SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

DIEGO JAVIER GUTIERREZ BERNAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
BOGOTÁ
2020

SOLUCIÓN DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

DIEGO JAVIER GUTIERREZ BERNAL

Diplomado de opción de grado presentado para optar el título de INGENIERO DE SISTEMAS

DIRECTOR:
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE SISTEMAS
BOGOTÁ
2020

TABLA DE CONTENIDO

TABLA DE CONTENIDO 3
INTRODUCCIÓN 4
DESARROLLO 5
Escenario 1 5
Escenario 2 31
CONCLUSIONES 84
REFERENCIAS BIBLIOGRÁFICAS 85
ANEXOS 86

INTRODUCCIÓN

En el presente trabajo se identificara el desarrollo e implementación de todos los conocimientos adquiridos mediante las actividades realizadas a lo largo del curso, entre algunas de las herramientas utilizadas están los aplicativos GNS3 o Packet Tracer según lo necesite los escenarios planteados, comandos y posteriores demostraciones en los informes presentados y a evaluar.

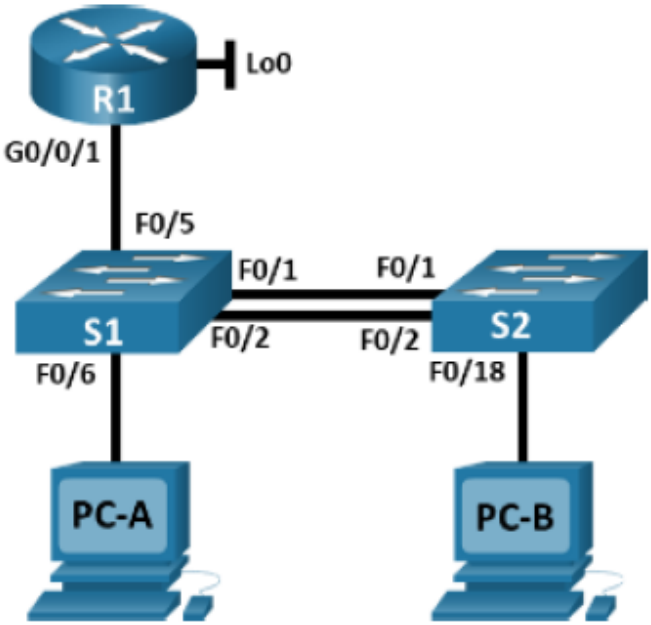
En cuanto al primer escenario, estableceremos el desarrollo de las configuraciones tanto de elementos de una red como lo son equipos, router y switch con conexiones IPv4 e IPv6 mediante la configuración de enrutamientos DHCP, VLAN y demás

Finalmente, en el segundo escenario mediante el uso de conexiones IPv4 e IPv6 con los elementos anteriormente mencionados emplearemos el uso de configuración de estos mediante comandos para el uso de protocolos, seguridad, direcciones dinámicas entre otros.

DESARROLLO

Escenario 1

Topología



En este primer escenario se configurarán los dispositivos de una red pequeña. Debe configurar un router, un switch y equipos que admitan tanto la conectividad IPv4 como IPv6 para los hosts soportados. El router y el switch también deben administrarse de forma segura. Configurará el enrutamiento entre VLAN, DHCP, Etherchannel y port-security.

Tabla de VLAN

VLAN	Nombre de la VLAN
2	Bikes
3	Trikes
4	Management
5	Parking
6	Native

Tabla de asignación de direcciones

Dispositivo / interfaz	Dirección IP / Prefijo	Puerta de enlace predeterminada
R1 G0/0/1.2	10.19.8.1 /26	No corresponde
	2001:db8:acad:a: :1 /64	No corresponde
R1 G0/0/1.3	10.19.8.65 /27	No corresponde
	2001:db8:acad:b: :1 /64	No corresponde
R1 G0/0/1.4	10.19.8.97 /29	No corresponde
	2001:db8:acad:c: :1 /64	No corresponde
R1 G0/0/1.6	No corresponde	No corresponde
R1 Loopback0	209.165.201.1 /27	No corresponde
	2001:db8:acad:209: :1 /64	No corresponde
S1 VLAN 4	10.19.8.98 /29	10.19.8.97
	2001:db8:acad:c: :98 /64	No corresponde
	fe80: :98	No corresponde
S2 VLAN 4	10.19.8.99 /29	10.19.8.97
	2001:db8:acad:c: :99 /64	No corresponde
	fe80: :99	No corresponde
PC-A NIC	Dirección DHCP para IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:a: :50 /64	fe80::1
PC-B NIC	DHCP para dirección IPv4	DHCP para puerta de enlace predeterminada IPv4
	2001:db8:acad:b: :50 /64	fe80::1

Nota: No hay ninguna interfaz en el router que admita VLAN 5.

Instrucciones

Parte 1: Inicializar y Recargar y Configurar aspectos básicos de los dispositivos

Paso 1: Inicializar y volver a cargar el router y el switch

- Borre las configuraciones de inicio y las VLAN del router y del switch y vuelva a cargar los dispositivos. Procedimiento realizado en el router 1

```
Router>enable
Router# delete vlan.data
Delete filename [vlan.data]?
Delete flash:/vlan.data? [confirm]
%Error deleting flash:/vlan.data (No such file or directory)

Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC
disabled
```

Procedimiento realizado en el switch 1

```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 0010.11B5.2B08
Xmodem file system is available.
```

Procedimiento realizado en el switch 2

```
Switch>enable
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
3560-24PS starting...
Base ethernet MAC Address: 0010.11B5.2B08
Xmodem file system is available.
```

Después de recargar el switch, configure la plantilla SDM para que admita IPv6 según sea necesario y vuelva a cargar el switch. Procedimiento realizado en el switch 1.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer ?
  access              Access bias
  default             Default bias
  dual-ipv4-and-ipv6  Support both IPv4 and IPv6
  routing             Unicast bias
  vlan                Vlan bias
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot
take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
```

Procedimiento realizado en el switch 2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#sdm prefer ?
  access              Access bias
  default             Default bias
  dual-ipv4-and-ipv6  Support both IPv4 and IPv6
  routing             Unicast bias
  vlan                Vlan bias
Switch(config)#sdm prefer dual-ipv4-and-ipv6 routing
Changes to the running SDM preferences have been stored, but cannot
take effect until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.
Switch(config)#do reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C3560 Boot Loader (C3560-HBOOT-M) Version 12.2(25r)SEC, RELEASE
SOFTWARE (fc4)
cisco WS-C3560-24PS (PowerPC405) processor (revision P0) with
122880K/8184K bytes of memory.
```

Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Desactivar la búsqueda DNS	*No ip domain-lookup*
Nombre del router	R1
Nombre de dominio	ccna-lab.com
Contraseña cifrada para el modo EXEC privilegiado	ciscoenpass
Contraseña de acceso a la consola	ciscoconpass
Establecer la longitud mínima para las contraseñas	10 caracteres
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**

Tarea	Especificación
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	*line vty 0 4* *login local*
Configurar VTY solo aceptando SSH	*transport input ssh*
Cifrar las contraseñas de texto no cifrado	*service password-encryption*
Configure un MOTD Banner	*banner motd "SOLO PERSONAL CAPACITADO"*
Habilitar el routing IPv6	*ipv6 unicast routing*
Configurar interfaz G0/0/1 y subinterfaces	Establezca la descripción Establece la dirección IPv4. Establezca la dirección local de enlace IPv6 como **fe80: :1** Establece la dirección IPv6. Activar la interfaz.
Configure el Loopback0 interface	Establezca la descripción Establece la dirección IPv4. Establece la dirección IPv6. Establezca la dirección local de enlace IPv6 como **fe80::1**
Generar una clave de cifrado RSA	Módulo de 1024 bits

Configuraciones básicas router1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#ip domain-name ccna-lab.com
R1(config)#enable secret ciscoenpass
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit
R1(config)#security password min-length 10
R1(config)#username admin privilege 15 secret admin1pass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "SOLO PERSONAL CAPACITADO"
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
```

Configuración interfaces y subinterfaces IPv4 e IPv6 y verificación de configuraciones iniciales y seguridad

```
SOLO PERSONAL CAPACITADO

User Access Verification

Password:

R1>enable
Password:
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface g0/1
R1(config-if)# int g0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)# int g0/1.3
```

```
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)# int g0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)# int g0/1.6
R1(config-subif)#encapsulation dot1Q 6
R1(config-subif)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface g0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.2,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.3,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.4,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.6,
changed state to up

R1(config-if)#
```

Configuración del Loopback0

```
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up

R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown
R1(config-if)#exit
```

Generación de una clave de cifrado rsa cisco

```
R1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:45:23.561: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
```

Paso 3: Configure S1 y S2.
Las tareas de configuración incluyen lo siguiente:

Tarea	Especificación
Desactivar la búsqueda DNS.	
Nombre del switch	**S1 o S2, según proceda**
Nombre de dominio	**ccna-lab.com**
Contraseña cifrada para el modo EXEC privilegiado	**ciscoenpass**
Contraseña de acceso a la consola	**ciscoconpass**
Crear un usuario administrativo en la base de datos local	Nombre de usuario: **admin** Password: **admin1pass**
Configurar el inicio de sesión en las líneas VTY para que use la base de datos local	

Tarea	Especificación
Configurar las líneas VTY para que acepten únicamente las conexiones SSH	
Cifrar las contraseñas de texto no cifrado	
Configurar un MOTD Banner	
Generar una clave de cifrado RSA	**Módulo de 1024 bits**
Configurar la interfaz de administración (SVI)	Establecer la dirección IPv4 de capa 3 Establezca la dirección local de enlace IPv6 como **FE80: :98 para S1 y FE80: :99 para S2** Establecer la dirección IPv6 de capa 3
Configuración del gateway predeterminado	Configure la puerta de enlace predeterminada como 10.19.8.97 para IPv4

Configuración básica S1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#ip domain-name ccna-lab.com
S1(config)#enable secret ciscoenpass
S1(config)#line con 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit
S1(config)#username admin privilege 15 secret admin1pass
S1(config)#line vty 0 4
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "SOLO PERSONAL CAPACITADO"
S1(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:10:19.629: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

Configuración básica S2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S2
S2(config)#ip domain-name ccna-lab.com
S2(config)#enable secret ciscoenpass
S2(config)#line con 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit
S2(config)#username admin privilege 15 secret admin1pass
S2(config)#line vty 0 4
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#banner motd "SOLO PERSONAL CAPACITADO"
S2(config)#crypto key generate rsa general-key modulus 1024
The name for the keys will be: S2.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:14:49.317: %SSH-5-ENABLED: SSH 1.99 has been enabled
S2(config)#
```

Configuración VLAN 4 S1

```
Press RETURN to get started!

SOLO PERSONAL CAPACITADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ipv6 unicast-routing
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#ipv6 address 2001:db8:acad:c::98/64
S1(config-if)#ipv6 address fe80::98 link-local
S1(config-if)#exit
S1(config)#ip default-gateway 10.19.8.97
```

Configuración VLAN 4 S2

```
Press RETURN to get started!

SOLO PERSONAL CAPACITADO

User Access Verification

Password:

S2>enable
Password:
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ipv6 unicast-routing
S2(config)#interface vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#ipv6 address 2001:db8:acad:c::99/64
S2(config-if)#ipv6 address fe80::99 link-local
S2(config-if)#exit
S2(config)#ip default-gateway 10.19.8.97
S2(config)#no shutdown
```

Parte 2: Configuración de la infraestructura de red (VLAN, Trunking, EtherChannel)

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tarea	Especificación
Crear VLAN	VLAN 2, nombre Bikes VLAN 3, nombre Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1, F0/2 y F0/5
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso de host para VLAN 2	Interface F0/6

Tarea	Especificación
Configurar la seguridad del puerto en los puertos de acceso	Permitir 3 direcciones MAC
Proteja todas las interfaces no utilizadas	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Creación nombres VLAN's S1

```
SOLO PERSONAL CAPACITADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#exit
S1(config)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#exit
S1(config)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#exit
S1(config)#vlan 6
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#exit
S1#
```

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
2    Bikes                             active
3    Trikes                            active
4    Management                        active
5    Parking                           active
6    Native                            active
```

Configuración “trunk” 802.1Q que utilicen la VLAN 6 nativa

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state
to up


S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/2
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#exit
```

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/5
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#exit
S1(config)#exit
```

Comprobación de configuración y uso de VLAN 6 “Nativa”

```
S1#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none
S1#
S1#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none

S1#show interface f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S1#
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#
Creating a port-channel interface Port-channel 1
S1(config-if-range)#exit
S1(config)#interface port-channel 1
S1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto"
can not be configured to "trunk" mode.
S1(config-if)#switchport trunk encapsulation dot1Q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit
S1(config)#exit
```

Configurar el puerto de acceso de host para VLAN 2

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1(config)#exit
S1#


S1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
--------------------------------
1    default                          active    Po1, Fa0/1, Fa0/2,
Fa0/3
                                               Fa0/4, Fa0/7, Fa0/8,
Fa0/9
                                               Fa0/10, Fa0/11,
Fa0/12, Fa0/13
                                               Fa0/14, Fa0/15,
Fa0/16, Fa0/17
                                               Fa0/18, Fa0/19,
Fa0/20, Fa0/21
                                               Fa0/22, Fa0/23,
Fa0/24, Gig0/1
                                               Gig0/2
2    bikes                            active    Fa0/6
3    Trikes                           active
4    Management                       active
5    Parking                          active
6    Native                           active
```

Configurar la seguridad del puerto en los puertos de acceso

```
S1#
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#exit
S1(config)#exit
S1#
```

Proteja todas las interfaces no utilizadas

```
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range g0/1-2, f0/3-4, f0/7-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#shutdown
S1(config-if-range)#switchport port-security
S1(config-if-range)#switchport port-security violation shutdown
S1(config-if-range)#exit
S1(config)#exit
```

Paso 5: Configure el S2.
Entre las tareas de configuración de S2 se incluyen las siguientes:

Tarea	Especificación
Crear VLAN	VLAN 2, name Bikes VLAN 3, name Trikes VLAN 4, name Management VLAN 5, nombre Parking VLAN 6, nombre Native
Crear troncos 802.1Q que utilicen la VLAN 6 nativa	Interfaces F0/1 y F0/2
Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2	Usar el protocolo LACP para la negociación
Configurar el puerto de acceso del host para la VLAN 3	Interfaz F0/18
Configure port-security en los access ports	permite 3 MAC addresses
Asegure todas las interfaces no utilizadas.	Asignar a VLAN 5, Establecer en modo de acceso, agregar una descripción y apagar

Creación nombres VLAN's S2

```
SOLO PERSONAL CAPACITADO

User Access Verification

Password:

S2>enable
Password:
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#exit
S2(config)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#exit
```

```
S2(config)#vlan 4
S2(config-vlan)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state
to up

S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#exit
S2(config)#vlan 6
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#exit


S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
--------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5,
Fa0/6
                                               Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                               Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                               Fa0/15, Fa0/16,
Fa0/17, Fa0/18
                                               Fa0/19, Fa0/20,
Fa0/21, Fa0/22
                                               Fa0/23, Fa0/24,
Gig0/1, Gig0/2
2    Bikes                            active
3    Trikes                           active
4    Management                       active
5    Parking                          active
6    Native                           active
```

Configuración “trunk” 802.1Q que utilicen la VLAN 6 nativa

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#exit
```

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/2
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 6
S2(config-if)#exit
S2(config)#exit
S2#
```

Comprobación de configuración y uso de VLAN 6 “Nativa”

```
S2#show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none

S2#show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 6 (Native)
Voice VLAN: none
```

Crear un grupo de puertos EtherChannel de Capa 2 que use interfaces F0/1 y F0/2

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#
Creating a port-channel interface Port-channel 1
S2(config-if-range)#exit
S2(config)#interface port-channel 1
S2(config-if)#switchport trunk encapsulation dot1Q
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if)#exit
S2(config)#exit
```

Configurar el puerto de acceso de host para VLAN 3

```
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 3
S2(config-if)#exit
S2(config)#exit
S2#

S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
--------------------------------
1    default                          active    Po1, Fa0/1, Fa0/2,
Fa0/3
                                               Fa0/4, Fa0/5, Fa0/6,
Fa0/7
                                               Fa0/8, Fa0/9, Fa0/10,
Fa0/11
                                               Fa0/12, Fa0/13,
Fa0/14, Fa0/15
                                               Fa0/16, Fa0/17,
Fa0/19, Fa0/20
                                               Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                               Gig0/1, Gig0/2
2    Bikes                            active
3    Trikes                           active    Fa0/18
4    Management                       active
5    Parking                          active
6    Native                           active
```

Configurar la seguridad del puerto en los puertos de acceso

```
S2>enable
Password:
Password:
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 3
S2(config-if)#switchport port-security violation shutdown
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#exit
S2#
```

Proteja todas las interfaces no utilizadas

```
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface range g0/1-2, f0/3-4, f0/7-24
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#shutdown
S2(config-if-range)#switchport port-security
S2(config-if-range)#switchport port-security violation shutdown
S2(config-if-range)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
```

Parte 2: Configurar soporte de host

Paso 1: Configure R1

Las tareas de configuración para R1 incluyen las siguientes:

Tarea	Especificación
Configure Default Routing	Crear rutas predeterminadas para IPv4 e IPv6 que dirijan el tráfico a la interfaz Loopback 0
Configurar IPv4 DHCP para VLAN 2	Cree un grupo DHCP para VLAN 2, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-a.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada
Configurar DHCP IPv4 para VLAN 3	Cree un grupo DHCP para VLAN 3, compuesto por las últimas 10 direcciones de la subred solamente. Asigne el nombre de dominio ccna-b.net y especifique la dirección de la puerta de enlace predeterminada como dirección de interfaz del router para la subred involucrada

Configuración IPv4 DHCP para Vlan2

```
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool vlan2
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#ip dhcp excluded-address 10.19.8.2 10.19.8.51
R1(config)#
```

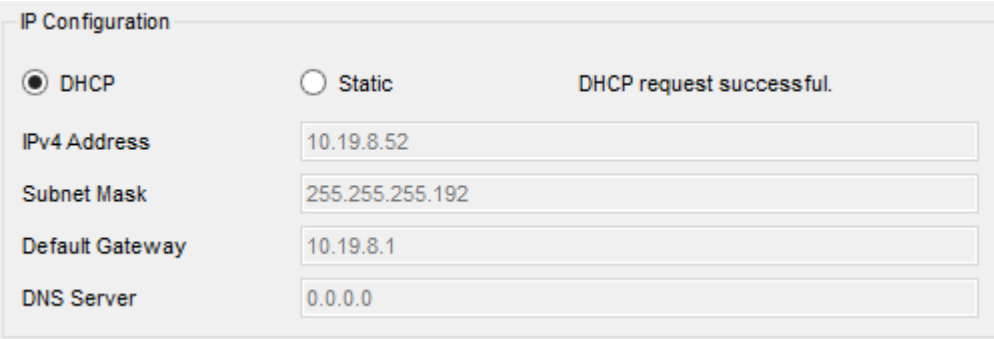
Configuración IPv4 DHCP para Vlan3

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool vlan3
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#ip dhcp excluded-address 10.19.8.66 10.19.8.83
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Paso 2: Configurar los servidores

Configure los equipos host PC-A y PC-B para que utilicen DHCP para IPv4 y asigne estáticamente las direcciones IPv6 GUA y Link Local. Después de configurar cada servidor, registre las configuraciones de red del host con el comando ipconfig /all.

Configuración de red de PC-A	
Descripción	Mediante el uso de **"ipconfig /all"**
Dirección física	0002.16D2.0162
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1




```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: ccna-a.net
   Physical Address................: 0002.16D2.0162
   Link-local IPv6 Address.........: FE80::202:16FF:FED2:162
   IPv6 Address....................: 2001:DB8:ACAD:A::50
   IPv4 Address....................: 10.19.8.52
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: FE80::1
                                     10.19.8.1
   DHCP Servers....................: 10.19.8.1
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-
E8-59-4B-3C-00-02-16-D2-01-62
```

Configuración de red de PC-B	
Descripción	Mediante el uso de **“ipconfig /all”**
Dirección física	0002.16D2.0162
Dirección IP	10.19.8.52
Máscara de subred	255.255.255.192
Gateway predeterminado	10.19.8.1
Gateway predeterminado IPv6	FE80::1

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: ccna-b.net
   Physical Address.....: 00D0.D348.7E22
   Link-local IPv6 Address.....: FE80::2D0:D3FF:FE48:7E22
   IPv6 Address.....: 2001:DB8:ACAD:B::50
   IPv4 Address.....: 10.19.8.84
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: FE80::1
                         10.19.8.65
   DHCP Servers.....: 0.0.0.0
   DHCPv6 IAID.....:
   DHCPv6 Client DUID.....: 00-01-00-01-42-07-DA-3E-00-D0-
D3-48-7E-22
```

Parte 3: Probar y verificar la conectividad de extremo a extremo

Use el comando ping para probar la conectividad IPv4 e IPv6 entre todos los dispositivos de red.

Nota: Si fallan los pings en las computadoras host, desactive temporalmente el firewall de la computadora y vuelva a realizar la prueba.

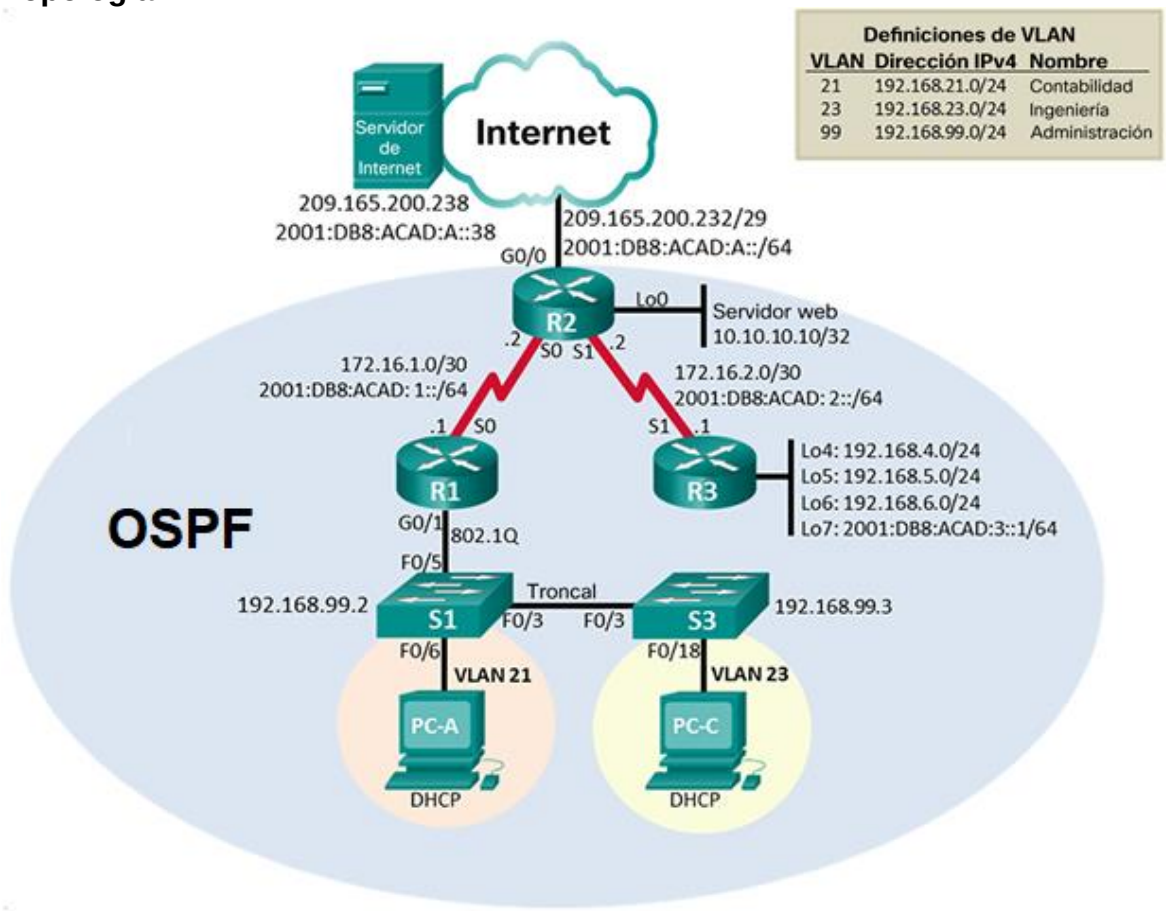
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	de Internet	Dirección IP	Resultados de ping
PC-A	R1, G0/0/1.2	Dirección	10.19.8.1	Afirmativo
		IPv6	2001:db8:acad:a: :1	Afirmativo
	R1, G0/0/1.3	Dirección	10.19.8.65	Afirmativo
		IPv6	2001:db8:acad:b: :1	Afirmativo
	R1, G0/0/1.4	Dirección	10.19.8.97	Afirmativo
		IPv6	2001:db8:acad:c: :1	Afirmativo
	S1, VLAN 4	Dirección	10.19.8.98	Afirmativo
		IPv6	2001:db8:acad:c: :98	Negativo
	S2, VLAN 4	Dirección	10.19.8.99.	Afirmativo
		IPv6	2001:db8:acad:c: :99	Negativo

Desde	A	de Internet	Dirección IP	Resultados de ping
	PC-B	Dirección	IP address will vary.	Negativo
		IPv6	2001:db8:acad:b: :50	Negativo
	R1 Bucle 0	Dirección	209.165.201.1	Afirmativo
		IPv6	2001:db8:acad:209: :1	Afirmativo
PC-B	R1 Bucle 0	Dirección	209.165.201.1	Afirmativo
		IPv6	2001:db8:acad:209: :1	Afirmativo
	R1, G0/0/1.2	Dirección	10.19.8.1	Afirmativo
		IPv6	2001:db8:acad:a: :1	Afirmativo
	R1, G0/0/1.3	Dirección	10.19.8.65	Afirmativo
		IPv6	2001:db8:acad:b: :1	Afirmativo
	R1, G0/0/1.4	Dirección	10.19.8.97	Afirmativo
		IPv6	2001:db8:acad:c: :1	Afirmativo
	S1, VLAN 4	Dirección	10.19.8.98	Afirmativo
		IPv6	2001:db8:acad:c: :98	Negativo
	S2, VLAN 4	Dirección	10.19.8.99.	Afirmativo
		IPv6	2001:db8:acad:c: :99	Negativo

Escenario 2

Topología



Parte 1: Inicializar dispositivos

Paso 1: Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router# erase startup-config
Volver a cargar todos los routers	Router#reload

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch>enable Switch# erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show vlan

Eliminar el archivo startup-config de todos los routers,

Router 1

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Router 2

```
Router>enable
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Router 3

```
Router>enable
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

Volver a cargar todos los routers

Router 1

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################
##### [OK]
```

Router 2

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################
```

Router 3

```
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC
disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################
##### [OK]
```

Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior

Switch 1

```
Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00E0.8F96.8946
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
###########################################################################
##### [OK]
```

Switch 3

```
Switch>enable
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 00E0.F72E.A136
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.

Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4


Loading "flash:/c2960-lanbase-mz.122-25.FX.bin"...
################################################################################
```

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches

Switch 1

```
Switch>enable
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

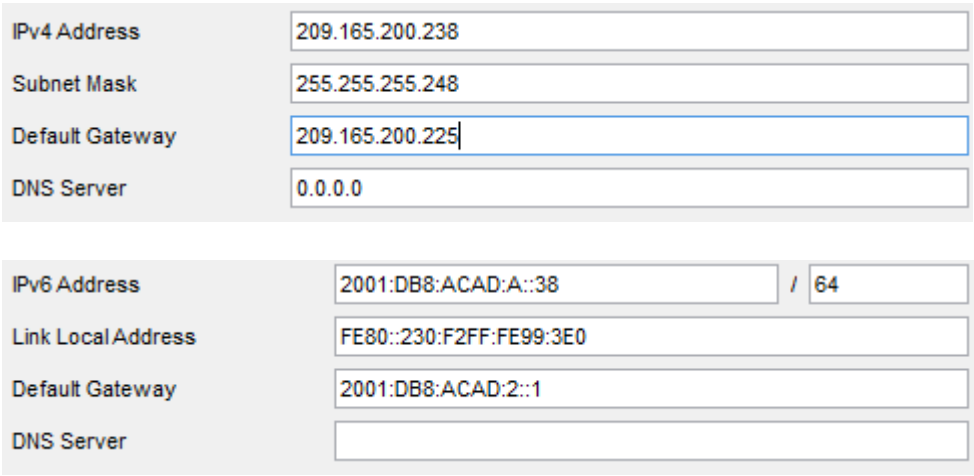
Switch 3

```
Switch>enable
Switch# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                 Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Parte 2: Configurar los parámetros básicos de los dispositivos
Paso 1: Configurar la computadora de Internet
Las tareas de configuración del servidor de Internet incluyen lo siguiente (para obtener información de las direcciones IP, consulte la topología):

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1



Paso 2: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco

Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Configuraciones router 1

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "SE PROHIBE EL ACCESO NO AUTORIZADO"
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

Configuraciones interfaz y rutas router 1, verificación configuración anterior

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ipv6 unicast-routing
R1(config)#interface s0/0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface,
may impact performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Habilitar el servidor HTTP	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz
Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la dirección IPv4.
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0.

Configuraciones router 2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#ip http server
R2(config)#service password-encryption
R2(config)#banner motd "SE PROHIBE EL ACCESO NO AUTORIZADO"
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

Configuraciones interfaz y rutas router 1, verificación configuración anterior en la interfaz S0/0/0

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#interface s0/0/0
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
```

Interfaz S0/0/1

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface s0/0/1
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if)#
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Interfaz G0/0 (simulación de Internet)

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#interface g0/0
R2(config-if)#ip address 209.165.200.238 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
```

Interfaz loopback 0 (servidor web simulado)

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up

R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Ruta predeterminada

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface,
may impact performance
R2(config)#ipv6 route ::/0 g0/0
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

Paso 4: Configurar R3
La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	R3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Configuraciones router 3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd "SE PROHIBE EL ACCESO NO AUTORIZADO"
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Configuraciones interfaz y rutas router 1, verificación configuración anterior en la interfaz S0/0/1

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#interface s0/0/1
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

R3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to up
```

Interfaz loopback 4

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface loopback 4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed
state to up

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Interfaz loopback 5

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface loopback 5

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed
state to up

R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Interfaz loopback 6

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface loopback 6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed
state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Interfaz loopback 7

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# interface loopback 7

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed
state to up

R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Rutas predeterminadas

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface,
may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#exit
```

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S1
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "SE PROHIBE EL ACCESO NO AUTORIZADO"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	
Mensaje MOTD	Se prohíbe el acceso no autorizado.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd "SE PROHIBE EL ACCESO NO AUTORIZADO"
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Paso 7: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0		Afirmativo
R2	R3, S0/0/1		Afirmativo
PC de Internet	Gateway predeterminado		Afirmativo

Desde R1 a R2

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
```

Desde R2 a R3

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/5 ms
```

Desde PC de Internet (Server web) a Gateway predeterminado

```
C:\>ping 209.165.200.238

Pinging 209.165.200.238 with 32 bytes of data:

Reply from 209.165.200.238: bytes=32 time<1ms TTL=128
Reply from 209.165.200.238: bytes=32 time=5ms TTL=128
Reply from 209.165.200.238: bytes=32 time=5ms TTL=128
Reply from 209.165.200.238: bytes=32 time<1ms TTL=128

Ping statistics for 209.165.200.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 2ms
```

Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN
Paso 1: Configurar S1
La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.

Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	
Apagar todos los puertos sin usar	

Crear la base de datos de VLAN

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 21
S1(config-vlan)#name Contabilidad
S1(config-vlan)#exit
S1(config)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#exit
S1(config)#vlan 99
S1(config-vlan)#name Administracion
S1(config-vlan)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Asignar la dirección IP de administración.

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#exit
S1(config)#exit
S1#
```

Asignar el gateway predeterminado

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.99.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

Forzar el enlace troncal en la interfaz F0/3

```
S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state
to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#exit
S1#
```

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Forzar el enlace troncal en la interfaz F0/5

```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit


SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#show interface f0/5 switchport
Name: Fa0/5
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Configurar el resto de los puertos como puertos de acceso

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range g0/1-2, f0/1-2, f0/4, f0/6-24
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
```

Asignar F0/6 a la VLAN 21

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#exit
```

Apagar todos los puertos sin usar

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range g0/1-2, f0/1-2, f0/4, f0/7-24
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down
```

Paso 2: Configurar el S3
La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 23	
Apagar todos los puertos sin usar	

Crear la base de datos de VLAN

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S3>enable
Password:
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#exit
S3(config)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#exit
S3(config)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Asignar la dirección IP de administración

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S3>enable
Password:
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state
to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Asignar el gateway predeterminado.

```
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#ip default-gateway 192.168.99.1
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Forzar el enlace troncal en la interfaz F0/3

```
S3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

```
S3#show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Configurar el resto de los puertos como puertos de acceso

```
S3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface range g0/1-2, f0/1-2, f0/4-24
S3(config-if-range)#switchport mode access
S3(config-if-range)#exit
```

Asignar F0/18 a la VLAN 23

```
S3(config)#interface f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#exit
```

Apagar todos los puertos sin usar

```
S3(config)#interface range g0/1-2, f0/1-2, f0/4-17, f0/19-24
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to
administratively down

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

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

Paso 3: Configurar R1
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	

Configurar la subinterfaz 802.1Q .21 en G0/1

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1.21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Configurar la subinterfaz 802.1Q .23 en G0/1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1.23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Configurar la subinterfaz 802.1Q .99 en G0/1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1.99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Activar la interfaz G0/1

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.21, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.23, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.99, changed state to up
```

Paso 4: Verificar la conectividad de la red

Utilice el comando ping para probar la conectividad entre los switches y el R1.

Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99		Afirmativo
S3	R1, dirección VLAN 99		Afirmativo
S1	R1, dirección VLAN 21		Afirmativo
S3	R1, dirección VLAN 23		Afirmativo

Desde S1 a R1 Vlan 99

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S1>enable
Password:
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Desde S3 a R1 Vlan 99

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

S3>enable
Password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Desde S1 a R1 Vlan 21

```
S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Desde S3 a R1 Vlan 23

```
S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

Parte 4: Configurar el protocolo de routing dinámico OSPF
Paso 1: Configurar OSPF en el R1
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	

Configuración OSPF área 0

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router ospf 10
R1(config-router)#router-id 1.1.1.1
```

Anunciar las redes conectadas directamente

```
R1(config-router)#network 192.168.99.1 0.0.0.0 area 0
R1(config-router)#network 192.168.23.1 0.0.0.0 area 0
R1(config-router)#network 192.168.21.1 0.0.0.0 area 0
R1(config-router)#network 172.16.1.1 0.0.0.3 area 0
```

Establecer todas las interfaces LAN como pasivas

```
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
```

Configuración OSPFv3 EN R1

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router ospf 10
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#interface s0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#ipv6 ospf 10 area 0
R1(config-if)#exit
```

Paso 2: Configurar OSPF en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Configurar OSPF área 0

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router ospf 10
R2(config-router)#router-id 2.2.2.2
```

Anunciar las redes conectadas directamente

```
R2(config-router)#network 172.16.1.0 0.0.0.3 area 0
R2(config-router)#
02:29:19: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
```

Establecer la interfaz LAN (loopback) como pasiva

```
R2(config-router)#passive-interface loopback 0
```

Configuración OSPFv3 en R2

```
User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ipv6 unicast-routing
R2(config)#interface g0/0
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ipv6 address FE80::2 link-local
R2(config-if)#exit
R2(config)#ipv6 router ospf 10
R2(config-rtr)#router-id 2.2.2.2
R2(config-rtr)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all
routers.
R2(config-rtr)#exit
R2(config)#interface g0/0
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exo
03:12:02: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on Serial0/0/0
from LOADING to FULL, Loading Do
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ipv6 ospf 10 area 0
R2(config-if)#exit
R2(config)#exit
```

Paso 3: Configurar OSPF en el R3
La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar OSPF área 0	
Anunciar redes IPv4 conectadas directamente	
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	
Desactive la sumarización automática.	

Configurar OSPF área 0

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router ospf 10
R3(config-router)#router-id 3.3.3.3
```

Anunciar redes IPv4 conectadas directamente

```
R3(config-router)#network 172.16.2.0 0.0.0.3 area 0
R3(config-router)#
03:19:57: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1 from
LOADING to FULL, Loading Done

R3(config-router)#network 192.168.4.1 0.0.0.0 area 0
R3(config-router)#network 192.168.5.1 0.0.0.0 area 0
R3(config-router)#network 192.168.6.1 0.0.0.0 area 0
```

Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas

```
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
```

Configuración OSPFv3 en R3

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#ipv6 router ospf 10
R3(config-rtr)#router-id 3.3.3.3
R3(config-rtr)#interface s0/0/1
R3(config-if)#ipv6 ospf 10 area 0
R3(config-if)#
03:25:46: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#
03:26:04: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

R3(config-if)#interface loopback 7
R3(config-if)#ipv6 address FE80::3 link-local
R3(config-if)#ipv6 ospf 10 area 0
R3(config-if)#exit
R3(config)#
```

Paso 4: Verificar la información de OSPF

Verifique que OSPF esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso OSPF, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	Show ip protocols
¿Qué comando muestra solo las rutas OSPF?	Show ip route ospf
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Show ip ospf

Comprobación de configuración de procesos OSPF en R1

```
R1#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.99.1 0.0.0.0 area 0
    192.168.23.1 0.0.0.0 area 0
    192.168.21.1 0.0.0.0 area 0
    172.16.1.0 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/1.21
    GigabitEthernet0/1.23
    GigabitEthernet0/1.99
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:08:12
  Distance: (default is 110)
```

Comprobación de configuración de procesos OSPF en R2

```
R2#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.3 area 0
    172.16.2.0 0.0.0.3 area 0
    10.10.10.10 0.0.0.0 area 0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:04:53
    2.2.2.2              110      00:03:52
  Distance: (default is 110)
```

Comprobación de configuración de procesos OSPF en R3

```
R3#show ip protocols

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.2.0 0.0.0.3 area 0
    192.168.4.1 0.0.0.0 area 0
    192.168.5.1 0.0.0.0 area 0
    192.168.6.1 0.0.0.0 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:23:53
    2.2.2.2              110      00:03:25
    3.3.3.3              110      00:02:38
  Distance: (default is 110)
```

Comprobación de rutas OSPF en R1

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/65] via 172.16.1.2, 01:01:29, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.2.0 [110/128] via 172.16.1.2, 01:01:45, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/129] via 172.16.1.2, 00:11:19, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/129] via 172.16.1.2, 00:11:09, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/129] via 172.16.1.2, 00:11:09, Serial0/0/0
```

Comprobación de rutas OSPF en R2

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#show ip route ospf
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/65] via 172.16.2.1, 00:15:00, Serial0/0/1
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/65] via 172.16.2.1, 00:14:50, Serial0/0/1
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/65] via 172.16.2.1, 00:14:50, Serial0/0/1
O    192.168.21.0 [110/65] via 172.16.1.1, 01:06:12, Serial0/0/0
O    192.168.23.0 [110/65] via 172.16.1.1, 01:06:12, Serial0/0/0
O    192.168.99.0 [110/65] via 172.16.1.1, 01:06:12, Serial0/0/0
```

Comprobación de rutas OSPF en R3

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R3>enable
Password:
R3#show ip route ospf
     10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/65] via 172.16.2.2, 00:16:26, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O       172.16.1.0 [110/128] via 172.16.2.2, 00:16:26, Serial0/0/1
O    192.168.21.0 [110/129] via 172.16.2.2, 00:16:26, Serial0/0/1
O    192.168.23.0 [110/129] via 172.16.2.2, 00:16:26, Serial0/0/1
O    192.168.99.0 [110/129] via 172.16.2.2, 00:16:26, Serial0/0/1
```

Comprobación de la sección OSPF en R1

```
R1#show ip ospf
 Routing Process "ospf 10" with ID 1.1.1.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 4
        Area has no authentication
        SPF algorithm executed 12 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00f3bc
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Comprobación de la sección OSPF en R2

```
R2#show ip ospf
 Routing Process "ospf 10" with ID 2.2.2.2
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00f3bc
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Comprobación de la sección OSPF en R3

```
R3#show ip ospf
 Routing Process "ospf 10" with ID 3.3.3.3
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 4
        Area has no authentication
        SPF algorithm executed 5 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x00f3bc
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Parte 5: Implementar DHCP y NAT para IPv4
Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23
Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Reserva de las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
```

Reserva de las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas

```
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
```

Crear un pool de DHCP para la VLAN 21.

```
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#end
R1#
```

Crear un pool de DHCP para la VLAN 23

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#end
R1#
```

Paso 2: Configurar la NAT estática y dinámica en el R2
La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** – **209.165.200.228**
Definir la traducción de NAT dinámica	

Creación de una base de datos local con una cuenta de usuario

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
```

Crear una NAT estática al servidor web.

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#
```

Asignar la interfaz interna y externa para la NAT estática

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface loopback 0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#interface s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#
```

Configuración de la NAT dinámica dentro de una ACL privada

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255
R2(config)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

Defina el pool de direcciones IP públicas utilizables.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
netmask 255.255.255.248
R2(config)#exit
R2#
```

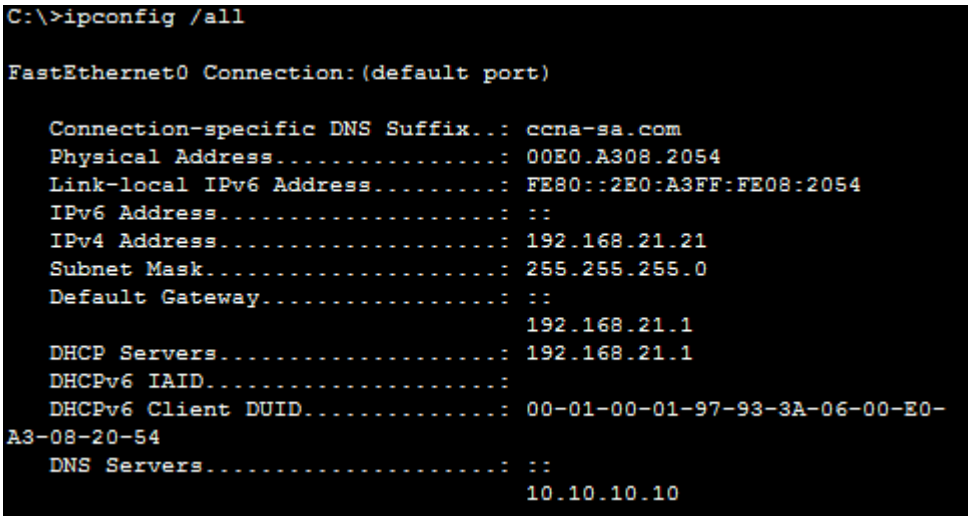
Definir la traducción de NAT dinámica

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#exit
R2#
```

Paso 3: Verificar el protocolo DHCP y la NAT estática
Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Correcto
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Correcto
Verificar que la PC-A pueda hacer ping a la PC-C **Nota:** Quizá sea necesario deshabilitar el firewall de la PC.	Correcto
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**	

Verificar que la PC-A haya adquirido información de IP del servidor de DHCP



Verificar que la PC-C haya adquirido información de IP del servidor de DHCP

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: ccna-sa.com
   Physical Address................: 00E0.8F93.01E5
   Link-local IPv6 Address.........: FE80::2E0:8FFF:FE93:1E5
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.23.21
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.23.1
   DHCP Servers....................: 192.168.23.1
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-A4-65-33-E8-00-
E0-8F-93-01-E5
   DNS Servers.....................: ::
                                     10.10.10.10
```

Verificar que la PC-A pueda hacer ping a la PC-C
Nota: Quizá sea necesario deshabilitar el firewall de la PC.

```
C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time=1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345**

Parte 6: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	**5 de marzo de 2016, 9 a. m.**
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	
Verifique la configuración de NTP en R1.	

Ajuste la fecha y hora en R2.

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#clock set 9:00:00 05 march 2016
R2#
```

Configure R2 como un maestro NTP.

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ntp master 5
```

Configurar R1 como un cliente NTP.

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
```

Configure R1 para actualizaciones de calendario periódicas con hora NTP.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ntp update-calendar
R1(config)#exit
R1#
```

Verifique la configuración de NTP en R1.

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay
offset            disp
*~172.16.1.2    127.127.1.1     5    1        16      3      6.00
2.00              0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

Parte 7: Configurar y verificar las listas de control de acceso (ACL)
Paso 1: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT**
Aplicar la ACL con nombre a las líneas VTY	
Permitir acceso por Telnet a las líneas de VTY	
Verificar que la ACL funcione como se espera	

Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2

```
SE PROHIBE EL ACCESO NO AUTORIZADO

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Aplicar la ACL con nombre a las líneas VTY

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#
```

Permitir acceso por Telnet a las líneas de VTY

```
R2(config-line)#transport input telnet
```

Verificar que la ACL funcione como se espera

```
R1#
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSE PROHIBE EL ACCESO NO AUTORIZADO


User Access Verification


R2#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
```

Paso 2: Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access list
Restablecer los contadores de una lista de acceso	Clear ip access-list counters
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface
¿Con qué comando se muestran las traducciones NAT?	Show ip nat translations **Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red.
¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?	Clear ip nat translation

Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció

```
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255 (2 match(es))
    20 permit 192.168.5.0 0.0.0.255
    30 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))
```

Restablecer los contadores de una lista de acceso

```
R2# clear access-list counters
R2#show access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.5.0 0.0.0.255
    30 permit 192.168.6.0 0.0.0.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1
```

¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?

```
R2#show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
  Internet address is 172.16.1.2/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
```

¿Con qué comando se muestran las traducciones NAT?

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
---  209.165.200.229   10.10.10.10        ---                ---
tcp 209.165.200.225:1025192.168.21.21:1025 209.165.200.229:80
209.165.200.229:80
```

CONCLUSIONES

En el primer escenario, en la topología encontramos que el switch mas utilizado para este tipo de aplicaciones en el entorno “Packet Tracer” es el 2960, pero este no permitía realizar configuraciones hacia las redes IPv6, es por esto que se optó por un router que manejara este tipo de configuración el cual fue el 3560 que admite realizar configuraciones en “dual stack”, manejo de puertos y configuraciones para Vlan.

El uso de subredes, mediante el manejo de Vlan, y el encapsulamiento Dot1Q denota cambios en la configuración básica de los routers y switches utilizados en una red ampliando el número de equipos que queramos manejar implementando modos “trunk” para su comunicación y maximización de utilidad de los elementos a emplear en la red a configurar.

En cuanto al segundo escenario, encontramos algunas de las características ya establecidas en el primero, pero además encontramos los cambios en la comunicación de los equipos hacia servidores y conexiones “HTTP”.

Además se pudo establecer el uso de privilegios, los cuales aumentan la seguridad de acceso a los equipos y su configuración interna y externa, así mismo, la implementación de comandos los cuales fueron demostrando el cambio en la conectividad de los elementos de la red, este los cuales están routers, switches, equipos y hasta servidores web

Finalmente, establecemos que el poder implementar los conocimientos básicos del principio e ir avanzando en las diferentes configuraciones a lo largo del curso, ayudan a cumplir los objetivos que los distintos escenarios propusieron, no solo como colocar comandos y ejecutar sino a poder avanzar que hace cada uno de ellos y cuando poder colocar y su correcto funcionamiento en poder llevar a cabo este tipo de configuraciones a la vida profesional.

REFERENCIAS BIBLIOGRÁFICAS

VESGA, J. Diseño y configuración de redes con Packet Tracer [OVA]. {En línea}. (2014). {25 Noviembre de 2020}. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9

CISCO. "Protocolos y comunicaciones de red. Fundamentos de Networking". {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3

CISCO. "Capa de red. Fundamentos de Networking". {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6

CISCO. "División de redesIP en subredes. Fundamentos de Networking". {En línea}. (2019). {25 Noviembre de 2020}.Disponible en: https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8

UNAD. "Configuración de Switches y Routers [OVA]". {En línea}. (2017). {25 Noviembre de 2020}. Disponible en: https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. "Redes Conmutadas. Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#4

UNAD. "Principios de Enrutamiento [OVA]. {En línea}". (2017). {25 Noviembre de 2020}. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. "VLAN Principios de Enrutamiento y Conmutación". {En línea}. (2019). {25 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#6

CISCO. "Listas de Control de Acceso. Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}. Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#7

CISCO. "DHCP Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}. Disponible en:https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#8

CISCO. "NAT para IPv4. Principios de Enrutamiento y Conmutación". {En línea}. (2019). {27 Noviembre de 2020}.Disponible en: https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#9

ANEXOS

Anexo de los escenarios desarrollados en la aplicación Packet Tracer: https://drive.google.com/drive/folders/1XFX-B6YDOjXL2NON_ePkmvmGleD9dbsH?usp=sharing

Anexo del artículo científico en formato IEEE: https://drive.google.com/drive/folders/1XFX-B6YDOjXL2NON_ePkmvmGleD9dbsH?usp=sharing

Anexo link del video en YouTube: https://youtu.be/B0u1VyAFQQQ