

**ESCUELA POLITÉCNICA NACIONAL**  
**FACULTAD DE ELÉCTRICA Y ELECTRÓNICA**  
**REDES DE COMUNICACIONES ÓPTICAS**



**TALLER #7**

**INTEGRANTES:**

- Ronaldo Almachi
- Jonathan Chávez
- Francisco Salazar
- Danilo Vásconez

**TEMA:** Verificar la capacidad del canal en una red (óptica) de comunicaciones.

**PERIÓDO:** 2021-A

Contenido	
Introducción.....	3
Jperf.....	3
PRTG Network Monitor .....	4
Wireshark .....	5
Equipos y Herramientas.....	5
Generación y sensado de tráfico .....	5
Monitoreo con PRTG .....	8
Referencias .....	13

## Introducción

### Jperf

Es una interfaz gráfica de usuario basada en Java que permite utilizar el popular programa iperf para medir la velocidad máxima entre dos equipos. Sirve para medir el rendimiento que se obtiene en las pruebas LAN-LAN, LAN-WAN y también pruebas WiFi. [1]

Iperf es compatible tanto con el protocolo TCP como el protocolo UDP, además, se puede configurar el tamaño de ventana TCP y otros parámetros muy avanzados como el buffer, el tamaño máximo del segmento y más. Se puede mostrar la velocidad en diferentes unidades de medida, como en Mbits, MBytes, Gbps y otras, además, configurar el intervalo de reporte de los datos, la duración de la prueba, e incluso los streams paralelos a enviar. Al utilizar TCP y UDP, se debe definir el mismo puerto TCP o UDP tanto en el servidor como en el cliente, de lo contrario, no podrán comunicarse el cliente con el servidor. Por supuesto, este programa es compatible tanto con redes IPv4 como también con redes IPv6. [1]

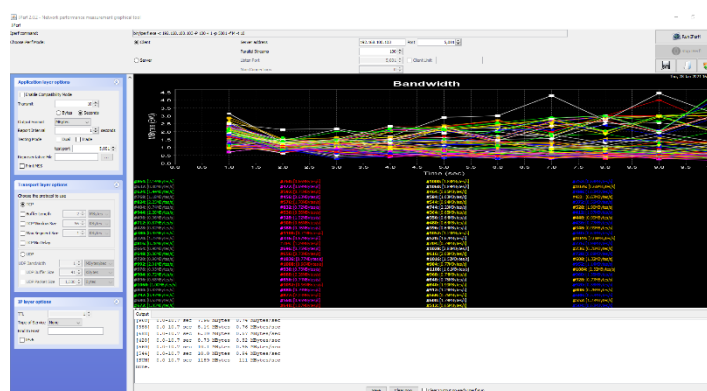


Fig. 1. Interfaz gráfica Jperf. [1]

### Características: [1]

- Permite medir el ancho de banda entre dos hosts, ya sean cableados, inalámbricos o a través de Internet.
- Permite ver en tiempo real cómo se transfieren los datos
- Permite configurar diferentes hilos TCP simultáneamente, para comprobar el rendimiento con muchas conexiones concurrentes.
- Soporta UDP, se puede transferir tráfico UDP con varios hilos concurrentes para exprimir el ancho de banda de la red local
- Permite la visualización de los datos en Mbps y Gbps, ideal para redes de alta velocidad.
- No se recomienda usar este programa para redes Multigigabit o superiores a 1 Gbps, en su lugar, es mejor utilizar el programa iperf3.
- Permite medir la velocidad de subida (por defecto), la velocidad de subida y descarga (por separado, primero se comprueba la velocidad de subida y luego de descarga), y finalmente también deja configurar la medición de descarga y subida de forma simultánea.
- Modificar la ventana TCP en el sistema operativo.
- Permite configurar tanto servidor Iperf como cliente Iperf, definiendo direcciones IP y puertos cuando sea necesario, dependiendo de lo que hayamos elegido.
- Es compatible con sistemas operativos Windows, Linux y macOS, al estar basado en Java podremos tener la posibilidad de ejecutarlo en diferentes sistemas operativos.
- Internamente utiliza iperf2 para la comunicación, realmente jPerf es una interfaz gráfica de usuario basada en Java.

## PRTG Network Monitor

La herramienta PRTG Network Monitor es una solución de monitorización “Todo en Uno” y libre de agentes (no necesita instalar ningún agente externo en el equipo a monitorizar). Combina tecnologías estándares de monitoreo (SNMP, WMI, NetFlow, JFlow, entre otros) con una completa serie de características fáciles de usar. A través de una interfaz intuitiva y tecnología de última generación, se adecua como una solución ideal para redes de cualquier tamaño, desde empresas pequeñas hasta grandes corporaciones. [2]

Funciona con una sola licencia, sin costos ocultos, sin complementos y sin complejidad para el usuario final. PRTG asegura la disponibilidad de los componentes de red, mide su tráfico y su uso, reduce costos evitando interrupciones, optimizando las conexiones, ahorrando tiempo y controlando los Acuerdos de Nivel de Servicio (SLAs). [2]

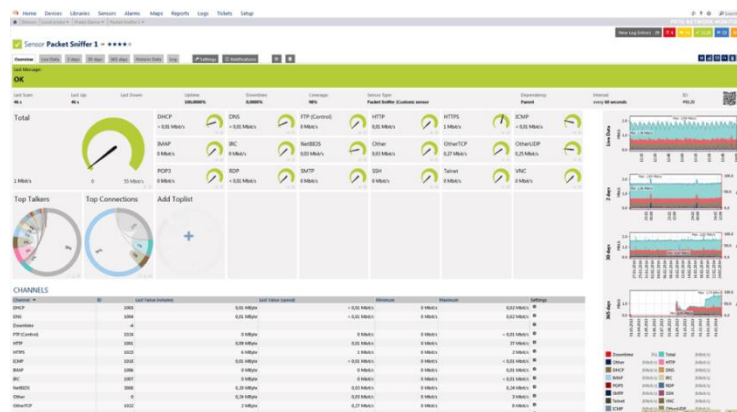


Fig. 2. Interfaz gráfica de PRTG. [2]

### Características: [2]

- El tráfico en la red interna y hacia/desde internet.
- Verifique su ancho de banda contratado ya sea en soluciones de internet como enlaces dedicados punto a punto.
- El rendimiento y las características (estado de puertos, trafico, estado de VPN, tiempos de respuesta, QoS, autenticación, etc) de sus equipos de red (switches, routers, Access points, firewalls, módems, etc.)
- Las características y el rendimiento de sus servidores físicos (Discos, arreglos RAID, estado del procesador, memoria RAM, fuentes de poder, ventiladores, etc.)
- El rendimiento y las características de funcionamiento de sus S.O. de servidores (GNU/Linux, Windows Server, etc.)
- El funcionamiento de sus aplicaciones y páginas web (servidores web (IIS/Apache), ingresos, autenticaciones, tiempos de respuesta, chequeos de contenido, etc.)
- El rendimiento de sus bases de datos (Microsoft SQL, PostgreSQL, Oracle, MySQL, MongoDB, supervisión por conexiones ADO, conexiones, sesiones y otros.)
- Servidores de archivo (archivos, directorios, cuotas, sistemas NetApp, servidores FTP, etc.)
- Servidores de correo (Exchange, SMTP, IMAP, POP3, etc).
- Sistemas de virtualización (Hyper-V, VMware, Citrix Xen Server, Virtuozzo, Amazon CloudWatch, etc.)
- Servidores de autenticación (LDAP, RADIUS, Active Directory).
- Cualquier dispositivo, aplicación, servicio o servidor compatible con la tecnología de SNMP (v1, v2, v2c, v3), WMI, Netflow, SSH, JSON, entre otros.

## Wireshark

Es un analizador de protocolos open-source que actualmente está disponible para plataformas Windows y Unix. Su principal objetivo es el análisis de tráfico, pero además es una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red. Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. Gracias a que Wireshark “entiende” la estructura de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico. [3]



Fig. 3. Logo de Wireshark. [3]

## Equipos y Herramientas

- Computadora personal
- Virtual Box/ VMware
- Wireshark
- Prtg
- Jperf
- S.O.
  - Windows 7
  - Windows 10
  - Kali Linux

## Generación y sensado de tráfico

**Verificar la capacidad (física/lógica) de una red de comunicaciones a través de la generación y sensado de tráfico.**

### *Monitoreo con jperf*

En primer lugar, vamos a realizar la generación y sensado de tráfico con Jperf. Para esto se instaló el mencionado software en el ordenador que tiene sistema operativo de Windows 10, y una máquina virtual con sistema operativo Kali Linux. Con este software fue posible saber la capacidad del canal que se tiene enlazado entre ambas máquinas, además se realizó la prueba con protocolo TCP y UDP. La computadora de Windows 10 fue configurada como el cliente, mientras que la máquina virtual de Kali fue configurada como Server. Para comprobar se realizó captura de tráfico mediante Wireshark. Lo que se obtuvo fue lo siguiente:

## Protocolo TCP

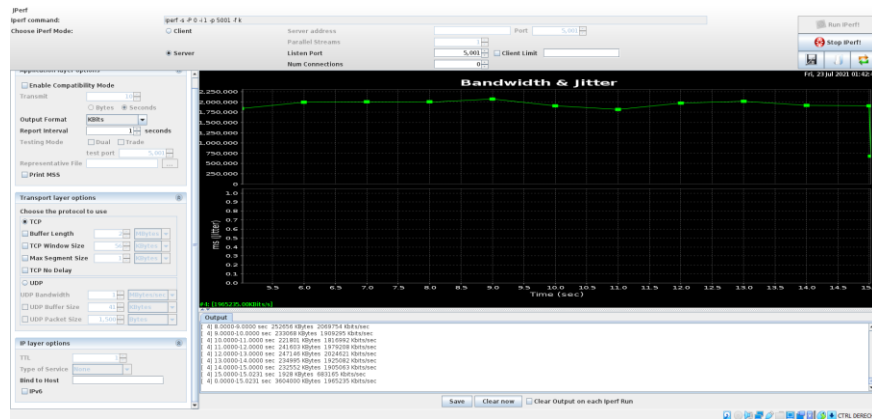


Fig. 4. Server

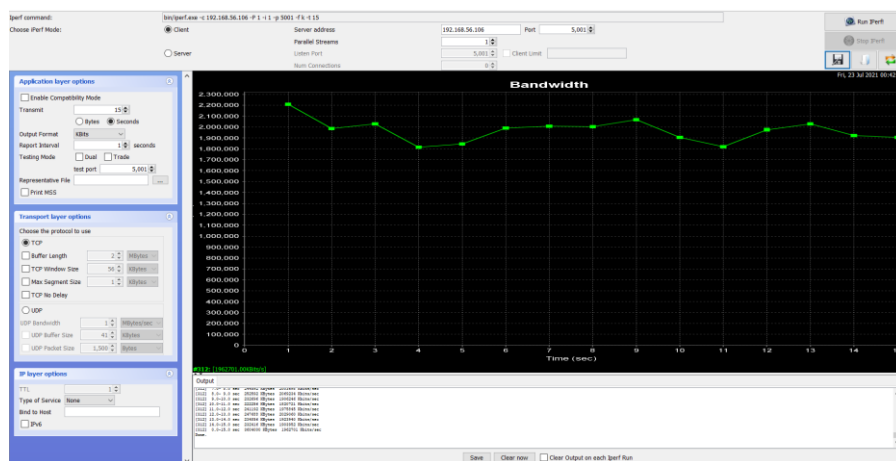


Fig. 5. Cliente

Observando ambas gráficas se puede decir que el ancho de banda (capacidad del canal) está entre 1.8 Mbts/seg hasta 2.2 Mbts/seg desde el cliente. En la Fig. 6 observamos el tráfico capturado por Wireshark, mismo que captó todos los paquetes TCP que se transportaron por el canal. Esta prueba nos indicó que es posible hacer la transmisión de paquetes TCP entre distintas máquinas, estas máquinas se encuentran en la misma red por lo cual resultó sencillo hacer la conexión entre máquinas. Sin embargo, se conoce de la posibilidad de realizar la conexión entre máquinas con direcciones IPv6, sin embargo para el presente taller la prueba realizada con IPv6 no fue exitosa. En la captura realizada por Wireshark podemos analizar los paquetes que fueron transmitidos, sus tramas, protocolo y toda la información que este software nos brinda, siendo el de análisis de tráfico más usado.

No.	Time	Source	Destination	Protocol	Length	Info
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698454162 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [PSH, ACK] Seq=3698454162 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698454222 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698454682 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698457942 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698459202 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698460462 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698461722 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [PSH, ACK] Seq=3698462982 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698464242 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698465502 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698466762 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698468022 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698469282 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [PSH, ACK] Seq=3698470542 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698471802 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698473062 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698474322 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698475582 Ack=1 Win=2186624 Len=1200
2436	19.727417	192.168.56.1	192.168.56.106	TCP	1114	28167 → 5001 [ACK] Seq=3698476842 Ack=1 Win=2186624 Len=1200

Fig. 6. Tráfico TCP

## Protocolo UDP

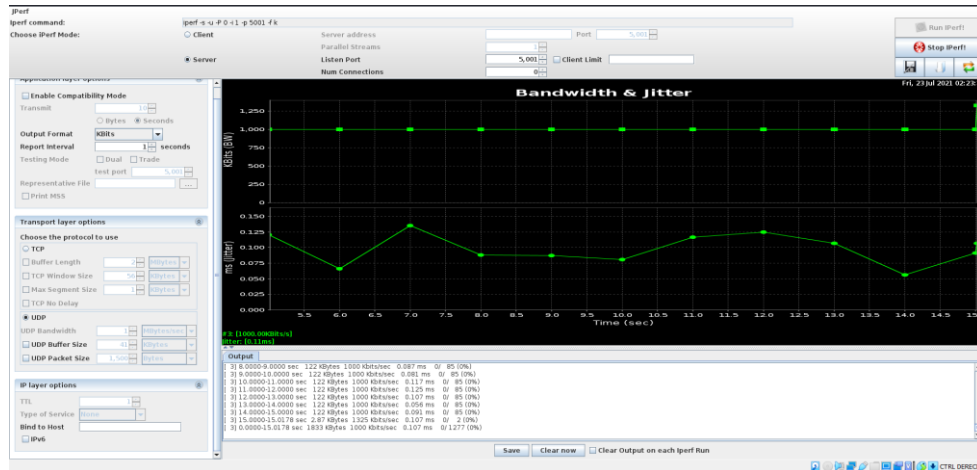


Fig. 7. Server

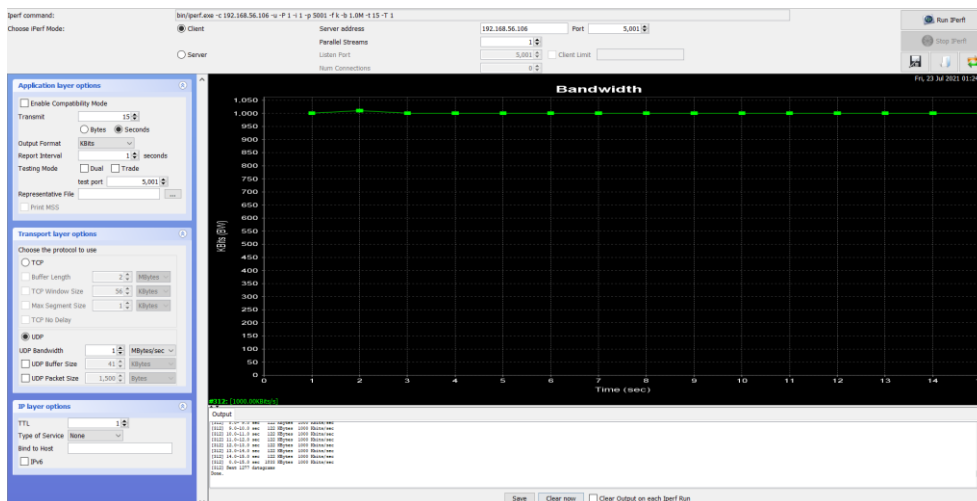


Fig. 8. Cliente

En esta ocasión con el protocolo UDP observamos que en la máquina server obtiene la gráfica del jitter que había presente en el canal. Además, su capacidad de canal es más regular que con TCP, dando así una capacidad de 1 Mbit/seg. En la captura de tráfico se puede observar que se envían los paquetes de UDP acompañados con paquetes de IPv4. Se puede observar que el comportamiento del canal es distinto dependiendo del tipo de paquetes que este transporta, teniendo como dato importante que en UDP existe jitter. Además, se dice que la eficiencia del transporte en ambos tipos de tráfico es eficientes, pues no hay señal de pérdidas, sin embargo esto en la realidad es utópico.

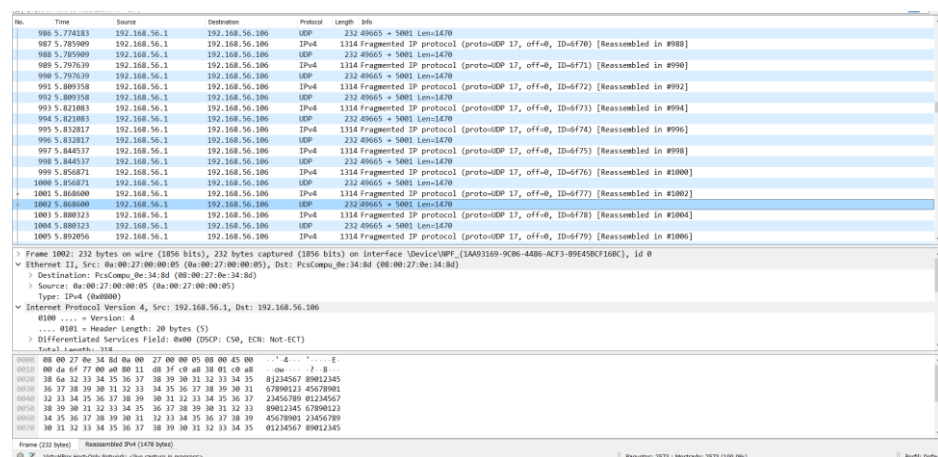


Fig. 9. Tráfico UDP

## Monitoreo con PRTG

PRTG es un software de monitoreo de red que requiere conexión a internet, también se tiene una herramienta offline que funciona muy bien en Windows, por lo que usaremos 2 máquinas virtuales, en Windows 10 se tendrá el software de monitoreo PRTG, mientras que Kali Linux será nuestro dispositivo para monitorear, para hacer esto es necesario crear una red interna entre las dos máquinas, esto es una ventaja que nos ofrece Virtual Box.

A continuación, se presenta las direcciones IP de la red interna creada para el monitoreo.

```
Ethernet adapter Ethernet:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::78e9:d629:2390:3ecb%5  
IPv4 Address . . . . . : 192.168.191.2  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.191.254
```

Fig. 10 Dirección IP de la red interna para Windows 10

```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
group default qlen 1000  
link/ether 08:00:27:12:9a:6f brd ff:ff:ff:ff:ff:ff  
inet 192.168.191.1/24 brd 192.168.191.255 scope global eth1  
    valid_lft forever preferred_lft forever  
inet6 fe80::a00:27ff:fe12:9a6f/64 scope link  
    valid_lft forever preferred_lft forever
```

Fig. 11 Dirección IP de la red interna para Kali Linux

## Instalación de PRTG

La instalación en PRTG es muy sencilla en Windows ya que únicamente vamos a descargar un ejecutable de manera gratuita, que tiene una prueba gratuita sin límites de 30 días.

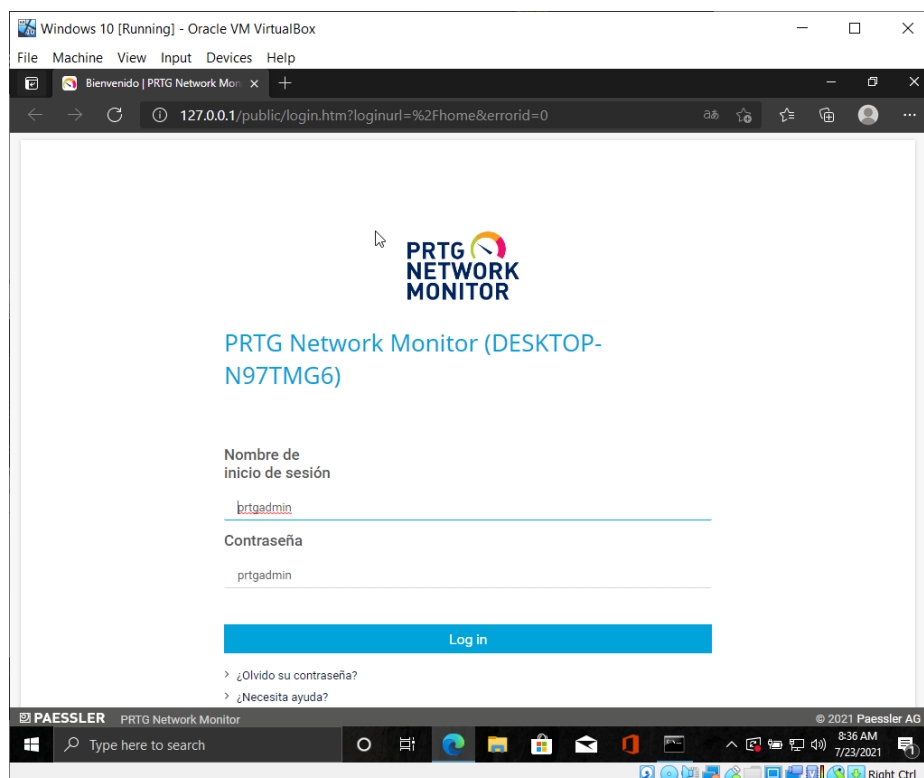


Fig. 12 PRTG ejecutándose en Windows

## Uso de PRTG



Es muy sencillo usar PRTG ya que es una herramienta que nos permite la detección automática de dispositivos en red , además que se añaden automática los sensores disponibles, tal y como se lo puede ver en la figura 13 y 14

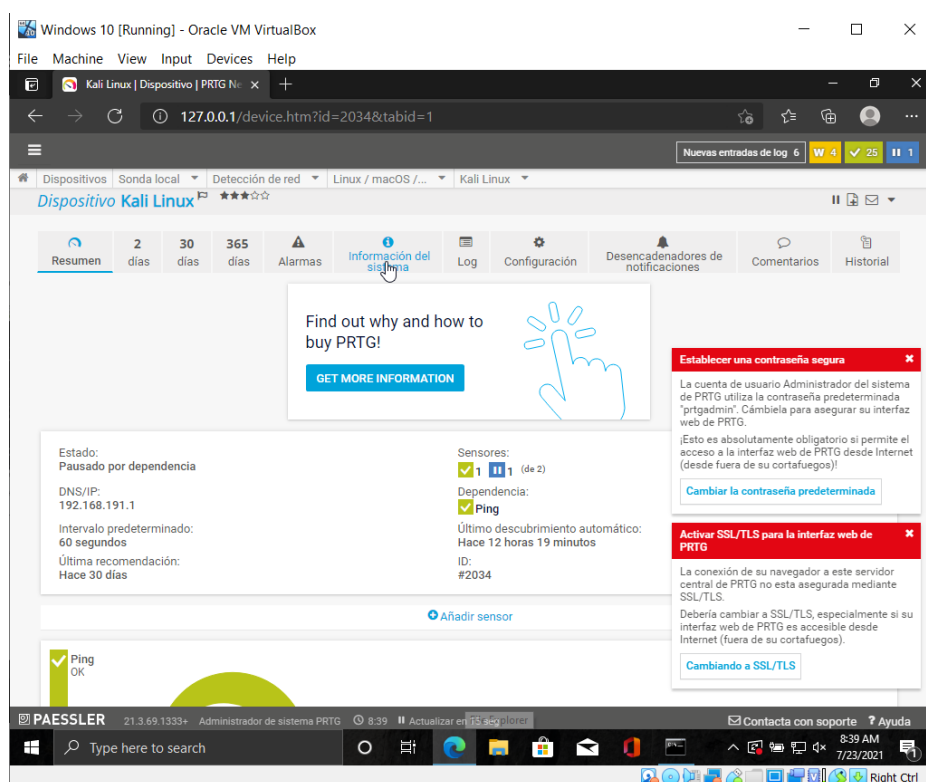


Fig. 13 Sensor ping con la dirección IP de Kali Linux

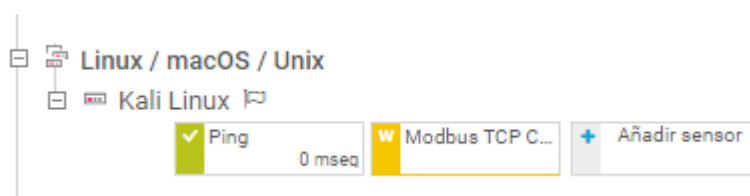


Fig. 14 Dispositivo activo con un sensor ping

A continuación, tenemos los detalles de la conexión referentes al tiempo y sensado con respecto a la herramienta PING

Último escaneo: 57 s	Último OK: 57 s	Último fallo: 4 d 2 h 9 m	Tiempo disponible: 84.4621%
Tiempo de fallo: 15.5379%	Cobertura: 3%	Tipo de sensor: Ping	Repercusión en el rendimiento: <div><div></div><div></div><div></div><div></div><div></div></div>
Dependencia: Linux / macOS / Unix	Intervalo: 30 s	Autonomous: No	ID: #2038

Fig. 15 Detalles del escaneo con el sensor ping

También se tiene un grafico en tiempo real en donde se puede apreciar la velocidad máxima alcanzada por el sensor, el pico mas alto se refiere a la primera conexión, ya después de eso la conexión se mantiene estable.

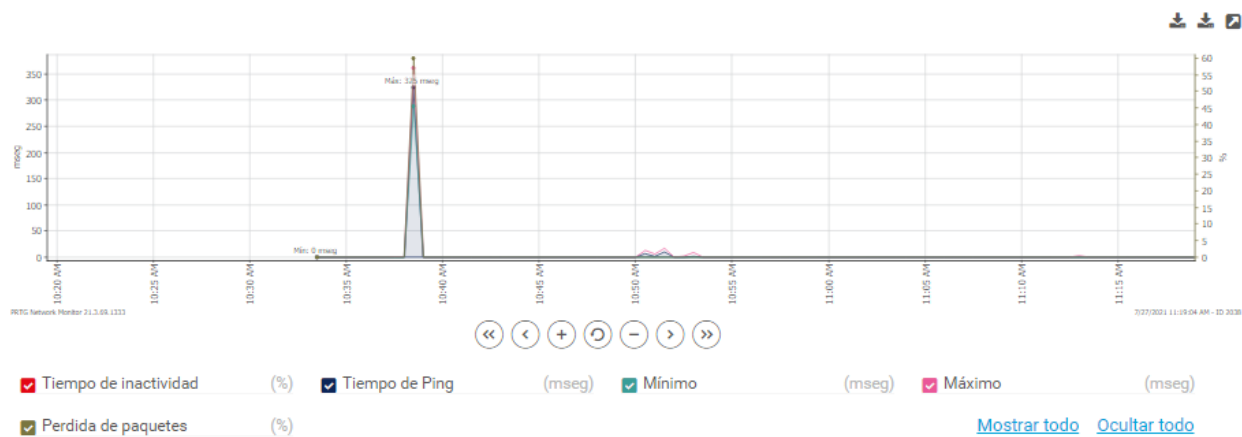


Fig. 16 Grafico en tiempo real del sensor PING

PRTG nos ofrece un registro de conexiones, ya que constantemente está en ejecución se puede apreciar un registro detallado con hora y fecha de cuando se hizo la conexión, además de un estimado de los paquetes perdidos.

Fecha Hora	Tiempo de Ping	Mínimo	Máximo	Perdida de paquetes	Tiempo de inactividad	Cobertura
7/27/2021 11:17:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:17:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:16:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:16:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:15:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:15:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:14:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:14:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:13:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:13:03 AM	1 mseg	0 mseg	3 mseg	0 %	0 %	100 %
7/27/2021 11:12:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:12:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:11:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:11:03 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %
7/27/2021 11:10:33 AM	0 mseg	0 mseg	0 mseg	0 %	0 %	100 %

Fig. 17 Registro de conexión del sensor PING

PRTG nos ofrece un monitoreo de red local, es decir en este apartado se tiene múltiples sensores como lo son HTTP y Ping, de manera general, si se requiere un sensor para un protocolo en específico se puede añadir sin problema, pero se debe considerar que al estar constantemente funcionando consume recursos lo que puede hacer que la Windows 10 se haga lento.

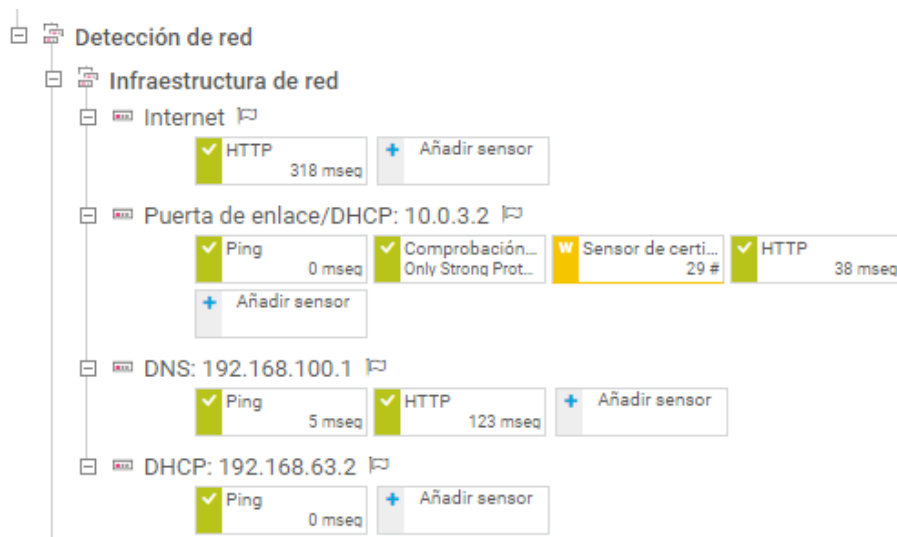


Fig. 18 Detección automática de la red, Internet

En la figura 19 y 20, tenemos los detalles del sensor HTTP, aquí tenemos la velocidad con la que ingresamos a una página web de manera general, esto se puede corroborar con la gráfica en tiempo real.

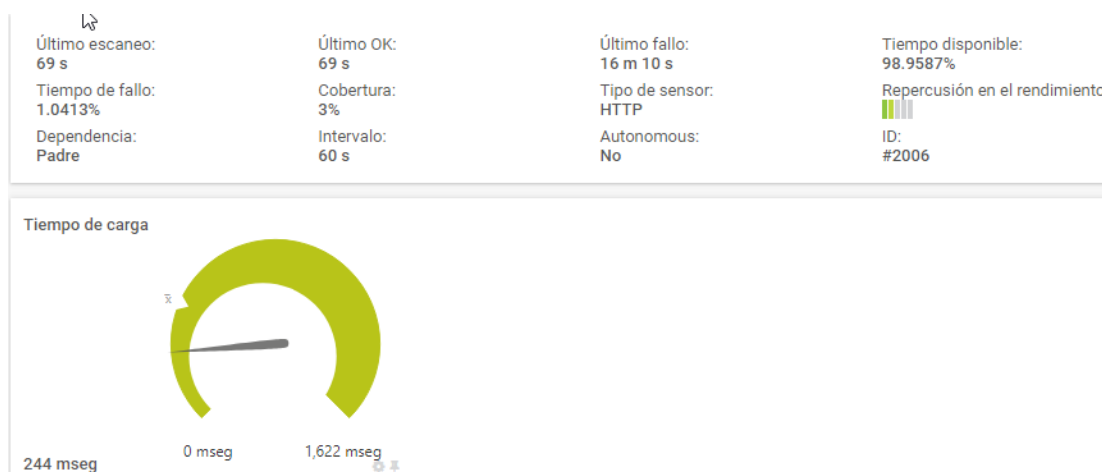


Fig. 19 Detalles del sensor HTTP



Fig. 20 Grafico en tiempo real del sensor HTTP

En este caso se puede notar que cuando existe algún error de conexión este se registra con detalles en PRTG, tal y como muestra en la figura 21.

Fecha Hora	Tiempo de carga	Tiempo de inactividad	Cobertura
7/27/2021 10:56:38 AM	255 mseg	0 %	100 %
7/27/2021 10:55:38 AM	211 mseg	0 %	100 %
7/27/2021 10:54:38 AM	230 mseg	0 %	100 %
7/27/2021 10:53:38 AM	Error	Error	100 %
7/27/2021 10:52:38 AM	Error	Error	100 %
7/27/2021 10:51:38 AM	Error	Error	100 %
7/27/2021 10:50:39 AM	Error	Error	100 %
7/27/2021 10:50:38 AM	Error	Error	100 %
7/27/2021 10:49:37 AM	256 mseg	0 %	100 %
7/27/2021 10:48:37 AM	237 mseg	0 %	100 %
7/27/2021 10:47:28 AM	1,257 mseg	0 %	100 %
7/27/2021 10:45:44 AM	1,622 mseg	0 %	100 %
7/27/2021 10:44:17 AM	371 mseg	0 %	100 %
7/27/2021 10:42:44 AM	522 mseg	0 %	100 %
7/27/2021 10:41:16 AM	393 mseg	0 %	100 %
7/27/2021 10:40:12 AM	289 mseg	0 %	100 %
7/27/2021 10:39:04 AM	285 mseg	0 %	100 %

Fig. 21 Registro de conexión

## Monitoreo con IPERF3

Para usar la herramienta iperf3, vamos a usar la misma conexión realizada para PRTG, en este apartado se debe descargar iperf3 de su página oficial, dicho archivo debe ser guardado en una localidad del disco, después con la ayuda del CMD de Windows 10, ejecutamos el iperf3.exe, en este caso se lo configuro como servidor y está listo para dar servicio a un cliente como se puede ver en la figura 22, para que iperf3 funcione debe estar constantemente activo.

```

C:\> Command Prompt - iperf3.exe -s 192.168.191.2
[ 5] 0.00-10.00 sec 0.00 Bytes 0.00 bits/sec sender
[ 5] 0.00-10.00 sec 1.84 GBytes 1.58 Gbits/sec receiver
-----
Server listening on 5201
-----
Accepted connection from 192.168.191.1, port 53632
[ 5] local 192.168.191.2 port 5201 connected to 192.168.191.1 port 53634
[ ID] Interval      Transfer      Bandwidth
[ 5] 0.00-1.00 sec  99.0 MBytes  825 Mbits/sec
[ 5] 1.00-2.00 sec  101 MBytes  849 Mbits/sec
[ 5] 2.00-3.00 sec  133 MBytes  1.12 Gbits/sec
[ 5] 3.00-4.00 sec  139 MBytes  1.17 Gbits/sec
[ 5] 4.00-5.00 sec  123 MBytes  1.02 Gbits/sec
[ 5] 5.00-6.00 sec  130 MBytes  1.10 Gbits/sec
[ 5] 6.00-7.00 sec  136 MBytes  1.14 Gbits/sec
[ 5] 7.00-8.00 sec  134 MBytes  1.13 Gbits/sec
[ 5] 8.00-9.00 sec  134 MBytes  1.12 Gbits/sec
[ 5] 9.00-10.00 sec 138 MBytes  1.16 Gbits/sec
[ 5] 10.00-10.00 sec 0.00 Bytes  0.00 bits/sec
-----
[ ID] Interval      Transfer      Bandwidth
[ 5] 0.00-10.00 sec 0.00 Bytes  0.00 bits/sec sender
[ 5] 0.00-10.00 sec 1.24 GBytes 1.06 Gbits/sec receiver
-----
Server listening on 5201
-----

```

Fig. 22 IPERF3 activado en el cmd de Windows

En Kali Linux iperf3, es mucho más sencillo de usar puesto que únicamente se debe instalarlo y darle los permisos necesarios, una vez instalado ejecutamos iperf3 como cliente y empieza el monitoreo, tal cual se puede ver en las figuras 22 y 23, tenemos información acerca del intervalo de tiempo para transferencia de archivos, una velocidad de

transferencia y un ancho de banda, al ser presentado en terminal de Kali Linux se debe tener ciertos conocimientos para interpretar dichos resultados.

```
(kali㉿kali)-[~]
$ iperf3 -c 192.168.191.2
Connecting to host 192.168.191.2, port 5201
[ 5] local 192.168.191.1 port 53634 connected to 192.168.191.2 port 5201
[ ID] Interval      Transfer    Bitrate    Retr  Cwnd
[ 5]  0.00-1.00  sec    100 MBytes  840 Mbits/sec    0   245 KBytes
[ 5]  1.00-2.00  sec    101 MBytes  846 Mbits/sec    0   245 KBytes
[ 5]  2.00-3.00  sec    133 MBytes  1.12 Gbits/sec    0   245 KBytes
[ 5]  3.00-4.00  sec    140 MBytes  1.17 Gbits/sec    0   245 KBytes
[ 5]  4.00-5.00  sec    122 MBytes  1.03 Gbits/sec    0   245 KBytes
[ 5]  5.00-6.00  sec    130 MBytes  1.09 Gbits/sec    0   245 KBytes
[ 5]  6.00-7.00  sec    136 MBytes  1.14 Gbits/sec    0   245 KBytes
[ 5]  7.00-8.00  sec    135 MBytes  1.13 Gbits/sec    0   245 KBytes
[ 5]  8.00-9.00  sec    134 MBytes  1.12 Gbits/sec    0   245 KBytes
[ 5]  9.00-10.00 sec    138 MBytes  1.16 Gbits/sec    0   245 KBytes
-- -- -- -- --
```

Fig. 23 IPERF3 activado en Kali Linux

## Referencias

- [1] S. D. Luz, «JPerf : Manual para medir ancho de banda entre dos ordenadores,» [En línea]. Available: <https://www.redeszone.net/tutoriales/redes-cable/jperf-mide-ancho-de-banda/>.
- [2] «PRTG NETWORK MONITOR: CONOZCA LA HERRAMIENTA,» [En línea]. Available: <https://skyframebolivia.com/blog/2019/10/14/conozca-prtg-network-monitor/>.
- [3] «Wireshark,» [En línea]. Available: <https://www.osi.es/es/herramientas-gratuitas/wireshark>.