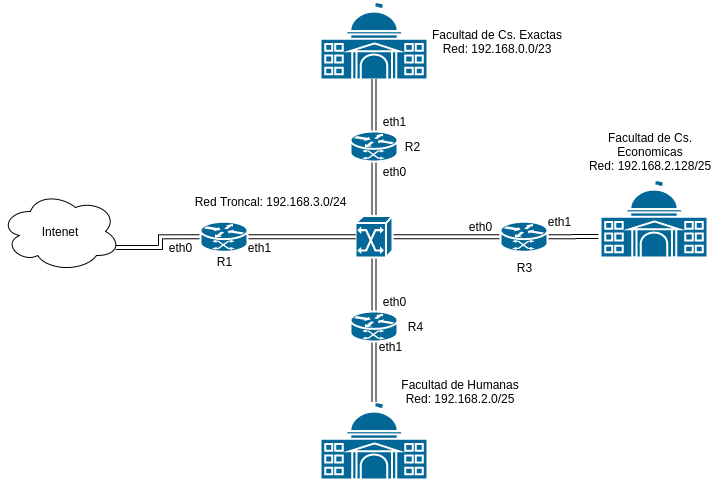
|  |  |  |
| --- | --- | --- |
| Nota: 6 | | |
| Ej 1 | Ej 2 | Ej 3 |
| 65% | 40% | 80% |

Examen Final CDAR

17/02/2021

# Netfilter/Iptables

Suponga ser el administrador de todos los router de la siguiente topología:



* 1. Intérprete, explique e indique para qué sirve y reconozca si hay algún inconveniente en la siguientes reglas de netfilter en el router R1:
* iptables -t filter -A FORWARD -s 192.168.0.0/24 -j ACCEPT

**Indica que todo lo que atraviesa el router 1 y proviene del de la facultad de ciencias exactas con direccion desde 192.168.0.1 a la dirección 192.168.0.255 ( esto es porque es /24 y la subred de exactas es /23) debe ser aceptado**

* iptables -t filter -A FORWARD -s 192.168.2.0/25 -j REJECT

**Indica que todo lo proveniente de Facultad de Humanas debe ser rechazado, además va a mandar un mensaje de que se rechazó**

* iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to 192.168.0.100:8443

**Indica que todo lo que venga de afuera(desde Internet) que tenga protocolo TCP y destino el puerto 443 lo envíe a la direccion 192.168.0.100 de la facultad de exactas y al puerto 8443**

* iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

**Esta mal esta regla ya que quiere enmascarar del lado de Internet del lado público, debería ser -o eth1 para que enmascare todo el tráfico de las sub-redes**

* iptables -t filter -A INPUT -s 192.168.2.0/25 -i eth0 -j REJECT

**También está mal ya que nunca se podrá ingresar al router 1 desde la dirección**

**192.168.2.0/25 desde la interfaz eth0. Debería decir eth1 y asi rechazaría todo lo proveniente de la facultad de humanas**

* 1. ¿Qué regla agregaría o modificaría en el router R1, si desea que ninguna facultad pueda conectarse al router R1? (Debe colocar la o las reglas nuevas o modificadas)

**Pondría al principio de todo como primera regla:**

**iptables -t filter -A INPUT -i eth1 -j REJECT**

**Así rechazo todo lo que quiera entrar por eth1**

* 1. ¿Cómo haría para que la Facultad de Humanas y la Facultad de Cs Económicas puedan tener internet, teniendo en cuenta que esta funciona en los puertos 443 y 80 de tcp? (Debe colocar la o las reglas nuevas o modificadas)

**iptables -t NAT -A POSTROUTING -o eth0 MASQUERADE**

**iptables -t filter -A FORWARD -s 192.168.2.128/25 -p TCP -j ACCEPT**

**iptables -t filter -A FORWARD -s 192.168.2.0/25 -p TCP -j ACCEPT**

**iptable -t filter -A FORWARD -j REJECT**

* 1. ¿Cómo haría para que las facultades no se puedan ver entre ellas, teniendo en cuenta netfilter/iptables?

Haría las correspondientes configuraciones en los routers 2, 3 y 4 para que se rechacen los ingresos de las otras subredes

En router 2

iptables-t-filter -A INPUT -i eth0 -s 192.168.2.0/25 -j REJECT ( aca exactas rechaza a humanas)

iptables-t-filter -A INPUT -i eth0 -s 192.168.2.128/25 -j REJECT ( aca exactas rechaza a económicas)

En router 3

iptables-t-filter -A INPUT -i eth0 -s 192.168.0.0/23 -j REJECT ( aca económicas rechaza a exactas)

iptables-t-filter -A INPUT -i eth0 -s 192.168.2.0/25 -j REJECT ( aca económicas rechaza a humanas)

En router 4

iptables-t-filter -A INPUT -i eth0 -s 192.168.0.0/23 -j REJECT ( aca humanas rechaza a exactas)

iptables-t-filter -A INPUT -i eth0 -s 192.168.2.128/25 -j REJECT ( aca humanas rechaza a económicas)

# Direcciones IP

1. Explique con sus palabras en forma clara y concreta, cuál fue el principal problema que tuvo que enfrentar IPv4 y cómo fue solucionado hasta la aparición de IPv6. ¿Por qué cree que aún se sigue utilizando IPv4 en su mayoría?

**Las direcciones IP identifican un punto de acceso ( interfaz ).Cuando se lanzó IPv4 el problema que tenía es que no es eficiente en la distribución de direcciones ya que si tengo por ejm 300 host una red clase C no me alcanza ya que tiene capacidad para 254 y una red clase B me sobran demasiadas direcciones ya que me da 26534 direcciones para los host.Las máscaras eran /24 /16 o /8 .Entonces surgió el VLSM ( Variable Lenght Subnet Mask “Máscara de red de longitud variable” )la máscara puede ir cambiando y es /( barra ) lo que se necesite, de esta forma tengo una máscara de acuerdo al tamaño de red que tengo.**

**IPv4 utiliza una dirección de IP de 32 bits, las IPv6 utilizan IP de 128 bits, en los países desarrollados están utilizando IPv6 y IPv4 ,las 2, a futuro la idea es utilizar IPv6 ya que son muchas mas direcciones IP.Todavía se sigue utilizando IPv4 porque no está adecuada aún la red para usar IPv6 , se va haciendo de forma gradual ya que hay aplicaciones viejas que corren sobre IPv4 y no funcionarían con IPv6.**

1. Explique con sus palabras en forma clara y concreta, cómo funciona el algoritmo de Traceroute y para qué sirve.

**Es un programa que se puede ejecutar en cualquier host de internet. Cuando ponemos un host de destino, el host origen envía unos paquetes al host de destino, éstos paquetes para llegar atraviesan una serie de routers. Cuando un router recibe uno de estos paquetes envía un mensaje al host origen con el nombre y la dirección del router, el paquete atraviesa todos los routers necesarios para llegar a destino y cada router envia el mensaje, una vez que llego el host destino el host destino tambien envia un mensaje al origen.**

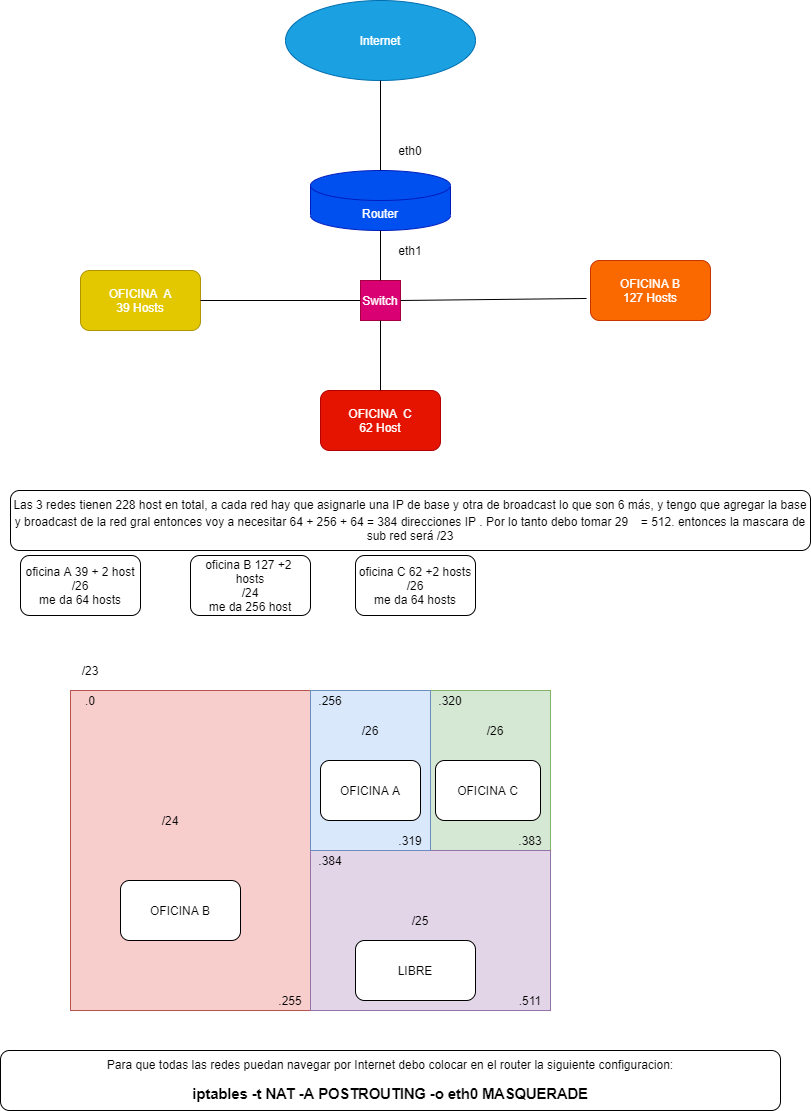
**El destino registra el tiempo transcurrido entre el momento que envía el paquete y el que recibe el mensaje de la correspondiente respuesta, y además registra el nombre y la dirección del router. De esta forma puede armar la ruta seguida por los paquetes. Por lo gral son 3 los paquetes que envía para obtener la ruta.**

1. Proponga un diagrama de red en donde coexistan y naveguen a internet a través de un único modem/router (que cuenta con 1 sola boca ethernet LAN disponible), las siguientes áreas:

* Oficina A: Se requieren conectar 39 computadoras por cable
* Oficina B: Se requieren conectar 127 computadoras por cable
* Oficina C: Se requieren conectar 62 computadoras por cable

En caso de necesitar equipos de tipo: HUB/SWITCH/ROUTER considere que los ROUTERS cuentan como máximo con 4 bocas (también conocidas como puertos físicos o interfaces) y los HUB/SWITCH cuentan como máximo con 8.

Indique además del diagrama, en forma clara y concreta, la cantidad de equipos totales que deberá adquirir (el modem/router frontera es provisto por la operadora de internet), el rango de direcciones completo para cada área y el ruteo necesario para que todas naveguen a internet. En caso de existir direcciones IP con alguna funcionalidad específica, indique cuáles son y descríbalas. **Todos los comandos que no sean aclarados, no serán considerados. Si realiza el diagrama en papel, el mismo deberá ser claro y legible.**

****

# Verdadero o Falso Para el caso de las **falsas** explique por qué y para las **verdaderas** brinde un ejemplo que demuestre la veracidad.

1. Si se tiene una topología store and forward como: A ---> Router ---> B y el primer bit de un paquete de 1Kb tarda en llegar 1ms de A al Router, entonces el primer bit tarda en llegar 2 ms de A a B.

**FALSO pueden ser enlaces de distintos tipos cuya velocidad de transmisión es distinta, entonces puede tardar lo mismo, más o igual, también influye la longitud de los enlaces.**

1. El comando “ifconfig 192.168.0.8/24” asigna la direccion 192.168.0.8 al host donde se esta ejecutando dicho comando

**FALSO falta colocar la interfaz que tiene asignada esa IP, por ejm. debería ser :**

**“ifconfig eth1 192.168.0.8/24**

**De esta forma a la interfaz eth1, del dispositivo que estoy ejecutando este comando, le asigno la IP mencionada.**

1. Si tengo dos redes privadas comunicadas a través de internet, no es posible aplicar ningún mecanismo para comunicar dos host de cada una ya que las direcciones privadas no son accesibles desde internet.

**FALSO se podría, aplicando NAT en cada router frontera de las redes.**

1. Si se realiza un ping a un destino por cuya ruta existe un ciclo, se genera un mensaje de error Network Unreachable

**FALSO, se produce el error de “Time-to-Live Exceeded”, no se encuentra nunca la respuesta**

1. El filtrado de un paquete en un router depende del orden en que se escriban las reglas.

**VERDADERO Para cada paquete se va comprobando si se le aplica cada regla de la cadena:**

**Si una regla NO se aplica a un paquete, se pasa a la siguiente regla de la cadena.**

**Si una regla SI se aplica a un paquete, se ejecuta la acción definida en dicha y finaliza ahí , no sigue ejecutando las siguientes reglas, por eso es importante el orden de como colocar las reglas.**

**Un ejm es el ejercicio 1c de este exámen que primero se enmascara toda la red , luego se pone lo que se acepta para a lo último rechazar todo el trafico restante.**