



IF-6000

Redes en los negocios

Juan José Morales Hernández

jjmoraleshernandez@ina.cr

88217288

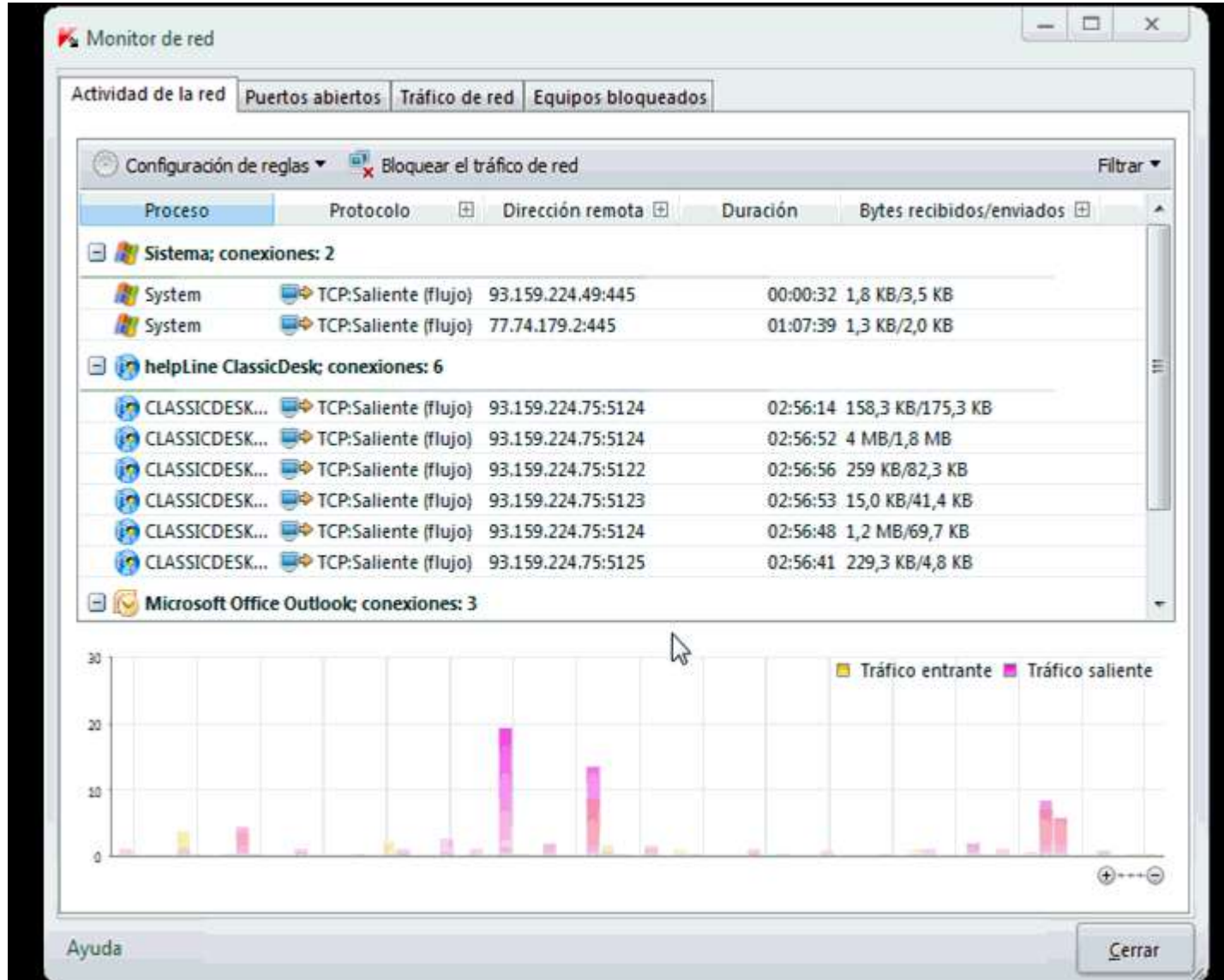
Administración de red

- ▶ Para predecir cambios para crecimiento.
- ▶ Detectar cambios inesperados en la red.
- ▶ Inicio de monitoreo de la red.
- ▶ Monitorización de enlaces.
- ▶ Ejemplos de monitor de tráfico.
- ▶ SNMP
- ▶ CMIP(Protocolo de Información de Administración Común, Common Management Information Protocol) ---OSI---
- ▶ Resolución de errores.

Administración de red

- ▶ Comandos de ayuda.
- ▶ Ping: paquete de eco
- ▶ Traceroute: ruta que un paquete tomó para llegar a su destino. Máximo 30 saltos.
- ▶ Telnet: emulación de terminal.
- ▶ Netstat: estadísticas de protocolo y de las conexiones IP activas..
- ▶ Arp: direcciones de hardware de los hosts locales y el gateway predeterminado.
- ▶ Ipconfig: muestra configuraciones básicas.

Monitorizar red vs Analizar red



Monitorizar red vs Analizar red

Capturing from Conexión de área local [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.76.123? Tell 187.242.76.1
2	0.00339900	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.111.184? Tell 187.242.108.1
3	0.02668100	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.84.177? Tell 187.242.84.1
4	0.12599600	108.162.232.197	187.242.80.190	TCP	60	80→49284 [FIN, ACK] Seq=1 Ack=1 win=30 Len=0
5	0.12646100	187.242.80.190	108.162.232.197	TCP	54	49284→80 [ACK] Seq=1 Ack=2 win=256 Len=0
6	0.12667400	187.242.80.190	108.162.232.197	TCP	54	49284→80 [FIN, ACK] Seq=1 Ack=2 win=256 Len=0
7	0.13302300	187.242.80.190	64.233.176.99	SSL	55	Continuation Data
8	0.14627300	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.8.144? Tell 187.242.8.1
9	0.16877000	108.162.232.197	187.242.80.190	TCP	60	80→49284 [ACK] Seq=2 Ack=2 win=30 Len=0
10	0.21232700	64.233.176.99	187.242.80.190	TCP	66	443→49201 [ACK] Seq=1 Ack=2 win=361 Len=0 SLE=1 SRE=2
11	0.27194000	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.80.199? Tell 187.242.80.1
12	0.37966100	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.11.37? Tell 187.242.8.1
13	0.38945600	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.82.69? Tell 187.242.80.1
14	0.41095400	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.111.136? Tell 187.242.108.1
15	0.46558800	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.77.55? Tell 187.242.76.1
16	0.64587000	Cisco_57:3e:da	Broadcast	ARP	60	who has 187.242.111.190? Tell 187.242.108.1
17	0.67477200	Cisco_57:3e:da	Broadcast	ARP	60	who has 10.136.94.152? Tell 10.136.64.1

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Cisco_57:3e:da (00:25:84:57:3e:da), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

```
0000  ff ff ff ff ff ff 00 25 84 57 3e da 08 06 00 01  .....% .W>.....
0010  08 00 06 04 00 01 00 25 84 57 3e da bb f2 4c 01  .....% .W>...L.
0020  00 00 00 00 00 00 bb f2 4c 7b 00 00 00 00 00 00  ..... L{.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..... .....
```

Conexión de área local: <live capture in proq... | Packets: 2924 · Displayed: 2924 (100.0%) | Profile: Default

1

2

3

Documentación de redes

“Administrar una red no solo es saber configurar los equipos de comunicaciones, sino administrar la información de la red”

¡Cómo saber dónde, cómo y cuando?

- ▶ Documentar...
 - ▶ Procedimientos
 - ▶ Bases de Conocimiento
- ▶ Documentar...
 - ▶ Configuraciones
 - ▶ Esquemas futuros
- ▶ Documentar...
 - ▶ Diseños
 - ▶ Planes de Contingencia.

Centro de operación de la red -COR (Network Operation Center)

- ▶ El lugar donde se efectúa la monitorización y la documentación de la red
 - ▶ - Acceso a herramientas de monitorización
 - ▶ - Sistemas de manejo de incidencias
 - ▶ - Sistemas de documentación • Diagramas • Bases de Datos

Centro de Operación de Red



- ◉ El 20% de los problemas de red, estarán acá, pero serán los más difíciles.

NOC







The background features abstract, overlapping green geometric shapes, primarily triangles and polygons, in various shades of green, ranging from light lime to dark forest green. These shapes are concentrated on the right side of the image, creating a dynamic, layered effect. The left side of the image is a solid, light gray background.

NOC

Porqué hacerlo?

- ▶ Para saber qué fue lo que cambié hace 9 meses.
- ▶ Para tener vacaciones tranquilas 😊
- ▶ Piense en estas preguntas:
 - ▶ ¿Y si “al que le toca” cambió de trabajo?
 - ▶ ¿Ya cerca de los cuarenta años, seguimos siendo inmortales?
 - ▶ “Vacaciones son vacaciones”

¿Porqué no hacerlo?

- ▶ La verdad “da pereza”
 - ▶ “Ahora no puedo, tengo mucho que hacer”.
 - ▶ “Estoy en algo importante, que lo haga otro”
- ▶ Hay que saber organizar la documentación
 - ▶ Necesita una metodología para cualquiera no sólo par mi, si no, se vuelve un desorden con el tiempo
- ▶ La red cambia constantemente
 - ▶ La información vieja es inútil e incluso peligrosa
 - ▶ La documentación no es un proyecto, es un proceso!

Recomendaciones

- ▶ Cree una política de documentación
 - ▶ Qué responsabilidad tiene cada uno?
 - ▶ Cómo es el proceso? Orden de las tareas?
 - ▶ Cómo se verifica la calidad? Metodologías
- ▶ Esquemas de nombres consistentes
 - ▶ Para equipos, cableado, etc.
- ▶ Etiquete TODO
 - ▶ Servidores, routers, switches, puntos inalámbricos, UPS, etc...
 - ▶ Cables - Tomas de red - Racks

Documentación

Se debe establecer una nomenclatura de documentación para los distintos componentes a señalar.

Todos los cables, paneles y salidas deben de estar etiquetados tanto a simple vista como en su interior.

Deben de realizarse esquemas lógicos claros de las instalaciones con todas las indicaciones de los distintos componentes.

Se confeccionarán planos de los edificios donde se ha instalado con indicación de los recorridos, situación de las cajas y armarios de distribución y todo lo que pueda tener influencia sobre el funcionamiento de la red

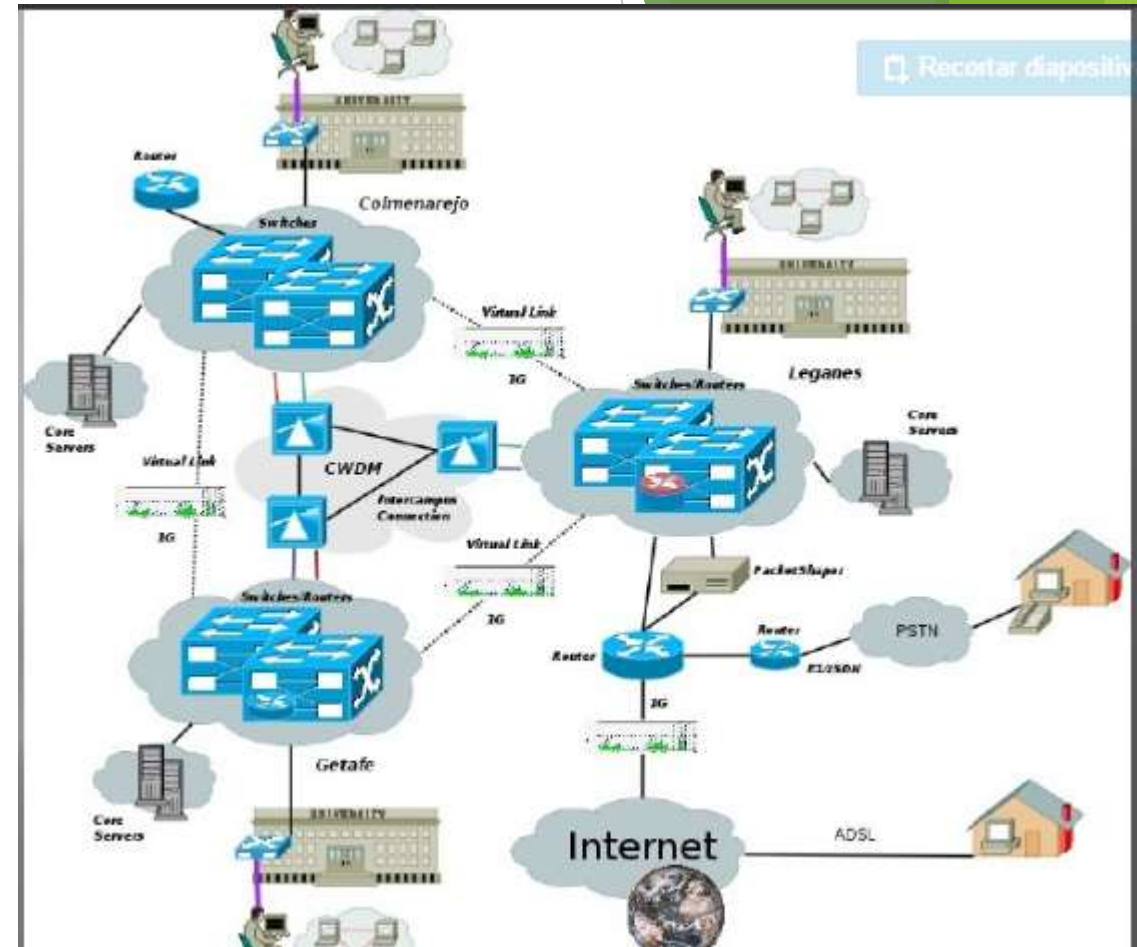
Documentación

- ▶ Cosas básicas, como la documentación de los switches...
 - ▶ A qué está conectado cada puerto?
 - ▶ Puede ser simplemente un archivo de texto con una línea por cada puerto del switch: •
 - ▶ health-switch1, port 1, Salón #29 - Director
 - ▶ health-switch1, port 2, Salón #43 - Recepcionista
 - ▶ health-switch1, port 3, Salón #100 - Salón de clase
 - ▶ health-switch1, port 4, Salón #105 - Oficina de profesores
 - ▶
 - ▶ health-switch1, port 25, Conexión al switch principal
 - ▶ Esta información puede hacerse disponible al equipo de red o grupo de soporte, en una wiki, un software, etc.
 - ▶ Recuerde etiquetar sus puertos

Documentación

Mapa de Red

Es la representación gráfica de la topología de la red, incluyendo tanto conexiones internas como externas. Esta documentación puede apoyarse en un plano del edificio en donde se instala la red. Suelen confeccionarse dos tipos de mapas de red: lógicos y físicos. En los lógicos o funcionales, se indica la funcionalidad del elemento que se describe, así como sus direcciones, función que desempeña, etc. En el caso del mapa físico, interesa sobre todo la especificación de la conectividad del cableado.



Documentación de redes

N°	Red	Subred	Máscara	Cant. IP	Broadcast	Descripción

[illegible]

documentacion

Mapa de Protocolos

Es la descripción de la organización lógica de la red, así como de los protocolos utilizados globalmente, por ejemplo, las direcciones de máscaras de red, configuración de los routers,, creación de dominios o grupos de trabajo, relaciones de confianza, etcétera.

documentación

Mapa de Nodos

Se compone de una descripción del hardware y del software que se instala en cada nodo, así como los parámetros de su configuración, modelos, marcas, direcciones de red, etc. La documentación debe permitir la creación de un histórico de cada nodo que registre la evolución de sus averías, actualizaciones de software, etcétera.

documentación

Mapa de Grupos y Usuarios

Consiste en la descripción de los grupos y usuarios de la red contemplando las posibilidades de acceso a los distintos recursos, así como los derechos de acceso a las aplicaciones, perfiles, privilegios, etcétera.

documentación

Calendario de Averías

Es el registro de averías del sistema, de modo que permita el análisis de las causas y probabilidad de fallo de los distintos componentes de la red, tanto software como hardware, y su evolución en el tiempo.

Ayuda para documentar

- ▶ Netdot: <https://netdot.uoregon.edu>
- ▶ IPplan: <http://iptrack.sourceforge.net>
- ▶ Netdisco: <http://netdisco.org>
- ▶ Rack Tables: <http://www.racktables.org>
- ▶ The NOC Project <http://nocproject.org>

Itil y Cobit en redes

- ▶ http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_configuraciones/vision_general_gestion_de_configuraciones/vision_general_gestion_de_configuraciones.php
 - ▶ Curso de Itil versión anterior
- ▶ <http://auditoriasistemas10c.blogspot.com/2011/11/procesos-til-relacion-por-area.html>
 - ▶ Relación de ITIL por área a las Redes y Sistemas
- ▶ <http://www.netmind.es/knowledge-center/itil-vs-cobit-a-quien-quieres-mas/>
 - ▶ Itil y COBIT

Trabajo a entregar

- ▶ Crear un Servicio de Service Desk en línea. Me envían por favor el usuario y contraseña para ingresar y administran el ticket.