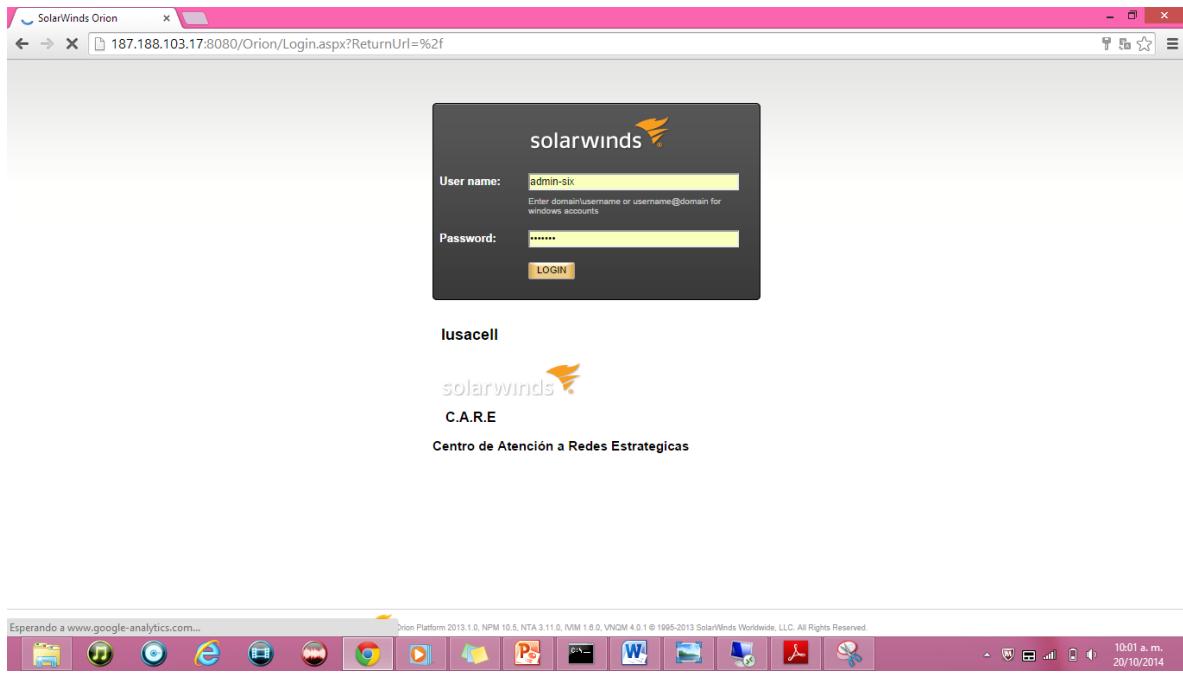


Figura 45 Aplicación Solarwinds

Después de accesar seleccionamos de la parte superior derecha de la consola web la opción settings, luego de Orion Website Administration seleccionamos Add Node.

Se despliega la ventana Add Node solicitando la información del nodo a agregar. Se ingresaron los datos, nombre o IP del host, método de poleo.



Figura 46 Pantalla para agregar el Nodo a Monitoreo

Se dio de alta el router en la aplicación de monitoreo Solarwinds con la IP pública que se configuró en este 187.188.103.29.

Se ingresa comunidad y versión de SNMP, en este caso la comunidad es netview y la versión V2.

Se realizó prueba de conectividad con el botón test la cual resultó exitosa, esto comprueba que el protocolo SNMP configurado en el router es correcto.

Name:  Polling IP Address:   IPv4 and IPv6 formats are both valid

Dynamic IP Address (DHCP or BOOTP)

Polling Method

- No Status:** External Node  
No data collection for this node.
- Status Only:** ICMP  
Collect status, response time and packet loss data only, using ICMP (ping).
- Windows Servers:** WMI and ICMP  
Collect CPU, memory, volume and ICMP data for Windows Servers that do not support SNMP.
- Most Devices:** SNMP and ICMP - Recommended  
Collect CPU, memory, volume and ICMP data for most SNMP-enabled devices.

SNMP Version:  SNMPv2c is used, by default, when SNMPv3 is neither required nor supported.  
 SNMP Port:   
 Allow 64 bit counters

Community String:  Press down arrow to view all  
 Read/Write Community String:

Figura 47 IP Pública configurada en el Sistema de Monitoreo

Admin > Node Management >

### Add Node

DEFINE NODE > CHOOSE RESOURCES > ADD POLLERS > CHANGE PROPERTIES >

#### Define Node

Specify the node you want to add by completing the fields below. Are you adding a large number of nodes? Try the [Network Discovery](#).

Polling Hostname or IP Address:  IPv4 and IPv6 formats are both valid

Dynamic IP Address  
(DHCP or BOOTP)

Polling Method

- No Status:** External Node  
No data collection for this node.
- Status Only:** ICMP  
Collect status, response time and packet loss data only, using ICMP (ping).
- Windows Servers:** WMI and ICMP  
Collect CPU, memory, volume and ICMP data for Windows Servers that do not support SNMP.
- Most Devices:** SNMP and ICMP - Recommended  
Collect CPU, memory, volume and ICMP data for most SNMP-enabled devices.

SNMP Version:  SNMPv2c is used, by default, when SNMPv3 is neither required nor supported.  
 SNMP Port:   
 Allow 64 bit counters

Community String:  Press down arrow to view all  
 Read/Write Community String:

Test Successful!

Figura 48 Test exitoso de la IP Pública

Se realizó una acción de descubrimiento donde todas las MIB'S son recolectadas, nos desplegó una nueva ventana donde podemos observar todas las interfaces que tiene el nodo y una casilla donde habilitaremos lo que queremos monitorear. Las variables que por default nos mostró son:

Estatus del nodo

Dirección IP

Tipo de máquina

Nombre del sistema (nombre del nodo)

Descripción

Sistema Operativo

Las variables que continuamente se miden en el nodo son:

Promedio de tiempo de respuesta y paquetes perdidos

Y las variables que mide en cada interfaz del nodo son:

Promedio de bits transmitidos y paquetes perdidos

Porcentaje de utilización de ancho de banda

Total de errores

Promedio de paquetes recibidos y enviados

Una vez que Orion estableció la comunicación con el nodo de destino a través de SNMP, se presentó una lista de todos los recursos disponibles detectados.

Entre estos se encuentran las interfaces físicas que se configuraron, se seleccionaron las interfaces que queremos que el sistema grafique.

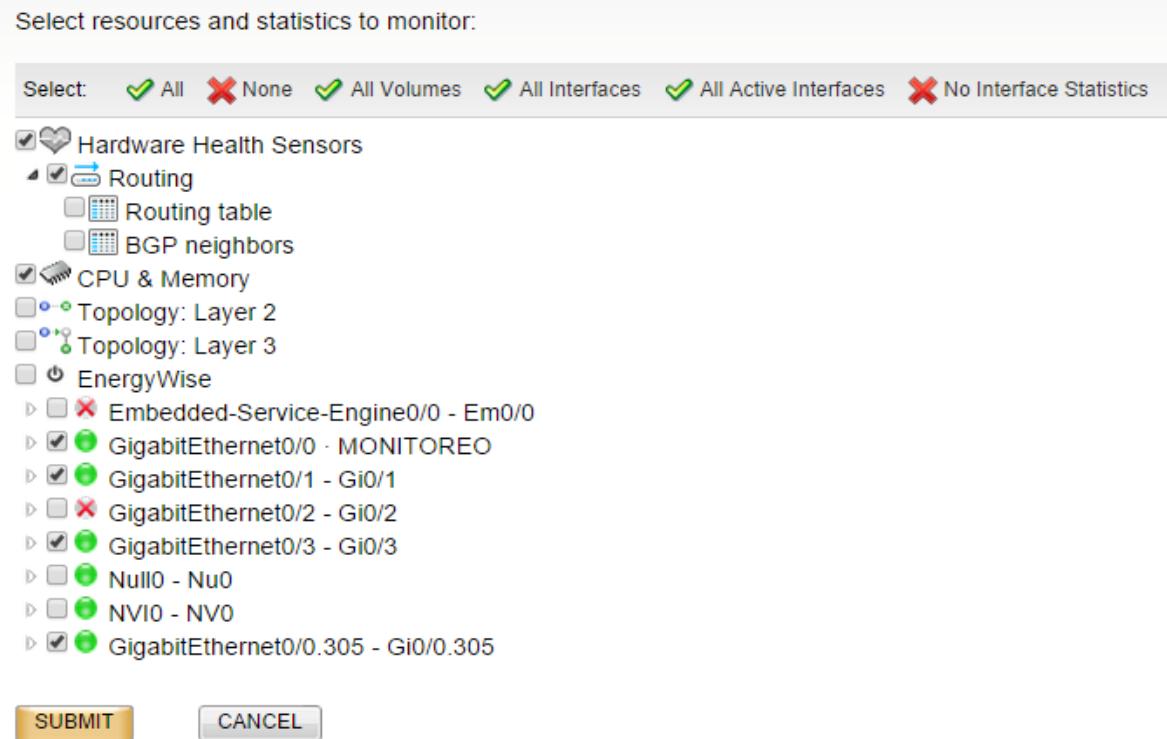


Figura 49 Interfaces descubiertas al momento de dar de alta en el monitoreo

Después de seleccionar que es lo que queremos monitorear, la pantalla de Change Properties se presenta.

Esta sección nos permitió modificar propiedades del nodo agregado tales como el nombre, intervalos de sondeo y colección de estadísticas específicamente de este, así como llenar el valor para este nodo, de los campos de propiedades personalizadas que estén ya definidas .

The screenshot shows the configuration page for a monitored node named 'TESIS SONIA AR'. The IP address is set to '187.188.103.29'. The 'Polling Method' section is expanded, showing four options: 'No Status: External Node' (disabled), 'Status Only: ICMP' (disabled), 'Windows Servers: WMI and ICMP' (disabled), and 'Most Devices: SNMP and ICMP - Recommended' (selected). Under this option, the 'SNMP Version' dropdown is set to 'SNMPv2c' (selected), and the 'SNMP Port' is set to '161'. A checked checkbox indicates 'Allow 64 bit counters'. Below these settings are two input fields: 'Community String: netview' and 'Read/Write Community String:'. A 'Test' button is located at the bottom of this section.

Figura 50 Cambio de propiedades en el Nodo a Monitorear

### 3.6 BLOQUE IV MONITOREO DE LA RED MEDIANTE LA OBTENCIÓN Y ANÁLISIS DE TRÁFICO

El Router y las interfaces configuradas ya se encuentran monitoreadas, debemos esperar a que el sistema empiece a polear para poder obtener las gráficas. Observar la Disponibilidad y el consumo, así como las gráficas de las interfaces.

### 3.7 BLOQUE V CONFIGURACIÓN DE ALERTA DE LA CAÍDA DEL NODO O ALGUNA INTERFAZ

Las alertas evaluarán los datos de sondeo y estadísticas en el momento que se obtengan del elemento monitoreado. Solarwinds comprara el criterio de la alerta definida, el estatus actual del elemento buscando encontrar que un umbral haya sido rebasado ( trigger, que dispara la alerta).

Primero definimos la alerta, ésta se deberá enviar cuando el nodo agregado TESIS\_SONIA AR o alguna de sus interfaces monitoreadas se encuentren down.

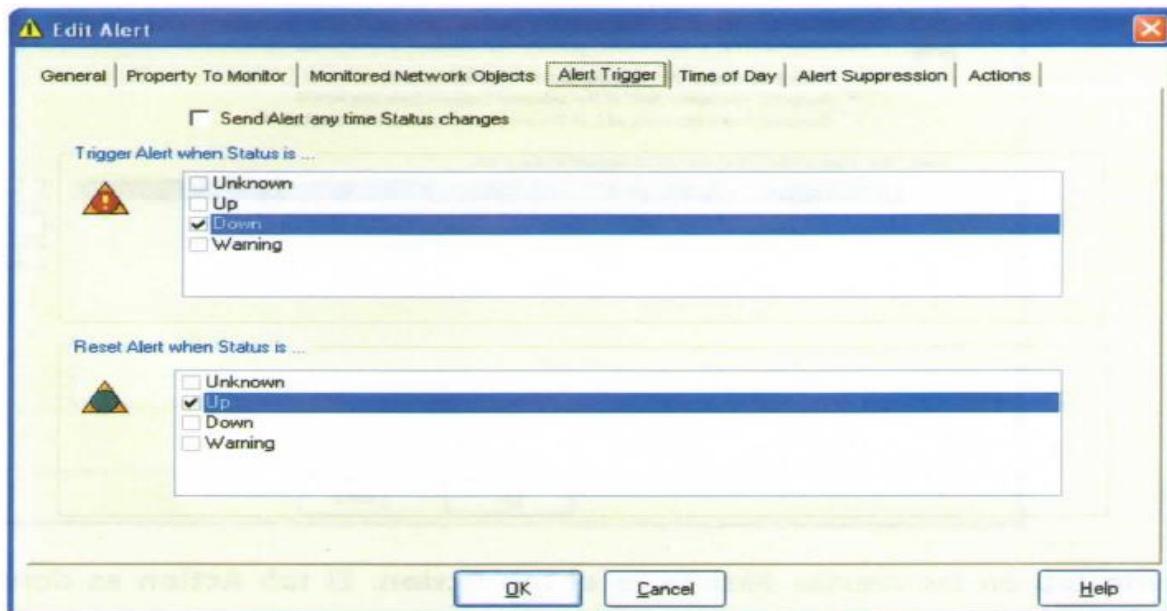


Figura 51 Consola de configuración de alertas

Una vez que se determina que un umbral ha rebasado lo que anteriormente determinamos, el elemento TESIS SONIA AR es puesto en un “estado de Alerta”.

Al alcanzar el “estado de Alerta”, se ejecutarán las acciones que definiremos a continuación.

Para definir las acciones de Alerta

Lo que configuramos en este bloque es que las alertas lleguen al correo esto con el fin de avisar que alguna interfaz o todo el nodo quedo fuera.

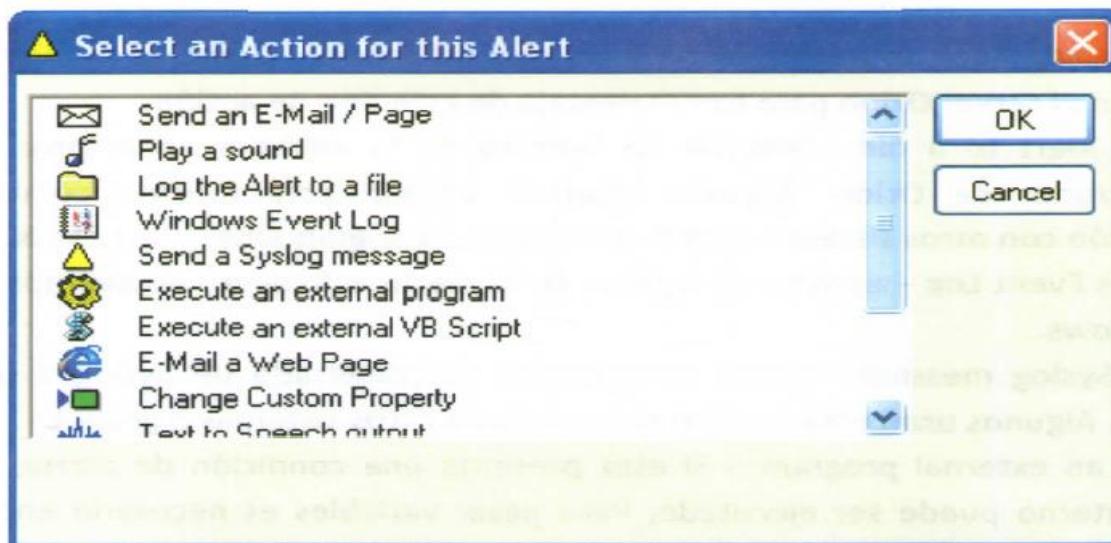


Figura 52 Send an E-mail envía un e-mail una o más direcciones de correo electrónico.

Con solarwinds tuvimos la opción de personalizar la información que se va a enviar en las alertas. Esto lo hicimos mediante macros, variables o table field names.

Usar variables tiene como objetivo el jalar información desde la tabla de la base de datos a la que la alerta hace referencia e incluirla en el mensaje personalizado de la acción.

La alerta sacará la información de la tabla de Nodos. Para ver una lista de los campos disponibles, utiliza el Database Manager o contacta al DBA responsable.

Si la alerta definida es sobre una interfaz monitoreada, la alerta saca la información de la tabla de interfaces.

De igual forma definimos las alertas de las interfaces solo cambiamos el texto de lo que se enviará vía correo electrónico.

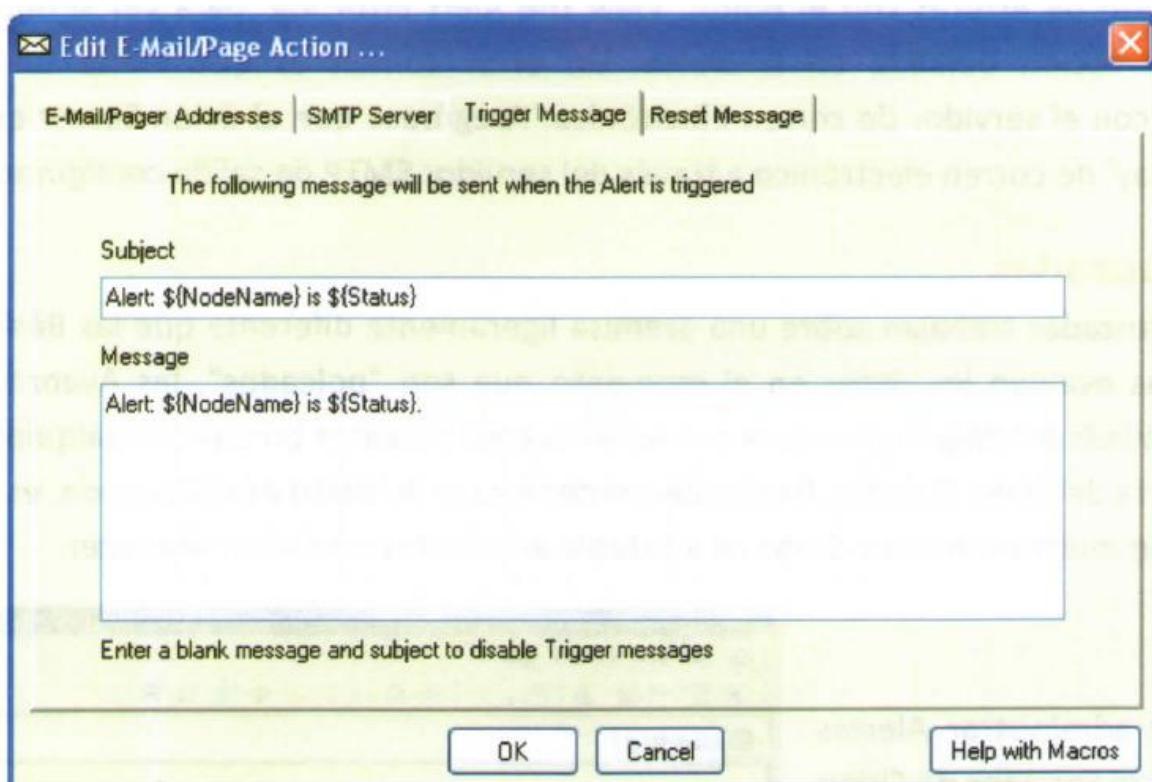


Figura 53 Definición de Alertas e Interfaces

### **3.8 BLOQUE VI CONFIGURACIÓN ALERTA VÍA MAIL Y SMS**

El envío de alertas por correo es a través de una cuenta corporativa de correo electrónico.

Los correos llegarán a la cuenta [savila@enlacetpe.mx](mailto:savila@enlacetpe.mx).

Se enviarán a través de un servidor corporativo con el que se cuenta para enviar sms, llamado rk2. Este servidor tiene conectado un modem externo GSM.

En el correo se configuró la acción de que en cuanto lleguen correos del remitente "Solarwinds" estos se envíen automáticamente mediante el servidor en este caso al número 5518027962

Creamos una nueva regla en la carpeta "Reglas de correo".

Selecciona "Todos los documentos" seleccionamos los correos que nos han llegado de las alertas "Crear condición" en el cuadro de diálogo. "Agregar". Selecciona "Cuando todos los correos se reciben" para asegurarte de que todos los correos sean enviados.

Haz clic en "Especificar acciones" y selecciona "Enviar copia a" del menú desplegable. En el cuadro de diálogo, ingresamos la dirección de correo electrónico en la que queremos recibir los correos reenviados.

Añadido a esto también agregamos una cuenta de Gmail savilaenlacetpe.mx.

# **CAPÍTULO 4.**

## **COMPORTAMIENTO DEL SISTEMA DE MONITOREO DE UNA RED EN FIBRA ÓPTICA**

#### **4.1 Configuración de router mediante cable de consola con la IP, para que tenga salida a internet.**

La configuración del router Cisco es la base para iniciar con este proyecto, como se mostró en el capítulo anterior el alta en el sistema de monitoreo fue exitosa; se obtuvieron las gráficas de disponibilidad, latencia y consumo, sin embargo para mayor seguridad del portal y de nuestra red, nuestro ISP solicitó se pusiera una IP de su red privada donde solo ellos pudieran accesar, esto debido a ciertos ataques que pudiéramos sufrir. La IP pública quedó configurada en el router sin embargo la que vamos a monitorear es la de nuestro proveedor, ya que está solo la alcanzan ellos desde su red corporativa.

La IP configurada en el router es la siguiente 10.207.121.82 esta IP quedó configurada en la interfaz 0/0 (WAN) del router la IP pública se configuró en la interfaz 0/1 del router (LAN)

Se presentaron algunos inconvenientes como el daño físico del equipo ONT donde llega la fibra óptica, no detectaba conexión del cable Ethernet que va de dicho equipo hacia el router se reemplazó de ONT y se conectó directamente al router como se muestra en la imagen



Figura 54 Equipo ONT (Optical Network Terminal)

En la imagen 54 se muestra el equipo donde se realizaron las primeras pruebas el cuál se dañó.



Figura 55 Nuevo equipo ONT que se reemplazó

Al intentar dar de alta en el sistema de monitoreo este no se alcanzaba el segmento que asignaron al router debido a un problema de gestión con el ISP, se solicitó se revisará el por qué.

El problema radicaba en que se tenía desconfigurada en el nuevo equipo lo que ellos llaman VLAN de gestión.

Se realiza la correcta configuración y se realiza prueba en la cual nos muestren que el router ya es alcanzable desde su red.

Realizan configuración de esta VLAN, en el nuevo equipo y en la siguiente imagen se muestra la prueba de que ya se tiene gestionable el router.

Figura 56 Muestra del alcance del equipo desde la Red del proveedor

Configurar el protocolo SNMP en el router, fue el siguiente paso ya que es la base para monitorear el equipo. La información que provee SNMP es usada para mostrar el estado del equipo y alertar cuando alguna situación se detecta. En pocos minutos habilitamos protocolo. Seguido de esto realizamos el alta en el sistema de monitoreo, con la nueva IP de monitoreo, que es la **10.207.121.82**

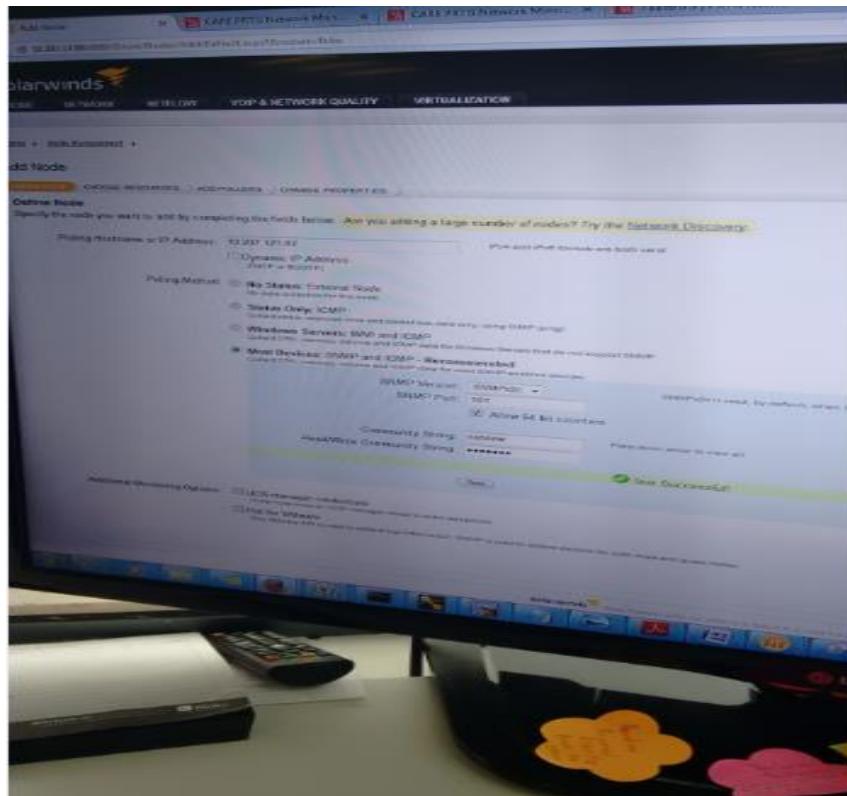


Figura 57 IP 10.207.121.82 dada de alta en sistema de monitoreo, se observa que se ingresó al nodo y al testear esta nos arroja el mensaje de “successful” lo cual nos indica que el protocolo SNMP con la comunidad netview configurado anteriormente en el router resultó exitosa.

En la siguiente imagen se muestra el alta en monitoreo donde el sistema descubre las interfaces a monitorear

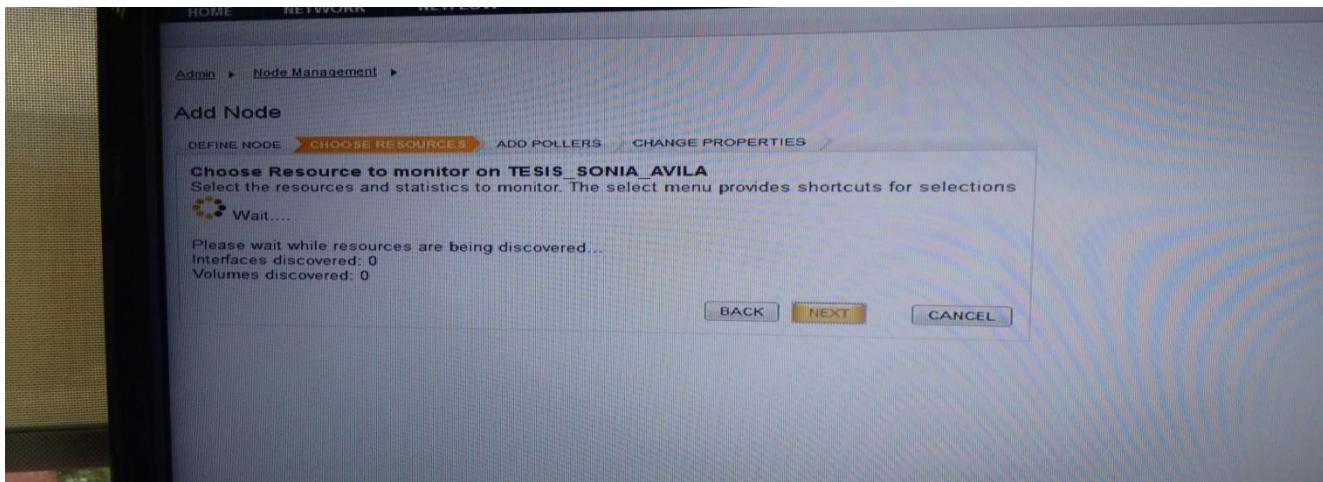


Figura 58 Interfaces a Monitorear

Seleccionamos las interfaces que deseamos monitorear para este proyecto necesitamos monitorear la interfaz WAN por lo cual la seleccionamos , tambien se seleccionó la LAN para en cuanto se ponga en producción el enlace nos arroje el trafico que está consumiendo.

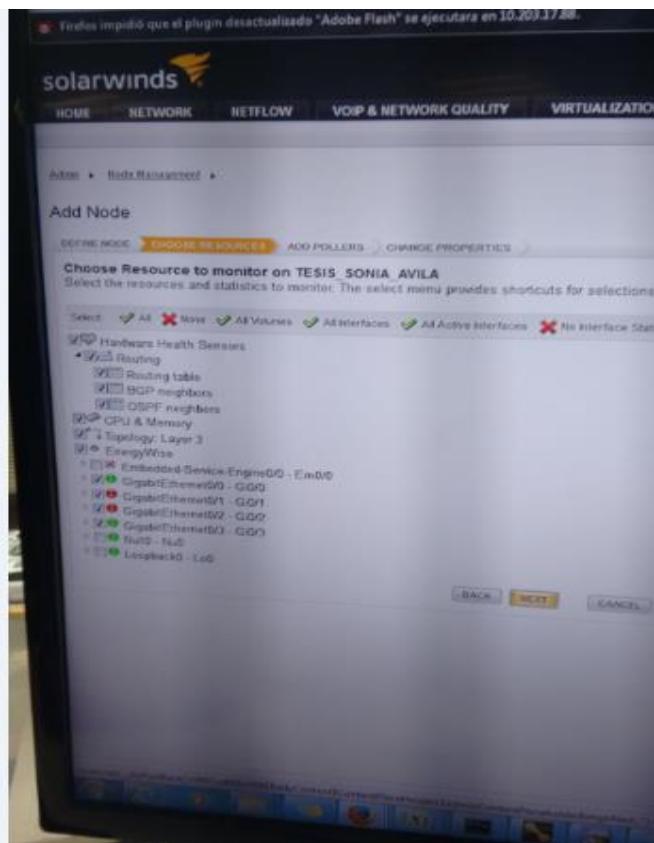


Figura 59 Interfaces descubiertas del equipo Router

Ingresamos datos y nombre del nodo

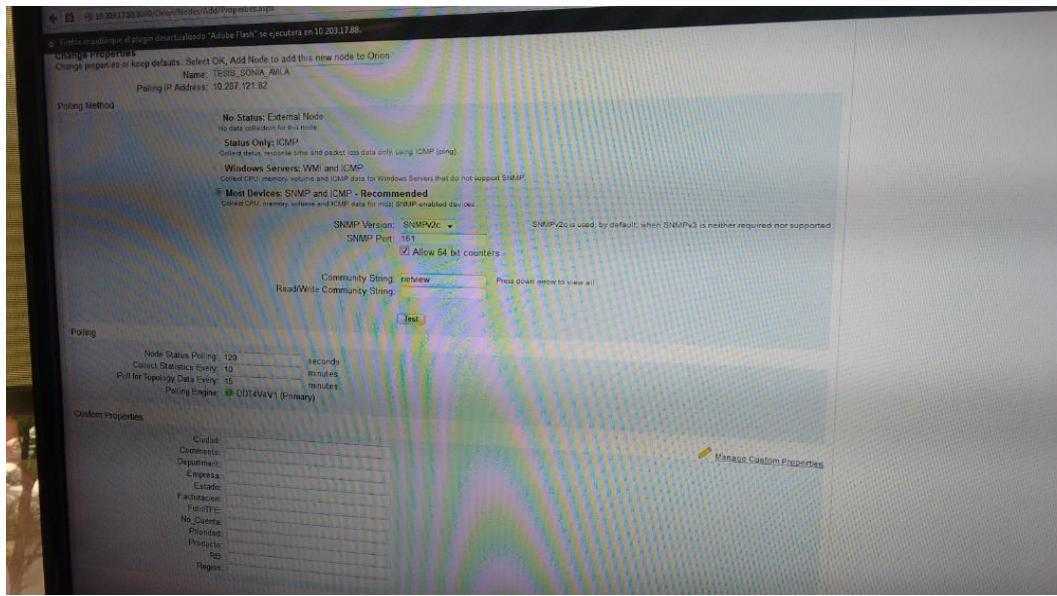


Figura 60 Pantalla donde se colocan las características e información sobre el Nodo

#### 4.2 Monitoreo de la red mediante la obtención y análisis del tráfico de la misma.

Damos tiempo a que el sistema obtenga las gráficas se obtiene disponibilidad, latencia y pérdida de paquetes y consumo, en las 3 gráficas siguientes se muestra el primer poleo que arrojó el sistema

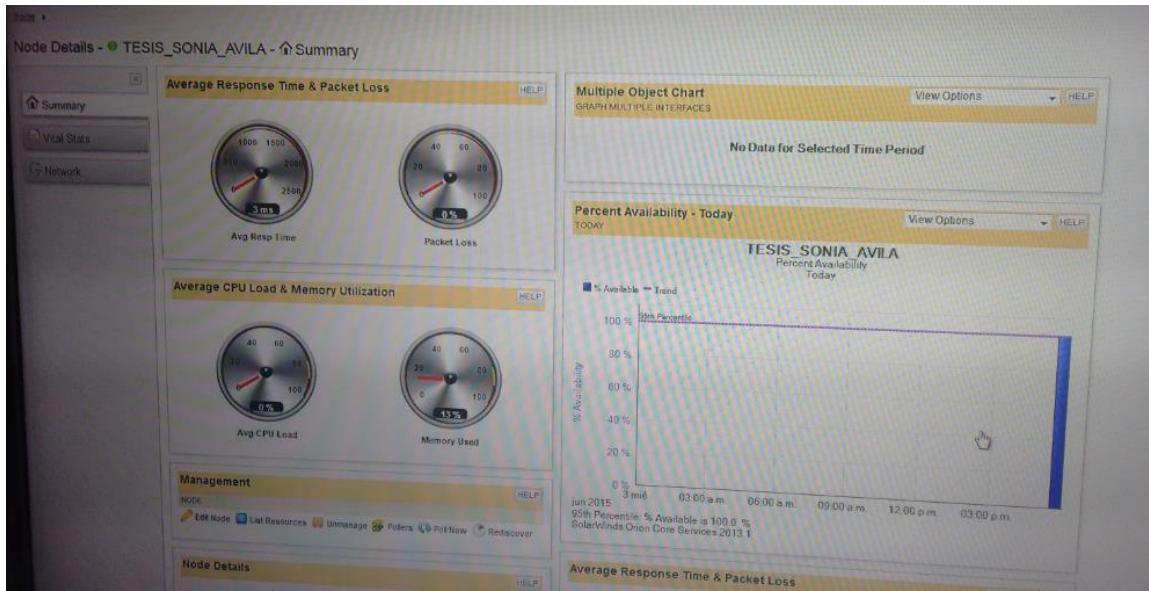


Figura 61 Gráfica de Disponibilidad primer poleo.

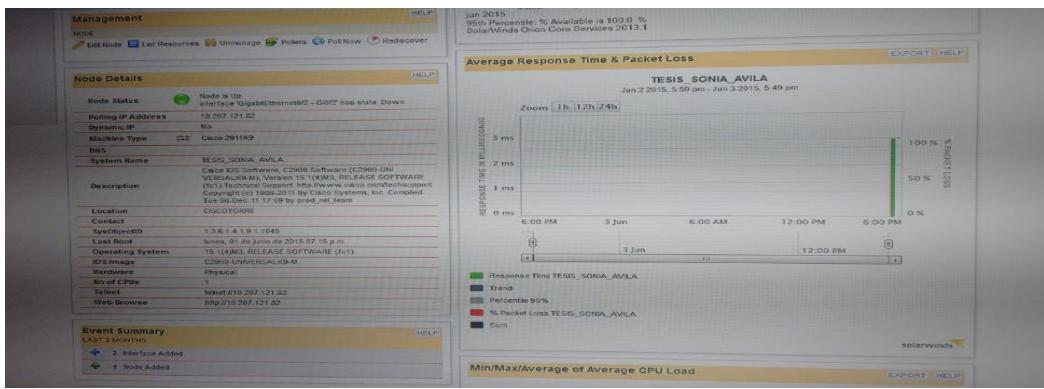


Figura 62 Gráfica de Latencia & Pérdida de paquetes primer polo.

En esta parte se muestran las dos interfaces LAN y WAN la interfaz LAN se observa en rojo debido a que no hay nada conectado en el router

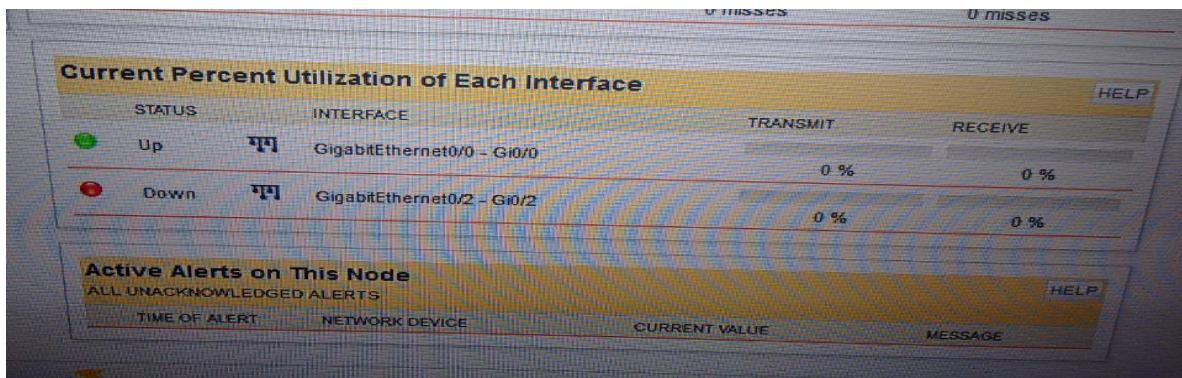


Figura 63 Interfaces Monitoreadas GigabitEthernet0/0 y GigabitEthernet0/2

Transcurrida una semana sacamos el resultado de las gráficas el cuál es el siguiente

Se observa que no se graficó por unos días, debido a que se desconectaron los equipos, aquí comprobamos que la aplicación Solarwinds arroja los resultados correctos en cuanto los equipos fueron desconectados se alarma el nodo y dejó de graficar, al volver a conectar la alarma se limpió y el sistema comenzó a graficar nuevamente.

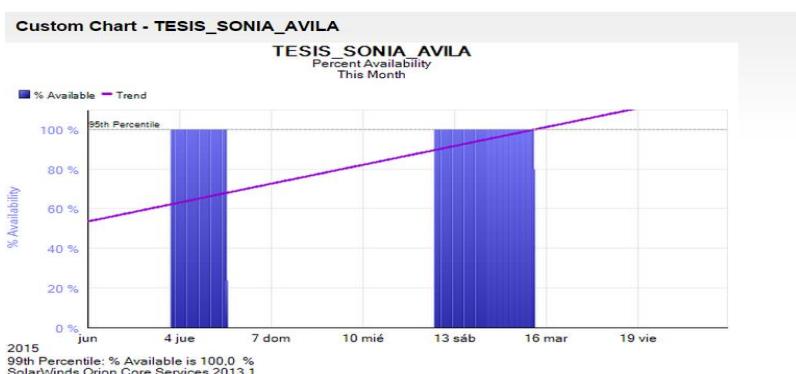


Figura 64 Grafica de Disponibilidad Transcurrida una semana

Orión realiza colección de estadísticas en los elementos monitoreados a través de consultas a un MIB SNMP obteniendo un vistazo adicional al rendimiento y operaciones de los elementos monitoreados.

Los intervalos default de sondeo son cada 120 segundos. Los intervalos default de colección de estadísticas son cada 10 minutos y 9 minutos, para nodos e interfaces

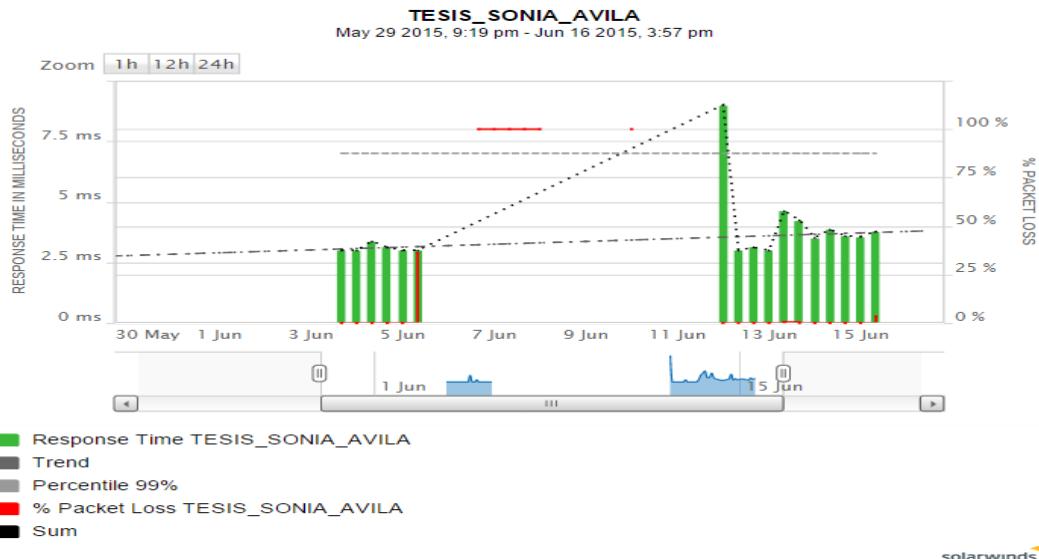


Figura 65 Gráfica de Latencia & paquetes perdidos aquí podemos observar el tiempo que tarda en responder el ping se tienen tiempos máximos de 7.5 ms.

Se anexan las gráficas tanto de disponibilidad, latencia & pérdida de paquetes después de graficar una semana; en la gráfica se observa la fecha y el nombre del nodo.

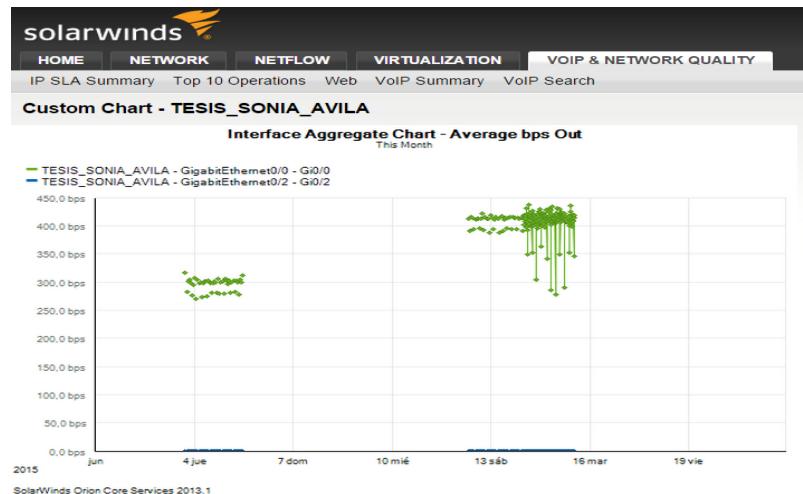


Figura 66 Gráfica de consumo, en sistema no detecta consumo ya que aún no conectamos nada al router y por ende no hay tráfico.

En la figura 67 se observan las gráficas obtenidas durante un periodo de 7 días. Se anexan las 3 gráficas de monitoreo obtenidas: Disponibilidad, Latencia & Pérdida de Paquetes y Consumo.

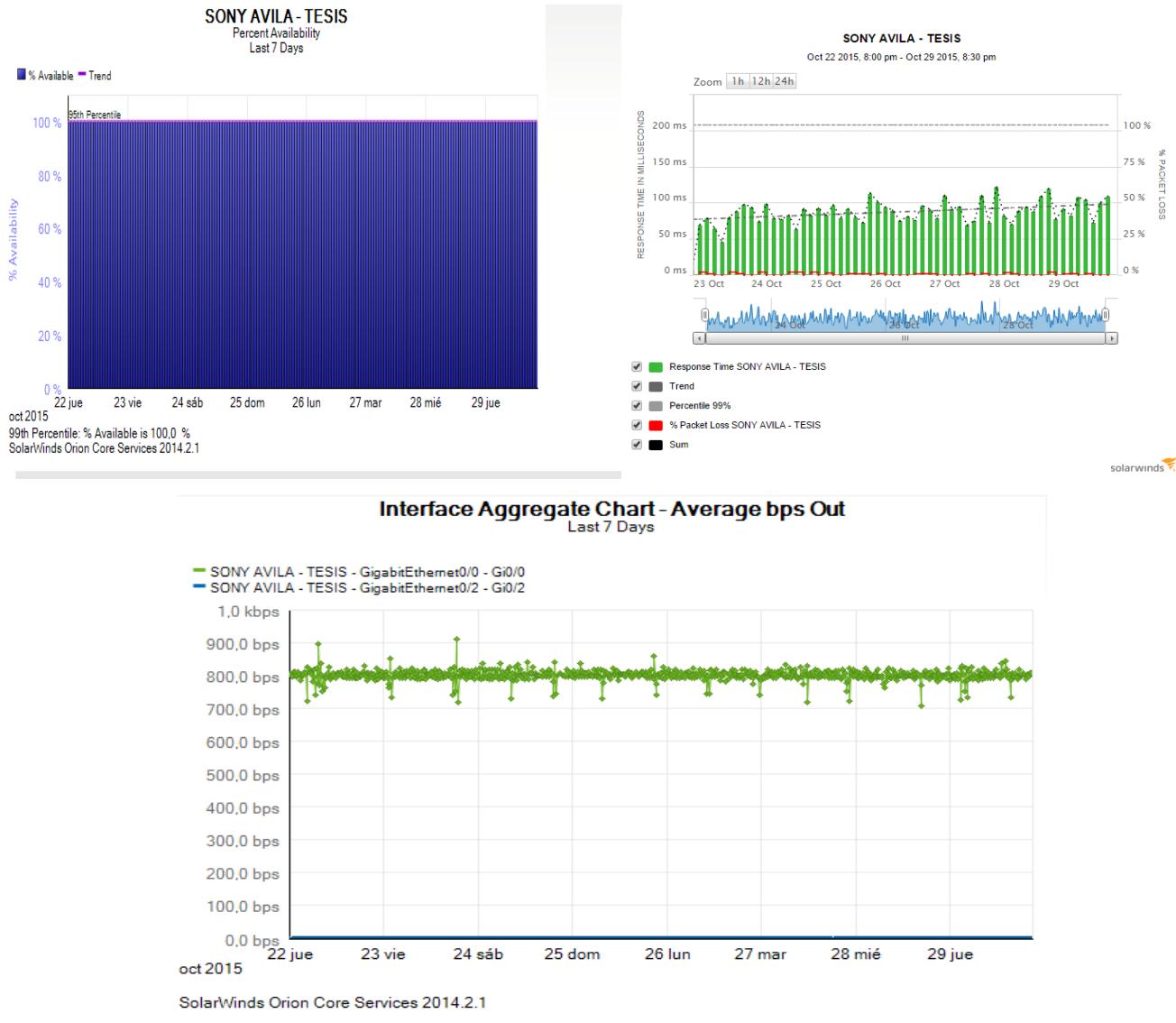


Figura 67 Gráficas de monitoreo durante una semana

#### **4.3 Configuración alerta de la caída del sistema en la plataforma de monitoreo Solarwinds interfaz en primera instancia en la interfaz WAN.**

Configurar alerta vía correo electrónico y configuración de la alerta SMS mediante servidor donde se encuentra alojada la aplicación Solarwinds.

Para la notificación de alertas vía mail utilizamos el sistema Solarwinds

A partir de Orion NPM que es un sistema administrador de redes puede procesar alarmas SNMP de cualquier dispositivo sin importar modelo o fabricante.

El sistema de monitoreo automático incorporado recibe estadísticas y genera alertas si encuentra modelos de datos inusuales.

Todos los eventos de red y alarmas son mostrados con la herramienta de registro de eventos.

El NPM caracteriza un sistema de alarma de lenguaje real el cual toma complejas alarmas SNMP.

En la figura 66 se muestra como se dieron de alta las alertas en el sistema de Monitoreo, desde el servidor donde está alojada la aplicación Solarwinds

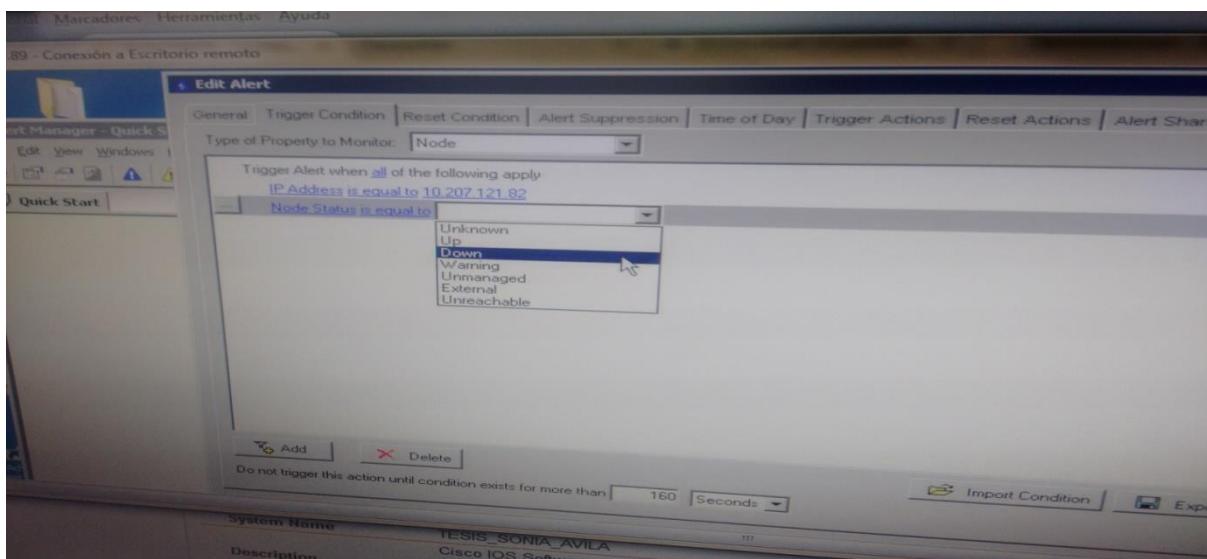


Figura 68 IP del router dada de alta en el sistema de Monitoreo a través del Servidor donde se encuentra alojada la aplicación Solar Winds.

Se da de alta la IP y las condiciones que deberá cumplir para que se envíen las alarmas.

El sistema detectara cuando este down la interfaz 0/0, y en un lapso de 10 minutos enviará el mensaje tanto al correo electrónico y vía SMS, esto con la finalidad de evitar falsas alarmas.

El tener “falsas alarmas” quiere decir que algunas veces se presentan oscilaciones en que solo nos alarmañan y podría ser que no fuera un evento real.

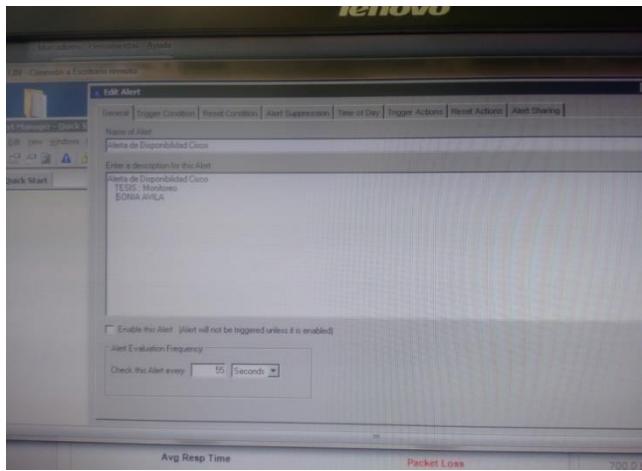


Figura 69 Configuración de alerta a enviar

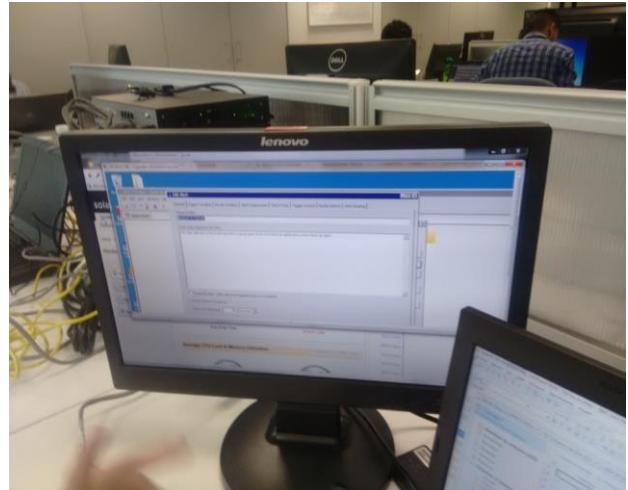


Figura 70 Pruebas realizadas sobre los diferentes mensajes que se pudieran recibir desde la aplicación Solarwinds

#### **4.4 Reconexión de equipos para probar Sistema de Monitoreo**

Durante las pruebas realizadas se cambió el nombre del equipo por SONY AVILA\_TESIS. La maqueta de prueba se desconectó y se volvió a conectar para continuar con las pruebas.

Se reconectan equipos para seguir realizando las pruebas, se observa que el sistema empieza a graficar.

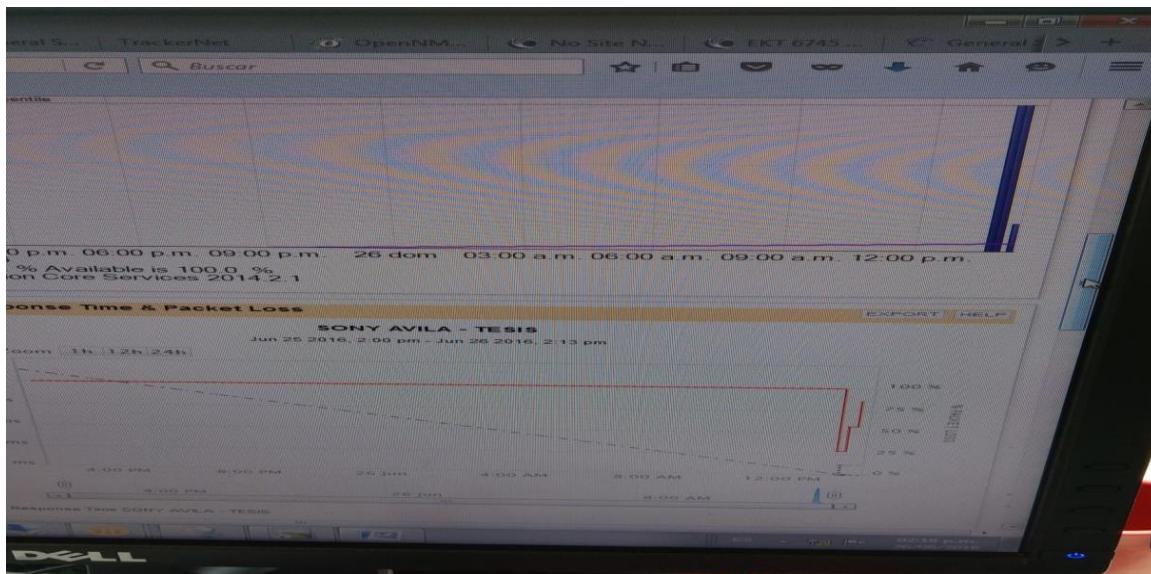


Figura 71 Primer poleo después de la reconexión Disponibilidad

Para asegurarnos de que al reconectar los equipos empiece a polear el sistema se realiza un ping extendido desde la computadora hacia la ip de gestión.

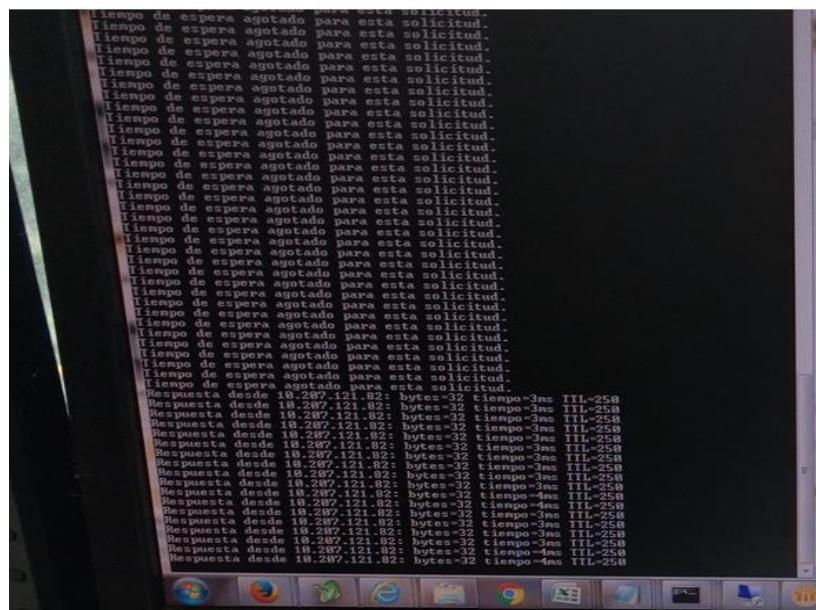


Figura 72 Ping extendido hacia la IP 10.207.121.82

Se observa que el Ping empieza a responder con esto comprobamos que el equipo ya es alcanzable desde la Red y por lo cual debe empezar a graficar en el sistema de Monitoreo.



Figura 73 Maqueta de Prueba reconectada nuevamente Equipo Cisco y equipo ONT conectados a la corriente eléctrica y a la fibra óptica.

Se realizan pruebas de conexión y desconexión de los equipos realizando las validaciones correspondientes con ping

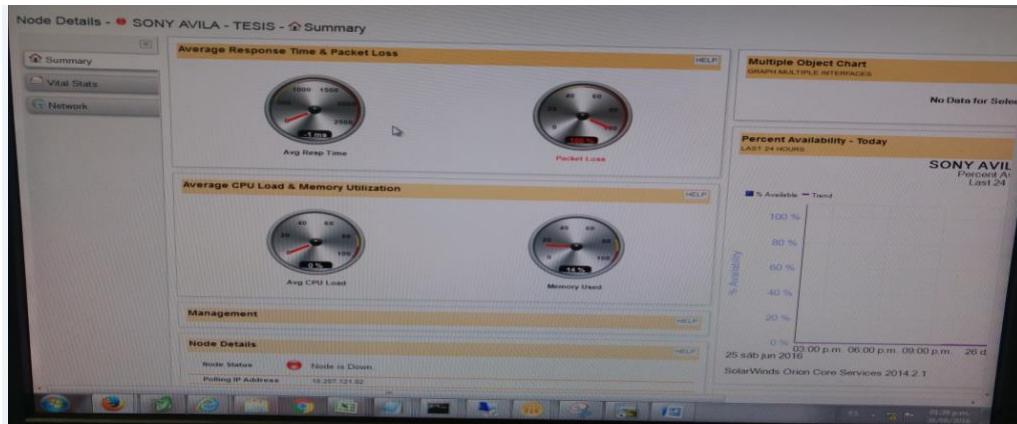


Figura 74 Interfaz Gráfica del Solarwinds donde se muestra el estatus del Nodo el cual está en estado de down

Se anexan las imágenes donde llegan las alarmas al celular se tomó una captura de pantalla

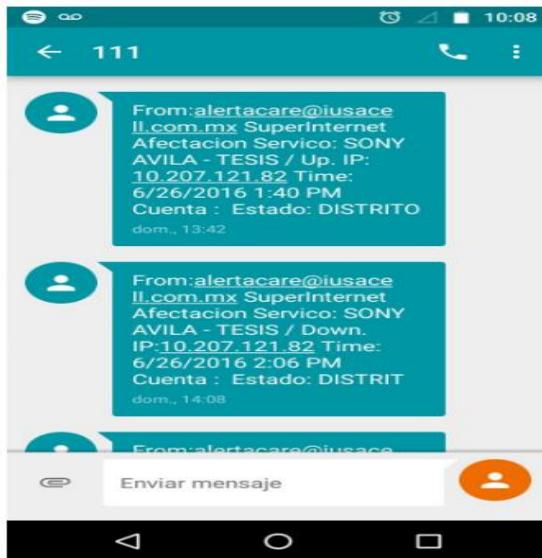


Figura 75 Captura de pantalla de los SMS que llegan al celular

El correo de Gmail se tiene configurado en el celular y se observa que también llegó la alerta, estas pruebas fueron realizadas el día 26 de junio aproximadamente a la 13:30 horas.

En las dos imágenes 73 y 74 podemos observar la hora y fecha de la llegada de la alarma  
En la figura 74 se observa que manda la alerta de cuando se reconectaron los servicios.  
Se observa el mensaje de UP y Down ya que se hicieron varias desconexiones en los equipos para comprobar el correcto funcionamiento.



Figura 76 Captura de Pantalla de la llegada del mensaje en correo Gmail

También se agrega imagen de la llegada del correo desde una computadora

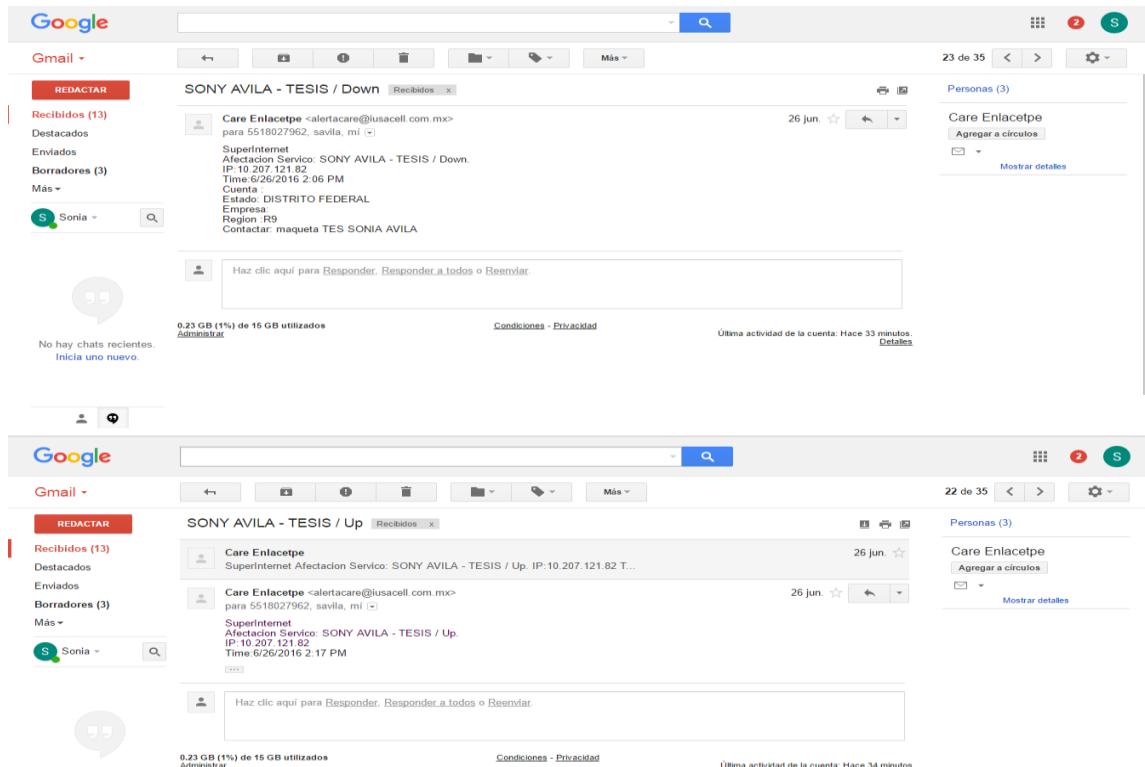


Figura 77 Alertas que envía el Sistema de Monitoreo al correo de Gmail visto desde una computadora

Se anexan las graficas que se obtuvieron durante las pruebas. La maqueta se dejó graficando durante algunos días para observar el comportamiento estos fueron los resultados.

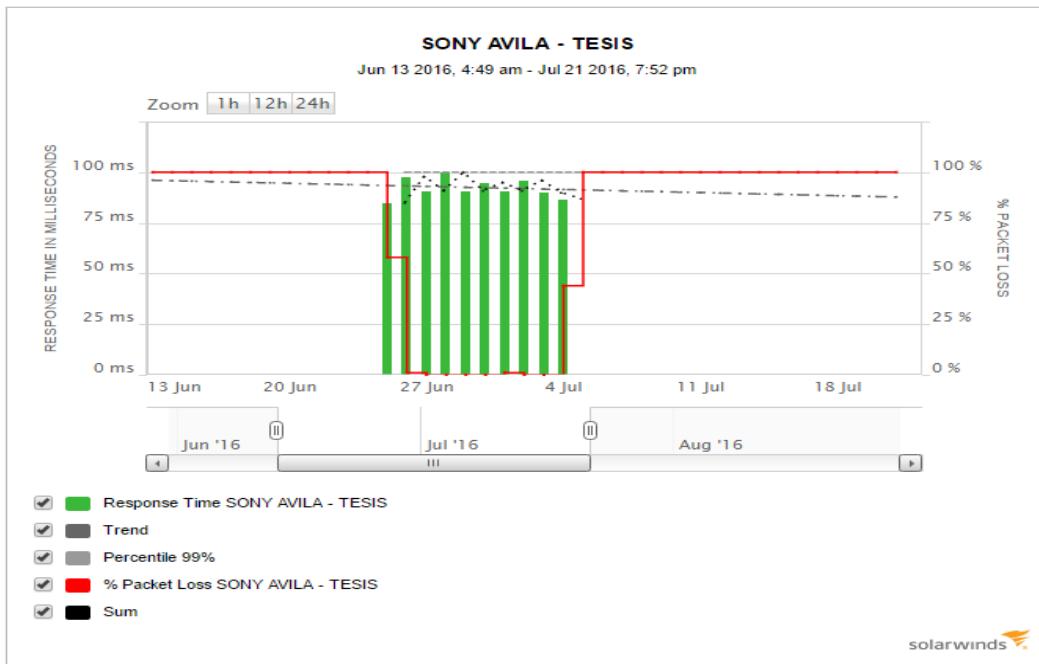
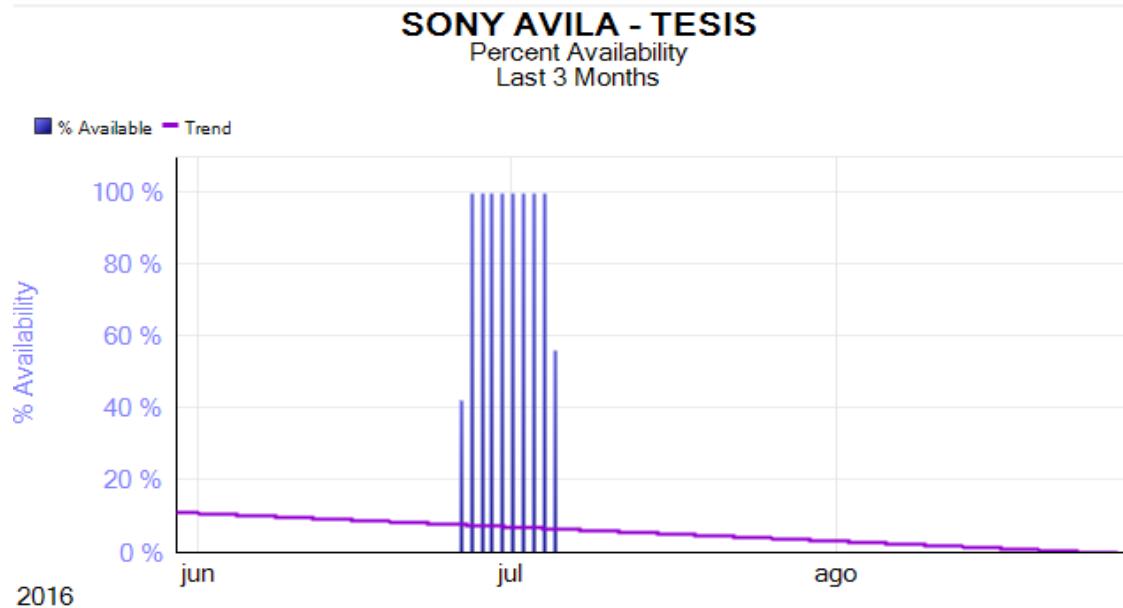


Figura 78 a) Gráfica de Latencia y Pérdida de Paquetes durante 7 días



SolarWinds Orion Core Services 2014.2.1

Figura 78 b) Gráfica de Disponibilidad durante 7 días

#### **4.5 Diseño de Red de Fibra óptica en nueva ubicación**

Se terminan las pruebas con el router Cisco, se configuró otra maqueta de prueba debido a que la que se tenía tuvo que ser removida está se colocó en otra ubicación.

Esta red se implementó desde cero debido a que no se contaba con un servicio de fibra óptica.

Se realizó la factibilidad para la nueva Red donde se entregara también por fibra óptica



Figura 79 Edificio donde se realizó maqueta para hacer pruebas.

En esta ubicación se realizó la nueva maqueta de prueba



Figura 80 Caja de derivación de fibra óptica de donde dependerá el servicio.



Figura 81 Fibra de 12 hilos con roseta existentes en el interior vertical del sótano



Figura 82 Trayectoria de fibra saldrá de la roseta y se colocará en la escalerilla vertical encinchada y etiquetada.



Figura 83 vertical en el piso donde se ubicará la maqueta



Figura 84 Punto donde llega la fibra y de ahí se tendrá que realizar el tendido del cuarto de comunicaciones



Figura 85 Trayectoria que se siguió para colocar la fibra óptica



Figura 86 Este es el punto donde se realizó la instalación y donde va a estar la maqueta para realizar las pruebas

Se anexa la lista de los materiales utilizados

80 mts. de Bifibra.

5 mts. de tubería de  $\frac{3}{4}$  pared delgada.

1 roseta residencial.

1 jumper.

Equipamiento a instalar.

30 etiquetas autoenrrollables.

50 cinchos de 30 cms.

#### 4.6 Configuración y pruebas con equipo router Huawei AR 1220

En paralelo a la instalación de fibra óptica se inicia con la configuración del equipo AR. Se optó por realizar las pruebas con otro equipo router este nuevo equipo que se eligió fue un router Huawei 1220. Este router tiene ciertas características las cuales resultaron favorables para llevar a cabo las pruebas, una de ellas es que ya tiene integrado un puerto óptico con esto se eliminó un dispositivo que fue la ONT ya que tuvimos la posibilidad de conectarlo directamente a la fibra óptica.

El AR1200 utiliza la estructura CPU de múltiples núcleos y conmutación no bloqueante. Además, sus niveles de rendimiento del sistema son líderes en la industria, lo que permite cumplir con los requerimientos de extensión de la red y desarrollo de servicios.



Figura 87 Router AR 1220 conectado a la PC para configuración

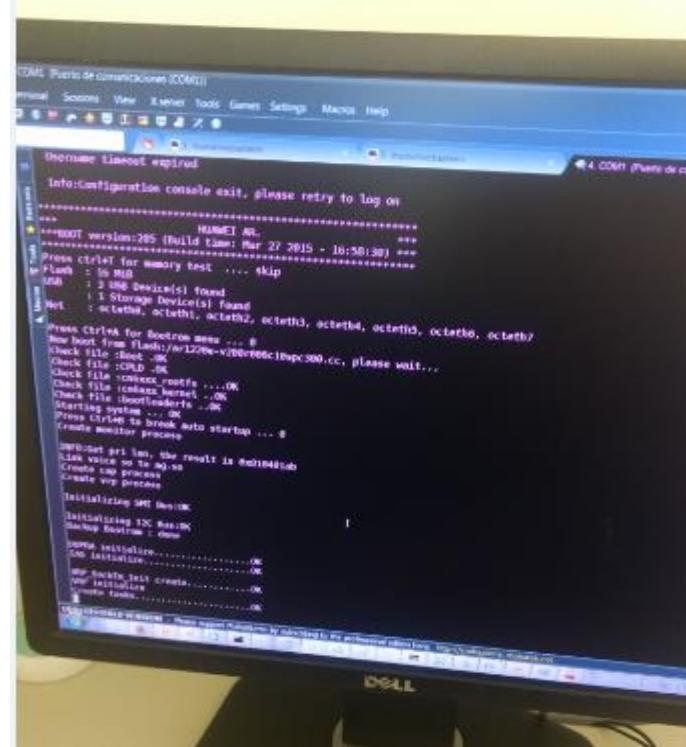


Figura 88 Pantalla para configuración de Router Huawei 1220 en MobaXterm

Se realiza la configuración del equipo router con salida a internet las IP's fueron las siguientes

IP DE GESTIÓN 10.253.25.212 (Está IP se pondrá en monitoreo)

255.255.252.0

GW 10.253.25.0

IP PÚBLICA 187.188.106.7

GW 187.188.106.1

MASCARA 255.255.255.0

Se realiza la configuración de las VLAN de servicio, se descanalizan en cada una de las interfaces.

Se asignan las IP's y se conecta el AR con el jumper de fibra óptica de la siguiente manera.



Figura 89 Equipo router AR 1220 conectado a la fibra óptica y ya encendido.

Se tiene alcanzable el equipo a través de la IP de gestión se accesa al equipo router y mediante telnet.

```

<TESIS SONIA>dis ip int br
*down: administratively down
^down: standby
<1>: loopback
<s>: spoofing
<CE>: E-Trunk down
The number of interface that is UP in Physical is 5
The number of interface that is DOWN in Physical is 7
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 9

Interface                                IP Address/Mask    Physical   Protocol
Cellular0/0/0                            unassigned        down      down
Cellular0/0/1                            unassigned        down      down
GigabitEthernet0/0/8                      unassigned        down      down
GigabitEthernet0/0/9                      unassigned        down      down
GigabitEthernet0/0/9.1824                 unassigned        down      down
GigabitEthernet0/0/10                     unassigned        down      down
NULL0                                     unassigned        up       up<s>
Pon2/0/0                                 unassigned        up       down
Pon2/0/0.1824                           187.188.106.7/24 up       up
Pon2/0/0.1839                           10.253.25.212/22 up       up
Pon2/0/0.4095                           unassigned        up       down
Pon2/0/1                               unassigned        down      down

<TESIS SONIA>

```

Figura 90 Interfaces configuradas en el router ya con la IP asignada.

Se realizan pruebas de internet hacia los DNS públicos de Google para comprobar que se tenían alcanzables. No se tenía salida a Internet.

```

C:\Users\zonia>tracert 187.188.106.7
Traza a la dirección fixed-188-106-187-188-106-7.iusacell.net [187.188.106.7]
sobre un máximo de 30 saltos:
  1  718 ms    1 ms    2 ms  192.168.1.254
  2  91 ms    94 ms   42 ms  dsl-servicio-1200.uninet.net.mx [200.38.193.226]
  3  54 ms    49 ms   65 ms  reg-mex-vallejo-102-hge0-7-0-2.uninet.net.mx [18
9.246.5.201]
  4  25 ms    24 ms   22 ms  dsl-189-247-253-105-dyn.prod-infinitum.com.mx [1
89.247.253.105]
  5  *          *          *          Tiempo de espera agotado para esta solicitud.
  6  92 ms    82 ms   102 ms  fixed-188-106-187-188-106-1.iusacell.net [187.18
8.106.1]
  7  *          *          *          Tiempo de espera agotado para esta solicitud.
  8  *          *          *          Tiempo de espera agotado para esta solicitud.
  9  *          *          *          Tiempo de espera agotado para esta solicitud.
  10 *          *          *          Tiempo de espera agotado para esta solicitud.
  11 *          *          *          Tiempo de espera agotado para esta solicitud.
  12 *          *          *          Tiempo de espera agotado para esta solicitud.
  13 *          *          *          Tiempo de espera agotado para esta solicitud.
  14 *          *          *          Tiempo de espera agotado para esta solicitud.
  15 *          *          *          Tiempo de espera agotado para esta solicitud.
  16 *          *          *          Tiempo de espera agotado para esta solicitud.
  17 *          *          *          Tiempo de espera agotado para esta solicitud.
  18 *          *          *          Tiempo de espera agotado para esta solicitud.
  19 *          *          *          Tiempo de espera agotado para esta solicitud.
  20 *          *          *          Tiempo de espera agotado para esta solicitud.
  21 *          *          *          Tiempo de espera agotado para esta solicitud.
  22 *          *          *          Tiempo de espera agotado para esta solicitud.
  23 *          *          *          Tiempo de espera agotado para esta solicitud.
  24 *          *          *          Tiempo de espera agotado para esta solicitud.
  25 *          *          *          Tiempo de espera agotado para esta solicitud.
  26 *          *          *          Tiempo de espera agotado para esta solicitud.
  27 *          *          *          Tiempo de espera agotado para esta solicitud.
  28 *          *          *          Tiempo de espera agotado para esta solicitud.
  29 *          *          *          Tiempo de espera agotado para esta solicitud.
  30 *          *          *          Tiempo de espera agotado para esta solicitud.

Traza completa.
C:\Users\zonia>

```

Figura 91 No se lograba salida a internet se realiza un trazado para detectar donde se estaba quedando la IP pública se observa que se queda en el Gateway de la IP pública.

Esto nos indica que todo el medio y ruteo se encuentra de forma correcta por lo que la falla está en la configuración del router.

Se realiza un cambio de configuración en las interfaces. Se vuelve a accesar al equipo AR. Y se realiza ping hacia internet.

```
<TESIS SONIA>
<TESIS SONIA>ping -a 187.188.106.7 4.2.2.2
  PING 4.2.2.2: 56 data bytes, press CTRL_C to break
    Reply from 4.2.2.2: bytes=56 Sequence=1 ttl=56 time=29 ms
    Reply from 4.2.2.2: bytes=56 Sequence=2 ttl=56 time=28 ms
    Reply from 4.2.2.2: bytes=56 Sequence=3 ttl=56 time=29 ms
    Reply from 4.2.2.2: bytes=56 Sequence=4 ttl=56 time=28 ms
    Reply from 4.2.2.2: bytes=56 Sequence=5 ttl=56 time=28 ms

  --- 4.2.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 28/28/29 ms
```

Figura 92 Ping hacia los DNS de Google alcanzando con exito

```
<TESIS SONIA>tracer -a 187.188.106.7 4.2.2.2
traceroute to 4.2.2.2(4.2.2.2), max hops: 30 ,packet length: 40,press CTRL_C to break
  1 187.188.106.1 2 ms  1 ms  2 ms
  2 10.180.59.70 7 ms  3 ms  2 ms
  3 10.180.59.71 2 ms  3 ms  3 ms
  4 38.104.248.153 3 ms  2 ms  3 ms
  5 154.24.23.25 17 ms 154.54.41.130 16 ms  16 ms
  6 154.54.47.45 25 ms 154.54.47.33 25 ms 154.54.47.45 25 ms
  7 154.54.41.66 31 ms 33 ms 154.54.44.230 29 ms
  8 154.54.28.74 29 ms 154.54.47.214 31 ms 32 ms
  9 * * *
 10 4.69.209.1 31 ms 4.69.209.5 29 ms 4.69.209.1 30 ms
 11 4.2.2.2 29 ms 30 ms 30 ms
<TESIS SONIA>
```

Figura 93 Trazado de la IP Publica hacia los DNS

Se comprueba que la Ip ya es alcanzable desde internet, con esto se comprueba que el equipo es alcanzable desde la nube

```
C:\Users\zonia>ping 187.188.106.7

Haciendo ping a 187.188.106.7 con 32 bytes de datos:
Respuesta desde 187.188.106.7: bytes=32 tiempo=52ms TTL=249
Respuesta desde 187.188.106.7: bytes=32 tiempo=23ms TTL=249
Respuesta desde 187.188.106.7: bytes=32 tiempo=33ms TTL=249
Respuesta desde 187.188.106.7: bytes=32 tiempo=58ms TTL=249

Estadísticas de ping para 187.188.106.7:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 23ms, Máximo = 58ms, Media = 41ms

C:\Users\zonia>
```

Figura 94 Ping hacia la IP pública desde un servicio de Internet

```
C:\Users\zonia>tracert 187.188.106.7
Traza a la dirección fixed-188-106-187-188-106-7.iusacell.net [187.188.106.7]
sobre un máximo de 30 saltos:
  1      2 ms      2 ms      3 ms  192.168.1.254
  2     88 ms     93 ms     92 ms  dsl-servicio-1200.uninet.net.mx [200.38.193.226]
  3     38 ms     26 ms     30 ms  reg-mex-vallejo-102-hge0-7-0-2.uninet.net.mx [18
9.246.5.201]
  4     23 ms     24 ms     23 ms  dsl-189-247-253-105-dyn.prod-infinitum.com.mx [1
89.247.253.105]
  5     *         *         *      Tiempo de espera agotado para esta solicitud.
  6     69 ms     25 ms     24 ms  fixed-188-106-187-188-106-1.iusacell.net [187.18
8.106.1]
  7     55 ms     55 ms     58 ms  fixed-188-106-187-188-106-7.iusacell.net [187.18
8.106.7]

Traza completa.

C:\Users\zonia>
```

Figura 95 Trazado hacia la IP pública desde un servicio de Internet.

Se configuró el equipo router con salida a internet se realiza configuración del SNMP, para poder monitorearlo mediante la aplicación Solarwinds.

Se dio de alta en monitoreo con la IP de gestión 10.253.25.212

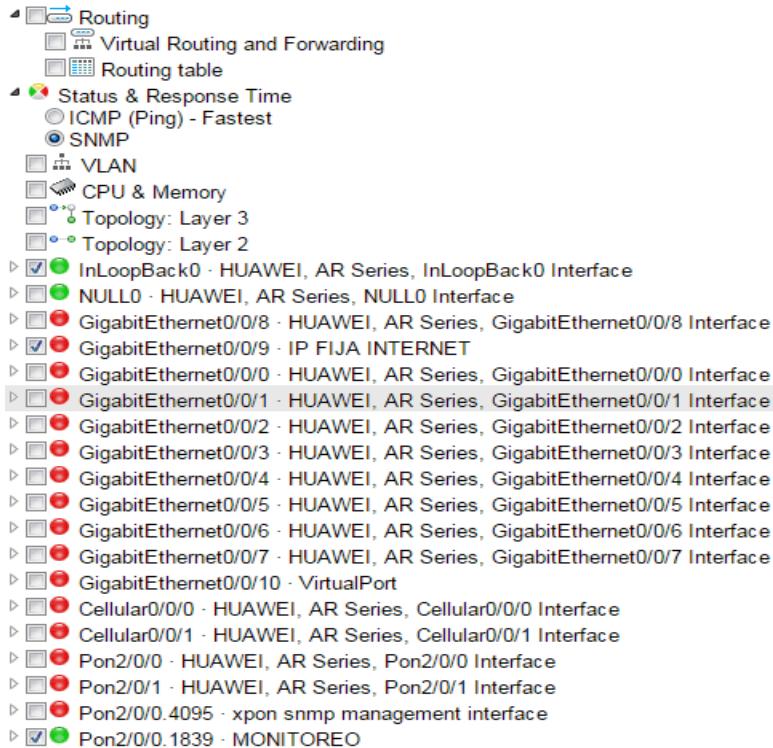


Figura 96 Interfaces que nos arroja el Sistema de Monitoreo para ser monitoreadas de las cuales sólo se eligieron las que están en uso

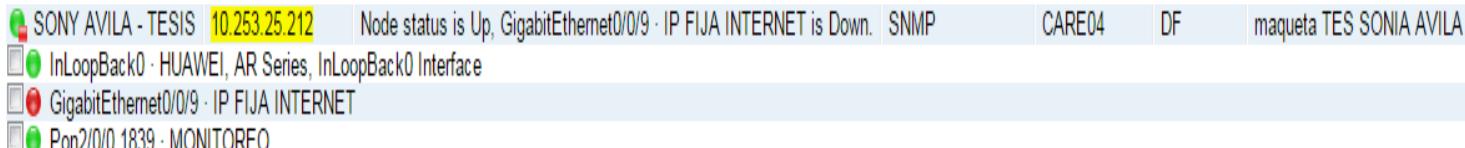


Figura 97 Equipo Router Huawei dado de alta en el sistema de monitoreo con la IP de gestión 10.253.25.212.

En la figura 96 observamos las interfaces que se eligieron para ser monitoreadas, las que tienen un círculo verde es por que se encuentran en estado up. En este caso la IP fija se encuentra en rojo debido a que no hay nada conectado en el equipo.

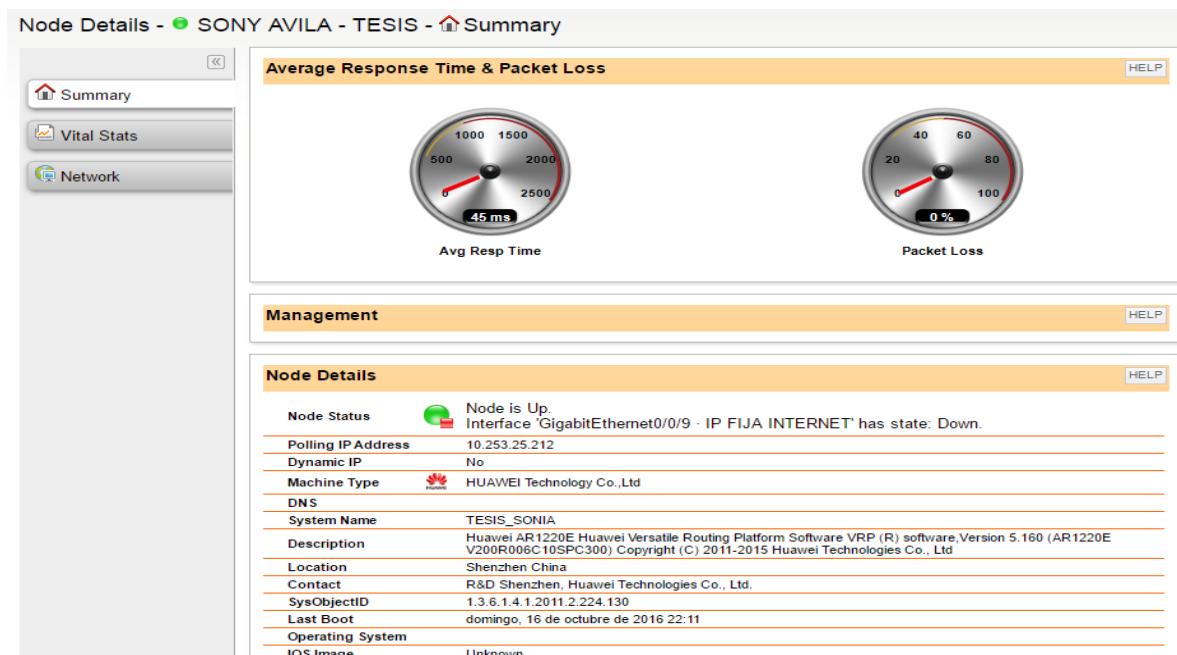


Figura 98 Equipo Ar Huawei 1220 en la vista de Monitoreo Solawinds.

En esta imagen podemos observar que el nodo ya está dado de alta en el sistema se observa un recuadro rojo en el node is up es la interfaz que se comentó anteriormente que no tiene nada conectado.

Se anexan las gráficas de monitoreo del Sistema, la gráfica de barras verdes muestra el tiempo que está tardando en responder el equipo podemos ver la fecha y tiempo en ms. El equipo tiene tiempos entre 40 y 45 ms por lo que podemos deducir que el enlace se encuentra saludable.

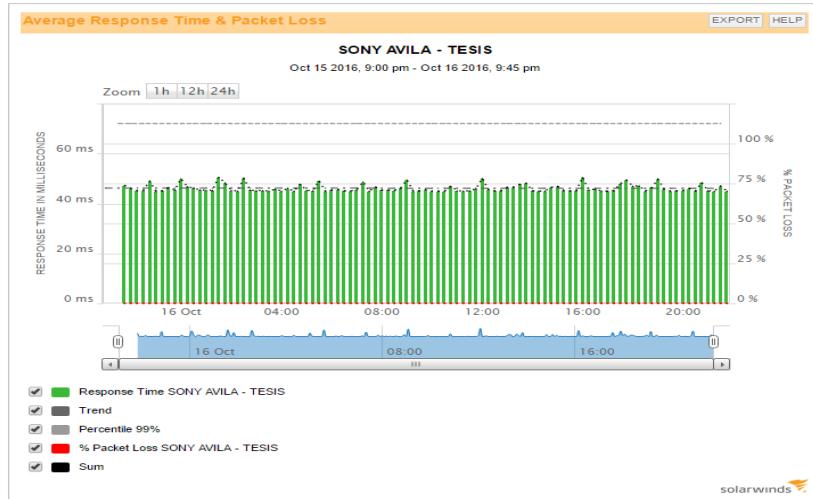


Figura 99 Gráfica de Latencia y pérdida de Paquetes

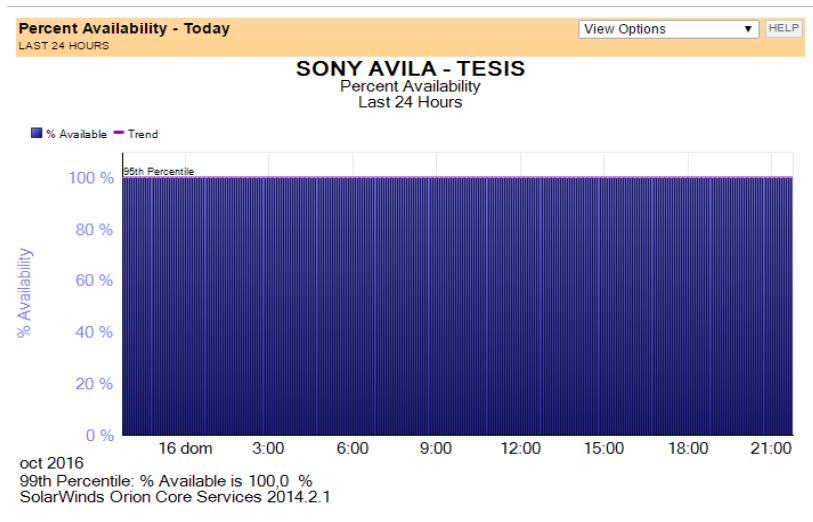


Figura 100 Gráfica de Disponibilidad, se observa que el enlace no ha tenido ninguna caída se encuentra operando de manera óptima.

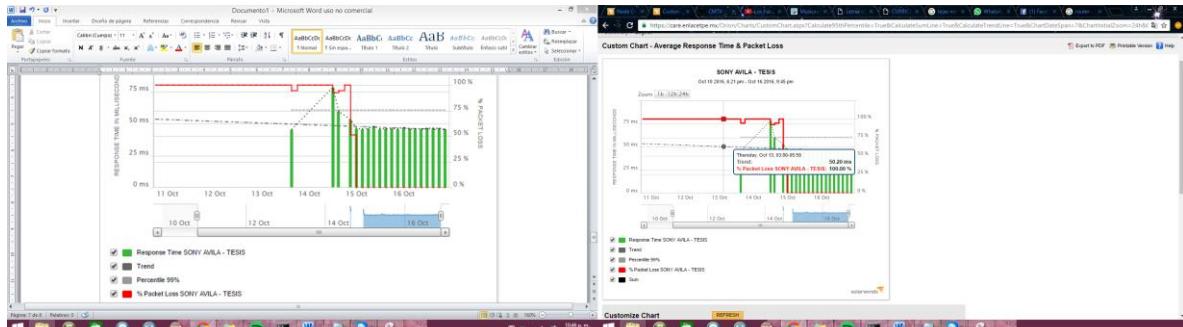


Figura 101 Gráfica de latencia y pérdida de paquetes cuando se estaban realizando las pruebas se observan conexión y desconexión de los equipos.

Se realiza configuración correspondiente tanto en el Sistema de Monitoreo para que se envíen las alertas al correo y en el correo de LOTUS PARA que se envíen vía SMS

Se realizan pruebas de conexión y conexión del equipo

17/11/2016 06:46 a.m.	Care Enlacetpe	SONY AVILA - TESIS / Up	3K
28/10/2016 05:21 p.m.	Care Enlacetpe	SONY AVILA - TESIS / Down	3K
28/10/2016 02:33 p.m.	Care Enlacetpe	SONY AVILA - TESIS / Up	3K
28/10/2016 02:19 p.m.	Care Enlacetpe	SONY AVILA - TESIS / Down	3K
13/10/2016 05:38 p.m.	Care Enlacetpe	SONY AVILA - TESIS / Down	3K

Figura 102 Alertas enviadas al correo de LOTUS durante las pruebas

En las siguientes figuras podemos observar las 3 alertas que llegarán estás pruebas fueron realizadas el día 13 de octubre. Se anexa la alerta que llega al correo de Lotus, Gmail y la alerta al celular.

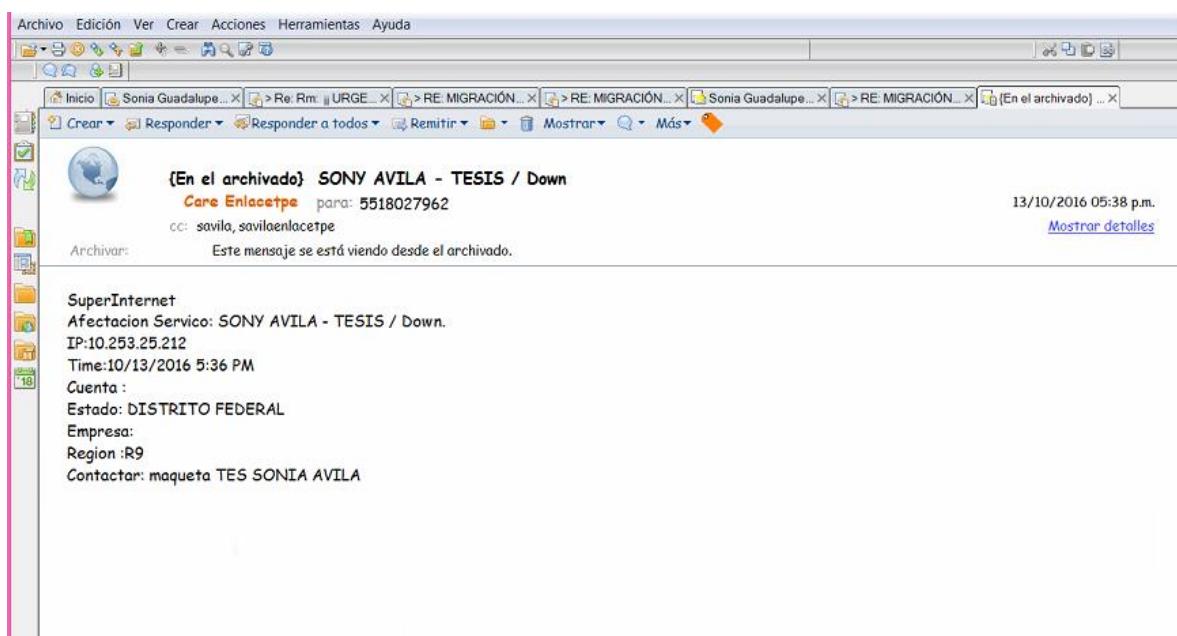


Figura 103 Alertas enviadas al correo de LOTUS durante las pruebas

SONY AVILA - TESIS / Down Recibidos x

Care Enlacetpe <alertacare@iusacell.com.mx> para 5518027962, savila, mí ▾ 13 oct. ⭐ ↻ ⌂

SuperInternet  
Afectacion Servicio: SONY AVILA - TESIS / Down.  
IP:10.253.25.212  
Time:10/13/2016 5:36 PM  
Cuenta :  
Estado: DISTRITO FEDERAL  
Empresa:  
Region :R9  
Contactar: maqueta TES SONIA AVILA

Haz clic aquí para [Responder](#), [Responder a todos](#) o [Reenviar](#).

0.23 GB (1%) de 15 GB utilizados [Administrar](#) [Condiciones - Privacidad](#) Última actividad de la cuenta: Hace 7 días. [Detalles](#)

Figura 104 Alertas enviadas al correo GMAIL durante las pruebas

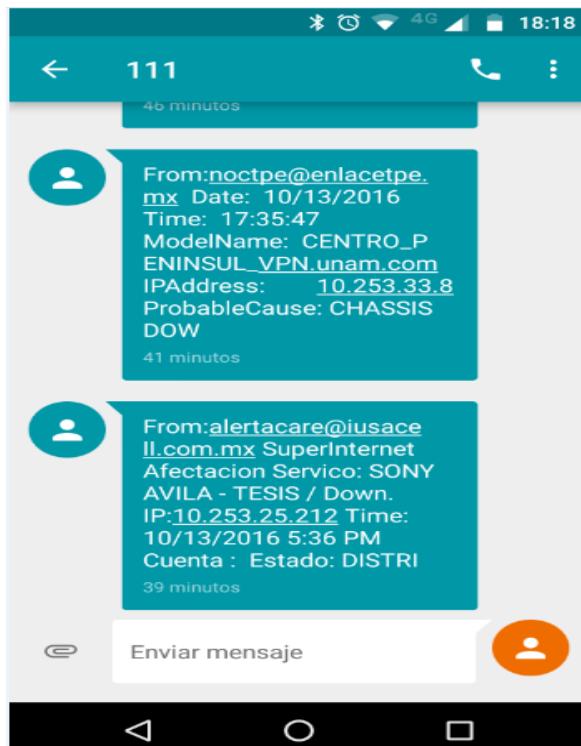


Figura 105 Alertas enviadas vía SMS durante las pruebas

## **CONCLUSIONES**

Este proyecto surge por la necesidad de tener un Monitoreo de Redes Confiable utilizando los recursos con los que se contaban en la Empresa. Monitorizar los servicios de la Red a nivel Protocolo SNMP, nos dará oportunidad de actuar de forma proactiva. Unificando varios elementos tales como el Sistema de Monitoreo Solarwinds con el envío de mensajes SMS mediante el servidor con un Modem externo que se ocupaba para otro fin. Se logra obtener un Sistema de Alertas que beneficiaría tanto al proveedor de Internet y al cliente. Los datos que logremos obtener con el proceso de monitorización son importantes ya que ayuda a los administradores de Red a tomar decisiones sobre los problemas que se presenten.

Al realizar las pruebas con los equipos físicos se presentaron varios detalles los cuáles nos obligaron a cambiar equipamiento y volver a configurar. Sin embargo ello nos permite concluir que no importa la marca de router que se utilice para proporcionar el servicio y poder monitorearlo, siempre que pueda ser gestionable mediante el protocolo SNMP.

Se realizan pruebas con otro equipo router debido a que la maqueta que se configuró tuvo que ser removida de la ubicación con esto se obtuvo experiencia en la configuración de los dos equipos y se realizó la maqueta en dos dispositivos diferentes para comprobar que es funcional en cualquier dispositivo y se puede observar el desempeño que tiene.

Gran parte de los conocimientos adquiridos en la carrera de Ingeniería en Comunicaciones y Electrónica fueron fundamentales para la elaboración de esta tesis ya que con base en estos se logró entender el funcionamiento básico de una red.

Finalmente concluimos y se logran concretar los objetivos propuestos, superando las expectativas ya que únicamente se había planteado hacer la maqueta con un equipo. Además de comprobar que es de gran ayuda el envío de alertas por los medios propuestos.

Esto es de suma importancia ya que podemos agilizar la solución antes de que el problema sea grave observando las gráficas de monitoreo podemos deducir la salud del enlace y revisar que es lo que está sucediendo evitando así la interrupción de los servicios.

Podríamos decir que hay dos fases en esta maqueta ya que antes de que se caiga el servicio con las gráficas podemos detectar si algo está fallando. Aquí el nivel de criticidad

sería medio y cuando el enlace cae completamente es grave pero podemos actuar de forma rápida con las alertas enviadas.

Se presentaron problemas en la maqueta debido a los falsos positivos que enviaba el sistema ya que algunas alarmas se disparaban por ventanas de mantenimiento programadas, o sucedió un día que el Servidor donde se alojaba la aplicación Solarwinds sufrió un percance y perdimos el monitoreo de los equipos. Por lo que también podemos concluir que este sistema es un 90% confiable por estos dos incidentes que se presentaron, esto se probó en dos escenarios diferentes.

## REFERENCIAS

- Diego Marcos Jorquera, Francisco Maciá Pérez y Juan Antonio Gil Martínez-Abarca “Modelo de gestión de red basado en sistema multiagente. Aplicación a la regeneración de nodos” <http://www.dtic.ua.es/grupoM/recursos/articulos/JDARE-06-I.pdf>  
Consultado 05/04/2015
- SNMPc Enterprise (2014 )<https://www.castlerock.com/products/snmpc/>  
Consultado 05/04/2015
- Facundo Velurtas “Optimización De Enlaces En Redes Ip. Control De Tráfico” [http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes\\_de\\_Datos/Tesis/Velurtas\\_Facundo.pdf](http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Velurtas_Facundo.pdf)  
Consultado 05/04/2015
- Sergio Daniel Cayuqueo “Monitoria y análisis de Red con Nagios” <http://cayu.com.ar/files/manuales-nagios.pdf>  
Consultado 06/04/2016
- **Luis Fernando Mejia Herrera “;Qué es Gestión y Monitoreo de Red?”** <http://servidorespararedes.blogspot.mx/2009/01/que-es-aplicaciones-web.html>  
Consultado 08/04/2015
- Sistema de Monitoreo Solarwinds <http://www.solarwinds.com/es/>  
Consultado 10/04/2015
- Análisis Estadístico del Tráfico de Red para la Detección de Anomalías y la Calidad de Servicio (2013) Pedro Casas Hernández [https://iie.fing.edu.uy/publicaciones/2013/Cas13/tesis\\_CASAS\\_udelar.pdf](https://iie.fing.edu.uy/publicaciones/2013/Cas13/tesis_CASAS_udelar.pdf)  
Consultado 12/04/2015
- “Sistema de Gestión de Diseño para el Core de una Red GPRS (2008) “Universidad de Chile <http://www.tesis.uchile.cl/handle/2250/104952>  
Consultado 13/04/2015
- Revisión de criterios y metodologías de diseño de redes para el monitoreo de la calidad del agua en ríos Universidad Nacional de Colombia (2008) <http://www.redalyc.org/articulo.oa?id=145012856006>
- Consultado 18/04/2015
- DIRECCIÓN IP <http://es.kioskea.net/contents/267-direccion-ip>

- Consultado 20/04/2015
- 
- ¿Cuál es mi IP? <http://www.rankia.com/blog/adsl/2252785-cual-ip>  
Consultado 20/04/2015
- “Diseño de la red del centro - Direcciones IP  
<http://recursostic.educacion.es/observatorio/web/ca/component/content/article/453-diseno-de-la-red-del-centro?start=2>  
Consultado 22/04/2015
- SolarWinds Orion Network Configuration Manager Evaluation Guide  
[http://www.solarwinds.com/documentation/orionNCM/Docs/translations/EGs/ES/OrionNCMEvaluationGuide\\_ES.pdf](http://www.solarwinds.com/documentation/orionNCM/Docs/translations/EGs/ES/OrionNCMEvaluationGuide_ES.pdf)  
Consultado 26/04/2015
- Christian Feliu Mendieta “Sistema de Gestión de Diseño para el Core de una Red GPRS”  
<http://www.tesis.uchile.cl/handle/2250/104952>  
Consultado 01/05/2016
- “Sistema de Información Científica Redalyc Red de Revistas Científicas de América Latina y el Caribe, España y Portugal” Revisión de criterios y metodologías de diseño  
de redes para el monitoreo de la calidad del agua en ríos  
<http://www.redalyc.org/articulo.oa?id=145012856006>  
Consultado 03/05/2016
- “Metodologías, Modelación Y Aplicación Para Fines De Regulación Tarifaria” Oficina de Desarrollo de las Telecomunicaciones 2008  
[https://www.itu.int/ITUD/finance/Studies/Efficient%20operator/Empresa\\_Eficiente\\_fi\\_nal\\_sp.pdf](https://www.itu.int/ITUD/finance/Studies/Efficient%20operator/Empresa_Eficiente_fi_nal_sp.pdf)  
Consultado 04/05/2016
- Universidad Tecnológica de la Mixteca (UTM ”El Router Cisco“)  
<http://mixteco.utm.mx/~resdi/historial/materias/router.pdf>  
Consultado 07/05/2016

- Configuración básica del router usando el Cisco Configuration Professional

[Configuración básica del router usando el Cisco Configuration Professional](#)

[http://www.cisco.com/cisco/web/support/LA/109/1090/1090651\\_basic-router-config-ccp-00.pdf](http://www.cisco.com/cisco/web/support/LA/109/1090/1090651_basic-router-config-ccp-00.pdf)

Consultado 08/05/2016

- [http://infolib2.lotus.com/resources/domino/traveler/8.5.2/doc/ta852abd001/es\\_No\\_tesTraveler.html](http://infolib2.lotus.com/resources/domino/traveler/8.5.2/doc/ta852abd001/es_No_tesTraveler.html)

Consultado 09/05/2016

## APENDICES

### Cisco 2900 Series Integrated Services Routers Data Sheet

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings. The Integrated Services Routers Generation 2 platforms are future-enabled with multi-core CPUs, support for high capacity DSPs (Digital Signal Processors) for future enhanced video capabilities, high powered service modules with improved availability, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS® Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation which can quickly adapt to evolving network requirements. Overall, the Cisco 2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market leading security, unified communications, wireless, and application services.

Figure 1. Cisco 2900 Series Integrated Services Routers



#### Product Overview

Cisco 2900 Series builds on the best-in-class offering of the existing Cisco 2800 Series Integrated Services Routers by offering four platforms (Figure 1): the Cisco 2901, 2911, 2921, and 2951 Integrated Services Routers.

All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice- and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platforms support the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper and fiber GE.

#### Key Business Benefits

The Integrated Services Routers Generation 2 (ISR G2) provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 2900 Series.

Table 1. Key Business Benefits of the Cisco 2900 Series Integrated Services Routers

Benefits	Description
Services Integration	The Cisco 2900 Series ISRs offer increased levels of services integration with voice, video, security, wireless, mobility, and data services, enabling greater efficiencies and cost savings.
Services On Demand	A single Cisco IOS® Software Universal image is installed on each ISR G2. The Universal image contains all of the Cisco IOS technology sets which can be activated with a software license. This allows your business to quickly deploy advanced features without downloading a new IOS image. Additionally, larger default memory is included to support the new capabilities. The Cisco Services Ready Engine (SRE) enables a new operational model which allows you to reduce capital expenditures (CapEx) and deploy a variety of application services as needed on a single integrated compute services module.

High Performance with Integrated Services	The Cisco 2900 Series enables deployment in high speed WAN environments with concurrent services enabled up to 75 Mbps. A multigigabit fabric (MGF) enables high-bandwidth module-to-module communication without compromising routing performance.
Network Agility	Designed to address customer business requirements, the Cisco 2900 Series modular architecture offers increased capacity and performance as your network needs grow. Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy Efficiency	The Cisco 2900 Series architecture provides energy-saving features that include the following: The Cisco 2900 Series offers intelligent power management and allows the customer to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future. Services integration and modularity on a single platform performing multiple functions, optimizes raw materials consumption and energy usage. Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the total cost of ownership, including materials and energy use. High efficiency power supplies are provided with each platform.
Investment Protection	The Cisco 2900 Series maximizes investment protection: Reuse of a broad array of existing modules supported on the original Integrated Services Routers provides a lower cost of ownership. A rich set of Cisco IOS Software features carried forward from the original Integrated Services Routers and delivered in a single universal image. Flexibility to adapt as your business needs evolve.

#### Platform Architecture and Modularity

The Cisco 2900 Series is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 2900 Series.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular Platform	The Cisco 2900 Series ISRs are highly modular platforms with several types of module slots to add connectivity and services for varied branch-office network requirements. The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades for future technologies without requiring a platform replacement.
Processors	The Cisco 2900 Series are powered by high-performance multi-core processors that can support the growing demands of high-speed WAN connections to the branch-office while also running multiple concurrent services.
Embedded IP Security (IPSec) VPN Hardware Acceleration	Embedded hardware encryption acceleration is enhanced to provide higher scalability, which combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (IPSec acceleration). The onboard encryption hardware replaces and outperforms the advanced integration modules (AIMs) of previous generations.

Architectural Feature	Benefits
Multigigabit Fabric (MGF)	The Cisco 2900 Series introduces an innovative multigigabit fabric (MGF) that allows for efficient module-to-module communication, enabling tighter services interactions across modules while reducing the overhead on the route processor.
TDM Interconnectivity Fabric	Unified communications services in the branch office are significantly enhanced with the use of a TDM interconnectivity fabric in the system architecture, allowing for scaling of DS-0 channel capacity.
Integrated Gigabit Ethernet Ports	All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports. One of the three 10/100/1000 Ethernet WAN ports on the Cisco 2921 and 2951 supports Small Form-Factor Pluggable (SFP)-based connectivity in lieu of a RJ-45 port and enabling fiber connectivity.
Innovative Universal-Serial-Bus (USB)-Based Console Access	A new, innovative USB console port offers management connectivity for devices without a serial port such as modern laptop computers. Traditional console and auxiliary ports are also available.
Optional Integrated Power Supply for Distribution of PoE and Universal DC Power Supply	An optional upgrade to the internal power supply provides inline power (802.3af-compliant PoE and Cisco Inline Power) to integrated switch modules. On the Cisco 2911, 2921, and 2951, an optional DC power supply is available that extends deployment into central offices and industrial environments. On the Cisco 2911, an optional DC-PoE power supply is available.
Optional External Redundant Power Supply (RPS)	The Cisco 2911, 2921, and 2951 allow for power redundancy through the use of an external RPS device, thereby decreasing network downtime and protecting the network from power-supply failures. Redundant power on the Cisco 2900 Series is supported through the Cisco RPS 2300 Redundant Power System. You can use the Cisco RPS 2300 to provide redundant power for Cisco 2900 Series ISRs as well as Cisco Catalyst® switches. In order to use the Cisco RPS 2300, an external RPS adapter is required (configurable option) to connect the platform to the external RPS.
PoE Boost	When connected to an external RPS device, the Cisco 2911, 2921, and 2951 can operate in a PoE boost configuration in lieu of redundant power mode - whereby the power capacity of the platform is increased to twice the normal level to power additional PoE ports.
Designed for Flexible Deployments	The Cisco 2911 and 2951 are designed for NEBS environments. The 2911 is 12" deep and has an optional fan filter for deployments in a variety of environments. An assembly that provides front-to-back airflow is also available for 23" racks.

#### Modularity Features and Benefits

The Cisco 2900 Series provides significantly enhanced modular capabilities (refer to Table 3) offering investment protection for customers. Most of the modules available on previous generations of Cisco routers, such as the Cisco 2800 Series, are supported on the Cisco 2900 Series. Additionally, modules can be used on other supported Cisco platforms to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

A complete list of supported modules, including a list of supported SFPs for the Cisco 2900 Series, is available at: <http://www.cisco.com/go/2900>.

Table 3. Modularity Features and Benefits

ISR Modules	Benefits
<p>Cisco Service Module</p> 	<p>Each service module slot offers high-data-throughput capability: Up to 4 Gbps aggregate toward the route processor. Up to 2 Gbps aggregate to other module slots over MGF. Service module (SM) slots are highly flexible with support for double-wide service modules (SM-Ds), which are Service Modules that require two SM slots. SM-Ds in the Cisco 2921 and 2951 provide flexibility for higher-density modules. A service module slot replaces the network module and the extension module for voice/fax (EVM) slots and is offered on Cisco 2911, 2921, and 2951 ISRs. An adapter module enables backward compatibility with existing network modules, enhanced network modules (NMEs), and EVMs. Service module slots provide twice the power capabilities relative to the network-module slots, allowing for flexibility for higher-scale and better-performance modules. Power to service module slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.</p>
<p>Cisco Enhanced High-Speed WAN Interface Card (EHWIC)</p> 	<p>The EHWIC slot provides enhancements to the prior generation's high-speed WAN interface card (HWIC) slots while providing maximum investment protection by natively supporting HWICs, WAN interface cards (WICs), voice interface cards (VICs), and voice/WAN interface cards (VWICs). Four integrated EHWIC slots on the Cisco 2901, 2911, 2921, and 2951 allow for more flexible configurations. Each HWIC slot offers high-data-throughput capability: Up to 1.6 Gbps aggregate toward the route processor. Up to 2 Gbps aggregate to other module slots over the MGF. Flexibility to support double-wide modules is enabled by combining two EHWIC slots. Up to 2 doublewide HWIC (HWIC-D) modules are supported.</p>
<p>Cisco Internal Services Module (ISM)</p> 	<p>A single ISM slot provides flexibility to integrate intelligent service modules on an internal slot within the chassis Each ISM slot offers high-data-throughput capability: Up to 4 Gbps aggregate toward the route processor. Up to 2 Gbps aggregate to other module slots over the MGF. The ISM replaces the AIM slot; existing AIM modules are not supported in the ISM slot. Power to ISM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.</p>
<p>Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3) Slots on Motherboard</p>	<p>PVDM3 slots natively support PVDM3 modules, providing support for richer density for rich-media voice and video. Each PVDM3 slot connects back to the system architecture through a 2 Gbps aggregate link through the MGF. Investment protection for PVDM2 modules is supported through an adapter module.</p>

ISR Modules	Benefits
	Power to the PVDM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Compact Flash Slots	Two external Compact Flash slots are available on the Cisco 2900 Series Integrated Services Routers. Each slot can support high-speed storage densities upgradeable to 4 GB in density.
USB 2.0 Ports	Two high-speed USB 2.0 ports are supported. The USB ports enable secure token capabilities and storage.

#### Cisco IOS Software

Cisco 2900 Series Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, the Integrated Services Routers Generation 2 platforms are supported on Cisco IOS Software releases 15M&T. Release 15.0(1)M is available immediately and provides support for a comprehensive portfolio of Cisco technologies, including the functionality and features delivered in releases 12.4 and 12.4T. New innovations in 15.0(1)M span multiple technology areas, including security, voice, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

#### Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all IOS technology feature sets is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Four major technology licenses are available on the Cisco 2900 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at <http://www.cisco.com/go/sa>. The four licenses are as follows:

- IP Base: This technology package is available as default.
- Data
- Unified Communications
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 2900 Series Integrated Services Routers, please visit <http://www.cisco.com/go/2900l>.

#### Key Branch-Office Services

The Cisco Integrated Services Routers are industry-leading platforms that offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with voice, video, security, mobility and application services. Businesses enjoy the benefit of deploying a single device that meets all their needs, reducing capital and operational expenses.

#### Unified Communications, Collaboration, and Voice-Gateway Services

The Cisco 2900 Integrated Services Router is the foundation for collaboration in the small and midsize branch office, serving as a critical component of a Cisco's video architecture (Medianet) and enterprise Unified Communications solution. With embedded voice services and a wide range of supported telephony interfaces, the Cisco 2900 Series delivers maximum deployment flexibility for the distributed enterprise. Unified communications is enabled through a rich signaling and media-processing infrastructure, including a variety of protocols, media interworking, signal and media security, transcoding, conferencing, and QoS. Cisco Integrated Services Routers also feature a wide range of voice-gateway interfaces, supporting a broad array of signaling and physical network interfaces.

The Cisco 2900 Series enables a full range of existing and emerging video services, with scaling improvements to support Cisco TelePresence® conferencing, security, and session control. The Cisco Unified Border Element extends these capabilities for business-to-business TelePresence communications. The Cisco 2900 Series adds support for the new Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3), which has been optimized for voice and video support. The new PVDM3 modules support all voice-gateway functions of earlier generations of PVDMs and add higher density and more processing power to support emerging rich-media applications. The Cisco 2900 Series provides 2 or 3 onboard PVDM3 slots, depending on the platform.

#### Cisco Unified Communications Manager Express and Survivable Remote Site Telephony

The Cisco Integrated Services Routers natively provide optional unified communications services within the Cisco IOS Software, minimizing the IT hardware footprint and total cost of ownership at the branch office. Cisco Unified Communications Manager Express (CME) provides a broad range of IP private-branch-exchange (PBX) and key-system features integrated into the router for the small and midsize branch office. Cisco Survivable Remote Site Telephony (SRST), also inherently available in Cisco IOS Software, and an option on the Cisco 2900 Series, helps ensure that branch-office employees have uninterrupted telephony services and features, even if the connection to a centralized Cisco Unified Communications Manager is disrupted.

Coupled with Cisco Unity® Express, the integrated solution for voicemail, Automated Attendant, and interactive voice response (IVR), the Cisco 2900 Series offers the branch office a complete range of unified communications services while delivering industry-leading security within a single platform.

#### VoiceXML Application Services

The Cisco 2900 Series also supports standards-certified VoiceXML browser services. VoiceXML is an open-standard markup language used to create voice-enabled web browsers and IVR applications. Just as HTML enables you to retrieve data with a PC, VoiceXML enables you to retrieve data using voice or dual-tone-multifrequency (DTMF) telephony input. The Cisco 2900 Series can deliver a much higher range of concurrent voice-gateway services combined with VoiceXML browser services, for up to 200 sessions on the Cisco 2951.

#### Cisco Unified Border Element

The Cisco Unified Border Element capabilities supported on the Cisco 2900 Series address the emerging requirements in an IP-centric interconnect for branch-office unified communications between enterprises and service provider networks. Cisco Unified Border Element provides intelligent border-element functions such as physical and logical ingress and egress demarcation points, signaling and media control, and consolidated security and management features. The Cisco 2900 Series supports higher scale than previously provided on the Cisco 2800 Series, up to three times the number of sessions.

#### Integrated Network Security for Data, Voice, Video, and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the Cisco' SAFE architectural framework that allows organizations to identify, prevent, and adapt to network security threats, the Cisco 2900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package for the Cisco 2900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks. The Cisco 2900 Series offers onboard hardware-based encryption acceleration to provide greater IPsec throughput with less overhead for the route processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch offices that includes features such as:

- Secure connectivity: Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN
- Integrated threat control: Responding to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, Cisco IOS Content Filtering, and Flexible Packet Matching (FPM)
- Identity management: Intelligently protecting endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI)

Detailed information about the security features and solutions supported on the Cisco 2900 Series is available at <http://www.cisco.com/go/routersecurity>.

#### Wireless and Mobility Services

##### Wireless LAN/WAN

The Cisco Integrated Services Routers supporting the Cisco Unified Wireless Architecture enable deployment of secure, manageable wireless LANs (WLANs) optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management. The Cisco Wireless LAN Controller Module on the Cisco 2900 Series allows small and medium-sized businesses (SMBs) and enterprise branch offices to cost-effectively deploy and manage secure WLANs. Cisco Wireless LAN Controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide WLAN functions, managing up to 6, 12, and 25 access points.

##### Wireless WAN

Cisco third-generation (3G) wireless WAN (WWAN) modules combine traditional enterprise router functions, such as remote management, advanced IP services such as voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO) providing you with a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please visit <http://www.cisco.com/go/3g>.

##### Integrated LAN Switching

The Cisco 2900 Integrated Services Routers (Cisco 2911 through Cisco 2951) support the new Cisco Enhanced EtherSwitch® Service Modules, which greatly expand router capabilities by integrating industry-leading Layer 2 or Layer 3 switching with feature sets identical to those found in the Cisco Catalyst 2960 and Catalyst 3650-E Series Switches performing local line-rate switching and routing.

The new Cisco Enhanced EtherSwitch Service Modules take advantage of the increased power capabilities on the Cisco 2900 ISRs. Additionally, the Cisco Enhanced EtherSwitch modules enable the newest Cisco power initiatives, Cisco EnergyWise, Cisco Enhanced Power over Ethernet (ePoE), per-port PoE power monitoring, and RPS-enabled PoE boost. These technologies allow you to meet increased endpoint power requirements without increasing the total power consumption of the branch.

#### Application Services

As organizations continue to centralize and consolidate their branch-office IT infrastructure in an effort to reduce cost and complexity, they are challenged to provide an excellent user experience, ensure continuous service availability, and deliver business-relevant applications when and where they are needed. To address these challenges, the Cisco 2900 Series provides the capability to host Cisco, third-party, and custom applications on a portfolio of high-performance Cisco Services Ready Engine (SRE) modules that transparently integrate into the router. The modules have their own processors, storage, network interfaces, and memory that operate independently of the host router resources, helping to ensure maximum concurrent routing and application performance while reducing physical space requirements, lowering power consumption, and consolidating management.

##### Application Acceleration

The Cisco 2900 Series seamlessly combines industry leading security, IOS-based traffic control and visibility, with Cisco application acceleration solutions. Cisco IOS Software features such as NBAR, IP SLA, and NetFlow provide visibility and monitoring of traffic patterns and application performance while IOS features such as QoS, ACLs, and PfR intelligently control the traffic to maximize the quality of the user experience and employee productivity. The user experience can be further enhanced through the addition of a Cisco WAAS Network Module which can be used to securely provide more advanced WAN optimization techniques such as TCP optimization, caching, compression, and application acceleration. Cisco Integrated Services Routers combined with Cisco WAAS Network Modules, provide optimal performance for applications delivered from a central data center to branch-office users. The solution allows you to consolidate costly server, storage, and backup infrastructure into data centers while maintaining LAN-like service levels for remote users.

#### Cisco Services Ready Engine

The Cisco Services Ready Engine solution is available in a Service Module (SM) and Internal Service Module (ISM) form factor. The Service Module hardware offers up to a seven times performance improvement over the previous generation Network Modules and provides a multi-core x86-64 processor. The SRE modules also support up to 1 terabyte of storage, RAID configurations, hardware-assisted virtualization and cryptography options. The Cisco SRE module enables on-demand provisioning of branch-office applications on the Cisco 2900 Series platforms so that you can deploy the right application, at the right time, in the right place. The hardware and software decoupling provided by the service-ready deployment model enables applications to be provisioned on the module at the time of its installation or remotely anytime thereafter. Supported solutions include Cisco Wide Area Application Services (WAAS), Cisco Unity Express, Cisco Application Extension Platform (AXP), Cisco Wireless LAN Controller (WLC), Cisco Video Surveillance, and other applications under development. The Service Ready Engine enables organizations of various sizes to future-proof their network by allowing them to quickly deploy new branch-office applications without deploying new hardware, reducing the cost of rolling out branch-office services.

#### WAAS Express

Organizations today face several unique wide area network (WAN) challenges: the need to provide employees with constant access to centrally located information, the requirement to continuously back up and replicate mission-critical data to centrally managed data centers, the desire to provide satisfactory experience for IP phone and video communication, and the mandate to control bandwidth costs without sacrificing application availability and performance.

Cisco WAAS Express is designed to help organizations address these challenges. Cisco WAAS Express extends the Cisco WAAS product portfolio with a small-footprint, cost-effective IOS-based software solution integrated into the ISR G2 to offer bandwidth optimization and application acceleration capabilities. Cisco WAAS Express increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native IOS-based services such as security, NetFlow, and QoS.

Cisco WAAS Express is fully interoperable with WAAS on SM-SRE modules, WAAS appliances and can be managed by a common WAAS Central Manager.

Cisco WAAS Express is available in IOS from version 15.1(2)T1.

Further information on Cisco WAAS Express can be found at <http://www.cisco.com/en/US/products/ps11211/index.html>.

#### Medianet for 2900 ISRs

As video becomes pervasive in an organization and more video devices are used, new demands are placed on the network. It can be challenging to accommodate video needs while reducing complexity, planning for capacity, and providing the best possible user experience.

#### Smarter Network, Endpoints, and Services

Traditional IP networks need to evolve to medianets to accommodate these changes. A medianet is an end-to-end IP architecture that helps to enable pervasive media experiences.

The medianet architecture includes a smarter network, smarter endpoints, shared media services, cloud services, and shared media services.

#### More Medianet Benefits

A medianet reduces total cost of ownership and scales video through features such as auto-configuration and media monitoring. At the same time, it helps to ensure a quality user experience while optimizing bandwidth use and efficiency.

For more information on Medianet for 2900ISR, please go to <http://www.cisco.com/en/US/netsol/ns1094/index.html>.

#### Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. Day-one device support

provides immediate manageability support for the Integrated Services Router, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every Integrated Services Router. The new Integrated Services Routers continue a tradition of broad and deep manageability features such as IP service-level agreement (IP SLA), Cisco IOS Embedded Event Manager (EEM), and NetFlow which allow you to know the status of your network at all times. These features, along with Simple Network Management Protocol (SNMP) and syslog, enable your organization's management applications.

Refer to Tables 4 and 5 below for details about network management and manageability support on Cisco 2900 Series Integrated Services Routers.

Table 4. Cisco 2900 ISR G2 Series IOS Software Features and Protocols Support

Feature	Support
Protocols	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BFD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulation	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic Management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS software refer to the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 5 lists the embedded management features available with Cisco IOS Software.

Table 5. Embedded Management Features Available with Cisco IOS Software

Feature	Description
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP Service-Level Agreements (SLAs) enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video in an IP network.

SNMP, RMON, Syslog, NetFlow, and TR-069	Cisco 2900 Series Integrated Services Routers also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.
---	--

The Cisco network management applications listed in Table 6 are standalone products that you can download or purchase to manage your Cisco network devices. The applications are built specifically for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Applications

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Network-wide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	<p>CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco Integrated Services Routers, using new instrumentation such as Cisco IOS EEM Generic Online Diagnostics (GOLD).</p> <p>In addition to supporting basic platform services of the Integrated Services Router, CiscoWorks also provides added-value support for the Cisco Services Ready Engine, enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.</p>
Network-wide staging, configuration, and compliance	CiscoWorks NCM	CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Voice configuration and provisioning	Cisco Unified Provisioning Manager	Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	Easily manage Cisco IOS Software activation and licenses for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.

Operational Phase	Application	Description
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

#### Summary

As your business strives to lower the total cost of ownership in running your network and increase your overall employee productivity with more centralized and collaborative network applications, you will need more intelligent branch-office solutions. The Cisco 2900 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 2900 Series is designed to consolidate the functions of many separate devices into a single, compact system.

Table 7. Cisco 2900 Integrated Services Router Product Specifications

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
<b>Services and Slot Density</b>				
Embedded Hardware-Based Cryptography and Acceleration	Yes	Yes	Yes	Yes
Cisco Unified SRST Sessions	35	50	100	250
Cisco Unified CCME Sessions	35	50	100	150
Total Onboard WAN 10/100/1000 Ports	2	3	3	3
RJ-45-Based Ports	2	3	3	3
SFP-Based Ports (use of SFP port disables the corresponding RJ-45 port)	0	0	1	1
Service Module Slots	0	1	1	2
Double-Wide Service Module Slots (use of a double-wide slot will occupy all single-wide service module slots in a 2900)	0	0	1	1
EHWIC Slots	4	4	4	4
Double-Wide EHWIC Slots (use of a double-wide EHWIC slot will consume two EHWIC slots)	2	2	2	2
ISM Slots	1	1	1	1

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Onboard DSP (PVDM) Slots	2	2	3	3
Memory DDR2 ECC DRAM - Default	512 MB	512 MB	512 MB	512 MB
Memory (DDR2 ECC DRAM) - Maximum	2 GB	2 GB	2 GB	2 GB
Compact Flash (External) - Default	slot 0: 256 MB slot 1: none			
Compact Flash (External) - Maximum	slot 0: 4 GB slot 1: 4 GB			
External USB 2.0 Flash Memory Slots (Type A)	2	2	2	2
USB Console Port (Type B) (up to 115.2 kbps)	1	1	1	1
Serial Console Port	1	1	1	1
Serial Auxiliary Port	1	1	1	1
Power-Supply Options	AC and PoE	AC, PoE, and DC	AC, PoE, and DC	AC, PoE, and DC
RPS Support (External)	No	Cisco RPS 2300	Cisco RPS 2300	Cisco RPS 2300
Power Specifications				
AC Input Voltage	100 to 240 VAC auto ranging			
AC Input Frequency	47 to 63 Hz			
AC Input Current Range AC Power Supply (Maximum)	1.5 to 0.6A	2.2 to 1.0A	3.4 to 1.4A	3.4 to 1.4A
AC Input Surge Current	<50A	<50A	<50A	<50A
Typical Power (No Modules) (Watts)	40	50	60	70
Maximum Power with AC Power Supply (Watts)	150	210	320	340

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Maximum Power with PoE Power Supply (Platform Only) (Watts)	175	250	370	405
Maximum Power with DC-PoE Power Supply (Platform Only) (Watts)	-	140	-	-
Maximum End-Point PoE Power Available from AC PoE Power Supply (Watts)	130	200	280	370
Maximum End-Point PoE Power Available from DC PoE Power Supply (Watts)	-	160	-	-
Maximum End-Point PoE Power Capacity with PoE Boost (Watts)	N/A	750	750	750
DC Input Voltage	N/A	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative
DC Input Current	N/A	(MAX) 8A (24V) 3.5A (60V)	(MAX) 12A (24V) 5A (60V)	(MAX) 12A (24V) 5A (60V)
Physical Specifications				
Dimensions (H x W x D)	1.75 x 17.25 x 17.3 in. (44.5 x 438.2 x 439.4 mm)	3.5 x 17.25 x 12 in. (88.9 x 438.2 x 304.8 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)
Rack Height	1RU (rack unit)	2RU	2RU	2RU
Rack-Mount 19 in. (48.3 cm) EIA	Included	Included	Included	Included
Rack-Mount 23 in. (58.4 cm) EIA	Optional	Optional	Optional	Optional
Wall-Mount (refer to installation guide for approved orientation)	Yes	Yes	No	No
Weight with AC Power Supply (No Modules)	13.4 lb (6.1 kg)	18 lb (8.2 kg)	29 lb (13.2 kg)	29 lb (13.2 kg)
Weight with AC PoE Power Supply (No	14.3 lb (6.5 kg)	19 lb (8.6 kg)	30 lb (13.6 kg)	30 lb (13.6 kg)

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Modules)				
Typical Weight Fully Configured	16 lb (7.3 kg)	21 lb (9.5 kg)	34 lb (15.5 kg)	34 lb (15.5 kg)
Airflow	Front to side	Side to side	Back and Side to Front	Back and Side to Front
Optional Airflow Kit	N/A	Front to back	N/A	N/A
Environmental Specifications				
Operating Conditions				
Temperature: 5,906 feet (1,800m) Maximum Altitude	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 9,843 feet (3,000m ) Maximum Altitude	32 to 77°F (0 to 25°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 13,123 feet (4,000m) Maximum Altitude	N/A	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)
Temperature: Short-Term (per NEBS) 5906 feet (1,800m) Maximum Altitude	N/A	23°F to 122°F (-5 to 50°C)	N/A	23°F to 122°F (-5 to 50°C)
Altitude	10,000 ft (3,000m)	13,000 ft (4,000m)	10,000 ft (3,000m)	13,000 ft (4,000m)
Relative Humidity	10 to 85%	5 to 85%	10 to 85%	5 to 85%
Short-Term (per NEBS) Humidity	N/A	5% to 90%, but not to exceed 0.024 kg water/kg of dry air	N/A	N/A
Acoustic: Sound Pressure (Typical/Maximum)	41/53 dBA	51.8/62.9 dBA	54.4/67.4 dBA	54.4/67.4 dBA
Acoustic: Sound Power (Typical/Maximum)	49/61 dBA	58.5/70.3 dBA	62.6/74.5 dBA	62.6/74.5 dBA
Non-Operating Conditions				
Temperature	-40 to 158°F (-40 to 70°C)	-40 to 176°F (-40 to 80°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Relative Humidity	5 to 95%	5 to 95%	5 to 95%	5 to 95%
Altitude	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)
Regulatory Compliance				
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

#### Supported Modules

The Cisco 2900 Series supports a wide range of modules that span industry-leading breadth of services at the branch office. For a list of modules supported on the Cisco 2900 Series, please visit: [http://www.cisco.com/en/US/products/ps10537/products\\_relevant\\_interfaces\\_and\\_modules.html](http://www.cisco.com/en/US/products/ps10537/products_relevant_interfaces_and_modules.html)

#### Ordering Information

The Cisco 2900 Series Integrated Services Routers are orderable and shipping. For information about how to order the Cisco 2900 Series, please visit the Cisco 2900 Series Ordering Guide. To place an order, visit the Cisco Ordering Home Page and refer to Table 8, which provides basic ordering information. For additional product numbers, including the Cisco 2900 Series bundle offerings, please check the Cisco 2900 Series Integrated Services Router Price List or contact your local Cisco account representative.

Table 8. Cisco 2900 Series Basic Ordering Information

Product Name	Product Description
Cisco2901/K9	Cisco 2901 with 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
Cisco2911/K9	Cisco 2911 with 3 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
Cisco2921/K9	Cisco 2921 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
Cisco2951/K9	Cisco 2951 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
SL-29-DATA-K9	Data License for Cisco 2901-2951
SL-29-UC-K9	Unified Communications License for Cisco 2901-2951
SL-29-SEC-K9	Security License for Cisco 2901-2951

#### Cisco Integrated Services Router Migration Options

Cisco 2900 Series Integrated Services Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to <http://www.cisco.com/go/tmp> and contact your local Cisco account representative for program details.

#### Warranty Information

The Cisco 2900 Series Integrated Services Routers have a ninety (90) day limited liability warranty.

#### Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, please visit <http://www.cisco.com/go/services>.

Cisco SMARTnet® technical support for the Cisco 2900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- 24-hour access to the industry's largest dedicated technical support staff

## **AR HUAWEI 1220**

Los routers de la serie AR1200 son routers corporativos de próxima generación basados en la plataforma de enrutamiento versátil (VRP) de Huawei. Son el resultado de la vasta experiencia de Huawei en el área de comunicaciones de datos, tecnologías inalámbricas, redes de acceso y redes core. El router AR1200 integra funciones de enrutamiento, conmutación, 3G, WLAN, voz y seguridad. Tiene una estructura de CPU de múltiples núcleos y conmutación no bloqueante. Además, sus niveles de rendimiento y expansibilidad son líderes en la industria, lo que permitirá cumplir con futuros requerimientos para el desarrollo de servicios. El AR1200 es una solución integrada para redes empresariales. Permite agilizar el suministro de múltiples servicios y protege las inversiones de los clientes. El AR1200 ofrece cuatro modelos: AR1220, AR1220V, AR1220W y AR1220VW.

### **Características**

#### **AR de tercera generación con rendimiento líder en la industria**

El AR1200 utiliza la estructura CPU de múltiples núcleos y conmutación no bloqueante. Además, sus niveles de rendimiento del sistema son líderes en la industria, lo que permite cumplir con los requerimientos de extensión de la red y desarrollo de servicios de las empresas.

#### **Red dual y acceso flexible de soporte**

El AR1200 no sólo es compatible con el modo inalámbrico WLAN, UMTS, LTE, sino que también es compatible con el modo de fibra de cable, cable de cobre, que proporcionan al cliente formas flexibles de acceder a la red.

#### **Servicios integrados en un solo router**

El AR1200 integra las funciones de enrutamiento, conmutación, 3G, WLAN, voz y seguridad.

#### **Plataforma de servicios abiertos**

El AR1200 se interconecta con los sistemas de TI de terceros mediante el uso de la plataforma de servicios abiertos (OSP) para proporcionar una solución de comunicación unificada para los usuarios corporativos. Los clientes, agentes, terceros proveedores y fabricantes pueden desarrollar y utilizar el AR1200, según sea necesario.

#### **Experiencia de voz excepcional**

El AR1200 ofrece varias funciones de voz para redes de datos corporativas, lo cual permite que las empresas se comuniquen de manera flexible y eficiente.

#### **Acceso seguro a los servicios**

Durante la prestación del servicio, el AR1200 garantiza la seguridad de las redes corporativas. Proporciona un mecanismo de protección de seguridad completo, que incluye el control de acceso del usuario, la detección de paquetes y la defensa de ataque activo. Este mecanismo protege las inversiones de los clientes.

#### **Implementación del servicio inteligente**

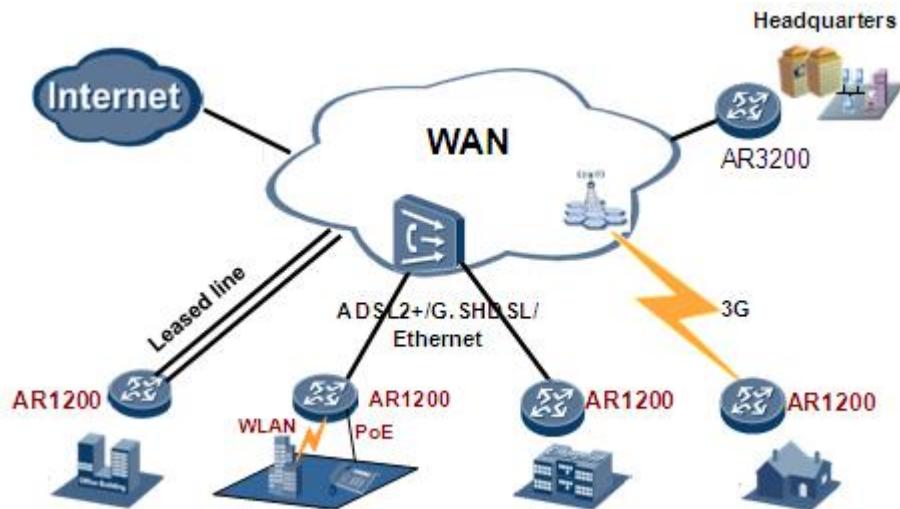
A medida que aumenta la escala de la empresa, los usuarios corporativos tienen elevados requerimientos para la implementación del servicio. El AR1200 ofrece un disco USB para implementar los dispositivos y la función de configuración automática para la implementación de servicios.

#### **Gestión de servicios simplificada**

Los usuarios corporativos requieren una gestión simple del servicio. El AR1200 ofrece las funciones de iTec, NQA, NetStream para simplificar la gestión del servicio.

#### Applications & Benefits

##### Acceso WAN



Los AR1200 funcionan como los routers de egreso de las sucursales de la empresa y proporcionan métodos de acceso flexibles para soportar las conexiones de red remotas. Un AR1200 puede satisfacer varios requerimientos de acceso, incluida la línea arrendada, Ethernet, xDSL, 3G y WLAN. Esto ahorra costos de implementación y mantenimiento y brinda un gran valor a los clientes.

##### Servicio de voz de alta calidad

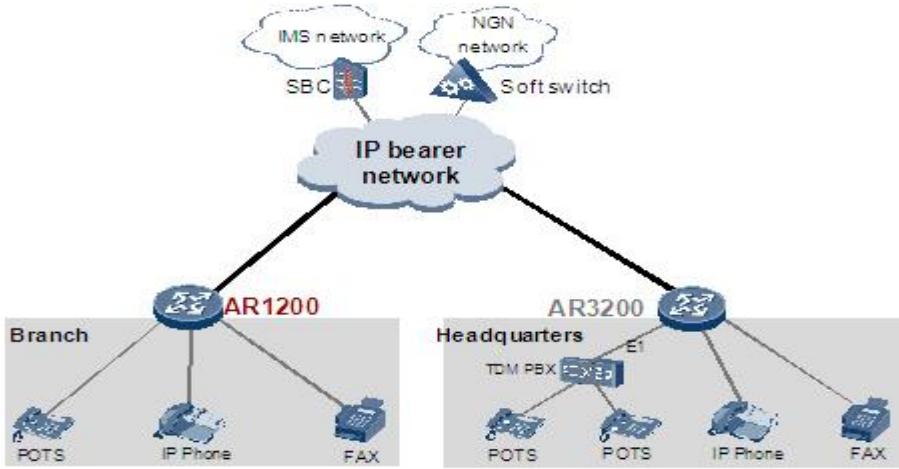
Como gateway de voz para redes corporativas, el AR1200 puede funcionar como PBX IP o gateway SIP.

Figura 1: Aplicación PBX de IP



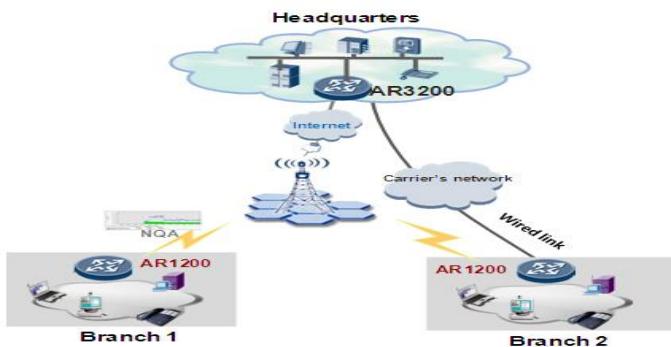
Los routers AR cuentan con una PBX integrada compatible con el número principal de la empresa, IVR y funciones de consulta de facturación para mejorar la imagen corporativa y eficiencia de la comunicación de la empresa. El AR1200 se instala en una sucursal para brindar la función de marcación inteligente. Cuando ocurre una falla en la WAN, la red PSTN se usa como respaldo para las llamadas. Cuando el servidor SIP de la casa central no está disponible, el servidor SIP local integrado del AR1200 lleva a cabo la comunicación entre las sucursales y entre una sucursal y la red PSTN. Esto asegura la confiabilidad del servicio de voz.

Figura 2: Aplicación de gateway SIP



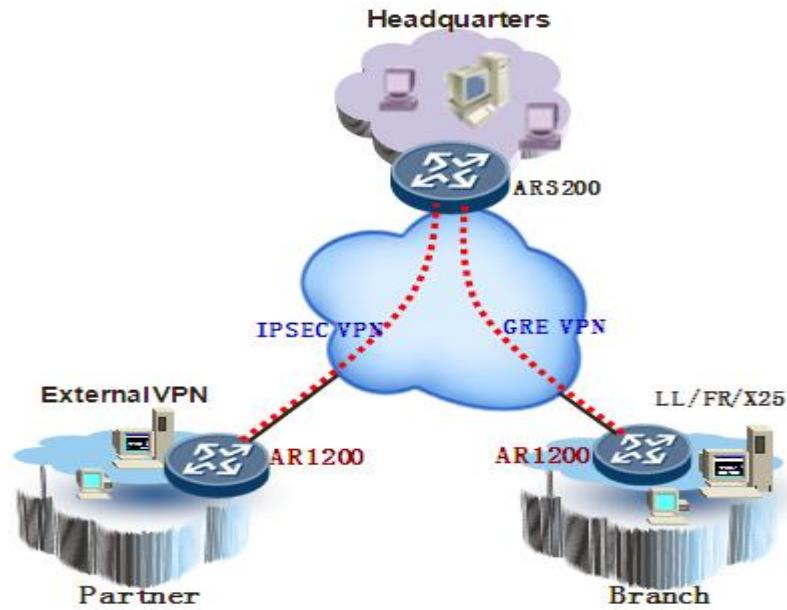
El AR1200 integra servicios de voz, fax e IP. Al brindar servicios de voz para usuarios corporativos, el AR1200 funciona como gateway de acceso SIP de una sucursal para convertir las señales telefónicas en señales VoIP. Las interfaces uplink del AR1200 están conectadas a la red IMS/NGN para permitir, en cualquier momento, el establecimiento de comunicaciones a través de cualquier medio (teléfonos, microteléfonos y computadoras, por ejemplo).

#### Acceso inalámbrico 3G en sucursal



El AR1200 cumple con los estándares de 3G, entre ellos, CDMA2000 EV-DO, WCDMA y TD-SCDMA, al tiempo que también observa los requerimientos de comunicaciones inalámbricas entre sucursales y la sede central. Los usuarios pueden utilizar un disco USB 3G para implementar servicios 3G en el AR1200, lo que ahorra ranuras de tarjetas de servicios. Además, el enlace de datos 3G se puede utilizar como backup para el enlace con cable para proteger los uplinks xDSL, FE/GE y RSIDI. El enlace de backup mejora la estabilidad de la red y reduce los costos de construcción de la red. El AR1200 ofrece la función NQA para detectar la calidad del enlace 3G, lo que garantiza el SLA.

#### VPN en sucursal



El AR1200 ofrece varias funciones de acceso seguro para implementar la comunicación entre las sucursales de la empresa, y entre sucursales y la sede central, y permitir que los socios puedan acceder a recursos de la empresa. Entre la casa central y las sucursales se establecen túneles (tales como VPN GRE y VPN IPSEC) para lograr seguridad en la transmisión y el acceso a los datos. El AR1200 permite la autenticación e implementación rápida de túneles para sucursales. Mediante un túnel, los socios pueden acceder a los recursos de la empresa y compartirlos.

## GLOSARIO

**ARP:** Address Resolution Protocol

**ASN:** Abstract Syntax Notatio

**DCC:** Direct Client-to-Client (DCC), es un protocolo de Internet Relay Chat (IRC) que permite interconectar dos peers o puntos usando un servidor IRC como saludo (handshaking) para permitir intercambiar archivos.

**DNS:** Domain Name System es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

**FTP:** File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un [protocolo de red](#) para la [transferencia de archivos](#) entre sistemas conectados a una red.

**HTTP:** Hypertext Transfer Protocol o HTTP, protocolo de transferencia de [hipertexto](#) es el [protocolo](#) de comunicación que permite las transferencias de información en la [World Wide Web](#).

**IANA:** Internet Assigned Numbers Authority Agencia de Asignación de Números de Internet.

**ICANN:** Internet Corporation for Assigned Names and Numbers

**ICMP:** Protocolo de Mensajes de Control de Internet o ICMP Internet Control Message Protocol es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).

**IDENT:** Servicio de identificación/autorización.

**IP:** Internet Protocol

**ISO:** Organización Internacional de Normalización (International Organization for Standardization, conocida por las siglas ISO) es una organización para la creación

de estándares internacionales compuesta por diversas organizaciones nacionales de estandarización.

**ISP:** Internet service provider proveedor de servicios de Internet.

**LAN:** Una red de área local o LAN , Local Area Network es una [red de computadoras](#) que abarca un área reducida a una casa, un departamento o un edificio.

**MIB:** Management Information Base (MIB) La Management Information Base (MIB) es la colección de objetos administrables definidos utilizando la SMI. Para estos objetos se sigue una estructura jerárquica en forma de árbol.

**MPLS:** Multiprotocol Label Switching es un mecanismo de transporte de datos estándar creado por la [IETF](#) y definido en el [RFC 3031](#). Opera entre la [capa de enlace de datos](#) y la [capa de red](#) del modelo [OSI](#). F

**NIC:** Network Interface Card o Network interface controller (NIC), Tarjeta de interfaz de red (TIR), es un componente de hardware que conecta una computadora a una red informática y que posibilita compartir recursos

**NMS:** [Network Management Station](#)

**OID:** Object Identifier el cual define de manera única cada objeto en el protocolo SNMP.

**OSI:** Open System Interconnection es el modelo de red descriptivo.

**PDU:** Protocol Data Unit - Unidad de datos de protocolo). Estos datagramas no necesitan ser mayores que 484 bytes,

**SMI:** Structure of Management Information, define el nombre y tipo de datos de los objetos gestionables.

**SMS:** Short Message Service Servicio de mensajes cortos. Es un sistema para enviar y recibir mensajes de texto para teléfonos móviles.

**SMTP:** Simple Mail Transfer Protocol, Protocolo de transferencia simple de correo electrónico. Es el protocolo, basado en texto, que permite transferir correo electrónico entre diferentes computadoras

**SNMP:** son las siglas de Simple Network Management Protocol, es un protocolo que permite realizar la gestión remota de dispositivos.

**TCP:** Protocolo de Control de Transmisión, es uno de los principales protocolos de la capa de transporte del modelo TCP/IP.

**TCP/IP:** es un conjunto de protocolos que permiten la comunicación entre los ordenadores pertenecientes a una red. La sigla TCP/IP significa Protocolo de control de transmisión/Protocolo de Internet

**VPN:** Virtual Private Network (VPN), es una tecnología de [red de computadoras](#) que permite una extensión segura de la [red de área local \(LAN\)](#) sobre una red pública o no controlada como [Internet](#).

**WAN:** (Wide Area Network en inglés), es una [red de computadoras](#) que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

**WWW:** World Wide Web, el sistema de documentos de hipertexto que se encuentran enlazados entre sí y a los que se accede por medio de Internet.