ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE SERVICIOS DE DATOS E INTERNET PARA SUCURSALES EN LA CIUDAD DE GUAYAQUIL, DE UNA INSTITUCIÓN DEL ESTADO"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

CLAUDIA GABRIELA LLERENA PINCAY

GUAYAQUIL-ECUADOR

AÑO: 2016

AGRADECIMIENTO

Agradezco a Dios por brindarme la oportunidad de formar parte de mi familia, que me han ayudado a formar como persona a lo largo de mi vida, inculcándome excelentes valores que me han ayudado a desarrollarme por la vida.

Doy un agradecimiento especial a mis padres y esposo que realizaron un esfuerzo desmedido por garantizar mi educación.

DEDICATORIA

Dedico este proyecto a mi esposo y familia, que son pilares fundamentales en mi vida, que me han acompañado en esta travesía que tiene altibajos pero con la unión se han podido vencer.

TRIBUNAL DE SUSTENTACIÓN

MGS. LENIN FREIRE C.

DIRECTOR DEL MSIA

MGS. KARINA ASTUDILLO B.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

MGS. RONNY SANTANA.

PROFESOR DELEGADO

POR LA UNIDADACADÉMICA

RESUMEN

Tanto en instituciones públicas como privadas La WAN es una parte primordial de las redes corporativas.

Cuando en las dependencias se presentan lentitud, interrupción, intermitencias en la conectividad de sus servicios, generan un obstáculo para la realización de las actividades de los usuarios. Considerando estos inconvenientes y para mantener la seguridad de la información es indispensable visualizar sus enlaces WAN,permitiendosolucionar problemas de cortes, rendimiento. Obteniendo como resultado la disponibilidad adecuada y mejorando la calidad de los servicios [1].

La aplicación que se implementara en estas dependencias del estado permitirá monitorear, controlar, diagnosticar, resolver en forma definitiva el rendimiento de la red WAN, obtendrán estadísticas de disponibilidad, consumo de Ancho de banda, en tiempo real o mediante datos históricos, mantendrá informado al personal técnico sobre cualquier inconveniente que

se presente, mediante el envío de alertas a su correo electrónico institucional, y de ser necesario se reportara al ISP automáticamente.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AB	Ancho de Banda.
CPU	Central ProcessorUnit (Unidad Central de Procesamiento).
DNS	DomainNameSystem (Sistema de Nombres de Dominio).
ITIL	InformationTechnologyInfrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información).
IP	Internet Protocol (Protocolo de Internet).
ISP	Internet ServiceProvider (Proveedor de Servicios de Internet).
LAN	Local Area Network (Red de Área Local).
MB	Megabyte.
MS	Milisegundo
PING	PacketInternetGrouper (Buscador o Rastreador de Paquetes en Redes).
PRTG	Paessler Router TrafficGrapher.
SLA	ServiceLevelAgreement (Acuerdo de Nivel de Servicio).
SMS	Short MessagesService (Servicio de Mensajes Cortos).
SNMP	Simple Network Management Protocol (Protocolo Simple de Administración de Red).
SNMP2Vc	Versión SNMP 2 Comunidad.

TCP/IP	Transmission Control Protocol/Internet Protocol (Protocolo de Control de Transmisión/Protocolo de Internet).
TI	Tecnología Informática.
TICS	Tecnologías de la Información y Comunicación
WAN	Wide Area Network (Red de Área Amplia).

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las redes WAN de las organizaciones públicas o privadas, se han vuelto cada vez más complejas y la exigencia de la operación es día a día más demandante, ya que soportan aplicaciones y servicios estratégicos de las organizaciones, por lo que la interconexión de todas las dependencias queposee una institución se ha convertido en una necesidad primordial hoy en día, debido a esto los encargados de TI en cada institución se han visto en la necesidad de contratar enlaces de datos e internet.

Cuando se presentan inconvenientes en la red provocan emergencias haciendo que los empleados no desempeñen su actividades e induciendo el descontento en cada uno de ellos, para esto se necesita minimizar los fallos; cuando se presente una incidencia poder de forma inmediata alertar a todo el equipo de TI o a los destinatarios que sean responsables del servicio para que brinden una solución al inconveniente.

La implementación de un aplicativo de monitoreo que pueda prevenir posibles fallos y notificaciones tempranas, que permite identificar

rápidamente el origen de esa incidencia, al tener una estructura jerárquica de dispositivos de servicios, de punto de control, ubicar en donde está el cuello de botella o el origen la causa raíz del problema o la incidencia;conseguirá que el tiempo de caída, el tiempo de degradación de servicios se reduzca al mínimo posible es un gran apoyo para el personal encargado de TICS y también a los usuarios.

La ejecución de esta herramienta, nos permite controlar los niveles de servicios contratados con nuestros proveedores previamente acordados en los porcentajes de Down time por mes; El aplicativo nos permitirá controlar el ancho contratado versus el ancho de banda real entregado y el consumido por cada unidad de nuestra institución, esto nos ayuda a validar que el ISP nos esté proveyendo el servicio contratado acordado y el más transcendental es determinar el “capacity” del ancho de banda por cada localidad, considerando el ancho de banda contratado versus el consumido para poder realizar reutilización del ancho de banda en otras dependencias incorporadas o Up Grade; el resultado de este análisis nos permite no convertir la inversión en un gasto, ya que al ser una institución del estado se manejan presupuestos preestablecidos por el gobierno y para este 2016 se

ha presentado una reducción considerable en el presupuesto para proyectos de TICS.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA.

Este órgano encargado de la administración, vigilancia y disciplina de las leyes y la justicia, se encuentra interesado en buscar una solución que le permita medir y garantizar las conexiones de datos, para mantener una alta disponibilidad en los servicios que presta.

Se ha evidenciado que los servicios que presta la entidad son afectados por periodos prolongados de tiempo, sin poder identificar el problema o brindar una solución oportuna a los incidentes suscitados, como pérdida de conectividad e intermitencia en el servicio.

Se aprecia que las intermitencias generalmente son producidas por la saturación presentada en el servicio de datos o el Internet contratado, esto no significa un uso racional de los mismos.

Es indispensable para la institución evidenciar de manera oportuna inconvenientes como cortes, problemas de rendimiento, degradación y saturación en el servicio,obtener estadísticas de disponibilidad, consumo de Ancho de banda, en tiempo real o mediante datos históricos, para buscar las causas y brindar las soluciones apropiadas.

Considerando que los servicios que brinda la institución a través de sus diferentes dependencias es de 24 x 7, se evidenció que los tiempos de falla o indisponibilidad de servicios de Datos e Internet son elevados, aproximadamente un 10% mensual, estamos hablando de alrededor de 72 horas en el mes, afectando aplicaciones y servicios estratégicos de la institución, actualmente no se posee una herramienta que pueda prevenir posibles fallos y notificaciones tempranas, que permitan solucionar incidentes de una manera oportuna. Por lo que es indispensable informar al personal equipo de TI o a los destinatarios que sean responsables del servicio sobre

cualquier inconveniente que se presente, mediante él envió de alertas a su correo electrónico institucional,y de ser necesario se reportará al ISP automáticamente.

Estos inconvenientes normalmente provocan una baja calidad de servicio delas aplicaciones montadas en la red. Para cada caso particular se deberá definir que es “uso racional de un enlace”. Sin olvidar la calidad de servicio que se debe brindar a nuestro usuario interno, el cual usa la conexión a Internet para realizar actividades cotidianas como; estar más en contacto con sus familias y amigos, realizar pagos, investigaciones, etc. Esto mediante aplicaciones que permiten voz y video sobre una red de datos, mensajería instantánea, mensajería tradicional (correo electrónico), etc. Estos son unos de los motivos para controlar o mejor dicho arbitrar y ordenar el tráfico en los enlaces.

1.2. SOLUCIÓN PROPUESTA.

Realizar la implementación y despliegue de una herramienta de monitoreo que permita solventar los inconvenientes presentados hasta ahora en la institución, luego del análisis de los aplicativos disponibles

en el mercado el aplicativo que más se adapta alas necesidades institucionales es “PRTG Network Monitor”.

Esta herramienta permitirá obtener varias estadísticas de disponibilidad de servicio, ya sean datos en tiempo real o históricos, con esto se podrá realizar un análisis detallado de los incidentes, ayudando en la búsqueda de una solución definitiva a los problemas suscitados en los servicios de Datos e Internet contratados.

Mediante sensores permitirá monitorear la conectividad, trafico in, out de los diferentes puertos del equipo, temperatura, entro otros, permitiendo evidenciar de una manera oportuna si los inconvenientes que presenta la institución a nivel de servicios de datos e internet, son atribuidos al ISP o son problema interno, esto servirá para Gestionar de una manera adecuada la solución reduciendo al mínimo los tiempos de indisponibilidad.

Permitirá realizar la configuración con rangos de advertencia y error, para las alertas, las cuales podrán ser notificadas oportunamente al

equipo de TI o a los destinatarios que sean responsables del servicio vía correo electrónico o SMS, con el fin de que se busque solución o aplicar medidas preventivas y evitar indisponibilidad de servicios.

Se tendrá un monitoreo real del ancho de banda en cada uno de los enlaces de datos e Internet instalados en las localidades de la provincia del Guayas. Con esto se realizara los análisis que ayudaran a determinar el “capacity” del ancho de banda por cada localidad, considerando el ancho de banda contratado versus el consumido para poder realizar reutilización del ancho de banda en otras dependencias incorporadas o Up Grade; permitirá mediantes reportes contrastar el SLA contratado al proveedor, adicional permitirá elegir las calidades de servicio. Se estudiará en qué casos convendrá recortar tráfico, priorizar o una combinación de ambos. Se contemplarán soluciones que surjan del análisis.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. INSTALACIÓN CONFIGURACIÓN DE LA HERRAMIENTA.

Una vez definidos los equipos a monitorear es indispensable realizar la instalación de la herramienta “PRTG Network Monitor”

2.1.1 Proceso de instalación “PRTG Network Monitor”.

- ✓ Hacemos doble clic en el archivo de instalación en el equipo que desea utilizar como servidor de PRTG.
- ✓ Seguimos el asistente de instalación e instalar el software.
- ✓ Al final de la instalación, PRTG abre una nueva ventana del

✓ navegador automáticamente. Se conecta a la interfaz web de PRTG, mostrara el árbol de dispositivos (ver Figuras 2.1), automáticamente escaneara su red. PRTG tratara de detectar todos los aparatos conectados, si desea puede iniciar el asistente de configuración.

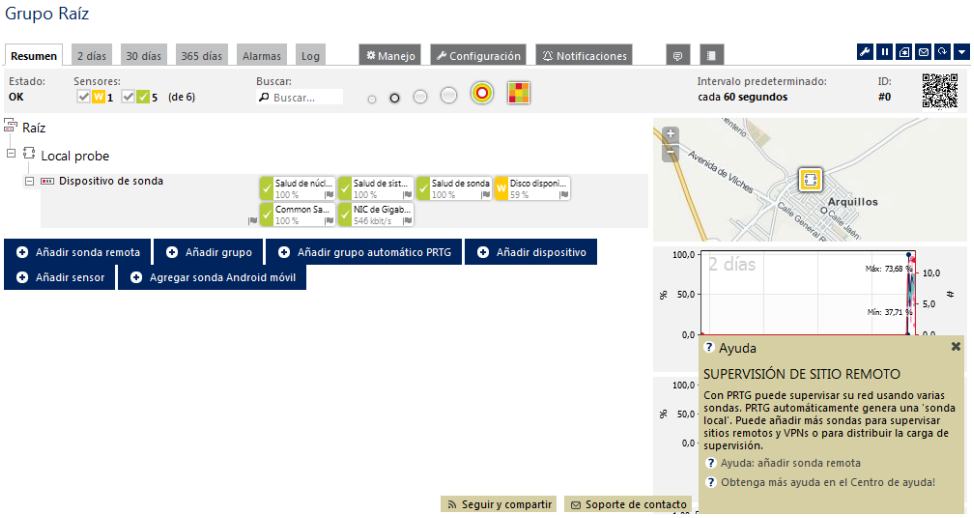


Figura 2.1.- Árbol de dispositivos

✓ Los navegadores compatibles con la interfaz web de PRTG son:

Google Chrome 44 o posterior (se recomienda),

Mozilla Firefox 39 o posterior, o

Microsoft Internet Explorer 11.

2.1.2Datos de acceso“PRTG Network Monitor”

Para realizar una correcta comunicación entre nuestros dispositivos es necesario configurar los datos de acceso, para esto PRTG utiliza un Protocolo que facilita el intercambio de información, administración entre los dispositivos de red. Estees “Protocolo Simple de Administración de Red” o SNMP[4] nombre que s ele atribuye por sus iniciales del inglés Simple Network Management Protocol. El Permite a los administradores supervisar el funcionamiento de la red.

Una vez instalado en nuestro servidor la herramienta “PRTG Network Monitor”, se definió con el equipo de TI y los responsables del servicio,que se trabajara con la versión SNMP 2Vc ya que esta incluye mejoras en las áreas de comunicaciones de rendimiento, la seguridad, confidencialidad.

Una vez definido el protocolo y la versión se define el nombre de la comunidad SNMP, la que servirá como manejador para las relaciones de gestión entre los equipos de nuestra Red, el nombre de la comunidad y la versión SNMP 2Vc deben ser

configurados tanto en el PRTG como en los equipos a monitorear.

2.2 Definición de políticas para el monitoreo de Red.

En conjunto con equipo de TI y los responsables del servicio se definieron las siguientes políticas necesarias para realizar un correcto monitoreo de los servicios de Datos e Internet, las cuales se detallan a continuación:

2.2.1 Distribución de grupos

Es necesario definir la distribución de grupos y nomenclaturas dentro de PRTG para cada uno de los dispositivos a monitorear, con la finalidad de mantener una correcta administración de los dispositivos en la herramienta, como se muestra en la Figura 2.2.

Figura 2.2.- Distribución de grupos

2.2.2 Solicitud de información

Una vez definida la política de distribución de grupos en el PRTG, es necesario configurar los dispositivos a monitorear, para realizar esto debemos validar la situación actual del servicio y solicitar configuración e información de los equipos del ISP, a continuación se detalla el procedimiento a seguir para la solicitud de información.

Para realizar la solicitud de información es indispensable tomar en cuenta las siguientes observaciones:

- ✓ Confirmar la operatividad de la localidad.

- ✓ Confirmarla instalación y operatividad del enlace de datos y o Internet
- ✓ Solicitar al proveedor de este servicio se realicen las Configuraciones necesarias para la habilitación de la comunidad SNMP versión 2, aquí se debe especificar el nombre de la comunidad.
- ✓ Para mantener una identificación apropiada de las interfaces se solicita al ISP, etiquete las interfaces de la siguiente manera:
    - o La interfaz configurada como LAN se llamara WAN_LOCAL
    - o La interfaz configurada como WAN se llamara WAN_Nombre del ISP
- ✓ Solicitar se informe la IP con la que se configuro la interfaz LAN del equipo, ya que esa es la interfaz, tiene direccionamiento IP WAN de nuestra entidad y es la que usaremos para que PRTG tenga acceso a los datos y poder monitorear las interfaces del servicio

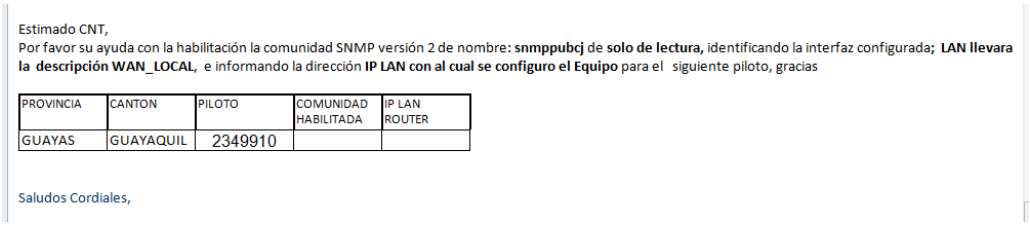
Tabla 1.- Datos enviados a proveedor para habilitación de comunidad SNMP.

PROVINCIA	CANTÓN	PILOTO	COMUNIDAD HABILITADA	IP LAN ROUTER

A continuación detallaremos la descripción de los datos con los cuales se debe llenar la tabla 1:

- ✓ PROVINCIA.- Provincia donde se instaló el servicio, para nuestras dependencias siempre será Guayas.
- ✓ CANTÓN.- Cantón donde se instaló el servicio, como el monitoreo únicamente se va aplicar en Guayaquil, en este campo ira “Guayaquil” para todos nuestros servicios a monitorear.
- ✓ PILOTO.- Esta información se encuentra en el “Acta de entrega de servicio”, la cual es entregada en el momento de la instalación a quien recibe el servicio, adicionalmente el proveedor de servicio de Datos o Internet envía el acta por correo electrónico al responsable del servicio en nuestra entidad.
- ✓ COMUNIDAD HABILITADA.- Esta información la otorga el técnico del proveedor de enlace, como confirmación de que se configuro la comunidad, esto en el correo de respuesta de nuestra solicitud de habilitación de la comunidad SNMP.
- ✓ IP LAN ROUTER.- Esta información la otorga el técnico del proveedor de enlace, en el correo de respuesta de nuestra solicitud de habilitación de la comunidad SNMP.

En la figura 2.3 se muestra el correo que se envía al proveedor del servicio solicitando la habilitación de la comunidad SNMP



Estimado CNT,
Por favor su ayuda con la habilitación la comunidad SNMP versión 2 de nombre: **snmppubcj** de **solo de lectura,** identificando la interfaz configurada; **LAN llevara la descripción WAN_LOCAL**, e informando la dirección **IP LAN con al cual se configuro el Equipo** para el siguiente piloto, gracias

PROVINCIA	CANTON	PILOTO	COMUNIDAD HABILITADA	IP LAN ROUTER
GUAYAS	GUAYAQUIL	2349910		

Saludos Cordiales,

Figura 2.3.- Solicitud de habilitación comunidad SNMP

2.2.3 Nomenclatura

Con la información otorgada por el proveedor (ver Figura 2.4) se agrega el enlace al software PRTG Network Monitor, la nomenclatura utilizada para los nombres con los que se agregaran los dispositivos tendrán el siguiente formato:

CIUDAD_PILOTO_LOCALIDAD(OPCIONAL)_ANCHO-DE-BANDA-EN-MEGAS (GUAYAQUIL_808425_VALDIVIA_6MB).

Este formato fue definido por el equipo de TI y los responsables del servicio, con el fin de mantener el mismo parámetro en todos los aparatos de enlaces y lograr una correcta administración.

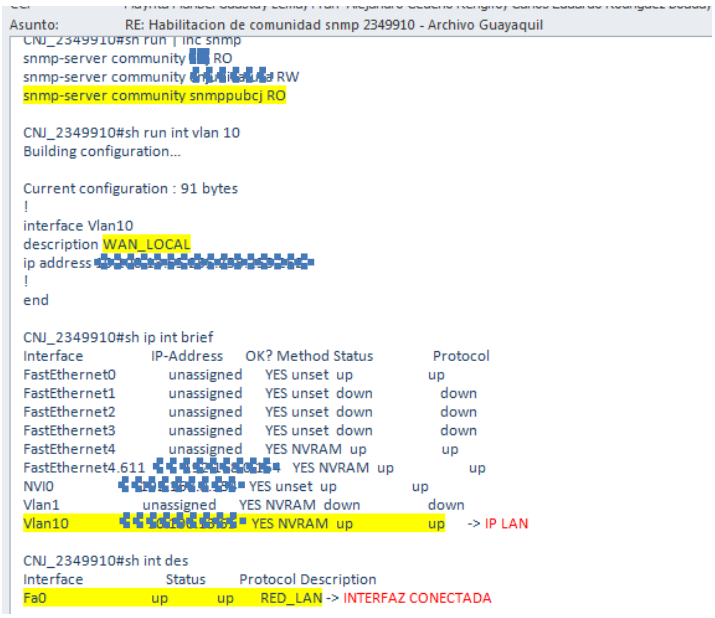


Figura 2.4.- Respuesta del Proveedor

2.2.4 Sensores a monitorear

Una vez que se ingrese el aparato, se debe considerar el orden y los sensores que se monitorearan, a continuación se detalla:

- ✓ Ping
- ✓ WAN_LOCAL
- ✓ WAN_NOMBRE_ISP
- ✓ Sensor de CPU(opcional)
- ✓ Sensores de temperatura (opcional)

Este listado de sensores fue definido por el equipo de TI y los responsables del servicio, con el fin de mantener una adecuada administración de los aparatos [5].

2.3 Agregar dispositivos al monitoreo

Una vez definidos todos los parámetros necesarios y con la información entregada por el proveedor del enlace, se procede a ingresar para nuestro monitoreo, cada uno de los enlaces de datos e internet de la ciudad de Guayaquil. Para realizar esta actividad se deben seguir los siguientes pasos:

- ✓ Ingresamos al grupo al que pertenece el enlace.
- ✓ Elegimos la opción añadir dispositivo o aparato (ver Figura 2.5)

Figura 2.5.- Añadir dispositivo o aparato

- ✓ En la ventana que nos presenta debemos colocar los datos requeridos (ver Figura 2.6)
    - o **Nombre del dispositivo.-** Nombre que se dará al dispositivo de acuerdo a la nomenclatura definida.
    - o **Versión IP** .- Elegir la versión del protocolo TCP/IP con la que está configurado el equipo puede ser V4 o V6
    - o **Dirección IPv# /nombre de DNS.-** Aquí se colocará la dirección IP que entrego el ISP en respuesta al correo de habilitación de comunidad SNMP.
    - o **Icono de dispositivo.-** Opcional, al momento de descubrir los sensores elegirá automáticamente el Icono
    - o **Manejo de sensores.-** Se debe definir como se realizará el manejo de sensores, se recomienda utilizar “Identificación automática de sensores (Una sola vez)”
    - o **Datos de acceso para dispositivos SNMP.-** Una vez colocados los datos anteriores nos desplazamos hasta ubicar la opción “Datos de acceso para dispositivos SNMP”, dentro de esta opción debemos elegir la versión SNMP y colocar el nombre de la comunidad.

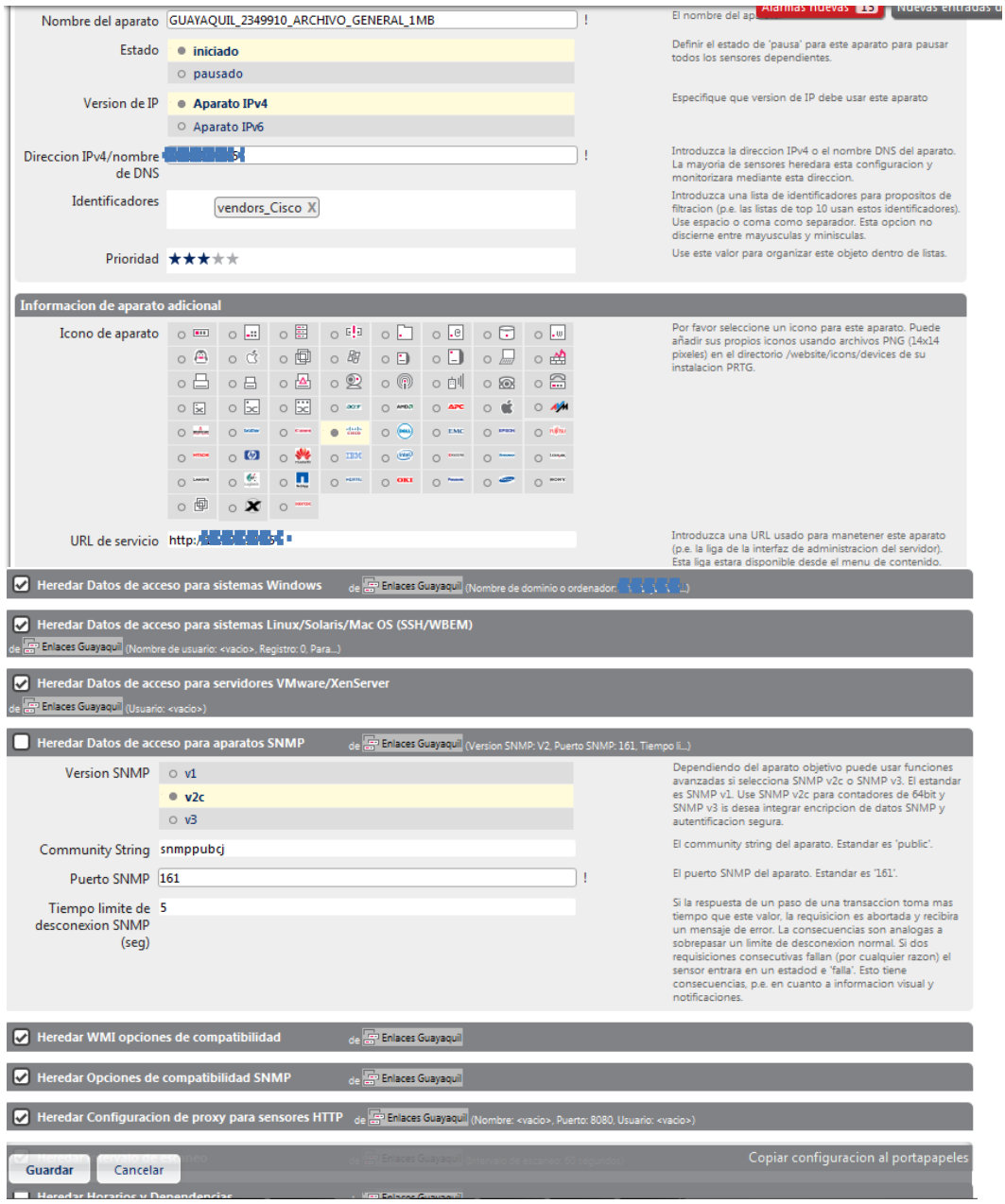


Figura 2.6.- Añadir dispositivo

- ✓ Una vez ingresada la información elegimos la opción continuar y automáticamente empezarán agregarse sensores de monitoreo en nuestro dispositivo.

Al finalizar el descubrimiento automático de sensores, visualizaremos varios sensores innecesarios (Ver Figura 2.7)por lo que procederemos a seleccionarlos y eliminarlos, únicamente monitorearemos los definidos por el equipo de TI y los responsables del servicio.

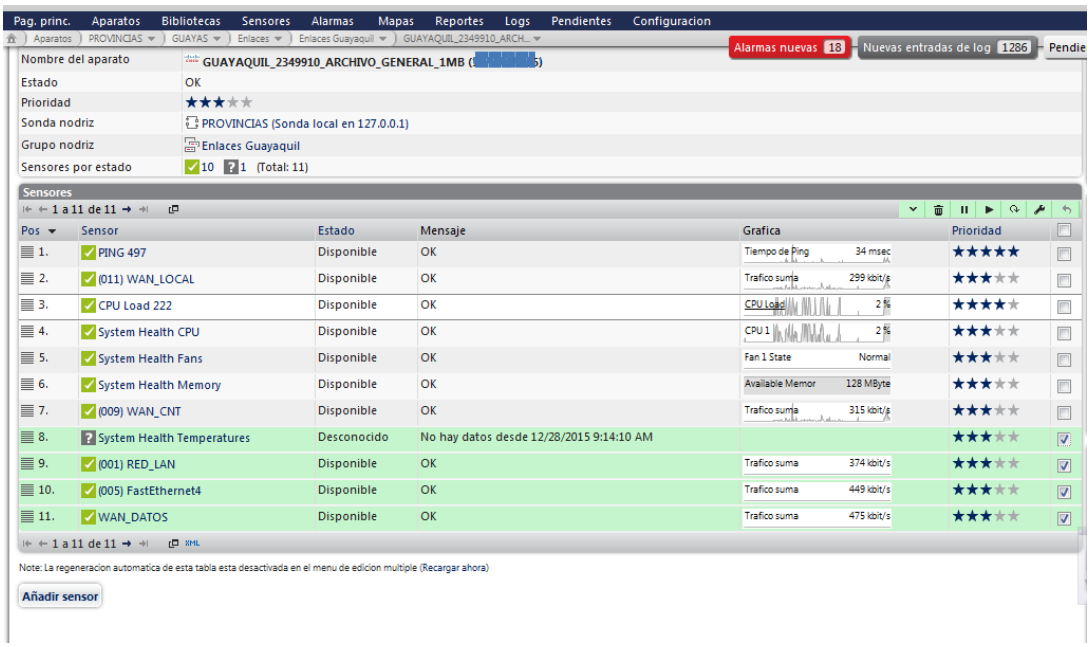


Figura 2.7.- Sensores agregados

2.4 Definición de políticas para advertencias y alertas.

Conjuntamente el equipo de TI y los responsables del servicio definieron las siguientes políticas para los niveles de advertencia y error Down Time, considerando los tiempos necesarios para tomar acciones preventivas en el caso de una advertencia, y soluciones inmediatas al momento de un error. Las advertencias deben ser colocadas una a una manualmente entrando a la configuración de los sensores, únicamente el sensor ping está configurado por defecto para mostrar alarmas al momento que pierde conectividad.

2.4.1 Sensor “PING”.

Cuando el sensor de conectividad PINGpierda conectividad o la latencia sea superior a 250 ms,el sensor se colocara de color rojo indicando una alarma de error de conectividad.

2.4.2 Sensor “WAN_LOCAL”“WAN_NOMBRE ISP”

En los sensores de tráfico con la finalidad de apreciar saturación de los servicios, se colocará umbrales en los canales

de tráfico.Apesar que la herramienta muestra tres datos de Tráfico que son: In,Out, Suma; únicamente se tomarán en consideración los canales In, Out, ya que estos muestran el consumo real de la interfaz.

Dependiendo del ancho de banda contratado se colocarán los umbrales, cuando el consumo se encuentre al 90% el sensor se pondrá en color naranja indicado una alarma de advertencia: “El consumo del AB está al 10% delimite”

Cuando el consumo del Ancho de Banda contratado este al 100%, el sensor se pondrá en color rojo indicando una alarma de Error: “Servicio Saturado Consumo AB al 100%).

2.5 Configuración de umbrales.

Para colocar los umbrales y los mensajes de advertencia y error se debe ejecutar los siguientes pasos

- ✓ Ingresar al sensor
- ✓ Elegir canales

- ✓ Seleccionar el canal en el que se colocará el umbral
- ✓ Colocar los valores máximos y mínimos dependiendo del Ancho de Banda contratado.
- ✓ Colocar los mensajes en las opciones Límite de advertencia y límite de error.

Para visualizar de mejor manera lo descrito,revisar la figura 2.8.

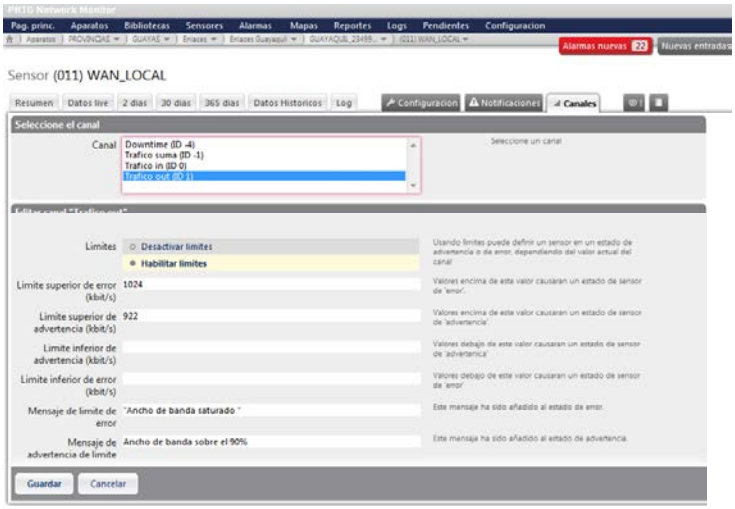


Figura 2.8.- Configuración de Umbrales

2.6Definición de políticas de notificación de alertas.

Dentro de los requerimientos de nuestra institución es necesario que al monitorear un enlace y este se encuentre saturado o no disponible genere automáticamente una alerta y esta sea enviada por mail a los

técnicos de TI o a los responsables del servicio. La finalidad de esta configuración es que por medio de estas notificaciones se valide si la falla detectada por el PRTG es atribuida a la entidad o al ISP, esto servirá para desacatar y/o solventar problemas de primer nivel brindando una solución ágil y oportuna, si al realizar las validaciones de primer nivel no se soluciona el inconveniente se deberá escalar inmediatamente al proveedor del servicio.

2.6.1 Grupos de usuario

En conjunto con equipo de TI y los responsables del servicio se definieron las siguientes políticas que deberán efectuarse para realizar las notificaciones de alertas:

- ✓ Crear usuarios del grupo de TI en la herramienta
- ✓ Crear grupos para:
    - o Técnicos encargados por zona o localidad
    - o Responsable de servicio
    - o Un grupo para todos los usuarios TI

2.6.2 Intervalo de tiempo para notificaciones

En conjunto con el equipo de TI y los responsables del servicio se definieron las siguientes políticas respecto al intervalo de tiempo y el nivel de escalonamiento para realizar las notificaciones de alertas:

- ✓ Cuando el sensor se encuentra en estado de error por 3 minutos se notificara al técnico responsable de la localidad.
- ✓ Si la alarma no es atendida, aceptada y se mantiene por 5 minutos se notificara a los responsables del servicio.
- ✓ Si la alarma no es atendida, aceptada y se mantiene por 10 minutos se notificara a todo el Equipo de TI.

2.7 Configuración de las notificaciones

Con el fin de realizar la configuración de notificaciones de alertas, se deben realizar las políticas definidas por equipo y los responsables de servicio referentes a grupos de usuario, una vez ejecutado esto se debe realizar lo siguiente:

- ✓ Ingresar al aparato o dispositivo.
- ✓ Ingresamos a la pestaña notificaciones.

- ✓ Elegimos “Solo usar disparador definido para este objeto” (ver Figura 2.9).

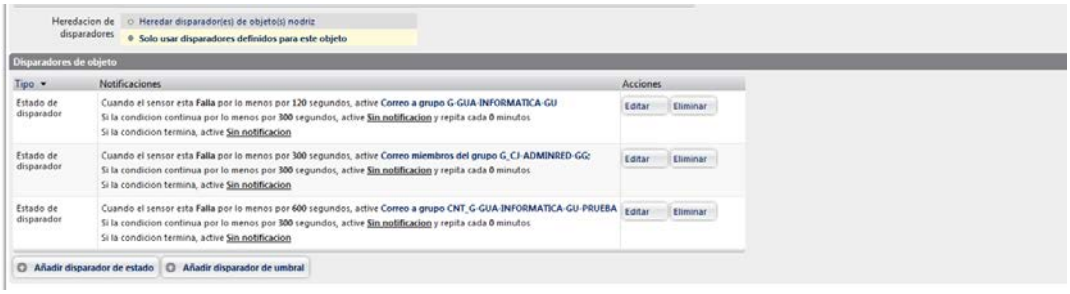


Figura 2.9.- Notificaciones de alarmas enviadas por e-mail

- ✓ Seleccionamos añadir disparador de estado por cada grupo que se vaya a notificar.
- ✓ Se configuran los tiempos de acuerdo a las políticas referidas al ítem 2.6.2 de este documento.

En la figura 2.10 se puede aprecia el contenido de la notificación enviada por correo electrónico para informar sobre la no disponibilidad de un enlace de datos.

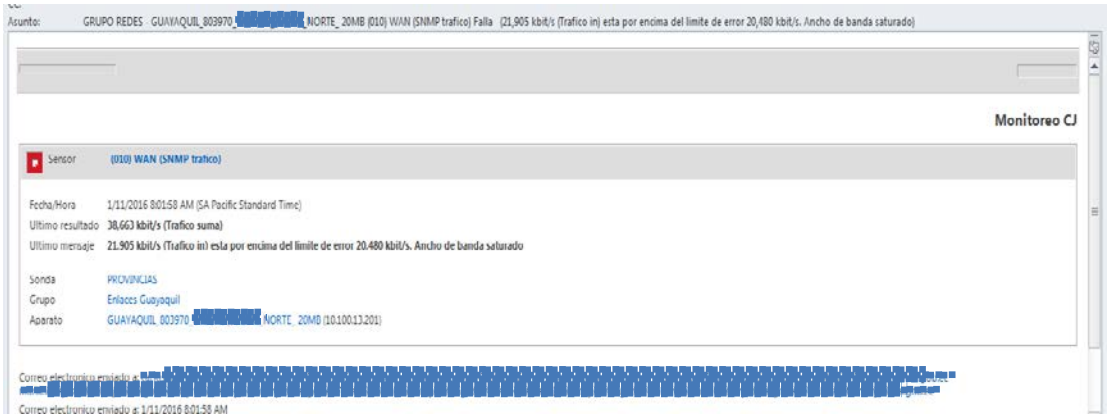


Figura 2.10.- Notificación

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1 Reportes

Para verificar la disponibilidad del servicio, así como realizar los análisis necesarios obtener estadísticas de consumo de Ancho de banda, realizar estudios considerando el ancho de banda contratado versus el consumido para poder realizar reutilización del ancho de banda en otras dependencias incorporadas o Up Grade en las localidades de nuestra institución.

3.1.1 Reportes Gráficas en tiempo real

La herramienta permite visualizar gráficas de consumo a tiempo real, para esto se debe ingresar al sensor del cual se necesita

la gráfica en tiempo real y elegimos la opción “Datos Live” (Ver Figura 3.1).

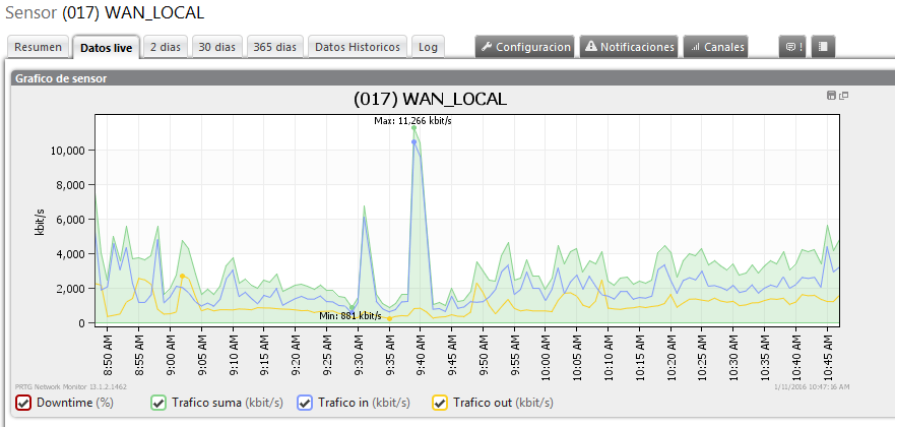


Figura 3.1.- Gráfica en tiempo real

3.1.2 Reportes históricos

En muchas ocasiones es necesario visualizar si los servicios presentaron inconvenientes en días anteriores, en horarios fuera de oficina. Para visualizar gráficas de fechas concretas, es necesario seguir el siguiente procedimiento.

- ✓ Ingresar al sensor
- ✓ Elegir la opción datos históricos
- ✓ Seleccionar las fechas de las que se desea el reporte
- ✓ El intervalo Promedio a un minuto
- ✓ Iniciar

Al realizar esto se ejecutara la gráfica para visualizar el proceso ver la Figura 3.2.

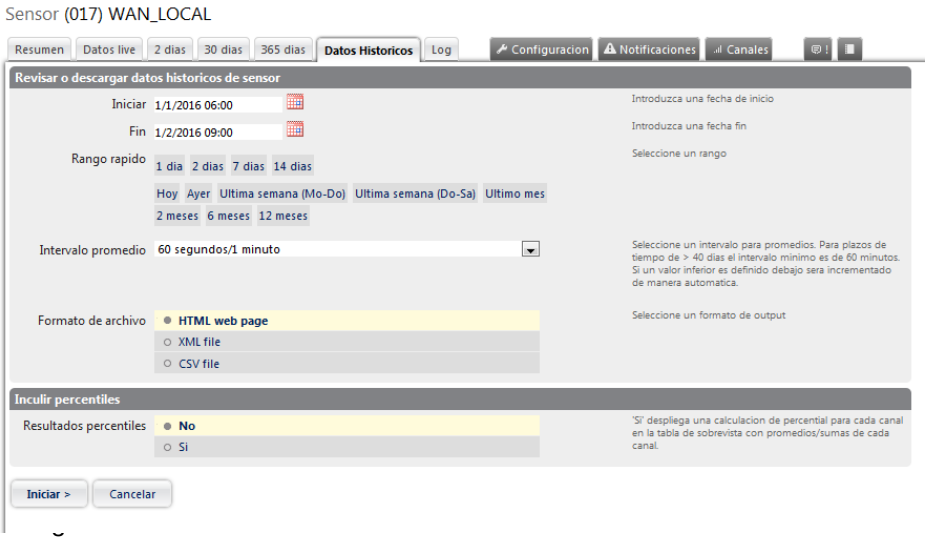


Figura 3 .2.- Gráfica de datos históricos

3.1.3. Reportes de disponibilidad.

Para realizar un contraste de los informes del proveedor, así como para apreciar la disponibilidad del servicio es necesario crear reportes mediante plantillas los mismos que al generarse se enviaran al correo de un usuario específico en formato PDF. Para esta esto debemos realizar el siguiente procedimiento.

- ✓ Menú Reportes
- ✓ Añadir Nuevo Reporte

- ✓ Se ingresan datos de configuración de reporte básica (Ver Figura 3.3)

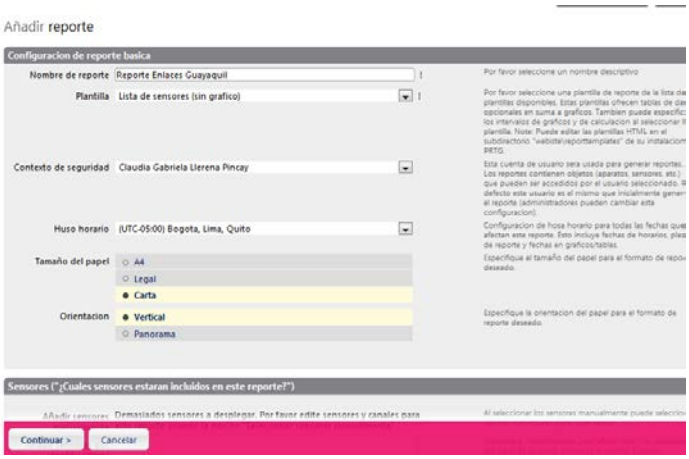


Figura 3.3.- Configuración de reportebásica

  - o Nombre de reporte.- Nombre que se asignará al reporte
  - o Plantilla.- Para realizar la validación de disponibilidad se sugiere lista de sensores sin grafico
- ✓ Seleccionamos la opción continuar.
- ✓ Seleccionamos los sensores que se desean monitorear Ver figura 3.4.

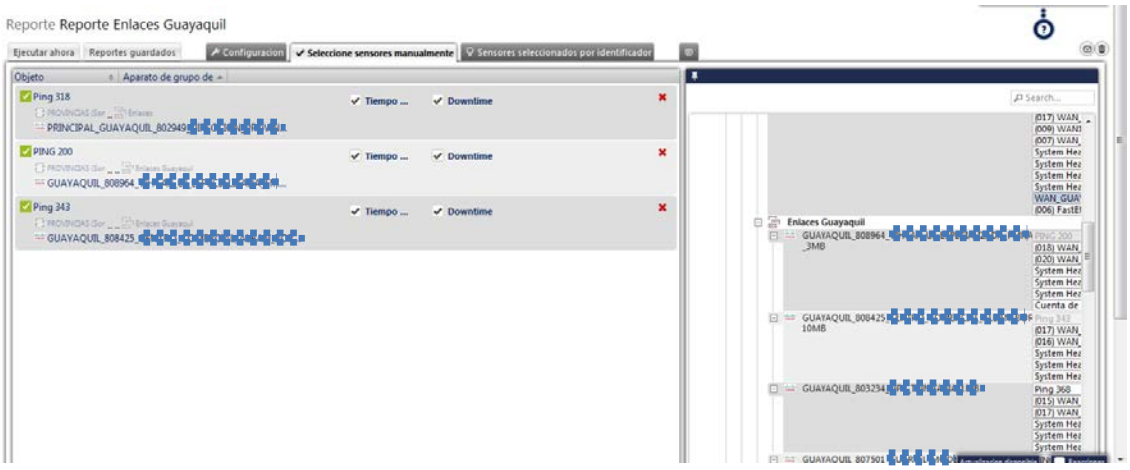


Figura 3.4.- Agregar sensores

3.1.3.1 Ejecución de Reportes

Una vez creado la plantilla de los reportes, es sencillo generar reportes mes a mes esto servirá para realizar contraste de informes con el ISP, así como para medir la disponibilidad del servicio.

Para ejecutar un reporte se debe realizar lo siguiente

- ✓ Ingresamos al menú reportes
- ✓ Elegimos el reporte
- ✓ Definimos las fechas
- ✓ Seleccionamos “Generar, guardar y enviar archivo PDF”

Para visualizar mejor el procedimiento ver la Figura 3.5.

Figura 3.5- Ejecución de reportes

Al recibir el correo electrónico se podrá apreciar el siguiente informe de disponibilidad el cual informa el tiempo de falla y el tiempo disponible, esta información la presenta en % y en tiempo (ver figura 3.6).

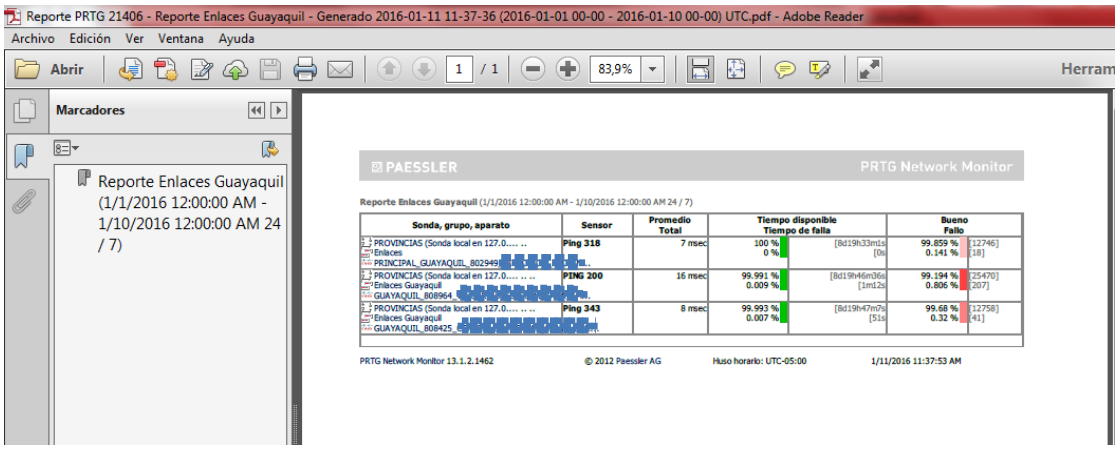


Figura 3.6 Informe de disponibilidad

3.2Pruebas de Análisis de tráfico en la red.

En la ciudad de Guayaquil existen 9 enlaces, cada uno de ellos posee un router entregado por el ISP los cuales deberán ser monitoreados para determinar soluciones para los problemas que se han venido presentando y así garantizar la calidad del servicio.

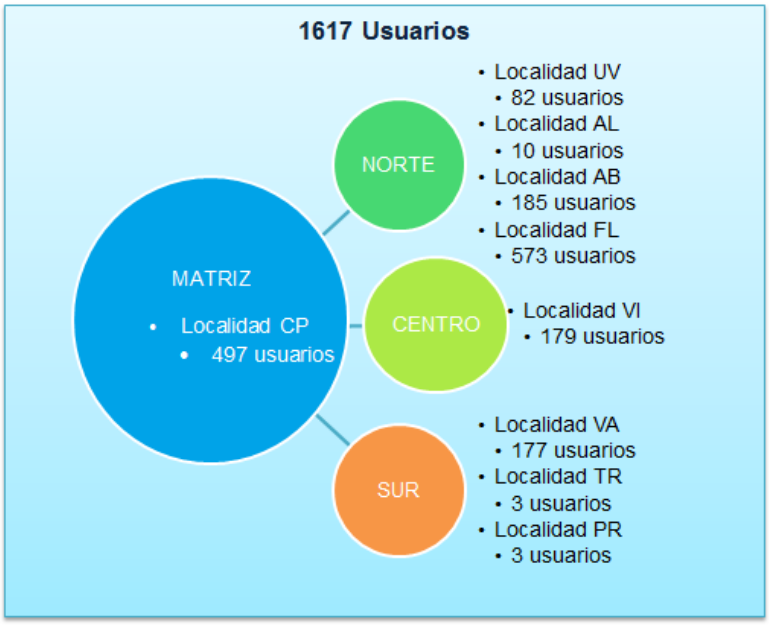


Figura 3.7.-Localidades de la institución

Para realizar esta implementación se basó en el marco teórico de las mejores prácticas de ITIL que nos brinda parámetros (estándares) que nos sirven para asegurar la provisión del servicio basándose en [2]:

1. Gestión de Nivel de Servicio.
2. Gestión Disponibilidad.

3. Gestión de Capacidad.
4. Gestión Financiera.
5. Gestión Continuidad.

La implementación se la dividió en varias fases; se lista las más representativas:

1. Licitación para seleccionar el aplicativo que se utilizará para realizar el escaneo y monitoreo de los componentes de la red de la institución, el favorecido fue “PRTG Network Monitor”, por tratarse de un aplicativo que cumple con el 95% del objetivo del proyecto tanto por el costo y tiempo de implementación.
2. Establecer los objetivos del proyecto y dividiéndolos por entregables y confirmar que los objetivos de este proyecto se apegan a los objetivos ya establecidos por el área.
    a. Seleccionar las diferentes localidades separadas por región y priorizar por las localidades que tienen más quejas sobre lentitud o latencia de los servicios informáticos y las localidades que se encuentren los centros de cómputo principal y alterno.
    b. Realizar un priorización de los servicios prestados por la institución para definir los umbrales de cada aplicativo

para las alarmas a implementar; se dividió en aplicativos que son de uso cotidiano y de mayor concurrencia como principales ya que son los que tienen mayor demanda de consumo y concurrencia.

3. Instalación y configuración del servidor y de la herramienta “PRTG Network Monitor”.
4. Capacitación para el manejo del usuario de la herramienta de monitoreo al personal de TICS.

Figura 3.8.-Arquitectura de Monitoreo de Red

3.3 Análisis de Tráfico Generado.

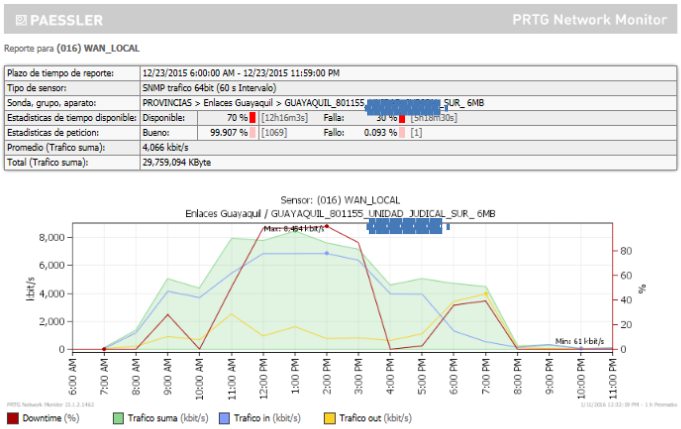
Una de las dependencias ubicadas en el Sur es Valdivia, está conformada por 3 Edificios, de los cuales, existen 177 usuarios laborando, distribuidos entre los 3 edificios. En estos Edificios se brindan los servicios informáticos tales como: internet, telefonía IP, aplicaciones internas de la institución, sistemas biométricos de acceso y marcación, sistema de cámaras IP para vigilancia y videoconferencias. Actualmente cuenta con un enlace de datos de 6Mbps.

3.3.1 Pruebas en escenarios.

- ✓ Prueba con Saturación en el ancho de banda.

  Se ha procedido con la generación de reportes de consumo de ancho de banda de Valdivia ubicada en el sur de la ciudad. El periodo de cual se consideró para este reporte es del día 23/12/2015, el intervalo promedio para la medición es de 1 minuto (60 segundos). Para el análisis únicamente se considera los canales de tráfico In, Out.

Como se aprecia en la gráfica de la figura 3.9 se ve saturación en dicho día, se comienza a registrar el tráfico generado en esa red tanto en el tráfico de entrada como en el tráfico de salida, incrementándose desde las 10:00am hasta las 16:00pm aproximadamente, de tal forma que la línea de Down time nos indica que existió saturación, superando los 6Mb que se tiene contratado para este enlace, esto se configuró en el umbral de manera que cuando supere el valor configurado (6Mb) mostrará la gráfica una línea de falla. Teniendo como estadística de disponibilidad del tiempo en este día el 70% y con una falla de un 30%.Esta información también se la puede apreciar con más detalle y con lapsos de separación de 1 hora.



Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Downtime	Cobertura
12/23/2015 5:00:00 AM – 6:00:00 AM								0 %
12/23/2015 6:00:00 AM – 7:00:00 AM	37,831 KByte	86 kbit/s	19,122 KByte	43 kbit/s	18,709 KByte	42 kbit/s	0 %	100 %
12/23/2015 7:00:00 AM – 8:00:00 AM	608,172 KByte	1,384 kbit/s	515,546 KByte	1,173 kbit/s	92,626 KByte	211 kbit/s	0 %	100 %
12/23/2015 8:00:00 AM – 9:00:00 AM	2,068.945 KByte	5,058 kbit/s	1,695,721 KByte	4,146 kbit/s	373,224 KByte	912 kbit/s	28 %	93 %
12/23/2015 9:00:00 AM – 10:00:00 AM	1,920,274 KByte	4,370 kbit/s	1,622,813 KByte	3,693 kbit/s	297,462 KByte	677 kbit/s	0 %	100 %
12/23/2015 10:00:00 AM – 11:00:00 AM	3,420,761 KByte	7,950 kbit/s	2,335,937 KByte	5,429 kbit/s	1,084,824 KByte	2,521 kbit/s	50 %	100 %
12/23/2015 11:00:00 AM – 12:00:00 PM	3,423,069 KByte	7,790 kbit/s	3,007,891 KByte	6,845 kbit/s	415,177 KByte	945 kbit/s	98 %	100 %

Figura 3.9.-Gráfica Valdivia SUR 23/12/2015

Para nuestra ayuda se ha utilizado el aplicativoExinda para generar un reporte y verificar el tráfico que está pasando por el enlace de Valdivia-Sur,en el cual se aprecia que el consumo significativo se realiza desde todos los equipos finales de Valdivia Sur hacia el Servidor Antivirus de la institución. Ver figura 3.10.

Top 1000 Outbound Conversations on Network 'Guayas'

Internal Host	External Host	Application	Data (MB)	Throughput (kbps)		Flows
				Average	Max	
[redacted]	[redacted]	CIFS	31.696	440.09	539.40	1
[redacted]	[redacted]	CIFS	31.669	463.27	594.43	1
[redacted]	[redacted]	CIFS	31.556	438.15	520.13	1
[redacted]	[redacted]	HTTPS	31.128	425.00	528.12	1
[redacted]	[redacted]	CIFS	31.025	438.20	596.28	1
[redacted]	[redacted]	CIFS	30.917	429.28	459.22	1
[redacted]	[redacted]	CIFS	30.813	458.95	517.72	1
[redacted]	[redacted]	CIFS	30.285	420.50	546.63	1
[redacted]	[redacted]	CIFS	30.264	427.46	521.33	1
[redacted]	[redacted]	CIFS	29.707	405.59	468.43	1
[redacted]	[redacted]	CIFS	28.956	408.98	564.70	1
[redacted]	[redacted]	HTTPS	28.674	939.60	1196.98	1
[redacted]	[redacted]	CIFS	28.310	429.48	523.00	1
[redacted]	[redacted]	CIFS	28.080	410.78	497.10	1
[redacted]	[redacted]	CIFS	28.009	402.54	509.67	1

Figura 3.10.-Gráfica Exinda – Top 8

Conclusión: Se aprecia que en el día que se consideró para este reporte existe saturación constante. Esto se puede apreciar en la gráfica 3.9.

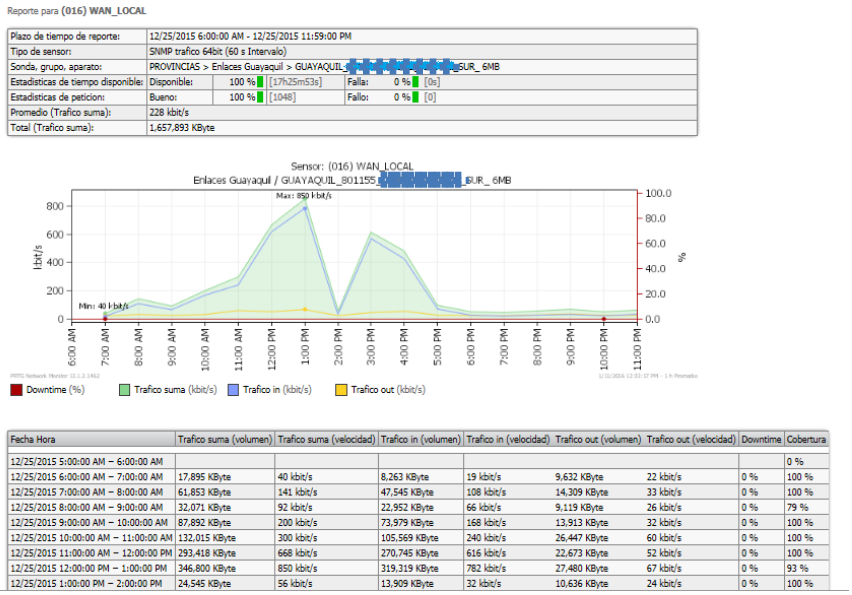
- ✓ Prueba sin Saturación en el ancho de banda.

  Se ha procedido con la generación de consumo de ancho de banda de Valdivia ubicada en el sur de la ciudad. El periodo del cual se consideró para este reporte es del día 25/12/2015, el intervalo promedio para la medición es de 1 minuto (60 segundos). Para el análisis únicamente se considera los canales de tráfico In, Out.

  Como se aprecia en la gráfica de la figura 3.11se comienza a registrar el tráfico generado en esa red tanto en el tráfico de entrada como en el tráfico de salida, de tal forma que la línea de Down time nos indica que no existió saturación, manteniéndose el tráfico por debajo de los 6Mb que se tiene contratado para este enlace. Teniendo como estadística de disponibilidad del tiempo en este día del 100% y con una falla del 0%.

Esta información también se la puede apreciar con más detalle y con lapsos de separación de 1 hora, por lo que podemos decir que la prueba ha sido exitosa.

Conclusión: Se aprecia que en el día que se consideró para este reporte no existe saturación, y sólo se tiene un tráfico por debajo de los 800Kbps, recordemos que en el Ecuador el gobierno declaró feriado nacional y no se laboró en la localidad.. Esto se puede apreciar en la gráfica 3.11.



Reporte para **(016) WAN_LOCAL**

Plazo de tiempo de reporte:	12/25/2015 6:00:00 AM - 12/25/2015 11:59:00 PM			
Tipo de sensor:	SNMP trafico 64bit (60 s Intervalo)			
Sonda, grupo, aparato:	PROVINCIAS > Enlaces Guayaquil > GUAYAQUIL_[redacted]SUR_6MB			
Estadisticas de tiempo disponible:	Disponible:	100 % [17h25m53s]	Falla:	0 % [0s]
Estadisticas de peticion:	Bueno:	100 % [1048]	Fallo:	0 % [0]
Promedio (Trafico suma):	228 kbit/s			
Total (Trafico suma):	1,657,893 KByte			

Sensor: (016) WAN_LOCAL
Enlaces Guayaquil / GUAYAQUIL_801155_[redacted]SUR_6MB

Fecha Hora	Trafico suma (volumen)	Trafico suma (velocidad)	Trafico in (volumen)	Trafico in (velocidad)	Trafico out (volumen)	Trafico out (velocidad)	Downtime	Cobertura
12/25/2015 5:00:00 AM – 6:00:00 AM								0 %
12/25/2015 6:00:00 AM – 7:00:00 AM	17,895 KByte	40 kbit/s	8,263 KByte	19 kbit/s	9,632 KByte	22 kbit/s	0 %	100 %
12/25/2015 7:00:00 AM – 8:00:00 AM	61,853 KByte	141 kbit/s	47,545 KByte	108 kbit/s	14,309 KByte	33 kbit/s	0 %	100 %
12/25/2015 8:00:00 AM – 9:00:00 AM	32,071 KByte	92 kbit/s	22,952 KByte	66 kbit/s	9,119 KByte	26 kbit/s	0 %	79 %
12/25/2015 9:00:00 AM – 10:00:00 AM	87,892 KByte	200 kbit/s	73,979 KByte	168 kbit/s	13,913 KByte	32 kbit/s	0 %	100 %
12/25/2015 10:00:00 AM – 11:00:00 AM	132,015 KByte	300 kbit/s	105,569 KByte	240 kbit/s	26,447 KByte	60 kbit/s	0 %	100 %
12/25/2015 11:00:00 AM – 12:00:00 PM	293,418 KByte	668 kbit/s	270,745 KByte	616 kbit/s	22,673 KByte	52 kbit/s	0 %	100 %
12/25/2015 12:00:00 PM – 1:00:00 PM	346,800 KByte	850 kbit/s	319,319 KByte	782 kbit/s	27,480 KByte	67 kbit/s	0 %	93 %
12/25/2015 1:00:00 PM – 2:00:00 PM	24,545 KByte	56 kbit/s	13,909 KByte	32 kbit/s	10,636 KByte	24 kbit/s	0 %	100 %

Figura 3.11.-Gráfica Valdivia SUR 23/12/2015

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En los últimos años la infraestructura de TI se han vuelto más complejas, para estos crecientes desafíos nos hemos equipado con una solución de monitorización que es PRTG Network Monitor[3], esta herramienta amigable, es de mucha utilidad ya que permite tener siempre una red activa, sin ningún percance, proporcionando una mejor calidad de servicio a los usuarios, reduciendo costos al comprobar el ancho de banda y el equipo necesario y evitando pérdidas causadas por fallos en el sistema.

2. El ganar tranquilidad debido a que mientras no se reciban notificación se puede estar seguro que todo está funcionado correctamente, es

importante ya que de esta manera se puede dedicar a otras tareas importantes.

RECOMENDACIONES

1. Para tener datos de disponibilidad reales se debe visualizar el reporte generado y verificar que contenga los datos correctos sin errores, con el objetivo de realizar un buen trabajo y generar los reportes solicitados de una manera eficaz.

2. Asignar un técnico responsable y presencial por cada localidad configurada, con el cual se tenga contacto para poder realizar las respectivas revisiones de las notificaciones de las alarmas.

3. Al ingresar un servicio al monitoreo de red PRTG, se debe solicitar el acta de entrega de servicio y confirmar con el técnico responsable si la localidad se encuentra en funcionamiento junto con el enlace operativo.

BIBLIOGRAFÍA

[1] Enerit Lean Technology, P RTG Network Monitor, http://www.enerit.net/monitoreo-y-helpdesk/prtg-network-monitor, fecha de consulta Diciembre 2015.

[2] OSIATIS S.A., Fundamentos de la Gestión TI, http://itil.osiatis.es/Curso_ITIL/Gestión_Servicios_TI/fundamentos_de_la_Gestión_TI/que_es_ITIL/que_es_ITIL.php, fecha de consulta Diciembre 2015.

[3] De la Cruz Jorge, PRTG, https://www.jorgedelacruz.es/category/prtg/, fecha de consulta Diciembre 2015.

[4] PAESSLER, PRTG Network Monitor, https://www.es.paessler.com/prtg, fecha de consulta Diciembre 2015.

[5] PAESSLER, PRTG Network Monitor, https://www.es.paessler.com/prtg, fecha de consulta Diciembre 2015.