**Laboratorio 07. RECO-02**

Jefer Alexis González Romero

**Introducción**

En este laboratorio se explorará el protocolo SNMP, que nos permite monitorear los equipos que conforman la red, permitiéndonos saber de forma remota, por ejemplo, su uso de CPU, funcionamiento de la red, software instalado y espacio en disco.

Además, al igual que en el laboratorio anterior, se continuará con la configuración de los routers, tanto en su aspecto físico como por medio de simulaciones en Cisco Packet Tracer, enfocándonos en su enrutamiento para lograr la comunicación entre diferentes redes.

En primer lugar, se explorará el enrutamiento estático, donde se configurarán las rutas manualmente en los routers. Luego, se avanzará hacia el enrutamiento dinámico, donde se configurará el protocolo DHCP, para que nos proporcione automáticamente una dirección IP. También se configurarán tres protocolos de enrutamiento dinámico, que son RIP con VLMS, EIGRP y OSPF, que nos permitirán conocer cómo funcionan y qué métricas usan para calcular la mejor ruta.

Para verificar la comunicación de los distintos enrutamientos, se utilizarán comandos como "traceroute" de ICMP para analizar los paquetes, detectar cualquier problema que pueda surgir en la red, y para revisar las rutas que toman los paquetes para llegar de un computador en una LAN a otro computador en otra LAN. También se utilizarán comandos como "show ip <protocolo> neighbors", "show ip route" y "show ip protocols" para ver las tablas de enrutamiento de los routers.

**Desarrollo del tema**

**Marco teórico**

Para comprender lo que se va a trabajar es necesario tener presentes unos conceptos, en primer lugar, **SNMP (**Simple Network Management Protocol) es un protocolo de capa de aplicación basado en IP que intercambia información entre una solución de administración de red y cualquier dispositivo habilitado para SNMP (Progress "Whast Up" Gold, s.f.).

Una herramienta que nos ayuda a diseñar redes y realizar simulaciones es **Cisco Packet Tracer**, que además nos permiten ver cómo los dispositivos interactúan entre sí (Cisco Networking Academy, s.f.) , dentro de esta herramienta aprenderemos a configurar **routers**, dispositivo de red que se utiliza para conectar diferentes redes y permitir que los dispositivos de una red se comuniquen con los de otra red (Laumaver, 2021).

Para lograr la conexión entre las redes el router debe realizar un **enrutamiento**, proceso de selección de rutas en cualquier red (AWS, n.d.), en este laboratorio se hará uso del **enrutamiento estático**, aquel en el que el administrador de la red debe encargarse de configurar manualmente cada uno de los routers que forman la misma. (Limones, 2021) y del **enrutamiento dinámico**, proceso para determinar la ruta óptima que debe seguir un paquete de datos a través de una red para llegar a un destino específico (English, s.f.).

Además del enrutamiento se debe hacer una **interconexión serial**, técnica utilizada para conectar dispositivos de red a través de líneas seriales, como líneas de teléfono o líneas de módem. La interconexión serial se utiliza para conectarse a dispositivos de red que no tienen una interfaz Ethernet. Y para la asignación de las direcciones de red IP, se empleará **subnetting**, técnica de dividir una red en subredes más pequeñas. Se utiliza para evitar problemas de congestión de red y mejorar la eficiencia del tráfico de red. (KeepCoding, n.d.).

Para ver por donde pasan los paquetes en la red se tendrá en cuenta el protocolo **ICMP** (Protocolo de Control de Mensajes de Internet), protocolo de capa de red utilizado para enviar mensajes de error y control de la red. ICMP se utiliza para informar a los dispositivos de red sobre errores en la entrega de paquetes, como el tiempo de espera agotado o una dirección de destino inalcanzable. (Datatracker, 1981). Este se protocolo se verá a través del comando **traceroute,** herramienta de red utilizada para determinar la ruta que un paquete de datos toma desde una computadora a otra. El comando traceroute envía paquetes de datos a través de la red y registra el tiempo que tardan en llegar a cada dispositivo en la ruta. (Castillo, 2018).

**Uso y aplicaciones**

**Parte 1 – Capa de red y aplicación**

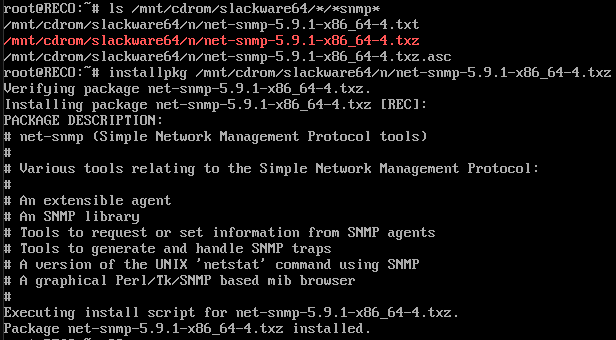
**Instalación de software**

1. **Administración de redes**

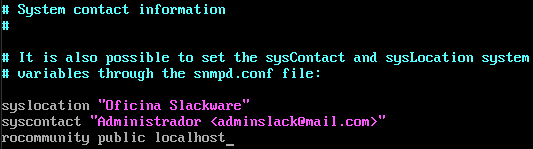
Instalar un servidor para monitorear la red y documentar el trabajo. Deben permitir monitorear todas sus máquinas virtuales, exceptuando Android, y mostrar en tiempo real la gestión de la red.

**Servidor en Slackware**

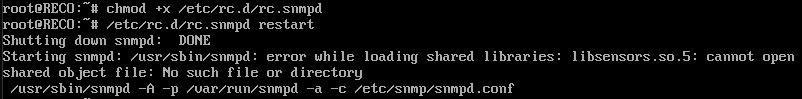
Primero realizaremos la instalación de *net-snmp-5.9.1-x86\_64.txz* que es una implementación del protocolo SNMP.



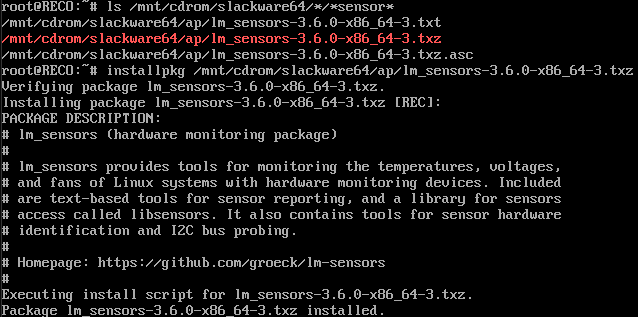
Después entraremos a configurar el archivo */etc/snmp/snmpd.conf* donde agregaremos la descripción de la ubicación física del dispositivo con *syslocation¸* la dirección de correo electrónico para el administrador del sistema con *syscontact* y por último *rocommunity* que es la definición de la comunidad de lectura, que se utiliza como credencia para acceder al agente SNMP y obtener la información.



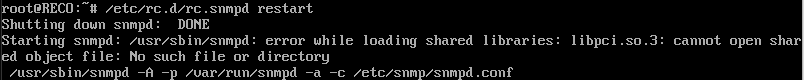
Cambiamos los permisos del archivo */etc/rc.d/rc.snmpd* para poder ejecutarlo con el comando */etc/rc.d/rc.snmpd restart.*

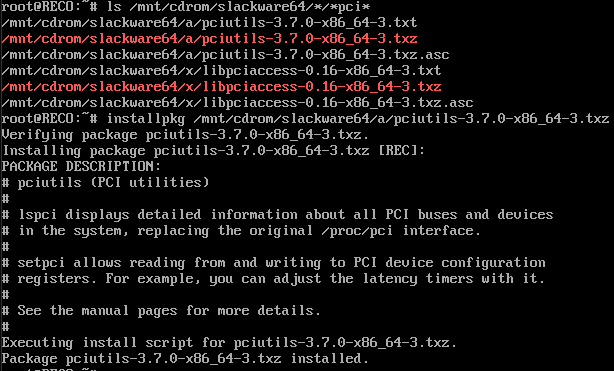


Nos pide que descarguemos el paquete *lm\_sensor-3.6.0-x86\_64-3.txz-*



Volvemos a intentar ejecutarlo y nos vuelve a pedir otro paquete *pciutils-3.7.0-x86-3.txz*





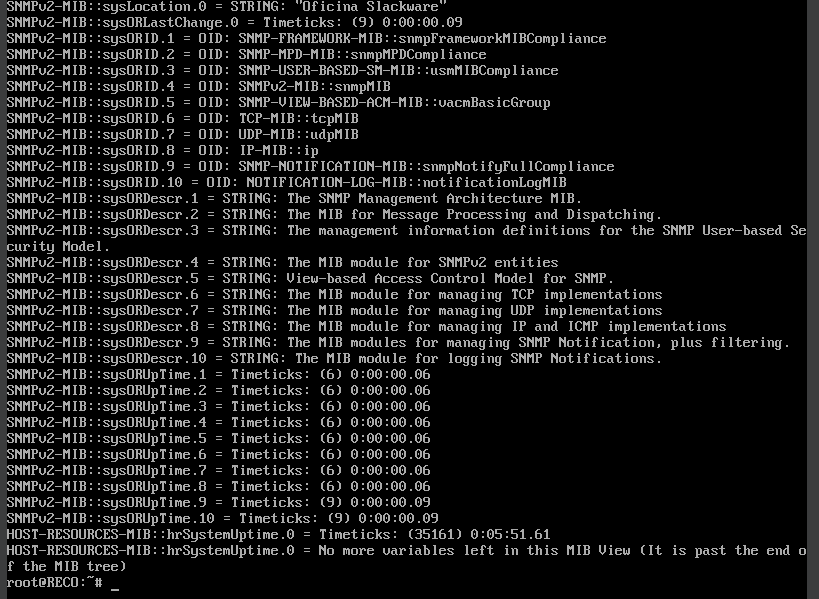
Ahora ya se podría ejecutar el servidor con el comando */etc/rc.d/rc.dnmpd restart.*



Monitoreamos el equipo donde tenemos el servidor con el comando *snmpget -v 2c -c public localhost/10.2.77.41 SNMPv2-MIB::sysUpTime.0,* donde *-v 2c* especifica la versión de SNMP que se va a utilizar, *-c public* la comunidad SNMP, seguido de la ip del equipo que se quiere monitorear y por último una variable de objeto que es opcional algunas son:

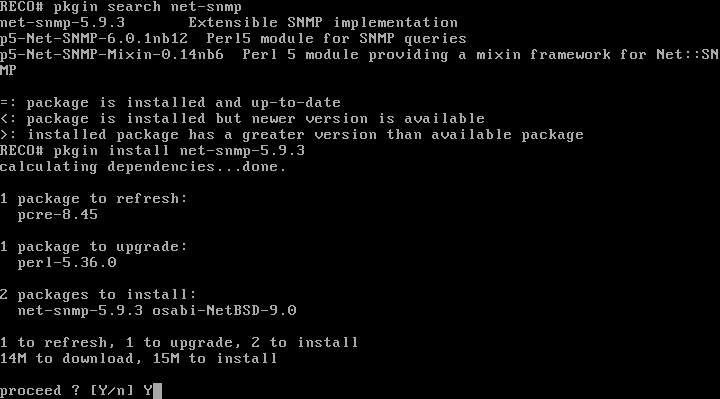
* **SNMPv2-MIB::sysDescr.0:** proporciona información sobre la descripción del sistema.
* **SNMPv2-MIB::sysUpTime.0:** proporciona información sobre el tiempo de actividad del sistema.
* **IF-MIB::ifInErrors:** número de errores que se han producido al recibir paquetes en una interfaz de red.
* **IF-MIB::ifOutErrors**: número de errores que se han producido al enviar paquetes en una interfaz de red.
* **TCP-MIB::tcpCurrEstab.0:** proporciona el número actual de conexiones establecidas en el sistema.

Vemos toda la información del dispositivo sin ninguna variable de objeto.

**

**NetBSD**

Descargamos *net-snmp-5.9.3* con el comando *pkgin install*

**

Texto

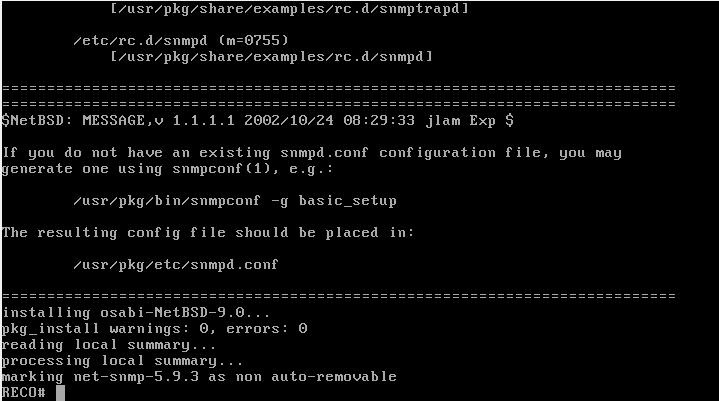
Descripción generada automáticamente

Nos saldrá un error, para poder realizar la descarga debemos forzar la instalación, para esto debemos crear el archivo *pkg\_install.conf* en la ruta */etc* dentro de este debemos escribir *CHECK\_OSABI=no.*

Imagen que contiene Forma

Descripción generada automáticamente

Volvemos a intentar la instalación con el comando *pkgin install net-snmp-5.9.3*



Ahora lo configuramos con el comando *snmpconf -i*

Texto

Descripción generada automáticamente

Seleccionamos que el archivo de configuración *snmpd.conf* con la opción 2.

Texto

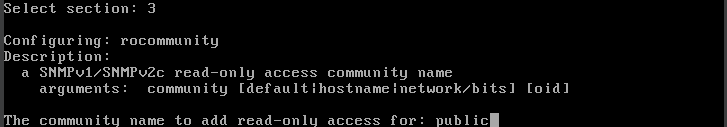
Descripción generada automáticamente

Configuraremos el control de acceso, para esto seleccionamos la opción 1

Texto

Descripción generada automáticamente

Ahora seleccionamos la versión de SNMP y a quién le permitiremos hablar a nuestro agente SNMP, seleccionamos la opción 3 que es la versión SNMPv1/SNMPv2c y permitiremos solo la lectura, después escribimos el nombre de la comunidad a la cual le permitiremos esto, que es public.



Salimos de la sección *Acces Control Setup* escribiendo *finished*

Texto

Descripción generada automáticamente

Ahora configuraremos la información del sistema, para esto seleccionamos la opción 5.

Texto

Descripción generada automáticamente

Comenzamos a configurar por la opción 1, que al igual que en Slackware pondremos la localización del sistema, en este caso pondré “Oficina NetBSD”

Texto

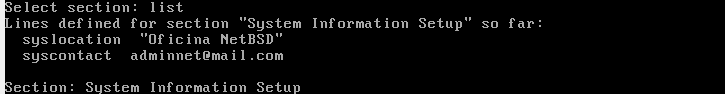
Descripción generada automáticamente

Continuamos con la opción 2 que es la información de contacto del administrador le fcolocaré *adminnet@mail.com*

Texto

Descripción generada automáticamente

Revisamos que haya quedado correctamente la información del sistema con *list*



Volvemos a ingresa *finish* y salimos de la configuración de SNMP con *quit*

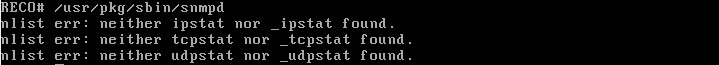
Texto

Descripción generada automáticamente

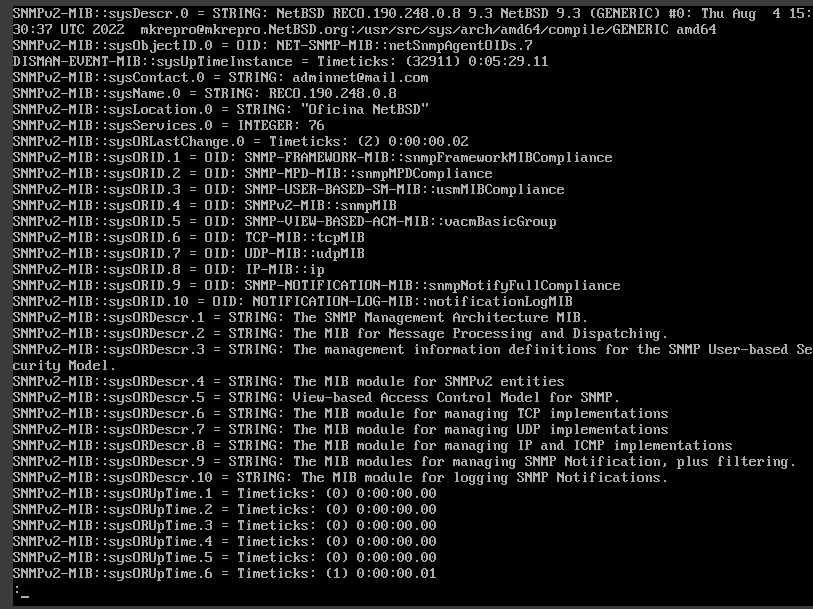
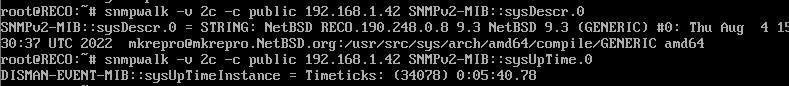
Copiamos el archivo de configuración de SNMP a */etc*



Iniciamos SNMP con el comando */usr/pkg/sbin/snmpd*



Ahora en Slackware corroboramos que se haya configurado correctamente viendo la información de la máquina de NetBSD con el comando *snmpwalk -v 2c -c public 192.168.1.42.*



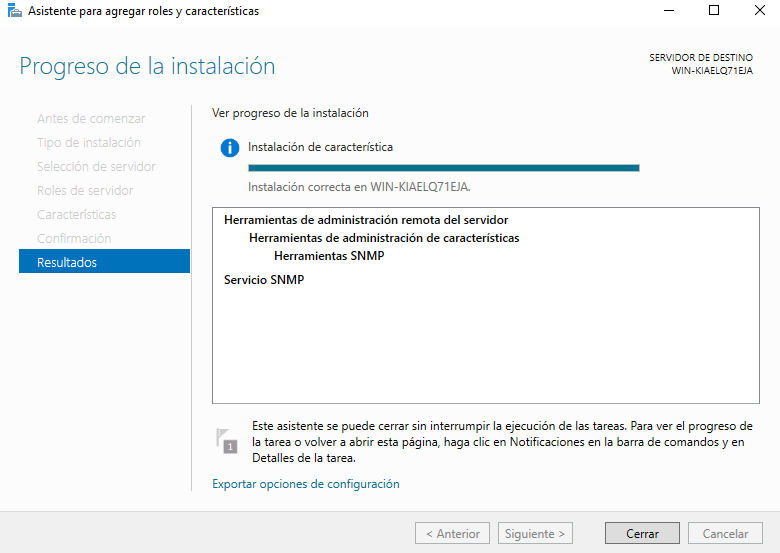
**Windows**

Abrimos el asistente para agregar roles y características y seleccionamos el servicio SNMP-

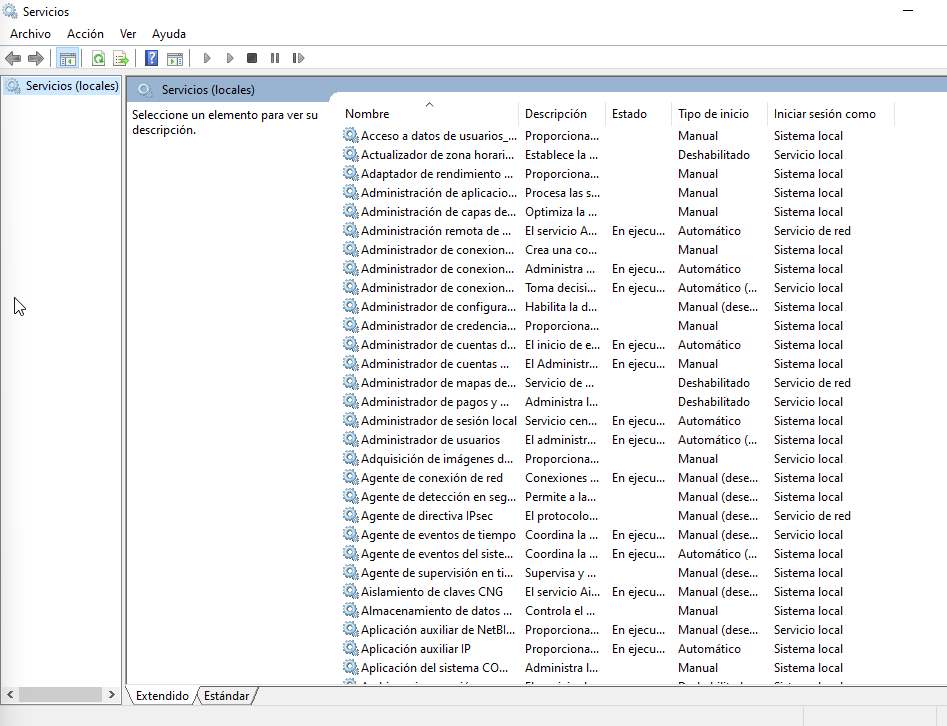
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Damos siguiente, esperamos a que se instale y cerramos el asistente.



Abrimos la herramienta servicios y seleccionamos *servicio SNMP.*



Se abre la pestaña de seguridad y agregamos una nueva comunidad, como se vio en Slackware y NetBSD, la comunidad se llama *public* y solo le daremos permisos de lectura a esta*.*

Interfaz de usuario gráfica, Aplicación

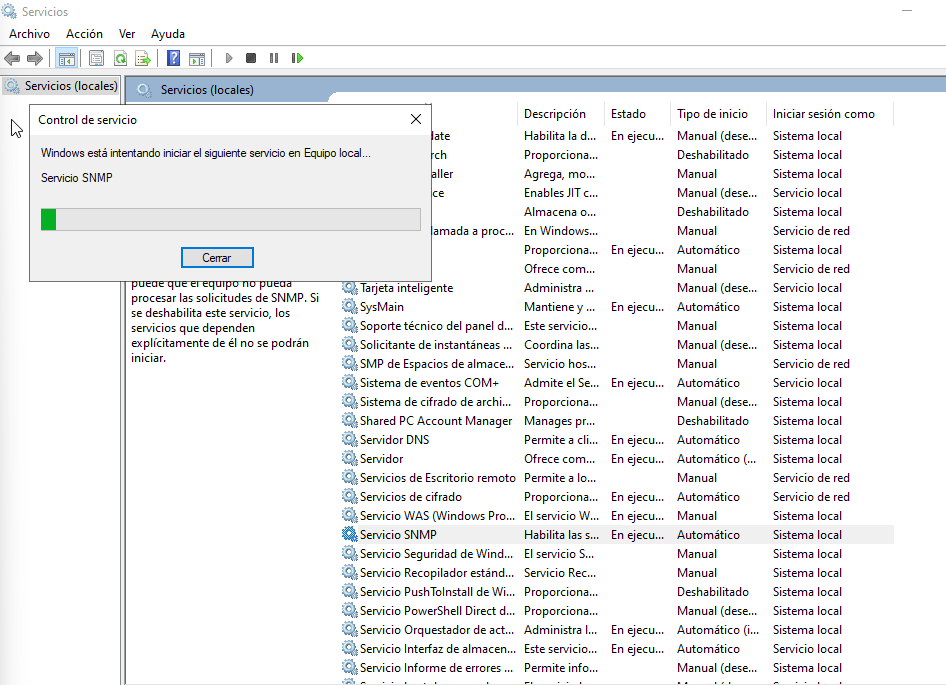
Descripción generada automáticamente

Seleccionamos que queremos recibir paquetes de cualquier host y damos en aceptar.

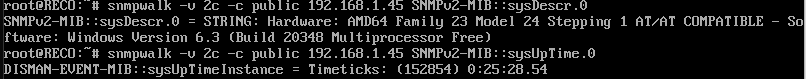
Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Por último, iniciamos el servicio dando click derecho en este y dándole en reiniciar.



Entramos a la máquina de Slackware y al igual que con NetBSD corroboramos que se haya configurado correctamente viendo la información de la máquina de Windows con el comando *snmpwalk -v 2c -c public 192.168.1.45.*

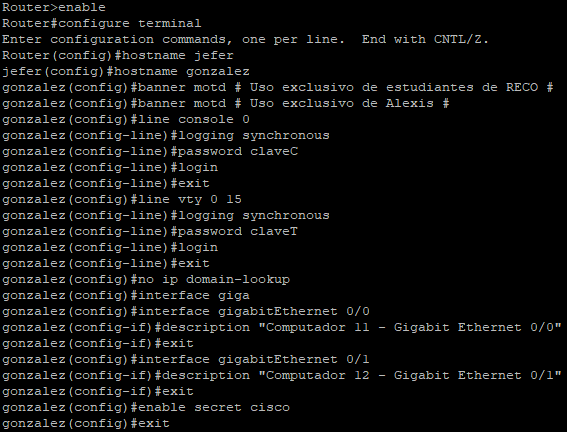
Texto

Descripción generada automáticamente

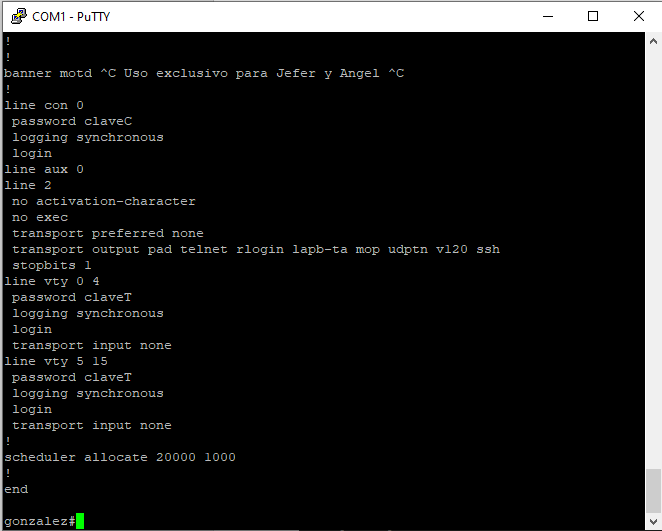
**Experimentos**

1. **Enrutamiento estático**

* Realice la siguiente configuración usando los equipos físicos.



* La configuración básica de un router
* Claves de acceso al modo privilegiado, consola y acceso remoto. la clave de acceso a modo privilegiado debe ser cisco, el de consola, claveC y el de acceso remoto (telnet), claveT.



* Nombre del router. Coloque el apellido de uno de los estudiantes del grupo al router

Texto

Descripción generada automáticamente

* Descripción de las interfaces que usen

Texto

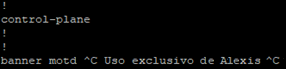
Descripción generada automáticamente

* No consultar servidor remoto de comandos

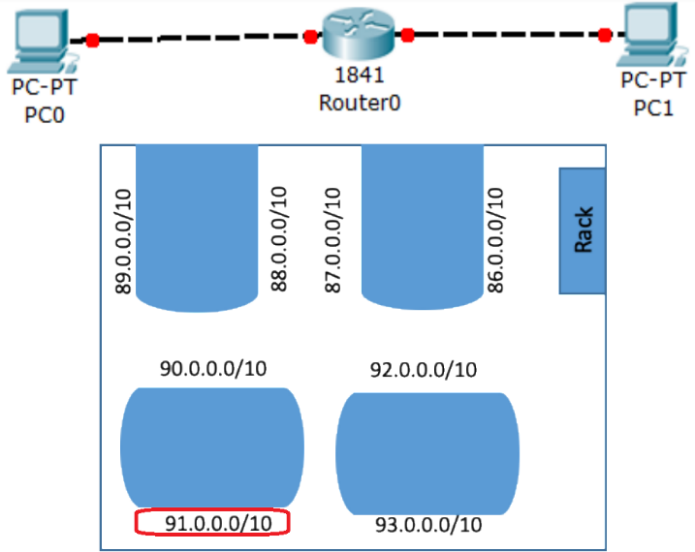
Texto

Descripción generada automáticamente

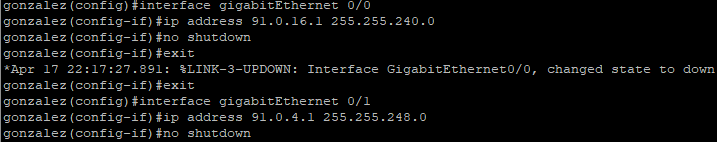
* Mensaje del día



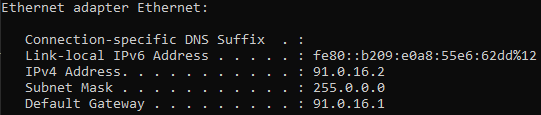
* Para la red de la izquierda use el rango que permita direccionar 2100 host y para la red de la derecha, un rango que permita direccionar 1000 host. Use el rango de direcciones IP según la ubicación del diagrama de las mesas del Laboratorio de Redes.

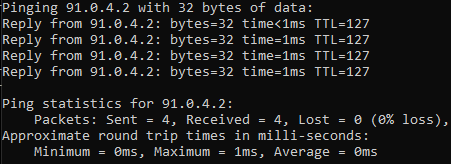


|  |  |  |  |
| --- | --- | --- | --- |
| **Número de hosts** | **Red en binario (Red – Subred - Hosts)** | **Red en decimal** | **Mascara** |
| 4000 | 01011011.00000000.00010000.00000000 | 91.0.16.0 | /20  255.255.240.0 |
| 600 | 01011011.00000000.00000100.00000000 | 91.0.4.0 | /22  255.255.248.0 |



* Pruebe conectividad entre los computadores



Imagen que contiene Tabla

Descripción generada automáticamenteTexto

Descripción generada automáticamente

* Únase con otro grupo de estudiantes e interconecte los router de manera similar a como se presenta en la siguiente imagen. Para la interconexión de los mismos use las tarjetas seriales de los equipos. Para la conexiones seriales acuerde la red con sus compañeros de grupo o siga las instrucciones del profesor. Use una subred de la re 100.0.0.0/24

Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamente

* Configure los routers con rutas estática de tal manera que pueda hacer ping entre todos los equipos de la red



Texto

Descripción generada automáticamenteTexto

Descripción generada automáticamente

* Usando el comando ICMP tracerouter, intente verificar la comunicación de los dos computadores.

Texto

Descripción generada automáticamente

* Ahora, configure las rutas estáticas para ver las redes de sus compañeros del otro grupo.



* Verifique operación con los comandos ping y traceroute

Texto

Descripción generada automáticamente con confianza baja

* Interconecte todas las redes de los grupos del curso y configure los routers de tal manera que puedan verse entre todas las redes Defina los rangos IP para las nuevas conexiones seriales entre todos.

Texto

Descripción generada automáticamente

* Verifique operación con los comandos ping y traceroute

Un conjunto de letras blancas en un fondo blanco

Descripción generada automáticamente con confianza mediaUn conjunto de letras blancas en un fondo blanco

Descripción generada automáticamente con confianza mediaImagen que contiene texto, tabla, computadora, escritorio

Descripción generada automáticamente

Texto

Descripción generada automáticamenteTexto

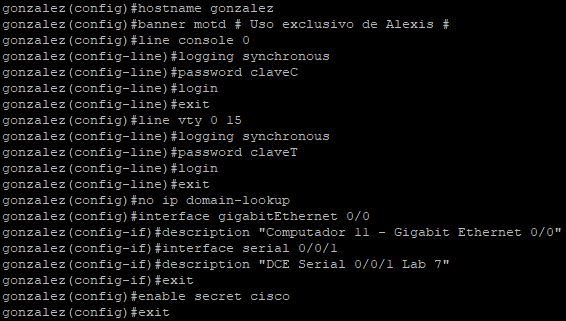
Descripción generada automáticamenteImagen que contiene Texto

Descripción generada automáticamente

**Parte 2 – Capa de red**

**Experimentos**

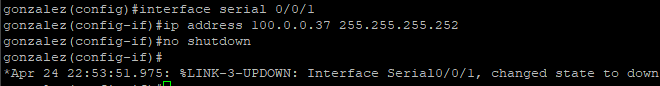
Configuración del router



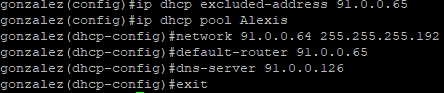
1. **DHCP**

* Calcule el subnetting presentado en la gráfica. Ahora, configure el protocolo DHCP en cada router que atienda redes locales

|  |  |  |  |
| --- | --- | --- | --- |
| **Número de hosts** | **Red en binario (Red – Subred - Hosts)** | **Red en decimal** | **Mascara** |
| 48 | 01011011.00000000.00000000.01000000 | 91.0.0.64 | /26  255.255.255.192 |

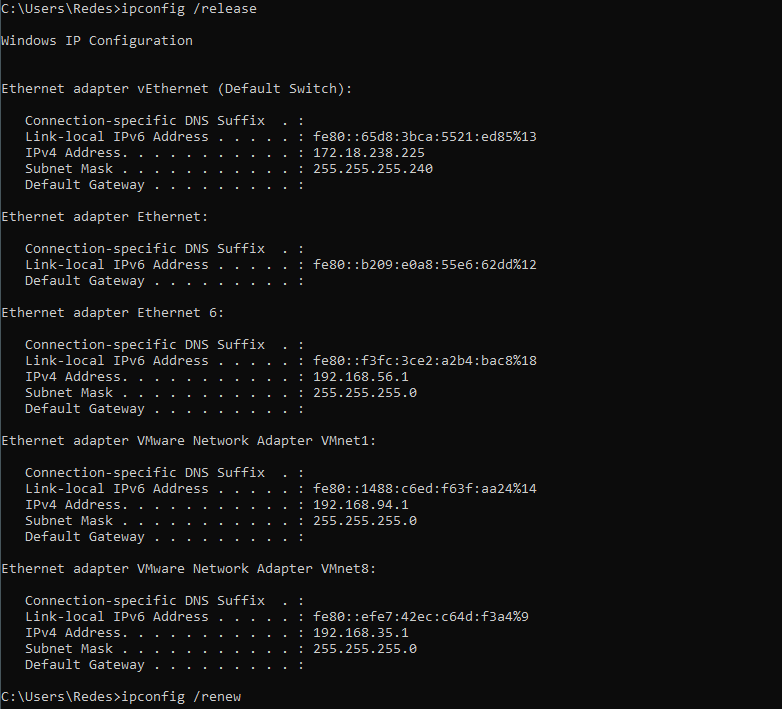




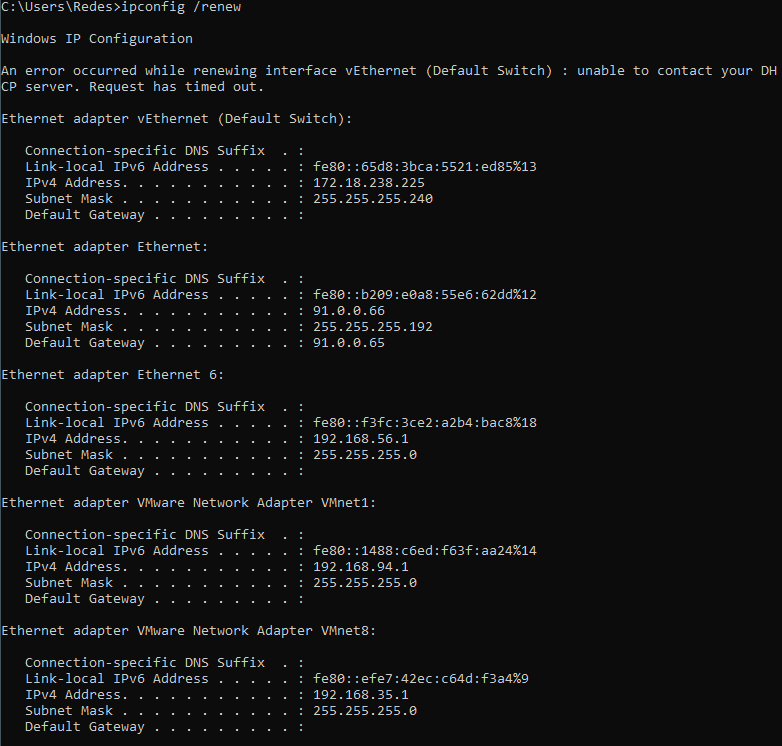


* Ejecute en los clientes los comandos ipconfig /reléase y ipconfig /renew y revise que los equipos reciban dirección IP

Comando ***ipconfig /realase*** para liberar la dirección IP actual

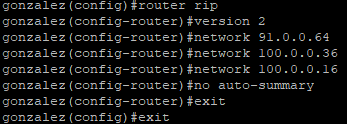


***ipconfig /renew*** para que se asigne una nueva dirección IP, en este caso se asignó *91.0.0.66*

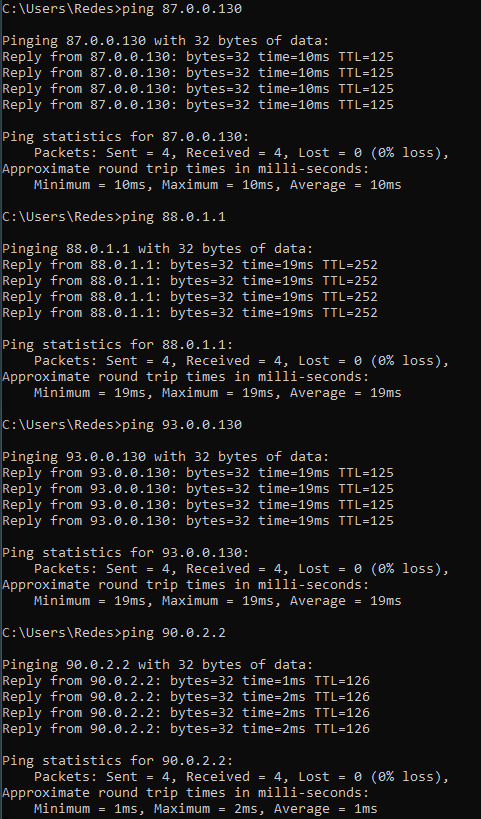
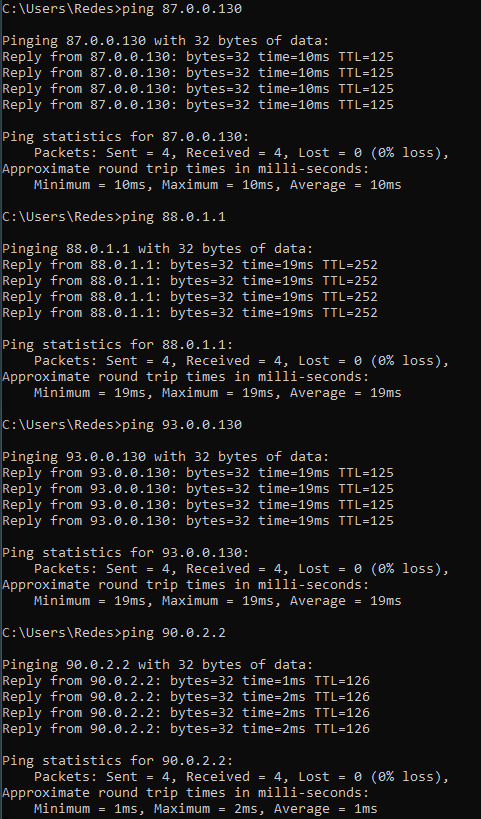


1. **RIP con VLMS**

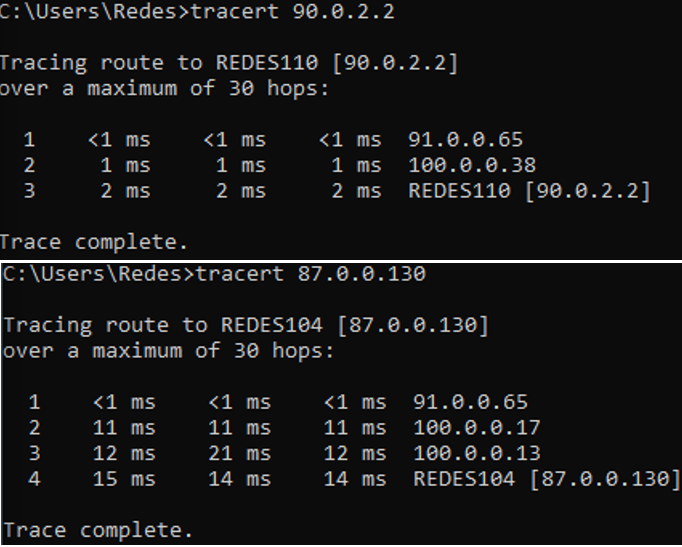
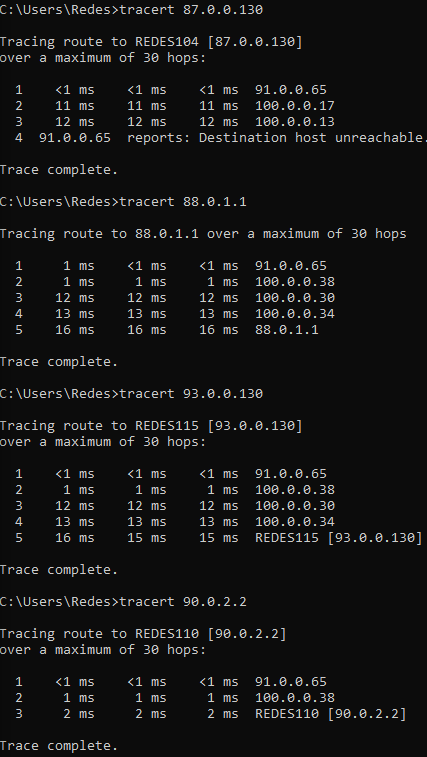
* Configura RIPv2 en los routers.



* ***router rip:*** Se utiliza para habilitar el protocolo RIP en el router.
* ***network ID\_RED:*** Agrega una red al proceso de enrutamiento RIP.
* ***no auto-summary:*** Deshabilita el resumen automático de las rutas, permitiendo ver todas las rutas detalladas. Por defecto, RIP resume automáticamente las rutas que tienen la misma métrica.
* ***exit:*** Sale del modo de configuración de router RIP y del modo de configuración global en el router.
* Revise las tablas de enrutamiento y la conectividad entre los equipos de la red. Conectividad (comando ping)



* Use el comando tracert/traceroute para revisar las rutas para llegar de un computador en una LAN a otro computador en otra LAN

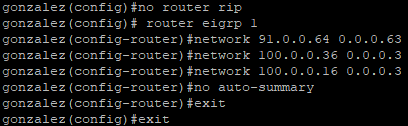


* ¿Qué métrica usa para calcular la mejor ruta?

Usa el número de saltos como métrica para calcular la mejor ruta.

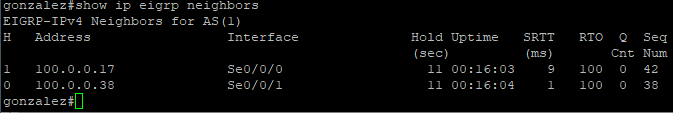
1. **EIGRP**

* Realice la configuración usando el protocolo EIGRP

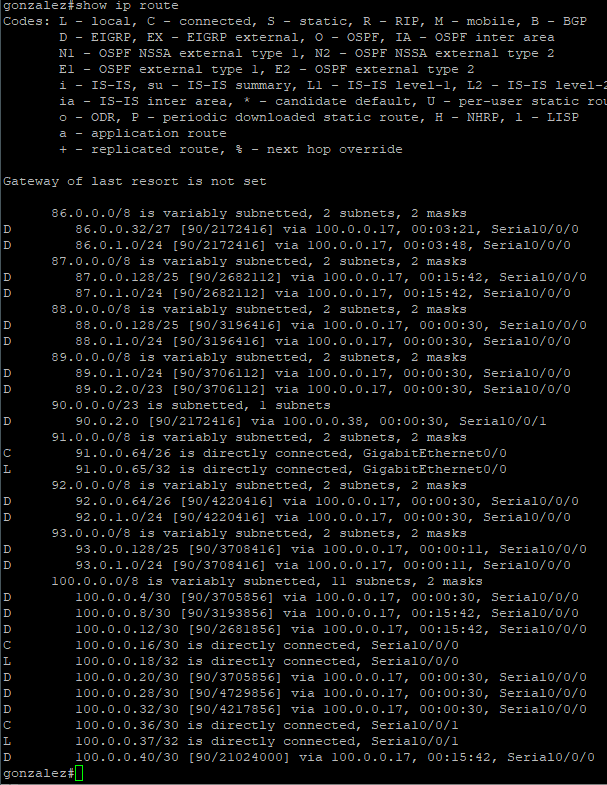


* Revise las tablas de enrutamiento.

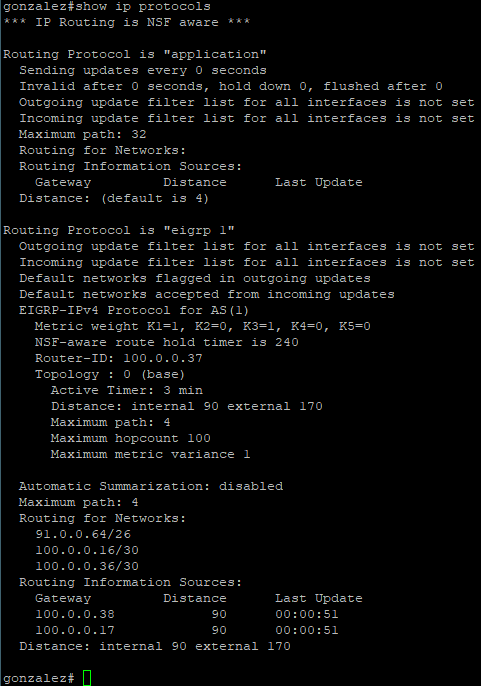
Con el comando ***ip eigrp neighbors*** se pueden ver los vecinos que están conectados al router que son:



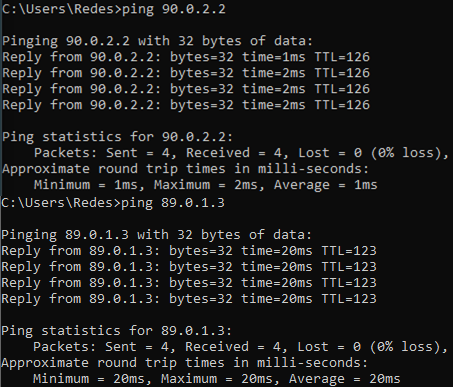
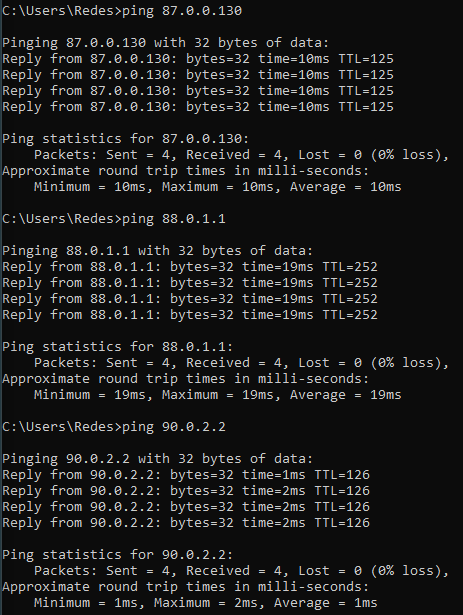
Con ***show*** ***ip route*** se ve la tabla de enrutamiento del router, en esta se muestra todas las redes a las que el router está conectado, junto con la dirección IP, la máscara de subred de cada una y la dirección IP del siguiente salto que se utilizará para llegar a la red.

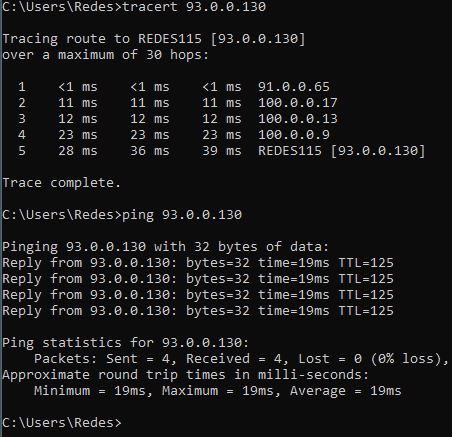


Para verificar el estado y la configuración de los protocolos de enrutamiento del router se usa el comando ***show ip protocols***

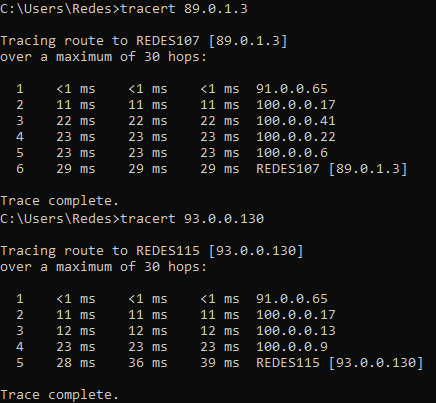
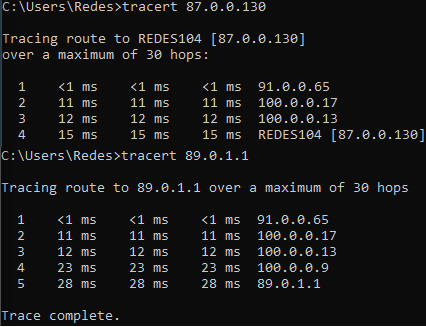
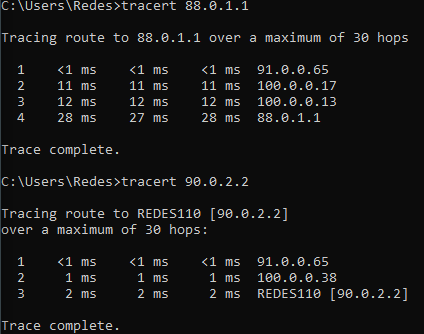


* Compruebe el funcionamiento de la red y la conectividad entre los computadores de la misma.





* Use el comando tracert/traceroute para revisar las rutas para llegar de un computador en una LAN a otro computador en otra LAN

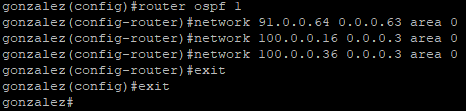


* ¿Qué métrica usa para calcular la mejor ruta?

Su métrica la calcula entre el retraso, ancho de banda, confiabilidad y carga.

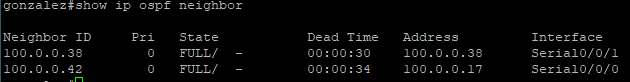
1. **OSPF**

* Realice la configuración necesaria para que todos los equipos de la red del laboratorio de redes se vean entre sí. Utilice el protocolo OSPF para en enrutamiento dinámico.

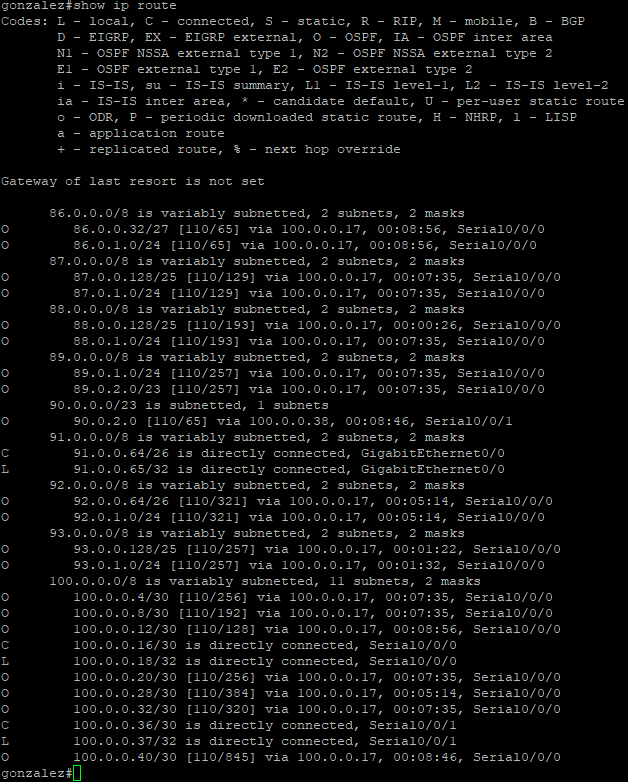


* Revise las tablas de enrutamiento generadas con OSPF

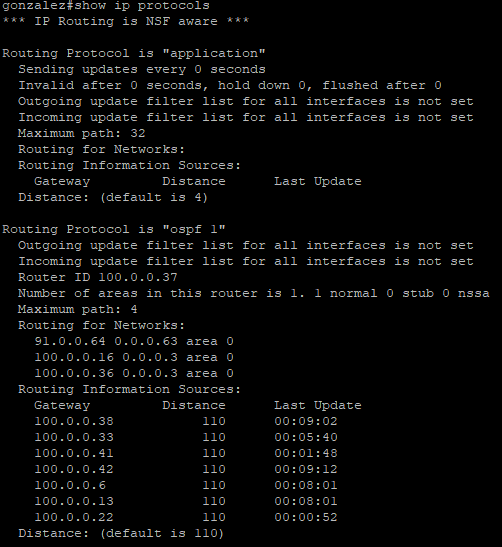
Con el comando ***ip ospf neighbors*** se pueden ver los vecinos que están conectados al router que son:



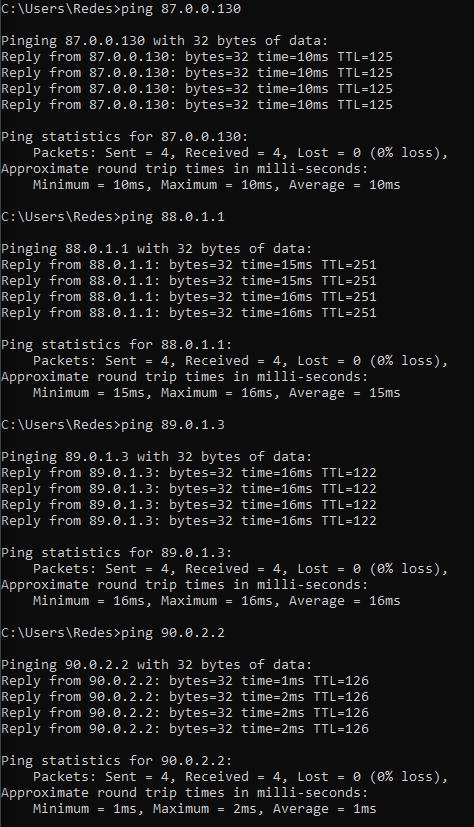
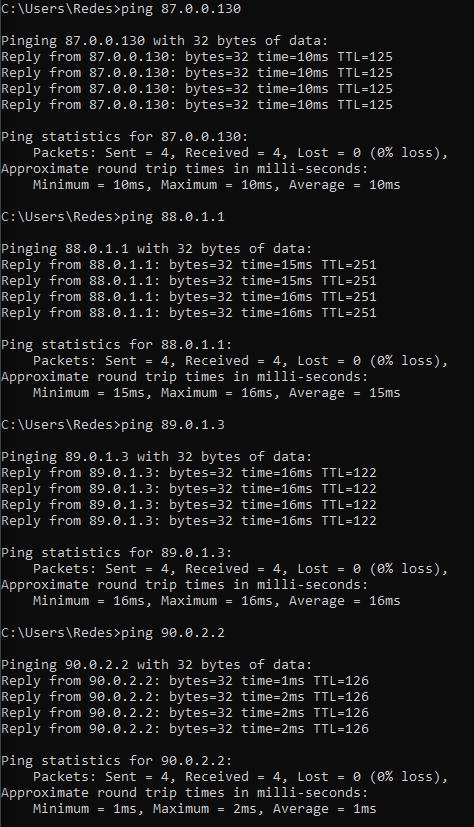
Con ***show*** ***ip route*** se ve la tabla de enrutamiento del router, en esta se muestra todas las redes a las que el router está conectado, junto con la dirección IP, la máscara de subred de cada una y la dirección IP del siguiente salto que se utilizará para llegar a la red.



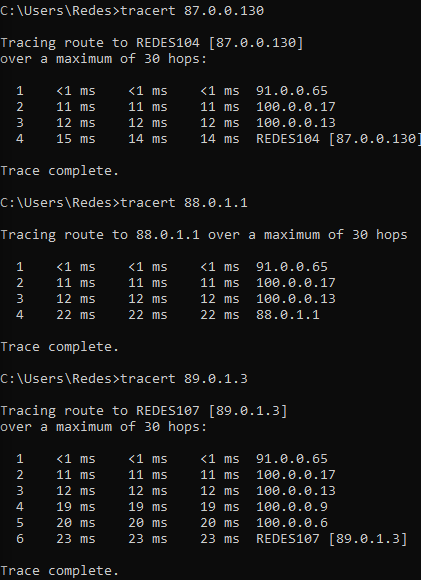
Para verificar el estado y la configuración de los protocolos de enrutamiento del router se usa el comando ***show ip protocols***



* Compruebe el funcionamiento de la red y la conectividad entre los computadores de la misma.



* Use el comando tracert/traceroute para revisar las rutas para llegar de un computador en una LAN a otro computador en otra LAN



* ¿Qué métrica usa para calcular la mejor ruta?

Utiliza una métrica basada en la velocidad de la interfaz de red de un router y se calcula como el inverso de la velocidad de la interfaz en bits por segundo. Es decir, a mayor velocidad de la interfaz, menor será el costo de la ruta y por lo tanto, se preferirá esa ruta. El costo se asigna a cada enlace de la red y se acumula a lo largo de un camino desde el origen hasta el destino. OSPF elige la ruta con el costo total más bajo como la mejor ruta.

**Conclusiones**

En resumen, el laboratorio busca proporcionar una comprensión más profunda de cómo se logra la conectividad en una red y cómo se puede monitorear y mantener su funcionamiento. Esto a través de la exploración del protocolo SNMP para monitorear los equipos de una red, así como en la configuración de routers para lograr la comunicación entre diferentes redes.

De igual forma, se abordó tanto el enrutamiento estático como el dinámico, y se configuran tres protocolos de enrutamiento dinámico, como RIP, EIGRP y OSPF. Además, se utilizaron diversos comandos para analizar los paquetes y detectar problemas en la red, así como para visualizar las tablas de enrutamiento de los routers.

# **Referencias**

*AWS*. (s.f.). Obtenido de https://aws.amazon.com/es/what-is/routing/

Castillo, J. A. (30 de Diciembre de 2018). *Profesional review*. Obtenido de https://www.profesionalreview.com/2018/12/30/tracert-traceroute/

*Datatracker*. (Septiembre de 1981). Obtenido de https://datatracker.ietf.org/doc/html/rfc792

English, J. (s.f.). *ComputerWeekly*. Obtenido de https://www.computerweekly.com/es/definicion/Enrutamiento-adaptativo-enrutamiento-dinamico#:~:text=El%20enrutamiento%20adaptativo%2C%20tambi%C3%A9n%20llamado,llegar%20a%20un%20destino%20espec%C3%ADfico.

*KeepCoding*. (s.f.). Obtenido de https://keepcoding.io/blog/que-es-subnetting/

*Laumaver*. (16 de Julio de 2021). Obtenido de https://laumayer.com/novedades-y-publicaciones/2021-julio/router-beneficios-caracteristicas-recomendaciones-soluciones-adecuadas/

Limones, E. (24 de Septiembre de 2021). *OpenWebinars*. Obtenido de https://openwebinars.net/blog/enrutamiento-estatico-vs-dinamico/#:~:text=El%20enrutamiento%20est%C3%A1tico%20es%20aquel,una%20de%20las%20rutas%20existentes.

*Progress "Whast Up" Gold*. (s.f.). Obtenido de https://www.whatsupgold.com/es/snmp#:~:text=Simple%20Network%20Management%20Protocol%20(SNMP,cualquier%20dispositivo%20habilitado%20para%20SNMP.