PRUEBA DE HABILIDADES CCNA 16-4-2019

CARLOS FABIÁN MONTOYA OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA INGENIERÍA DE SISTEMAS MEDELLÍN 2019

# EVALUACIÓN-PRUEBA DE HABILIDADES CCNA 16-4-2019

# DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

CARLOS FABIÁN MONTOYA OROZCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA INGENIERÍA DE SISTEMAS MEDELLÍN 2019

# TABLA DE CONTENIDO

RESUMEN	6
ABSTRACT	7
INTRODUCCIÓN	8
OBJETIVOS	9
DESARROLLO DE LOS DOS ESCENARIOS	10
ESCENARIO 1	10
ESCENARIO 2	
CONCLUSIONES	92
BIBLIOGRAFIAS	93

# TABLA DE ILUSTRACIONES

Ilustración 1	10
Ilustración 2	14
Ilustración 3	15
Ilustración 4	15
Ilustración 5	16
Ilustración 6	16
Ilustración 7	17
Ilustración 8	17
Ilustración 9	
Ilustración 10	18
Ilustración 11	19
Ilustración 12	19
Ilustración 13	20
Ilustración 14	20
Ilustración 15	21
Ilustración 16	21
Ilustración 17	22
Ilustración 18	23
Ilustración 19	24
Ilustración 20	25
Ilustración 21	25
Ilustración 22	27
Ilustración 23	27
Ilustración 24	28
Ilustración 25	28
Ilustración 26	29
Ilustración 27	30
Ilustración 28	31
Ilustración 29	32
Ilustración 30	32
Ilustración 31	33
Ilustración 32	34
Ilustración 33	34
Ilustración 34	35
Ilustración 35	35
Ilustración 36	36
Ilustración 37	36
Ilustración 38	37
Ilustración 39	37
Ilustración 40	37
Ilustración 41	39

Ilustración 42	
Ilustración 43	59
Ilustración 44	60
Ilustración 45	69
Ilustración 46	70
Ilustración 47	73
Ilustración 48	76
Ilustración 49	76
Ilustración 50	77
Ilustración 51	77
Ilustración 52	80
Ilustración 53	82
Ilustración 54	83
Ilustración 55	84
Ilustración 56	84
Ilustración 57	85
Ilustración 58	86
Ilustración 59	87
Ilustración 60	88
Ilustración 61	89
Ilustración 62	89
Ilustración 63	90
Ilustración 64	91
Ilustración 65	91

## RESUMEN

La prueba de habilidades en el siguiente trabajo busca identificar las competencias que se generaron después de haber cursado los 2 módulos de CCNA, en los cuales se integraron conceptos básicos de las redes, direccionamiento ip, seguridad, topología física, tipología lógica, implementación de seguridad de la red administración de dispositivos y gestión de recursos para la implementación de redes CISCO, es importante además destacar que cada uno de los parámetros que se ejecutaron buscaban solucionar un problema en particular, teniendo en cuenta cada uno de los recursos anteriores se gestionó de manera directa las aplicaciones en el escenario1 y escenario2.

La integración de conocimientos adquiridos y aplicaciones a destrezas alcanzadas en el curso aplicando asignación de redes, configuración de router mediante comandos básicos y avanzados que permitían corroborar el funcionamiento de cada uno de los escenarios, cada uno e los niveles de comprensión que se usó para su desarrollo en los diferentes escenarios permitían relacionar los diversos aspectos de networking en la aplicación del mismo. Con recursos de subneteo al inicio de la actividad en parámetros de red, tipología física y lógica, aplicación de comandos entre otros como asignación de interfaces a router, conexiones en switch y demás dispositivos desde la consola de configuración para cada una de las terminales actuales. En el presente trabajo se busca mostrar al lector la secuencia de acciones que se realizaron en la red y la búsqueda de la solución a los problemas planteados en la evaluación-prueba de habilidades prácticas CCNA.

Se presenta el paso a paso con comandos y pantallazos que permiten evidenciar la gestión y configuración de cada uno de los procesos en los escenarios 1 y 2.

# ABSTRACT

The skills test in the following work seeks to identify the competencies that were generated after completing the 2 CCNA modules, in which the basic concepts of networks, IP addressing, security, physical topology, logical typology, resource implementation and management of network security devices management for the implementation of CISCO networks, it is also important to keep in mind that each of the parameters that were executed sought to solve a particular problem, taking into account each of the previous resources Directly the applications in scenario1 and the scenario 2.

The integration of the knowledge and applications acquired to the skills achieved in the course through the application of the network assignment, the configuration of the router through basic and advanced commands that allow corroborating the operation of each of the scenarios, each and the levels of understanding that were used for its development in the course. different aspects allowed to relate the different aspects of the networks in their application. With subnet resources at the beginning of the activity in network parameters, physical and logical typology, command application, among others, such as assigning interfaces to a router, changing connections and other devices from the configuration console for each of the current terminals. This document seeks to show the reader the sequence of actions taken on the network and the search for the solution to the problems posed in the evaluation of practical skills of CCNA.

It is presented step by step with commands and screens that show the management and configuration of each of the processes in scenarios 1 and 2

# INTRODUCCIÓN

En el presente trabajo se busca integrar los conocimientos adquiridos durante los módulos de CISCO CCNA en colaboración con la UNAD, las cuales buscan identificar las competencias alcanzadas por el alumnos en el curso realizado, se presentan 2 escenarios con soluciones implementado herramientas ofrecidas durante el curso, cada uno de los escenarios presentan el levantamiento de la red de manera física y lógica, cada uno de los escenarios permiten reconocer y gestionar los comandos aprendidos para la solución sugerida en la prueba de habilidades.

Cada una de las soluciones aplicadas se detallan con sus códigos de terminal y cada uno las tomas de pantalla generalizada permitiendo identificar el entorno y la aplicación de los comandos como lo ping, telnet, show ip route, entre otros.

# OBJETIVOS

Objetivos generales:

- ✓ Aplicar los conocimientos adquiridos en CCNA.
- ✓ Configurar los escenarios establecidos por comandos en redes LAN/WAN

Objetivos específicos:

- ✓ Realizar configuración de topología de red física y lógica
- ✓ Implementar gestión de redes mediante consola.
- ✓ Direccionar los dispositivos de subredes y VLAN.
- ✓ Aplicar seguridad a dispositivos de la red.
- ✓ Administrar conexiones en dispositivos de la red
- ✓ Generar reportes desde los servidores de la red.
- ✓ Administrar la información que ingresa a la red por dispositivos asignados.
- ✓ Aplicar configuración avanzada en dispositivos NAT y gestores de red
- ✓ Diseñar soluciones prácticas a problemas frecuentes en la red.



#### llustración 1

## Parte 1: Asignación de direcciones IP:

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa.

Necesitamos 3 bit para 8 partes

27	2 <sup>6</sup>	2 <sup>5</sup>	24	2 <sup>3</sup>	2 <sup>2</sup>	2 <sup>1</sup>	2 <sup>0</sup>
128	64	32	0	0	0	0	0
1	1	1					

128+64+32= 224

246/8= 32

192.168.1.0 - 192.168.1.31 BOGOTA

192.168.1.32 - 192.168.1.63 MEDELLIN

192.168.1.64 - 192.168.1.95 CALI

192.168.1.96 - 192.168.1.127 S

192.168.1.128 - 192.168.1.159 S

192.168.1.160 -- 192.168.1.191 SUCURSAL1

192.168.1.192 --- 192.168.1.223 SUCURSAL2

192.168.1.224 - 192.168.1.255 SUCURSAL3

Mascara de subred 255.255.255.224

b. Asignar una dirección IP a la red.

MEDELLIN

Router

RED 192.168.1.32/27 PC0 lp: 192.168.1.34 Mascara: 255.255.255.224 Puerta enlace: 192.168.1.33 PC1 lp: 192.168.1.35 Mascara: 255.255.255.224 Puerta enlace: 192.168.1.33

BOGOTÁ RED 192.168.1.0/27 WS1 lp: 192.168.1.3 Mascara: 255.255.255.224 Puerta enlace: 192.168.1.1 SERVIDOR lp: 192.168.1.2 Mascara: 255.255.255.224 Puerta enlace: 192.168.1.1

CALI

RED 192.168.1.64/27

PC2

lp: 192.168.1.67

Mascara: 255.255.255.224

Puerta enlace: 192.168.1.65

PC3

lp: 192.168.1.66

Mascara: 255.255.255.224

Puerta enlace: 192.168.1.65

Parte 2: Configuración Básica.

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de lp en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de lp en interfaz Serial 0/1		192.168.1.130	
Dirección de lp en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

### Configuración Ip router

### MEDELLIN

Router>enable Router#conf terminal Router(config)#interface serial 0/0 Router(config-if)#ip address 192.168.1.99 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#exit Router(config)#interface fastEthernet 0/0 Router(config-if)#ip address 192.168.1.33 255.255.255.224 Router(config-if)#ip address 192.168.1.33 255.255.255.224 Router(config-if)#ip address 192.168.1.33 255.255.255.224

## BOGOTÁ

Router>enable Router#conf terminal Router(config)#interface serial 0/0 Router(config-if)#ip address 192.168.1.98 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#exit Router(config)#interface serial 0/0 Router(config-if)#ip address 192.168.1.130 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#no shutdown Router(config)#interface fastEthernet 0/0 Router(config-if)#ip address 192.168.1.1 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#ip address 192.168.1.1 255.255.255.224 Router(config-if)#ip address 192.168.1.1 255.255.255.224

CALI

Router>enable Router#conf terminal Router(config)#interface serial 0/0 Router(config-if)#ip address 192.168.1.131 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#exit Router(config)#interface fastEthernet 0/0 Router(config-if)#ip address 192.168.1.65 255.255.255.224 Router(config-if)#no shutdown Router(config-if)#exit

c. Verificar el balanceo de carga que presentan los routers.

	<pre>\$LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state up</pre>
PC0 192.1	<pre>\$LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to u</pre>
PC1	Router≻en Router≱show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
	Gateway of last resort is not set
<	<pre>192.168.1.0/27 is subnetted, 5 subnets R 192.168.1.0 [120/1] via 192.168.1.98, 00:00:16, Serial0/0/0 C 192.168.1.32 is directly connected, FastEthernet0/0 R 192.168.1.64 [120/2] via 192.168.1.98, 00:00:16, Serial0/0/0 C 192.168.1.96 is directly connected, Serial0/0/0</pre>
Time: 00:29:12	Router#
8-1	Сору
Connection	
📰 🖉 🧠 🐺	Copper Straight-Throug
6 C	へ <i>慌</i> 恤 小 厚 <sup>4:14 p. m. 8/12/2019</sup>

llustración 2

el balanceo es CALI>enable

Password: CALI#show ip eigrp topology

Para llegar desde una pc hasta otra siempre abran una sola ruta conectada a los seriales disponibles en este caso por los 3 router existentes en la red

d. Realizar un diagnóstico de vecinos uSando el comando cdp.

Trabaja a nivel de capa2 osea trama ahora vamos a simular..

PC0 192,168,1.32/27 Bwite Strate February Februa	192.168.1.0/27 0007A 192.168.1.128/27 192.168.1.14/27 CAL1 Switch2 PC2 PC3		<ul> <li>50.18</li> </ul>	4 14 14 MEDELLI 14 MEDELLI 14 Switch1 14 Switch1 14 Switch1 11 Constant D	Switch0 Switch0 N Switch0 BOGOT PC5 Servido	) CDP ) CDP ) CDP ) CDP (A CDP (CDP)		Capta 5	v rred to: * 0.184 s	× ~~~~~~~
PC1			Play Controls	Back	A	uto Capture / Pla	y	Capture / Forward		₽ ₽
			Event List Filte CDP	rs - Visible Events Edit Filters			Show	All/None		
									_	-
<		>							0	
Time: 00:03:00:509 Power Cycle Devices PLAY C Routers Routers	OMTROLE: Back Auto Capture / Play Capture / Forwi Capture / Torwing Capture / Play Capture / Forwing Capture / Forwing Capture / Play Capture / Forwing Cap	ard Scenario 0 .w Delet e PDU List Wind	Fire	Last Status Successful Successful Successful	Source CALI BOGOTA MEDEL	Destination BOGOTA MEDELLIN CALI	Type Co ICMP ICMP ICMP	Event List lor Time(sec) 0.000 0.000 0.000	Periodic N N N	Num ^ 0 1 2 5
📕 🖉 🗖 🧧 📕	i 🧿 🚸 🚱 💷 🖊 🛷 🦉	0	2					^ <i>(</i> ≋ 10 ⊄	), 🗐 🖁	:17 p. m. /12/2019
PDU Information at Device: BOGOTA OSI Model Inbound PDU Details At Device: BOGOTA Source: MEDELLIN Destination: Broadcast In Layer5 Layer5 Layer4 Layer3 Layer3	Out Layers Layer7 Layer5 Layer5 Layer4 Layer3									
Layer 2: HDLC Frame HDLC CDP Frame	Layer2									
Layer 1: Port Serial0/0/0	Layer1									
1. Serial0/0/0 receives the frame.										
Challenge Me	<< Previous Layer Next Layer >>									
2911 Generic Generic New Toggle P	Delete Successful BO DU List Window									
😘 🗐 🍋 🛷 🦉 Ilustración 4	() () ()									

Se ha recibido trama por parte de serial, estan trabajando con el proptocolo CDP.

o Junio2-2018(D)\1.UNAD\2019-II\DiplomadoCISCO\TareaGradoultima\escenario1Bn.pkt



#### Ilustración 5

Ahora si vamos a capa 2 nos da la informacipón de lo que hace una trama, se ha podio recibir la trama porque coincide la trama, acepta la trama y desencapsula la PDU, que hay en la trama, dentro de la trama hay la informaciónd el CDP, proceso del ruter de cisco, lo recibe y lo que hace es reinicia el temporizador de espera. Se envia mediante broadcast, terma--...

		Simulatio
	PDU Informati	ion at Device: Switch2
PC5	OSI Model	Outbound PDU Details
	At Device: Source: Sw Destination	Switch2 itch2 : Broadcast
	In Layers	Out Layers
	Layer7	Layer7
	Layer6	Layer6
192.168.1.96/27	Layer5	Layer5
PC0 192 168 1 32/27	Layer4	Layer4
	Laver3	Laver3
Switch0 MEDELLIN	Layer2	Layer 2: IEEE 802.3 Header 000A.414C.9203 >> 0100.0CCC.CCCC LLC SNAP COP Frame
	Laver1	Laver 1: Port(s): FastEthernet0/3
	3. The Swit	ch unicasts the frame out to the access port.
ime: 00:03:00.510 Power Cycle Devices PL	A) Challenge I	Me << Previous Layer Next Layer >>
<sup>™</sup> <b>■ ■</b> ≯ 🕅 🕅 🗊	2621XM 2811	201 2011 Generic Generic Naur Palata

Al llegar ala computadora no al recibe porque no hay un servicio como lo es ua PC ya que CDP es un protocolo propietario de cisco...

R		_			<ul> <li>Simulation I</li> </ul>	Panel
			PDU Informati	on at Device: Servidor		
	PC5	Servic	OSI Model	Inbound PDU Details		
		Switch1 192.168.1.0/27	At Device: Source: Sw Destination	Servidor itch1 : Broadcast		
			In Layers		Out Layers	
					Layer7	
	100 100 1 00 00	BOGOTA	Layer6		Layer6	
	192.100.1.90/2/		Layer5		Layer5	
PC0 192.168.1.32/27		192.168.1.128/27	Layer4		Layer4	
			Layer3		Layer3	
Switch0 MEDE	LLIN	С	Layer 2: IE 000C.CFD9 LLC SNAP (	EE 802.3 Header .8903 >> 0100.0CCC.CC CDP Frame	Layer2	
			Laver 1: Po	rt FastEthernet0	Laver1	
PC1						
			1. FastEther	net0 receives the frame		
Time: 00:04:00.512 Power Cy	cle Devices PLAY	CONTROLS: Back				
8 - 1 1 10 5 1841	1941 2620XM	2621XM 2811 2901	Challenge I	1e	<< Previous Layer	Next Layer >>
Roders					non Donto	
ustración 7						

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.



Ilustración 8



Ilustración 9



Ilustración 10





Ilustración 12

💐 Servidor							_	
Physical	Config	Services	Desktop	Custo	m Interfac	е		
	1-1-1			s <del>b</del>	-	-		
Com	Command Prompt							
SERVER	>ping 192.	168.1.67						
Pingir	g 192.168.	1.67 with 3	32 bytes of	data:				
Reply Reply Reply Reply	from 192.1 from 192.1 from 192.1 from 192.1	.68.1.67: by .68.1.67: by .68.1.67: by .68.1.67: by	ytes=32 tim ytes=32 tim ytes=32 tim ytes=32 tim	e=2ms TT e=1ms TT e=2ms TT e=1ms TT	L=126 L=126 L=126 L=126			
Ping s Pa Approx Mi	<pre>Ping statistics for 192.168.1.67: Packets: Sent = 4, Aeceived = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimm = lms, Maximum = 2ms, Average = lms</pre>							
SERVER	>ping 192.	168.1.32						
Pingir	g 192.168.	1.32 with 3	32 bytes of	data:				
Reply Reply Reply Reply	from 192.1 from 192.1 from 192.1 from 192.1	.68.1.99: b .68.1.99: b .68.1.99: b .68.1.99: b	ytes=32 tim ytes=32 tim ytes=32 tim ytes=32 tim	e=1ms TT e=2ms TT e=1ms TT e=1ms TT	L=254 L=254 L=254 L=254			
<pre>Ping statistics for 192.168.1.32: Packets: Sent = 4, Paccived = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = lns, Maximum = Zns, Average = ims</pre>								
SERVER	>							
<								
Last Chatur	Course	Destination	Trees	Calaa T	(ma(ma) D		Num A	
Successful	PC0	PC3	ICMP		0.000	N	19	
Successful	PC0	PC2	ICMP		0.000	N	20	
Successful	Servidor	PC1	ICMP		0.000	N	21	
							>	
				^	<i>(ii</i> 🖬 🕬	¢	:07 p. m. 3/12/2019	

Ilustración 13

💐 Servidor								-
Physical	Config	Services	Desktop	Cust	om Interf	асе		
				sla-		-	-	
Com	nand Pi	rompt						
SERVER	>ping 192.	168.1.67						
Pingin	g 192.168.	1.67 with 3	2 bytes of	data:				
Reply Reply Reply Reply	Reply from 192.168.1.67: bytes=32 time=2ms TTL=126 Reply from 192.168.1.67: bytes=32 time=1ms TTL=126 Reply from 192.168.1.67: bytes=32 time=2ms TTL=126 Reply from 192.168.1.67: bytes=32 time=1ms TTL=126							
Ping s Pa Approx Mi	tatistics ckets: Sen imate roun nimum = 1m	for 192.168 t = 4, Rece d trip time s, Maximum	2.1.67: eived = 4, es in milli = 2ms, Ave	Lost = -secone rage =	0 (0% los is: 1ms	s),		
SERVER	>ping 192.	168.1.32						
Pingin	g 192.168.	1.32 with 3	2 bytes of	data:				
Reply Reply Reply Reply	from 192.1 from 192.1 from 192.1 from 192.1 from 192.1	68.1.99: by 68.1.99: by 68.1.99: by 68.1.99: by	vtes=32 tim vtes=32 tim vtes=32 tim vtes=32 tim	ne=1ms ne=2ms ne=1ms ne=1ms	TTL=254 TTL=254 TTL=254 TTL=254			
Ping s Pa Approx Mi	<pre>Ping statistics for 192.168.1.32: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms</pre>							
<b>BERVER</b>								
<								_
Last Status Successful Successful Successful	Source PC0 PC0 Servidor	Destination PC3 PC2 PC1	Type ICMP ICMP ICMP	Color	Time(sec) 0.000 0.000 0.000	Periodic N N N	Num 19 20 21	~
				~		»	> :07 p. m /12/201	ı. 9

llustración 14

Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.





Ilustración 15

### MEDELLIN.

### Router#conf t

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router eigrp 200 Router(config-router)#network 192.168.1.32 0.0.0.31 Router(config-router)#network 192.168.1.99 0.0.0.31 Router(config-router)#no auto-summary



Ilustración 16

Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router eigrp 200 Router(config-router)#network 192.168.1.0 0.0.0.31 Router(config-router)#network 192.168.1.98 0.0.0.31 Router(config-router)# %DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) is up:

new	ad	jacency

n Bogota	-	×
Physical Config CLI		
IOS Command Line Interface		
		^
Press RETURN to get started.		
Router>en		
Router#conf t		
Safer configuration commands, one per line. and with CNIL/2.		
Router(config=router)inetwork 192,168,1.0,0.0.0.31		
Router (config-router) #network 192.168.1.130 0.0.0.31		
Router(config-router) #no auto-summary		
Router(config-router)#		
<pre>\$DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) re</pre>	sync:	
summary configured		~
1		· ·

Ilustración 17

Router>en

Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router eigrp 200 Router(config-router)#network 192.168.1.0 0.0.0.31 Router(config-router)#network 192.168.1.130 0.0.0.31 Router(config-router)#no auto-summary Router(config-router)#no auto-summary Router(config-router)# %DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) resync: summary configured

					_
💐 CALI			_		×
Physical Config	CLI				
		IOS Command Line Interface			
1 DUW-speed Seriel 191K bytes of NVRA 63488K bytes of AT Cisco IOS Software RELEASE SOFTWARE ( Technical Support: Copyright (c) 1986 Compiled Wed 18-Ju	M. A Comp (1841 fc2) http: -2007 (1-07 0	async) network interface(s) actFlash (Read/Write) Software (C1841-ADVIPSERVICESK9-M), Version 12. //www.cisco.com/techsupport by Cisco Systems, Inc. 4:52 by pt_team	.4(15)	т1,	~
Press RETURN to ge	t star	ted!			
%LINEPROTO-5-UPDOW up	N: Lin	e protocol on Interface FastEthernet0/0, changed	i stat	e to	
<pre>%LINK-5-CHANGED: I</pre>	nterfa	ce Serial0/0/0, changed state to up			
%LINEPROTO-5-UPDOW	N: Lin	e protocol on Interface Serial0/0/0, changed sta	ite to	up	
Router>en Router‡conf t Enter configuratic Router(config-rout Router(config-rout Router(config-rout BOUAL-5-NBRCHANGE: adjacency	n comm ter ei er)‡ne er)‡ IP-EI	ands, one per line. End with CNTL/Z. grp 200 twork 192.168.1.64 0.0.0.31 twork 192.168.1.131 0.0.0.31 GRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is	s up:	new	F
		Сору		Paste	

llustración 18

Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#router eigrp 200 Router(config-router)#network 192.168.1.64 0.0.0.31 Router(config-router)#network 192.168.1.131 0.0.0.31 Router(config-router)# %DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency

b. Verificar si existe vecindad con los routers configurados con EIGRP.

Existe vecindad:

MEDELLIN Router> Router>en Router#show ip eigrp neighbors IP-EIGRP neighbors for process 200 H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num 0 192.168.1.98 Se0/0/0 12 00:32:39 40 1000 0 20



Ilustración 19

BOGOTÁ Router>en Router#show ip eigrp neighbors IP-EIGRP neighbors for process 200 H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num 0 192.168.1.99 Se0/0/0 10 00:33:41 40 1000 0 15 1 192.168.1.131 Se0/0/1 12 00:10:59 40 1000 0 7

grado - Word						?	0	8
ISAR VISTA							Inicia	rsesión
						A Rucca		
BOGOTA					-		×	
hysical Config	CLI							
	IOS C	ommand Line	Inter	face				
							^	
Press RETURN to ge	t started.							
Router>en								
Router#show ip eig IP-EIGRP neighbors	for process 20	D						
H Address	Interface	Hold Uptime	SRTT	RTO Q	Seq			
1 192 168 1 99	Se0/0/0	(sec) 10 00-33-41	(ms) 40	1000 0	t Num 15			
1 192.168.1.131	Se0/0/1	12 00:10:59	40	1000 0	7			
outert								
Router#							~	
					Conv	Da	cto	
					Copy		000	
eighbor 192.168.1.13	0 (Serial0/0/0) is ι	ip: new						
			- 1	88			-11	- + 909
				90				0.17

Ilustración 20

CALI Router# Router>EN Router#show ip eigrp neighbors IP-EIGRP neighbors for process 200 H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms) Cnt Num 0 192.168.1.130 Se0/0/0 10 00:13:04 40 1000 0 21

0 132.168.1.130 Se0/0/0 10 00:13:04 40 1000 0 21 Router# Copy		Seq	Q	RTO	SRTT	Uptime	200 Hold	rp neighbors for process Interface	‡show ip eig RP neighbors dress	Route [P-E] H }
Copy		Num 21	Cnt 0	1000	(ms) 40	00:13:04	(sec 10	Se0/0/0	2.168.1.130	
Сору			_						*	loute
	Paste	Сору								
001 mm mm .						_				
				R		B				

Ilustración 21

%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is up: new adjacency

%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.99 (Serial0/0/0) resync: summary configured

%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98 (Serial0/0/0) is up: new adjacency

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

Se encuentra en la dirección de capa nivel 3.

Router>en

Router#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area \* - candidate default, U - per-user static route, o - ODR P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets C 192.168.1.0 is directly connected, FastEthernet0/0 D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:29:20, Serial0/0/0 D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:25:38, Serial0/0/1 C 192.168.1.96 is directly connected, Serial0/0/0 C 192.168.1.128 is directly connected, Serial0/0/1

192.168.1.0/27 is subnetted, 5 subnets C 192.168.1.0 is directly connected, FastEthernet0/0 D 192.168.1.32 [90/2172416] via 192.168.1.99, 00:29:20, Serial0/0/0 D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:25:38, Serial0/0/1 C 192.168.1.96 is directly connected, Serial0/0/0 C 192.168.1.128 is directly connected, Serial0/0/1



d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.



Ilustración 23

Como se mostró anteriormente si se tiene acceso a la red de la interfaz, se tendrá acceso a cada uno de los host.



Ilustración 24

Se realiza ping al servidor desde CALI



llustración 25

Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

A. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.



Ilustración 26

MEDELLIN-BOGOTÁ

Router>telnet 192.168.1.98 Trying 192.168.1.98 ...Open

[Connection to 192.168.1.98 closed by foreign host] Router>

Router>telnet 192.168.1.1 Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]

**MEDELLIN-CALI** 

Router>telnet 192.168.1.131 Trying 192.168.1.131 ...Open

[Connection to 192.168.1.131 closed by foreign host] Router>

## **BOGOTÁ-MEDELLIN**

Router>telnet 192.168.1.99 Trying 192.168.1.99 ...Open

[Connection to 192.168.1.99 closed by foreign host] Router>

**BOGOTÁ-CALI** 

Router>telnet 192.168.1.131 Trying 192.168.1.131 ...Open

[Connection to 192.168.1.131 closed by foreign host] Router>

Router>telnet 192.168.1.1 Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]

Router>telnet 192.168.1.1 Trying 192.168.1.1 ...Open

[Connection to 192.168.1.1 closed by foreign host]



Ilustración 27

B. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ip access-list extended permisos Router(config-ext-nacl)#permit icmp host 192.168.1.2 any echo Router(config-ext-nacl)#exit Router(config)#interface range fastEthernet 0/0 Router(config-if-range)#ip access-group permisos in Router(config-if-range)#exit Router(config)# Router(config)#



Ilustración 28



c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

MEDELLIN

Router>EN Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#access-list 3 deny 192.168.1.99 0.0.0.31 Router(config)#interface fastEthernet 0/0 Router(config-if)#ip access-group 3 out Router(config-if)#



Ilustración 31

#### CALI

Router>en Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#access-list 1 deny 192.168.1.99 0.0.0.31 Router(config)#access-list 2 deny 192.168.1.131 0.0.0.31 Router(config)#interface fastEthernet 0/0 Router(config-if)#ip access-group 2 out Router(config-if)#

```
SERVER>ping 192.168.1.34
Pinging 192.168.1.34 with 32 bytes of data:
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
SERVER>
```

Ilustración 32

Desde el servidor se tiene acceso a la red de MEDELLIN.... Y a cada uno de los host.

CALI



Ilustración 33



Ilustración 34

#### 💐 PC1



Ilustración 35



Ilustración 36



Ilustración 37

Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa. Fueron exitosas las listas de acceso

b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.
#### TELNET

Router#TELNET 192.168.1.131 Trying 192.168.1.131 ...Open [Connection to 192.168.1.131 closed by foreign host] Router# Router#



Copy

#### Ilustración 38







Ilustración 40

	ORIGEN	DESTINO	RESULTADO		
	Router MEDELLIN	Router CALI	Bien		
	WS_1	Router BOGOTA	Bien		
IELINEI	Servidor	Router CALI	Bien		
	Servidor	Router MEDELLIN	Bien		
	LAN del Router MEDELLIN	Router CALI	Bien		
	LAN del Router CALI	Router CALI	Bien		
TELNET	LAN del Router MEDELLIN	Router MEDELLIN	Bien		
	LAN del Router CALI	Router MEDELLIN	Bien		
	LAN del Router CALI	WS_1	Bien		
PING	LAN del Router MEDELLIN	WS_1	Bien		
	LAN del Router MEDELLIN	LAN del Router CALI	Bien		
	LAN del Router CALI	Servidor	Bien		
PING	LAN del Router MEDELLIN	Servidor	Bien		
	Servidor	LAN del Router MEDELLIN	Bien		
	Servidor	LAN del Router CALI	Bien		
	Router CALI	LAN del Router MEDELLIN	Bien		
	Router MEDELLIN	LAN del Router CALI	Bien		

# **ESCENARIO 2**

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.



Ilustración 41



Ilustración 42

- 1. Todos los routers deberán tener los siguiente:
  - Configuración básica.

PASSWORD: cisco para todos los dispositivos.

Utunja ===Utunja Ubucaramanga==Ubucaramanga Ucundinamarca=Ucundinamarca Sburaramanga==Class Stunja &Scundinamarca==cisco

# ROUTER TUNJA

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Rtunja

Rtunja(config)#Login block-for 220 attempts 3 within 110

Rtunja(config)#enable secret cisco

Rtunja(config)#aaa new-model

Rtunja(config)#aaa authentication login INTERNO group radius local enable

Rtunja(config)#username TUNJA privilege 7 password 0 network

Rtunja(config)#username Ubucaramanga privilege 0 Ubucaramanga

Rtunja(config)#username Ubucaramanga password 0 Ubucaramanga

Rtunja(config)#Username Utunja password 0 Utunja

Rtunja(config)#Username Ucundinamarca password 0 Ucundinamarca

Rtunja(config)#Interface fastEthernet 0/0

Rtunja(config-if)#ip address 209.17.220.220 255.255.255.0

Rtunja(config-if)#ip nat outside

Rtunja(config-if)#Duplex Auto

Rtunja(config-if)#Speed auto

Rtunja(config-if)#exit

Rtunja(config)#Interface fastEthernet 0/1

Rtunja(config-if)#No ip address Rtunja(config-if)#ip nat outside Rtunja(config-if)#Duplex Auto Rtunja(config-if)#Speed auto Rtunja(config-if)#Interface fastEthernet 0/1.1 Rtunja(config-subif)#Encapsulation dot1Q 1 native Rtunja(config-subif)#lp address 172.31.2.9 255.255.255.248 Rtunja(config-subif)#exit Rtunja(config)#Interface fastEthernet 0/1.20 Rtunja(config-subif)#Encapsulation dot1Q 20 Rtunja(config-subif)#lp address 172.31.0.128 255.255.255.192 Bad mask /26 for address 172.31.0.128 Rtunja(config-subif)#lp address 172.31.0.129 255.255.255.192 Rtunja(config-subif)#lp Access-group 102 in Rtunja(config-subif)#exit Rtunja(config)#Interface fastEthernet 0/1.30 Rtunja(config-subif)#Encapsulation dot1Q 30 Rtunja(config-subif)#lp address 172.31.0.193 255.255.255.192 Rtunja(config-subif)#lp Access-group 103 in Rtunja(config-subif)#exit Rtunja(config)#Interface serial0/0/0 Rtunja(config-if)#lp address 172.31.2.38 255.255.255.252 Rtunja(config-if)#lp ospf message-digest-key 1 md5 7 network Rtunja(config-if)#lp nat inside Rtunja(config-if)#Clock rate 64000 Rtunja(config-if)#exit Rtunja(config)#Interface serial0/0/1

Rtunja(config-if)#lp address 172.31.2.34 255.255.255.252 Rtunja(config-if)#lp ospf message-digest-key 1 md5 7 network Rtunja(config-if)#lp nat inside Rtunja(config-if)#Clock rate 64000 Rtunja(config-if)#exit Rtunja(config)#lnterface Vlan1 Rtunja(config-if)#No ip address Rtunja(config-if)#shutdown Rtunja(config-if)#exit Rtunja(config)#exit Rtunja(config)#exit

Rtunja#

Rtunja#conf t

Rtunja(config)#Router ospf 1

Rtunja(config-router)#Log-adjacency-changes Rtunja(config-router)#area 0 authentication message-digest Rtunja(config-router)#Network 172.31.0.128 0.0.0.63 area 0 Rtunja(config-router)#Network 172.31.0.192 0.0.0.63 area 0 Rtunja(config-router)#Network 172.31.2.8 0.0.0.7 area 0 Rtunja(config-router)#Network 172.31.2.32 0.0.0.7 area 0

Rtunja(config-router)#Network 172.31.2.8 0.0.0.7 area 0 Rtunja(config-router)#Network 172.31.2.32 0.0.0.7 area 0 Rtunja(config)#lp nat inside source static 172.31.2.26 209.17.220.10 Rtunja(config)#lp route 0.0.0.0 0.0.0.0 FastEthernet 0/0 Rtunja(config)#Access-list 20 permit 172.31.0.0 0.0.31.255 Rtunja(config)#Access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63 Rtunja(config)#Access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63 Rtunja(config)#Access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www Rtunja(config)#Access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp Rtunja(config)#lp dhcp excluded-address 172.31.1.65 172.31.1.70 Rtunja(config)#lp dhcp excluded-address 192.31.1.1 172.31.1.5 Rtunja(config)#lp dhcp excluded-address 172.31.0.1 172.31.0.5 Rtunja(config)#lp dhcp excluded-address 172.31.0.65 172.31.0.70

Rtunja(config)#lp dhcp excluded-address 172.31.0.65 172.31.0.70 Rtunja(config)#lp dhcp pool bucaramanga-30 Rtunja(dhcp-config)#Network 172.31.0.64 255.255.255.192 Rtunja(dhcp-config)#Default-router 172.31.0.65 Rtunja(dhcp-config)#lp dhcp Pool t-10 Rtunja(dhcp-config)#Network 172.31.1.0 255.255.255.192 Rtunja(dhcp-config)#Default-router 172.31.1.1 Rtunja(dhcp-config)#lp dhcp Pool t-20 Rtunja(dhcp-config)#Network 172.31.1.64 255.255.255.192 Rtunja(dhcp-config)#Default-router 172.31.1.65 Rtunja(dhcp-config)#Default-router 172.31.1.65 Rtunja(dhcp-config)#lp dhcp Pool bucaramanga-10 Rtunja(dhcp-config)#Network 172.31.0.0 255.255.255.192 Rtunja(dhcp-config)#Default-router 172.31.0.1 Rtunja(dhcp-config)#Default-router 172.31.0.1 Rtunja(dhcp-config)#Default-router 172.31.0.1

# %SYS-5-CONFIG\_I: Configured from console by console

#### Rtunja#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rtunja(config)#line console 0

Rtunja(config-line)#Exec-timeout 5 0

Rtunja(config-line)#Logging synchronous

Rtunja(config-line)#Login authentication INTERNO

Rtunja(config-line)#line vty 0 4

Rtunja(config-line)#Exec-timeout 5 0

Rtunja(config-line)#login

AAA is enabled. Command not supported. Use an aaa authentication methodlist

Rtunja(config-line)#Login authentication INTERNO

Rtunja(config-line)#end

Rtunja#

%SYS-5-CONFIG\_I: Configured from console by console

Rtunja#

Rtunja# Username: Utunja Password: Rtunja>en Password: Rtunja#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rtunja(config)#lp nat inside source static 172.31.2.26 209.17.220.10

Rtunja(config)#lp nat inside source list 20 interface fastEthernet0/0 overload Rtunja(config)#Access-list 20 permit 172.31.0.0 0.0.31.255 Rtunja(config)#exit Rtunja# %SYS-5-CONFIG\_I: Configured from console by console

Rtunja#exit

SWITCH TUNJA

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup

Switch(config)#hostname Stunja

Stunja(config)#enable password cisco

Stunja(config)#line console 0

Stunja(config-line)#password cisco

Stunja(config-line)#login

Stunja(config-line)#line vty 0 15

Stunja(config-line)#password cisco

Stunja(config-line)#login

Stunja(config-line)#exit

Stunja(config)#line console 0

Stunja(config-line)#logging synchronous

Stunja(config-line)#interface VLAN1

Stunja(config-if)#ip address 172.31.2.9 255.255.255.248

Stunja(config-if)#lp default-gateway 172.31.2.1

Stunja(config)#Int range fa0/1-2

Stunja(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

Stunja(config-if-range)#

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Stunja(config-if-range)#exit

Stunja(config)#interface VLAN1

Stunja(config-if)#no shutdown

Stunja(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Stunja(config-if)#exit

Stunja(config)#exit

Stunja#

%SYS-5-CONFIG\_I: Configured from console by console

Stunja#

ASIGNACIÓN PUERTO TRONCAL

Stunja#CONF T

Enter configuration commands, one per line. End with CNTL/Z.

Stunja(config)#interface fastEthernet 0/1 Stunja(config-if)#switchport mode trunk Stunja(config-if)#interface fastEthernet 0/1 Stunja(config-if)#switchport mode access Stunja(config-if)#switchport access VLAN1

## ROUTER BUCARAMANGA

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# hostname Rbucaramanga

Rbucaramanga(config)#login block-for 220 attempts 5 within 100

Rbucaramanga(config)#enable secret cisco

Rbucaramanga(config)#aaa new-model

Rbucaramanga(config)#aaa authentication login INTERNO group radius local enable

Rbucaramanga(config)#username TUNJA privilege 7 password 0 network

Rbucaramanga(config)#username Ubucaramanga password 0 Ubucaramanga

Rbucaramanga(config)#username Utunja password 0 Utunja

Rbucaramanga(config)#username Ucundinamarca password 0 Ucundinamarca

Rbucaramanga(config)#interface fastEthernet 0/0

Rbucaramanga(config-if)#no ip address

Rbucaramanga(config-if)#duplex auto

Rbucaramanga(config-if)#speed auto

Rbucaramanga(config-if)#interface fastEthernet 0/0.1

Rbucaramanga(config-subif)#encapsulation dot1Q 1 native

Rbucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248

Rbucaramanga(config-subif)#exit

Rbucaramanga(config)#interface fastEthernet 0/0

Rbucaramanga(config-if)#interface fastEthernet 0/0.10

Rbucaramanga(config-subif)#encapsulation dot1Q 10

Rbucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192

Rbucaramanga(config-subif)#ip helper-address 172.31.2.34

Rbucaramanga(config-subif)#ip access-group 101 in

Rbucaramanga(config-subif)#exit

Rbucaramanga(config)#interface fastEthernet 0/0

Rbucaramanga(config-if)#interface fastEthernet 0/0.30 Rbucaramanga(configsubif)#encapsulation dot1Q 30

Rbucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192

Rbucaramanga(config-subif)#ip helper-address 172.31.2.34

Rbucaramanga(config-subif)#ip access-group 103 in

Rbucaramanga(config-subif)#exit

Rbucaramanga(config)#interface serial0/0/0

Rbucaramanga(config-if)#ip address 172.31.2.33 255.255.255.252

Rbucaramanga(config-if)#ip ospf message-digest-key 1 md5 7 network

Rbucaramanga(config-if)#

bucaramanga>en Password:

Rbucaramanga#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rbucaramanga(config)#router ospf 1

Rbucaramanga(config-router)#log-adjacency-changes

Rbucaramanga(config-router)#area 0 authentication message-digest Rbucaramanga(config-router)#network 172.31.0.1 0.0.0.63 area 0 Rbucaramanga(config-router)#network 172.31.0.65 0.0.0.63 area 0 Rbucaramanga(config-router)#network 172.31.2.1 0.0.0.7 area 0 Rbucaramanga(config-router)#network 172.31.2.33 0.0.0.7 area 0 Rbucaramanga(config-router)#network 172.31.2.33 0.0.0.7 area 0

#### Ip classless

Rbucaramanga(config)#Access-list 101 permit ip 172.31.0.1 0.0.0.63 172.31.0.128 0.0.0.63 Rbucaramanga(config)#Access-list 101 permit udp host 0.0.0.0 eq bootpc host Rbucaramanga(config)#Access-list 101 permit ip 172.31.0.1 0.0.0.63 172.31.0.128 0.0.0.63 Rbucaramanga(config)#Access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255 eq bootps

Rbucaramanga(config)#Access-list 103 permit udp host 0.0.0.0 eq bootpc host Rbucaramanga(config)#Access-list 103 deny ip 172.31.0.65 0.0.0.63 172.31.1.0 0.0.0.63

Rbucaramanga(config)#Access-list 103 permit ip 172.31.0.65 0.0.0.63 any

Rbucaramanga(config)#

## SWICTH BUCARAMANGA

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup

Switch(config)#hostname Sbucaramanga

Sbucaramanga(config)#enable password class

Sbucaramanga(config)#line console 0

Sbucaramanga(config-line)#password cisco

Sbucaramanga(config-line)#login

Sbucaramanga(config-line)#line vty 0 15

Sbucaramanga(config-line)#password cisco

Sbucaramanga(config-line)#login

Sbucaramanga(config-line)#exit

Sbucaramanga(config)#line console 0

Sbucaramanga(config-line)#logging synchronous

Sbucaramanga(config-line)#interface VLAN1

Sbucaramanga(config-if)#ip address 172.31.2.1 255.255.255.248

Sbucaramanga(config-if)#ip default-gateway 172.31.2.1 Sbucaramanga(config)#int range fa0/0-1 interface range not validated - command rejected Sbucaramanga(config)#int range fa0/0-2 interface range not validated - command rejected Sbucaramanga(config)#int range fa0/0 interface range not validated - command rejected Sbucaramanga(config)#int range fa0/1-2 Sbucaramanga(config)#int range fa0/1-2 Sbucaramanga(config)if-range)#int range fa0/0-1 interface range not validated - command rejected Sbucaramanga(config)#int range fa0/1-2

Sbucaramanga(config-if-range)#int range fa0/1-2

Sbucaramanga(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

Sbucaramanga(config-if-range)#

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Sbucaramanga(config-if-range)# Sbucaramanga(config-if-range)#exit Sbucaramanga(config)#interface VLAN1 Sbucaramanga(config-if)#no shutdown

Sbucaramanga(config-if)# %LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Sbucaramanga(config-if)#exit Sbucaramanga(config)#exit Sbucaramanga# %SYS-5-CONFIG\_I: Configured from console by console

# ROUTER CUNDINAMARCA

Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Rcundinamarca

Rcundinamarca(config)#Login block-for 220 attempts 3 within 110

Rcundinamarca(config)#enable secret cisco

Rcundinamarca(config)#aaa new-model

Rcundinamarca(config)#aaa authentication login INTERNO group radius local enable

Rcundinamarca(config)#Username Ubucaramanga password 0 Ubucaramanga

Rcundinamarca(config)#Username Utunja password 0 Utunja Rcundinamarca(config)#Username Ucundinamarca password 0 Ucundinamarca Rcundinamarca(config)#exit Rcundinamarca# %SYS-5-CONFIG\_I: Configured from console by console

Rcundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rcundinamarca(config)#Interface fastEthernet 0/0

Rcundinamarca(config-if)#No ip address

Rcundinamarca(config-if)#Duplex Auto

Rcundinamarca(config-if)#Speed auto

Rcundinamarca(config-if)#Interface fastEthernet 0/0.1 Rcundinamarca(configsubif)#Encapsulation dot1Q 1 native

Rcundinamarca(config-subif)#lp address 172.31.2.17 255.255.255.248

Rcundinamarca(config-subif)#exit

Rcundinamarca(config)#Interface fastEthernet 0/0.10

Rcundinamarca(config-subif)#Encapsulation dot1Q 10

Rcundinamarca(config-subif)#exit

Rcundinamarca(config)#Interface fastEthernet 0/0.20

Rcundinamarca(config-subif)#exit

Rcundinamarca(config)#Interface fastEthernet 0/0.20

Rcundinamarca(config-subif)#Encapsulation dot1Q 20

Rcundinamarca(config-subif)#lp address 172.31.1.65 255.255.255.192

Rcundinamarca(config-subif)#lp helper-address 172.31.2.38

Rcundinamarca(config-subif)#lp Access-group 101 in

Rcundinamarca(config-subif)#exit

Rcundinamarca(config)#Interface fastEthernet 0/1.30 Rcundinamarca(config-subif)#Encapsulation dot1Q 30 Rcundinamarca(config-subif)#Ip address 172.31.1.1 255.255.255.192 Rcundinamarca(config-subif)#Ip helper-address 172.31.2.38 Rcundinamarca(config-subif)#Ip Access-group 102 in Rcundinamarca(config-subif)#exit Rcundinamarca(config-subif)#Encapsulation dot1Q 88 native Rcundinamarca(config-subif)#Encapsulation dot1Q 88 native Rcundinamarca(config-subif)#Ip address 172.31.2.25 255.255.255.248 Rcundinamarca(config-subif)#Ip address 172.31.2.37 255.255.255.252 Rcundinamarca(config-if)#Ip address 172.31.2.37 255.255.255.252 Rcundinamarca(config-if)#Ip ospf message-digest-key 1 md5 7 network Rcundinamarca(config-if)#Router ospf 1

Rcundinamarca(config-router)#area 0 authentication message-digest Rcundinamarca(config-router)#exit

Rcundinamarca(config)#

Rcundinamarca>EN Password:

Rcundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rcundinamarca(config)#Router ospf 1

Rcundinamarca(config-router)#Log-adjacency-changes

Rcundinamarca(config-router)#area 0 authentication message-digest Rcundinamarca(config-router)#Network 172.31.1.0 0.0.0.63 area 0

Rcundinamarca(config-router)#Network 172.31.1.64 0.0.0.63 area 0

Rcundinamarca(config-router)#Network 172.31.2.16 0.0.0.7 area 0 Rcundinamarca(config-router)#Network 172.31.2.36 0.0.0.3 area 0 Rcundinamarca(config-router)#Network 172.31.2.24 0.0.0.7 area 0 Rcundinamarca(config-router)#

IP CLASSLESS

Rcundinamarca(config-router)#Access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

Rcundinamarca(config)#Access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63

Rcundinamarca(config)#Access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63

Rcundinamarca(config)#Access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps

Rcundinamarca(config)#Access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0

0.0.255.255

Rcundinamarca(config)#Access-list 101 permit ip 172.31.1.64 0.0.0.63 any

Rcundinamarca(config)#

Rcundinamarca(config)#line console 0

Rcundinamarca(config-line)#Exec-timeout 6 0

Rcundinamarca(config-line)#Logging synchronous

Rcundinamarca(config-line)#Login authentication INTERNO

Rcundinamarca(config-line)#line vty 0 4

Rcundinamarca(config-line)#Exec-timeout 6 0

Rcundinamarca(config-line)#Login authentication INTERNO

Rcundinamarca(config-line)#line vty 5

Rcundinamarca(config-line)#Exec-timeout 6 0

Rcundinamarca(config-line)#end

Rcundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console

Rcundinamarca#

# SWICTH CUNDINAMARCA

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup

Switch(config)#hostname Scundinamarca

Scundinamarca(config)#enable password cisco

Scundinamarca(config)#line console 0

Scundinamarca(config-line)#password cisco

Scundinamarca(config-line)#login

Scundinamarca(config-line)#line vty 0 15

Scundinamarca(config-line)#password cisco

Scundinamarca(config-line)#login

Scundinamarca(config-line)#exit

Scundinamarca(config)#line console 0

Scundinamarca(config-line)#Logging synchronous

Scundinamarca(config-line)#interface VLAN1

Scundinamarca(config-if)#lp address 172.31.2.17 255.255.255.248

Scundinamarca(config-if)#lp default-gateway 172.31.2.1 Scundinamarca(config)#interface range fastEthernet 0/0-1 interface range not validated - command rejected Scundinamarca(config)#interface range fastEthernet 0/0-2 interface range not validated - command rejected Scundinamarca(config)#interface range fastEthernet 0/1-2

Scundinamarca(config-if-range)#shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

Scundinamarca(config-if-range)#

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Scundinamarca(config-if-range)#exit

Scundinamarca(config)#

Scundinamarca(config-if-range)#exit

Scundinamarca(config)#interface VLAN1

Scundinamarca(config-if)#no shutdown

Scundinamarca(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Scundinamarca(config-if)#exit Scundinamarca(config)#exit Scundinamarca# %SYS-5-CONFIG\_I: Configured from console by console

Scundinamarca#

# ASIGNACION PUERTO TRONCAL

#### Scundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z. Scundinamarca(config)#interface fastEthernet 0/1 Scundinamarca(config-if)#switchport mode trunk

## ASIGNACIOND DE PUERTO PARA PC

Scundinamarca(config)#interface fastEthernet 0/1 Scundinamarca(config-if)#interface fastEthernet 0/1 Scundinamarca(config-if)#switchport mode access Scundinamarca(config-if)#switchport access VLAN 1 Scundinamarca(config-if)#exit Scundinamarca(config)#exit Scundinamarca#

#### Router>en

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname Rcundinamarca

Rcundinamarca(config)#banner motd #!!CUIDADO ACCESO ASEGURADO!!#

Rcundinamarca(config)#enable secret cisco

Rcundinamarca(config)#line console 0

Rcundinamarca(config-line)#password cisco

Rcundinamarca(config-line)#login

Rcundinamarca(config-line)#exit

Rcundinamarca(config)#line vty 0 4

Rcundinamarca(config-line)#password cisco

Rcundinamarca(config-line)#login

Rcundinamarca(config-line)#exit

Rcundinamarca(config)#interface fastEthernet 0/0

Rcundinamarca(config-if)#ip address 172.33.2.8 255.255.255.248

Rtunja(config-if)#no shutdown

Rtunja(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Rcundinamarca(config-if)#exit

Rcundinamarca(config)#interface serial 172.31.2.37 255.255.255.252

En el punto anterior se adelantan pasos posteriors que facilitan la implementación de la simulación de toda la red.

□ Autenticación local con AAA.

SERVIDOR INTERNO Rcundinamarca>en Password:

Rcundinamarca#conf t

Rcundinamarca(config)#aaa new-model

Rcundinamarca(config)#aaa authentication login INTERNO group radius local enable

Rcundinamarca(config)#

Rcundinamarca(config)#interface Serial0/0/0

Rcundinamarca(config-if)#aaa authentication login INTERNO group radius local enable

Rcundinamarca(config)#radius-server host 172.31.2.1 key cisco

Rcundinamarca(config)#line vty 0 15

Rcundinamarca(config-line)#login authentication INTERNO

Rcundinamarca(config-line)#exit Rcundinamarca(config)#do wri

Rcundinamarca(config)#username usuario1 secret cisco

Rcundinamarca(config)#username admin secret cisco Rcundinamarca(config)#do wri Building configuration...

[OK]

💐 WEB INTERNO			– 🗆 X
Physical Config	Services Desktop C	ustom Interface	
SERVICES HTTP	^	AAA	
DHCP DHCPv6	Service   On  O	Off Radius Port	1645
TFTP	- Network Configuration -		
DNS	Client Name	Client IP	
AAA	Secret	ServerType	Radius 👻
NTP EMAIL	Client Name C	ient IP Server Type	Key Add
FTP		I.Z.1 Radius	Save
			Remove
	User Setup Username	Password	
	Username 1 usuario1	Password cisco	Add
	2 admin	cisco	Save
	, L		Remove
		^	<i>信</i> № ↓ ↓) (同 1:02 p.m. 11/12/2019

llustración 43

SERVIDOR EXTERNO Rtunja>en Password: Rtunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Rtunja(config)#aaa authentication login EXTERNO group radius local enable Rtunja(config)#aaa new-model Rtunja(config)#aaa authentication login EXTERNO group radius local enable Rtunja(config)#interface fastEthernet 0/0 Rtunja(config-if)#aaa authentication login EXTERNO group radius local enable Rtunja(config)#radius-server host 209.17.220.3 key cisco Rtunja(config)#line vty 0 15 Rtunja(config-line)#login authentication EXTERNO Rtunja(config-line)#EXIT Rtunja(config)#do wri Building configuration... Rtunja(config)#username usuario1E secret cisco Rtunja(config)#username adminE secret cisco Rtunja(config)#do wri

Building configuration...

Augustal Config CLI  IDS Command Line Interface  IDS Command Line Interface  IDS Command Line Interface  IDT IDS Config Servet cisco  IDT IDS Services Desktop Custom Interface  IDT DHCP DHCPV5 TTP DHS SYSLOG AAA NTP EMAIL FTP II Runja 209.17.220.1 Radius cisco Remove User Setup Username cisco Remove I adminE cisco Save Remove Rem	TUNJA										_		×
IDS Command Line Interface         NUMBER CONSTRUCTION OF THE SECRET CISCO         TUTO SECRET CISCO         TUTO SECRET CISCO         TUTO SECRET CISCO         VISE EXTERNO         MAA         MAA         SERVICES         Desktop Custom Interface         MAA         SERVICES         DHCPVO         ON O O OF Radus Port         SERVICES         DHCPVO         O O O OF Radus Port         OF TIP         DNS         SIGO Clent IP         SERVICES         DHCPVO         O O O OF Radus Port         O O O OF Radus Port         O O O OF Radus Port         O O O O OF Radus Port         O O O O O O O O O O O O O O O O O O O	hysical	Config	CL	I									
ALLASING CONLIGUENELLON OCI tunja (conf.g) Fueraname usuario1E secret cisco tunja (conf.g) Fueraname daminE secret cisco tunja (conf.g) Fueraname daminE secret cisco tunja (conf.g) Fueraname daminE secret cisco WEB EXTERNO -					IOS	Com	mand Li	ne 1	nterface				
WEB EXTERNO       -       ×         Physical Config Services Desktop Custom Interface       AAA         SERVICES       AAA         HTTP       AAA         DHCP       Envice Image: Clent IP         DHCP       Clent Name         Clent Name       Clent IP         Service       ServerType Radius         NTP       EMAIL         Itunja       209.17.220.1         Remove       Remove         User Setup       Username         Username       Password         Add       Save         Remove       Save	Guilding C [OK] Rtunja(con: Rtunja(con: Rtunja(con: Rtunja(con: Building c	onfigura fig)‡use: fig)‡use: fig)‡do t onfigura	rnar rnar wri tior	ne usu ne adm ne adm	ario1E ninE se	secre cret c	: cisco isco						^
Physical Config Services Desktop Custom Interface          SERVICES       HTTP         DHCP       DHCP         DHCP       Bervice         DHCP       On O Off Radus Port         DHCP       Iftig         DHCP       Iftig         DHCP       Clent IP         StySLOG       AAA         NTP       EMAIL         FTP       Itent Name         Clent Name       Clent IP         Servet       ServerType         Vername       Op:17:220.1         Remove       Remove         User Setup       Username         Username       Password         1       add         2       usuario1E	💐 WEB EXTE	RNO									- 0	×	
SERVICES       AAA         HTTP       DHCP         DHCP/s6       On O Off Radus Port 1645         TFTP       Ns         SYSLOG       AAA         NTP       Client Name         Client Name       Client IP         ServerType       Radius         TTP       Client Name         Client Name       Client IP         ServerType       Radius         User Setup       Username         Username       Password         1       adminE         2       usuario1E         clisco       Ramove	Physical	Config	5	Servic	es C	esktop	Custo	m In	terface				
HTTP       DHCP         DHCP       Service       On O Off Radus Port       1645         TFTP       Ns       Clent Name       Clent IP         SYSLGG       AAA       Server Type Radius <ul> <li>Clent Name</li> <li>Clent IP</li> <li>Server Type</li> <li>Key</li> <li>Add</li> </ul> Itemportation         NTP       Client Name       Client IP       Server Type         EMAIL       FTP       Client Name       Client IP       Server Type         User Setup       User Setup       Username       Password       Add         1       adminE       cisco       Save         2       usuario1E       cisco       Remove	SERVI	ICES							۵۵۵				
DHCP       Service       Image: Only of fill	HTT	ſP											
DHCPVb       Network Configuration         TTTP       DNS         SYSLOG       Secret         Secret       ServerType         Radius       Image: Client IP         EMAIL       FTP         FTP       Image: Client IP         User Setup       Save         User Setup       Dername         Image: Client IP       Password         Image: Client IP       Save         Remove       Save         Image: Client IP       Save         User Setup       Save         Image: Client IP       Save         Remove       Remove	DHO	CP		Serv	vice	•	n 🔿 Off		Radius Port	1645			
DNS         SYSLOG         AAA         SYSLOG         AAA         Secret         Client Name         Password         Lusario1E         Client Name         Client Name         Password         Add         Save         Remove	DHC	PV6		Ne	-								
SYSLOG         AAA         NTP         EMAIL         FTP         Querter Setup         Username         Password         1         adminE         cisco         Save         Remove         2         usarial         cisco         2         usarial         cisco         Remove		۲ ۲		ive	LWORK C	oniigura	luon		1.				
AAA     Secret     ServerType     Radius       NTP     Client Name     Client IP     ServerType     Key     Add       I     Rtunja     209.17.220.1     Radius     cisco     Save       User Setup     Username     Password     Image: Cisco     Add       1     adminE     cisco     Save       2     usuario1E     cisco     Remove	SYSL	.OG		Clie	nt Name				Client IP				
NTP       Client Name       Client IP       Server Type       Key       Add         FTP       1       Rtunja       209.17.220.1       Radius       cisco       Save         User Setup       Username       Password	AA	A		Sec	ret				ServerType	Radius		-	
EMAIL       I       Rtunja       209.17.220.1       Radius       cisco       Save         FTP       User Setup       Password       Remove         User Setup       Username       Password       Add         1       adminE       cisco       Save         2       usuario1E       cisco       Save         Remove       Remove       Remove	NT	Р			Client	Name	Client IP		Server Type	Key		_	
FTP Content roots of Save Remove User Setup Username Password 1 adminE cisco 2 usuario1E cisco Remove Remove	EMA	αL		1	Rtunia		209 17 220 1		Radius	cisco	Add		
User Setup User Setup Username Password 1 adminE cisco 2 usuario1E cisco Remove Remove	FTI	P									Save	3	
User Setup Username Password Add 1 adminE cisco 2 usuario IE cisco Remove											Remo	ve	
Username Password Add 1 adminE cisco Save 2 usuario1E cisco Remove					or Cotur						]		
Username Password Add 1 adminE cisco 2 usuario1E cisco Remove 2 admine cisco			Us	er Setup	, 			Bacquerd					
Username Password Add  adminE cisco  usuario1E cisco  Remove  215 p.				-	arrighting.			_	russiloru		1		
2 usuario1E cisco Remove				1	adminE	Userna	me	cisco	Password		Add		
Remove 215 p.				2	usuario1	E		cisco	•		Save	е	
215.0											Remo	ve	
2:15 p.			~								]		
												2:1	5 p. m

Ilustración 44

• Cifrado de contraseñas.

```
BUCARAMANGA
!!CUIDADO ACCESO ASEGURADO!!
User Access Verification
Password:
Rbucaramanga>en
Rbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rbucaramanga(config)#service password-encryption
Rtunja(config)#exit
Rbucaramanga(config)#show running-config
Rbucaramanga(config)#exit
Rbucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Rbucaramanga#show running-config
Building configuration...
Current configuration : 2289 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Rbucaramanga
login block-for 220 attempts 5 within 100
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
1
aaa new-model
aaa authentication login INTERNO group radius local enable
ip cef
no ipv6 cef
username TUNJA password 7 082F495A1E16171C
username Ubucaramanga password 7 08144E5B0A1817161F0A02032B
username Ucundinamarca password 7 08144F5B071D0C1913060D16292A
```

```
username Utunja password 7 0814585B071304
spanning-tree mode pvst
interface FastEthernet0/0
no ip address
duplex auto
speed auto
L
interface FastEthernet0/0.1
encapsulation dot1Q 1 native
ip address 172.31.2.1 255.255.255.248
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.31.0.1 255.255.255.192
ip helper-address 172.31.2.34
ip access-group 101 in
L
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.31.0.65 255.255.255.192
ip helper-address 172.31.2.34
ip access-group 103 in
L
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
L
interface Serial0/0/0
ip address 172.31.2.33 255.255.255.252
ip ospf message-digest-key 1 md5 7 network
clock rate 2000000
L
interface Serial0/0/1
no ip address
clock rate 2000000
shutdown
!
```

```
interface Vlan1
no ip address
shutdown
l
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
network 172.31.0.0 0.0.0.63 area 0
network 172.31.0.64 0.0.0.63 area 0
network 172.31.2.0 0.0.0.7 area 0
network 172.31.2.32 0.0.0.7 area 0
ip classless
L
ip flow-export version 9
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 101 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
access-list 101 permit ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.1.0 0.0.0.63
access-list 103 permit ip 172.31.0.64 0.0.0.63 any
line con 0
L
line aux 0
line vty 0 4
End
TUNJA
!!CUIDADO ACCESO ASEGURADO!!
```

User Access Verification

```
Password:
Rtunja>en
Password:
Rtunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Rtunja(config)#service password-encryption
Rtunja(config)#exit
Rtunja(config)#show running-config
Rtunja(config)#exit
Rtunja#
%SYS-5-CONFIG I: Configured from console by console
Rtunja#show running-config
Building configuration...
Current configuration : 3356 bytes
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Rtunja
login block-for 220 attempts 3 within 110
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
ip dhcp excluded-address 172.31.1.65 172.31.1.70
ip dhcp excluded-address 192.31.1.1 172.31.1.5
ip dhcp excluded-address 172.31.0.1 172.31.0.5
ip dhcp excluded-address 172.31.0.65 172.31.0.70
--More-
```

## CUNDINAMARCA

# **!!CUIDADO ACCESO ASEGURADO!!**

User Access Verification

Password:

Rcundinamarca>en Password: Rcundinamarca#conf t Enter configuration commands, one per line. End with CNTL/Z. Rcundinamarca(config)#service password-encryption Rcundinamarca(config)#exit Rcundinamarca# %SYS-5-CONFIG\_I: Configured from console by console

Rcundinamarca#show running-config Building configuration... %SYS-5-CONFIG\_I: Configured from console by console

Rcundinamarca#show running-config Building configuration...

```
Current configuration : 2654 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname Rcundinamarca

!

login block-for 220 attempts 3 within 110

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

aaa new-model

!

--More--
```

• Un máximo de internos para acceder al router.

#### BUCARAMANGA

## **!!CUIDADO ACCESO ASEGURADO!!**

**User Access Verification** 

Password:

Rbucaramanga>en Password: Rbucaramanga#conf t Enter configuration commands, one per line. End with CNTL/Z. Rbucaramanga(config)#line console 0 Rbucaramanga(config-line)#exec-timeout 1 10 Rbucaramanga(config-line)#exec-count 5 Rbucaramanga(config-line)#exit

TUNJA

## **!!CUIDADO ACCESO ASEGURADO!!**

**User Access Verification** 

Password: Rtunja>en Password: Password: Rtunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Rtunja(config)#line console 0 Rtunja(config-line)#exec-timeout 1 10 Rtunja (config-line)#exec-count 5 Rtunja(config-line)#exit Rtunja(config)#exit Rtunja# %SYS-5-CONFIG\_I: Configured from console by console

#### CUNDINAMARCA

#### **!!CUIDADO ACCESO ASEGURADO!!**

User Access Verification

Password:

## • Máximo tiempo de acceso al detectar ataques.

## CUNDINAMARCA

## **!!CUIDADO ACCESO ASEGURADO!!**

**User Access Verification** 

Password:

Rcundinamarca >en Password: Password: Rcundinamarca #conf t Enter configuration commands, one per line. End with CNTL/Z. Rcundinamarca (config)# Login block-for 220 attempts 3 within 110 Rcundinamarca (config)# enable secret cisco Rcundinamarca (config)# aaa new-model Rcundinamarca (config)# aaa authentication login INTERNO group radius local enable Rcundinamarca # %SYS-5-CONFIG\_I: Configured from console by console

TUNJA

**!!CUIDADO ACCESO ASEGURADO!!** 

**User Access Verification** 

Password:

Router#conf t Rtunja(config)#Login block-for 220 attempts 3 within 110 Rtunja(config)#enable secret cisco Rtunja(config)#aaa new-model Rtunja(config)#aaa authentication login INTERNO group radius local enable Rtunja(config)#username TUNJA privilege 7 password 0 network BUCARAMANGA

**!!CUIDADO ACCESO ASEGURADO!!** 

User Access Verification Password:

bucaramanga>en Password: Password: bucaramanga#conf t Enter configuration commands, one per line. End with CNTL/Z. bucaramanga (config)# Login block-for 220 attempts 3 within 110 bucaramanga (config)# enable secret cisco bucaramanga (config)# aaa new-model bucaramanga (config)# aaa authentication login INTERNO group radius local enable bucaramanga# %SYS-5-CONFIG\_I: Configured from console by console • Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

sco Packet Tracer St	tudent - (	C:\1RespaldoE	iscoDuro12Ju)	nio2018\1Respaldo Junio2-2018(D	)\1 —		$\times$		
Reference web externo	)				_		×		
Physical Co	onfig	Services	Desktop	Custom Interface					
SERVICES	s ^	]		TETD					
HTTP				IFIP			_		
DHCP		Service		On		◯ Off			
DHCPv6							_		
TFTP				File			^		
DNS		asa842-	8.bin						
		c1841-a	dvipservicesk	9-mz.124-15.T1.bin					
NTP		c1841-ip	base-mz.123	-14.T7.bin					
EMAIL		c1841-ip	basek9-mz.1	24-12.bin					
FTP		c2600-a	dvipservicesk						
		c2600-i-i	mz.122-28.bii	ı					
		c2600-ip	basek9-mz.1	24-8.bin					
		c2800nm	c2800nm-advipservicesk9-mz.124-15.T1.bin						
		c2800nm	-advipservic	esk9-mz.151-4.M4.bin					
		c2800nm							
		c2800nm	i-ipbasek9-m	z.124-8.bin					
	c2950-i6q4l2-mz.121-22.EA4.bin								
c2950-i6q4l2-mz.121-22.EA8.bin									
	c2960-lanbase-mz.122-25.FX.bin								
		c2960-la			<b>~</b>				
					Ren	iove Fi	le		
	$\sim$						-		
	_								
: 06:07:18 Po	ower Cyc	le Devices F	ast Forward	Time	R	ealtir	ne		

llustración 45

Ahora se verifica se que tenga conexión con el router de TUNJA en la fa 0/0 209.17.220.1, ya que desde allí se tendrá control del servidor TFTP.



Ilustración 46

**!!CUIDADO ACCESO ASEGURADO!!** 

**User Access Verification** 

Password:

Rtunja>en

Password:

Rtunja#copy running-config tftp

Address or name of remote host []? 209.17.220.1

Destination filename [Rtunja-confg]? backup\_running

Writing running-config...!!

[OK - 1227 bytes]

1227 bytes copied in 0 secs

Rtunja#

Ahora se verifica que se guarde la información y se procede al código.

Rtunja#show ver

Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 04:52 by pt\_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on

System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

--More—

Rtunja#

Rtunja#

Rtunja#copy flash tftp

Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin

Address or name of remote host []? 209.17.220.1

Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? DatosRouters

Writing c1841-advipservicesk9-mz.124-

[OK - 33591768 bytes]

33591768 bytes copied in 0.874 secs (4035465 bytes/sec)

Se realiza el guardado de los datos de manera general.

Ahora se verifican en el servidor TFTP
hysical	Config	s	ervices	Desktop	Custom Interface			
SERV HT	ICES TP	^			TFTP			
DHCP			Service		On		0 0	Off
TF	TP				File			^
SYS			DatosRo	uters				
AA	A		asa842-l	k8.bin				
N	ſP		backup_	running				
EMA	AIL		c1841-a	dvipservicesk	9-mz.124-15.T1.bin			
FTP			c1841-ipbase-mz.123-14.T7.bin					
			c1841-ip	basek9-mz.1	24-12.bin			
			c2600-advipservicesk9-mz.124-15.T1.bin					
			c2600-i-mz.122-28.bin					
			c2600-ipbasek9-mz.124-8.bin					
			c2800nm-advipservicesk9-mz.124-15.T1.bin					
			c2800nm	n-advipservic	esk9-mz.151-4.M4.bin			
			c2800nm-ipbase-mz.123-14.T7.bin					
			c2800nm	n-ipbasek9-m	z.124-8.bin			
			c2950-i6	a4l2-mz.121-	22.EA4.bin			
			c2950-i6	• a4l2-mz.121•	22.EA8.bin			~
						Re	move F	ile
		$\mathbf{v}$						

llustración 47

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

Desde tunja se programa los DHCP para los router tunja y Bucaramanga.

**!!CUIDADO ACCESO ASEGURADO!!** 

User Access Verification

Password:

Rtunja>en Password: Rtunja#en Rtunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Rtunja(config)#ip dhcp excluded-address 172.31.0.1 Rtunja(config)#ip dhcp excluded-address 172.31.0.65 Rtunja(config)#ip dhcp excluded-address 172.31.1.65 Rtunia(config)#ip dhcp excluded-address 172.31.1.1 Rtunja(config)#ip dhcp pool V10BU Rtunja(dhcp-config)#network 172.31.0.0 255.255.255.192 Rtunia(dhcp-config)#default-router 172.31.0.1 Rtunja(dhcp-config)#dns-server 172.31.2.28 Rtunia(dhcp-config)#ip dhcp pool V30BU Rtunja(dhcp-config)#network 172.31.0.64 255.255.255.192 Rtunja(dhcp-config)#default-router 172.31.0.65 Rtunja(dhcp-config)#dns-server 172.31.2.28 Rtunja(dhcp-config)#ip dhcp pool V30CU Rtunja(dhcp-config)#ip dhcp pool V20CU Rtunja(dhcp-config)#network 172.31.1.64 255.255.255.192 Rtunja(dhcp-config)#default-router 172.31.1.65 Rtunja(dhcp-config)#dns-server 172.31.2.28 Rtunja(dhcp-config)#ip dhcp pool V30CU Rtunja(dhcp-config)#network 172.31.1.0 255.255.255.192 Rtunja(dhcp-config)#default-router 172.31.1.1 Rtunja(dhcp-config)#dns-server 172.31.2.28 Rtunja(dhcp-config)#END Rtunja# %SYS-5-CONFIG\_I: Configured from console by console

## **!!CUIDADO ACCESO ASEGURADO!!**

**User Access Verification** 

Rbucaramanga>en Password: Rbucaramanga#en Rbucaramanga#conf t Enter configuration commands, one per line. End with CNTL/Z. Rbucaramanga(config)#int f0/0.10 Rbucaramanga(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

Rbucaramanga(config-subif)#ip helper-address 172.31.2.33 Rbucaramanga(config-subif)#int f0/0.30 Rbucaramanga(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

Rbucaramanga(config-subif)#ip helper-address 172.31.2.33 Rbucaramanga(config-subif)#end Rbucaramanga# %SYS-5-CONFIG\_I: Configured from console by console

## **!!CUIDADO ACCESO ASEGURADO!!**

**User Access Verification** 

Password:

Rcundinamarca>en Password: Rcundinamarca#en Rcundinamarca#conf t Enter configuration commands, one per line. End with CNTL/Z. Rcundinamarca(config)#int f0/0.20 Rcundinamarca(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

Rcundinamarca(config-subif)#ip helper-address 172.31.2.37 Rcundinamarca(config-subif)#int f0/0.30 Rcundinamarca(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up Rcundinamarca(config-subif)#ip helper-address 172.31.2.37 Rcundinamarca(config-subif)#end Rcundinamarca#

			0		,		
	💐 РСО					-	
	Physical Con	fig Deskto	OP Custom I	Interface			
5							
/30	IP Config	uration					Х
	IP Configura	ation					
	OHCP	0 5	tatic	DHCP reque	st successful.		
_	IP Address	:17	2.31.0.2				
	Subnet Mask	25	5.255.255.192				
)-PT C2	Default Gate	way 17	2.31.0.1				
20 VL/ TS VL/	DNS Server	17	2.31.2.28				
VLA VLA	IPv6 Config	uration					
		Auto Config	Static				
	IPv6 Address	;				/	
	Link Local Ad	ldress FE	80::260:70FF	:FEBA:1CED			
	IPv6 Gatewa	у					
	IPv6 DNS Se	rver					
AN1= 1							

# %SYS-5-CONFIG\_I: Configured from console by console

#### llustración 48

	۶	PC1						-	-	
	Р	hysical	Config	Desktop	Custom Inte	rface				
/30		IP Co	nfigura	tion						Х
			P	🔿 Sta	tic	DHCP	request successfu	ul.		
_		IP Addr	ess	172.3	1.0.66					
<b>]</b> ~		Subnet	Mask	255.2	255.255.192					
-PT		Default	Gateway	172.3	1.0.65					
10 TS VL/		DNS Se	erver	172.3	1.2.28					
VLA VLA		IPv6 C	Configurati	on						
			P 🔾 Auto	Config 🔘	Static					
		IPv6 Ac	dress						/	
		Link Lo	cal Addres	s FE80	::201:63FF:FE9	B:E7BA				
		IPv6 Ga	ateway							
		IPv6 DN	NS Server							
AN:= 1										

llustración 49

						\				
	Ę	PC4						_		
	Pł	nysical	Config	Desktop	Custom Interface					
РТ 2		TP Co	nfigura	tion					X	
VL		-IP Con	figuration							
VLA VLA			P	🔿 Stati	c					
		IP Addr	ess	172.31	1.1.66					
		Subnet Mask		255.25	255.255.255.192					
		Default	Gateway	172.31	1.1.65					
		DNS Se	rver	172.31	1.2.28					
		IPv6 Configuration								
		○ DHCP ○ Auto Config ④ Static								
N1= 1. N20=1		IPv6 Ac	ldress					/		
N88=1		Link Lo	cal Addres	s FE80:	:202:4AFF:FE6D:2A	09				
		IPv6 Ga	ateway							
		IPv6 DN	Server							

#### llustración 50

- olt	💐 PC5					_	
_	Physical	Config	Desktop	Custom Interface			
Recc Cam	IP C	onfigura	ation				Х
Gira	IP Co	nfiguration					
igen	DHO	CP	🔿 Stati	с	DHCP request successful.		
	IP Add	lress	172.31	.1.2			
	Subne	t Mask	255.25	5.255.192			
	Defaul	t Gateway	172.31	2.28			
PC	DNS S	erver					
LAN	IPv6	Configurati	on				
юнс		CP 🔿 Auto	Config 🔘	Static			
	IPv6 A	ddress				/	
	Link Lo	ocal Addres	s FE80:	:20C:CFFF:FE2B:B36	57		
	IPv6 G	ateway					
	IPv6 D	NS Server					

llustración 51

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

# **!!CUIDADO ACCESO ASEGURADO!!**

User Access Verification

Password:

Rtunja>en Password: Rtunja#en Rtunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Rtunja(config)#ip nat inside source static 172.31.2.28 209.165.220.4 Rtunja(config)#access-list 1 permit 172.0.0.0 0.255.255.255 Rtunja(config)#ip nat inside source list 1 interface f0/1 overload Rtunja(config)#int f0/1 Rtunja(config-if)#ip nat outside Rtunja(config-if)#ip nat outside Rtunja(config-if)#int f0/0.1 Rtunja(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up ip nat insid Rtunja(config-subif)#ip nat inside Rtunja(config-subif)#int f0/0.30 Rtunja(config-subif)# %LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

Rtunja(config-subif)#ip nat inside Rtunja(config-subif)#int s0/0/0 Rtunja(config-if)#ip nat inside Rtunja(config-if)#ip nat inside Rtunja(config-if)#ip nat inside Rtunja(config-if)#exit Rtunja(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3 Rtunja(config)#router ospf 1 Rtunja(config)router)#default-information originate Rtunja(config-router)#default-information originate Rtunja(config-router)#exit Rtunja(config)#exit Rtunja(config)#exit Rtunja# %SYS-5-CONFIG\_I: Configured from console by console

Rtunja#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.3.0.0/29 is subnetted, 1 subnets

- C 172.3.2.8 is directly connected, FastEthernet0/1 172.30.0.0/22 is subnetted, 1 subnets
- C 172.30.0.0 is directly connected, Serial0/0/0 172.31.0.0/22 is subnetted, 1 subnets

C 172.31.0.0 is directly connected, Serial0/0/1

C 209.17.220.0/24 is directly connected, FastEthernet0/0 Rtunja#

## **!!CUIDADO ACCESO ASEGURADO!!**

User Access Verification

Password:

Rbucaramanga>en

Password:

Rbucaramanga#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route



Ilustración 52

4. El enrutamiento deberá tener autenticación.

Se realiza autenticación en cada uno de los routers. TUNJA-CUNDINAMARCA Y BUCARAMANGA. **!!CUIDADO ACCESO ASEGURADO!! User Access Verification** Password: Rbucaramanga>en Password: Rbucaramanga#conf t Enter configuration commands, one per line. End with CNTL/Z. Rbucaramanga(config)#int s0/0/0 Rbucaramanga(config-if)#ip ospf authentication message-digest Rbucaramanga(config-if)#ip ospf message-digest-key 1 md5 cisco Rbucaramanga(config-if)#end Rbucaramanga# %SYS-5-CONFIG\_I: Configured from console by console **!!CUIDADO ACCESO ASEGURADO!!** User Access Verification

Password:

Rtunja>en Password: Rtunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Rtunja(config)#int s0/0/0 Rtunja(config-if)#ip ospf authentication message-digest Rtunja(config-if)#ip ospf message-digest-key 1 md5 cisco Rtunja(config-if)#end Rtunja# %SYS-5-CONFIG\_I: Configured from console by console !!CUIDADO ACCESO ASEGURADO!! User Access Verification Password:

Rcundinamarca>en

Password:

Rcundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Rcundinamarca(config)#int s0/0/0

Rcundinamarca(config-if)#ip ospf authentication message-digest

Rcundinamarca(config-if)#ip ospf message-digest-key 1 md5 cisco

Rcundinamarca(config-if)#end

Rcundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console

Rbucaramanga(config)#enable secret cisco

Rbucaramanga(config)#aaa new-model

Rbucaramanga(config)#aaa authentication login INTERNO group radius local enable

Rbucaramanga(config)#username TUNJA privilege 7 password 0 network Rbucaramanga(config)#username Ubucaramanga password 0 Ubucaramanga Rbucaramanga(config)#username Utunja password 0 Utunja

Rbucaramanga(config)#username Ucundinamarca password 0 Ucundinamarca

5. Listas de control de acceso:

 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

!!CUIDADO ACCESO ASEGURADO!!
User Access Verification
Password:
Scundinamarca>en

Password:

Scundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Scundinamarca(config)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

Scundinamarca(config)#access-list 111 permit ip any any

Scundinamarca(config)#int f0/0.20

Scundinamarca(config-subif)#ip access-group 111 in

Scundinamarca(config-subif)#end

Scundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console



#### llustración 53

• Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

!!CUIDADO ACCESO ASEGURADO!!

User Access Verification Password: Scundinamarca>en Password: Scundinamarca#conf t Enter configuration commands, one per line. End with CNTL/Z. Scundinamarca(config)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

Scundinamarca(config)#access-list 112 deny ip any any

Scundinamarca(config)#int f0/0.30

Scundinamarca(config-subif)#ip access-group 112 in

Scundinamarca(config-subif)#end

Scundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console



llustración 54

• Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

IICUIDADO ACCESO ASEGURADO!! User Access Verification Password: Stunja>en Password: Stunja#conf t Enter configuration commands, one per line. End with CNTL/Z. Stunja(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80 Stunja(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21 Stunja(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20 Stunja(config)#int f0/0.30 Stunja(config-subif)#ip access-group 111 in

Stunja(config-subif)#end

### Stunja#

%SYS-5-CONFIG\_I: Configured from console by console



#### Ilustración 55



Ilustración 56

• Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

## !!CUIDADO ACCESO ASEGURADO!!

**User Access Verification** 

Password:

Stunja>en

Password:

Stunja#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Stunja(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63 Stunja(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63 Stunja(config)#int f0/0.20

Stunja(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20,

changed state to up

Stunja(config-subif)#ip access-group 112 in

Stunja(config-subif)#end

## Stunja#

%SYS-5-CONFIG\_I: Configured from console by console



Ilustración 57



llustración 58

 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

## **!!CUIDADO ACCESO ASEGURADO!!**

User Access Verification Password: Sbucaramanga>en Password: Sbucaramanga#conf t Snter configuration commands, one per line. End with CNTL/Z. Sbucaramanga(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255 Sbucaramanga(config)#int f0/0.30 Sbucaramanga(config-subif)#ip access-group 111 in Sbucaramanga(config-subif)#end Sbucaramanga# %SYS-5-CONFIG\_I: Configured from console by console



Ilustración 59

Figura: 59

 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

**!!CUIDADO ACCESO ASEGURADO!!** 

User Access Verification

Password:

Sbucaramanga>en

Sassword:

Sbucaramanga#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Sbucaramanga(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

Sbucaramanga(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

Sbucaramanga(config)#int f0/0.10

Sbucaramanga(config-subif)#ip access-group 112 in

Sbucaramanga(config-subif)#end

Sbucaramanga#

%SYS-5-CONFIG\_I: Configured from console by console



llustración 60

• Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

Sbucaramanga#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Sbucaramanga(config)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63 Sbucaramanga(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0

0.0.0.63

Sbucaramanga(config)#access-list 113 permit ip any any

Sbucaramanga (config)#int f0/0.10

Sbucaramanga(config-subif)#ip access-group 113 out

Sbucaramanga(config-subif)#end

Sbucaramanga#

%SYS-5-CONFIG\_I: Configured from console by console

Stunja#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Stunja(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63 Stunja(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63 Stunja(config)#access-list 113 permit ip any any Stunja(config)#int f0/0.20 Stunja(config-subif)#ip access-group 113 out Stunja (config-subif)#end Stunja# %SYS-5-CONFIG\_I: Configured from console by console

!!CUIDADO ACCESO ASEGURADO!!

User Access Verification

Password:

Scundinamarca>en

Password:

Scundinamarca#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Scundinamarca(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

Scundinamarca(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63

Scundinamarca(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

Scundinamarca(config)#access-list 113 permit ip any any

Scundinamarca(config)#int f0/0.20

Scundinamarca(config-subif)#ip access-group 113 out

Scundinamarca(config-subif)#end

## Scundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console



### llustración 61



Ilustración 62



llustración 63

 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

## SBUCARAMANGA#conf t

Enter configuration commands, one per line. End with CNTL/Z. SBUCARAMANGA(config)#access-list 3 permit 172.31.2.0 0.0.0.7 SBUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7 SBUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7 SBUCARAMANGA(config)#line vty 0 15 SBUCARAMANGA(config-line)#access-class 3 in SBUCARAMANGA(config-line)#end SBUCARAMANGA# %SYS-5-CONFIG\_I: Configured from console by console

STUNJA#conf t

Enter configuration commands, one per line. End with CNTL/Z. STUNJA (config)#access-list 3 permit 172.31.2.0 0.0.0.7 STUNJA (config)#access-list 3 permit 172.3.2.8 0.0.0.7 STUNJA (config)#access-list 3 permit 172.31.2.8 0.0.0.7 STUNJA (config)#line vty 0 15 STUNJA (config-line)#access-class 3 in STUNJA (config-line)#end STUNJA# %SYS-5-CONFIG\_I: Configured from console by console

Scundinamarca#conf t Enter configuration commands, one per line. End with CNTL/Z. Scundinamarca (config)#access-list 3 permit 172.31.2.0 0.0.0.7 Scundinamarca (config)#access-list 3 permit 172.3.2.8 0.0.0.7 Scundinamarca (config)#access-list 3 permit 172.31.2.8 0.0.0.7 Scundinamarca (config)#line vty 0 15 Scundinamarca (config-line)#access-class 3 in Scundinamarca (config-line)#end Scundinamarca#

%SYS-5-CONFIG\_I: Configured from console by console

💐 SwitchTunja				-		×
Physical Config	CLI					
	I	OS Command Lir	ne Interface			
%LINK-5-CHANGED: In	terface	FastEthernet0/1, ch	anged state to up			^
%LINEPROTO-5-UPDOWN up	I: Line ;	protocol on Interface	FastEthernet0/1,	changed	state to	
%LINK-5-CHANGED: In	terface	FastEthernet0/2, cha	anged state to up			
<pre>%LINEPROTO-5-UPDOWN up</pre>	I: Line ;	protocol on Interface	<pre>FastEthernet0/2,</pre>	changed	state to	
%LINK-5-CHANGED: In	terface	FastEthernet0/3, ch	anged state to up			
%LINEPROTO-5-UPDOWN up	I: Line :	protocol on Interface	a FastEthernet0/3,	changed	state to	
STUNJA>en STUNJA‡telnet 172.3 Trying 172.31.2.9 .	31.2.9 Open2	dvertencia Acceso re	stringido			
User Access Verific	ation					
Username: Administr Password:	ador					
l lustración 64						
💐 SwitchBUCARAMAN	IGA		_		_	
Physical Config	CLI					
		IOS Command	Line Interfac	e		
SBUCARAMANGA‡en SBUCARAMANGA‡telr	net 172.	31.2.1	Destringido			

User Access Verification Username: Administrador

Password:

Ilustración 65

×

## CONCLUSIONES

- Se logro identificar la topologia de red y su configuración lógica.
- Se impemento asignación de direccionamiento estatico y dinamico.
- Se geneo comprobaciój d e la red mediante los commandos, ping, telnet entre otros.
- Se genereo protocolos de enrutamiento RIP, EIGRP entre otros.
- Se genero autenticaciónd e accesos a los diferentes dispositivos.
- Se aplico asignación de VLANS entre otras arquitecturas de red.
- Se configure cada uno de los dispositivos generando las soluciones de cada escenario.
- Se realizaron las configuraciones por terminales de manera adecuada a los probelmas establecidos.
- Se configure cada uno de los escenarios permitiendo tener conectividad requerida en cada uno de los puntos de red.
- Se aplico seguridad a los dispositivos de manera óptima y eficiente.
- Se realizo la administración de las redes

## BIBLIOGRAFIAS

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://staticcourseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Temática: OSPF de una sola área

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://staticcourseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y

Conmutación. Recuperado de https://staticcourseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

Temática: DHCP

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-

assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Temática: Conceptos de Routing

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación.

Recuperado de https://static-course-

assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

Temática: Enrutamiento entre VLANs

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://staticcourseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1