

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

LUIS ALEJANDRO GUZMÁN GUERRERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2021

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

LUIS ALEJANDRO GUZMÁN GUERRERO

DIPLOMADO DE OPCION DE GRADO PRESENTADO PARA OPTAR EL
TITULO DE INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTA
2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 15 de noviembre de 2021

AGRADECIMIENTOS

Como primera medida el principal agradecimiento es para Dios quien me a ha dado la facultad y el conocimiento para elaborar e investigar sobre este proyecto, además deseo dedicar este trabajo a las personas mas importantes en mi vida que son mi pilar y mi más grande motivación (Esposa y mis hijos) quienes día a día me alientan, me dan esa fuerza y resistencia que hace que pueda conseguir mis metas y proyectos.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN	10
DESARROLLO	11
CONCLUSIONES	41
BIBLIOGRAFÍA.....	42

LISTA DE TABLAS

Tabla 1 Direccionamiento	12
Tabla 2 Equipos utilizados Packet tracer	13

LISTA DE FIGURAS

Ilustración 1 Escenario 1	11
Ilustración 2 Simulación de Escenario 1	12
Ilustración 3 Configuración PC1.....	19
Ilustración 4 Interface Trunk	21
Ilustración 5 Estado Spaning-tree	23
Ilustración 6 Estado Standby	23
Ilustración 7 Estado Trunk	25
Ilustración 8 Configuración PC2 y PC3.....	26
Ilustración 9 Pings de respuesta segmentos PC1.....	26
Ilustración 10 Pings de respuesta segmentos PC2.....	27
Ilustración 11 Pings de respuesta segmentos PC3.....	27
Ilustración 12 Pings de respuesta segmentos PC4.....	28
Ilustración 13 Tabla ruteo OSPFv4	30
Ilustración 14 Tabla de ruteo OSPFv6	31
Ilustración 15 Adyacencia vecinos BGP R2.....	32
Ilustración 16 Adyacencia vecinos BGP R1	33
Ilustración 17 Verificación de usuario de ingreso AAA.....	37
Ilustración 18 Vista de hora actual del Router	38
Ilustración 19 Asociación con Server NTP D1 y R3	38
Ilustración 20 Server Syslog recibiendo eventos	39
Ilustración 21 Configuración SNMP Router	40

GLOSARIO

Direccionamiento IP: Término utilizado para referirse a la asignación de un identificador único de un dispositivo en una red.

Listas de Acceso: Son filtros utilizados por los equipos los cuales nos permiten generar reglas de permisos basadas en Ip, protocolos o Puertos.

Ethernet Channel: Este es un proceso que se realiza de manera lógica en los dispositivos con el fin de aumentar el ancho de banda y redundancia a las interfaces troncales en las redes de datos.

Protocolos de red: Son los estándares definidos por la IEEE que regulan y definen un mecanismo universal para las comunicaciones y que son optadas por los diferentes fabricantes para que puedan interoperar dispositivos de diferentes marcas entre sí sin tener ningún tipo de falla.

Enrutamiento: Es la manera en que se pueden comunicar los diferentes dispositivos en una red este se encuentra en la capa 3 del modelo OSI, y es quien decide los caminos por donde debe viajar un paquete hacia su destino, existen dos clases de enrutamiento (Estático y Dinámico).

Vlans: Estas son redes virtuales que se crean lógicamente en los equipos para lograr segmentar las mismas y ayudar en la optimización de los recursos, dando agilidad y mejor rendimiento a la red al ejecutar tareas.

Wlan: Estas son redes Wireless o redes inalámbricas y se caracterizan por usar las ondas electromagnéticas que tienen la propiedad de viajar sobre aire y expandir las conexiones sin tener algún medio físico para comunicarse.

Redundancia: Es un concepto muy común en las redes ya que refiere a los mecanismos y protocolos que nos ayudan a tener varias opciones de comunicación evitando depender de un solo equipo para su funcionamiento, esto hace que podamos garantizar la funcionalidad de una red en el caso que falle algún dispositivo.

RESUMEN

En este trabajo o laboratorio realizado se logro poner en practica los conceptos adquiridos durante la formación en el campo de las redes y comunicaciones en el diplomado de profundización CCNP donde logramos interactuar con equipos CISCO ya que son el mayor fabricante en el área de redes, a través de los 6 pasos implementados trabajamos conceptos de conmutación, redundancia, disponibilidad, seguridad de router, configuramos enrutamientos dinámicos y estáticos, analizamos el comportamiento de los diferentes protocolos usados por medio del software Packet Tracert en las diferentes capas del modelo OSI aprendiendo también como la electrónica apporto mucho para la transmisión de datos en los diferentes medios de comunicación que existen en la actualidad.

ABSTRACT

In this work or laboratory carried out, it was possible to put into practice the concepts acquired during the training in the field of networks and communications in the CCNP deepening diploma where we managed to interact with CISCO teams since they are the largest manufacturer in the area of networks, to Through the 6 steps implemented, we work on concepts of switching, redundancy, availability, router security, configure dynamic and static routing, analyze the behavior of the different protocols used by means of the Packet Tracert software in the different layers of the OSI model, also learning how to Electronics contribute a lot to the transmission of data in the different media that exist today.

INTRODUCCIÓN

En el campo de las telecomunicaciones y las redes con el paso del tiempo se viene mejorando y actualizando los diferentes protocolos implementados los cuales son controlados por los entes internacionales como la IEEE, por esto al profundizar en el diplomado CCNP se buscar entender y poder aplicar los conceptos aprendidos con el animo de ofrecer alternativas o soluciones a las diferentes organizaciones según sus necesidades.

Al abordar temas como Ipv4, Ipv6, DHCP, HSRP, BGP, OSPF, EIGRP; SSH, VLAN, EthernetChannel, WLC, RADIUS, AAA, SHA, MD5, Syslog, NTP y otros conceptos que trabajaremos a lo largo de este informe, aplicándolos con este escenario planteado en el curso comprenderemos estos conceptos y practicaremos realizando análisis mas exhaustivo del comportamiento de los paquetes a través de una red funcional y con las mejores practicas avaladas por los entes internacionales y por los fabricantes de los diferentes dispositivos que se trabajan en este campo como lo son los Routers, Switches y algunos servidores.

Para esto se tomará como base los conceptos y el uso de un software proporcionado por el fabricante Cisco Packet Tracer el cual puede simular el comportamiento real de los dispositivos y con sus herramientas de análisis de tráfico de red se pude entender con más claridad los conceptos y llevarlos a la práctica todo con el fin de prestar un servicio de red seguro, escalable, con alto rendimiento que optimice los procesos en las empresas u hogares que lo requieran.

DESARROLLO

1. ESCENARIO 1

Ilustración 1 Escenario 1

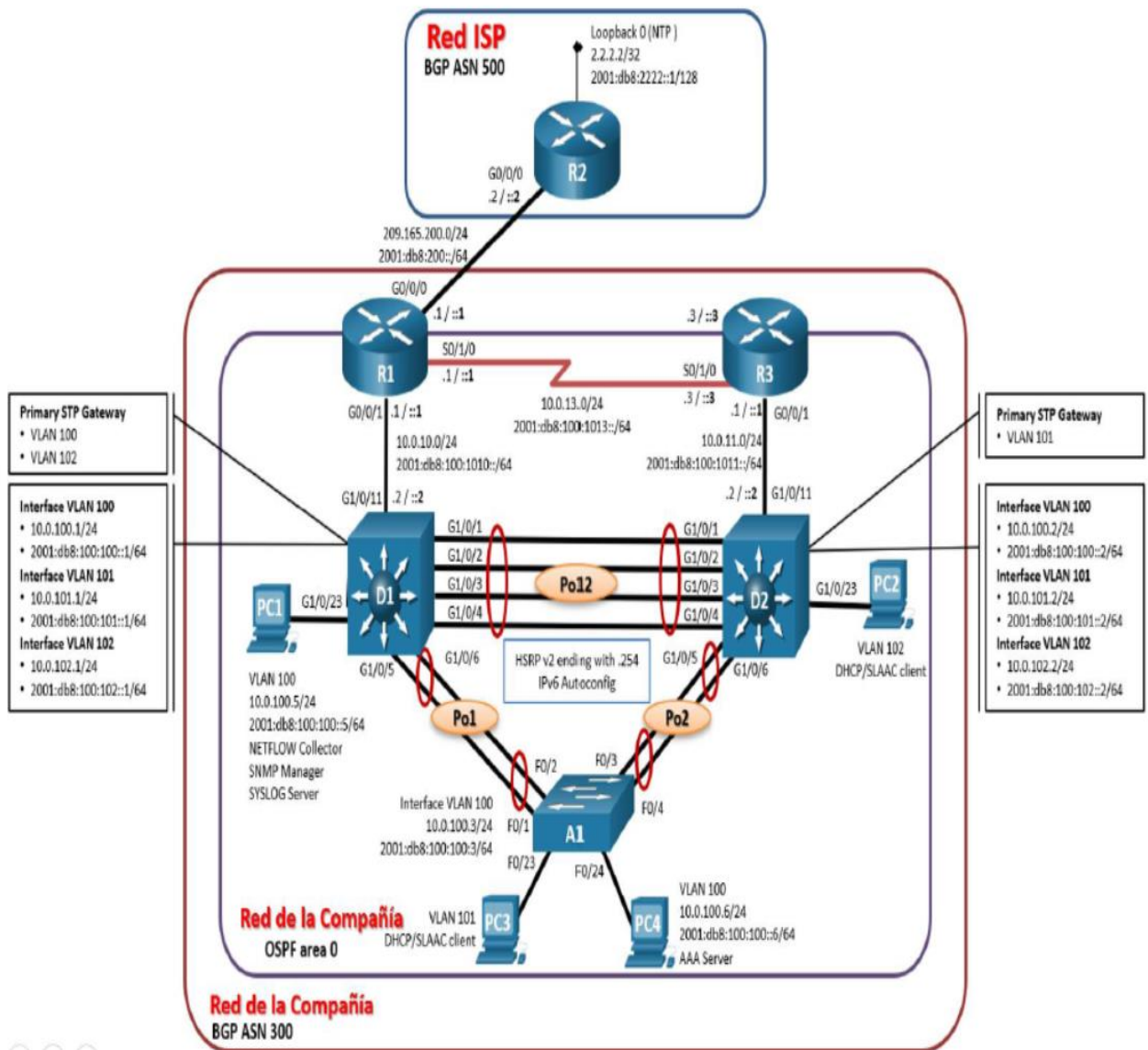


Ilustración 2 Simulación de Escenario 1

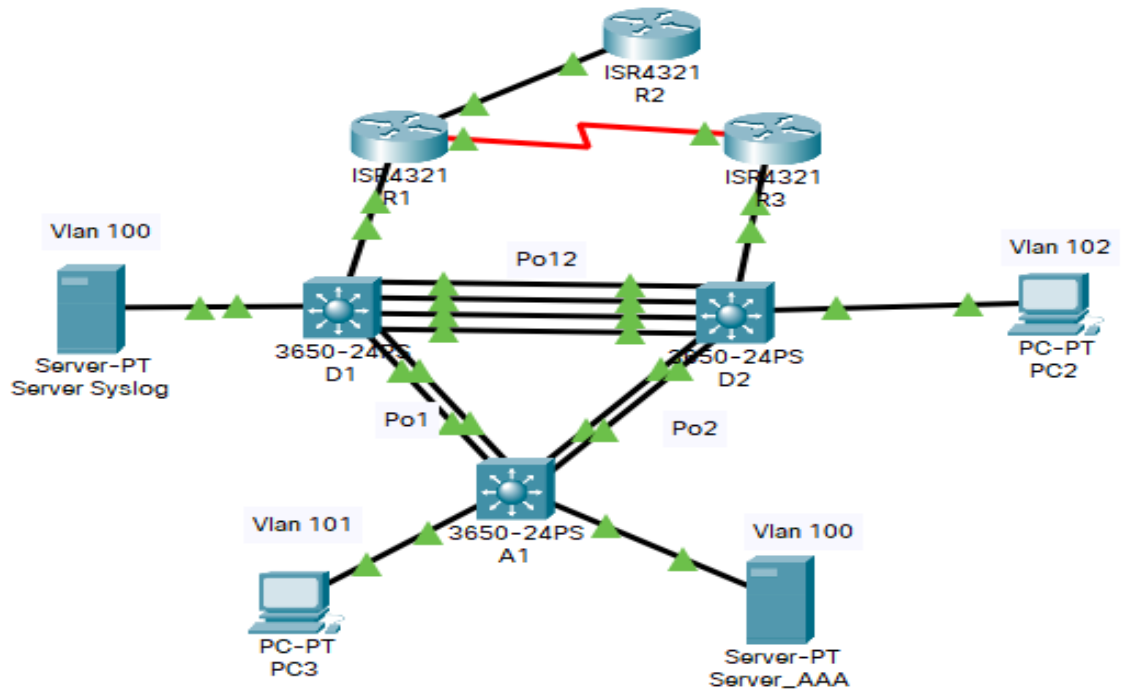


Tabla 1 Direccionamiento

Dispositivo	Interfaz	Dirección IPv4	Dirección IPv6	IPv6 Link-Local
R1	G0/0/0	209.165.200.225/27	2001:db8:200::1/64	fe80::1:1
	G0/0/1	10.0.10.1/24	2001:db8:100:1010::1/64	fe80::1:2
	S0/1/0	10.0.13.1/24	2001:db8:100:1013::1/64	fe80::1:3
R2	G0/0/0	209.165.200.226/27	2001:db8:200::2/64	fe80::2:1
	Loopback0	2.2.2.2/32	2001:db8:2222::1/128	fe80::2:3
R3	G0/0/1	10.0.11.1/24	2001:db8:100:1011::1/64	fe80::3:2
	S0/1/0	10.0.13.3/24	2001:db8:100:1013::3/64	fe80::3:3
D1	G1/0/11	10.0.10.2/24	2001:db8:100:1010::2/64	fe80::d1:1
	VLAN 100	10.0.100.1/24	2001:db8:100:100::1/64	fe80::d1:2
	VLAN 101	10.0.101.1/24	2001:db8:100:101::1/64	fe80::d1:3
	VLAN 102	10.0.102.1/24	2001:db8:100:102::1/64	fe80::d1:4
D2	G1/0/11	10.0.11.2/24	2001:db8:100:1011::2/64	fe80::d2:1
	VLAN 100	10.0.100.2/24	2001:db8:100:100::2/64	fe80::d2:2
	VLAN 101	10.0.101.2/24	2001:db8:100:101::2/64	fe80::d2:3
	VLAN 102	10.0.102.2/24	2001:db8:100:102::2/64	fe80::d2:4
A1	VLAN 100	10.0.100.3/23	2001:db8:100:100::3/64	fe80::a1:1
PC1	NIC	10.0.100.5/24	2001:db8:100:100::5/64	EUI-64
PC2	NIC	DHCP	SLAAC	EUI-64
PC3	NIC	DHCP	SLAAC	EUI-64
PC4	NIC	10.0.100.6/24	2001:db8:100:100::6/64	EUI-64

Parte 1: Construir la red y configurar los parámetros básicos de los dispositivos y el direccionamiento de las interfaces

Tabla 2 Equipos utilizados Packet tracer

Dispositivo	Modelo	Versión software
Router	ISR4321/K9	15.5
Switch Capa 3	C3650-24PS	4.26

Configuración de los equipos:

A continuación, se muestra las diferentes configuraciones iniciales implementadas en los equipos SW y Router que se presentan en el Escenario disponible, en este vamos a configurar las interfaces el nombre una banner o mensaje de ingreso a los equipos direccionamiento asignada a cada una y su activación.

Router R1

```

hostname R1
ipv6 unicast-routing                Se habilita enrutamiento Ipv6
no ip domain lookup                desactiva la traducción nombres
banner motd # R1, ENCOR Skills Assessment, Scenario 1 #
line con 0                          Se ingresa a la configuración consola
exec-timeout 0 0                    Tiempo de inactividad
logging synchronous
exit
interface g0/0/0                    Configuración de interface
ip address 209.165.200.225 255.255.255.224    Asignación Ipv4
ipv6 address fe80::1:1 link-local
ipv6 address 2001:db8:200::1/64            Asignación Ipv6
no shutdown
exit
interface g0/0/1
ip address 10.0.10.1 255.255.255.0
ipv6 address fe80::1:2 link-local
ipv6 address 2001:db8:100:1010::1/64
no shutdown
exit
interface s0/1/0
ip address 10.0.13.1 255.255.255.0
ipv6 address fe80::1:3 link-local
ipv6 address 2001:db8:100:1013::1/64

```

```
no shutdown
exit
```

Router R2

```
hostname R2
ipv6 unicast-routing
no ip domain lookup
banner motd # R2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
interface g0/0/0
ip address 209.165.200.226 255.255.255.224
ipv6 address fe80::2:1 link-local
ipv6 address 2001:db8:200::2/64
no shutdown
exit
```

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
ipv6 address fe80::2:3 link-local
ipv6 address 2001:db8:2222::1/128
no shutdown
exit
```

Se crea una interface Logica

Los demás dispositivos se configuran de la misma manera solo que cambia su direccionamiento IP con respecto a la tabla anteriormente presentada.

Router R3

```
hostname R3
ipv6 unicast-routing
no ip domain lookup
banner motd # R3, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
interface g0/0/1
ip address 10.0.11.1 255.255.255.0
ipv6 address fe80::3:2 link-local
ipv6 address 2001:db8:100:1011::1/64
```

```
no shutdown
exit
```

```
interface s0/1/0
ip address 10.0.13.3 255.255.255.0
ipv6 address fe80::3:3 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

Switch D1

```
hostname D1
ip routing
ipv6 unicast-routing
no ip domain lookup
banner motd # D1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
vlan 100
name Management
exit
```

Se crean Vlan
Se asigna nombre a la Vlan

```
vlan 101
name UserGroupA
exit
```

```
vlan 102
name UserGroupB
exit
```

```
vlan 999
name NATIVE
exit
```

Se crea Vlan
Se nombra como la Nativa

```
interface g1/0/11
no switchport
ip address 10.0.10.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1010::2/64
no shutdown
exit
```

```
interface vlan 100
ip address 10.0.100.1 255.255.255.0
ipv6 address fe80::d1:2 link-local
ipv6 address 2001:db8:100:100::1/64
no shutdown
exit
```

Se ingresa a la interface Vlan
Se asigna dirección Ipv4
Se asigna dirección Local Link
Se asigna dirección Ipv6

```
interface vlan 101
ip address 10.0.101.1 255.255.255.0
ipv6 address fe80::d1:3 link-local
ipv6 address 2001:db8:100:101::1/64
no shutdown
exit
```

```
interface vlan 102
ip address 10.0.102.1 255.255.255.0
ipv6 address fe80::d1:4 link-local
ipv6 address 2001:db8:100:102::1/64
no shutdown
exit
```

```
ip dhcp excluded-address 10.0.101.1 10.0.101.109
ip dhcp excluded-address 10.0.101.141 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.109
ip dhcp excluded-address 10.0.102.141 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
```

Se crea pool de direcciones que no son ofrecidas a los clientes DHCP

Se crea servidor DHCP
Se asigna la red
Se define un Gateway

```
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

```
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Se toma un rango

Switch D2

```
hostname D2
ip routing
ipv6 unicast-routing
```

```
no ip domain lookup
banner motd # D2, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
vlan 100
name Management
exit
```

```
vlan 101
name UserGroupA
exit
vlan 102
name UserGroupB
exit
```

```
vlan 999
name NATIVE
exit
```

```
interface g1/0/11
no switchport
ip address 10.0.11.2 255.255.255.0
ipv6 address fe80::d1:1 link-local
ipv6 address 2001:db8:100:1011::2/64
no shutdown
exit
```

```
interface vlan 100
ip address 10.0.100.2 255.255.255.0
ipv6 address fe80::d2:2 link-local
ipv6 address 2001:db8:100:100::2/64
no shutdown
exit
```

```
interface vlan 101
ip address 10.0.101.2 255.255.255.0
ipv6 address fe80::d2:3 link-local
ipv6 address 2001:db8:100:101::2/64
no shutdown
exit
```

```
interface vlan 102
ip address 10.0.102.2 255.255.255.0
ipv6 address fe80::d2:4 link-local
ipv6 address 2001:db8:100:102::2/64
no shutdown
exit
```

```
ip dhcp excluded-address 10.0.101.1 10.0.101.209
ip dhcp excluded-address 10.0.101.241 10.0.101.254
ip dhcp excluded-address 10.0.102.1 10.0.102.209
ip dhcp excluded-address 10.0.102.241 10.0.102.254
ip dhcp pool VLAN-101
network 10.0.101.0 255.255.255.0
default-router 10.0.101.254
exit
```

```
ip dhcp pool VLAN-102
network 10.0.102.0 255.255.255.0
default-router 10.0.102.254
exit
```

```
interface range g1/0/1-10, g1/0/12-24, g1/1/1-4
shutdown
exit
```

Switch A1

```
hostname A1
no ip domain lookup
banner motd # A1, ENCOR Skills Assessment, Scenario 1 #
line con 0
exec-timeout 0 0
logging synchronous
exit
```

```
vlan 100
name Management
exit
```

```
vlan 101
name UserGroupA
exit
```

```
vlan 102
name UserGroupB
```

```

vlan 999
name NATIVE
interface vlan 100
ip address 10.0.100.3 255.255.255.0
ipv6 address fe80::a1:1 link-local
ipv6 address 2001:db8:100:100::3/64
no shutdown
exit
interface range f0/5-22
shutdown

```

Copie el archivo running-config al archivo startup-config en todos los dispositivos:

```

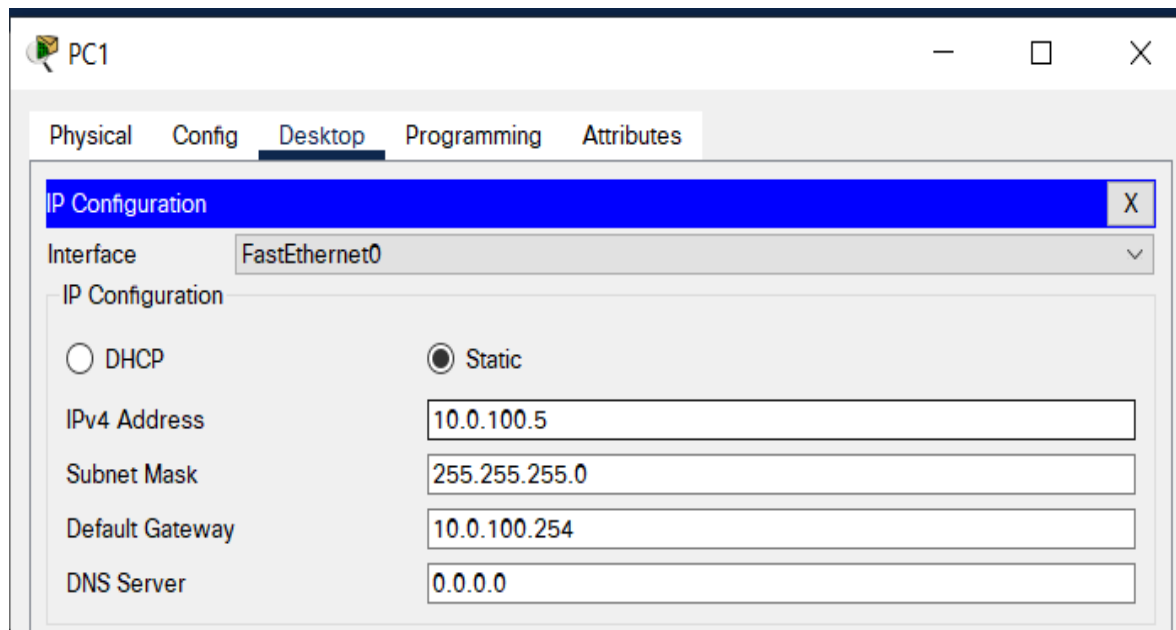
D1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

```

Se copia la configuración
Nombre con que se guarda

Configure el direccionamiento de los host PC 1 y PC 4 como se muestra en la tabla de direccionamiento. Asigne una dirección de puerta de enlace predeterminada de 10.0.100.254, la cual será la dirección IP virtual HSRP utilizada en la Parte 4.

Ilustración 3 Configuración PC1



Parte 2: Configurar la capa 2 de la red y el soporte de Host

En esta parte de la prueba de habilidades, debe completar la configuración de la capa 2 de la red y establecer el soporte básico de host. Al final de esta parte, todos los switches deben poder comunicarse. PC2 y PC3 deben recibir direccionamiento de DHCP y SLAAC.

Las tareas de configuración son las siguientes:

2.1 En todos los switches configure interfaces troncales IEEE 802.1Q sobre los enlaces de interconexión entre switches.

```
D1# interface GigabitEthernet1/0/1
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

Se ingresa a la configuración de Int
Convierte la interface en troncal Acti
Se asigna como interface troncal

```
D1# interface GigabitEthernet1/0/2
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

```
D1# interface GigabitEthernet1/0/3
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

```
D1# interface GigabitEthernet1/0/4
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

```
D1# interface GigabitEthernet1/0/5
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

```
D1# interface GigabitEthernet1/0/6
switchport mode dynamic desirable
switchport mode trunk
no shutdown
```

De igual manera se realizó en los Sw D2 y A1

2.2 En todos los switches cambie la VLAN nativa en los enlaces troncales.

```
D1# interface GigabitEthernet1/0/1
switchport trunk native vlan 999
```

Se ingresa a la configurac de la inte
Se asigna la vlan Nativa

```
D1# interface GigabitEthernet1/0/2
switchport trunk native vlan 999
```

```
D1# interface GigabitEthernet1/0/3
switchport trunk native vlan 999
```

```
D1# interface GigabitEthernet1/0/4
switchport trunk native vlan 999
```

```
D1# interface GigabitEthernet1/0/5
switchport trunk native vlan 999
```

```
D1# interface GigabitEthernet1/0/6
switchport trunk native vlan 999
```

De igual manera se realizó en los Sw D2 y A1

Ilustración 4 Interface Trunk

```
D1#show inter trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po1       1-1005
Po12      1-1005

Port      Vlans allowed and active in management domain
Po1       1,100,101,102,999
Po12      1,100,101,102,999

Port      Vlans in spanning tree forwarding state and not pruned
Po1       1,100,101,102,999
Po12      1,100,101,102,999
```

2.3 En todos los switches habilite el protocolo Rapid Spanning-Tree (RSTP)

```
D1(config)#spanning-tree mode rapid-pvst      comando para habilitar RSTP
D2(config)#spanning-tree mode rapid-pvst
A1(config)#spanning-tree mode rapid-pvst
```

2.4 En D1 y D2, configure los puentes raíz RSTP (root bridges) según la información del diagrama de topología, D1 y D2 deben proporcionar respaldo en caso de falla del puente raíz (root bridge).

```
D1#spanning-tree vlan 100,102 priority 24576      Se asigna prioridad a Vlan
```

```
D1(config)# interface Vlan100
D1(config-if)# standby 1 ip 10.0.100.254
D1(config-if)# standby 1 priority 200
D1(config-if)# standby 1 preempt
```

```
D1(config)# interface Vlan101
D1(config-if)# standby 1 ip 10.0.101.254
D1(config-if)# standby 1 priority 100
D1(config-if)# standby 1 preempt
```

```
D1(config)# interface Vlan102
D1(config-if)# standby 1 ip 10.0.102.254
D1(config-if)# standby 1 priority 200
D1(config-if)# standby 1 preempt
```

```
D2#spanning-tree vlan 101 priority 24576
```

```
D2(config)# interface Vlan100
D2(config-if)# standby 1 ip 10.0.100.254
D2(config-if)# standby 1 priority 100
D2(config-if)# standby 1 preempt
```

```
D2(config)# interface Vlan101
D2(config-if)# standby 1 ip 10.0.101.254
D2(config-if)# standby 1 priority 200
D2(config-if)# standby 1 preempt
```

```
D2(config)# interface Vlan102
D2(config-if)# standby 1 ip 10.0.102.254
D2(config-if)# standby 1 priority 100
D2(config-if)# standby 1 preempt
```

Ilustración 5 Estado Spaning-tree

```
D1(config)#do show span vlan 100
VLAN0100
  Spanning tree enabled protocol rstp
  Root ID    Priority    24676
            Address    0006.2A3B.078D
            This bridge is the root
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    24676 (priority 24576 sys-id-ext 100)
            Address    0006.2A3B.078D
            Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time 20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Gi1/0/23      Desg FWD 19       128.23  P2p
Pol           Desg FWD 3        128.29  Shr
Pol2          Desg FWD 3        128.30  Shr
```

Ilustración 6 Estado Standby

```
D2#show standby brief
          P indicates configured to preempt.
          |
Interface  Grp  Pri P State   Active           Standby           Virtual IP
Vl100     104  100 P Standby 10.0.100.1      local            10.0.100.254
Vl1       106  100 P Active  local          unknown          FE80::5:73FF:FEA0:106
Vl101     114  150 P Active  local          10.0.101.1      10.0.101.254
Vl1       116  150 P Active  local          unknown          FE80::5:73FF:FEA0:116
Vl102     124  100 P Standby 10.0.102.1      local            10.0.102.254
Vl1       126  100 P Active  local          unknown          FE80::5:73FF:FEA0:126
```

2.5 En todos los switches, cree EtherChannels LACP como se muestra en el diagrama de topología.

```
D1(config)#interface port-channel 1
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

Interface Por-channel
 Convierte la interface en troncal Acti
 Se establece como troncal
 Se asigna la vlan Nativa
 no negocia la interface

```
D1(config)#interface port-channel 12
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

```
D2(config)#interface port-channel 2
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

```
D2(config)#interface port-channel 12
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

```
A1(config)#interface port-channel 1
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

```
A1(config)#interface port-channel 2
switchport mode dynamic desirable
switchport mode trunk
switchport trunk native vlan 999
switchport nonegotiate
```

Agregar las interfaces al Channel-group

```
D1(config)#interface range g1/0/1-4
D1(config-if-range)# channel-group 12 mode active
```

Rango de interfaces agrupar
Se ingresan al grupo 12

```
D1(config)#interface range g1/0/5-6
D1(config-if-range)# channel-group 1 mode active
```

```
D2(config)#interface range g1/0/1-4
D2(config-if-range)# channel-group 12 mode active
```

```
D2(config)#interface range g1/0/5-6
D2(config-if-range)# channel-group 2 mode active
```

```
A1(config)#interface range g1/0/1-2
A1(config-if-range)# channel-group 1 mode active
```

```
A1(config)#interface range g1/0/3-4
A1(config-if-range)# channel-group 2 mode active
```

Ilustración 7 Estado Trunk

```
D1(config)#do show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    999
Po12      on        802.1q         trunking    999

Port      Vlans allowed on trunk
Po1       1-1005
Po12      1-1005

Port      Vlans allowed and active in management domain
Po1       1, 100, 101, 102, 999
Po12      1, 100, 101, 102, 999
```

2.6 En todos los switches, configure los puertos de acceso del host (host access port) que se conectan a PC1, PC2, PC3 y PC4.

```
D1# interface GigabitEthernet1/0/23
switchport access vlan 100
switchport mode Access
no shutdown
```

Se ingresa a la interface
Se le asigna un Vlan de acceso
se define el modo de operacion
Se prende la interface

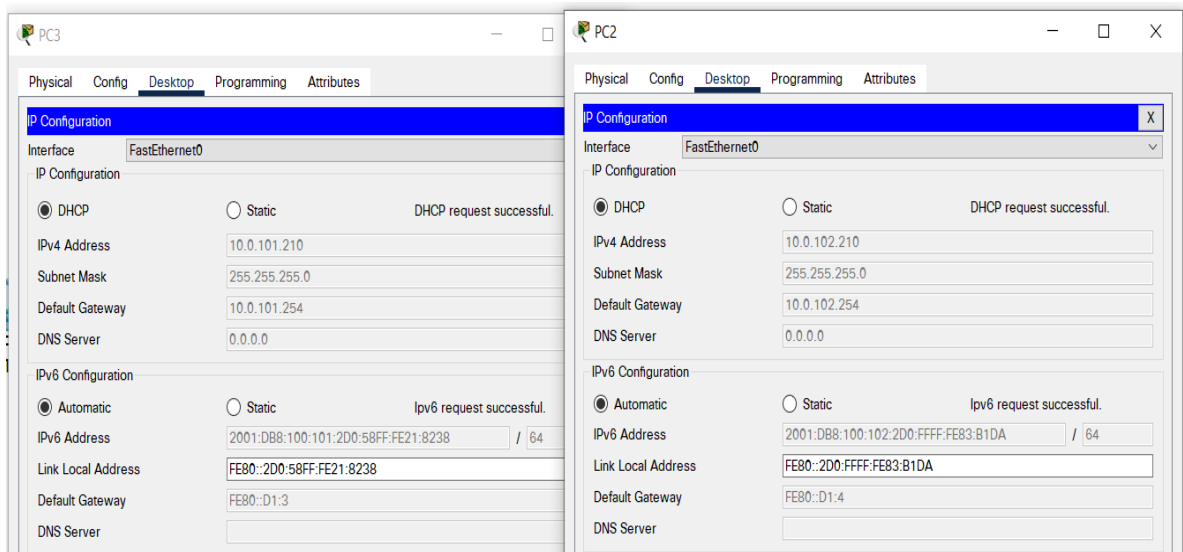
```
D2# interface GigabitEthernet1/0/23
switchport access vlan 102
switchport mode Access
no shutdown
```

```
A1# interface GigabitEthernet1/0/23
switchport access vlan 101
switchport mode Access
no shutdown
```

```
A1# interface GigabitEthernet1/0/24
switchport access vlan 100
switchport mode Access
no shutdown
```

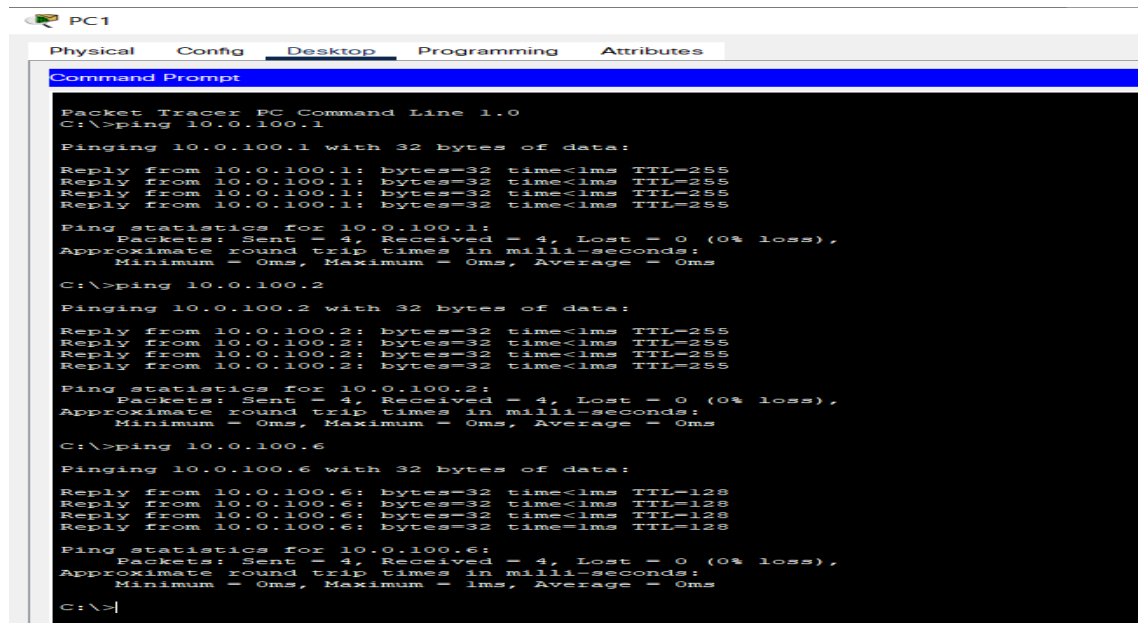
2.7 Verifique los servicios DHCP IPv4, PC2 y PC3 son clientes DHCP y deben recibir direcciones IPv4 válidas.

Ilustración 8 Configuración PC2 y PC3



2.8 Verifique la conectividad de la LAN local
 PC1 debería hacer ping con éxito a:
 D1: 10.0.100.1, D2: 10.0.100.2, PC4: 10.0.100.6

Ilustración 9 Pings de respuesta segmentos PC1



PC2 debería hacer ping con éxito a:
D1: 10.0.102.1, D2: 10.0.102.2

Ilustración 10 Pings de respuesta segmentos PC2

The network diagram shows a central router A1 (3650-24PS) connected to two edge routers D1 and D2 (3650-24PS). D1 is connected to ISP R1 (ISR4321), and D2 is connected to ISP R2 (ISR4321). PC3 (PC-PT) is connected to D1, and PC4 (PC-PT) is connected to D2. A red path is highlighted from PC2 to D1 and D2.

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.102.1

Pinging 10.0.102.1 with 32 bytes of data:

Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255
Reply from 10.0.102.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.0.102.2

Pinging 10.0.102.2 with 32 bytes of data:

Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255
Reply from 10.0.102.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.102.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

PC3 debería hacer ping con éxito a:
D1: 10.0.101.1, D2: 10.0.101.2

Ilustración 11 Pings de respuesta segmentos PC3

The network diagram is identical to the one in Illustration 10, showing the topology of routers and PCs.

```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.101.1

Pinging 10.0.101.1 with 32 bytes of data:

Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255
Reply from 10.0.101.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.101.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.0.101.2

Pinging 10.0.101.2 with 32 bytes of data:

Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255
Reply from 10.0.101.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.101.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

PC4 debería hacer ping con éxito a:
D1: 10.0.100.1, D2: 10.0.100.2, PC1: 10.0.100.5

Ilustración 12 Pings de respuesta segmentos PC4

The image displays a network topology diagram on the left and a screenshot of a PC4 Command Prompt window on the right. The network diagram shows three routers (ISR4321 R1, R2, R3) and three switches (3650-24PS D1, D2, A1). R1 and R2 are connected to D1 and D2. R2 and R3 are connected to D2 and A1. R1 and R3 are connected to A1. PC-PT PC3 and PC-PT PC4 are connected to A1. A red line highlights a path from R1 to R2 to R3 to A1. The Command Prompt window shows the following output:

```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.0.100.1
Pinging 10.0.100.1 with 32 bytes of data:
Reply from 10.0.100.1: bytes=32 time<lms TTL=255
Reply from 10.0.100.1: bytes=32 time<lms TTL=255
Reply from 10.0.100.1: bytes=32 time<lms TTL=255
Reply from 10.0.100.1: bytes=32 time<lms TTL=255
Ping statistics for 10.0.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.0.100.2
Pinging 10.0.100.2 with 32 bytes of data:
Reply from 10.0.100.2: bytes=32 time<lms TTL=255
Reply from 10.0.100.2: bytes=32 time<lms TTL=255
Reply from 10.0.100.2: bytes=32 time<lms TTL=255
Reply from 10.0.100.2: bytes=32 time<lms TTL=255
Ping statistics for 10.0.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 10.0.100.5
Pinging 10.0.100.5 with 32 bytes of data:
Reply from 10.0.100.5: bytes=32 time<lms TTL=128
Reply from 10.0.100.5: bytes=32 time<lms TTL=128
Reply from 10.0.100.5: bytes=32 time<lms TTL=128
Reply from 10.0.100.5: bytes=32 time<lms TTL=128
Ping statistics for 10.0.100.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Parte 3: Configurar los protocolos de enrutamiento

En esta parte, debe configurar los protocolos de enrutamiento IPv4 e IPv6. Al final de esta parte, la red debería estar completamente convergente. Los pings de IPv4 e IPv6 a la interfaz Loopback 0 desde D1 y D2 deberían ser exitosos.

Nota: Los pings desde los hosts no tendrán éxito porque sus puertas de enlace predeterminadas apuntan a la dirección HSRP que se habilitará en la Parte 4. Las tareas de configuración son las siguientes:

3.1 En la “Red de la Compañía” (es decir, R1, R3, D1, y D2), configure single-area OSPFv2 en area 0.

```
R1(config)#router ospf 4                Se selecciona Numero de proceso
R1(config-router)#router-id 0.0.4.1     se selecciona Id Proceso
R1(config-router)#network 10.0.10.1 0.0.0.255 area 0   Se anuncia la red
R1(config-router)#network 10.0.13.0 0.0.0.255 area 0   Se anuncia la red
```

```
R3(config)#router ospf 4
R3(config-router)#router-id 0.0.4.3
R3(config-router)#network 10.0.11.0 0.0.0.255 area 0
R3(config-router)#network 10.0.13.0 0.0.0.255 area 0
D1(config)#router ospf 4
D1(config-router)#router-id 0.0.4.131
D1(config-router)#network 10.0.10.0 0.0.0.255 area 0
D1(config-router)#network 10.0.100.0 0.0.0.255 area 0
D1(config-router)#network 10.0.101.0 0.0.0.255 area 0
D1(config-router)#network 10.0.102.0 0.0.0.255 area 0
```

```
D1(config)#router ospf 4
D1(config-router)#passive-interface default           Se selecciona como pasiva
D1(config-router)#no passive-interface g1/0/11      Se activa la interface
```

```
D2(config)#router ospf 4
D2(config-router)#router-id 0.0.4.132
D2(config-router)#network 10.0.11.0 0.0.0.255 area 0
D2(config-router)#network 10.0.100.0 0.0.0.255 area 0
D2(config-router)#network 10.0.101.0 0.0.0.255 area 0
D2(config-router)#network 10.0.102.0 0.0.0.255 area 0
```

```
D2(config)#router ospf 4
D2(config-router)#passive-interface default
D2(config-router)#no passive-interface g1/0/11
```



```
D1(config-if)#ipv6 ospf 6 area 0
D1(config-if)#exit
```

```
D1(config)#router ospf 6
D1(config-router)#passive-interface vlan 100
D1(config-router)#passive-interface vlan 101
D1(config-router)#passive-interface vlan 102
```

```
D2(config)#router ospf 6
D2(config-router)#router-id 0.0.6.132
D2(config)#interface g1/0/11
D2(config-if)#ipv6 ospf 6 area 0
D2(config)#interface vlan 100
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 101
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#interface vlan 102
D2(config-if)#ipv6 ospf 6 area 0
D2(config-if)#exit
D1(config)#router ospf 6
D1(config-router)#passive-interface vlan 100
D1(config-router)#passive-interface vlan 101
D1(config-router)#passive-interface vlan 102
```

Ilustración 14 Tabla de ruteo OSPFv6

```
R1#show ipv6 route ospf
IPv6 Routing Table - 12 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O 2001:DB8:100:100::/64 [110/2]
   via FE80::D1:1, GigabitEthernet0/0/1
O 2001:DB8:100:101::/64 [110/2]
   via FE80::D1:1, GigabitEthernet0/0/1
O 2001:DB8:100:102::/64 [110/2]
   via FE80::D1:1, GigabitEthernet0/0/1
O 2001:DB8:100:1011::/64 [110/65]
   via FE80::3:3, Serial0/1/0
R1#
R1#
```

Ctrl+F6 to exit CLI focus

Copy

3.3 En R2 en la “Red ISP”, configure MP-BGP.

Configure dos rutas estáticas predeterminadas a través de la interfaz Loopback 0:

- Una ruta estática predeterminada IPv4.
- Una ruta estática predeterminada IPv6.

```
R2(config)#ip route 2.2.2.2 255.255.255.255 209.165.200.225    Se crea ruta
estática lpv4
```

```
R2(config)# ipv6 route 2001:DB8:2222::1/128 2001:DB8:200::1    Se crea ruta
estática lpv6
```

Configure R2 en BGP ASN 500 y use el router-id 2.2.2.2.

```
R2(config)# router bgp 500                                     Se crea proceso de ruteo BGP
```

```
R2(config-router)#bgp router-id 2.2.2.2                       Se asigna ID de proceso
```

Configure y habilite una relación de vecino IPv4 e IPv6 con R1 en ASN 300.

```
R2(config-router)# neighbor 209.165.200.225 remote-as 300    se asigna
relación con el otro Sistema autónomo
```

El router no permite configuración BGP IPV6, tampoco permite configurar address family

```
R2(config-router)# network 2.2.2.2 mask 255.255.255.255      Se anuncia Red
```

Ilustración 15 Adyacencia vecinos BGP R2

```
R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 500
BGP table version is 4, main routing table version 6
3 network entries using 396 bytes of memory
3 path entries using 156 bytes of memory
1/1 BGP path/bestpath attribute entries using 184 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 816 total bytes of memory
BGP activity 3/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.200.225 4    300     9      8       4    0   0 00:06:25      4

R2#
```

Ctrl+F6 to exit CLI focus

Copy

3.4 En R1 en la “Red ISP”, configure MP-BGP.

Configure dos rutas resumen estáticas a la interfaz Null 0:

- Una ruta resumen IPv4 para 10.0.0.0/8.
- Una ruta resumen IPv6 para 2001:db8:100::/48.

```
R1(config)# ip route 10.0.0.0 255.0.0.0 Null0
```

El router no permite la configuración de ruta estática para la interface null en IPV6

Configure R1 en BGP ASN 300 y use el router-id 1.1.1.1.

```
R1(config-router)#bgp router-id 1.1.1.1
```

Ilustración 16 Adyacencia vecinos BGP R1

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 300
BGP table version is 3, main routing table version 6
 2 network entries using 264 bytes of memory
 2 path entries using 104 bytes of memory
1/1 BGP path/bestpath attribute entries using 184 bytes of memory
 2 BGP AS-PATH entries using 48 bytes of memory
 0 BGP route-map cache entries using 0 bytes of memory
 0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 632 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor      V   AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down   State/PfxRcd
209.165.200.226 4   500     7      5        3    0    0 00:03:10      4

R1#
R1#
```

Ctrl+F6 to exit CLI focus Copy

Configure una relación de vecino IPv4 e IPv6 con R2 en ASN 500.

```
R1(config-router)# neighbor 209.165.200.226 remote-as 500
```

El router no permite configuración BGP IPV6, tampoco permite configurar address family

En IPv4 address family:

- Deshabilite la relación de vecino IPv6.
- Habilite la relación de vecino IPv4.
- Anuncie la red 10.0.0.0/8.

El router no permite configuración BGP IPV6, tampoco permite configurar address family por tal motivo se realiza el anuncio de redes sin Address family.

```
R1(config-router)#network 10.0.0.0 mask 255.0.0.0
```

Parte 4: Configurar la Redundancia del Primer Salto (First Hop Redundancy)

4.1 En D1, cree IP SLAs que prueben la accesibilidad de la interfaz R1 G0/0/1.

4.2 En D2, cree IP SLAs que prueben la accesibilidad de la interfaz R3 G0/0/1.

En este punto como la implementación se realizó en packet tracer versión 8.01 en el cual los SW 3650 no reciben estos comandos, los cuales son usados para rastrear un ip y verificar que se tenga alcance y avisar en caso de caída o cambio de estado.

```
D1(config)# ip sla 4
D1(config-ip-sla)# icmp-echo 10.0.10.1
D1(config-ip-sla-echo)# frequency 5
D1(config-ip-sla-echo)# exit
D1(config)# ip sla schedule 4 life forever start-time now
```

4.3 En D1 configure HSRPv2.

En este punto se realizará configuración para mantener redundancia entre las vlan y balancear el tráfico entre los 2 SW.

Configuración Vlan 100

```
D1(config)#interface vlan 100
D1(config-if)# standby version 2
D1(config-if)# standby 104 ip 10.0.100.254
D1(config-if)# standby 104 priority 150
D1(config-if)# standby 104 preempt
D1(config-if)# standby 106 ipv6 autoconfig
D1(config-if)# standby 106 priority 150
D1(config-if)# standby 106 preempt
```

Version de HSRP
Ip virtual de comunicación
La prioridad de la interface
Habilita la preferencia
Autoconfigura IPV6 comunicacion
La prioridad de la interface
Habilita la preferencia

Configuration Vlan 101

```
D1(config)#interface vlan 101
D1(config-if)# standby version 2
D1(config-if)# standby 114 ip 10.0.101.254
D1(config-if)# standby 114 preempt
D1(config-if)# standby 116 ipv6 autoconfig
D1(config-if)# standby 116 preempt
```

Configuración Vlan 102

```
D1(config)#interface vlan 102
D1(config-if)# standby version 2
D1(config-if)# standby 124 ip 10.0.102.254
D1(config-if)# standby 124 priority 150
D1(config-if)# standby 124 preempt
D1(config-if)# standby 126 ipv6 autoconfig
D1(config-if)# standby 126 priority 150
D1(config-if)# standby 126 preempt
En D2, configure HSRPv2.
```

Configuration Vlan 100

```
D2(config)#interface vlan 100
D2(config-if)# standby version 2
D2(config-if)# standby 104 ip 10.0.100.254
D2(config-if)# standby 104 preempt
D2(config-if)# standby 106 ipv6 autoconfig
D2(config-if)# standby 106 preempt
```

Configuración Vlan 101

```
D2(config)#interface vlan 101
D2(config-if)# standby version 2
D2(config-if)# standby 114 ip 10.0.101.254
D2(config-if)# standby 114 priority 150
D2(config-if)# standby 114 preempt
D2(config-if)# standby 116 ipv6 autoconfig
D2(config-if)# standby 116 priority 150
D2(config-if)# standby 116 preempt
```

Configuration Vlan 102

```
D2(config)#interface vlan 102
D2(config-if)# standby version 2
D2(config-if)# standby 124 ip 10.0.102.254
D2(config-if)# standby 124 preempt
D2(config-if)# standby 126 ipv6 autoconfig
D2(config-if)# standby 126 preempt
```

Parte 5: Seguridad

- 5.1 En todos los dispositivos, proteja el EXEC privilegiado usando el algoritmo de encriptación.

Para el ingreso al EXEC privilegiado se usa el comando enable y para colocar contraseña usamos el siguiente comando este se ejecuta en cada dispositivo:

```
D2(config)#enable secret cisco12345cisco
```

- 5.2 En todos los dispositivos, cree un usuario local y protéjalo usando el algoritmo de encriptación SCRYPT.

Con el siguiente comando generamos el usuario con las condiciones solicitadas usamos el siguiente comando este se ejecuta en cada dispositivo:

```
D2(config)#username sadmin privilege 15 password cisco12345cisco
```

- 5.3 En todos los dispositivos (excepto R2), habilite AAA.

Con el siguiente comando habilitamos el AAA usamos el siguiente comando este se ejecuta en cada dispositivo:

```
R1(config)#aaa new-model                      Habilita AAA
```

- 5.4 En todos los dispositivos (excepto R2), configure las especificaciones del servidor RADIUS.

Con estos comandos se configura el servidor radius local para que autentique con el servidor AAA y el puerto de comunicación el siguiente comando este se ejecuta en cada dispositivo:

```
R1(config)#radius server RADIUS  
R1(config-radius-server)# address ipv4 10.0.100.6 auth-port 1812  
R1(config-radius-server)# key $strongPass
```

- 5.5 En todos los dispositivos (excepto R2), configure la lista de métodos de autenticación AAA.

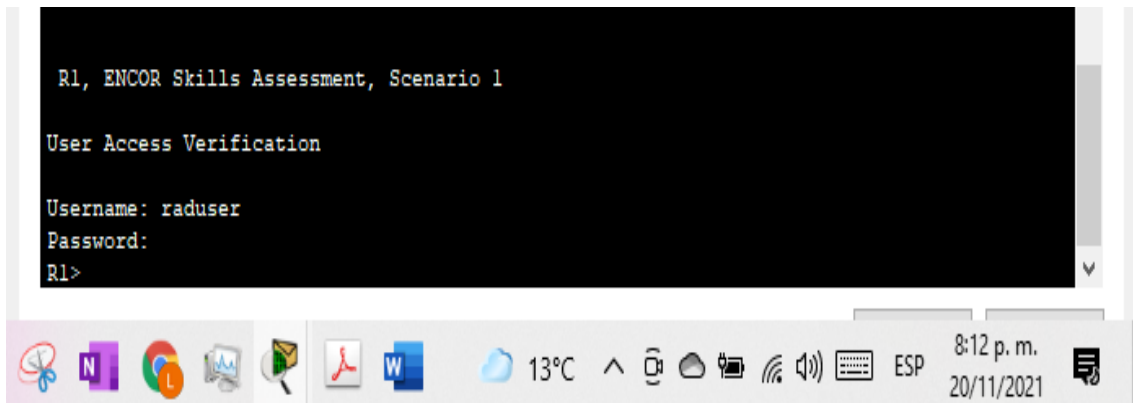
Con este comando se crea la lista de autenticación de manera local con el servidor AAA el siguiente comando este se ejecuta en cada dispositivo:

```
R1(config)# aaa authentication login AUT-RADIUS group radius local
```

5.6 Verifique el servicio AAA en todos los dispositivos (except R2).

Se realiza la validación de usuario con el servidor AAA y que este se ejecute de manera correcta para la autenticación de los usuarios permitidos para ingresar a los equipos.

Ilustración 17 Verificación de usuario de ingreso AAA



```
R1, ENCOR Skills Assessment, Scenario 1

User Access Verification

Username: raduser
Password:
R1>
```

The screenshot shows a terminal window with a black background and white text. The text displays the router's name and scenario, followed by a 'User Access Verification' prompt. The user 'raduser' has been entered, and the password field is currently empty. The terminal prompt 'R1>' is visible at the bottom of the window. Below the terminal window is a Windows taskbar with various application icons, system tray icons including a weather widget showing 13°C, and a clock displaying 8:12 p.m. on 20/11/2021.

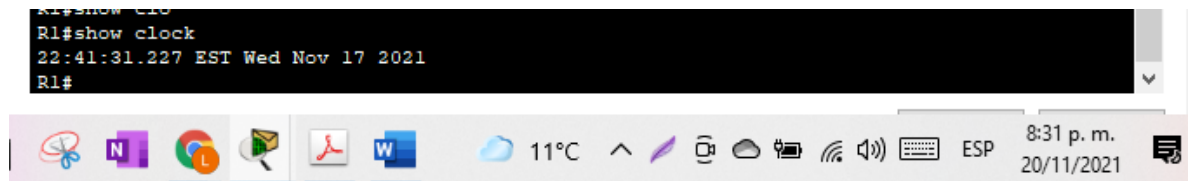
Parte 6: Configure las funciones de Administración de Red

6.1 En todos los dispositivos, configure el reloj local a la hora UTC actual.

Se ejecuta el siguiente comando en los equipos con esta estructura Hora, día, mes y año.

```
R1#clock set 8:28:00 17 Nov 2021
```

Ilustración 18 Vista de hora actual del Router



6.2 Configure R2 Como un NTP maestro.

Con este comando ejecutamos el servicio de servidor NTP como maestro en R2.

```
R2(config)#ntp master 3
```

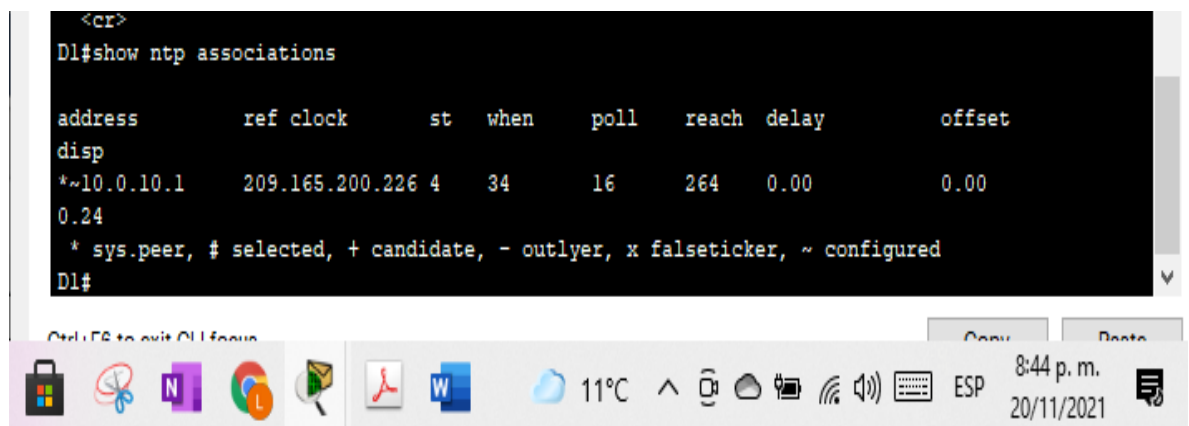
6.3 Configure NTP en R1, R3, D1, D2, y A1.

En este caso debemos identificar la interface adyacente hacia el servidor Master NTP R2 y en cada dispositivo configuramos el siguiente comando:

```
R1(config)#ntp server 209.165.200.226
```

La Ip varía dependiendo del dispositivo.

Ilustración 19 Asociación con Server NTP D1 y R3



```

R3#show ntp associations

address          ref clock      st  when    poll  reach  delay  offset
disp
*~10.0.13.1      209.165.200.226 4   0       16    377    4.00   2.00
0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R3#

```

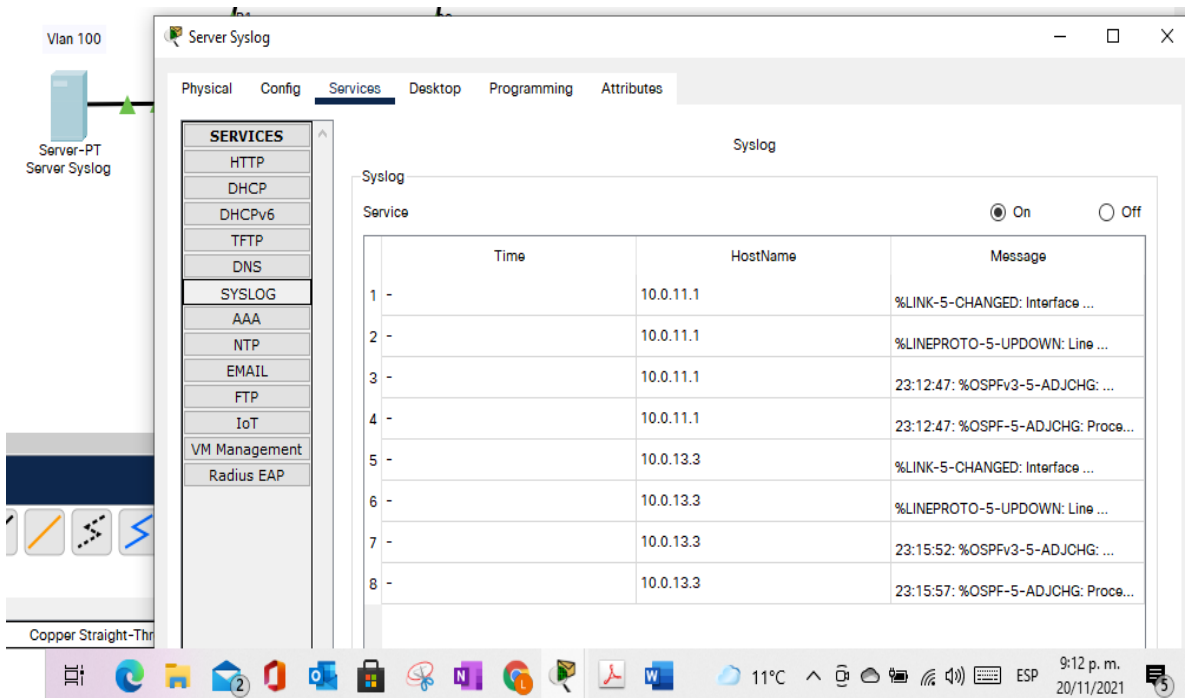
6.4 Configure Syslog en todos los dispositivos excepto R2

En este caso se configura en todos los dispositivos usando el siguiente comando apuntando a la Ip del servidor syslog 10.0.100.5 con la idea de tener visual de los logs generados por los equipos.

R3(config)# logging 10.0.100.5

Se genero eventos manuales para ver la funcionalidad del servidor.

Ilustración 20 Server Syslog recibiendo eventos



6.5 Configure SNMPv2c en todos los dispositivos excepto R2

Se realiza la configuración de los equipos para el protocolo SNMPv2 con el fin de poder tomar datos del dispositivo en tiempo real como lo es consumo de ram, estado interfaces, trafico etc. esto se realiza en cada dispositivo.

```
R1(config)#ip access-list standard SNMP-SERVER           Se crea lista acceso
R1(config-std-nacl)#permit host 10.0.100.5           Se define IP Autorizado
R1(config)#snmp-server contact Alejandro Guzman       Se define contacto
R1(config)#snmp-server community ENCORSA ro SNMP-SERVER se enlaza
la comunidad creada con la lista de acceso.
```

Nota: se anexa imagen con la configuración donde se implementó en Packet Tracer pero este no permite los comandos completos.

Ilustración 21 Configuración SNMP Router

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
no synchronization
neighbor 209.165.200.226 remote-as 500
network 10.0.0.0
!
ipv6 router ospf 6
log-adjacency-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
ip route 10.0.0.0 255.0.0.0 Null0
!
ip flow-export version 9
!
ipv6 route ::/0 2001:DB8:200::2
!
ip access-list standard SNMP-SERVER
permit host 10.0.100.5
!
banner motd ^C R1, ENCOR Skills Assessment, Scenario 1 ^C
!
radius server RADIUS
address ipv4 10.0.100.6 auth-port 1812
key $trongPass
!
snmp-server community ENCORSA RO
!
logging 10.0.100.5
line con 0
exec-timeout 0 0
logging synchronous
login authentication AUT-RADIUS
!
```

CONCLUSIONES

Al realizar esta practica se puede aclarar muchas dudas sobre el comportamiento de los paquetes a través de una red, dependiendo del tipo de protocolo aplicado para cada servicio, aprendí que las organizaciones tienen múltiples necesidades en sus redes según su propósito y la dimensión de la red, en esto ingresan los protocolos entregados por los entes internacionales IEEE con el fin de estandarizar la comunicación en las diferentes capas del modelo OSI.

Se pudo revisar temas vitales en las redes como lo son las segmentaciones de Red y VLAN que ayudan a administrar y separar trafico importante para las compañías además de ofrecer mejores opciones de seguridad y rendimiento de los dispositivos de red, se configuro canales Ethernetchannel con el fin de proveer redundancia y disponibilidad creando conexiones virtuales entre interfaces físicas, adicional se crearon servidores DHCP para el direccionamiento IPV4, con redundancia a través del protocolo HSRP creado una Ip virtual de comunicación con los host.

En las capas 3 y 4 del modelo OSI se trabajo los temas de enrutamiento dinámico y estático en direcciones IPV4 e IPV6 conocer sus ventajas y limitaciones logrando aplicar los protocolos OSF y BGP logrando enrutamiento dinámico trabajando el área Backbone 0 y comunicación por medio de sistemas autónomos en BGP Externo conectando nuestro ISP proveedor de servicio, además de esto se logro configurar servidores AAA, RADIUS, SNMP, NDP los cuales nos proporcionan servicios de sincronización horaria en tiempo real, autenticación de usuarios por medio de los servidores Radius y AAA, entender las ventajas que ofrece implementar monitoreo a través de servidores Syslog y servidor SNMP con el fin de controlar y optimizar la red esto es vital para toda clase de organizaciones.

BIBLIOGRAFÍA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Tarea, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>