

The background of the image is a photograph of a modern building with a curved, metallic facade, possibly the Walt Disney Concert Hall. The building's surface is composed of many triangular and polygonal panels that reflect light, creating a shimmering effect. The architecture is characterized by sharp angles and a dynamic, flowing shape. A dark blue rectangular box is superimposed over the center of the image, containing the text.

**MAKE SYSADMIN
GREAT AGAIN**

Cómo jugar con el tráfico de red



¡HOLA!

Soy **ReD**

Defensor de la privacidad

Entusiasta de la tecnología

Especialista en seguridad

Cofundador de M4H

Cofundador de Hacklabs

Formador cuando me dejan

Herramientas de Red

1. Captura de tráfico
2. Generar tráfico
3. Emular redes



1. Captura de tráfico

Los sniffers son tus amigos

Sniffers

Captura de tramas
Modo promiscuo
Superusuario

Dependiendo de la topología de la red se desplegarán de una u otra forma.

Sniffers - Características

Capturas

Convierte la captura en formato inteligible por humanos.

Detección

Detección de problemas de red antes de que pueda llevar a problemas mayores.

Debugear

Permite el debugging de las aplicaciones con uso de red.

Auditoría

Permite la auditoría y almacenamiento del tráfico capturado.

Flujo

Análisis de tramas de forma individual o dentro de un flujo.

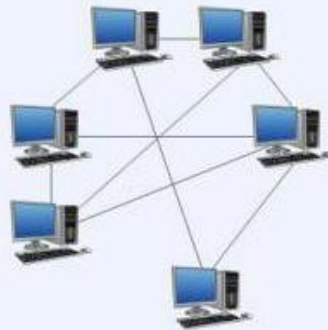
IDS

Detección de intrusos IDS.

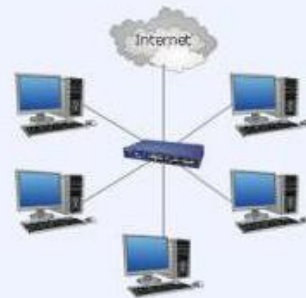
Sniffers - Donde colocarlos



Fully Connected Network Topology



Mesh Network Topology



Star Network Topology

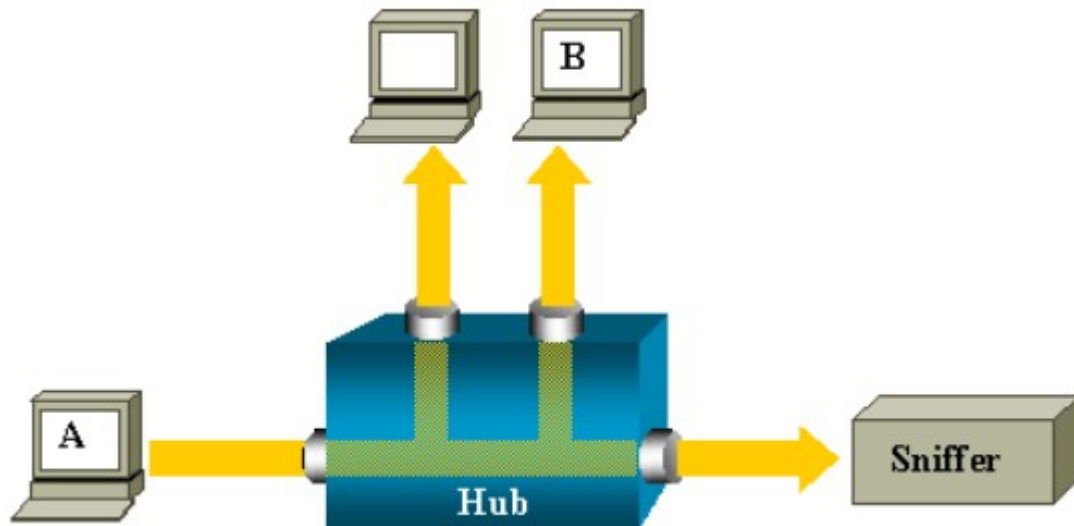


Common Bus Topology

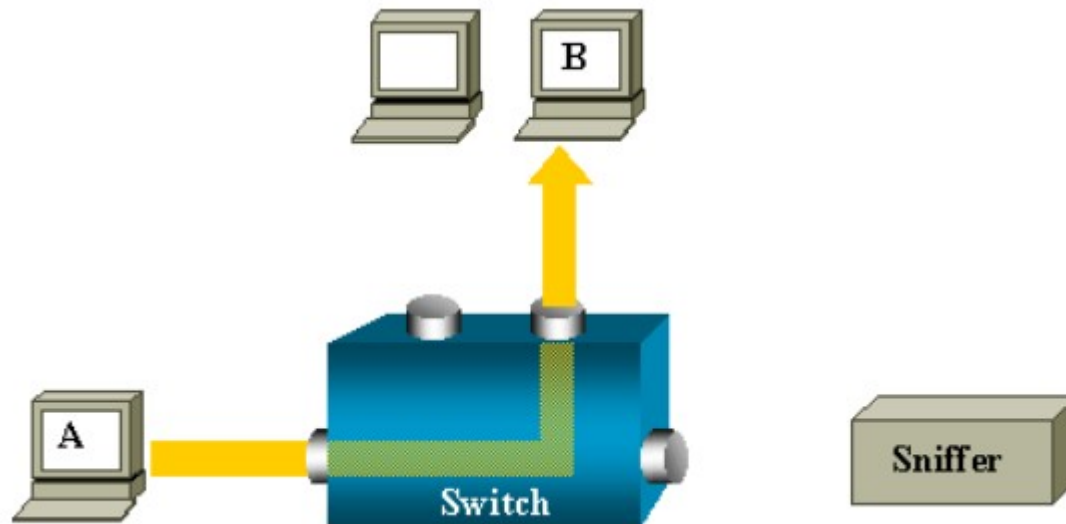


Ring Network Topology

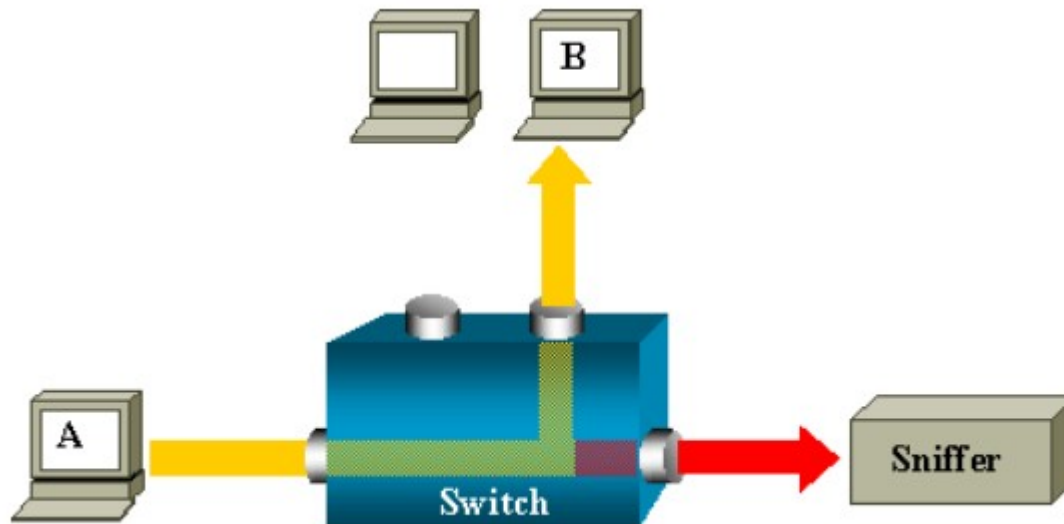
Sniffers - Donde colocarlos



Sniffers - Donde colocarlos

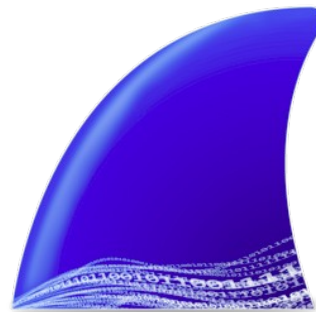


Sniffers - Donde colocarlos



Sniffers - Software

TCPDUMP



T-SHARK

Sniffers - Consola

Tcpdump

Versión 4.9.2

3-clause BSD

Viene con *NIX

Tshark

Versión 2.6.2

GPL

Viene paquete externo

Mejores filtros.

Sniffers - Consola

tcpdump -i any
tcpdump -i eth0
tcpdump -D
tcpdump host 8.8.8.8
tcpdump src/dst
192.168.10.1

tcpdump net
192.168.10.1/24
tcpdump port 3389
tcpdump portrange 21-80
tcpdump icmp/ip/udp/tcp
tcpdump -v/-vv

Sniffers - Consola

```
operez@datio:~$ sudo tcpdump -n -q -i any port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
19:08:28.627358 IP 192.168.42.62.34492 > 2.20.44.83.80: tcp 0
19:08:28.627380 IP 192.168.42.62.45210 > 2.20.44.120.80: tcp 0
19:08:28.651026 IP 2.20.44.120.80 > 192.168.42.62.45210: tcp 0
19:08:28.651047 IP 2.20.44.83.80 > 192.168.42.62.34492: tcp 0
19:08:29.019475 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.076824 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 0
19:08:29.076871 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.076955 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 142
19:08:29.130603 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 0
19:08:29.131679 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 1388
19:08:29.131714 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.131721 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 1388
19:08:29.131733 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.132596 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 1388
19:08:29.132613 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.132628 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 103
19:08:29.132635 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.133044 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
19:08:29.195027 IP 51.254.128.161.80 > 192.168.42.62.40334: tcp 0
19:08:29.195067 IP 192.168.42.62.40334 > 51.254.128.161.80: tcp 0
```

Timestamp	Sender IP	Port	Destination IP	Port
19:08:29.195067	192.168.42.62	40334	51.254.128.161	80

Sniffers - Consola

tcpdump -i eth0 tcp port 80 and dst 8.8.8.8

tcpdump -i eth0 not icmp and not tcp

tcpdump -w fichero_captura.pcap

tcpdump -r fichero_captura.pcap

Cheat sheet

<http://packetlife.net/media/library/12/tcpdump.pdf>

Sniffers - PCAP

API

Para la captura de paquetes.

En *nix es la librería libpcap y en windows WinPcap

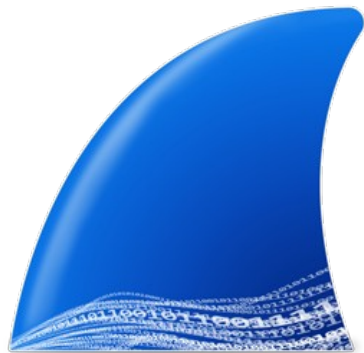
Fichero

Con formato y extensión .pcap
capinfos

		Global Header
PCAP FILE	Packet 1	Packet Header
		Packet Data
	Packet 2	Packet Header
		Packet Data

Sniffers - Con GUI - WIRESHARK

Analizador de protocolos
Más de **480** protocolos (GSM y USB)
Reconstrucción de sesiones TCP



ETHEREAL
PACKET SNIFFER

DEMO

Place your screenshot here

Wireshar k

Sniffers - Traer entorno remoto

```
ssh root@server sudo tcpdump -i any -w - 'not port 22' | wireshark -k -i -
```

```
ssh root@server 'tshark -f "port !22" -i any -w -' | wireshark -k -i -
```

BONUS



2. Generar tráfico

Comprobando límites de tu red

Generadores de tráfico

Pruebas de rendimiento de la red
Pruebas de estrés de aplicaciones
Pruebas de firewalls

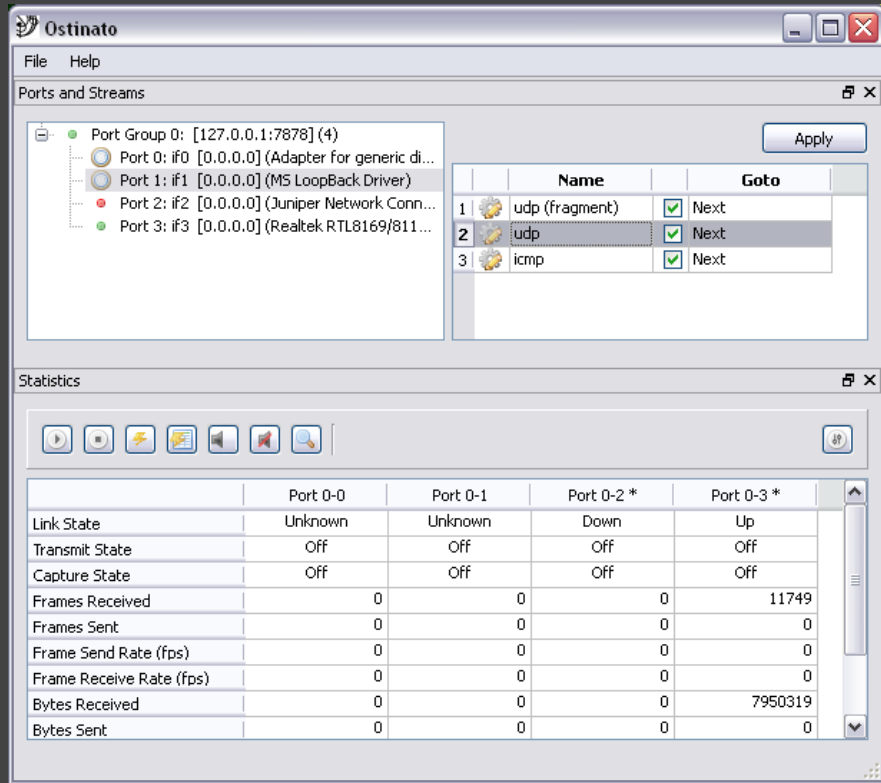
“Sin hardware específico”

Generadores de tráfico - ostinato

Interface amigable
API python para automatizaciones
Gestión de ratios de envío

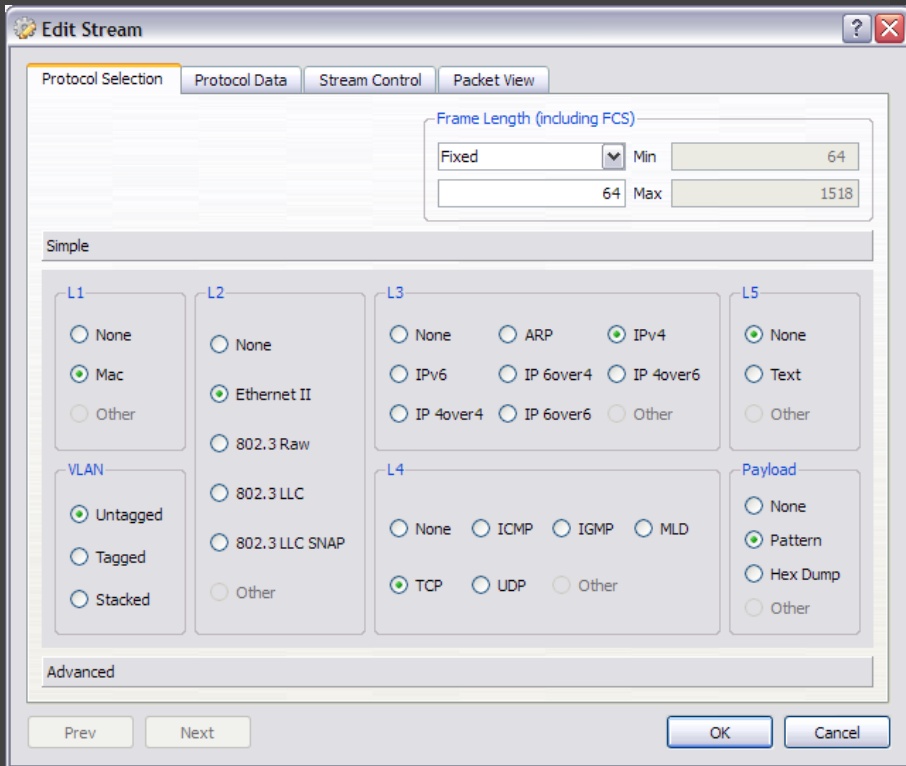


“Es como wireshark pero al revés”



DEMO

Ostinato



DEMO

Ostinato



3. Emular redes

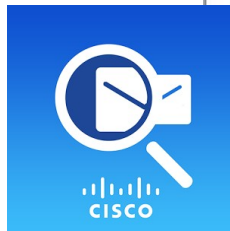
Monta tu propia infraestructura de red

Emular redes

Sistemas simulados (packet tracer)
Sistemas emulados (GNS3)
Entorno de pruebas y aprendizaje

Nos ofrece sistemas reales “sin coste”

Emular redes - packet tracer



Cisco Packet Tracer Student - C:\Program Files (x86)\Cisco Packet Tracer 6.2sv\saves\Router\EIGRP\ip...

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object Set Tiled Background Viewport

lo 1: 2002::/64

1841 Router0

1841 Router1

1: check eigrp neighbors are up
2: check eigrp route is in Router 1
D 2002::/64 [90/2297856]
3: configured "neighbor FE80::2D0:BCFF:FE50:4B01 s0/0/0" on Router
4: neighbor adjacency should be down on both
5. configured "neighbor FE80::290:21FF:FEE5:CB01 s0/0/0" on Router
6. Adjacency should be re-established
7. ipv6 route should be available again on Router1

Time: 00:10:27 Power Cycle Devices Fast Forward Time

Routers

1841 1941 2620XM

2620XM

Scenario 0

New Delete

Toggle PDU List Window

Realtime

Fire	Last Status	Source	D
------	-------------	--------	---

Emular redes - GNS3

Gratis

Software Open Source con licencia GPL v3

De pago algunas imágenes propietarias

Cliente servidor

Está compuesto por un módulo cliente y otro servidor que se comunican normalmente por el puerto 3080

Multiplataforma

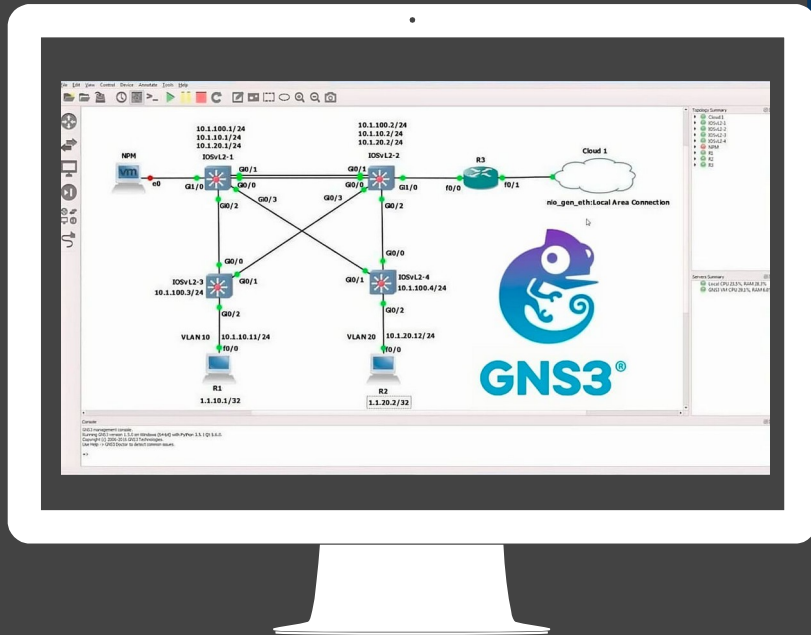
Win, linux y mac además de versiones virtualizadas para virtualbox, VMware workstation y VMware ESXi

Multi S.O.

Cisco, Juniper, MikroTik, Sophos, Fortigate, OpenWRT, Checkpoint, Alcatel-Lucent ...



DEMO

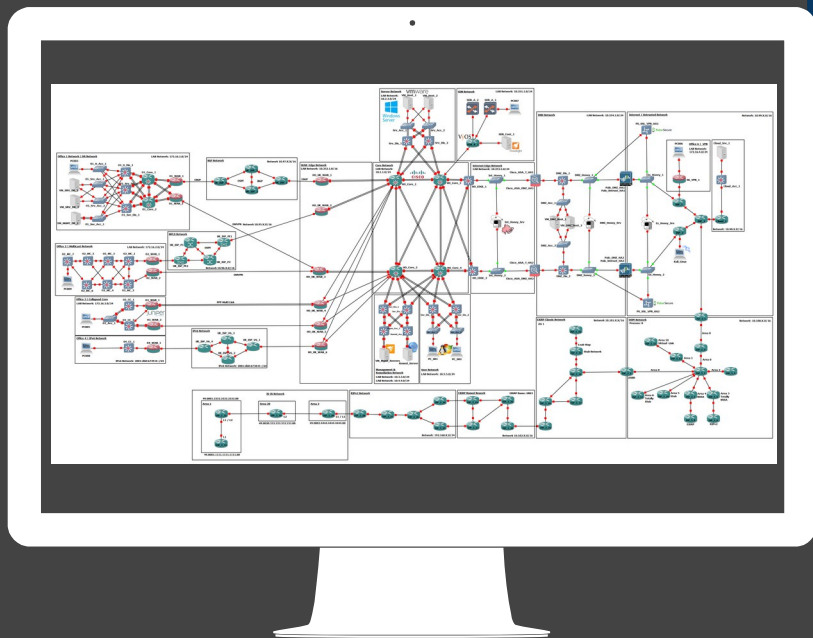


GNS3

SYSADMIN DAY
2018



Esquema detallado



GNS3

GNS3 March Backup Screenshot Final v3.png

¡Gracias!

¿Preguntas?

red@nosoloaulas.com