UNIVERSIDAD EIA

Administración de Redes

Simulación # 15

OBJETIVOS DE APRENDIZAJE:

- Realizar las configuraciones básicas del router
- Configurar las ACL estándar
- Configurar las ACL extendidas
- Verificar una ACL

DIAGRAMA DE TOPOLOGÍA:

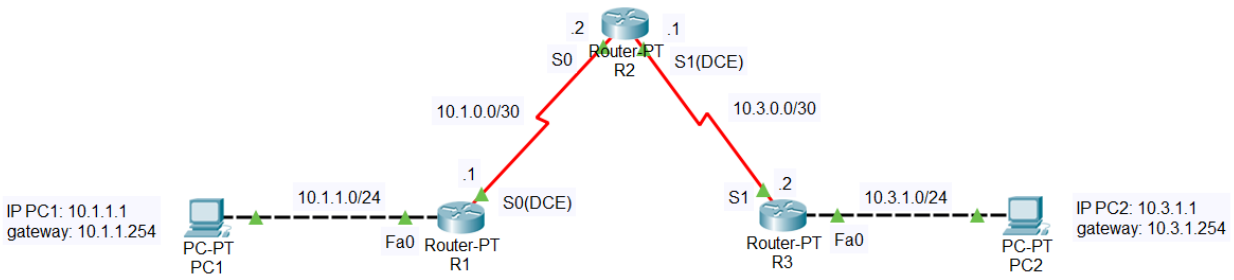

Figura 1 Diagrama de Topología

TABLA DE DIRECCIONAMIENTO:

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway Predeterminado
R1	Fa 0/0	10.1.1.254	255.255.255.0	NA
	S 0/0	10.1.0.1	255.255.255.252	NA
R2	S 0/0	10.1.0.2	255.255.255.252	NA
	S 1/0	10.3.0.1	255.255.255.252	NA
R3	Fa 0/0	10.3.1.254	255.255.255.0	NA
	S 1/0	10.3.0.2	255.255.255.252	NA
PC1	NIC	10.1.1.1	255.255.255.0	10.1.1.254
PC2	NIC	10.3.1.1	255.255.255.0	10.3.1.254

INTRODUCCIÓN:

En esta actividad se configurará ACL (Listas de Control de Acceso) para efectuar seguridad en la red.

TAREA 1: Realizar las configuraciones básicas del router

Realice las configuraciones básicas de los routers R1, R2 y R3 de acuerdo con las siguientes pautas generales:

1. Configure el nombre de host del router.
2. Deshabilite la búsqueda DNS.
3. Configure la contraseña en modo EXEC como **clase**.
4. Configure un mensaje del día.
5. Configure la contraseña para las conexiones de consola como **redes**.
6. Configure la contraseña para las conexiones VTY como **redes**.
7. Configure máscaras y direcciones IP en todos los dispositivos. La frecuencia de reloj es **64 000**.
8. Habilite OSPF con el ID de proceso 1 en todos los routers para todas las redes usando el área por defecto.
9. Verifique la conectividad IP completa mediante el comando **ping**.

TAREA 2: Configurar las ACL estándar

Configure las ACL estándar nombradas en las líneas vty de R1 y R3, de modo que los hosts directamente conectados a sus subredes FastEthernet tengan acceso a Telnet. Deniegue todos los demás intentos de conexión. Asigne a estas ACL estándar el nombre **VTY-Local**. Documente sus procedimientos de prueba.
En las líneas, use el comando *access-class <nombre de la lista> in/out* (Escriba in, ya que el acceso es para los PCs).
En el modo de configuración global de cada router cree la ACL estándar con *ip access-list standard VTY-Local* y luego configure las sentencias indicadas.

Ejemplo

```
ip access-list standard VTY-Local
 permit 10.1.1.0 0.0.0.255
 deny any
```

TAREA 3: Configurar las ACL extendidas

Complete los siguientes requisitos mediante las ACL extendidas en R2:

- Nombre a la ACL block. Use para serial 0 *block1*, y para la seria 1 *block2.*
  En cada interfaz use el comando: *ip access-group <nombre de la lista> in/out* (Escriba in porque será el tráfico que se origina desde las subredes que vienen hacia el router)
  En el modo de configuración global cree cada ACL extendida con *ip access-list extended <nombre de la lista>* y luego configure las siguientes sentencias según sea el caso.
- Prohíba que el tráfico que se origina desde las subredes conectadas de R1 alcance a las subredes conectadas de R3. Recuerde que el protocolo con el que trabajará será ICMP (el de ping)
- Prohíba que el tráfico que se origina desde las subredes conectadas de R3 alcance a las subredes conectadas de R1. Recuerde que el protocolo con el que trabajará será ICMP (el de ping)
- Permita todo el tráfico restante.

Ejemplo:

```
ip access-list extended block1
 deny icmp 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
 permit ip any any
```

TAREA 4: Verificar una ACL

Paso 1. Probar telnet.

- La PC1 debe poder hacer ping a R1.
- La PC2 debe poder hacer ping a R3.
- R2 debe tener denegado el acceso ping a R1 y R3.

Paso 2. Probar el tráfico.

- Los pings entre PC1 y PC2 deben fallar.

PRÁCTICA FINALIZADA. GUARDE LA SIMULACIÓN.

NOTA: Práctica basada en CCNA EXPLORATION, 2010