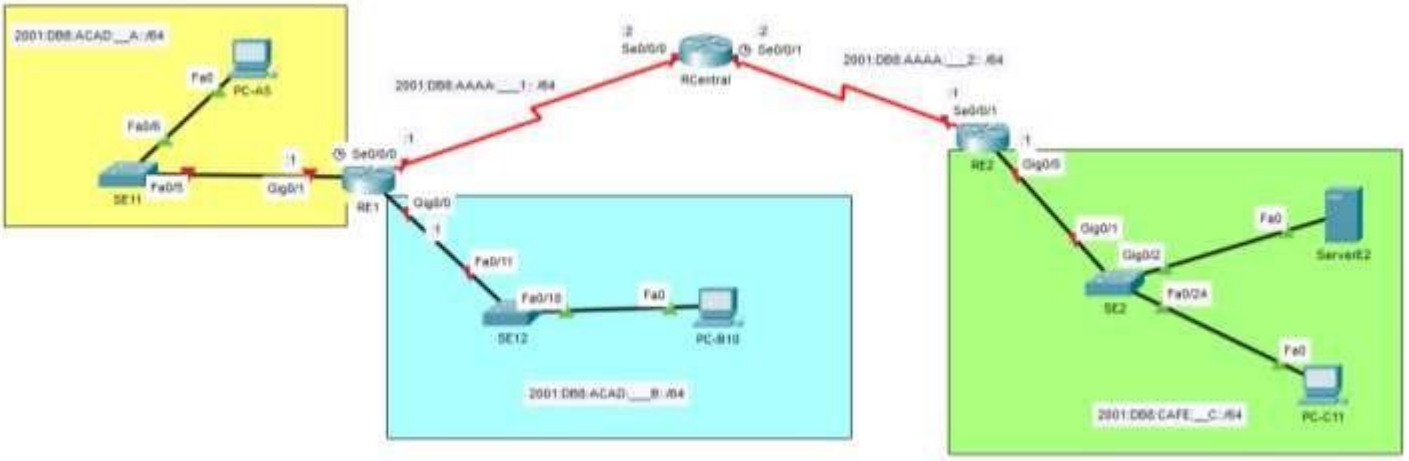
FECHA DE REALIZACION: 19-31/07/2023	**GRUPO: IRD-32**
FECHA DE REPORTE: 31/07/2023	**REVISÓ: DRA. P. NORMA MAYA PÉREZ**
ASIGNATURA: CONMUTACIÓN EN REDES DE DATOS	**APROBÓ: Comisión de Interconexión de Redes**
UNIDAD TEMÁTICA: III Introducción a la Seguridad en Redes (Módulo 3-5 Seguridad de la Red–CCNA3v7)	
TEMAS: - Configuración de listas control de acceso (ACL) IPv6	CUATRIMESTRE: Tercero
Nombre de participante:	Competencia obtenida:
LUGAR: Laboratorio Cisco	Observaciones:

REQUISITOS TEÓRICOS DE LA PRÁCTICA:

Dado el siguiente escenario de red de la empresa "XYZ" desea implementar Direccionamiento IPV6 en la que se requiere comunicarse en las áreas distribuidas en diferentes zonas geográficas, estableciendo algunas políticas de acceso en la red para controlar el tráfico para establecer un enlace de comunicación de datos eficiente.



Aspectos básicos/situación:

Aplicará sus habilidades y conocimientos de Introducción a la Seguridad y Configuración de listas control de acceso (ACL) para IPv6.

Puede filtrar el tráfico IPv6 mediante la creación de listas de control de acceso (ACL) de IPv6 y su aplicación a las interfaces, en forma similar al modo en que se crean ACL de IPv4 con nombre. Los tipos de ACL de IPv6 son extendidas y con nombre. Las ACL estándar y numeradas ya no se utilizan con IPv6. Para aplicar una ACL de IPv6 a una interfaz vty, use el nuevo comando ipv6 access-class. El comando ipv6 traffic-filter todavía se usa para aplicar una ACL de IPv6 a las interfaces.

Recursos necesarios:

Software Packet tracer 8.2.1 o superior, equipo de cómputo con acceso a internet, Microsoft Word versión 2010 o superior, adobe reader.

OBJETIVO DE LA PRÁCTICA

Configurar el direccionamiento y enrutamiento, así como restringir el tráfico en la red configurando ACL IPv6 en la topología asignada.

Marco Teórico: Defina los conceptos relacionados a la práctica

Nota: consultar Módulo 3-5 Seguridad de la Red en CCNA3v7 Netacad y material publicado en classroom

PROCEDIMIENTO:

PARTE I. Direccionamiento y enrutamiento.

I.1 Completar Tabla de Direccionamiento, basándose en la topología de Paacket tracer.

Device	Interface	IP Address	Default Gateway
RE1	G0/0	2001:DB8:ACAD:05B::1 /64	N/D
	G0/1	2001:DB8:ACAD:05A::1 /64	N/D
	S0/0/0 (DCE)	2001:DB8:AAAA:051::1 /64	N/D
RCentral	S0/0/0	2001:DB8:AAAA:051::2 /64	N/D
	S0/0/1 (DCE)	2001:DB8:AAAA:052::2 /64	N/D
RE2	G0/0	2001:DB8:CAFE:05C::1 /64	N/D
	S0/0/1	2001:DB8:AAAA:052::1 /64	N/D
PC-A5	NIC	2001:DB8:ACAD:05A::5 /64	FE80::1
PC-B10	NIC	2001:DB8:ACAD:05B::10 /64	FE80::1
PC-C11	NIC	2001:DB8:CAFE:05C::11 /64	FE80::1
ServerE2	NIC	192.168.45.254/24	---
		2001:DB8:CAFE:05C::254 /64	FE80::1

Nota: El valor del Cuarto Hexteto es su No. de lista. Ejemplo el número de lista 1: 2001:DB8: AAAA: 001:: /64, el número de lista 10: 2001:DB8:AAAA:101:: /64

I.2 Deshabilite la búsqueda del DNS y configurar el nombre de host, contraseña del modo EXEC privilegiado como **class32** y encrypte las contraseñas en los Routers y Switches indicados en la topología de packet tracer.

I.3 Configurar telnet (líneas VTY como **cisco**), en los Routers.

I.4 Configurar direccionamiento IPv6 en los Routers y dispositivos finales.

```
*** SE11 ********************************************************
enable
conf t
no ip domain-lookup
hostname SE11
enable secret class32
service password-encryption
end
```

copy run star

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname SE11
SE11(config)#enable secret class32
SE11(config)#service password-encryption
SE11(config)#end
SE11#copy run start
%SYS-5-CONFIG_I: Configured from console by console

Destination filename [startup-config]?
Building configuration...
[OK]
```

********** RE1**********

enable
conf t
no ip domain-lookup
hostname RE1
line vty 0 4
password cisco
login
exit
enable secret class32
service password-encryption
ipv6 unicast-routing
interface G0/0
ipv6 address 2001:DB8:ACAD:40B::1/64
ipv6 address FE80::1 link-local
no shutdown
exit
int g0/1
ipv6 address 2001:DB8:ACAD:40A::1/64
ipv6 address FE80::1 link-local
no shutdown
exit
interface Serial0/0/0
ipv6 address 2001:DB8:AAAA:401::1/64
ipv6 address FE80::1 link-local
no shutdown
clock rate 128000
exit
do show ipv6 int brief

-- configurar los equipos faltantes

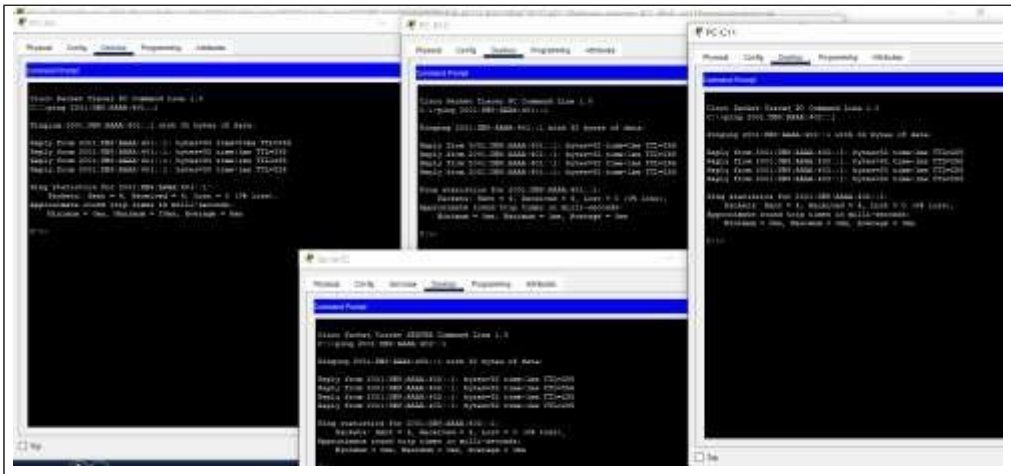
```
enable
conf t
no ip domain-lookup
hostname RE1
line vty 0 4
password cisco
login
exit
enable secret class32
service password-encryption
ipv6 unicast-routing
interface G0/0
ipv6 address 2001:DB8:ACAD:05B::1/64
ipv6 address FE80::1 link-local
no shutdown
exit
int g0/1
ipv6 address 2001:DB8:ACAD:05A::1/64
ipv6 address FE80::1 link-local
no shutdown
exit
interface Serial0/0/0
ipv6 address 2001:DB8:AAAA:051::1/64
ipv6 address FE80::1 link-local
no shutdown clock rate 128000
exit
```

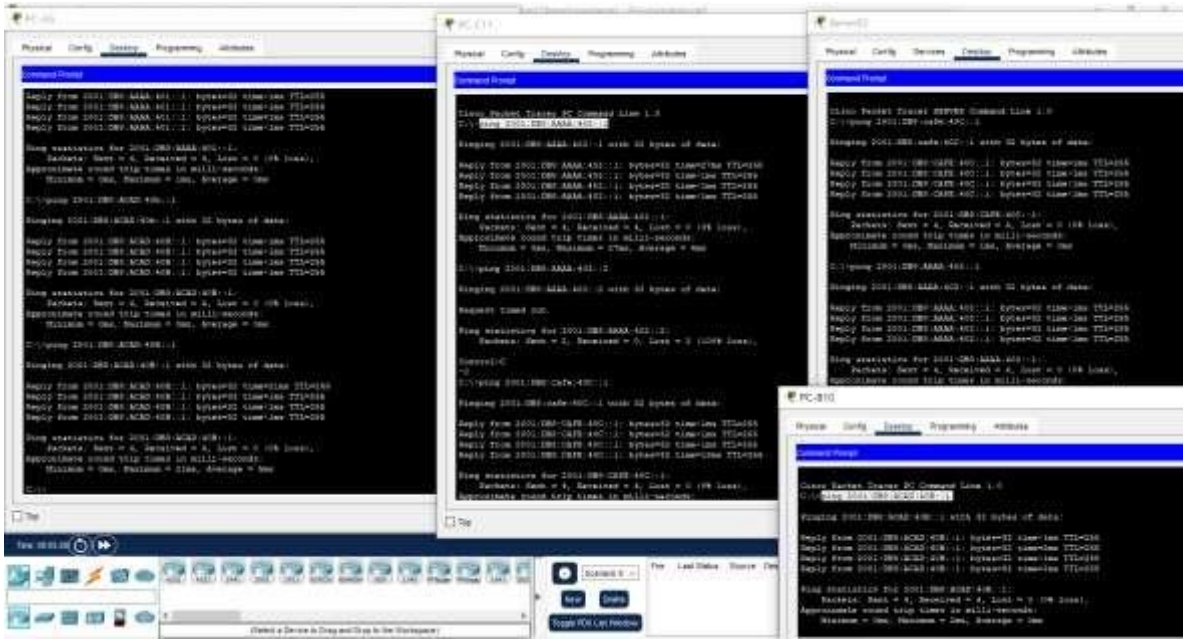
----------RE2

```
enable
conf t
no ip domain-lookup
hostname RE2
line vty 0 4
password cisco
login
exit
enable secret class32
service password-encryption
ipv6 unicast-routing
interface G0/0
ipv6 address 2001:DB8:CAFE:05C::1/64
ipv6 address FE80::1 link-local
no shutdown
exit
interface Serial0/0/1
ipv6 address 2001:DB8:AAAA:052::1/64
ipv6 address FE80::1 link-local
no shutdown clock rate 128000
exit
```

```
en
conf t
ipv6 access-list RCentral-RESTRICT-VTY
deny tcp host 2001:DB8:CAFE:05C::11 2001:DB8:AAAA::/48 eq 23
permit tcp any any eq 23
permit tcp any any eq 22
permit ipv6 any any
exit

line vty 0 4
ipv6 access-class RCentral-RESTRICT-VTY in
exit

int g0/0
ipv6 traffic-filter RCentral-RESTRICT-VTY in
end
```

I.5 Verificar conectividad local de cada LAN antes de pasar al siguiente paso y resuelva cualquier problema presentado.





```
C:\>ping 2001:DB8:ACAD:5A::5

Pinging 2001:DB8:ACAD:5A::5 with 32 bytes of data:

Reply from 2001:DB8:ACAD:5A::5: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:5A::5: bytes=32 time<1ms TTL=127
Reply from 2001:DB8:ACAD:5A::5: bytes=32 time=1ms TTL=127
Reply from 2001:DB8:ACAD:5A::5: bytes=32 time<1ms TTL=127

Ping statistics for 2001:DB8:ACAD:5A::5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 2001:DB8:CAFE:5C::11

Pinging 2001:DB8:CAFE:5C::11 with 32 bytes of data:

Reply from 2001:DB8:CAFE:5C::11: bytes=32 time=22ms TTL=125
Reply from 2001:DB8:CAFE:5C::11: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:CAFE:5C::11: bytes=32 time=2ms TTL=125
Reply from 2001:DB8:CAFE:5C::11: bytes=32 time=2ms TTL=125

Ping statistics for 2001:DB8:CAFE:5C::11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 22ms, Average = 7ms
```

I.6 habilitar enrutamiento OSPF para IPv6 con id proceso 32 y área *su Numero de Lista*, los Router-id son:

RE1- 1.1.1.1, RCentral- 2.2.2.2, RE2 - 3.3.3.3

********** RE1******* *** OSPFv3 IPv6 **********

```
enable
conf t
ipv6 unicast-routing
ipv6 router ospf 32
router-id 1.1.1.1
int g0/0
ipv6 ospf 32 area 50
exit
int g0/1
ipv6 ospf 32 area 50
exit
```

RE1

```
enable
conf t
ipv6 unicast-routing
ipv6 router ospf 32
router-id 1.1.1.1
int g0/0
ipv6 ospf 32 area 5
exit
int g0/1
ipv6 ospf 32 area 5
exit
interface S0/0/0
ipv6 ospf 32 area 5
exit
ipv6 route ::/0 2001:DB8:AAAA:51::2
```

interface S0/0/0 ipv6
ospf 32 area 50end
show ipv6 route

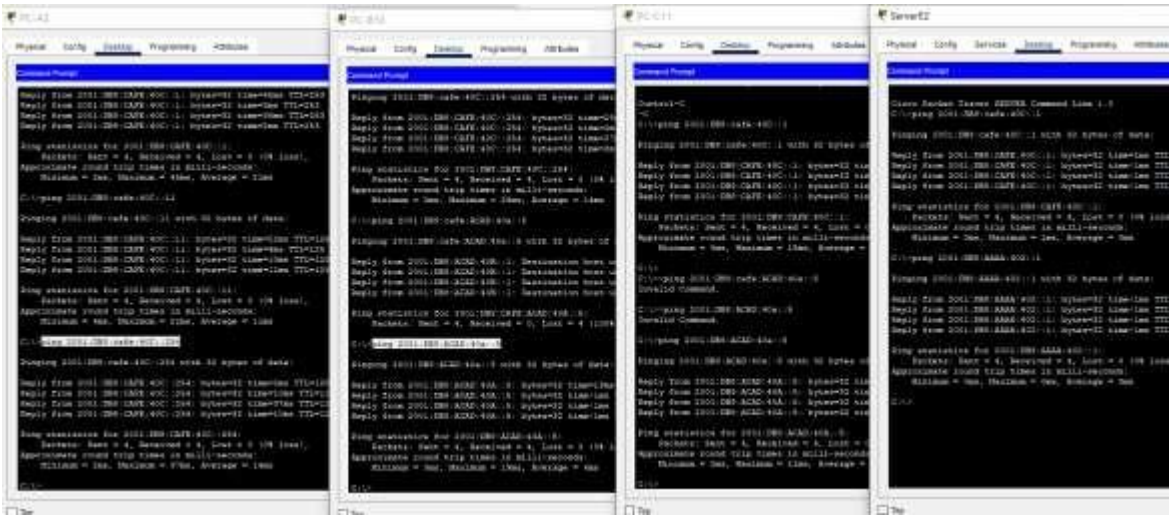
8

-- configurar los equipos faltantes

I.7 Verificar la tabla de enrutamiento y la conectividad en toda la red indicada en la topología. En caso de encontrar fallas, resuelva antes de continuar los pasos siguientes.

a) Se debería poder hacer ping entre todas las computadoras y al servidor de la topología.

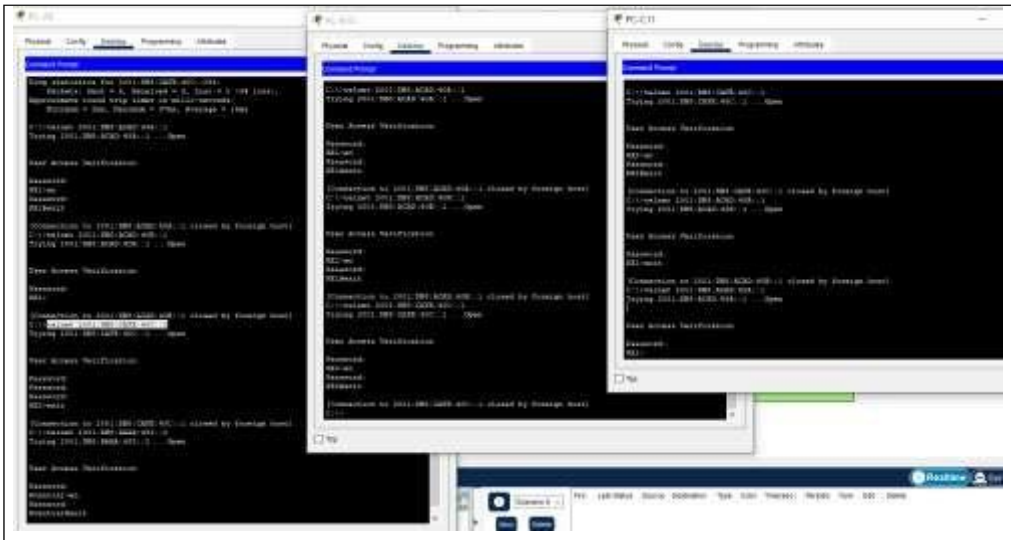
Correcto, hay conectividad de extremo a extremo de PC-A a PC-C



I.8 Verifique conectividad con telnet desde cada PC y del Servidor a cada Router antes de pasar al paso I.9

Desde PC-A5
C:\>**telnet 2001:DB8:ACAD:_A::1**
Trying 2001:DB8:ACAD:_A::1 ...Openwarning users that unauthorized access is prohibited
User Access Verification
Password:
R1>en
Password:
R1#exit
[Connection to 2001:DB8:ACAD:_A::1 closed by foreign host]
C:\>

```
C:\>telnet 2001:DB8:AAAA:051::2
Trying 2001:DB8:AAAA:51::2 ...Open


User Access Verification

Password:
```



I.9 En RE1 configurar lo siguiente:

a) Asigne grupo32-lab.com como nombre de dominio.
b) Cree una base de datos de usuarios local con el nombre de usuario **admin** y la contraseña **admin32**
c) Genere una clave criptográfica rsa para ssh con un tamaño de módulo de 1024 bits.
d) Habilite el inicio de sesión en las líneas VTY con la base de datos local.
e) Cambie las líneas VTY de transport input a «all» solo para SSH.

```
R1(config)#
enable
conf t
ip domain-name grupo32-lab.com
username admin password admin32
enable secret class32
line vty 0 4
login local
transport input ssh
exit
crypto key generate rsa
en How many bits in the modulus [512]: 1024
```

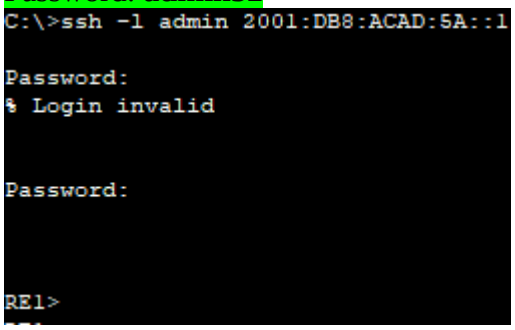

```
enable
conf t
ip domain-name grupo32-lab.com
username admin password admin32
enable secret class32
line vty 0 4
login local
transport input ssh
exit
crypto key generate rsa
en How many bits in the modulus [512]: 1024
```

f) Acceda al RE1 mediante SSH desde todas las computadoras y servidor de la topología. Debe ser exitoso en Telnet ya no se puede accesar a RE1, porque se reemplazó con SSH

Desde la PC-A5, PC-B10, PC-C11

C:> **ssh -l admin 2001:DB8:ACAD:40A::1**

Password: **admin32**



g) Solucione los problemas de conectividad, porque las ACL que se crean en la parte II del caso práctico, restringirán el acceso a ciertas áreas de la red. Verifique la conectividad total de la red empresarial, en caso de no tener éxito, resuelva problemas identificados.

PARTE II Configuración de listas ACL IPv6

III.1 Configurar los servicios IPv6 en el Servidor:

a) FTP (User: grupo32, contraseña:class32) con permisos de leer, renombrar, escribir y listar.

b) DNS (dominio: grupoird32.pka.pt)

II.2 Cree una ACL en la que la PC-C11 no tenga acceso de telnet a RCentral pero **Si** a RE2, los demás equipos **Si** tienen acceso a telnet a RCentral y también los demás equipos tienen acceso SSH a RE1.

a) Configure la ACL en el router correcto

**********RE2**********

```
en
conf t
ipv6 access-list RCentral-RESTRICT-VTY
deny tcp host 2001:DB8:CAFE:__C::11 2001:DB8:AAAA::/48 eq 23
permit tcp any any eq 23
permit tcp any any eq 22
permit ipv6  any  any
exit

line vty 0 4
ipv6 access-class RCentral-RESTRICT-VTY in
exit
```

```
en
conf t
ipv6 access-list RCentral-RESTRICT-VTY
deny tcp host 2001:DB8:CAFE:05C::11 2001:DB8:AAAA::/48 eq 23
permit tcp any any eq 23
permit tcp any any eq 22
permit ipv6 any any
exit
```

int g0/0
ipv6 traffic-filter RCentral-RESTRICT-VTY in
end

```
int g0/0
ipv6 traffic-filter RCentral-RESTRICT-VTY in
end
```

b) Visualice la nueva ACL

RE2#**show access-lists**

```
RE2#show access-lists
IPv6 access list RCentral-RESTRICT-VTY
    deny tcp host 2001:DB8:CAFE:5C::11 2001:DB8:AAAA::/48 eq telnet (12 match(es))
    permit tcp any any eq telnet
    permit tcp any any eq 22
    permit ipv6 any any (8 match(es))
```

c) Verifique que la ACL del paso 1, en la que la PC-C11 no tenga acceso de telnet a RCentral pero SI a RE2, los demás equipos SI tienen acceso a telnet de R2 y también los demás equipos tengan acceso SSH a RE1

```
C:\>telnet 2001:DB8:AAAA:52::2
Trying 2001:DB8:AAAA:52::2 ...
% Connection timed out; remote host not responding
C:\>
```

¿Qué hace las instrucciones en la ACL R2-RESTRICT-VTY explique?

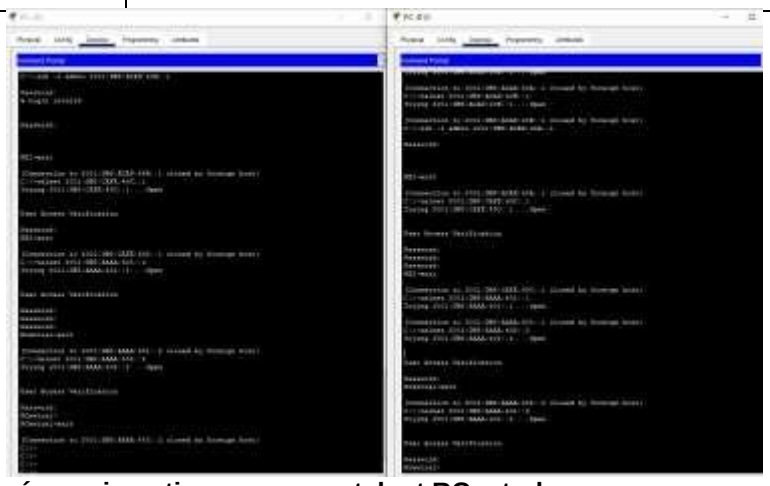
permit tcp any any **eq 23** → **permite solo el trafico telnet**

permit tcp any any **eq 22** → **permite solo el trafico telnet**

permit ipv6 any any → **permite cualquier otro tráfico**

int g0/1

ipv6 traffic-filter R2-RESTRICT-VTY in → habilita la ACL en la interfaz



Las demás equipos tiene acceso a telnet RCentral

PC B10

```
C:\>telnet 2001:DB8:AAAA:52::2
Trying 2001:DB8:AAAA:52::2 ...Open


User Access Verification

Password:
Password:
RCENT>
```

PC-A5

```
C:\>telnet 2001:DB8:AAAA:52::2
Trying 2001:DB8:AAAA:52::2 ...Open


User Access Verification

Password:
RCENT>
RCENT>
```

d) Use el comando **show ipv6 access-list** para ver la ACL RESTRICTED-LAN.

```
RE1# show ipv6 access-list
IPv6 access list NO-ACCESS-FTP
    deny tcp 2001:DB8:ACAD:5B::/64 host 2001:DB8:CAFE:5C::254 eq ftp (12 match(es))
    permit tcp any any eq ftp
    permit ipv6 any any (144 match(es))
IPv6 access list NO-ACCESS-DNS
    deny udp 2001:DB8:ACAD:5A::/64 host 2001:DB8:CAFE:5C::254 eq domain (4 match(es))
    permit tcp any any eq domain
    permit ipv6 any any (218 match(es))
```

e)

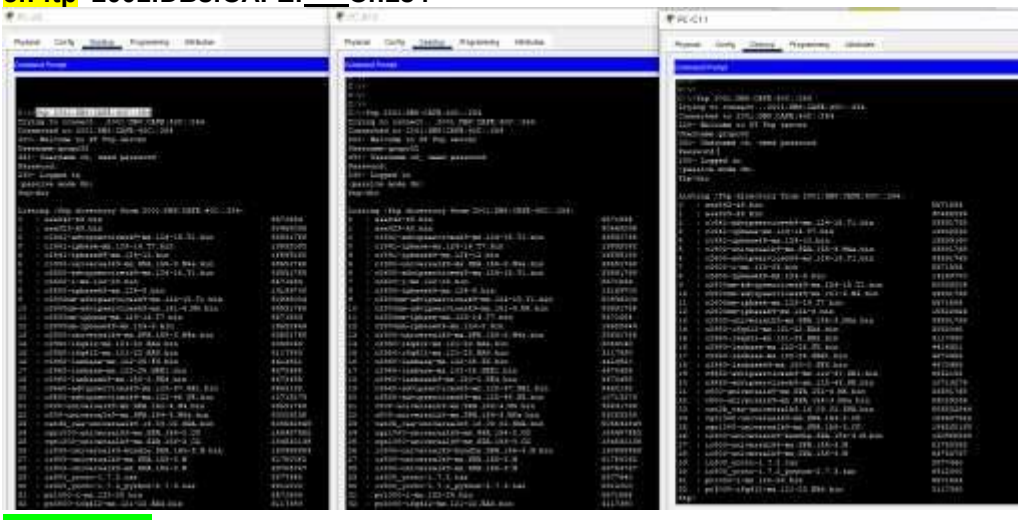
```
RE2#show ipv6 access-list
IPv6 access list RCentral-RESTRICT-VTY
  deny tcp host 2001:DB8:CAFE:_C::11 2001:DB8:AAAA::/48 eq telnet (48 match(es))
  permit tcp any any eq telnet (61 match(es))
  permit tcp any any eq 22
  permit ipv6 any any (4 match(es))
```

Observe que cada instrucción identifica el número de aciertos o coincidencias que se produjeron desde la aplicación de la ACL a la interfaz

II.3 Cree una ACL en la que la red 2001:DB8:ACAD:_B::/64 no tiene acceso al servidor FTP, pero si tiene acceso a los demás servicios y acceso remoto en los 3 routers.

a) Verifique que se tienen acceso antes de aplicar la nueva ACL.

Desde el editor de comandos
c:: ftp 2001:DB8:CAFE:___C::254



Quit salimos

```
[Connection to 2001:DB8:AAAA:52::2 closed by foreign host]
C:\>ftp 2001:DB8:CAFE:5C::254
Trying to connect...2001:DB8:CAFE:5C::254
```

b) Configure la ACL en el router correcto

**********RE1**
ipv6 access-list NO-ACCESS-FTP
deny tcp 2001:DB8:ACAD:_B::/64 **host 2001:DB8:CAFE:_C::254 eq ftp**
permit tcp any any **eq ftp**
permit ipv6 any any
exit
int g0/0
ipv6 traffic-filter **NO-ACCESS-FTP** in
end

c) Visualice la nueva ACL

d)

RE1#**sh access-lists**
IPv6 access list NO-ACCESS-FTP
deny tcp 2001:DB8:ACAD:_B::/64 host 2001:DB8:CAFE:_C::254 eq ftp (24 match(es))
permit tcp any any eq ftp
permit ipv6 any any (80 match(es))

RE1#**sh ipv6 access-list**
IPv6 access list NO-ACCESS-FTP
deny tcp 2001:DB8:ACAD:_B::/64 host 2001:DB8:CAFE:_C::254 eq ftp (24 match(es))
permit tcp any any eq ftp
permit ipv6 any any (80 match(es))

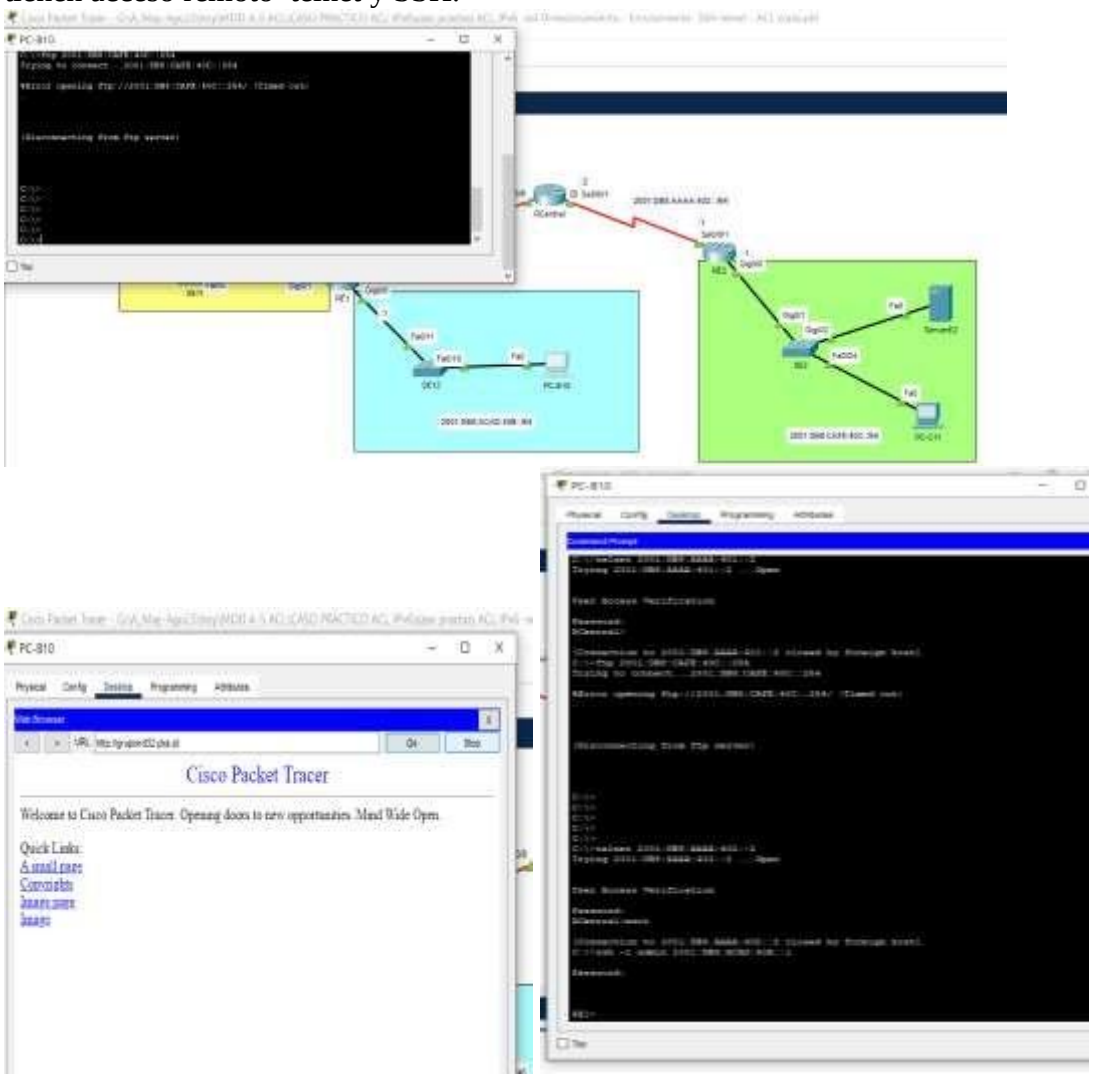
Observe que cada instrucción identifica el número de aciertos o coincidencias que se produjeron desde la aplicación de la ACL a la interfaz

```
RE1#sh access-lists
IPv6 access list NO-ACCESS-FTP
    deny tcp 2001:DB8:ACAD:5B::/64 host 2001:DB8:CAFE:5C::254 eq ftp (24 match(es))
    permit tcp any any eq ftp
    permit ipv6 any any (157 match(es))
IPv6 access list NO-ACCESS-DNS
    deny udp 2001:DB8:ACAD:5A::/64 host 2001:DB8:CAFE:5C::254 eq domain (4 match(es))
    permit tcp any any eq domain
    permit ipv6 any any (218 match(es))

RE1#
```

Ipv6

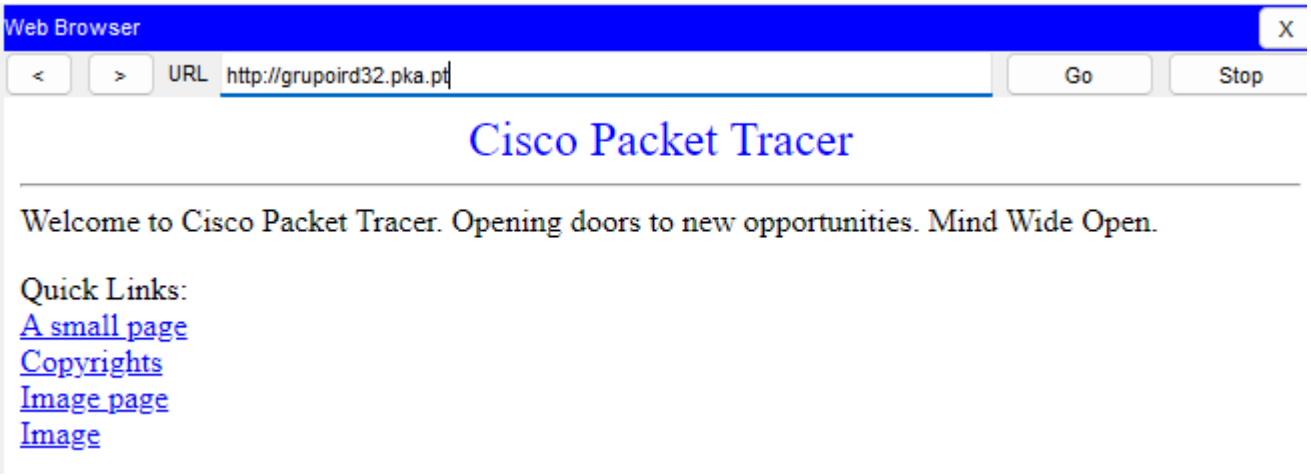
```
RE1#sh ipv6 access-list
IPv6 access list NO-ACCESS-FTP
    deny tcp 2001:DB8:ACAD:5B::/64 host 2001:DB8:CAFE:5C::254 eq ftp (24 match(es))
    permit tcp any any eq ftp
    permit ipv6 any any (157 match(es))
IPv6 access list NO-ACCESS-DNS
    deny udp 2001:DB8:ACAD:5A::/64 host 2001:DB8:CAFE:5C::254 eq domain (4 match(es))
    permit tcp any any eq domain
    permit ipv6 any any (218 match(es))

RE1#
```

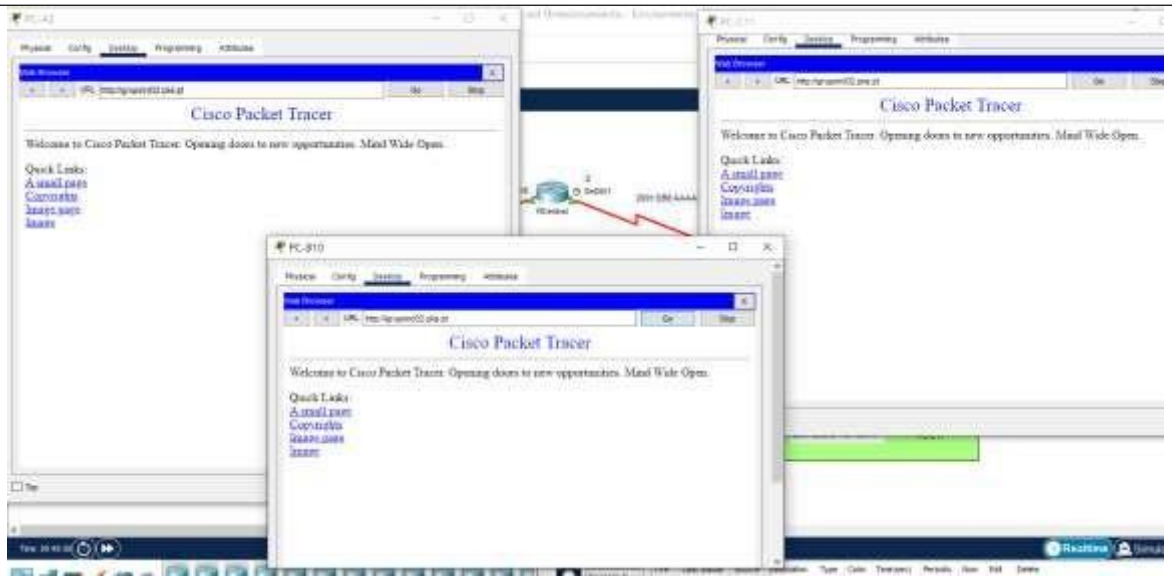
d) Verifique que la ACL implementada, en la que la PC-B no tiene acceso a FTP pero si a todos los demás servicios , los demás equipos SI tienen acceso FTP y todos los equipos permitidos de la ACL del paso II.2, tienen acceso remoto telnet y SSH.



II.4 Cree una ACL en la que la red 2001:DB8:ACAD:__A::/64 no tiene acceso al servidor DNS, pero si todo tiene acceso a todos los demás servicios y acceso remoto a los 3 routers.

a) Verifique que se tienen acceso antes de aplicar la nueva ACL.


Web Browser
X
<
>
URL
http://grupoird32.pka.pt
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image



b) Configure la ACL en el router correcto

**************RE1**

```
ipv6 access-list NO-ACCESS-DNS
deny udp 2001:DB8:ACAD:_A::/64 host 2001:DB8:CAFE:_C::254 eq 53
permit tcp any any eq 53
permit ipv6 any  any
exit
int g0/1
ipv6 traffic-filter NO-ACCESS-DNS in
end
```

```
en
conf t
ipv6 access-list NO-ACCESS-DNS
deny udp 2001:DB8:ACAD:05A::/64 host 2001:DB8:CAFE:05C::254 eq 53
permit tcp any any eq 53
permit ipv6 any any
exit
int g0/1
ipv6 traffic-filter NO-ACCESS-DNS in
end
```

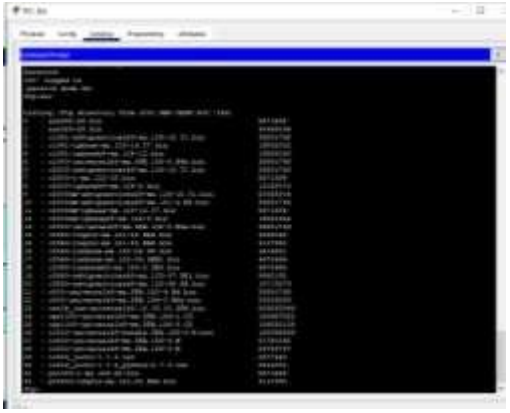
c) Visualice la nueva ACL

RE1#show access-lists

```
IPv6 access list NO-ACCESS-FTP
    deny tcp 2001:DB8:ACAD:__B::/64 host 2001:DB8:CAFE:___C::254 eq ftp (12 match(es))
    permit tcp any any eq ftp
    permit ipv6 any any (55 match(es))
IPv6 access list NO-ACCESS-DNS
    deny udp 2001:DB8:ACAD:___A::/64 host 2001:DB8:CAFE:___C::254 eq domain (11 match(es))
    permit tcp any any eq domain
    permit ipv6 any any
```

RE1#show ipv6 access-list
IPv6 access list NO-ACCESS-FTP
deny tcp 2001:DB8:ACAD:___B::/64 host 2001:DB8:CAFE:___C::254 eq ftp (12 match(es))
permit tcp any any eq ftp
permit ipv6 any any (55 match(es))
IPv6 access list NO-ACCESS-DNS
deny udp 2001:DB8:ACAD:___A::/64 host 2001:DB8:CAFE:___C::254 eq domain (11 match(es))
permit tcp any any eq domain
permit ipv6 any any

d) Verifique que la ACL, en la que la Red del PC-A5 no tiene acceso a DNS pero si a todos los demás servicios , los demás equipos SI tienen acceso DNS y todos los equipos permitidos de la ACL paso II.2 y II.3, tienen acceso remoto telnet y SSH.



```
El#sh ipv6 access-list
Pv6 access list NO-ACCESS-FTP
   deny tcp 2001:DB8:ACAD:5B::/64 host 2001:DB8:CAFE:5C::254 eq ftp (24 match(es))
   permit tcp any any eq ftp
   permit ipv6 any any (157 match(es))
Pv6 access list NO-ACCESS-DNS
   deny udp 2001:DB8:ACAD:5A::/64 host 2001:DB8:CAFE:5C::254 eq domain (4 match(es))
   permit tcp any any eq domain
   permit ipv6 any any (218 match(es))
```

PARTE III. RESULTADOS **se considera desempeño y participación de clase + Reporte del caso práctico**

Colocar las imágenes de los resultados obtenidos en el caso práctico.

III.1 Verifique la conectividad de los equipos y resuelva problemas de comunicación.

III.2 Verifique las ACL's implementadas en la red de la empresa.

show access-list

show ipv6 access-list

Explique la diferencia en estos dos comandos.

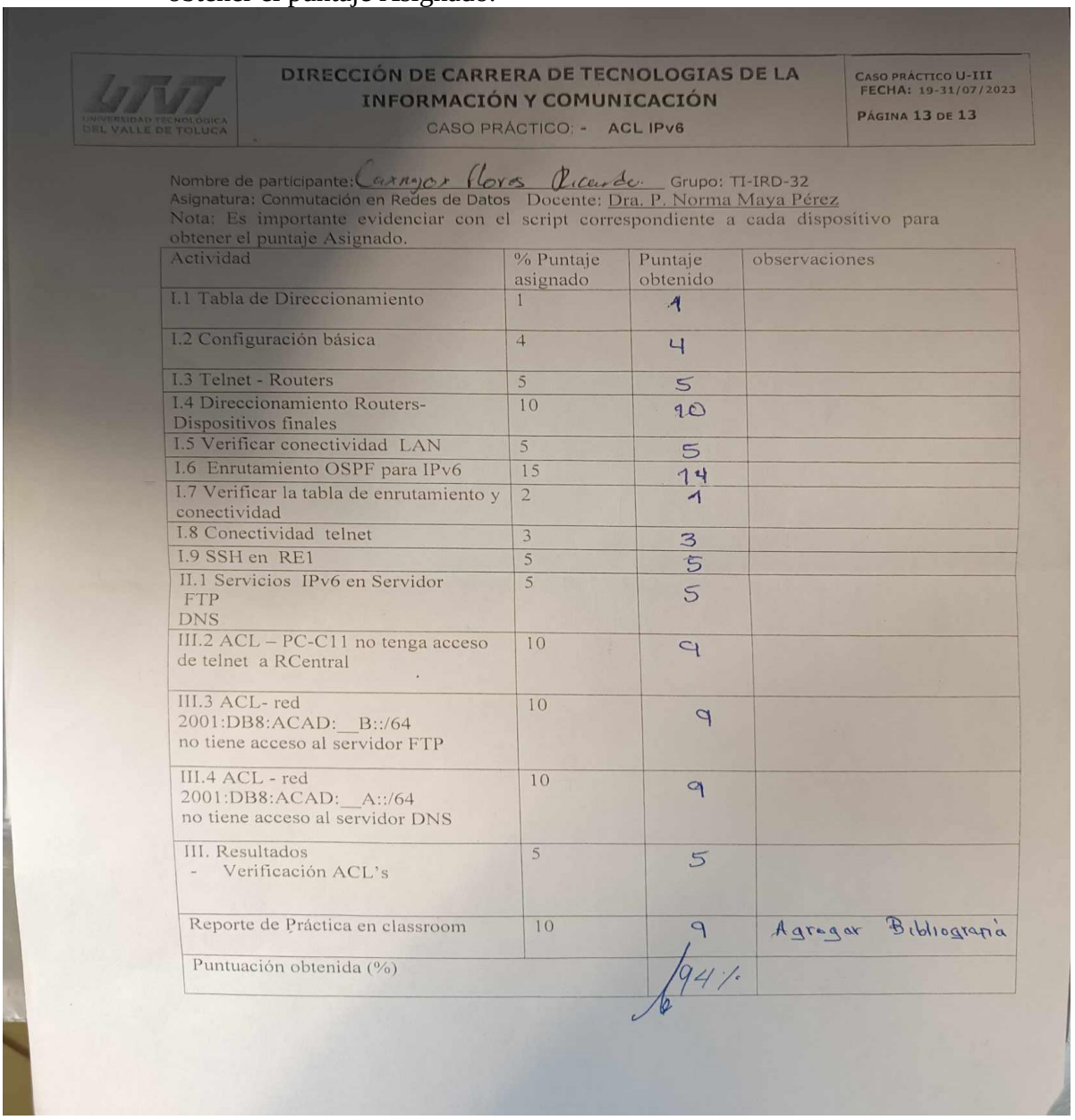
CONCLUSIONES. *(Colocar conclusiones del caso práctico)*

BIBLIOGRAFÍA (Colocar por lo menos 2 fuentes de referencia bibliográfica en formato APA) -

Show Access-lists es solo para mostrar las ACL de ipv4 y el show ipv6 access-list es para Mostrar las ACL de ipv6

En conclusión, las listas de control de acceso (ACL) en IPv6 desempeñan un papel fundamental en la gestión del tráfico y la seguridad en las redes que utilizan el protocolo de Internet versión 6 (IPv6). Al igual que las ACL en IPv4, las ACL en IPv6 permiten a los administradores de red controlar el flujo de paquetes a través de una interfaz de red, lo que les permite permitir o denegar el tráfico según ciertos criterios definidos.

Nombre de participante:_____Grupo: TI-IRD-32
Asignatura: Conmutación en Redes de Datos Docente: Dra. P. Norma Maya Pérez
Nota: Es importante evidenciar con el script correspondiente a cada dispositivo para obtener el puntaje Asignado.



DIRECCIÓN DE CARRERA DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN
CASO PRÁCTICO: - ACL IPv6
CASO PRÁCTICO U-III FECHA: 19-31/07/2023 PÁGINA 13 DE 13

Nombre de participante: Carrazor Flores Ricardo Grupo: TI-IRD-32
Asignatura: Conmutación en Redes de Datos Docente: Dra. P. Norma Maya Pérez
Nota: Es importante evidenciar con el script correspondiente a cada dispositivo para obtener el puntaje Asignado.

Actividad	% Puntaje asignado	Puntaje obtenido	observaciones
I.1 Tabla de Direccionamiento	1	1	
I.2 Configuración básica	4	4	
I.3 Telnet - Routers	5	5	
I.4 Direccionamiento Routers-Dispositivos finales	10	10	
I.5 Verificar conectividad LAN	5	5	
I.6 Enrutamiento OSPF para IPv6	15	14	
I.7 Verificar la tabla de enrutamiento y conectividad	2	1	
I.8 Conectividad telnet	3	3	
I.9 SSH en RE1	5	5	
II.1 Servicios IPv6 en Servidor FTP DNS	5	5	
III.2 ACL – PC-C11 no tenga acceso de telnet a RCentral	10	9	
III.3 ACL- red 2001:DB8:ACAD:__B::/64 no tiene acceso al servidor FTP	10	9	
III.4 ACL - red 2001:DB8:ACAD:__A::/64 no tiene acceso al servidor DNS	10	9	
III. Resultados - Verificación ACL's	5	5	
Reporte de Práctica en classroom	10	9	Agregar Bibliografía
Puntuación obtenida (%)		94%	