Laboratorio No. 8 –Capa de red y aplicación

Cepeda Alza Johann Alfonso

Posso Guevara Juan Camilo

Escuela Colombiana de ingeniería Julio Garavito

Laboratorio Redes Computacionales

Bogotá D, C.

2021-1

Contenido

[Objetivo 2](#_Toc71838166)

[Herramientas a utilizar 2](#_Toc71838167)

[Infraestructura base 2](#_Toc71838168)

[Experimentos 5](#_Toc71838169)

[1. Asignación de direcciones IP a las redes LAN 7](#_Toc71838170)

[2. EIGRP 8](#_Toc71838171)

[3. Configure el enrutamiento usando OSPF 13](#_Toc71838172)

[Instalación de software base 15](#_Toc71838173)

[1. Servidor DNS Primario Linux - BIND 16](#_Toc71838174)

# Objetivo

En este laboratorio se busca configurar y observar el comportamiento de los protocolos de enrutamiento dinámico y mirar la operación de los protocolos de la capa de red con la interconexión de redes y aplicación a través de su configuración usando Packet Tracer.

# MARCO TEORICO

Protocolos de la capa de aplicación:

FTP (File Transfer Protocol - Protocolo de transferencia de archivos) para transferencia de archivos.

DNS (Domain Name System - Sistema de nombres de dominio).

DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de anfitrión).

HTTP (HyperText Transfer Protocol) para acceso a páginas web.

HTTPS (Hypertext Transfer Protocol Secure) Protocolo seguro de transferencia de hipertexto.

POP (Post Office Protocol) para recuperación de correo electrónico.

SMTP (Simple Mail Transport Protocol) para envío de correo electrónico.

SSH (Secure SHell) TELNET para acceder a equipos remotos.

TFTP (Trivial File Transfer Protocol).

LDAP (Lightweight Directory Access Protocol).

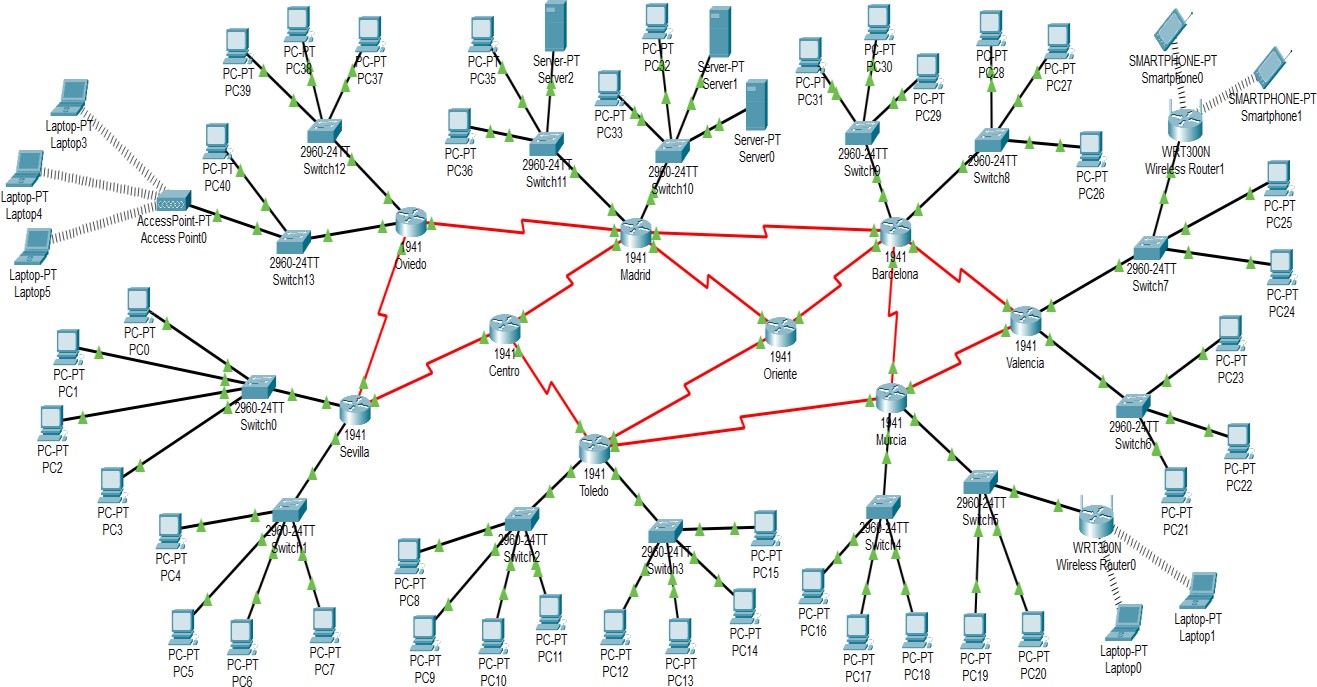
XMPP, (Extensible Messaging and Presence Protocol) - Protocolo estándar para mensajería instantánea. El protocolo de la capa de aplicación en el que se hará énfasis este laboratorio es el protocolo

DNS: El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

# Montaje Base

A continuación, se procedió a elaborar la siguiente red, en packetracer y a la designación de las distintas redes y subredes pertenecientes a cada parte de la ciudad conforme a lo indicado



Para el cual obtuvimos las siguientes redes las cuales fueron asignadas a cada equipo de la red .

**CEPEDA 120.1.0.0/16**



**POSSO 20.2.0.0/16**

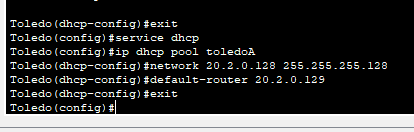
|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | #Host | Red/mask | Broadcast/WillCard |
| Toledo-centro | 2 | 20.2.0.4/30 | 0.0.0.3 |
| Toledo-oriente | 2 | 20.2.0.8/30 | 0.0.0.3 |
| Toledo-Murcia | 2 | 20.2.0.12/30 | 0.0.0.3 |
| Sevilla-centro | 2 | 20.2.0.16/30 | 0.0.0.3 |
| Sevilla-oviedo | 2 | 20.2.0.20/30 | 0.0.0.3 |
| Madrid-oviedo | 2 | 20.2.0.24/30 | 0.0.0.3 |
| Madrid-centro | 2 | 20.2.0.28/30 | 0.0.0.3 |
| Madrid-oriente | 2 | 20.2.0.32/30 | 0.0.0.3 |
| Madrid-barcelona | 2 | 20.2.0.36/30 | 0.0.0.3 |
| Barcelona-oriente | 2 | 20.2.0.40/30 | 0.0.0.3 |
| Barcelona-Murcia | 2 | 20.2.0.44/30 | 0.0.0.3 |
| Barcelona-valencia | 2 | 20.2.0.48/30 | 0.0.0.3 |
| Valencia-murcia | 2 | 20.2.0.52/30 | 0.0.0.3 |
| HRMurcia | 2 | 20.2.0.56/30 | 0.0.0.3 |
| HRValencia | 2 | 20.2.0.60/30 | 0.0.0.3 |
| Sevilla | 30 | 20.2.0.64/27 | 0.0.0.31 |
|  | 75 | 20.2.1.0/25 | 0.0.0.127 |
| Toledo | 40 | 20.2.0.128/26 | 0.0.0.63 |
|  | 120 | 20.2.1.128/25 | 0.0.0.127 |
| Murcia | 190 | 20.2.3.0/24 | 0.0.0.255 |
|  | 200 | 20.2.4.0/24 | 0.0.0.255 |
| Valencia | 340 | 20.2.8.0/23 | 0.0.1.255 |
|  | 240 | 20.2.6.0/24 | 0.0.0.255 |
| Barcelona | 180 | 20.2.2.0/24 | 0.0.0.255 |
|  | 630 | 20.2.16.0/23 | 0.0.1.255 |
| Madrid | 800 | 20.2.20.0/23 | 0.0.1.255 |
|  | 1000 | 20.2.24.0/23 | 0.0.1.255 |
| Oviedo | 550 | 20.2.12.0/23 | 0.0.1.255 |
|  | 230 | 20.2.5.0/24 | 0.0.0.255 |
|  |  |  |  |

## Asignación de direcciones IP a las redes LAN

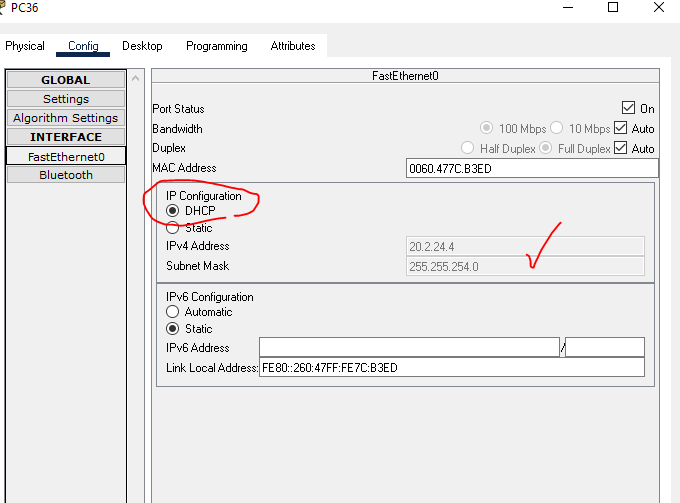
Para la configuración básica hacemos uso del protocolo DHCP con el cual nos ayudara a la asignación rápida de las ip en cada uno de los equipos , para ello primero se agregó cada una de las redes a las cuales no queremos que el protocolo DHCP asigne a los host( ip del Router local)



Una vez hecho esto agregamos las redes en el Router por medio del comando ip dhcp pool, la red y su máscara y el Router por defecto.



Por último, teniendo en cuenta que los equipos tienen que estar en modo dhcp revisamos que la asignación se haga, y así comprobamos que la asignación se realizó adecuadamente:



* 1. .

## EIGRP

Tome **una copia** el montaje del punto anterior y sobre ella configure el protocolo de enrutamiento EIGRP.

Para realizar este laboratorio utilizaremos otro mecanismo de conexión a los routers. Hasta el momento hemos configurado los routers de dos formas:

1. Accediendo directamente a la consola (CLI) del equipo. Válido en packet tracer pero no viable en redes reales, como ya hemos hablado en diversas ocasiones
2. Accediendo por la consola remota a través de un computador y un cable de consola. Válido tanto en packet tracer como en equipos reales si se tiene acceso directo a los equipos

Ahora realizará la configuración de los routers accediendo a ellos de forma remota. Este mecanismo es el más utilizado en redes grandes, se trata de una conexión remota haciendo uso de protocolos de la aplicación que permiten convertirse en una consola de un equipo a través de la red. Para esto usaremos el protocolo TELNET, el cual pertenece a la capa de aplicación, éste permite convertir un computador en consola remota de otro equipo.

Usando el comando TELNET ip\_router, conéctese a los routers para configurar el protocolo de enrutamiento.

* 1. Realice la configuración usando el protocolo EIGRP

En cada router use los siguientes comandos.

router(config)#router eigrp 1

router(config-router)#network ID\_RED Wildcard /\* por cada red \*/ router(config-router)#no auto-summary

router(config-router)#exit router(config)#exit

**Nota**: La Wildcard podría decirse que es el inverso de la máscara, así, si la máscara es 255.255.255.0, la wildcard será 0.0.0.255

* 1. Revise las tablas de enrutamiento generadas con EIGRP. ¿Qué métrica usa para calcular la mejor ruta?

En cada router verifique la configuración de EIGRP y las tablas de enrutamiento. Para esto digite:

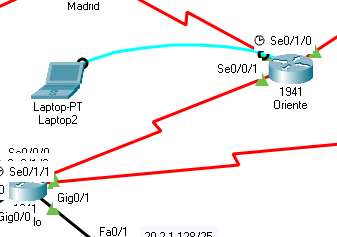
router#show ip eigrp neighbors router#show ip route router#show ip protocols

* 1. Compruebe el funcionamiento de la red y la conectividad entre los computadores de la misma.
  2. Use el comando tracert para revisar las rutas para llegar de un computador en una LAN a otro computador en otra LAN
  3. Baje un enlace serial y verifique la ruta que siguen ahora los paquetes entre dos computadores que usaban antes el enlace que fue bajado.
  4. Interconecte los montajes de los estudiantes así:
     + Estudiante1.Valencia con Estudiante2.Sevilla
     + Estudiante2.Murcia con Estudiante3.Oviedo

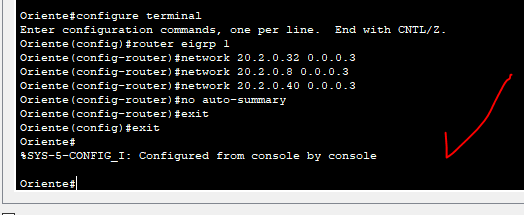
**Nota**: Si está trabajando individual, hable con otro grupo para que le facilite un montaje. Recuerde pedir uno que no coincida con el esquema de direcciones IP que usted está usando.

* 1. Verifique que haya conectividad entre todas las redes.
  2. Desde el computador Laptop0 de cada montaje, verifique que puede acceder a cualquier router de la red y mirar su configuración.
  3. Muestre a su profesor el montaje

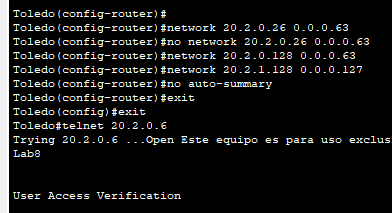
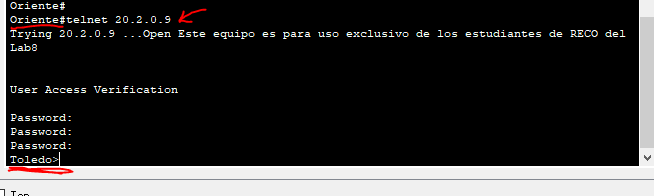
Se hace conexión a uno de los routers de la red , en este caso nos conectamos al Router Oriente por medio de cable consola.



Una vez allí , procedemos a configurar el Router para el enrutamiento eigrp, para cada una de sus redes

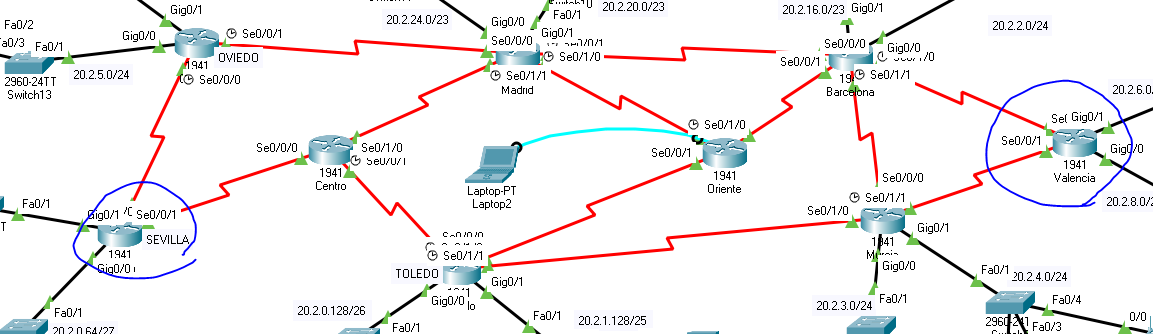


Una vez agregada las redes , le ponemos no auto summary y damos ,exit, como el proposito es configurar todos los equipos de la red remotamente desde el mismo equipo nos conectamos a otro equipo de la red, en este caso como ninguno sabe como llegar a otro equipo lejano nos vamos conectando a los equipos vecinos (es decir los equipos que tienen una conexión en una de las subredes del equipo en el que estamos), en este caso vamos a Toledo por medio del comando **telnet** .

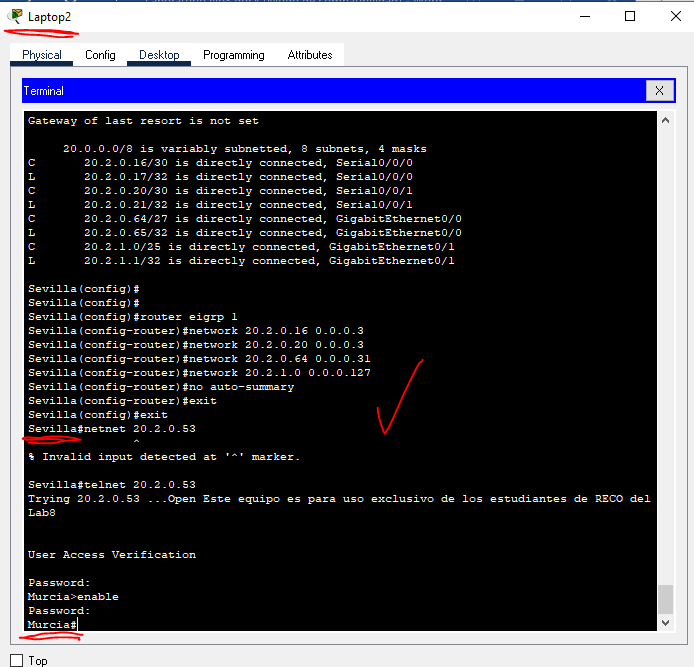


Una vez en este equipo esta configurado vamos recorriendo todos los routers de toda la red .

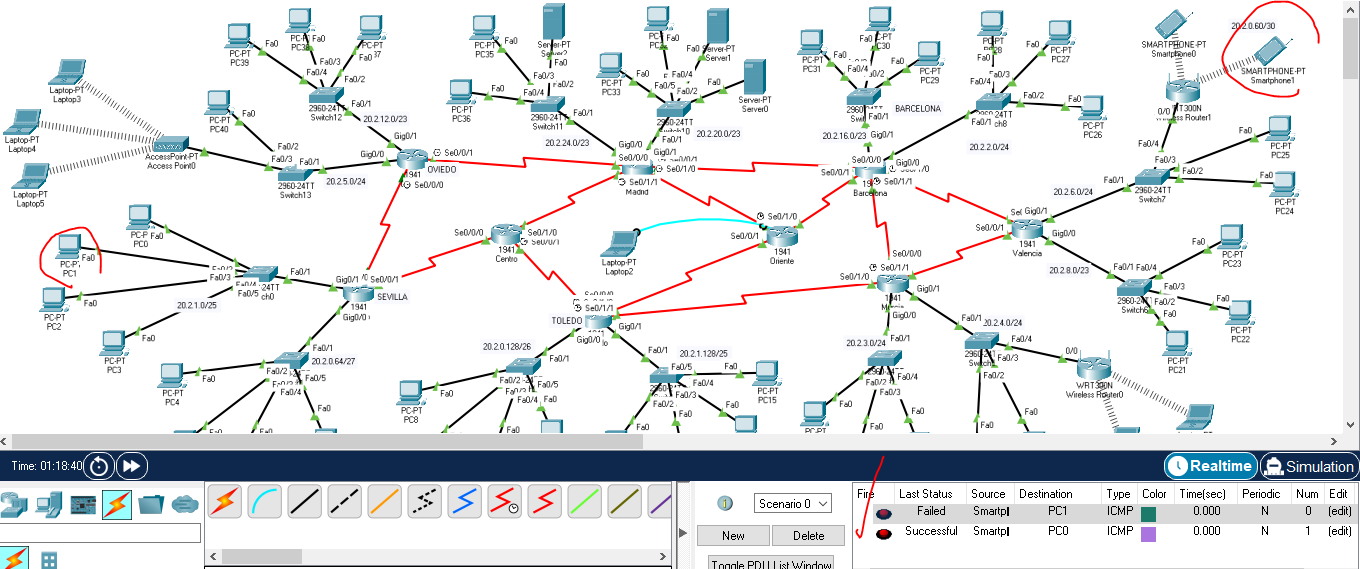
Para probar que hicimos bien toda la configuración con este mismo comando desde el mismo equipo donde hemos hecho toda la configuración de todos los routers nos intentamos conectar de un extremo a otro , en este caso vamos a probar que el equipo SEVILLA se puede comunicar remotamente con VALENCIA,



Finalmente revisamos y efectivqamente existe la conexion



Otra prueba para este punto es conectar un host con otro host al otro lado de la red, en este caso vamos a probar la conexión desde un celular desde valencia a un pc en Sevilla. Y estos fueron los resultados



Lo que demuestra que las conexiones se realizaron correctamente.

## Configure el enrutamiento usando OSPF

Usando otra copia del archivo de base configurado en el punto 1, realice la configuración necesaria para que todos los equipos de la red definida se vean entre sí utilizando el protocolo OSPF para en enrutamiento dinámico.

* 1. Configure OSPF

En cada router use los siguientes comandos. Ejemplo: router.

router(config)#router ospf *n*

router(config-router)#network *ID\_RED Wildcard* area *x*

router(config-router)#exit router(config)#exit

*/\* n=zona. Use 1 \*/*

/\* x=área. Use 0 \*/

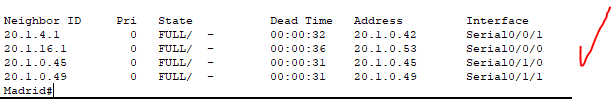
**Nota**: La Wildcard podría decirse que es el inverso de la máscara, así, si la máscara es 255.255.255.0, la

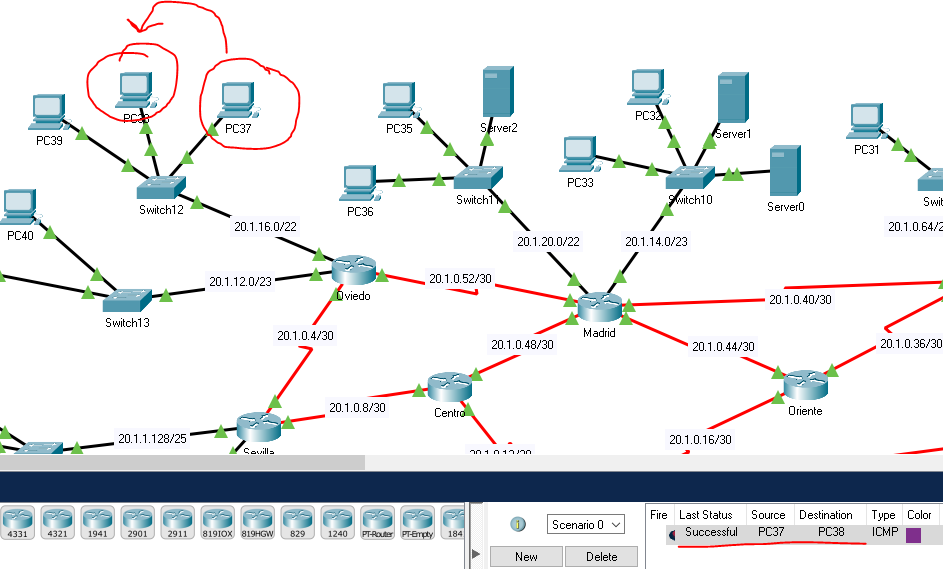
wilcard será 0.0.0.255

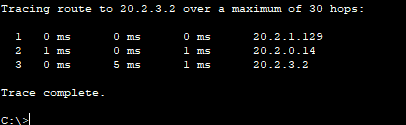
* 1. Revise las tablas de enrutamiento generadas con OSPF

En cada router verifique la configuración de EIGRP y las tablas de enrutamiento. Para esto digite:

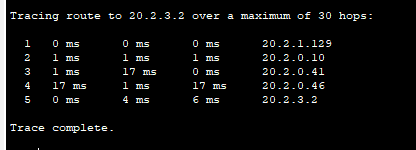
router#show ip ospf neighbors router#show ip route router#show ip protocols



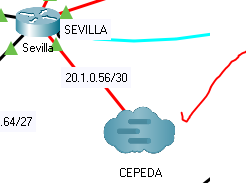
* 1. Compruebe el funcionamiento de la red y la conectividad entre los computadores de la misma.
  2. Use el comando tracert para revisar las rutas para llegar de un computador en una LAN a otro computador en otra LAN



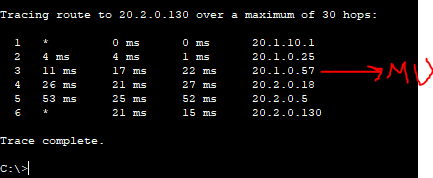
* 1. Baje enlaces seriales y verifique las rutas que siguen ahora los paquetes entre dos computadores que usaban antes los enlaces que fueron bajados.



* 1. Interconecte los montajes de los estudiantes del grupo de la misma manera que lo hicieron en el punto anterior.

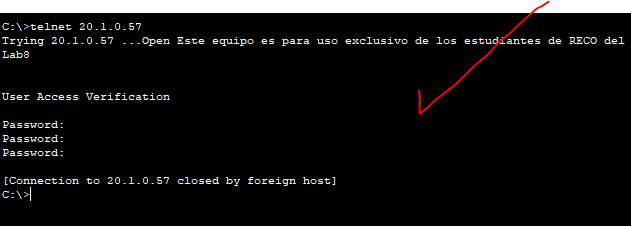


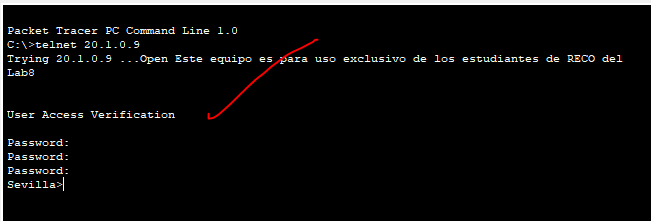
* 1. Realice pruebas de conectividad entre los dos montajes



La red señalada es la conexión multiuser

* 1. Desde el computador Laptop5 de cada montaje, verifique que puede acceder a cualquier router de la red y mirar su configuración.





* 1. Muestre al profesor su montaje final.

# Instalación de software base

Como hemos visto en clase, otro servicio clave en un ambiente empresarial es el servicio Resolución de dominio - DNS. En este laboratorio vamos a configurar dicho servicio usando dos dominios de prueba.

Los dominios que se van a configurar son

1. estudiante1.com.co # ApellidoEstudiante1.com.co
2. estudiante2.edu.co # ApellidoEstudiante2.edu.co
3. estudiante3.org.co # ApellidoEstudiante3.org.co

NOTA: reemplace “estudiante\_n” por el apellido de los miembros del grupo. Ej: ardila.com.co

En cada dominio se deben definir

1. 3 nombres de servidores con sus equivalencias en IPv4 (Use las del rango que se les asignó al principio del semestre). Use los servicios que hemos montado como base para decidir los nombres de los servidores.
2. 2 servidores con sus equivalencias en IPv6 (Escoja las direcciones IPv6 que desee)
3. 2 alias para 2 servidor con dirección IPv4 y 1 servidor con dirección IPv6 (Seleccione los nombres que quiera ponerle)

La implementación debe realizarse usando máquinas virtuales, una FreeBSD, una Windows Server y otra Linux Slackware y se debe instalar de la siguiente manera:

* + - Para el dominio estudiante1.com.co
      * Servidor DNS primario en una máquina virtual FreeBSD
      * Servidores DNS secundarios en una máquina virtual Slackware y Windows Server
    - Para el dominio estudiante2.edu.co
      * Servidor DNS primario en una máquina virtual Slackware.
      * Servidores DNS secundarios en una máquina virtual FreeBSD y Windows Server. En el caso de grupo de 3 estudiantes, cambiar la FreeBSD por Ubuntu.
    - Para el dominio estudiante3.org.co
      * Servidor DNS primario en una máquina virtual Ubuntu.
      * Servidores DNS secundarios en una máquina virtual FreeBSD y Slackware.

La máquina secundaria de estudiante1.com.co y primaria estudiatne2.edu.co es la misma, igual ocurre con la primaria estudiante1.com.co y secundaria estudiante3.org.co y así sucesivamente (en total se configurará el servicio de DNS en 2, 3 o 4 servidores, según la cantidad de estudiantes del grupo). Para las pruebas de funcionamiento, cambie la configuración de DNS Cliente de las otras máquinas virtuales que ha configurado y haga pruebas de resolución de nombres.

## Servidor DNS Primario Linux - BIND

A continuación, se presenta una guía para configurar el servicio de DNS primario.

* 1. Si lo requiere, instale el paquete de DNS del CD/Imagen de Linux

**Comandos**

Servidor# mount /dev/cdrom /mnt/cdrom

/\* Montar el CD de Linux \*/

Servidor# cd /mnt/cdrom/slackwareXXX/n

/\*Ir al directorio específico \*/

Servidor# installpkg bindxxx.txz

/\*Instalar paquete de servicio DNS \*/

Servidor# umount /mnt/cdrom

/\* Desmontar el CD de Linux \*/

* 1. Revise que los paquetes quedaron instalados (ej en el caso de Slackware use pkgtools para revisar).
  2. Configure el servicio

|  |  |  |
| --- | --- | --- |
| Servidor# vi /etc/named.conf | | |
|  | options {  // Se define un directorio en donde se almacenará la información de los  // dominios administrados. En este ejemplo se creó una carpeta DNS dentro de  // de la carpeta /etc. directory "/etc/DNS";  /\*  If there is a firewall between you and nameservers you want to talk to, you might need to uncomment the query-source directive below. Previous versions of BIND always asked |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| questions using port 53, but BIND 8.1 uses an unprivileged port by default.  \*/  // query-source address \* port 53;  };  // Zona para ir a los root server a resolver dominios no conocidos zone "." IN {  type hint;  file "*named.ca*";  };  // Se crea una zona por cada dominio que se vaya a administrar. Se guarda la información en un archivo.  zone "*mi\_dominio*" IN { type master;  file "*mi\_dominio.hosts*";  // Puede ser un nombre de archivo cualquiera, la recomendación es que le archivo se llame como se llama el dominio y use la extensión hosts pero podría llamares de cualquier forma. Ej. Archivo, datos.txt o abcdfg.xyz  allow-update { none; };  };  // Para crear la zona reversa (segunda funcionalidad del servicio de DNS). Pero  // no la vamos a configurar ahora.  // zone "0.0.127.in-addr.arpa" IN {  // type master;  // file "127.0.0.rev";  // allow-update { none; };  //};  Servidor# mkdir /etc/DNS  Servidor# vi /etc/DNS/named.ca  Busque en internet la lista e IPs de los ROOTSERVER. Solo deje las equivalencia IPv4 (Puede borrarlas o ponerlas en comentarios)  ;  ; root name servers  ;  . 3600000 IN NS A.ROOT-SERVERS.NET.  ;  ; root name servers by address  ;  // Buscar en internet la lista de root servers. | | | | | | |  |
|  |  | A.ROOT-SERVERS.NET | 3600000 | IN | A | abc.def.ghi.jkl |  |
|  |  | ;A.ROOT-SERVERS.NET | 3600000 | IN | AAAA | 2001:503:BA3E::2:30 |  |
|  |  | B.ROOT-SERVERS.NET | 3600000 | IN | A | mno.pqr.stu.vwx |  |
|  |  | C. … |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Servidor# vi /etc/DNS/mi\_dominio.hosts  Cada estudiante deberá configurar su archivo.  ;  ; /etc/DNS/mi\_dominio.hosts file  ;  ;  ; INCLUDE UPDATE SOA HEADER  $INCLUDE named.soa ; puede incluirse o escribirse directamente la  ; información aquí.  ;  ; Name Server(s)  ;  *mi\_dominio*. IN NS *esteServidor.mi\_dominio*. ;Pongale un nombre  ; a esteServidor.  ; Ej. dns.mi\_dominio  ;  ; Mail Server(s)  ;  ; *mi\_dominio*. MX 10 *servidor\_correo.mi\_dominio*.  ;  ; Address for localhost  ;  localhost.mi\_dominio. IN A 127.0.0.1  ;  ; Addresses for the canonical names  ;  esteServidor.midominio. IN A dir\_IP\_servidorDNS nom\_real1.*mi\_dominio*. IN A *dir\_IP\_servidorHTTP nom\_real2.mi\_dominio*. IN A *dir\_IP\_servidorXXXXX*  ; no se presenta la forma como se configura IPv6. Debe revisarse qué cambia.;  ; Aliases  ;  alias1.*mi\_dominio*. IN CNAME real1.*mi\_dominio*. alias2.*mi\_dominio*. IN CNAME real2.*mi\_dominio*.  Servidor# vi /etc/DNS/named.soa  puede ser un archivo adicional o estar dentro de la zona | | |
|  | ;  ; /etc/DNS/named.soa file  ;  ; name server SOA file  ; |  |

|  |  |  |
| --- | --- | --- |
|  | @ IN SOA *esteServidor.mi\_dominio. root.mi\_dominio*. ( 2020050101 ; serial  // El número usualmente es un consecutivo. El que el  // administrador desee usar, ej 001, 002, etc. En este  // ejemplo se usó aaaammddxx (aaaa: año, mm: mes,  // dd: día y xx: número consecutivo del día en el que  // se están haciendo las modificaciones).  43200 ; refresh  3600 ; retry  432000 ; expire  86400 ; minimum time-to-live  ) |  |
| Servidor# /usr/sbin/named | | |

* 1. ¿Qué son los registros A y AAAA en el archivo de rootserves?

Un registro A hace coincidencia de un dominio (o subdominio) con una dirección IP. En otras palabras, apunta su nombre de dominio a la dirección IP de su hosting, lo que permite que el tráfico web llegue a dicho servidor. Esta es la función principal del DNS. Un registro A típico luce así:

Registros A: Para direcciones IPv4

Registros AAAA: Para direcciones IPv6

* 1. ¿Qué son los registros NS, MX, A y CNAME en el archivo de dominio particular?

Registro NS:

Los registros de Servidor de nombres (NS, del inglés "Name Server") determinan los servidores que

comunicarán la información del DNS de un dominio. Por lo general, dispones de registros de

servidor de nombres principales y secundarios para tu dominio. Cuando utilizas servicios de Google

Cloud, puedes configurar registros NS que señalen a los servidores de Google cuando se hagan

consultas de DNS.

Registro MX:

específica donde los emails deberían ser entregados.

Registro A:

Específica las direcciones IP correspondientes a tus dominios y sub-dominios.

Registro CNAME:

Específica las redirecciones desde tus sub-dominios de los dominios a otros dominios/subdominios.

* 1. Revise los logs del Sistema para revisar que el servicio está funcionando bien.
  2. Pruebe su funcionamiento en un cliente
     1. Configure un computador cliente para que use el servidor DNS que acaba de configurar.
     2. Use el comando nslookup para revisar su operación
        1. ¿Para qué sirve el comando nslookup?
        2. Pruebe su forma de operación.
        3. Cambie el servidor DNS que lo atiende al servidor DNS de la Escuela y realice las mismas consultas del punto anterior. Documente los resultados.
        4. Use el comando set type=NS. ¿Qué obtuvo? Explique los resultados.
        5. Use el comando set debug. ¿Qué obtuvo? Explique los resultados.
        6. Use el comando set type=A. ¿Qué obtuvo? Explique los resultados.
        7. Use el comando set q=MX. ¿Qué obtuvo? Explique los resultados.
  3. Pruebe su funcionamiento en el servidor DNS
     1. Realice el paso anterior directamente en el servidor DNS, ¿funciona?, ¿por qué? ¿Qué es el resolv.conf?
     2. Solucione el problema y muestre la configuración IP final del servidor
  4. Configure el servicio de resolución de dominios - DNS de tal manera que se active durante el arranque del sistema.
  5. Muestre la configuración a su profesor.

Conclusiones:

* Mediante este laboratorio se aprendió en detalle todo lo que implica el montaje de una

infraestructura computacional.

* Se aprendió a configurar servidores DNS tanto primarios como secundarios.
* Se aprendió el uso de varias plataformas computacionales, tanto en Linux Slackware

como en Windows Server.

* Se aprendió a montar un File Server, una Base de Datos y un Web Server e

interconectarlos en una pequeña red LAN.

Bibliografía:

* https://es.wikipedia.org/wiki/Capa\_de\_aplicaci%C3%B3n
* http://campusvirtual.escuelaing.edu.co/moodle/pluginfile.php/157281/mod\_resource/content/1/06
* -capaAplicacion2019-1.pdf
* http://campusvirtual.escuelaing.edu.co/moodle/pluginfile.php/156480/mod\_resource/content/1/05-capaTransporte\_2019-1.pdf
* http://www.estrellateyarde.org/configurar-la-red-en-linux/configurar-la-resolucion-de-nombres-dedominio-dns-en-linux
* https://disenowebakus.net/llevando-datos-de-la-base-mysql-a-las-paginas-php.php
* http://sufriendoenredes.blogspot.com/2015/10/servidor-dns-secundario-en-windows.html
* solvetic.com/tutoriales/article/3284-instalar-y-configurar-servidor-dns-windows-server-2016/