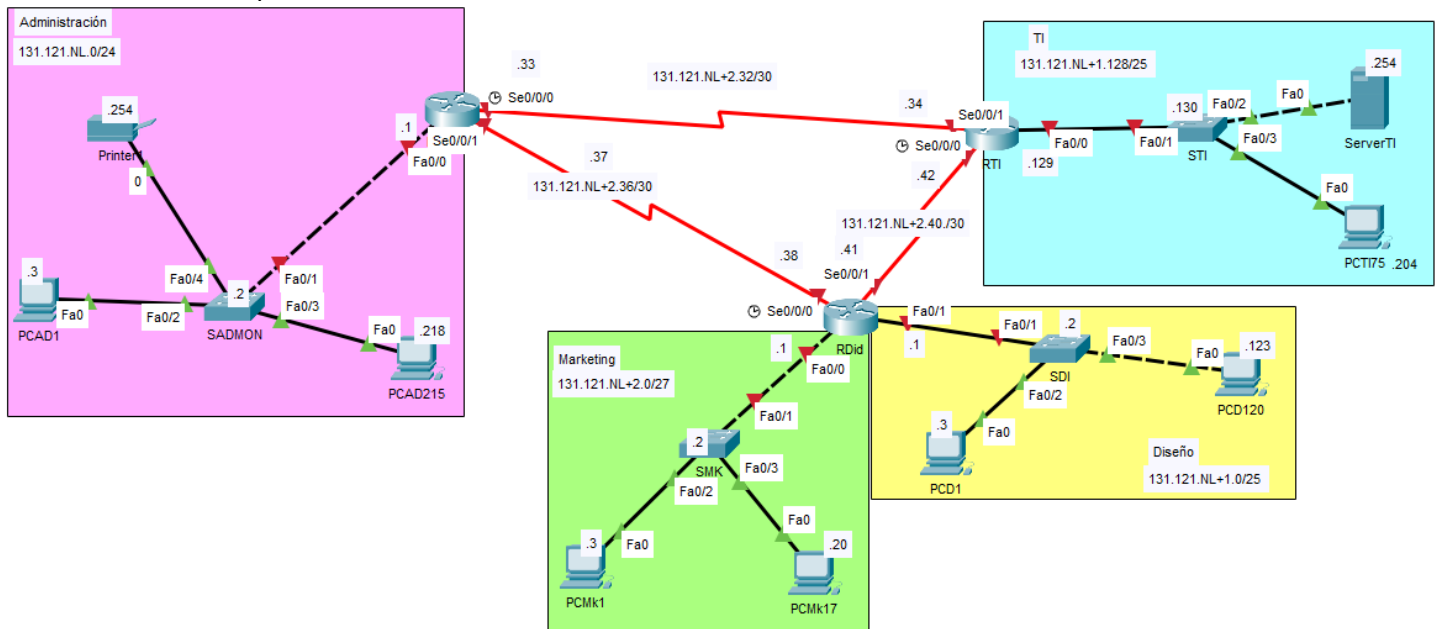


FECHA DE REALIZACIÓN: 12-17/07/2023	GRUPO: IRD-32
FECHA DE REPORTE: 19/07/2023	REVISÓ: DRA. P. NORMA MAYA PÉREZ
ASIGNATURA: CONMUTACIÓN EN REDES DE DATOS	APROBÓ: Comisión de Interconexión de Redes
UNIDAD TEMÁTICA: III Introducción a la Seguridad en Redes (Módulo 3-5 Seguridad de la Red–CCNA3v7)	
TEMAS: - Introducción a la Seguridad y Configuración de listas control de acceso (ACL)	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 “ABC” y direccionamiento IP Address **131.121.____.0 /21**, 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.



Nota: El valor del 3er. Octeto es su No. de lista.

Aspectos básicos/situación:

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

Recursos necesarios:

Software Packet tracer 8.2.0 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 estándar IPv4 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, considerando las primera dirección de cada subred en las interfaces de los routers, la segunda dirección para las VLANs , la última dirección el servidor y printer1 y las restantes para los demás equipos conectados en cada LAN) y basándose en la topología de Paacket tracer.

Dispositivo	Interfaz	Dirección IPv4	Mascara de Subred	Gateway Predeterminado
RAdmon	F0/0	131.121.5 .1	255.255.255.0	N/A
	S0/0/0 DCE	131.121.7 .33	255.255.255.252	N/A
	S0/0/1	131.121.7.37	255.255.255.252	N/A
RTI	F0/0	131.121. 6 .129	255.255.255.128	N/A
	S0/0/0 DCE	131.121. 7 .42	255.255.255.252	N/A
	S0/0/1	131.121.7.34	255.255.255.252	N/A
RDId	F0/0	131.121.7.1	255.255.255.224	N/A
	F0/1	131.121. 6 .1	255.255.255.128	N/A
	S0/0/0 DCE	131.121. 7.38	255.255.255.252	N/A
	S0/0/1	131.121. 7.41	255.255.255.252	N/A
SADMON	Vlan 1	131.121. 5 .2	255.255.255.0	131.121. 5.1
STI	Vlan 1	131.121.6 .130	255.255.255.128	131.121. 6.129
SDI	Vlan 1	131.121. 6.2	255.255.255.128	131.121. 6 .1
SMK	Vlan 1	131.121. 7 .2	255.255.255.224	131.121. 7 .1
PCAD1	NIC	131.121. 5 .3	255.255.255.0	131.121. 5.1
PCAD215	NIC	131.121. 5 .218	255.255.255.0	131.121.5.1
Printer1	NIC	131.121. 5 .254	255.255.255.0	131.121.5.1
PCTI75	NIC	131.121. 6 .204	255.255.255.128	131.121. 6.19
ServerTI	NIC	131.121. 6.254	255.255.255.128	131.121. 6 .129
PCD1	NIC	131.121. 6 .3	255.255.255.128	131.121. 6 .1
PCD120	NIC	131.121. 6 .123	255.255.255.128	131.121. 6 .1
PCMK1	NIC	131.121. 7 .3	255.255.255.224	131.121. 7 .1
PCMK17	NIC	131.121. 7 .20	255.255.255.224	131.121. 7 .1

I.2 Verificar el diseño de la red en packet tracer de acuerdo a la topología especificada y verificar medios de conexión y la conexión de interfaces de forma correcta.

I.3 Deshabilite la búsqueda del DNS y Configurar direccionamiento en cada equipo de la topología.

I.4 Configurar enrutamiento OSPF con id proceso 32 y área su Numero de Lista, deshabilite la actualizaciones de routing no necesarias, determine si la sumarización automática es necesaria o en caso contrario deshabilite y los Router-id son: RAdmon- 1.1.1.1, RDId- 1.1.1.2, RTI - 1.1.1.3

I.5 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.

PARTE II Configuración de listas ACL IPv4 estándar

II.1 La empresa establece que el área de administración y Diseño tienen acceso a la LAN de ServerTI, en tanto que Marketing NO se otorga acceso. (Configure una ACL nombrada AC_ServerTI)

*****RTI

```
ip access-list standard AC_ServerTI
deny 131.121.  .0 0.0.0.31
permit any
exit
int F0/0
ip access-group AC_ServerTI out
```

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ip access-list standard AC_ServerTI
Router(config-std-nacl)#deny 131.121.7.0 0.0.0.31
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#int F0/0
Router(config-if)#ip access-group AC_ServerTI out
Router(config-if)#
```

II.2 La PCAD1 tienen restringido el acceso a la LAN del área de Diseño. (ACL numerada con su NL+1)

*****Rdid

```
enable
config t
Access-list 51 remark Deny PCAD1 to LAN Diseño
access-list 51 deny host 131.121. .3
access-list 51 permit any
int F0/1
ip access-group 51 out
exit
```

```

RDid>enable
RDid#config t
Enter configuration commands, one per line. End with CNTL/Z.
RDid(config)#Access-list 6 remark Deny PCAD1 to LAN Diseo
RDid(config)#access-list 6 deny host 131.121.5.3
RDid(config)#access-list 6 permit any
RDid(config)#int F0/1
RDid(config-if)#ip access-group 6 out
RDid(config-if)#exit

```

II.3 Verificación de ACL's

PARTE III Configuración de listas ACL IPv4 extendidas

III.1 Configurar los servicios en ServerTI:

- FTP (User: grupo32, contraseña:class32) con permisos de leer, escribir y listar.
- DNS (dominio: grupoird32.pka.pt)

	Username	Password	Permission
1	grupo32	class32	RWL

No.	Name	Type	Detail
0	grupoird32.pka.pt	A Record	131.121.6.254

III.2 Habilitar las políticas de acceso ACL extendidas siguientes.

- La PCD1 no puede tener acceso al servicio FTP, todas las demás SI. (ACL numerada 142)

```

RDid(config)#
enable
conf t
access-list 142 deny tcp host 131.121. .3 host 131.121. .254 eq ftp
access-list 142 permit ip any any
int f0/1
ip access-group 142 in
end

```

```
C:\>  
C:\>ftp 131.121.6.254  
Trying to connect...131.121.6.254  
  
%Error opening ftp://131.121.6.254/ (Timed out)  
  
(Disconnecting from ftp server)
```

- b) El área de diseño no tiene acceso al DNS, todas las demás áreas si tienen el acceso. (ACL nombrada ACCESS_DNS)

RDid(config-ext-nacl)#

Enable

Conf t

ip access-list extended ACCESS_DNS

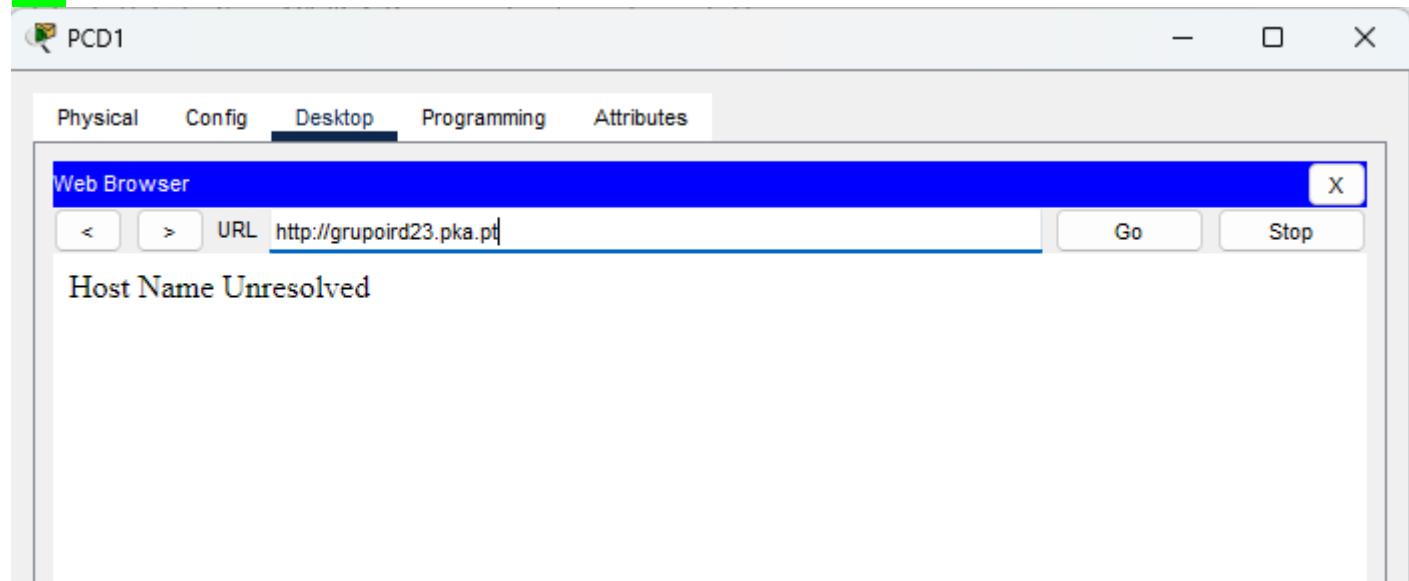
deny udp 131.121. .0 0.0.0.127 any eq 53

permit ip any any

interface F0/1

ip access-group ACCESS_DNS in

end







- c) PCMK17 no tiene acceso a la impresora, pero los demás equipos si tienen acceso total a LAN de Printer1 (ACL nombrada BLOCK_Printer)

RDid(config)#

Enable

```
Conf t
ip access-list extended BLOCK_Printer
deny ip host 131.121.7.20 host 131.121.5.254
permit ip any any
int F0/0
ip access-group BLOCK_Printer in
end
```

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Failed	PCMK17	Printer1	ICMP		0.000	N	0	(edit)
	Successful	PCMK1	Printer1	ICMP		0.000	N	1	(edit)

Scenario (Ctrl+Shift+N)

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

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

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

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

show access-list

```
RDid#show access-list
Standard IP access list 6
 10 deny host 131.121.5.3
 20 permit any (69 match(es))
Extended IP access list ACCESS_DNS
 10 deny udp 131.121.6.0 0.0.0.127 any eq domain (52 match(es))
 20 permit ip any any (73 match(es))
Extended IP access list BLOCK_Printer
 10 deny ip host 131.121.7.20 host 131.121.5.254 (12 match(es))
 20 permit ip any any (52 match(es))
Extended IP access list 142
 10 deny tcp host 131.121.6.3 host 131.121.6.254 eq ftp (29 match(es))
 20 permit ip any any (3 match(es))
RDid#
```

CONCLUSIONES. (Colocar conclusiones del caso práctico)

La práctica sobre ACL demostró la importancia y la eficacia de las listas de control de acceso para filtrar y controlar el tráfico de red. Mediante la implementación de reglas específicas, las ACL permiten permitir o denegar el acceso a recursos y servicios en función de criterios predefinidos.

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

Mifsud, E. (n.d.). *MONOGRÁFICO: Listas de control de acceso (ACL) - Utilización de ACLs en routers* /

Observatorio Tecnológico.

<http://recursostic.educacion.es/observatorio/web/es/component/content/article/1065-listas-de-control-de-acceso-acl?start=3>

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	5		
I.2 Diseño de Topología	1		
I.3 Configurar direccionamiento	10		
I.4 Enrutamiento	15		
II.1 ACL estándar nombrada II.2 ACL estándar numerada	20		
III.2 Habilitación de Servicios ServerTI	4		
III.2 ACL extendidas a) acceso al servicio FTP b) acceso al servicio DNS c) No acceso PMk17 a Printer	25		
Resultados IV.2 Verificación ACL's	10		
Reporte de Práctica en classroom	10		
Puntuación obtenida (%)			