

Tema: ACLs Parte I

Contenidos

- Configuración básica
- Creación y aplicación de ACLs estándar

Objetivos Específicos

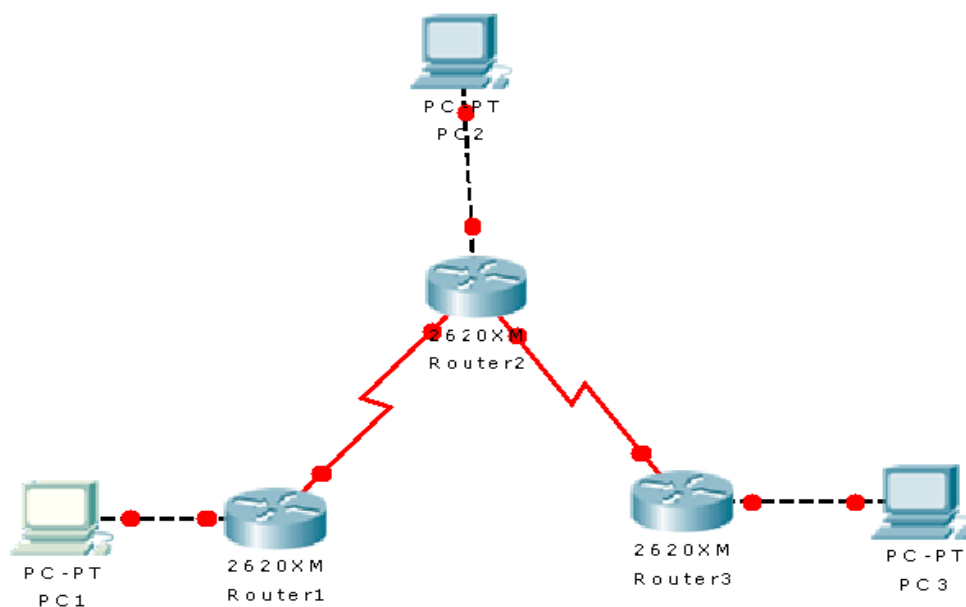
- Crear listas de control de acceso estándar
- Poder ubicar las listas de control de acceso en el router

Materiales y Equipo

- Computadora con simulador Packet Tracer
- 3 router
- 3 Computadoras
- 3 Cables seriales
- 3 Cables de consola
- 3 Convertidores serial a USB

Procedimiento

1. Armar la siguiente topología en el simulador.



NOTA: En esta configuración las dos interfaces del Router2 usan cables DCE

2. Borre las configuraciones de los router

Router#erase startup-config

Router#reload

Configuración básica.

3. Configuración de los routers

a) Router1

- Nombre de host: BORDE
- Contraseña de privilegiado encriptada: class
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 200.100.50.1 /24
- Dirección y máscara de S0: 204.204.7.1/30

b) Router2

- Nombre de host: CENTRO
- Contraseña de privilegiado encriptada: class
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 206.93.105.1 /24
- Dirección y máscara de S0: 204.204.7.2/30
- Dirección y máscara de S1: 201.100.11.1/30

c) Router3

- Nombre de host: EXTREMO
- Contraseña de privilegiado encriptada: cisco
- Contraseña de terminales virtuales (vty): ciscotel
- Dirección y máscara de Eth0: 199.6.13.1 /24
- Dirección y máscara de S0: 201.100.11.2/30

4. Configuración de las estaciones de trabajo

PC-1: Dirección ip: 200.100.50.2, máscara de subred: 255.255.255.0, gateway: 200.100.50.1

PC-2: Dirección ip: 206.93.105.2, máscara de subred: 255.255.255.0, gateway: 206.93.105.1

PC-3: Dirección ip: 199.6.13.2, máscara de subred: 255.255.255.0, gateway: 199.6.13.1

5. Configure RIPv2 en los tres enrutadores

6. Use el comando *show ip route* para verificar que en cada router aparezcan las rutas.

7. Realizar pruebas de conectividad entre computadoras con los comandos ping y traceroute

8. Almacenar los cambios hechos en la configuración en la NVRAM

9. En cualquier momento que quiera verificar el funcionamiento de una línea en específico de una ACL, utilice el comando *show access-lists*, el cual muestra las listas de control de acceso y las coincidencias (matches) en cada línea.

Creación y aplicación de ACLs estándar

A continuación se muestra la sintaxis de creación y asignación de las ACL estándar.

```
Router(config)#access-list numACL permit/deny origen [wild-mask]
Router(config)# interface interface_x
Router (config-if)# ip access-group numACL in/out
```

El comando de configuración global access-list define una ACL estándar con un número entre 1 y 99.

Ejemplo I

10. Crear y aplicar una ACL estándar que bloquee el tráfico proveniente de PC-1 y con destino PC-3 (cualquier otro tráfico será permitido).
11. Como primer paso se selecciona el enrutador idóneo para crear la ACL. Por ser estándar debe estar **lo más cerca posible del destino**, así que una buena elección es Extremo (Router 3) interfaz Ethernet 0.
12. Escribir la ACL en el enrutador seleccionado.

```
EXTREMO#configure terminal
EXTREMO(config)#access-list 1 deny 200.100.50.2 0.0.0.0
EXTREMO(config)#access-list 1 permit any
EXTREMO(config)#interface Ethernet 0
EXTREMO(config-if)#ip access-group 1 out
EXTREMO(config-if)#CTRL+Z
```

13. Comprobar el funcionamiento de la ACL. Realizar un ping y traceroute desde PC-1 hasta PC-3. Se debe dar una respuesta no exitosa.
14. Cambie la dirección IP de PC-1 a la *200.100.50.3* y realice nuevamente la prueba (deberá de ser exitosa ya que solamente se ha limitado a la dirección *200.100.50.2*).
15. Cambie nuevamente a la dirección IP original a PC-1.
16. Desactivar la *ACL 1*, usando los siguientes comandos:

```
EXTREMO#configure terminal
EXTREMO(config)#interface Ethernet 0
EXTREMO(config-if)#no ip access-group 1 out
EXTREMO(config-if)#CTRL+Z
```

17. Realizar nuevamente pruebas de conectividad entre las PC-1 y PC-3 (deben ser exitosas)

Ejemplo II

18. Ahora cree y aplique una ACL estándar que bloquee el tráfico con origen PC-1 y destino PC-2, y que además permita el tráfico con origen PC-3 y destino PC-2. (Cualquier otro tráfico será negado).

19. Selección del enrutador: Más cerca del destino CENTRO.

20. Escribir la ACL estándar

```
CENTRO#configure terminal
CENTRO(config)#access-list 2 deny host 200.100.50.2
CENTRO(config)#access-list 2 permit host 199.6.13.2
CENTRO(config)#access-list 2 deny any
CENTRO(config)#interface Ethernet 0
CENTRO(config-if)#ip access-group 2 out
CENTRO(config-if)#CTRL+Z
```

21. Realizar pruebas de ping y traceroute desde PC-1 y PC3 hacia PC2. Se obtendrán pruebas exitosas solo desde PC-3.

22. Desactivar la ACL 2 en la interfaz Ethernet 0

```
CENTRO#configure terminal
CENTRO(config)#interface Ethernet 0
CENTRO(config-if)#no ip access-group 2 out
CENTRO(config-if)#CTRL+Z
```

Ejemplo III

23. Configure una ACL que bloquee y permita el tráfico de toda la red y no solo de un host en particular.

```
CENTRO#configure terminal
CENTRO(config)#access-list 3 deny 200.100.50.0 0.0.0.255
CENTRO(config)#access-list 3 permit 199.6.13.0 0.0.0.255
CENTRO(config)#access-list 3 deny any
CENTRO(config)#interface Ethernet 0
CENTRO(config-if)#ip access-group 3 out
CENTRO(config-if)#CTRL+Z
```

24. Ahora compruebe que toda la red en que pertenece PC1 ha sido bloqueada, para esto cambie la dirección IP de PC1 a 200.100.50.10

25. Desactivar la ACL 3 en la interfaz Ethernet 0.

26. Hacer pruebas de conectividad nuevamente.

Ejercicio I

27. Utilizando la *wild-mask*, cree una ACL 4 con destino PC-3 con los siguientes requerimientos:
- Permita solamente el tráfico de las IP's impares (exceptuando la IP 200.100.50.24) de la LAN del router *BORDE*.
 - Deniegue el tráfico de la mitad superior del rango de IP's, pertenecientes a la LAN del router *CENTRO*.
28. Muestre a su instructor el funcionamiento de la ACL.
29. Borre las configuraciones de los router (este paso será verificado por el instructor).
30. Ordene y entregue el equipo.

Bibliografía

- Network+ 2005 In Depth, Tamara Dean; Course Technology PTR; 1 edition (March 15, 2005)
- Local Area Networks (McGraw-Hill Forouzan Networking Series), Forouzan McGraw-Hill Education - Europe (February 1, 2002)
- CCNA Study Guide Fourth Edition, Sybex
- Guías Prácticas de la FET, REDES WAN

Guía 8: ACLs Parte I

Alumno:

Máquina No:

Docente:

GL:

Fecha:

EVALUACION					
	%	1-4	5-7	8-10	Nota
CONOCIMIENTO	Del 20 al 30%	Conocimiento deficiente de los fundamentos teóricos	Conocimiento y explicación incompleta de los fundamentos teóricos	Conocimiento completo y explicación clara de los fundamentos teóricos	
APLICACIÓN DEL CONOCIMIENTO	Del 40% al 60%				
ACTITUD	Del 5% al 10%	No tiene actitud proactiva.	Actitud propositiva y con propuestas no aplicables al contenido de la guía.	Tiene actitud proactiva y sus propuestas son concretas.	
TOTAL	100%				