Facultad de Ingeniería

Ingeniería en Informática y Sistemas

Redes I

Ing. Dennis Donis

Alexander Gabriel Villatoro Muñoz 1182118

# Hoja de trabajo 1 y Laboratorio 1 – Redes I

Parte I – Estándares, protocolos y RFC’s

1. Describa brevemente el objetivo de los RFC’s 2118 y 1603.

**2118**: el Protocolo punto a punto proporciona un método estándar para transporte de datagramas multiprotocolo a través de enlaces punto a punto. El Protocolo de control de compresión proporciona un método para negociar y utilizar protocolos de compresión sobre PPP enlaces encapsulados.

**1603**: tiene la responsabilidad de desarrollar y revisar especificaciones destinadas a Internet estándares.

1. ¿Cuál es el RFC que discute las guías y procedimientos del grupo de trabajo IRTF?

**RFC 7418**

1. Indique y describa brevemente dos RFCs históricos.

**RFC 792**: Internet Control Message Protocol se utiliza para datagramas de servicio host a host en un sistema de redes interconectadas llamado el Catenet. Los dispositivos de conexión de red se denominan Gateways. Estas pasarelas se comunican entre sí con fines de control a través de un Gateway to Gateway Protocol.

**RFC 768**: User Datagram Protocol este protocolo proporciona un procedimiento para que los programas de aplicación envíen mensajes a otros programas con un mínimo de mecanismo de protocolo. El protocolo está orientado a transacciones, y entrega y protección duplicada, no están garantizados.

1. Investigue tres estándares desarrollados por ITU-T
2. **H.323**: familia de estándares de multimedia y de VoIP
3. **H.264**: algoritmo de compresión de video más utilizado
4. **H.265**: sucesor del popular algoritmo de compresión de video H.264
5. Investigue tres estándares desarrollados por ANSI
6. **IEEE 802.1**: Relación entre partes del documento y el modelo OSI, contiene información de normas de gestión de red e interconexión de redes, establece los estándares de interconexión relacionados con la gestión de redes.
7. **IEEE 802.2**: Conceptualiza el enlace lógico (LLC), es la parte superior de la capa de enlace en las redes de área local.
8. **IEEE 802.3**: Intento de estandarizar Ethernet.
9. Investigue dos estándares para interfaces desarrollados EIA.
10. **TIA/EIA-570-A**: es el estándar de cableado para telecomunicaciones residenciales y comerciales menores. Las especificaciones de infraestructura de cableado dentro de este estándar incluyen soporte para seguridad, audio, televisión, sensores, alarmas e intercomunicadores. El estándar se debe implementar en construcciones nuevas, extensiones y remodelaciones de edificios de uno o de varios inquilinos.
11. **TIA/EIA-607**: es el estándar de Requisitos de Conexión a Tierra y Conexión de Telecomunicaciones para Edificios Comerciales que admite un entorno de varios proveedores y productos, así como las prácticas de conexión a tierra para distintos sistemas que pueden instalarse en las instalaciones del cliente
12. Investigue tres regulaciones para transmisión AM y FM desarrollados por FCC.
13. En un mercado con 45 estaciones de radio o más, una entidad puede ser propietaria de un máximo de ocho estaciones de radio, de las cuales hasta cinco pueden destinarse al mismo servicio (AM o FM).
14. En un mercado con 15 a 29 estaciones de radio, una entidad puede ser propietaria de un máximo de seis estaciones de radio, de las cuales hasta cuatro pueden destinarse al mismo servicio.
15. En un mercado con 30 a 44 estaciones de radio, una entidad puede ser propietaria de un máximo de siete estaciones de radio, de las cuales hasta cuatro pueden destinarse al mismo servicio.

Parte II – Modelos de referencia

1. Nombre las 7 capas del modelo OSI, describa brevemente la función de cada una, liste los protocolos utilizados en cada capa, y el nombre de PDU correspondiente cada capa.

|  |  |  |  |
| --- | --- | --- | --- |
| **Capa del modelo OSI** | **Descripción** | **Protocolos** | **PDU** |
| 1 | **Física =** Se da a conocer las características del hardware de red. | DLS, ISDN, Bluetooth, ADSL, USB. | Bit |
| 2 | **Enlace =** Controla la transferencia de los datos por medio de la red. | Ethernet, FDDI, ARP, PPP. | Trama |
| 3 | **Red =** Manda la dirección de los datos y de igual forma la transferencia entre las redes. | IP, IGP, RIP, IPX/SPX. | Paquete |
| 4 | **Transporte =** Controla la transferencia de los datos y verifica que los datos transmitidos sean idénticos a los que se transfirieron. | UDP, TCP | TPDU |
| 5 | **Sesión =** Establece la conexión entre los sistemas que cooperan. | NetBIOS, ISNS, FTP, SAP. | SPDU |
| 6 | **Presentación =** Garantiza que la información transmitida al sistema receptor sea comprensible y compatible por esté. | AFP, NFS. | PPDU |
| 7 | **Aplicación =** Establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. | HTTP, FTP, SMTP, POP, SSH, SNMP, DNS, IMAP, TFTP. | APDU |

1. Realice un comparativo entre el modelo OSI y el modelo TCP/IP. Indique cuáles capas del modelo OSI están agrupadas en el modelo TCP/IP.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Capa OSI** | **Nombre Capa OSI** | **Nombre TCP/IP** | **Protocolos TCP/IP** | **Protocolos OSI** |
| 1 | Física | Física | Física | DLS, ISDN, Bluetooth, ADSL, USB. |
| 2 | Enlace | Enlace | Enlace | Ethernet, FDDI, ARP, PPP. |
| 3 | Red | Red | Internet | IP, IGP, RIP, IPX/SPX. |
| 4 | Transporte | Transporte | Transporte | UDP, TCP |
| 5 | Sesión | Aplicación | NFS, NIS, DNS, LDAP, telnet, FTP, rlogin, RSH, RIP, RDISC, SNM | NetBIOS, ISNS, FTP, SAP. |
| 6 | Presentación | Aplicación | NFS, NIS, DNS, LDAP, telnet, FTP, rlogin, RSH, RIP, RDISC, SNMP | AFP, NFS. |
| 7 | Aplicación | Aplicación | NFS, NIS, DNS, LDAP, telnet, FTP, rlogin, RSH, RIP, RDISC, SNMP | HTTP, FTP, SMTP, POP, SSH, SNMP, DNS, IMAP, TFTP. |

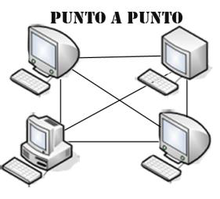
1. Describa que es un PDU y liste el nombre del PDU correspondiente a cada capa del modelo OSI.

El PDU o también conocido como “unidades de datos de protocolo” o de mejor como” protocol data unit (PDU)” es un término de interconexión de sistema abierto (OSI) utilizado en telecomunicaciones que se refiere a un grupo de información agregada o eliminada por una capa del modelo OSI. Cada capa del modelo usa la PDU para comunicarse e intercambiar información, que solo puede ser leída por la capa de pares en el dispositivo receptor y luego se pasa a la siguiente capa superior después de la extracción, en las cuales unas de sus funciones es establecimiento y unión de la conexión como de igual forma control de flujo, errores, etc.

|  |  |  |
| --- | --- | --- |
| **Capa OSI** | **Nombre** | **PDU** |
| 1 | Física | Bit |
| 2 | Enlace | Trama |
| 3 | Red | Paquete |
| 4 | Transporte | TPDU |
| 5 | Sesión | SPDU |
| 6 | Presentación | PPDU |
| 7 | Aplicación | APDU |

1. Conceptualice gráficamente cada una de las topologías lógicas de red existentes (realizar un diagrama por cada topología lógica).

**Point-to-Point** = Esta topología física sirve para llevar los datos del sistema local a un sistema remoto o bien de una red local a una red remota.

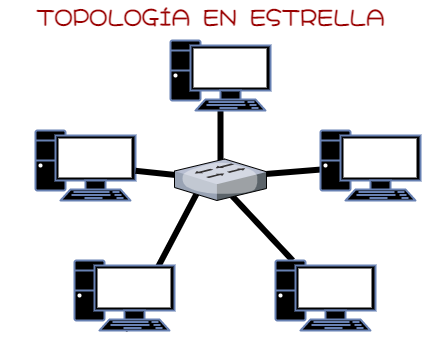


**Bus** = Es la topología en la cual solamente se tiene un único canal de comunicación al cual se conectan los diferentes dispositivos, esta forma cada dispositivo comparte el mismo canal.

A picture containing text, music, piano

Description automatically generated

**Estrella** = Es una red de computadoras en las cuales las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto central.



**Anillo** = Es una conexión que se hace entre nodos formando una única ruta continua, para las señales a través de cada nodo (un anillo), los datos viajan de un nodo a otro, y cada nodo maneja cada paquete.

Diagram

Description automatically generated

**Malla** = Cada nodo está conectados con los demás. Es decir, todos tienen conexiones en todas las direcciones y se encargan de enviar los mensajes por la mejor ruta o la más corta posible. En caso de falla buscan otra más lejana, pero tienen como prioridad principal que el mensaje sea entregado a su destinatario.

Diagram

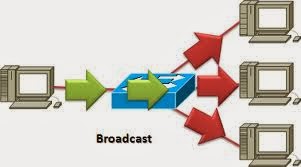
Description automatically generated

**Árbol** = Es la unión de la topología de estrella y la de bus, ya que cuenta con un dispositivo central (switch o hub) al que conectan los nodos, compartiendo en este caso el mismo canal de comunicaciones. La información llega a todos los nodos, pero partiendo de una raíz.

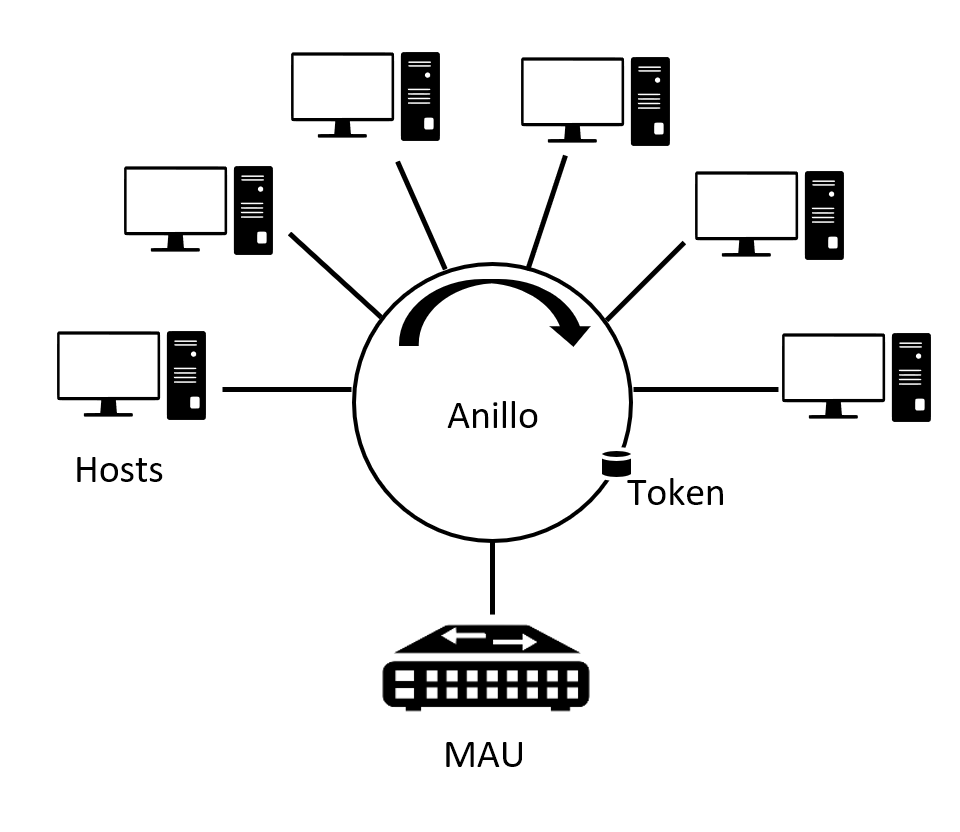
A picture containing text, piano

Description automatically generated

**Broadcast**: simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe un orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada, es como funciona Ethernet.



**Transmisión de Tokens**: Controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red.

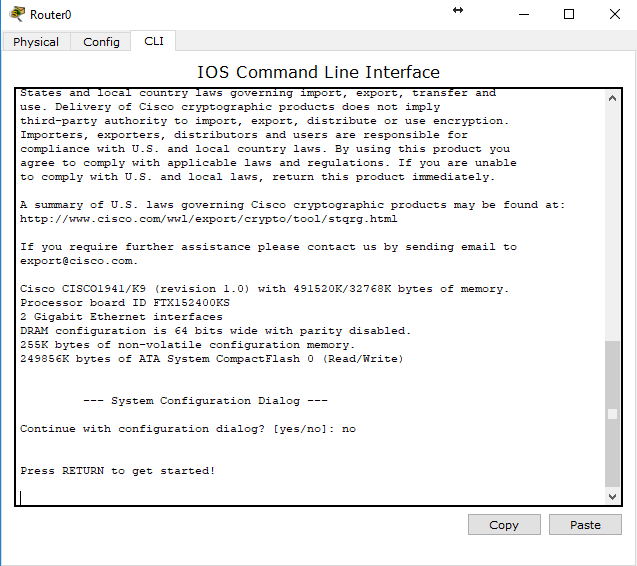


Parte III – Práctica

1. Individual
2. Descargar e instalar en su computadora personal el software de simulación de redes **Cisco Packet Tracer versión 8.0.1** Para descargar el software debe registrarse en el sitio <https://www.netacad.com> y luego bajar el software ubicado en Recursos > Descargar Packet Tracer
3. En Packet Tracer, en un documento nuevo, agregar un Router 1941



1. Dando doble click al router, ingresar a la pestaña CLI. Cuando le pregunte si desea continuar con el “configuration dialog” responder “no”.



1. Desde el modo CLI del router deberá identificar lo siguiente:
   1. Versión del sistema operativo que corre el router (Cisco IOS Software) = **Version 15.1(4)M4**
   2. Tamaño de la memoria no volátil (NVRAM) = **255K bytes**
   3. Cantidad de interfaces Gigabit = **2 Gigabit Ethernet interfaces**
   4. Colocar en este documento printscreen de cada uno de los modos de configuración del sistema operativo Cisco IOS del Router:
      1. Modo User Exec

Graphical user interface, text

Description automatically generated

* + 1. Modo privilegiado (Privileged EXEC)

Text

Description automatically generated

* + 1. Modo de Configuración Global

Text

Description automatically generated

* + 1. Modo Configuración de Interfaz (Usar interfaz gigabitEthernet 0/0)

Text, letter

Description automatically generated

1. Desde CLI realizar lo siguiente:
   1. Colocar de hostname al router en nombre “RouterLab”
   2. Colocar contraseña al Modo Privilegiado del IOS utilizando el comando “enable secret <password>”
   3. Investigar y colocar el comando para colocar contraseña en modo cifrado al Modo Privilegiado del IOS.
   4. Correr el comando “show running-config” y copiar la salida del comando en este documento.

Text

Description automatically generated

Deberá subir al espacio del portal el archivo generado en Packet Tracer, con el nombre “Hoja1\_NombreApellido\_Carnet.pkt”, junto con este reporte en WORD con el mismo nombre.

**Comand line Interface – CLI**

*Comandos básicos línea de comando – MS Windows*

1. ¿Qué hace?
2. ¿Cómo se utiliza?
3. ¿Qué información proporciona?
4. ¿Cómo obtener Ayuda?
5. ¿Cuándo es útil?

**Ipconfig**

1. Muestra los valores de configuración de red de TCP/IP actuales.
2. config [/allcompartments] [/? | /all | /renew [adapter] | /release [adapter] | /renew6 [adapter] | /release6 [adapter] | /flushdns | /displaydns | /registerdns /showclassid adapter | /setclassid adapter [classid] | /showclassid6 adapter |/setclassid6 adapter [classid] ].
3. Los valores de la red TCP/IP actuales.
4. Ipconfig /?
5. Cuando se quiera saber la información y los datos del equipo para el protocolo TCP/IP y permite liberar y renovar la dirección IP de un adaptador de red.

Text

Description automatically generated

**Route**

1. Permite realizar entradas manuales en las tablas de enrutamiento de la red.
2. ROUTE [-f] [-p] [-4|-6] command [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface].
3. Muestra una tabla con las rutas actuales conocidas por IP para el host.
4. Route /?
5. Para visualizar y modificar la tabla de rutas.

Text

Description automatically generated

**Netstat**

1. Muestra estadísticas relativas al protocolo y las conexiones TCP/IP en curso.
2. netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]
3. **Netstat –a** muestra todas las conexiones, y **netstat –r** muestra la tabla de rutas, además de las conexiones que se encuentren activas.
4. Netstat /?
5. Muestra todas las conexiones y puertos, muestra estadísticas Ethernet, muestra los números de puertos y direcciones en formato numérico, y de más.

Text

Description automatically generated

**Ping**

1. Es una herramienta que ayuda a verificar la conectividad del equipo a nivel IP.
2. ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p] [-4] [-6] target\_name.
3. Si la conexión o la transferencia de datos resulta con éxito, nos proporciona un mensaje de éxito y si esta transferencia de datos detecta errores o no se conecta nos proporciona un mensaje que los datos no se transfirieron adecuadamente.
4. Ping /?
5. Es muy útil para diagnosticar problemas de conexión.

Text

Description automatically generated

**Tracert**

1. Es una utilidad que permite visualizar trazas. Utiliza el campo TTL del paquete IP en mensajes de petición de eco y de error (tiempo excedido) ICMP para determinar la ruta desde un host a otro a través de una red, para lo cual muestra una lista de las interfaces de routers por las que pasan dichos mensajes.
2. tracert [-d] [-h maximum\_hops] [-j host-list] [-w timeout] [-R] [-S srcaddr] [-4] [-6] target\_name.
3. Da información acerca de la ruta que toma un paquete que será enviado desde nuestro equipo hasta un host de destino, bien sea en una red local o en Internet a un dominio en concreto.
4. Tracert /?
5. Determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino.

Text

Description automatically generated

**Nslookup**

1. Resuelve problemas con el Servicio de Nombres de Dominio (DNS)
2. nslookup [-opt ...] # interactive mode using default server, nslookup [-opt ...] - server # interactive mode using 'server', nslookup [-opt ...] host # just look up 'host' using default server, nslookup [-opt ...] host server # just look up 'host' using 'server'
3. Proporciona el nombre de host y la dirección IP del servidor DNS.
4. nslookup /?
5. Imprimir la información acerca del host o dominio usando el servidor predeterminado, y establecer valores.

Text

Description automatically generated

**Arp**

1. Muestra y modifica las tablas de traducción de direcciones IP a físicas utilizadas por Protocolo de resolución de direcciones (ARP).
2. ARP -s inet\_addr eth\_addr [if\_addr] ARP -d inet\_addr [if\_addr] ARP -a [inet\_addr] [-N if\_addr] [-v].
3. Muestra, elimina, agrega informacion a las tablas de traducción de IP.
4. Arp /?
5. Resulta útil para visualizar la caché de resolución de direcciones.

Graphical user interface

Description automatically generated

**Whoami**

1. Obtener el nombre del usuario.
2. WHOAMI [/UPN | /FQDN | /LOGONID], WHOAMI {[/USER] [/GROUPS] [/CLAIMS] [/PRIV]} [/FO format] [/NH], WHOAMI /ALL [/FO format] [/NH]
3. Utilizado para imprimir el nombre de usuario efectivo del usuario actual cuando se invoca, es el nombre de usuario en sesión.
4. Whoami /?
5. Esta utilidad se puede utilizar para obtener el nombre de usuario y la información del grupo junto con los identificadores de seguridad respectivos (SID), reclamaciones, privilegios, identificador de inicio de sesión (ID de inicio de sesión) para el usuario actual en el sistema local.

A picture containing text, orange, dark

Description automatically generated

*Comandos Básicos Línea de Comando – Linux*

1. ¿Qué hace?
2. ¿Cómo se utiliza?
3. ¿Qué información proporciona?
4. ¿Cómo obtener Ayuda?
5. ¿Cuándo es útil?

**Ifconfig**

1. Este comando nos permite poner direcciones IP, gestionar interfaces, configurar las interfaces y todo lo relacionado con la propia red.
2. ifconfig [-a] [-v] [-s] <interface> [[<AF>] <address>] [add <address>[/<prefixlen>]][del <address>[/<prefixlen>]] [[-]broadcast [<address>]] [[-]pointopoint <address>]] [netmask <address>] [dstaddr <address>] [tunnel <address>] [outfill <NN>] [keepalive <NN>] [hw <HW> <address>] [mtu <NN>] [[-]trailers] [[-]arp] [[-]allmulti] [multicast] [[-]promisc] [mem\_start <NN>] [io\_addr <NN>] [irq <NN>] [media <type>] [txqueuelen <NN>] [[-]dynamic] [up|down]
3. Todo relacionado a la red
4. Ifconfig -help o -h
5. Para poder gestionar interfaces, poner direcciones IP, configurar interfaces y más.

Text

Description automatically generated

**Route**

1. Nos permite ver la ruta que usa nuestro equipo Linux para conectarse a la red.
2. route [-nNvee] [-FC] [<AF>]route [-v] [-FC] {add|del|flush} ... route {-h|--help} [<AF>] route {-V|--version} -v, --verbose -n, --numeric -e, --extend, -F, --fib, -C, --cache.
3. La tabla de enrutamiento.
4. Route -h o -help
5. Al momento de querer gestionar la tabla de enrutamiento de la conexión. Añadir, borrar rutas y agregar Gateway.

Text

Description automatically generated

**Netstat**

1. Obtiene información básica sobre el estado de la red en aspectos como enrutamiento, estado de la conexión, mascara de red, nombre de interfaz, etc.
2. netstat [-vWeenNcCF] [<Af>] -r, netstat {-V|--version|-h|--help}, netstat [-vWnNcaeol] [<Socket> ...], netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }.
3. Nos muestra el enrutamiento, estado de la conexión, mascara de red, nombre de interfaz, etc.
4. Netstat -h o -help
5. Es útil para poder ver las conexiones activas, desplegar puertos de escucha, añadir una columna desplegando el PID, imprimir información de forma continua, desplegar la tabla de ruteo, ver el puerto en uso por un programa, y más.

Text

Description automatically generated

**Ping**

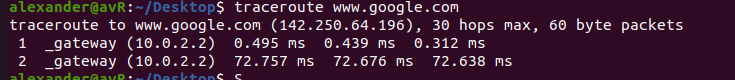
1. Ayudar a determinar si es que hay conexión en la red, sea local o Internet.
2. ping -a, -b, -c, -n, -i, -t
3. Podemos conseguir la información de un IP de destino, numero de paquetes enviados y recibidos, porcentajes de paquetes perdidos, tiempo total de verificación de conexión y más.
4. Ping -h o -help
5. Nos ayuda para poder hacer un ping audible, hacer un ping a una dirección broadcast, definir número de paquetes a enviar, desplegar las direcciones de red como números, definir el intervalo entre transmisiones sucesivas, definir el TTL, etc.

Text

Description automatically generated with medium confidence

**Traceroute**

1. Analizar en detalle y brindar una solución de problemas de red al mostrar el número de saltos necesarios para llegar al host de destino para llegar a destino y para terminar los paquetes enviados.
2. traceroute [ -46dFITnreAUDV] [ -f first\_ttl ] [ -g gate,... ] [ -i device ] [ -m max\_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow\_label ] [ -w MAX,HERE,NEAR ] [ -q nqueries ] [ -s src\_addr ] [ -z sendwait ] [ --fwmark=num ] host [ packetlen ]
3. Demuestra la información de la IP hasta la IP de destino y de esta forma se puede detectar algún tipo de error en su trayecto de conexión.
4. traceroute
5. Se puede hacer para ver si existe algún error en la conexión, se puede forzar el uso de paquetes ICMP y, por último, se puede definir la cantidad de saltos totales, etc.



**Nslookup**

1. Permite que el usuario consulte de forma manual los servidores de nombres para resolver un nombre de host dado.
2. nslookup root, [no]recurse, domain=NOMBRE, retro=#, type=X podemos definir consultas como: A, AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV
3. Ver la información DNS de un sitio en especial. Al ejecutarlo veremos información como la dirección IP, nombre canónico, etc.
4. Nslookup
5. Se puede acceder al root del equipo de destino, enviar una respuesta recursiva a la consulta, definir el nombre de dominio, definir el número de reintentos y definir el tipo de consulta a realizar.



**Dig**

1. Es usado para solucionar problemas asociados al DNS del servidor. Dig analiza la información relacionada con el DNS como registros, CNAME, registro MX y demás.
2. dig [@global-server] [domain] [q-type] [q-class] {q-opt} {global-d-opt} host [@local-server] {local-d-opt} [ host [@local-server] {local-d-opt} [...]].
3. Nos muestra un registro de una direccion IP, y lista de servidores root.
4. Dig -h o -help
5. Se utiliza para obtener un registro inverso de una dirección IP, obtener solo un valor, obtener la lista de servidores root, etc.

Text

Description automatically generated

**Arp**

1. Es un comando que será de gran ayuda para la gestión de las tablas ARP del Kernel.
2. arp [-vn] [<HW>] [-i <if>] [-a] [<hostname>] arp [-v], [-i <if>] -d <host> [pub], arp [-vnD] [<HW>] [-i <if>] -f [<filename>] , arp [-v] [<HW>] [-i <if>] -s <host> <hwaddr> [temp], arp [-v] [<HW>] [-i <if>] -Ds <host> <if> [netmask <nm>] pub.
3. Demuestra las tablas ARP del Kernel.
4. Arp -h o -help
5. Se utiliza para ver el cache ARP actual, desplega la información de forma numérica, define la interfaz a analizar y limpia el cache ARP.

Text

Description automatically generated

**Whoami**

1. Imprima el nombre de usuario asociado con el ID de usuario efectivo actual.
2. Whoami, whoami –help, whoami –version.
3. Da el nombre de usuario efectivo del usuario actual cuando se invoca.
4. Whoami --help
5. Poder saber el nombre de usuario de la sesión actual, saber la versión del comando.

