UNIVERSIDAD DE LOS ANDES
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN
INFRAESTRUCTURA DE COMUNICACIONES
Profesor: Harold Enrique Castro Barrera
hcastro@uniandes.edu.co
Asist. De laboratorio: Laura María Ruiz Gómez
lm.ruizg@uniandes.edu.co

LABORATORIO 4 – MONITORIZACIÓN DE SERVICIOS DE DATOS CON PRTG NETWORK MONITOR

1. OBJETIVO (S)

Realizar una monitorización de los servicios desplegados en una topología de red a pequeña escala, permitiendo una descripción en términos de variables de tráfico y de calidad de servicio entre clientes y servidores. Adicionalmente, conocer de forma más cercana el comportamiento de los distintos protocolos implicados en la prestación de los diferentes servicios. Para este fin se utiliza la herramienta PRTG Network Monitor y se realizarán pruebas de estrés y carga sobre el servidor web, usando la herramienta JMeter.

2. LECTURAS PREVIAS

- Capítulo 9 - Principles of Network Applications. Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th edición.

3. INFORMACIÓN BÁSICA

Para esta práctica utilizará la configuración de laboratorio realizada en la práctica #3. Sobre este escenario usted va configurar y desplegar los servicios de monitoreo utilizando la herramienta PRTG Network Monitor. Con esta herramienta identificará el estado de los servidores, el tráfico de red generado, y el estado de las variables de calidad de servicio.

Se recomienda leer la guía completamente antes de iniciar a resolver las actividades propuestas, con el objetivo de tener presente las actividades y los entregables a desarrollar.

4. PROCEDIMIENTO

PRTG Network Monitor es una aplicación que opera sobre una máquina con sistema operativo Windows para monitorización de redes con sistemas Windows o GNU/Linux. Tiene la capacidad de monitorizar redes LAN, WAN, WLAN y VPNs. PRTG monitoriza la disponibilidad de la red, el uso de Ancho de Banda, Calidad de Servicio, Carga de Memoria, uso de CPU, y otras tantas mediciones. Provee a los administradores de sistemas lecturas en tiempo real, tendencias de uso periódicos para optimizar la eficiencia, distribución y posicionamiento de routers, firewalls, servidores y otros dispositivos de red.

PRTG monitoriza la red utilizando diferentes protocolos como SNMP, WMI, Packet Sniffer y Cisco

NetFlow, entre otros. Tiene la capacidad de grabar constantemente los parámetros de uso de la red y la disponibilidad de los sistemas en la red. Los datos grabados son almacenados en una base de datos interna, para su posterior análisis.

PRTG Network Monitor puede soportar miles de sensores y opcionalmente puede trabajar con múltiples agentes remotos, para monitorizar múltiples sitios o segmentos de red desde un dispositivo central. Está compuesto de dos módulos que ejecutan la monitorización:

- El servidor núcleo (*core)*, el cual se encarga del almacenamiento de datos y del servicio HTTPS. El servicio web permite acceder a los datos guardados desde cualquier máquina, teniendo usuario y contraseña.
- Las sondas. Estas son elementos que agrupan los dispositivos que se quieren monitorizar. En general, hay una sonda por cada ubicación de red que se quiere monitorizar; así, los elementos de red que pertenecen a una misma red se agrupan bajo una misma sonda. Las sondas se dividen en sonda local y sondas remotas.

PRTG usa una organización jerárquica para cumplir con su objetivo. Así, una implementación del software de monitorización posee un servidor núcleo (*core*) que tiene cierto número de sondas, las cuales a su vez poseen dispositivos y estos dispositivos poseen sensores. Estos sensores realizan el seguimiento de parámetros específicos para cada aparato, como los mencionados anteriormente (ancho de banda, tiempos de respuesta, etc.).

Las sondas (grupo de dispositivos y sensores) monitorizan autónomamente y envían el resultado de la monitorización al servidor *core*. Si la conexión entre el servidor y la sonda falla, ésta sigue monitorizando y almacena temporalmente los resultados, hasta reanudar la comunicación con el servidor.

La conexión entre la sonda y el servidor es iniciada por la sonda y es asegurada por el protocolo SSL, lo cual quiere decir que los datos compartidos por el servidor y la sonda se envían encriptados. El servidor provee un puerto TCP/IP abierto que espera permanentemente solicitudes de las sondas. Como precaución de seguridad, las sondas deben ser manualmente reconocidas por el administrador antes de que cualquier sensor pueda ser creado y monitorizado. El administrador puede rechazar una sonda y desconectarla.

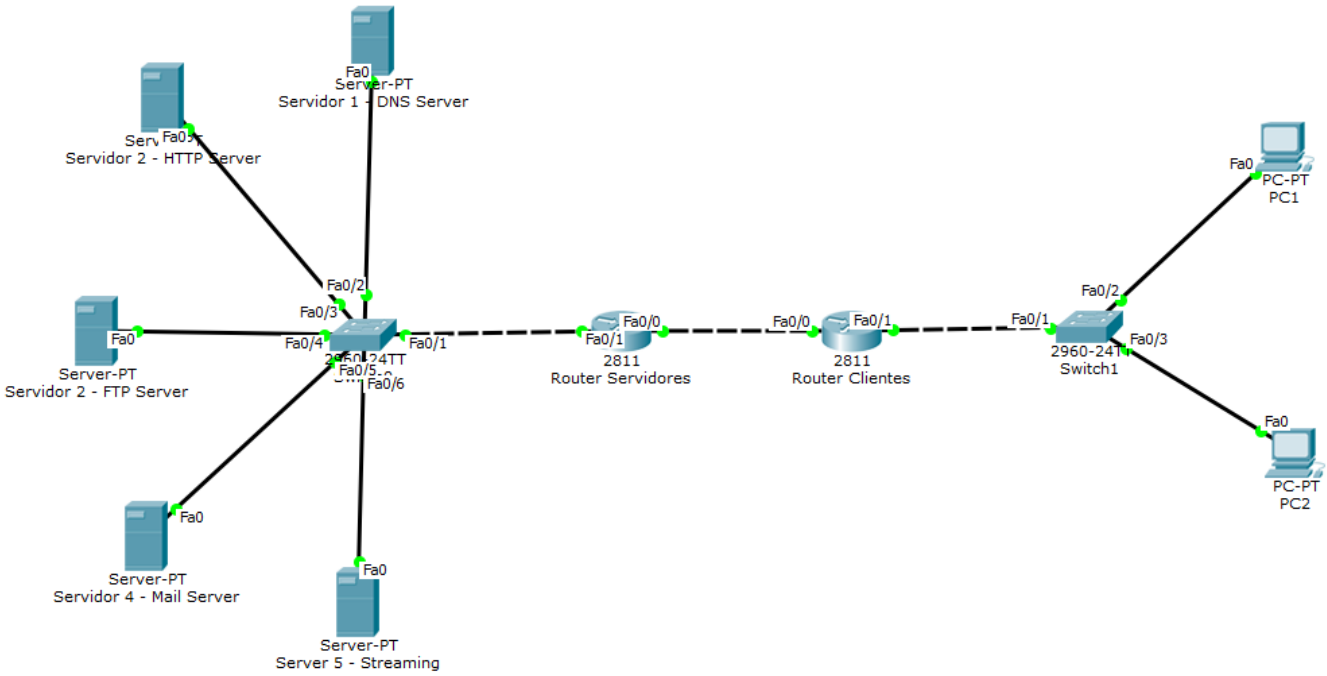
PRTG crea la primera sonda automáticamente, llamada sonda local (*Local probe*). Esta se ejecuta sobre la misma máquina del servidor *core* y realiza la monitorización de todos los sensores. Una sonda local tiene la capacidad de monitorización de una red LAN. Esta sonda se conecta al servidor mediante la dirección "localhost" (127.0.0.1) y SSL.

NOTA: Este documento describe únicamente lo referente a los requerimientos de monitorización de los servicios. Los servicios en cada uno de los servidores fueron implementados en la práctica anterior (Laboratorio #3) y deben estar funcionando antes de comenzar este laboratorio. Sin embargo, hay que tener en cuenta que eventualmente habrá que cambiar algunos parámetros de la configuración en las máquinas para funcionar dentro de la topología.

Este laboratorio presenta una topología de red real a pequeña escala, donde se integran equipos de cómputo que ofrecen diferentes servicios (HTTP, DNS, FTP, SMTP y POP3 o IMAP) y clientes que utilizan los servicios disponibles para consumir recursos informáticos y generar tráfico en la red. Sobre esta infraestructura usted instalará, configurará y desplegará los servicios de análisis y monitoreo de PRGT Network Monitor.

Como segunda parte de la práctica se utilizará la herramienta Apache JMeter. Esta es una aplicación hecha en Java que soporta diferentes tipos de pruebas (entre ellas, de performance, de carga, de estrés) sobre distintos tipos de recursos - estáticos y dinámicos - sobre aplicaciones y sobre servidores. Con esta aplicación se realizarán pruebas de carga y de estrés sobre un servidor web (http) previamente configurado.

La imagen a continuación muestra la topología que se utiliza en el desarrollo del documento, incluyendo las funcionalidades asignadas a los dispositivos:



Topología de laboratorio utilizada para la monitorización de tráfico y análisis de protocolos de red

TABLA DE DIRECCIONAMIENTO					
Dispositivo	Interfaz de Red	URL	Dirección IP	Mascara de Subred	Gateway Predeterminado
Servidor 1 - DNS Server	NIC	dns.labredes.com	192.168.10.**X+1**	255.255.255.0	192.168.10.1
Servidor 2 - HTTP Server	NIC	web.labredes.com	192.168.10.**X+2**	255.255.255.0	192.168.10.1
Servidor 3 - FTP Server	NIC	ftp.labredes.com	192.168.10.**X+3**	255.255.255.0	192.168.10.1
Servidor 4 - Mail Server	NIC	mail.labredes.com	192.168.10.**X+4**	255.255.255.0	192.168.10.1
Servidor 5 - Streaming	NIC	streaming.labredes.com	192.168.10.**X+5**	255.255.255.0	192.168.10.1
PC - Usuario 1 a Usuario 48	NIC	No aplicable	192.168.20.**X+1** y 192.268.20.**x+2**	255.255.255.0	192.168.20.1
Router de Servicios	FastEthernet 0/0	No aplicable	192.168.30.1	255.255.255.0	No aplicable
	FastEthernet 0/1	No aplicable	192.168.10.1	255.255.255.0	No aplicable
Router de Clientes	FastEthernet 0/0	No aplicable	192.168.30.2	255.255.255.0	No aplicable
	FastEthernet 0/1	No aplicable	192.168.20.1	255.255.255.0	No aplicable

Nota: La **X** que aparece en la tabla de direccionamiento debe ser reemplazada con el número de grupo que le fue asignado (Ejemplo: para el Grupo 1: 192.168.10.**X+1** ->192.168.10.**2**).

En esta topología las máquinas de Servidores y Usuarios representan máquinas virtuales que usted deberá desplegar sobre las maquinas disponibles en el laboratorio de Redes e Interconectividad ML340. Deberá usar dos equipos, uno disponible en el laboratorio con dos tarjetas de red y un equipo que deberá traer el grupo de estudiantes para correr dichas máquinas virtuales, en la máquina del grupo correrá los clientes, y en la que se encuentra en el laboratorio los servidores.

Es necesario para tener acceso a la infraestructura, conectar los cables de red de los equipos de trabajo al punto de red 5 y 6 del Patch Panel asociado a su puesto de trabajo. El puerto de red 5 le brinda acceso al equipo que soporta las máquinas virtuales de los clientes que se encuentran en la red 192.168.20.0 y el puerto de red 6 tiene acceso a la red de los servidores 192.168.10.0.

4.1. Requerimientos para el despliegue del servicio PRTG Network Monitor

Nota: En esta sección y la siguiente se pedirá tomar capturas de distintas variables monitorizadas en la red y del proceso para generar el tráfico. **Guardar estas capturas**, ya que serán necesarias para el laboratorio.

El procedimiento de monitorización se realiza sobre la topología de red mostrada anteriormente, la cual está instalada sobre la tecnología para virtualización VMWare WorkStation u Oracle VM Virtualbox.

El Servidor Core y la sonda local del software PRTG para monitorización deberán ser instalados en el servidor dns.grupoXlabredes.com (192.168.10.X+1), el cual es adicionalmente el servidor DNS de la infraestructura y maneja las zonas de resolución directa e inversa el dominio grupoXlabredes.com. Los principales generadores de tráfico son los servidores web.grupoXlabredes.com, ftp.grupoXlabredes.com. El servidor web.grupoXlabredes.com (192.168.10.X+2) presta los servicios web sobre TCP; el servidor ftp.grupoXlabredes.com (192.168.10.X+3) tiene configurado e instalado el servicio de transferencia de archivos FTP y los demás servicios desplegados en el laboratorio 3.

A cada uno de los clientes, los cuales están ubicados en la red 192.168.20.0/24, se le debe instalar una sonda remota PRTG siguiendo las indicaciones dadas en las referencias.

Para realizar la monitorización, primero se debe generar tráfico en la red desde uno o varios de los equipos cliente, haciendo peticiones DNS, HTTP, FTP, SMB, SMTP y POP3. Estos procedimientos de describen a continuación.

1. Descargar PRTG Network Monitor del sitio web oficial del fabricante.
   http://www.paessler.com

2. Instalar el servidor PRTG Network Monitor sobre la maquina Windows Server que provee el servicio DNS.

3. Utilice sondas remotas para obtener los valores de las diferentes variables a medir. Incluir, según corresponda a cada dispositivo los sensores necesarios para identificar el estado de las variables:
   a. Sensores locales de Carga: Disco, Procesador, Memoria, Interfaces para cada uno de los servidores.
   b. Sensores locales y Sensor de Ping para el Cliente en Windows 7.
   c. Sensor de Ping y Sensor Trafico HTTP al Servidor Web.
   d. Sensor de Ping y Sensor Trafico DNS al Servidor DNS.

e. Sensor de Ping y Sensor Trafico FTP, SMB o SAMBA al Servidor de Archivos.
f. Sensor de Ping y Sensor Trafico SMTP, POP3 o IMAP al Servidor Correo.
g. Sensor de Ping y Sensor Trafico a las interfaces locales de los enrutadores.

1. **Realizar un análisis de las medidas obtenidas; indicar si hubo problemas en términos de disponibilidad y rendimiento, y establecer las soluciones a los mismos, o establecer las mejoras que se podrían establecer en la topología de red.**

2. **Los sensores de ancho de banda miden la cantidad de tráfico que pasa por una interfaz de red. ¿En las topologías usadas, éste tráfico se debe únicamente a las peticiones FTP, HTTP, RTSP y DNS?**

3. **Explicar algunos de los mensajes mostrados en alarmas y logs, relacionados con su equipo cliente. ¿Qué información adicional a la obtenida de las capturas muestran estos mensajes, en el caso específico de la topología usada?**

4. **¿Qué cambios deberían observarse en las variables de calidad de servicio (sensores DNS, HTTP, FTP, SMTP, POP3, SMB o SAMBA) al aumentar/disminuir la velocidad de transmisión del canal WAN y mantener la demanda de servicios?**

4.2. Pruebas con JMeter

1. Instalar la aplicación JMeter en la máquina cliente.

2. Establecer y ejecutar un plan de pruebas para análisis de carga y de estrés sobre el servidor Web. Se debe discriminar y justificar la escogencia de factores como número de pruebas, número de hilos de ejecución (threads), elementos que conforman las pruebas (receptores, muestreadores, etc.).

5. **Explicar las condiciones asumidas en cada caso en el informe de laboratorio.**

6. **Tomar capturas de pantalla de los diferentes resultados obtenidos (dependiendo de los receptores escogidos); realizar un análisis de estos resultados, en especial mencionar cómo estos resultados ayudan a establecer parámetros del servicio Web, como por ejemplo, tráfico máximo soportado, número de usuarios soportados por unidad de tiempo u otros.**

7. **¿Permiten los resultados obtenidos plantear modificaciones sobre el servidor que mejoren su comportamiento, en términos de rendimiento y disponibilidad?**

8. **De acuerdo a los resultados obtenidos, proponer mejores prácticas de diseño en la topología de red, teniendo en cuenta los servicios de datos que se ofrecen. Para esto especificar cuál sería el nuevo diseño de red (ubicación de los servicios, conexiones entre estos, servicios de red adicionales, buenas prácticas a nivel de seguridad, etc.) para cumplir con mejores condiciones de prestación de los servicios. Adicionalmente, enumere y justifique los aspectos más importantes de la infraestructura que un prestador de servicios debe tener en cuenta al ofrecer servicios por Internet.**

6. ENTREGABLES

Informe de Laboratorio con:

- Documentación de las diferentes pruebas realizadas a la topología de laboratorio.
- Descripciones solicitadas.
- Respuestas a las preguntas planteadas (informe).

Utilizar como referencia para la presentación de informes de laboratorio el documento "Normas de estilo para presentación de documentos y reportes técnicos en informática", disponible en Sicua+.

7. REFERENCIAS

[1] Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th ed.
[2] Documentación Oficial PRTG Network Monitor
[3] JMeter User Manual

8. REFERENCIAS WEB

[4] Web Oficial PRTG - http://www.paessler.com
[5] Web Oficial JMeter - http://jmeter.apache.org

HISTORIAL DE REVISIONES

FECHA	AUTOR	OBSERVACIONES
15/01/2015	**Jesse Padilla Agudelo** pa.jesse10@uniandes.edu.co	Versión inicial del documento. Trabajo derivado de las guías de laboratorio PRTG y Wireshark e Implementación de servicios y análisis de tráfico sobre sistemas Linux: instalación y configuración. Diseñada por Eliana Bohórquez y Rodolfo Cáliz.
24/07/2015	**Laura María Ruiz Gómez** lm.ruizg@uniandes.edu.co	Modificaciones en la topología de la red. Correcciones de redacción y estilo.
03/03/2017	**Laura María Ruiz Gómez** lm.ruizg@uniandes.edu.co	Modificaciones en la topología de la red. Correcciones de estilo menores.