Departamento de Ingeniería Electrónica, de Sistemas Informáticos y Automática

TECNOLOGÍA DE REDES

PRÁCTICAS DE LABORATORIO

CURSO 2003-2004

20 de Febrero de 2004

INDICE

PRÁCTICAS de TECNOLOGIA DE REDES

ASISTENCIA

Las prácticas tendrán lugar en el Laboratorio de Arquitectura y Redes (Sótano, pasillo de la izquierda del edificio V.R.C, aula 7457) no siendo obligatoria la asistencia. Sí es obligatoria la presentación de las prácticas resueltas y funcionando en horario de laboratorio.

Se entregarán todos los enunciados de prácticas al principio. El alumno deberá realizarlas a lo largo de las sesiones de prácticas. Una vez realizadas serán evaluadas por el profesor de prácticas, que resolverá cualquier duda presentada en la práctica. LA PRÁCTICA SE DEBE TRAER PREPARADA PARA SU PUESTA EN MARCHA EN EL LABORATORIO.

EVALUACIÓN

a) Las prácticas han de ser aptas para aprobar la asignatura.

Las prácticas de laboratorio se calificarán de forma numérica en función de:

- Nivel técnico y calidad de redacción de la memoria de prácticas.
- Revisión del trabajo de prácticas funcionando por el profesor de prácticas.

b) Memoria de prácticas

Se entregará una memoria impresa de las prácticas realizadas, junto con un disco que contendrá los ficheros fuente de los diseños o programas si ha lugar. En la memoria debe aparecer claramente el nombre del alumno. Cada memoria de prácticas debe estar redactada mediante procesador de textos o equivalente y contendrá como mínimo los siguientes apartados:

1.- Portada donde aparezca claramente nombre, curso y fecha.
2.- Índice del documento.
3.- Un epígrafe para cada práctica, donde aparezca:

- Enunciado.
- Diseño del circuito con esquemas.
- Comentarios sobre el montaje y/o problemas presentados y como se han resuelto.
- Respuesta a las cuestiones planteadas en el enunciado.
- Posibilidades de ampliación/mejora si ha lugar.

4.- Anexos donde aparezcan fotocopias y/o documentación técnica si se considera necesario. Bibliografía que se ha empleado.

Todos los programas y diseños han de aparecer comentados. Se valorará la claridad en este aspecto. Por imperativos legales la memoria no se devolverá al alumno.

MATERIAL USADO

Para la realización de las prácticas se hará uso del siguiente material:

1. Manuales específicos de programas que se obtendrán de Internet o de la pagina de la asignatura.
2. Simulador de Redes BOSON.
3. Snifer de RED Ethereal.
4. Instalación SUSE LINUX.
5. Acceso a los servidores del aula.

PRÁCTICA Nº 1: CONFIGURACIÓN de REDES UNIX y EMPLEO DE HERRAMIENTAS DE RED.

OBJETIVOS

Aprender como conocer las características TCP/IP de un sistema.

MATERIAL

PC con instalación SuSE LINUX.
Conexión a Servidores vía ssh/vnc.

PROCEDIMIENTO

Utilizando los ficheros y comandos que se describen en la primera parte de la documentación, se deben hacer los ejercicios de la segunda.

Primera parte: Descripción de ficheros y comandos

Ficheros

Todos los ficheros que vamos a ver son ficheros Unix BSD. En otros sistemas Unix suelen estar ubicados en otros puntos, pero se mantienen links hacia las posiciones aquí indicadas para mantener compatibilidad con BSD. En Windows no siempre hay ficheros equivalentes. A menudo, la información que en Unix dan estos ficheros, debe conseguirse en Windows mediante el comando *winipcfg*.

/etc/hosts

Lista de direcciones IP y nombres de máquinas que les corresponden. En general, sólo contiene entradas para su máquina y tal vez alguna otra "importante", como servidores de nombres o encaminadores. El servidor de nombres de nuestra máquina lo usa para proporcionar a otras máquinas traducción de nuestro nombre a nuestra dirección IP. En este fichero siempre aparece una línea para el *loopback* (dirección 127.0.0.1).

/etc/networks

Contiene las direcciones de red que aparecen en la tabla de encaminamiento. No es la única fuente de información para construir esa tabla. Nuestro sistema no lo usa para ello.

/etc/netmasks

Contiene las máscaras de red de las redes conocidas.

/etc/ethers

Contiene las relaciones entre nombres de host y direcciones ethernet. Este fichero sólo es usado si nuestra máquina debe actuar como servidora de red para máquinas sin disco, para contestar a peticiones RARP.

/etc/protocols

Nombres y números identificadores de los protocolos implementados

/etc/services

Lista los puertos que corresponde a cada aplicación.

Comandos

Los comandos que se dan a continuación corresponden a un sistema Unix, pero también los tienes disponibles en Windows (excepto el primero). Para conocer más sobre ellos, así como las opciones que ofrecen, usa el manual interactivo (man comando).

ssh

SSH es la abreviatura de secure shell, permite conectar con la máquina remota y ejecutar comandos en dicha máquina, permite mantener una sesión cifrada entre sistemas. Con telnet ocurre algo parecido, ya que uno de los problemas que plantea es que la contraseña se envía en claro por la red. Con ssh no porque utiliza autenticación. Nosotros lo utilizaremos para conectarnos al servidor redes.diesia.uhu.es.

ssh hostname

-c cifrado
-p puerto del servidor al que debe conectarse
$ ssh -c 3des -p 7000 hostname

NAME
ssh - OpenSSH secure shell client (remote login program)

SYNOPSIS
ssh [-l login_name] [hostname | user@hostname] [command]

ssh [-afgknqtvxACPX46] [-c blowfish | 3des] [-e escape_char] [-i identity_file] [-l login_name] [-o option] [-p port] [-L port:host:hostport] [-R port:host:hostport] [hostname | user@hostname] [command]

DESCRIPTION
ssh (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel.

hostname

Da el nombre de nuestra máquina.

ping

El comando ping se utiliza generalmente para testear aspectos de la red, como comprobar que un sistema está encendido y conectado; esto se consigue enviando a dicha máquina paquetes ICMP (de tipo ECHO_REQUEST), tramas que causarán que el núcleo del sistema remoto responda con paquetes ICMP, pero esta vez de tipo ECHO_RESPONSE.

```
ping [-n <x>] [-l <y>] [-i <z>] [-f] <ipaddr>
```

-n <x> Envía <x> paquetes ICMP
-l <y> Envía paquetes de longitud <y>
-i <z> Limita la vida del paquete (TTL) a <z>
-f Activa el bit Don't fragment
<ipaddr> Dirección IP de destino

```
ping smtp.uc3m.es
PING smtp.uc3m.es (163.117.136.123): 56 data bytes
64 bytes from 163.117.136.123: icmp_seq=0 ttl=253 time=3.4 ms
64 bytes from 163.117.136.123: icmp_seq=1 ttl=253 time=1.7 ms
64 bytes from 163.117.136.123: icmp_seq=2 ttl=253 time=1.8 ms
64 bytes from 163.117.136.123: icmp_seq=3 ttl=253 time=2.3 ms
64 bytes from 163.117.136.123: icmp_seq=4 ttl=253 time=2.4 ms
64 bytes from 163.117.136.123: icmp_seq=5 ttl=253 time=1.9 ms
64 bytes from 163.117.136.123: icmp_seq=6 ttl=253 time=2.0 ms
64 bytes from 163.117.136.123: icmp_seq=7 ttl=253 time=1.6 ms
64 bytes from 163.117.136.123: icmp_seq=8 ttl=253 time=1.6 ms
64 bytes from 163.117.136.123: icmp_seq=9 ttl=253 time=2.2 ms
64 bytes from 163.117.136.123: icmp_seq=10 ttl=253 time=1.8 ms
<Ctrl+C>
--- smtp.uc3m.es ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max = 1.6/2.0/3.4 ms
```

arp

Muestra la situación actual de nuestra tabla ARP. También puede usarse para actualizar dicha tabla. Su nombre proviene del protocolo (*address resolution protocol*).

Segunda parte: Ejercicios

Haz los ejercicios con asterisco tanto sobre redes.diesia.uhu.es como sobre el PC. Si la respuesta es la misma en ambos casos (el método) simplemente indícalo. En todos los ejercicios hay que indicar brevemente cómo se ha llegado a la respuesta.

1) En tu PC, ¿dónde se sitúa el fichero que hace las funciones del fichero /etc/services de Unix? ¿Y los equivalentes a /etc/protocols y /etc/networks ?

2*) ¿Cuál es la dirección IP de tu máquina? /etc/hosts C:\WINNT\Hosts.sam

UNIX: ifconfig -a
PC: ipconfig

3*) ¿Qué máscara se aplica a tu máquina? /etc/netmasks

UNIX: ifconfig -a
PC: ipconfig

4*) ¿Cuáles son tus identificadores de red y máquina? Se ve a través de la máscara y la dirección IP.

5*) ¿Qué contiene la tabla ARP de tu máquina? (no escribas la tabla completa, basta con decir cómo la ves)

arp -a

6*) ¿Cuál es la dirección ethernet de tu ordenador?

UNIX: arp -a | grep nombre_maquina, o bien ifconfig -a (también con ifconfig eth0, si conocemos las interfases).
PC: winipcfg

7*) ¿Cómo puedes saber cuál es la dirección física de otra máquina de tu misma red? Por ejemplo, ¿cuál es la dirección física de la máquina nat.diesia.uhu.es?

arp nombre maquina. Si no aparece, hacer ping y de nuevo arp.
nslookup nombre maquina.

8*) ¿Cómo puedes saber si un ordenador (por ejemplo redes.diesia.uhu.es) está en tu red?

Tienes que obtener su dirección IP, y mirar en esa dirección sin utilizar nslookup; Una forma de obtener la dirección IP es a través de ping -s

9*) ¿Cómo puedes saber qué puerto corresponde a una aplicación?

cat /etc/services | grep nombre_aplicación. También con netstat –a, pero sólo aparecerán los que están activos.
PC: Mirar en C:\WINNT\Services

10*) ¿Cuánto tiempo necesitará un datagrama para llegar a su destino desde tu máquina? Calcula, por ejemplo, el tiempo necesario, más o menos, para alcanzar la máquina www.uhu.es.

ping ó ping -s

11*) ¿Qué camino sigue el datagrama anterior para llegar a su destino?

Traceroute / ping –sRv www.uhu.es

PC: Tracert / ping –r

12) Calcula, usando ping, la tasa de errores del camino entre dos ordenadores.

ping –I 1 dest tam num_env. Conviene ejecutar en paralelo varias veces.

PRÁCTICA Nº 2 : CONFIGURACIÓN DE REDES Y ANALISIS DE PAQUETES USANDO SNIFFER

OBJETIVOS

Aprender como conocer las características TCP/IP de un sistema. Aprender a usar un snifer para detectar fallos de red.

MATERIAL

PC con instalación SuSE LINUX.
Conexión a Servidores vía ssh/vnc.
Sniffer de paquetes Ethereal.

PROCEDIMIENTO

Utilizando los ficheros y comandos que se describen en la primera parte de la documentación, se deben hacer los ejercicios de la segunda.

Primera parte: Descripción de comandos

Además de los comandos que se vieron en el primer laboratorio TCP/IP, son útiles los que se dan a continuación. Recuerda que corresponden a un sistema Unix, aunque algunos también están disponibles en Windows. Para conocer más sobre ellos, así como las opciones que ofrecen, usa el manual interactivo (se usa tecleando man <comando>).

Ethereal

Se utiliza para capturar todos los paquetes que circulan por un determinado dispositivo de red instalado en el ordenador. Tiene comando de “Start” para comenzar la captura y comando de “Stop” para finalizar la captura. Una vez recogida la traza de paquetes se puede observar cada uno de ellos aportando información de su contenido.

Arrancar el ordenador del aula en Windows2000 y conectarse de forma remota al servidor redes.diesia.uhu.es. Ejecutar los comandos en el servidor y en el PC y analizar las trazas resultantes de la operación.

ifconfig

Da información básica sobre la configuración de los interfaces. Se usa para detectar problemas con las direcciones IP, máscaras de subred, o direcciones de broadcast. Siendo superusuario, se usa para configurar los interfaces, activar o desactivar arp, o alterar el costo asociado a un interfaz en la tabla de encaminamiento.

Lo más aproximado en Windows es *winipcfg*, en Windows NT/2k/XP se emplea *ipconfig*.

netstat

Es el comando más usado para control de red. Puede ofrecer información sobre la tabla de encaminamiento, estado de los interfaces, actividad en cada puerto, contenido de la tabla ARP, etc.

route

Usado para ver y actualizar la tabla de encaminamiento. Sólo puede usarse con privilegios de superusuario.

Ejemplo:

/sbin/route

```
Kernel routing table
Destination Gateway Genmask Flags MSS Window Use Iface
localnet * 255.255.255.0 U 1500 0 23 eth0
loopback * 255.0.0.0 U 3584 0 2 lo
default si3101.si.ehu.es * UG 1500 0 19 eth0
```

traceroute

Sirve para hacer un seguimiento del camino seguido por los datagramas a través de la red hasta llegar a su destino. No lo tenemos disponible en servidor_redes, pero parte de su funcionalidad puede conseguirse con ping. En Windows hay una versión del mismo llamada *tracert*.

Ejemplo:

traceroute izar.eusnet.org

```
traceroute to 194.224.110.2 (194.224.110.2), 30 hops max, 40 byte packets
1 si3101.si.ehu.es (158.227.112.1) 1.316 ms 1.702 ms 2.778 ms
2 158.227.194.224 (158.227.194.224) 3.747 ms 3.591 ms 3.245 ms
3 S4-4.EB-Bilbao1.red.rediris.es (130.206.210.1) 4.982 ms 5.147 ms 4.396
ms
4 A1-0-6.EB-Madrid1.red.rediris.es (130.206.224.21) 13.108 ms 11.319 ms
10.832 ms
5 A1-0-1.EB-Madrid0.red.rediris.es (130.206.224.69) 12.726 ms 12.031 ms
12.295 ms
6 Ibernet-2.red.rediris.es (130.206.192.238) 118.191 ms 72.564 ms 80.904
ms
7 194.179.3.130 (194.179.3.130) 147.024 ms 160.054 ms 228.512 ms
8 194.179.16.156 (194.179.16.156) 853.409 ms 814.393 ms 582.425 ms
9 194.224.110.2 (194.224.110.2) 1282.63 ms 965.919 ms *
```

Segunda parte: Ejercicios

Haz los ejercicios con asterisco tanto sobre redes.diesia.uhu.es como sobre el PC. Si la respuesta es la misma en ambos casos (el método) simplemente indícalo. En todos los ejercicios hay que indicar brevemente cómo se ha llegado a la respuesta. Apunta tus respuestas en hoja aparte, para acompañar a la memoria de prácticas.

1) ¿Cuál es el mínimo número de puertos libres (denominados *no private* en Unix) en redes?

cat /proc/net/sockstat

2) ¿Cuál es el valor del ttl (Time To Live) usado en redes?

/sbin/sysctl –a | grep net.ipv4.ip_default_ttl

3) ¿Cuál es el valor del temporizador de inactividad (keepalive)?

/sbin/sysctl –a | grep net.ipv4.tcp_keepalive_time

4*) ¿Cuántos interfaces de red tiene tu máquina? ¿Cuáles son sus direcciones físicas? ¿Y sus direcciones IP?

ifconfig -a. netstat -i

Con winipcfg/ipconfig en Windows solo aparece un interfaz. No referencia al local (loopback).

5) En un interfaz que esté funcionando con normalidad no debe haber tramas encoladas pendientes de envío u overruns (eso sería señal de que o el cable no está bien conectado o la tarjeta no funciona bien, o el ordenador no recoge las tramas de la tarjeta a tiempo). Revisa ese parámetro en los interfaces de tu máquina (no tengas en cuenta el *loopback*)

netstat -i . Sobre el PC no se puede saber, no saca esas estadísticas

6) Una tasa de errores demasiado elevada (más de 100 puede ser una cifra orientativa) en la entrada o salida de un interfaz es un síntoma de problemas. Si hay muchos errores de salida, quiere decir que la red está saturada o que hay un problema físico en la conexión con la red. Si son muchos los de entrada, puede ocurrir alguna de las dos cosas anteriores, o que la máquina local está sobresaturada de trabajo. Revisa esos parámetros en los interfaces de tu máquina (no tengas en cuenta el *loopback*). Si sospechas que la red está saturada (más de un 5% de colisiones) ¿Cómo comprobarás cual es la tasa de colisiones que se están dando?

netstat -i . Sobre el PC no se puede saber, no saca esas estadísticas

7*) Mirando en el fichero /etc/services podemos ver cuáles son los puertos que corresponden a cada servidor de aplicaciones. Pero eso no nos sirve para saber qué

puertos son los que están usando los clientes que estemos ejecutando. ¿Cómo puedes saber eso?

netstat -a

8) Podemos ver el programa que tiene el puerto ejecutando netstat como usuario root.

netstat -p

9*) ¿Con qué otras redes está conectada tu red? ¿A través de qué encaminadores se pasa a esas otras redes?

route; netstat -r (este último saca también los nombres). En Windows sólo se puede utilizar el último.

10) ¿Cómo podemos saber si en un puerto concreto hay alguna actividad? ¿Y para saber qué conexiones hay abiertas en un momento dado en un puerto?

netstat –a | grep <nombre.puerto> ej: ssh

11*) ¿Por qué encaminadores pasa un datagrama hasta alcanzar su destino? Haz la prueba con www.uhu.es

traceroute www.google.com En W95:tracert, o bien ping -r 4 www.uhu.es

12) Analizando la ejecución de traceroute dada en el ejemplo, responde las siguientes preguntas:

-¿Cuantos encaminadores de la UHU se atraviesan en el camino?

-¿Qué paso del camino lleva más tiempo recorrer?

13) Sitúate en la URL *http://www.slac.stanford.edu/comp/net/wan-mon/traceroute-srv.html* y analiza a partir de las facilidades que en ella se ofrecen los caminos que siguen los datagramas provenientes de distintas partes del mundo para llegar hasta la red de la UHU. Estudia cuáles son los puntos críticos en esos caminos.

14) Averigua la dirección del servidor DNS.

Cat /etc/resolv.conf

15) Comprueba que el servidor DNS está activo. ¿Cuál es el nombre del servidor DNS?

16) Interroga al servidor DNS sobre la dirección IP de www.uhu.es

PRÁCTICA Nº 3 : PROGRAMACIÓN DE ROUTERS.

OBJETIVOS

Introducción al manejo de Routers de CISCO y el sistema operativo CISCO IOS.

MATERIAL

PC con instalación SuSE LINUX.
Conexión a Servidores vía ssh/vnc.
Emulador de Redes BOSON.

CONCEPTOS BÁSICOS

1.- Introducción.

Los enrutadores cisco tienen tres posibilidades de acceso para ser configurados:

- **Consola**: Usaremos el hyperterminal de un PC para establecer la conexión.
- **Auxiliar**: igual que la consola pero a través de un módem.
- **Telnet**. Una vez activo el enrutador podemos acceder desde cualquier ordenador conexo a la red que permita realizar telnet.

En ambos la mecánica de conexión es la misma: al principio se nos presenta un mensaje de bienvenida, a continuación, pulsando enter, entramos en el modo usuario. En este estado hay pocas instrucciones a nuestra disposición, sobre todo de diagnóstico (Ping, traceroute, show version, etc...). En el modo administrador, tenemos control sobre la configuración del enrutador. Los comandos que vamos a emplear son los siguientes:

- **Enable**: pasa de modo usuario a administrador.
- **Disable**: pasa de modo administrador a modo usuario.
- **Logout**: sale incluso de modo usuario dejando la conexión libre.

2.- La CLI.

La CLI (*Command Line Interface*) es el intérprete de comandos de los enrutadores cisco. Tiene la misma mecánica en todos los modelos, independientemente del software que soporten. A continuación presentamos algunas utilidades de la misma:

- **<TAB>** completa el comando si hemos escrito lo suficiente del mismo como para identificarlo. Ejemplo, si pulsamos s + <TAB>, no obtenemos nada, pero si pulsamos sh + <TAB> vemos que aparece show. Esto es porque con s también hay otros comandos pero con sh sólo empieza show.

- **?** Proporciona una ayuda respecto a las opciones posibles para la CLI. Es decir, si pusamos sh ? veremos todas las opciones accesibles desde este comando.

2.1.- El sistema de ficheros.

Los archivos principales que nos encontraremos en un enrutador son:

- **Rommonitor**: Es un sistema operativo básico del enrutador. Se ejecuta al encenderlo, realiza labores de autodiagnóstico y en función del registro de configuración busca y descomprime la IOS.
- **IOS**: Es un segundo sistema operativo que contiene todas las funcionalidades de enrutamiento y de servicios necesarios. La IOS está comprimida en una memoria no volátil (típicamente la flash memory), y en el proceso de arranque se descomprime volcándose en la RAM donde inmediatamente se ejecuta.
- **startup-config**: Es el fichero de configuración del sistema. Se halla en la nvRAM o en la flash. Se carga en la RAM al comenzar tomando el nombre de running-config.
- **running-config**: Es el fichero activo de configuración. Se inicializa con una copia del startup-config, a partir de ahí reflejará cualquier cambio que realicemos. Dichos cambios tienen efecto desde el mismo momento en que dejamos de editar este fichero. Si no salvamos su contenido dentro de la startup-config, desaparecerán al reiniciar el equipo.

Los comandos más relevantes que podemos emplear para gestionar el sistema de fichero son:

- **Show versión**: muestra la versión de la IOS, así como el nombre del fichero utilizado y detalles sobre el mismo (tamaño, fecha, etc...). Además listará el registro de configuración (config-register).
- **Show running-config**: Lista el fichero running-config.
- **Show startup-config**: Lista el fichero startup-config.
- **Show flash:** Lista el contenido de la flash.
- **Show nvram**: Lista el contenido de la nvram.
- **Write**: salva la configuración actual en el fichero startup-config.
- **Erase** [dispositivo:fichero]: borra el fichero especificado.
- **Copy** [dispositivo:fichero_origen] [dispositivo:fichero_destino]: Copia un fichero de un sitio a otro. Ejemplo: copy tftp:c2600-mi-z.bin flash:c2600-mi-z.bin. Con esta instrucción el enrutador busca un servidor tftp desde el que descargar un fichero de IOS cuyo nombre es c2600-mi-z.bin, sobre la flash sin modificar dicho nombre.

El proceso de configuración tiene lugar de la siguiente forma : una vez en modo privilegiado usaremos los siguientes comandos para editar el running-config:

- **Configure terminal** (conf t en modo abreviado). Al ejecutarlo vemos que nos cambia el prompt avisándonos que estamos en disposición de acceder al corazón del router.
- **Int** [interfaz]: con este comando podemos entrar en la configuración especifica de un interfaz. Al ejecutarlo veremos como nos vuelve a cambiar el prompt informándonos del nivel en el que estamos.
- **Ip address** [dirección IP] [máscara]: en cualquier interfaz lo primero que tenemos que habilitar para poder establecer una conexión es su IP.

- **No shutdown**: Con esto habilitamos el interfaz. En principio todos los interfaces están desactivados. Para eliminar una instrucción (shutdown) lo único que tenemos que hacer es precederla con la palabra “no” y ya está.
- **Encapsulation** [modo de encapsulamiento]: En los interfaces serial (no así en los ethernet) es necesario especificar algún tipo de encapsulamiento a nivel 2.
- **Line con 0**: Igualmente, cualquier otro dispositivo reflejado en la running-config es accesible desde el modo de configuración con sólo escribirlo y pulsar enter. En este caso entramos en la configuración de consola.
- **End** Así salimos del modo de configuración.
- **Router rip**: Además de en los interfaces, ciertas instrucciones se agrupan bajo un mismo nivel. Por ejemplo con este comando entramos en el nivel de configuración del protocolo rip.
- **Network** [red] Esta instrucción se anida bajo el nivel de rip y le indica qué red (o redes si la repetimos) ha de propagar a otros enrutadores vecinos.

2.2.- Niveles de protección. Las claves.

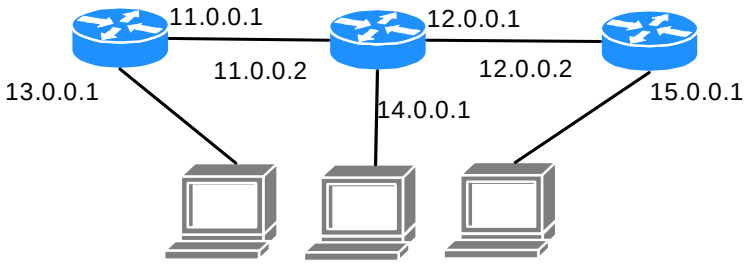
Existen varios niveles de protección que podemos activar en el enrutador:

- **Password** [clave]: nos indica la clave de acceso dentro del nivel deseado (entrada por consola, por telnet o auxiliar).
- **Passwod encryption**: oculta la clave usada al observador cifrándola.
- **Enable secret** clave: es una clave de ámbito general.

También existen una serie de comandos que nos permiten informar de ciertas configuraciones. Estos son:

- **Hostname** [nombre] Asigna un nombre al enrutador.
- **Description** [mensaje] Ejecutada bajo un interfaz, sirve para recordarnos adónde nos conecta.
- **Banner motd** [carácter][mensaje][carácter] El mensaje nos aparecerá cada vez que nos conectemos al router, sobretodo si lo hacemos vía telnet.

PROCEDIMIENTO



Utilizar tres routers CISCO de la serie 3000 con dos interfaces ethernet, una en cada slot, a excepción del central que tendrá un slot con una interfaz y el otro con dos interfaces.

Los PCs no son necesarios para contestar a las cuestiones. Aunque configurados con una dirección de red válida pueden servir para probar la red a partir de la cuestión número 8.

1. Accede al modo usuario y al privilegiado y describe tres comandos que no aparezcan en uno y sí en el otro.

2. ¿Se puede ver el sistema de ficheros de la IOS desde el modo usuario?

¿Qué versión hay?

¿Cuál es el nombre del fichero de la IOS?

Anota el valor hexadecimal del registro de configuración.

3. ¿Se puede ver el running-config desde el modo usuario?

Cita tres instrucciones preestablecidas en la configuración.

¿Cuántos interfaces tiene el router y de qué tipo son?

4. Entra en el modo configuración y cita tres instrucciones operativas en este modo que no estén disponibles en el modo privilegiado.

5. Ejecuta copy running-config startup-config. Establece en las interfaces Ethernet unas direcciones IP de clase C que sean válidas, diferentes de las del diagrama.

¿Aparece en el running-config?

¿Y en el startup-config?

Ejecuta copy running-config startup-config y comprueba ahora las diferencias entre ambos.

Cambia la IP de las interfaces por otras y vuelve a listarlos, anota las diferencias. ¿Qué deberíamos ver?

6. Lista los ficheros que haya en la flash.

7. Entra en el modo de configuración y designa un nombre diferente para cada router.

8. Configura los interfaces de los tres routers para que puedan llegar los pings de uno a otro como están en el diagrama de la página anterior. Anota aquí las direcciones y el mensaje del ping resultante.

9. Designa también una referencia dentro del interfaz que nos identifique la conexión. Por ejemplo “Conexión al enrutador central “.

10. Ejecuta un ping desde el router de un extremo hasta el del otro. Comenta el resultado.

11. Anota la dirección hardware de los interfaces ethernet existentes. ¿Cuál es la MTU?

12. Lista la tabla de rutas de cada uno de los routers y anota las redes identificadas. ¿Hay alguna aprendida por RIP?

13. Habilita RIP en todos los interfaces de los routers izquierdo y central. Visualiza la tabla de rutas y comenta las diferencias. Haz ping desde el router izquierdo a los dos interfaces del router central, ¿Llegan? Haz ping al router derecho, comenta detalladamente el resultado.

14. Habilita RIP en el router derecho en todos sus interfaces. Haz ping de extremo a extremo. Analiza el proceso y comenta las diferencias con las tablas de rutas actuales.

15. Configura el router para que nos reciba con un mensaje de bienvenida.

16. Especifica una clave. Haz logout e intenta entrar.

17. Especifica una clave cifrada. Anota la clave original y la que aparece en el running-config. Haz logout e intenta entrar. ¿Cuál de las dos es la que sirve?

PRÁCTICA Nº 4 : ACCESO A OTROS ROUTERS: PROTOCOLO DESCUBRIMIENTO DE CISCO.

OBJETIVOS

Acceso a Routers. Manejo de comandos del protocolo CDP.

MATERIAL

PC con instalación SuSE LINUX.
Conexión a Servidores vía ssh/vnc.
Emulador de Redes BOSON.

CONCEPTOS BÁSICOS

1.- Introducción.

El protocolo de descubrimiento de Cisco (CDP) permite a los administradores de redes acceder a un resumen de las configuraciones de otros routers directamente conectados. CDP se ejecuta sobre la capa de enlace de datos.

Aparece activado por defecto, lo que permite al dispositivo detectar los dispositivos cisco CDP vecinos, sin importar qué protocolos de capa 3 y 4 estén ejecutando.

- **No cdp run**: desactiva CDP
- **Cdp run**: activa CDP

Aun así, es necesario activarlo explícitamente en cada uno de los interfaces del dispositivo

- **cdp enable**: activa CDP sobre la interfaz
- **no cdp enable**: desactiva CDP sobre la interfaz

El uso principal de CDP es descubrir protocolos y plataformas en los dispositivos vecinos.

PROCEDIMIENTO

1. Crear una topología de red conectando tres routers, cada uno de ellos con dos interfaces ethernet, en triángulo. Asignar direcciones IP a cada interfaz.

2. Comprueba que el protocolo CDP está activo por defecto con show cdp.

3. Desactiva CDP y comprueba el cambio. Después vuelve a activarlo.

4. Accede al modo privilegiado y activa el protocolo CDP sobre cada una de las interfaces de los routers.

5. Visualiza el valor de la configuración global de CDP mediante el comando show cdp. ¿Cada cuanto tiempo se envían actualizaciones CDP?. ¿Cuánto tiempo se mantiene la información guardada de los vecinos?.

6. Cambiar el tiempo entre actualizaciones CDP: cdp timer {tiempo nuevo}.

7. Cambiar el tiempo que se mantiene la información guardada: cdp holdtime {tiempo nuevo}.

8. Verificar cambios con show cdp.

9. Utiliza los comandos show cdp neighbors y show cdp neighbors detail para visualizar actualizaciones de CDP en el router local. Comentar los resultados comparativamente e indicar los valores de los siguientes parámetros:

a. Identificadores de dispositivo
b. Lista de direcciones
c. Identificador de puerto
d. Lista de capacidades
e. Versión
f. Plataforma

10. Utiliza el comando show cdp interface para ver los valores de los temporizadores CDP, el estado de la interfaz y la encapsulación utilizada por CDP en cada interfaz.

11. Identificar las direcciones IP del router vecino y tiempo desde que se recibió esa información mediante una trama CDP utilizando el comando show CDP entry {nombre de dispositivo}.

12. Desactivar CDP en una interfaz.

13. Volver a ejecutar show cdp interface y show cdp neighbours detail. Comenta los resultados.

PRÁCTICA Nº 5 : GESTIÓN DE TRAFICO.

OBJETIVOS

Aplicar métodos de enrutamiento orientados a la gestión del trafico IP.

MATERIAL

PC con instalación SuSE LINUX.
Conexión a Servidores vía ssh/vnc.
Emulador de Redes BOSON.

CONCEPTOS BÁSICOS

1.- RUTAS.

La propagación de rutas mediante protocolos de enrutamiento (RIP, OSPF, EIGRP, etc...) no siempre es deseada en puntos de la red donde la seguridad pueda verse comprometida. No obstante, el tráfico ha de ser dirigido de alguna forma. Para ello se utilizan las llamadas rutas estáticas, éstas consisten en inscripciones directas sobre la tabla de rutas de nuestro equipo.

La sintaxis es: Router(config)#**ip route** (red de destino) (máscara) (IP del siguiente salto por el que se llega a dicha red) [coste]. Por ejemplo: ip route 10.0.0.0 255.0.0.0 192.168.56.103.

Esta instrucción establece una entrada en la tabla de rutas que indica a nuestro equipo que, cuando reciba un paquete con una IP de destino perteneciente a la red 10.0.0.0 con máscara A, debe enviarlo a un router conexo a él cuya dirección es la 192.168.56.103 (exactamente es la dirección del interfaz que “mira” a nuestro equipo).

Las rutas estáticas no se propagan por Rip aunque lo tengamos activado. El coste se utiliza para comparar rutas alternativas a una misma red. Pondremos un valor de acuerdo a la fiabilidad del enlace. Un caso especial de ruta estática es la denominada “ruta por defecto” (default gateway) que es aquella que tomarán todos los paquetes cuyas redes no estén especificadas. Es una alternativa de último recurso para evitar el descarte del paquete.

En los routers cisco hay varias formas de especiticar una ruta estática:

Router(config)#**ip default-network** (red de la IP de escape).
Router(config)#**ip default-gateway** (IP de escape); válida si no hay routing.
Router(config)#**ip route** 0.0.0.0 0.0.0.0 (IP de escape) ; más común.

2.- Filtros.

Después del enrutamiento, el **uso de filtros** es la segunda funcionalidad en importancia atribuida a un router. Los filtros se aplican al tráfico de un determinado interfaz para permitir o bloquear determinados paquetes según sus características. La implementación de los filtros en routers Cisco se realiza mediante lo que se llaman listas de acceso

(*access list*), que contienen el conjunto de restricciones a aplicar sobre el interfaz. Hay tres tipos de listas:

a) Estándar: Se configuran en modo global con la instrucción:

Acces-list (nº) (permit/deny) (red origen) (máscara);
Acces-list (nº) (permit/deny) host (ip origen);
Acces-list (nº) (permit/deny) any;

El número lo elegiremos entre el 1 y el 99. Permit significa que el paquete será enrutado y deny descartado. Como elemento a cotejar disponemos de la red origen del paquete, su IP, o cualquiera si ponemos any.

b) Extendidas:

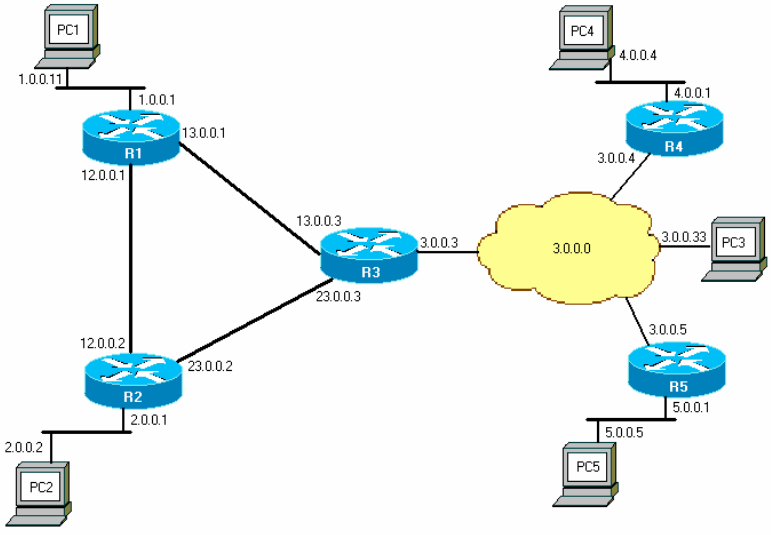
Acces-list (nº) ... ; un número del 100 al 199
...(permit/deny)... ; indica si el paquete va a ser admitido o descartado.
... (protocolo)... ; especifica el protocolo encapsulado (TCP,UDP,ICMP..)
....(red origen)... ; como antes se puede poner aquí host para indicar un
...(máscara)... ; sólo PC en vez de una red, o bien el comodín any.
...(operador)... ; por ejemplo eq significa igual, lt menor que y se aplica
...(operando)...;sobre el operando que es un puerto.
...(red orígen) (máscara) (operador) (puerto) ; lo mismo pero refiriéndonos al destino.
... [established] ; coteja todos los flujos tcp excepto el primero.

c) Con nombre: igual que las extendidas sólo que se definen con un nombre en vez de con un número:

ip access-list (standard/extended) (nombre); ahora pulsamos intro y cambiamos a un modo que nos permite introducir las condiciones que comienzan con (permit/deny) y resto de parámetros.

Una vez definida la lista, para aplicarla sobre un interfaz, nos introducimos en el nivel de configuración correspondiente y ejecutamos: Router(config-ethernet0)#**access-group** (nº) (in/out)

PROCEDIMIENTO PARTE A: RUTADO



1. Construye el diseño mostrado en la figura y configura los interfaces con las redes indicadas, utiliza un switch “Catalyst 1900” para la red 3.0.0.0. Verifica la conectividad inmediata realizando pings entre cada par de dispositivos.

2. Ejecuta sh ip route sobre los routers 1, 3 y 5. Anota las entradas presentes. ¿Podría llegar un ping desde el router 1 hasta el 5? Explica por qué.

3. Habilita RIP en los routers 3, 4 y 5. Usando el comando sh ip route anota la tabla de rutas del R3. ¿Cuáles ha aprendido por rip?. ¿Cómo conoce las demás?. Lista en una tabla qué equipos informan de qué ruta a cual.

4. ¿Llegaría un ping desde el R4 hasta el interfaz serie del R3? ¿Y desde el PC5 hasta dicho interfaz?. Anota el conjunto de equipos entre los cuales llegaría cualquier ping. Describe la trayectoria que seguiría un ping entre PC5 y PC4. ¿Y de PC3 a PC5?. ¿Llegaría un ping desde PC3 a la 13.0.0.1? Si se interrumpe, aclara dónde.

5. Usa rutas estáticas en el R1 para poder alcanzar la red 3.0.0.0. ¿Qué hay que escribir?. ¿Llegaría ahora el ping desde PC3?. Mira la tabla de rutas ¿qué letra aparece al principio? ¿qué significan las letras C,R y S?. ¿Llegaría desde PC3 a PC1?. ¿Qué habría que añadir para que llegara?. Configura el router con tu respuesta.

6. ¿Llegaría un ping desde el router 3 al PC2?. ¿Por qué?. Establece rutas estáticas en R3 para alcanzar la red 2.0.0.0, anota aquí la instrucción. ¿Y si el ping lo genera el PC3, alcanzamos la dirección 23.0.0.2? ¿Y la 2.0.0.1?.Explica por qué.

7. Añade una ruta por defecto en R2 que apunte hacia R3. ¿Nos llegarían ahora los pings desde el PC3 hasta R2?.¿y de R3 a PC2?. ¿Y de PC2 a PC3?. Razona las respuestas y en el último caso describe la ruta que recorre el ping definiendo en cada nodo su tabla de rutas y la decisión que toma.

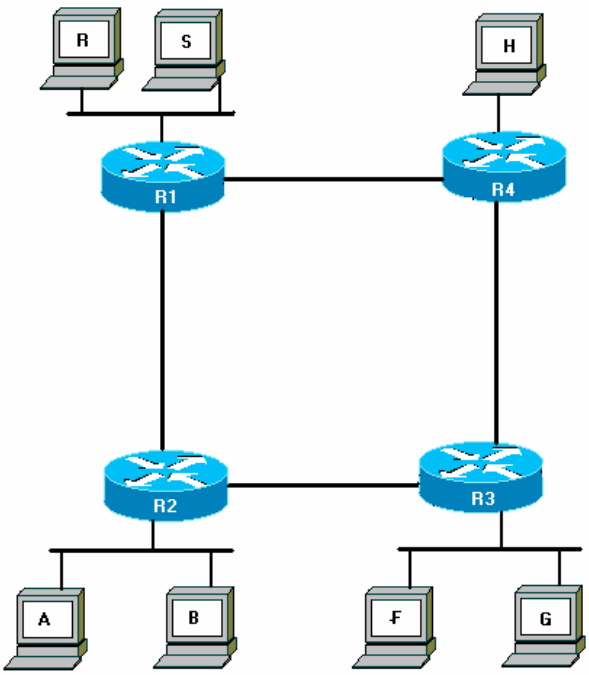
8. En la situación actual ¿llegaría un ping desde R2 a R1?. ¿Qué camino tomaría?. Y desde R2 al interfaz ethernet de R1?, ¿qué camino tomaría a la ida? ¿y la vuelta, tomaría el mismo camino?.

9. Añade ahora otra ruta por defecto en R1 hacia R2. ¿Está ahora todo conectado?. Llegaría un ping desde R3 a la 12.0.0.2?. ¿Qué instrucciones añadirías para lograrlo?.

10. Describe la trayectoria indicando las decisiones que toma cada nodo especificando además su tabla de rutas, de un ping desde PC1 hasta PC3. ¿Y si eliminamos la ruta estática en R1 hacia la red 3.0.0.0?

11.¿Por qué no llegan los pings desde PC1 hasta PC4?. Establece el menor conjunto de rutas estáticas o por defecto a incluir para asegurar la conexión absoluta de la red. Anota las tablas de rutas finales de los routers R2, R3 y R5.

PARTE B: FILTROS Y LISTAS



12. Diseña el esquema de la figura e implementa unas listas de acceso estándar que aseguren el cumplimiento de las siguientes reglas:

F no le está permitido contactar con nadie externo a su LAN.
H puede conectar con A (servidor web) y B (servidor de correo) además de G, pero con nadie más.
A no puede tener comunicación con R ni S.
B no puede comuicarse con R pero sí con S.

¿Se te ocurre alguna otra forma de hacerlo? Anótala. ¿Cuál es la mejor? ¿Por qué?.

13. ¿Cómo lo harías usando las extendidas?.

14. Suponiendo que sólo puedas aplicar las reglas a los paquetes entrantes, anota aquí el conjunto de listas de acceso extendidas necesario.

15. ¿Cómo protegerías de un telnet al equipo H?.