

TDRC

Empezamos a 17:35

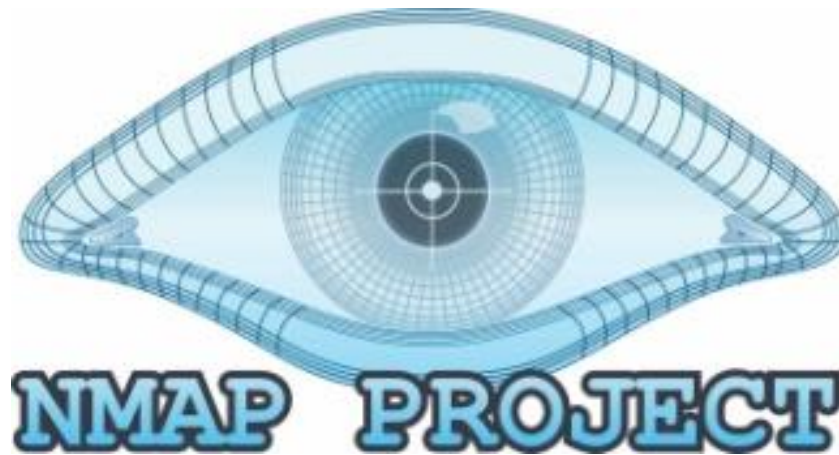
SEMINARIO 2: Herramientas y utilidades de diagnóstico en red. Comandos básicos Cisco

Antonio Fernández Ares

A.M.Mora García – M.A. López Gordo

Índice

- Herramientas diagnóstico de red:
 - nmap
 - Tracert
 - Wireshark
- Comandos básicos CISCO
 - Definiciones de comandos
 - Resolución de casos prácticos
- Cisco Packet Tracer



Herramientas y utilidades de diagnóstico en red

NMAP

NMAP

Recordatorio: Direcciones IP, Puertos y sockets

- Breve recordatorio de que es una:
 - Dirección IP
 - 32 bits que identifica de manera lógica un dispositivo en una red IP.
 - Puerto
 - 16 bits que identifica el proceso al que hay que entregar el mensaje.
 - Socket
 - Interfaz de entrada-salida que permite intercomunicación entre procesos.
 - Se identifica mediante una dirección IP y un puerto.
 - Dos tipos:
 - Socket stream: Hacen uso del protocolo TCP.
 - Socket datagram: Hacen uso del protocolo UDP.

NMAP

Sondeo de puertos: NMAP

- NMAP es una aplicación que permite sondear los puertos abiertos de los equipos activos en una red.
- Permite:
 - Determinar los equipos en una red determinada.
 - Determinar los puertos abiertos de un equipo determinado.
 - En muchos casos, los servicios empleados.
 - Determinar el sistema operativo de un equipo determinado.
 - Determinar algunas características del hardware de red.
- Se suele usar:
 - Para el bien: comprobar que nuestros equipos no tienen más puertos abiertos de los necesarios.
 - Para el mal: comprobar que los equipos de otros «permiten» accesos externos «indeseados».

NMAP

Ejemplos aplicados:

- Material empleado:
 - NMAP.
 - En repositorios de la mayoría de distribuciones de GNU/Linux.
 - Otros Sistemas Operativos: <https://nmap.org/download.html>
 - Servidor de pruebas:
scanme.nmap.org
- Documentación adicional:
 - <https://linux.die.net/man/1/nmap>
 - <https://nmap.org/man/es/man-briefoptions.html>

NMAP

Autoevaluación:

- ¿Cómo podemos emplear el comando NMAP para sondear los host activos en una red?
- ¿Cómo podemos emplear el comando NMAP para sondear los puertos abiertos en un host?
- ¿Cómo podemos conocer el sistema operativo del host? ¿Es totalmente fiable?
- ¿Cuántos puertos pueden ser comprobados?
- ¿Cómo podemos emplear NMAP para detectar un cortafuego entre el host y nosotros?
- ¿Emplear el comando NMAP tiene algún efecto en los LOGs del host? ¿Se puede controlar este impacto?

TRACEROUTE

Herramientas y utilidades de diagnóstico en red

TRACEROUTE

Traceroute

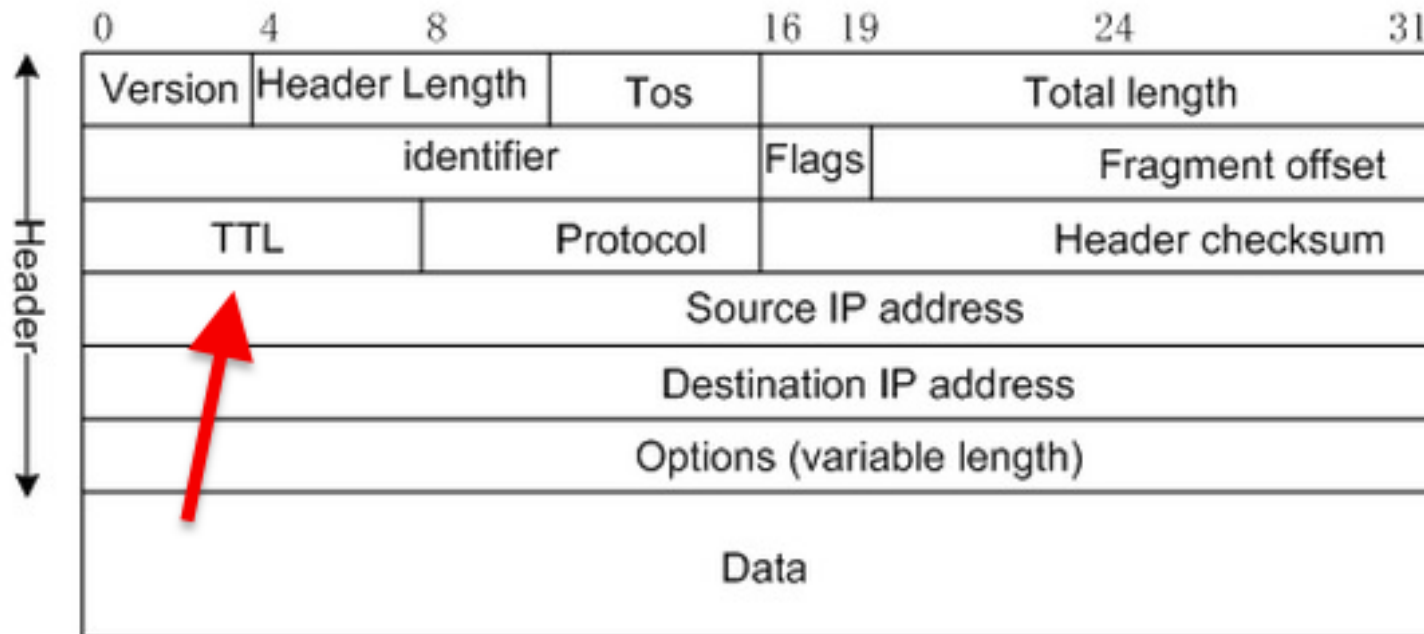
Trazabilidad de los paquetes de red

- Es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host o punto de red.
- Se obtiene también una estadística del RTT o latencia de red de esos paquetes.
- La ruta se determina mediante el envío de paquetes eco ICMP.

Traceroute

Como funciona

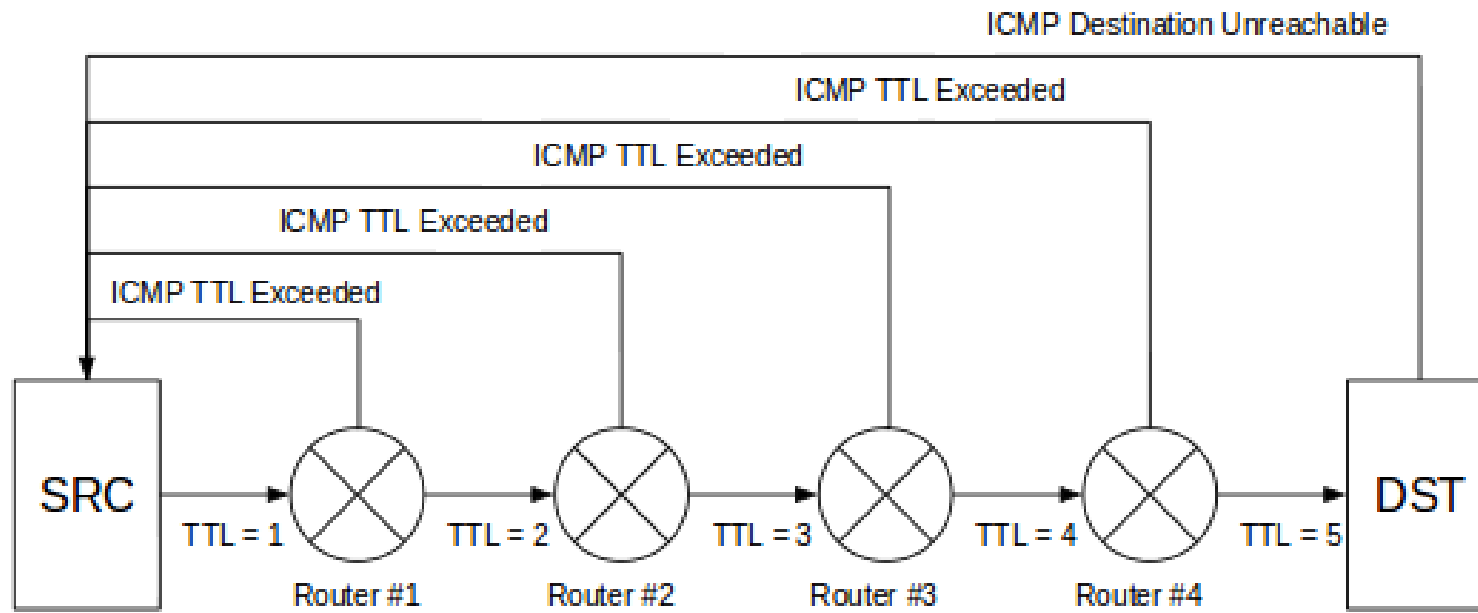
- Cada paquete IP tiene un campo denominado TTL (time-to-live).
- Máximo número de saltos que puede dar un paquete antes de ser descartado.



Traceroute

Como funciona II

- En traceroute, se re-define el campo TTL en cada respuesta incrementándolo en 1 hasta que alcanza su destino final.



Traceroute

Ejemplos aplicados:

- Material empleado:
 - traceroute.
 - En repositorios de la mayoría de distribuciones de GNU/Linux.
 - Otros Sistemas Operativos: tracert.exe
- Documentación adicional:
 - <https://linux.die.net/man/8/traceroute>

Traceroute

Autoevaluación:

- ¿Qué nos indica la salida del comando traceroute?
- ¿Se pueden ocultar los nombres DNS?
- ¿Es la ruta obtenida siempre la misma?
- ¿En que mecanismo se basa traceroute?



WIRESHARK

Herramientas y utilidades de diagnóstico en red

WIRESHARK

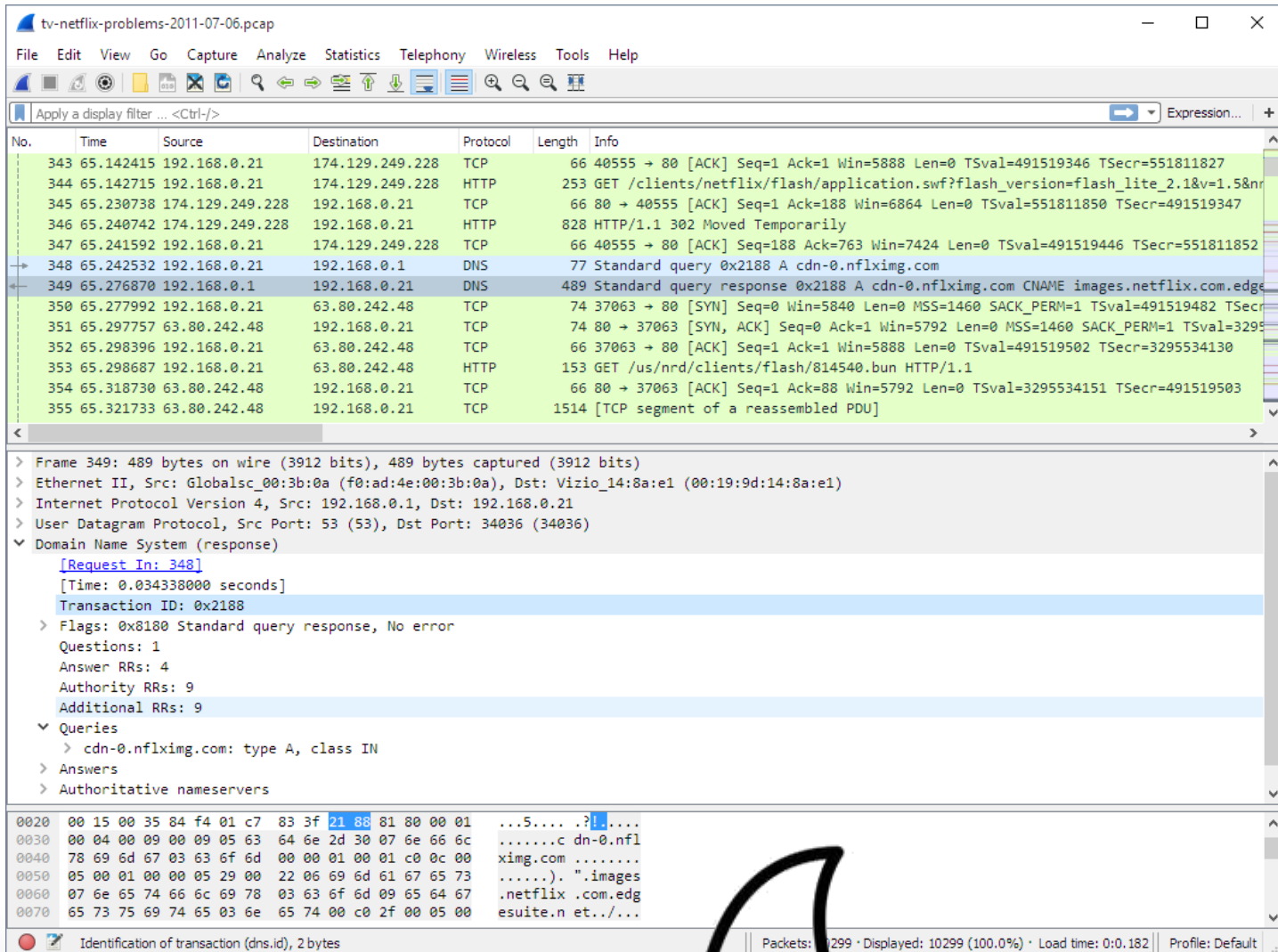
Wireshark

Analizando el tráfico de red

- Analizador es protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicación.
- Similar a tcpdump, iperf con GUI!

Wireshark

Un primer vistazo a la GUI



tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&n...
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge...
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr=...
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295...
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsec_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

▼ Queries

> cdn-0.nflximg.com: type A, class IN

> Answers

> Authoritative nameservers

0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... .?.....

0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl

0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com

0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images

0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg

0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et.../...

Identification of transaction (dns.id), 2 bytes

Packets: 1299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Wireshark

Ejemplos aplicados:

- Material empleado:
 - wireshark.
 - En repositorios de la mayoría de distribuciones de GNU/Linux.
 - Otros Sistemas Operativos:
<https://www.wireshark.org/#download>
 - Repositorio de tráfico de red:
 - <https://wiki.wireshark.org/SampleCaptures>
- Documentación adicional:
 - <https://www.wireshark.org/docs/>



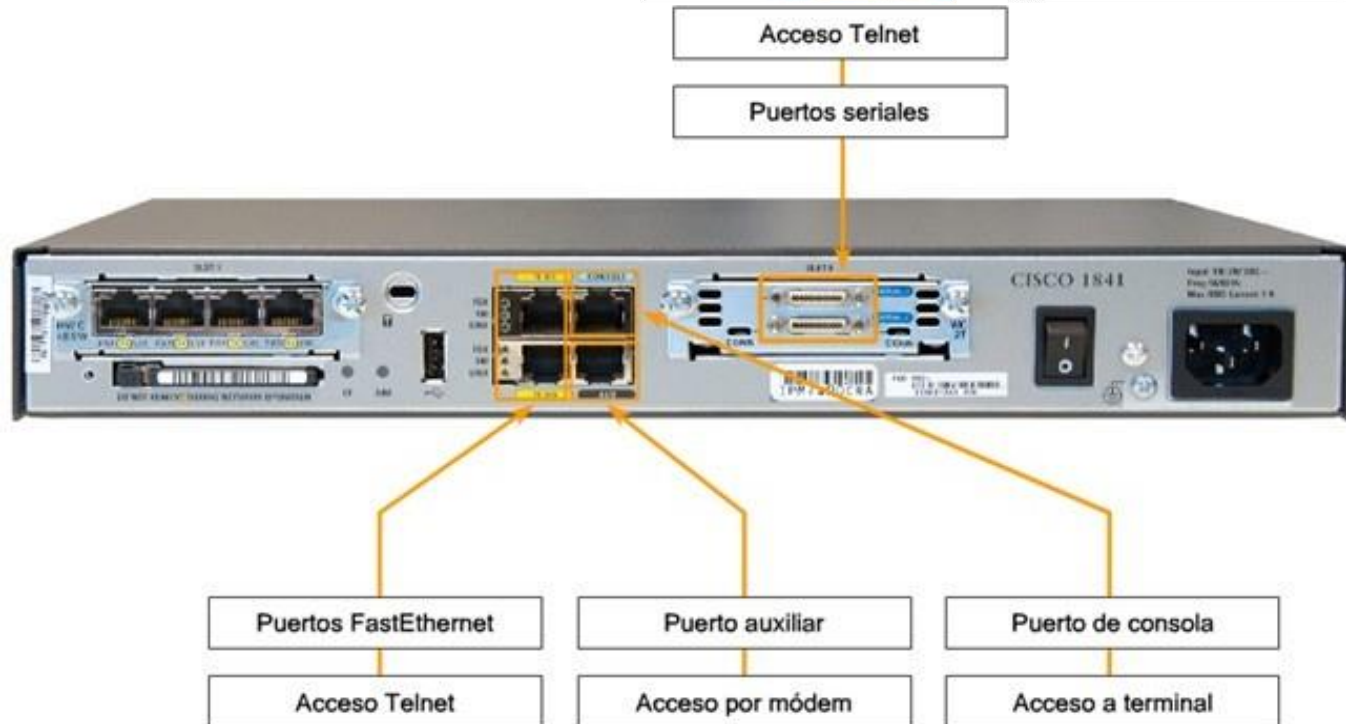
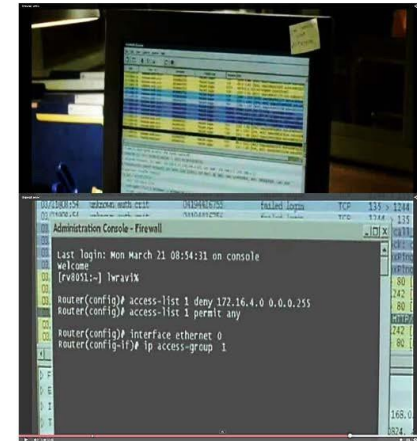
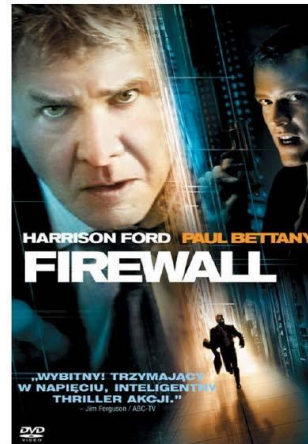
Comandos básicos y CISCO PACKET TRACER

CISCO

Comandos básicos de configuración

❑ Hardware

- Interfaces
- Sistemas de ficheros



Comandos básicos de configuración

❑ Inicio

- Modo privilegiado
 - Modo usuario
 - Reiniciar
- :enable
:disable
:reload

❑ Archivos de configuración

- Mostrar configuración actual
 - Mostrar configuración de arranque
- :show running-config
:show startup-config

❑ Modo de configuración

- Configuración global
 - Salir de configuración
- :configure terminal
: exit , ctrl-z

Comandos básicos de configuración

❑ Configuración global:

- Nombre del dispositivo :hostname
- Base de datos DNS :ip host
- Desactivar búsquedas DNS :no ip domain-lookup
- Contraseña modo privilegio :enable secret
- Mensaje de seguridad :banner motd#
- Activación servicio web :ip http server

❑ Configuración de la interfaz (desde el modo de configuración global)

- Modo configuración interfaz :interface
- Direccionamiento IP :ip address
- Comentario :description
- Habilitar la interfaz :no shutdown
- Deshabilitar la interfaz :shutdown

➤ Configuración de acceso VTY

- Modo de configuración VTY : line vty 0 4
- Solicitud de login : login
- Contraseña : password <contraseña>

Comandos básicos de diagnóstico

❑ Comandos de diagnóstico:

- Configuración actual :show running-config
- Interfaces, IOS, tiempo arrancado :show version
- Resumen estado de interfaces e IPs :show ip interfaces brief
- Estadísticas y métrica de protocolos :show interface xx
- Tabla de rutas :show ip route
- Procesos ejecutándose :show processes cpu
- Conexiones establecidas al equipo :show users

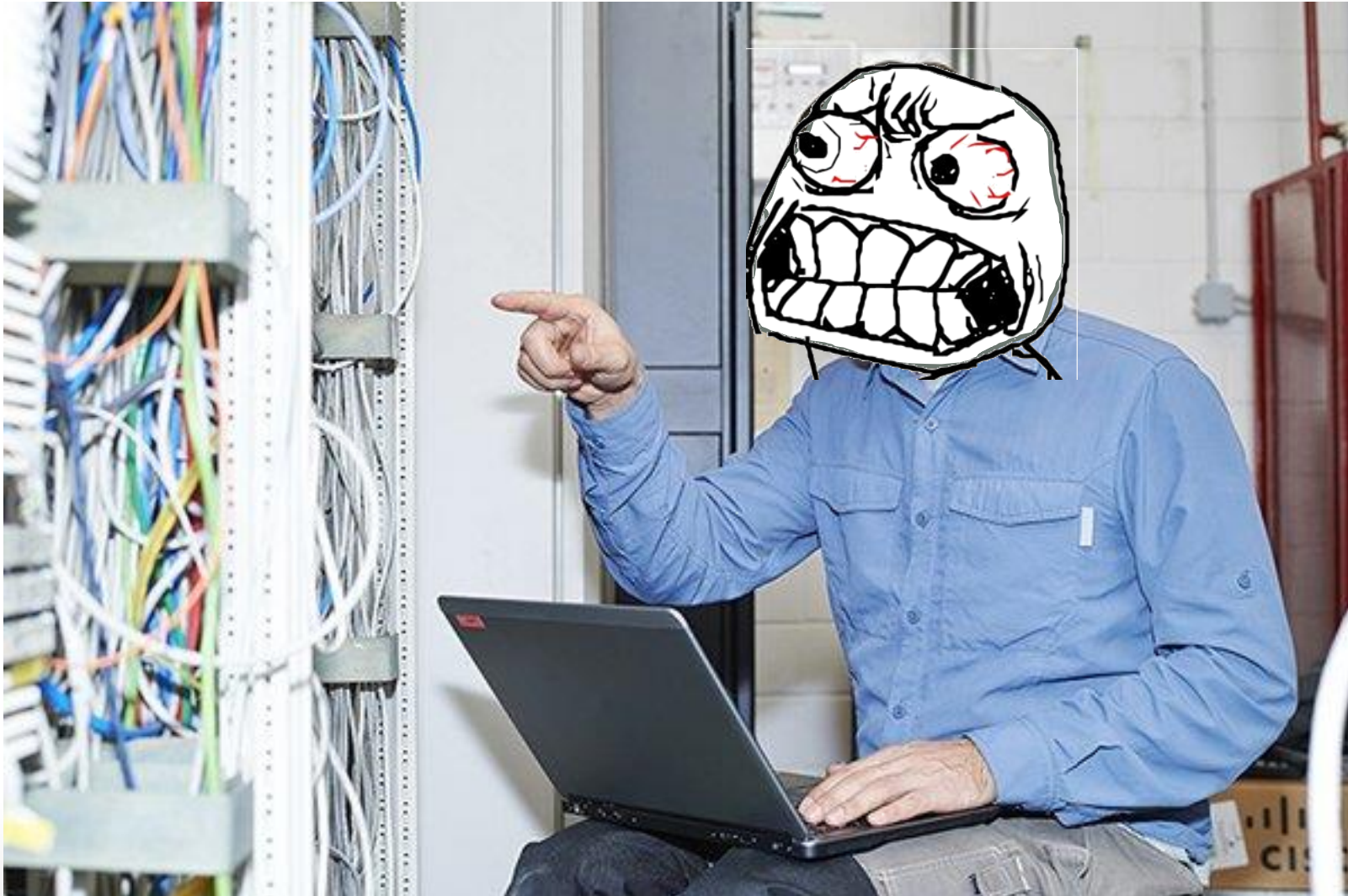
❑ Edición y ayuda

- Ayuda :help, ?, <space>?, >tab>
- Edición :arrows

EJERCICIO: Configure una ip en el interfaz FE0/0 de su router, conéctelo a su consola y ejecute los comandos de diagnóstico. Anote los valores y dibuje un esquema del ejercicio.



¡Vamos con algunos casos prácticos!



Caso práctico: Configuración global

- OBJETIVO: Configurar nuestro router para:
 - Cambiarle el hostname
 - Cambiar el password de acceso.
 - Deshabilitar las búsquedas DNS

Caso práctico: Configuración global

- OBJETIVO: Configurar nuestro router para:
 - Cambiarle el hostname
 - Cambiar el password de acceso.
 - Deshabilitar las búsquedas DNS
- PASOS:
 - Acceder al router
 - Entrar en el modo configuración
 - Cambiar el nombre
 - Cambiar el password
 - Deshabilitar la búsquedas DNS

Caso práctico: Configuración global

```
1 $telnet <nombre router o dirección>
2
3 Login: login id
4 Password: *****
5
6 Router> enable
7 Router# configure terminal
8
9 Router(config)#
10 Router(config)# hostname LANister
11
12 LANister(config)#
13
14 LANister(config)# enable secret
15 ForTheHorde
16 LANister(config)#
17
18 LANister(config)# no ip domain-lookup
19 LANister(config)#
```

Caso práctico: Asignar IP a interface

- OBJETIVO: Configurar nuestro router para:
 - Asignar la IP 192.168.12.2/24 a la interface gigabitethernet 0/1

Caso práctico: Asignar IP a interface

- OBJETIVO: Configurar nuestro router para:
 - Asignar la IP 192.168.12.2/24 a la interface gigabitethernet 0/1
- PASOS:
 - Entrar modo configuración de la interface
 - Asignar dirección IP
 - Levantar la interface
 - Salir de la interface

Caso práctico: Asignar IP a interface

- OBJETIVO: Configurar nuestro router para:
 - Asignar la IP 192.168.12.2/24 a la interface gigabitethernet 0/1

```
1 Router(config)# interface gigabitethernet 0/1
2 Router(config-if)#
3
4 Router(config-if)# ip address 192.168.12.2 255.255.255.0
5 Router(config-if)#
6
7 Router(config-if)# no shutdown
8 Router(config-if)#
9
10 Router(config-if)# exit
11 Router(config)#
```

Si deseas saber un poco más

- Software para simular redes (“gratuito”)
 - <https://www.netacad.com/es/courses/packet-tracer>
- Certificaciones CCNA:
 - <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-routing-switching.html>