ENRUTAMIENTO Y CONFIGURACIÓN DE REDES

Ricardo López Bulla

EJE 4

Propongamos

Fuente: Shutterstock/258980774

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

ÍNDICE

INTRODUCCIÓN

Cada día, el ser humano se ve en la necesidad de desarrollar habilidades y de **cualificarse** para estar a la vanguardia en lo concerniente al área donde se desempeña, así como para estar en capacidad de coordinar, dirigir y tomar decisiones con responsabilidad en las organizaciones, sobre todo los administradores de redes informáticas, quienes tienen a su disposición herramientas fundamentales para que una organización funcione de la mejor manera. Ejemplos de estas decisiones son las políticas internas que se manejan en la red informática y la manera en que se accede a la información, ya sea de forma estática o dinámica.

Cualificar

Cualificar es dar a alguien formación especializada para que desempeñe una actividad profesional.

Dentro de estas políticas es fundamental establecer parámetros para garantizar la seguridad de la información dentro de las empresas. En este eje, el administrador de la red obtendrá la capacidad de gestionar políticas de seguridad mediante las listas de control de acceso (ACL).

Listas de control de acceso

Para lograr un funcionamiento eficaz de la red informática, los administradores deben identificar qué tipo de tráfico puede fluir dentro la red y qué tipo se debe restringir. Con los enrutadores, el administrador puede lograr un filtrado básico de la información que facilita la *World Wide Web* (www), que es la red mundial de ordenadores. Esto es posible gracias a las listas de control de acceso (ACL).

Funcionamiento

Como su nombre lo expresa, las ACL son listas que brindan una instrucción precisa de los paquetes que se van a permitir o denegar dentro de las interfaces del enrutador. Estos parámetros tienen unas premisas para operar: fuente y destino del mensaje, tipo de tráfico o protocolo y número de puerto asociado TCP/UDP.

Una vez creada una ACL, se puede vigilar y administrar el tipo de tráfico que circula por las redes. Esto lo implementa el ***router*** mediante los diferentes protocolos, como IP e IPX (intercambio de paquetes entre las redes).

UDP
TCP (transmission control protocol): protocolo de la capa 4 (transporte) del modelo OSI. TCP descrito RFC 793. Protocolo orientado a la conexión: negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico.

Empleabilidad de las ACL

- Permiten realizar una selección en el tráfico que se maneja en las redes informáticas, garantizando un mejor rendimiento de la red.
- Brindan un nivel básico de seguridad a las redes informáticas dentro de las empresas. Esta seguridad se manifiesta en el acceso que se brinda en la red.
- Permiten administrar la clase de información, con el fin de limitar la cantidad de paquetes que se propaga en las redes.

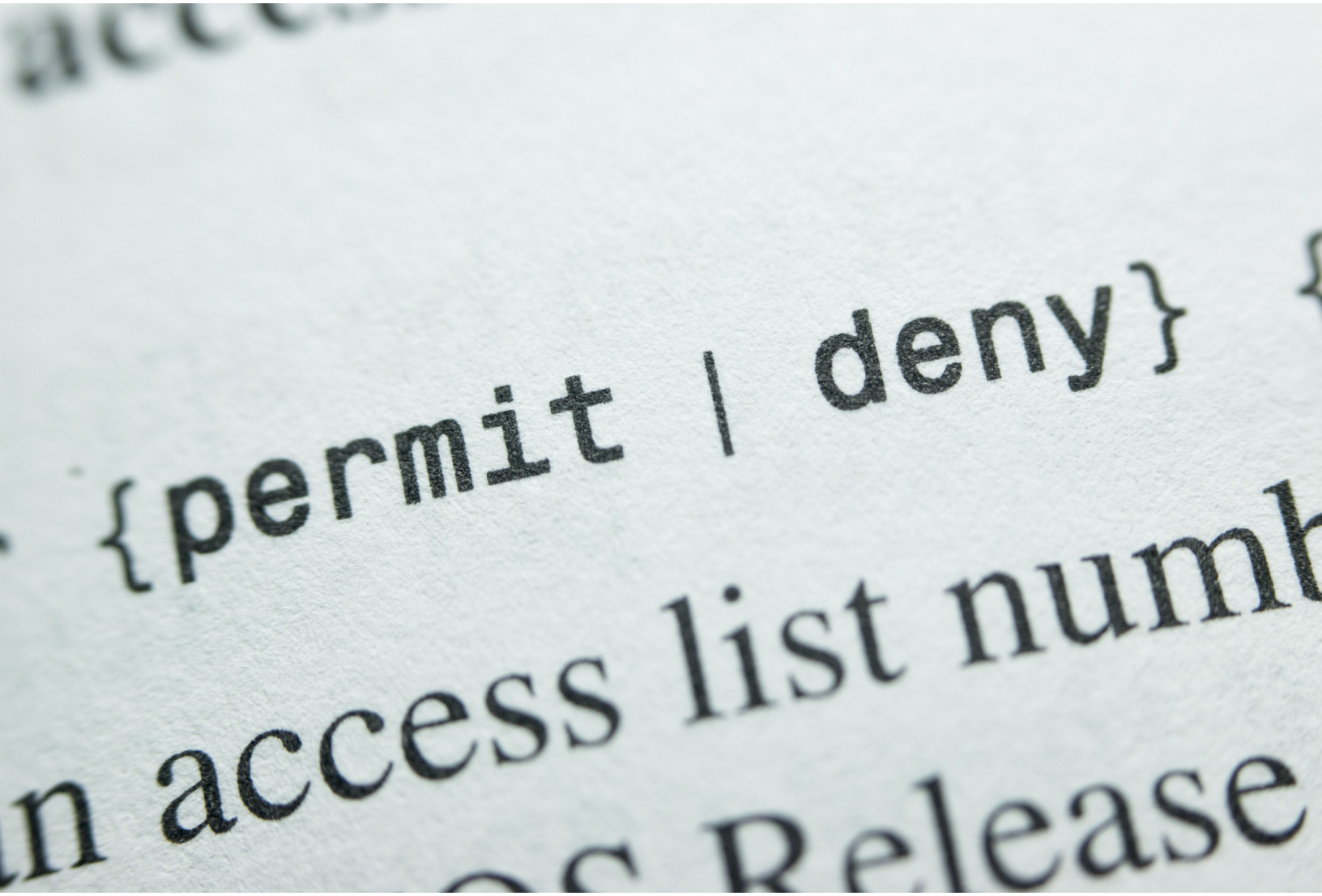

Figura 1. Sentencias ACL
Fuente: shutterstock/353579582

¿Cómo funcionan las ACL?

Las ACL son listas de sentencias de instrucciones: *permit* (permitir) y *deny* (denegar). Estas se definen como entradas de control de acceso (ACE) que concretan los paquetes que pueden entrar y reenviarse mediante las interfaces de los enrutadores. A medida que los paquetes se encaminan a las interfaces de los ***routers***, estos analizan el paquete y miran si se puede enrutar. Una vez analizado este parámetro, los enrutadores detallan si existe una ACL en el paquete. Si hay una respuesta positiva, el paquete es contrastado en la lista de enrutamiento del ***router***. Si este paquete es aceptado, inmediatamente es analizado en la tabla de enrutamiento en donde se establece la interfaz de destino. Luego, los enrutadores analizan si la interfaz de destino posee una ACL. Si no es así, el paquete se reenvía a la interfaz de destino.

Las ACL se configuran de dos maneras, según el tráfico que maneje el diseñador dentro de la red:

- **ACL de entrada:** se caracterizan porque los paquetes que llegan al ***router*** tienen un proceso antes de alcanzar la interfaz de salida del enrutador. Esto ahorra recursos a la red. Si el paquete no coincide en la tabla de enrutamiento, se descarta.

- **ACL de salida:** se caracterizan porque los paquetes que llegan se encaminan a la interfaz de salida, lo cual precisa un análisis a través de la ACL de salida. Se suelen implementar cuando se presenta un único filtro a los paquetes que tienen su origen en múltiples interfaces de entrada, antes de alcanzar la misma interfaz de salida.

Encaminar
Dirigir algo hacia un punto determinado.

Por defecto
Automáticamente. Si no, se elige otra opción.

Tipos de ACL IPv4

Existen dos tipos de ACL IPv4: estándar y extendida. En esta asignatura abordaremos las ACL estándar, las cuales se pueden crear asignando un *nombre* o un *número* para caracterizarlas. Ejemplo: las ACL estándar tienen un rango numérico de 1 a 99 y 1300 a 1999.

Las ACL estándar se caracterizan porque brindan la posibilidad de permitir o denegar el tráfico de las direcciones IPv4 de origen. La manera en que se configura una ACL estándar es la siguiente:

R1(config)# access-list {numero – lista acceso} {deny/permit} {dirección-red} wildcard

A continuación, encontraremos ejemplos de ACE y su interpretación:

a. *R1(config)# access-list 10 deny 192.168.1.1*: no hay máscara *wildcard*. Cuando sucede esto, se asimila que la máscara está por defecto 0.0.0.0. Esta ACE deniega la dirección 192.168.1.1.

b. *R1(config)# access-list 10 permit 192.168.1.0 0.0.0.255:* permite el ***host*** 192.168.1.0 o cualquier *host* dentro de la subred 192.168.1.0.

c. *R1(config)# access-list 10 deny 192.168.1.1 0.0.255.255:* deniega cualquier ***host*** perteneciente a la red 192.168.0.0.

d. *R1(config)# access-list 10 permit 192.168.1.1 0.255.255.255:* permite cualquier ***host*** perteneciente a la red 192.0.0.0.

Un parámetro fundamental dentro de las ACL estándar es habilitar las ACE dentro de las interfaces del enrutador. Para configurar este parámetro partiremos del ejemplo "b". El comando habilita la sentencia como filtro de salida sobre la interfaz. Esta configuración se implementa en la siguiente gráfica.

Filtro
Sistema de selección en un proceso, según criterios previamente establecidos.

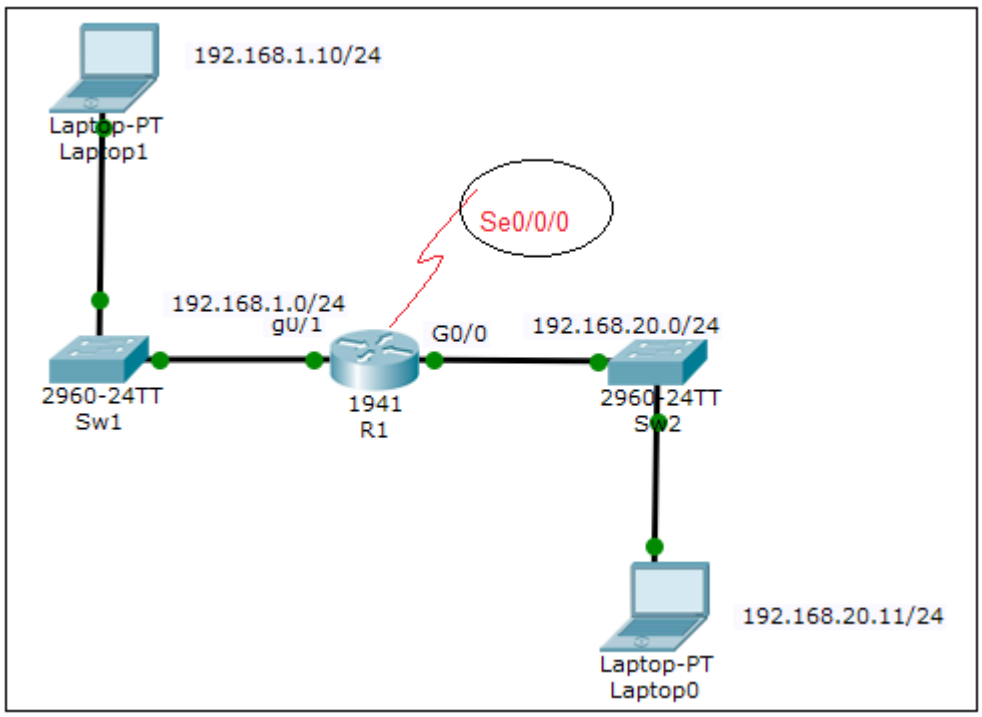

Figura 2.
Fuente: propia

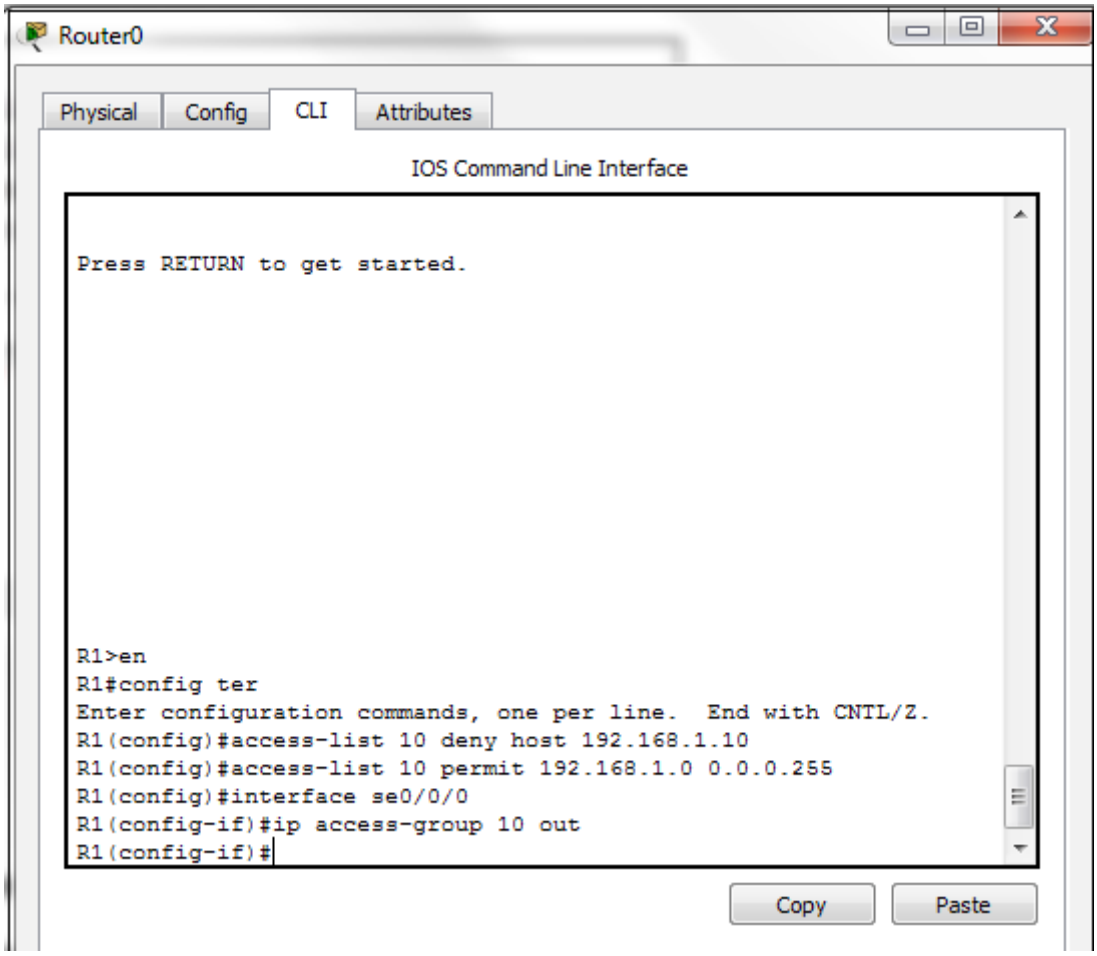

Figura 3.
Fuente: propia

Verificación de las ACL

Mediante el comando *show access-lists* se puede comprobar si las ACL están bien configuradas. En la siguiente figura se aprecian las sentencias ACE.

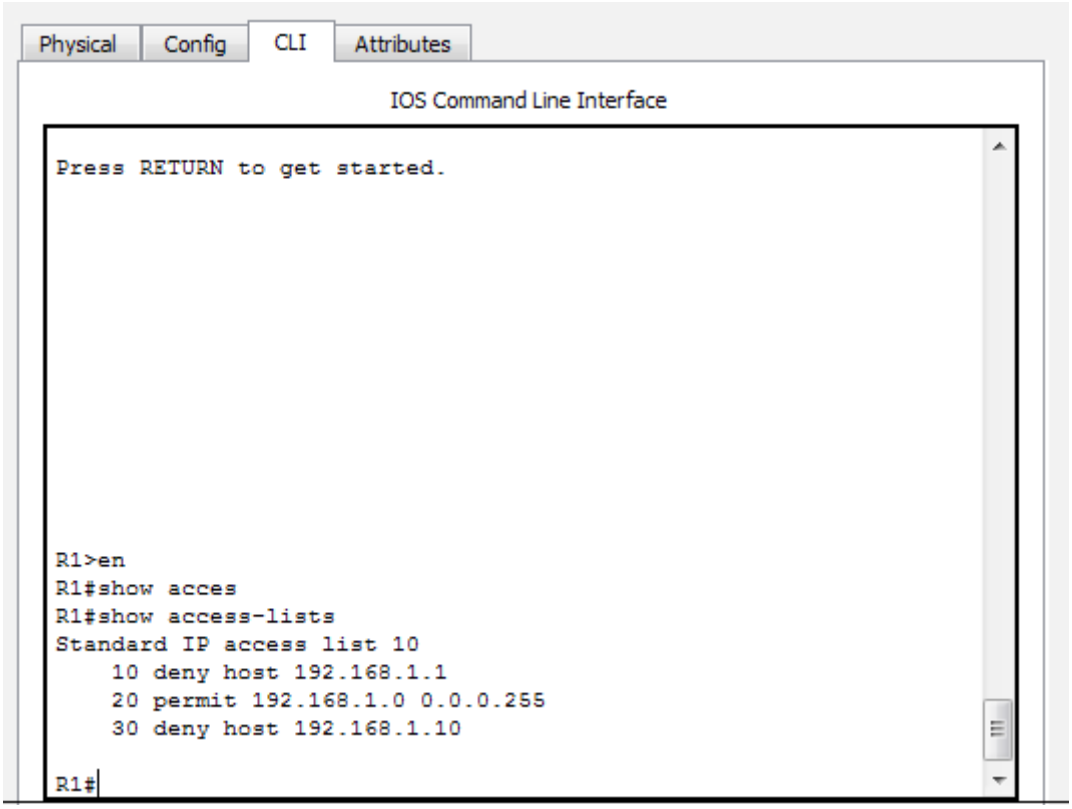

Figura 4.
Fuente: propia

La configuración que se planteó forma parte de las ACL estándar con número. A continuación, se darán a conocer las ACL estándar con nombre, las cuales tienen una particularidad: facilitar su funcionamiento y entendimiento. Al configurar estas ACL los comandos varían. A continuación, se muestra el proceso de configuración.

En el modo configuración global del ***router*** configuramos:

R1(config)# ***ip access-list {standard} name***

Los nombres se caracterizan porque conllevan números y letras. Se asimila la manera en que se escriben, con mayúscula o minúscula. Deben ser únicos y nunca deben comenzar por un número.

Una vez creada la ACL con nombre se procede a crear las sentencias: denegar o permitir el tráfico. Esto se realiza en el modo de configuración de la ACL con nombre de la siguiente manera:

R1(config)# ***ip access-list {standard} name***

R1(config-std-nacl)# ***{permit / deny / remark} network-address {wildcard}***

> **¡Importante!**
>
> El comando remark adiciona un comentario en las entradas de las ACL para entenderlas mejor a la hora de implementarlas.

Por último, se configuran las ACL con nombre a una interfaz. Es importante detallar si los paquetes llegan (*in*) o salen de la interfaz (*out*). Se recomienda escribir los nombres en mayúscula, esto permite reconocer las sentencias. A continuación, se muestra cómo se configura este comando:

R1(config)# ***interface g0/0***

R1*(config-if)# ip Access-group name [in / out]*

- **ACL extendidas:** estas se identifican porque brindan la posibilidad de filtrar el tráfico mediante caracteres como: protocolo que se implementa, dirección IPv4 de origen/destino y puertos TCP o UDP de origen/destino.

- **ACL-IPv6:** son sentencias parecidas a las manejadas con el protocolo IPv4. En IPv6 encontramos un solo tipo de ACL, el cual corresponde a la ACL extendida con nombre en IPv4.

TCP
TCP (transmision control proctocol: protocolo de control de transmisión). Protocolo orientado a conexión, fiable.

UDP
UDP (user datagram protocol: protocolo de datagramas de usuario). Protocolo no orientado a conexión, no fiable, pero más rápido.

Configuración

Como se mencionó, el objeto de estudio de esta asignatura abarcará solo las ACL estándar. Las ACL extendidas son implementadas a través del protocolo IPv6, por este motivo solo mencionaremos los comandos. Esto no será evaluado.

Figura 5. Protocolo de internet versión 6
Fuente: shutterstock/486567814

En el modo de configuración del enrutador se coloca el comando: *ipv6 access-list name*. Después se deniega o permite el tráfico con el objetivo de especificar los paquetes que se descartarán y cuáles se dejarán pasar o reenviar. Esto se implementa con el comando: *{deny / permit} ipv6 network-address ipv6*. Con estos comandos se crea la ACL IPv6.

Network address translation (NAT)

Surge de la necesidad de preservar las direcciones IPv4 públicas (se describe en el RFC 1631). Este objetivo lo alcanza NAT al momento en que las organizaciones adquieren una dirección IPv4 privada y están en la capacidad de traducir las direcciones IP privadas a IP públicas cuando lo consideren necesario. NAT brinda seguridad y privacidad a las organizaciones, debido a que no permite que las direcciones IPv4 sean visibles a las redes del entorno.

Al momento de establecer NAT sobre los enrutadores se pueden tener no solo una dirección IPv4, sino muchas IP (públicas). Este grupo de direcciones se conoce como: conjunto de NAT. Estos enrutadores que operan con NAT se conocen como fronterizos o de borde en una red informática. Se caracterizan por poseer un solo medio para conectarse con la red adyacente. Una vez que el dispositivo al interior de la red informática quiera establecer contacto con un dispositivo en otro dominio de red, lo hace mediante los enrutadores fronterizos con NAT habilitado.

Términos asociados a NAT

Existen términos indispensables para comprender el funcionamiento de NAT. La red al interior se compone del conjunto de redes que están dispuestas a ser traducidas (red interna). La red externa la componen las redes remotas o adyacentes.

Adyacente
Situado en la inmediación o proximidad de algo.

NAT se compone de varios tipos de direcciones: dirección local interna, dirección global interna, dirección local externa y dirección global externa. A continuación, encontraremos una descripción de las direcciones:

- **Dirección interna:** se traduce por medio de NAT en los dispositivos.
- **Dirección externa:** asociada al dispositivo receptor.
- **Dirección local:** segmentos de red a nivel interno de la red.
- **Dirección global:** asociada en el segmento externo de la red.

Al combinar los términos "interna-externa" con "global-local" se pueden determinar direcciones puntuales en las redes informáticas. Por ejemplo, al tener dirección local interna se hace referencia a la dirección IP de origen analizada al interior de la red. Al presentarse la dirección global interna se hace referencia a la dirección IP analizada desde la red remota o adyacente. La dirección local externa hace referencia a la dirección de destino, analizada desde la red remota o adyacente. La dirección global interna hace referencia a la dirección de destino analizada desde la red interna.

NAT realiza sus funciones de dos maneras:

- **Estática:** se distingue porque en su configuración asigna direcciones IP mediante las direcciones globales y locales.
- **Dinámica:** se distingue porque en su configuración se coloca una dirección IP no registrada a otra dirección IP que sí lo está del grupo de direcciones IP que posee un registro.

Configuración

- **NAT estática:** en el modo de configuración global del ***router*** se implementan los siguientes comandos:

R1(config)# ip nat inside source static ip-local ip-global. Con esta configuración se establece una conversión de manera estática entre una dirección IP local interna y una dirección IP global interna.

R1(config)# interface g0/0 **(se designa la interfaz interna)**

R1(config-if)# ip nat inside

Después se designa la interfaz externa del enrutador mediante el comando:

R1(config)# interface g0/1

R1(config)# ip nat outside

- **NAT dinámica (de carácter temporal):** en el modo de configuración global del ***router*** se implementan los siguientes comandos:

  - *R1(config)# ip nat pool name ip-inicial ip-final {mascara-red / longitud-prefijo}:* se define el grupo de direcciones que se va a implementar.

  - *R1(config)# access-list lista_acceso permit wildcard:* se implementa una ACL para tener presente a cuáles ***hosts*** se les va a permitir o denegar el tráfico.

  - *R1(config)# ip nat inside source list lista de acceso pool nombre:* permite establecer la NAT dinámica partiendo de la dirección IP de origen.

  - *R1(config-if)# ip nat inside:* permite establecer la interfaz interna.

  - *R1(config-if)# ip nat outside:* permite establecer la interfaz externa.

Verificación NAT

Para verificar que la configuración de NAT está de la mejor manera se utilizan los siguientes comandos:

- *R1# show ip nat translations:* determina las conversiones activas.
- *R1# show ip nat statistics:* determina las estadísticas de conversión.

Ventajas

- Seguridad a la red.
- Se preservan las direcciones al momento de traducirlas y administrarlas de manera interna por parte de las organizaciones.
- Ahorro en los recursos de la red como, por ejemplo, el tiempo que gastaban las redes en redirigir cada ***host*** y que necesitaban acceder a redes adyacentes.

Figura 6. Servidor DHCP
Fuente: shutterstock/716347543

Protocolo DHCP

Este protocolo de configuración dinámica de ***host*** se encuentra descrito en RFC 2131. Para entrar en contexto, DHCP es un protocolo que permite asignar direcciones dentro de las organizaciones a los terminales que se puedan encontrar dentro de la red (PC, impresora, tabletas, etc.) de manera dinámica, haciendo más fácil la administración de la red. Al implementar un servidor DHCP en dichas organizaciones se permite que la administración de las direcciones IP y su asignación sea por medio de un único servidor. Debido a esta propiedad, el protocolo DHCP brinda eficiencia.

DHCPv4

El protocolo DCHPv4 proporciona direcciones IPv4 e información a la red de manera dinámica, debido a que los usuarios de PC de escritorio abarcan gran cantidad de la red. DHCPv4 es un aliado a la hora de la administración por parte de los encargados de la red, permitiendo un ahorro en los tiempos de gestión. En DHCPv4 se pueden encontrar diversas maneras para realizar el proceso de asignación de direcciones, las cuales permiten flexibilidad en el proceso:

Abarcan
Rodear, contener o comprender algo.

- **Asignación manual:** se da de manera manual por el administrador de la red al usuario designado (cliente).

- **Asignación automática:** DHCP permite asignación automática de información de direccionamiento (dirección IP-máscara de subred-***gateway***). Para la configuración del servidor DHCP es necesario un bloque de direcciones (conjunto de direcciones) para la asignación a los clientes DHCP en una red.

- **Asignación dinámica:** este proceso consta del arrendamiento por parte de DHCPv4 enfocado a una dirección IPv4 de un grupo de direcciones en un tiempo definido por el servidor o cuando el cliente decida prescindir del servicio. Este método es el que tiene mayor grado de aceptación en la actualidad y es el que se manejará en esta asignatura. El encargado de la red tiene a cargo configurar los servidores DHCPv4. Mediante este proceso se establecen los tiempos en los que se va arrendar el servicio. Al vencer el servicio, el cliente solicita una nueva dirección; muchas veces se le asocia la misma dirección IPv4.

DHCP opera de manera cliente-servidor. Al momento de establecer la comunicación entre el cliente con un servidor de DHCPv4, este servidor arrienda la dirección IPv4 al cliente. Paso seguido, el cliente accede a la red por medio de la IPv4 arrendada. Finalizado el tiempo del arriendo, el cliente se pone en comunicación con el servidor para seguir o no con el arriendo. Esto garantiza que las direcciones que ya no están en uso sean entregadas.

Configuración del cliente DHCPv4

Para configurar el cliente DHCPv4 se tienen en cuenta cinco pasos básicos:

1. El primer paso se origina cuando el cliente envía un mensaje de difusión **DHCP-DISCOVER** con su dirección MAC para identificar servidores DHCPv4 disponibles.

2. **Detección de DHCP (DHCPDISCOVER):** cuando el mensaje DHCPDISCOVER llega a los servidores de DHCPv4, el cliente desconoce la dirección IPv4 durante el inicio del proceso. Este utiliza direcciones de difusión a nivel de capa 2 y 3 para relacionarse con el servidor.

3. **Oferta de DHCP (DHCPOFFER):** al momento de recibir el mensaje DHCPDISCOVER por parte del servidor, este guarda una dirección IPv4, la cual estará disponible para arrendar al cliente. Además, el servidor de DHCPv4 envía un mensaje DHCPOFFER al cliente que realiza la solicitud. A diferencia del mensaje DHCPDISCOVER, el mensaje DHCPOFFER se transmite como una unidifusión y, para resaltar, se implementa la dirección MAC de capa 2 del servidor como IP de origen y la dirección MAC de capa 2 asociada al cliente como destino.

4. **Solicitud de DHCP (DHCPREQUEST):** una vez el cliente recibe el mensaje DHCPOFFER del servidor, responde con un mensaje DHCPREQUEST, el cual se implementa en el origen o en la renovación del arriendo.

5. **Acuse de recibo de DHCP (DHCPPACK):** una vez el servidor recibe el mensaje DHCPREQUEST, corrobora la información del arriendo mediante un PING a la dirección designada, con la finalidad de cerciorarse de que no esté en uso. Después de realizado el PING, el servidor habilita una nueva entrada ARP para el arrendamiento del cliente y envía un mensaje DHCPPACK, el cual tiene carácter unidifusión. Al momento de recibir el mensaje DHCPPACK por parte del cliente, este analiza la información de configuración e inmediatamente encamina una búsqueda de ARP hacia la dirección designada. Si no presenta respuesta al ARP, el cliente determina que la dirección es válida y la toma como propia e inicia su implementación.

Configuración de DHCPv4

Paso 1: excluir direcciones IPv4

Mediante el comando ***ip dhcp excluded-address*** se les permite a los enrutadores excluir una o varias direcciones cuando se desea realizar la asignación a los clientes. Este parámetro se puede implementar cuando se quiera guardar direcciones de carácter estático a determinados ***host***s, como la dirección del enrutador. Configuración del comando:

```
R1(config)# ip dhcp excluded-address dirección-ip {dirección-ip-final}
```

Paso 2: configurar un pool DHCPv4

Mediante el comando ***ip dhcp pool {pool-name}*** se asigna un grupo de direcciones al servidor. Configuración del comando:

```
R1(config)# ip dhcp pool {pool-name}
```

Paso 3: configuración de tareas específicas

Es necesario tener configurados el conjunto de direcciones y el *gateway*. Para cumplir con este requisito se implementa el comando *network:*

R1(dhcp-config)# network dirección-ip {máscara /longitud-prefijo}. Se define el rango de direcciones disponibles.

Cuando se implementa el comando *default-router* se establece la puerta de enlace o *gateway del router*. Esta puerta de enlace es la que tiene mayor cercanía con los clientes. Este comando se implementa de la siguiente manera:

R1(dhcp-config)# default-router gateway

Otros comandos que se implementan en DHCPv4 son:

- La dirección IPv4 asociada al servidor DNS que se manifiesta para un cliente DHCPv4. El comando que se utiliza para DNS es:

  R1(dhcp-config)# dns-server dirección-ip

- El comando *domain-name dominio* se implementa para asignar un nombre al dominio. El comando que se utiliza para configurar el dominio es:

  R1(dhcp-config)# domain-name dominio

Verificación del servidor DHCPv4

Para verificar que la configuración del servidor DHCPv4 está de la mejor manera se utilizan los siguientes comandos:

- **R1# show running-config l section dhcp:** permite visualizar los parámetros asociados a DHCPv4.

- **R1# show ip dhcp binding:** permite detallar las relaciones entre la dirección IPv4 y la dirección MAC otorgadas por DHCPv4.

- **R1# show ip dhcp server statistics:** permite visualizar los mensajes de envío/recepción del ***router*** y llevar la contabilidad de los mensajes que se enviaron y se recibieron.

Configuración del cliente DHCPv4

En las organizaciones pequeñas y oficinas domésticas (SOHO) es necesario configurar clientes DHCPv4, esto se asocia de manera inteligente con el ISP. La configuración del cliente se debe implementar sobre la interfaz Ethernet del enrutador, la cual brinda acceso a un módem. El comando que permite esta configuración es:

SOHO
Small office home office: organización pequeña a nivel de hogar e institución con un número corto de empleados.

Router(config)# interface ethernet 0

Router(config-if)# ip address dhcp

Router(config-if)# no shutdown

Router(config-if)# end

Verificación del cliente DHCPv4

Para verificar que la configuración de cliente DHCPv4 está de la mejor manera se utiliza el siguiente comando:

Router# show running-config

DHCPv6

El *Dinamic host configuration protocol for* IPv6 (DHCPv6) es definido en RFC 3315. En él, las direcciones de unidifusión global se pueden configurar manual o dinámicamente. La forma dinámica tiene dos maneras de configuración:

1. **Configuración automática de dirección sin estado (Slaac):** los dispositivos alcanzan una dirección IPv6 de unidifusión global con la ausencia de un servidor DHCPv6. Slaac implementa dos tipos de mensajes: de solicitud y de anuncio de *router* ICMPv6, los cuales brindan direccionamiento a un servidor DHCP.

   - **Mensaje solicitud de router (RS):** este mensaje es transmitido a la dirección IPv6 (multidifusión – FF02::2) de los enrutadores que forman parte de la red.

   - **Mensaje anuncio de router (RA):** tiene como objetivo brindar información a los clientes configurados y aprender sus direcciones IPV6 de una manera automática. Este mensaje es transmitido a la dirección (multidifusión – *FF02::1)* a todos los dispositivos de la red. Cuando se desee transmitir un mensaje RA se debe habilitar el enrutamiento IPv6, lo cual se logra mediante el siguiente comando: ***Router*(config)# ipv6 unicast-routing.**

¡Importante!

Si se desea modificar el mensaje RA que proviene de una interfaz de un enrutador y manifestar qué DHCPv6 sin estado está en uso, se implementa el siguiente comando: Router(config-if)# ipv6 nd other-config-flag.

- **Configuración de un router como servidor DHCPv6 sin estado**

Existen varios pasos para configurar un enrutador como **servidor DHCPv6:**

1. **Habilitar el enrutamiento IPv6:** los parámetros son los siguientes:

   Router(config)# ipv6 unicast-routing.

2. **Configurar pool de DHCPv6:**

   Router(config-dhcpv6)# ipv6 dhcp pool {pool-name}.

3. **Configurar los parámetros del *pool:*** en el mensaje RA hay una información que el servidor de DHCPv6 sin estado no facilita al cliente, de manera que este servidor se puede configurar para que otorgue información, como, por ejemplo: la dirección del servidor DNS y el dominio. Los parámetros que permiten la configuración de DNS y el dominio son:

   Router(config-dhcpv6)# dns-server dns-server-address

   Router(config-dhcpv6)# domain-name {domain-name}

4. **Configurar la interfaz DHCPv6:** los parámetros que permiten la configuración de la interfaz DHCPv6 son:

   Router(config)# interface type number

   Router(config-if)# ipv6 dhcp server {pool-name}

   Router(config-if)# ipv6 nd other-config-flag

- **Configuración de un *router* como cliente DHCPv6 sin estado**

  Existen varios pasos para configurar un enrutador como cliente DHCPv6. El cliente DHCPv6 sin estado puede ser una PC personal, un ***smartphone*** o una tableta. El ***router*** designado como cliente basa su configuración en una dirección IPv6 ***link-local*** para intercambiar información mediante mensajes IPv6 (mensajes RS). A continuación, se enuncian cada uno de estos:

  Router(config)# interface g0/0

  Router(config-if)# ipv6 enable

  Router(config-if)# ipv6 address autoconfig

  Router(config-if)# end

- Verificación DHCPv6 sin estado

  Para verificar que la configuración de DHCPv6 sin estado esté configurada de la mejor manera se utilizan los siguientes comandos:

- **Router# show ipv6 dhcp pool:** visualiza el nombre del ***pool*** de DHCPv6 y sus características.

- **Router# show running-config:** detalla cada uno de los comandos implementados en la configuración.

- **Router# show ipv6 interface g0/0:** visualiza que el enrutador tiene ***stateless address autoconfig enabled*** (configuración automática de dirección sin estado habilitada), así como una IPv6 de unidifusión global.

- **Router# debug ipv6 dhcp detail:** visualiza mensajes DHCPv6 que fueron vinculados con el cliente y el servidor.

2. **Servidor DHCPv6 con estado:** el proceso es similar a la configuración de un servidor DHCPv6 sin estado.

   1. **Habilitar el enrutamiento IPv6:** el comando IPv6 unicast-routing habilita el enrutamiento IPv6, dicho comando no es indispensable a la hora de designar un servidor DHCPv6 con estado, pero es necesario a la hora de enviar mensajes RA.

      Router(config)# ipv6 unicast-routing.

2. **Configurar el pool de DHCPv6:** el parámetro ipv6 dhcp pool {pool-name} origina un ***pool***. A continuación, se detallan los parámetros de configuración de pool de DHCPv6:

   Router(config-dhcpv6)# ipv6 dhcp pool {pool-name}.

3. **Configurar los parámetros del *pool:*** el servidor de DHCPv6 con estado facilita la configuración pertinente de direccionamiento, así como parámetros adicionales. Mediante el comando ***address longitud/prefijo*** se determina el grupo de direcciones que otorgará el servidor. El parámetro ***lifetime*** se refiere al arrendamiento válido dado en segundos. Otro parámetro que maneja el servidor DHCPv6 con estado es el DNS y el dominio.

   Router(config-dhcpv6)# address prefix/length [lifetime valid-lifetime preferred-lifetime l infinite]

   Router(config-dhcpv6)# dns-sever dns-server-address

   Router(config-dhcpv6)# domain-name {domain-name}

4. **Configurar la interfaz DHCPv6: los parámetros que permiten la configuración de la interfaz DHCPv6 son:**

   Router(config)# interface type number

   Router(config-if)# ipv6 dhcp server {pool-name}

   Router(config-if)# ipv6 nd managed-config-flag

- **Configuración de un *router* como cliente DHCPv6 con estado**

  Los parámetros que se implementan en la configuración de un enrutador como cliente DHCPv6 con estado son: habilitar dentro de la interfaz *ipv6 enable,* lo cual permite asimilar una dirección *link-local* para transmitir mensajes RS y el parámetro de configuración de interfaz *ipv6 address dhcp,* que permite al enrutador un funcionamiento como cliente DHCPv6. A continuación, se enuncia el proceso de configuración de un ***router*** como cliente DHCPv6 con estado:

  Router(config)# interface g0/0

  Router(config-if)# ipv6 enable

  Router(config-if)# ipv6 address dhcp

  Router(config-if)# end

- **Verificación DHCPv6 con estado**

  Para verificar que la configuración de DHCPv6 con estado esté configurada de la mejor manera se utilizan los siguientes comandos:

  - ***Router#* show ipv6 dhcp pool:** visualiza el nombre del ***pool*** de DHCPv6 con estado y sus características.

  - ***Router#* show ipv6 dhcp binding:** detalla la relación que se forma entre las direcciones ***link-local*** y la asignada por el servidor.

  - ***Router#* show ipv6 interface g0/0:** visualiza la dirección IPv6 de unidifusión global en el enrutador del cliente.

BIBLIOGRAFÍA

Aznar López, A. (2005). ***La red internet. El modelo TCP/IP***. Madrid, España: Grupo Abantos Formación y Consultoría.

Bellido Quintero, E. (2014). ***Equipos de interconexión y servicios de red (UF1879)***. Málaga, España: IC Editorial.

Boronat Seguí, F. (2013). ***Direccionamiento e interconexión de redes basadas en TCP/IP: IPv4/IPv6, DHCP, NAT, encaminamiento RIP y OSPF***. Valencia, España: Editorial de la Universidad Politécnica de Valencia.

Carceller Cheza, R. (2013). ***Servicios en red***. Madrid, España: Macmillan Iberia S. A.

Castaño Ribes, R. J. (2013). ***Redes locales***. Madrid, España: Macmillan Iberia S. A.

Hallberg, B. (2007). ***Fundamentos de redes***. Madrid, España: McGraw-Hill Interamericana.

Hillar, G. C. (2004). ***Redes: diseño, actualización y reparación.*** Buenos Aires, Argentina: Editorial Hispano Americana S. A.

Íñigo Griera, J. (2008). ***Estructura de redes de computadores***. Barcelona, España: Editorial UOC.

Jiménez Camacho, R. (2014). ***Análisis del mercado de productos de comunicaciones (UF1869)***. Málaga, España: IC Editorial.

Martínez Yelmo, I. (2015). ***IPv6-Lab: entorno de laboratorio para la adquisición de competencias relacionadas con IPv6.*** Madrid, España: Universidad de Alcalá.

Molina Robles, F. J. (2014). ***Servicios de red e internet***. Madrid, España: RA-MA Editorial.

Moreno Pérez, J. C. (2014). ***Sistemas informáticos y redes locales***. Madrid, España: RA-MA.

Santos González, M. (2014). ***Diseño de redes telemáticas.*** Madrid, España: RA-MA Editorial.

Velte, T. J. (2008). ***Manual de Cisco®***. Madrid, España: McGraw-Hill Interamericana.