

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



TRABAJO COLABORATIVO
PRACTICA DE LABORATORIO

WILSON TÉLLEZ FIGUEROA
COD: 80246892

Presentado a:
EFRAIN ALEJANDRO PEREZ
GRUPO: 203092_46

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA.
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
CEAD JOSÉ ACEVEDO GÓMEZ

SEPTIEMBRE DE 2017

INTRODUCCION

Continuando con el proceso de aprendizaje del diplomado CCNA 2 se elabora informe de la siguiente practica de laboratorio realizada con las herramientas de trabajo Packet Tracer y Wireshark propuestas para el mismo.

En esta practica se realizan diversas configuraciones sobre Routers, Switches y Pc's donde aplicaremos lo aprendido en módulos anteriores como lo es la configuración básica de los mismos y mediante el software Wireshark realizaremos captura de datos para ver los mensajes RA, filtrando paquetes IPV6 y analizando los mensajes que se generan al realizar las diferentes configuraciones sobre los dispositivos.

Para esta practica se presentan los comandos utilizados para realizar las diferentes configuraciones y pantallas donde se evidencian los resultados obtenidos durante la práctica, demostrando así su correcto desarrollo y proceso de aprendizaje.

Práctica de laboratorio: configuración de DHCPv6 sin estado y con estado

Topología



Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IPv6	Longitud de prefijo	Gateway predeterminado
R1	G0/1	2001:DB8:ACAD:A::1	64	No aplicable
S1	VLAN 1	Asignada mediante SLAAC	64	Asignada mediante SLAAC
PC-A	NIC	Asignada mediante SLAAC y DHCPv6	64	Asignado por el R1

Objetivos

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

Parte 2: configurar la red para SLAAC

Parte 3: configurar la red para DHCPv6 sin estado

Parte 4: configurar la red para DHCPv6 con estado

Información básica/situación

La asignación dinámica de direcciones IPv6 de unidifusión global se puede configurar de tres maneras:

- Solo mediante configuración automática de dirección sin estado (SLAAC)
- Mediante el protocolo de configuración dinámica de host sin estado para IPv6 (DHCPv6)
- Mediante DHCPv6 con estado

Con SLAAC (se pronuncia “slac”), no se necesita un servidor de DHCPv6 para que los hosts adquieran direcciones IPv6. Se puede usar para recibir información adicional que necesita el host, como el nombre de dominio y la dirección del servidor de nombres de dominio (DNS). El uso de SLAAC para asignar direcciones host IPv6 y de DHCPv6 para asignar otros parámetros de red se denomina “DHCPv6 sin estado”.

Con DHCPv6 con estado, el servidor de DHCP asigna toda la información, incluida la dirección host IPv6.

La determinación de cómo los hosts obtienen la información de direccionamiento dinámico IPv6 depende de la configuración de indicadores incluida en los mensajes de anuncio de router (RA).

En esta práctica de laboratorio, primero configurará la red para que utilice SLAAC. Una vez que verificó la conectividad, configurará los parámetros de DHCPv6 y modificará la red para que utilice DHCPv6 sin estado. Una vez que verificó que DHCPv6 sin estado funcionó correctamente, modificará la configuración del R1 para que utilice DHCPv6 con estado. Se usará Wireshark en la PC-A para verificar las tres configuraciones dinámicas de red.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con IOS de Cisco versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que el router y el switch se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Nota: la plantilla **default bias** que utiliza el Switch Database Manager (SDM) no proporciona capacidades de dirección IPv6. Verifique que se utilice la plantilla **dual-ipv4-and-ipv6** o la plantilla **lanbase-routing** en SDM. La nueva plantilla se utilizará después de reiniciar, aunque no se guarde la configuración.

```
S1# show sdm prefer
```

Siga estos pasos para asignar la plantilla **dual-ipv4-and-ipv6** como la plantilla de SDM predeterminada:

```
S1# config t
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
S1(config)# end
```

```
S1# reload
```

Recursos necesarios

- 1 router (Cisco 1941 con IOS de Cisco versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con IOS de Cisco versión 15.0(2), imagen lanbasek9 o comparable)
- 1 computadora (Windows 7 o Vista con Wireshark y un programa de emulación de terminal, como Tera Term)
- Cables de consola para configurar los dispositivos con IOS de Cisco mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Nota: los servicios de cliente DHCPv6 están deshabilitados en Windows XP. Se recomienda usar un host con Windows 7 para esta práctica de laboratorio.

Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos de configuración, como los nombres de dispositivos, las contraseñas y las direcciones IP de interfaz.

Paso 1: realizar el cableado de red tal como se muestra en la topología.

Paso 2: inicializar y volver a cargar el router y el switch según sea necesario.

Paso 3: Configurar R1

- a. Desactive la búsqueda del DNS.

- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Guardar la configuración en ejecución en la configuración de inicio.

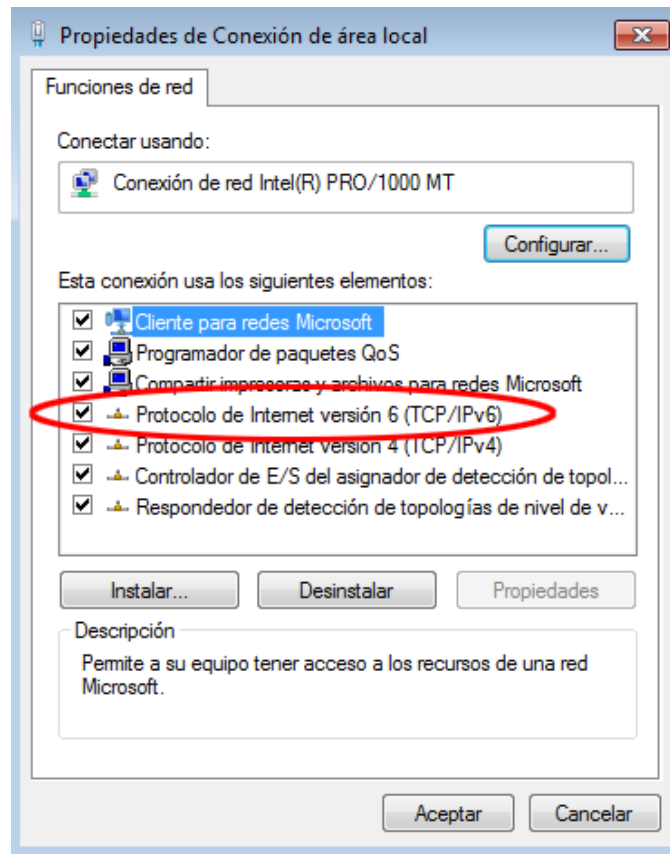
Paso 4: configurar el S1.

- a. Desactive la búsqueda del DNS.
- b. Configure el nombre del dispositivo.
- c. Cifre las contraseñas de texto no cifrado.
- d. Cree un mensaje MOTD que advierta a los usuarios que se prohíbe el acceso no autorizado.
- e. Asigne **class** como la contraseña cifrada del modo EXEC privilegiado.
- f. Asigne **cisco** como la contraseña de vty y la contraseña de consola, y habilite el inicio de sesión.
- g. Establezca el inicio de sesión de consola en modo sincrónico.
- h. Desactive administrativamente todas las interfaces inactivas.
- i. Guarde la configuración en ejecución en la configuración de inicio.

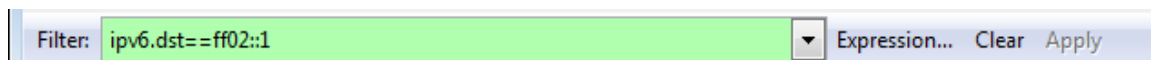
Parte 2: configurar la red para SLAAC

Paso 1: preparar la PC-A.

- a. Verifique que se haya habilitado el protocolo IPv6 en la ventana Propiedades de conexión de área local. Si la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) no está marcada, haga clic para activarla.



- b. Inicie una captura del tráfico en la NIC con Wireshark.
- c. Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes. La entrada de filtro que se usa con Wireshark es **ipv6.dst==ff02::1**, como se muestra aquí.



Paso 2: Configurar R1

- a. Habilite el routing de unidifusión IPv6.
- b. Asigne la dirección IPv6 de unidifusión a la interfaz G0/1 según la tabla de direccionamiento.
- c. Asigne FE80::1 como la dirección IPv6 link-local para la interfaz G0/1.
- d. Active la interfaz G0/1.

Paso 3: verificar que el R1 forme parte del grupo de multidifusión de todos los routers.

Use el comando **show ipv6 interface g0/1** para verificar que G0/1 forme parte del grupo de multidifusión de todos los routers (FF02::2). Los mensajes RA no se envían por G0/1 sin esa asignación de grupo.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
```

```
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

Paso 4: configurar el S1.

Use el comando **ipv6 address autoconfig** en la VLAN 1 para obtener una dirección IPv6 a través de SLAAC.

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

Paso 5: verificar que SLAAC haya proporcionado una dirección de unidifusión al S1.

Use el comando **show ipv6 interface** para verificar que SLAAC haya proporcionado una dirección de unidifusión a la VLAN1 en el S1.

```
S1# show ipv6 interface
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::ED9:96FF:FEE8:8A40
  No Virtual link-local address(es):
  Stateless address autoconfig enabled
  Global unicast address(es):
    2001:DB8:ACAD:A:ED9:96FF:FEE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
    valid lifetime 2591988 preferred lifetime 604788
  Joined group address(es):
    FF02::1
    FF02::1:FFE8:8A40
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachable are sent
  Output features: Check hwidb
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
  Default router is FE80::1 on Vlan1
```

Paso 6: verificar que SLAAC haya proporcionado información de dirección IPv6 en la PC-A.

- En el símbolo del sistema de la PC-A, emita el comando **ipconfig /all**. Verifique que la PC-A muestre una dirección IPv6 con el prefijo 2001:db8:acad:a::/64. El gateway predeterminado debe tener la dirección FE80::1.

```

Adaptador de Ethernet Conexión de área local:

    Sufixo DNS específico para la conexión. . . : 
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000
    MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>

    Dirección IPv4. . . . . : 192.168.96.139<Preferido>
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . : fe80::1:1
    Servidores DNS. . . . . : fec0:0:0:ffff::1%1
                                fec0:0:0:ffff::2%1
                                fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

- En Wireshark, observe uno de los mensajes RA que se capturaron. Expanda la capa Internet Control Message Protocol v6 (Protocolo de mensajes de control de Internet v6) para ver la información de Flags (Indicadores) y Prefix (Prefijo). Los primeros dos indicadores controlan el uso de DHCPv6 y no se establecen si no se configura DHCPv6. La información del prefijo también está incluida en este mensaje RA.

Filter: **ipv6.dst==ff02::1**

No.	Time	Source	Destination	Protocol	Length	Info
3518	3972.07973	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3673	4130.43155	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3840	4284.68370	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
3989	4435.87602	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 3518: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

- Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x1816 [correct]
 - Cur hop limit: 64
 - Flags: 0x00
 - 0... .. = Managed address configuration: Not set
 - .0... .. = Other configuration: Not set
 - ..0... .. = Home Agent: Not set
 - ...0... .. = Prf (Default Router Preference): Medium (0)
 -0... .. = Proxy: Not set
 -0... .. = Reserved: 0
 - Router lifetime (s): 1800
 - Reachable time (ms): 0
 - Retrans timer (ms): 0
 - ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
 - ICMPv6 Option (MTU : 1500)
 - ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)
 - Type: Prefix information (3)
 - Length: 4 (32 bytes)
 - Prefix Length: 64
 - Flag: 0xc0
 - Valid Lifetime: 2592000
 - Preferred Lifetime: 604800
 - Reserved
 - Prefix: 2001:db8:acad:a:: (2001:db8:acad:a::)

Parte 3: configurar la red para DHCPv6 sin estado

Paso 1: configurar un servidor de DHCP IPv6 en el R1.

- a. Cree un pool de DHCP IPv6.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
```

- b. Asigne un nombre de dominio al pool.

```
R1(config-dhcpv6)# domain-name ccna-statelessDHCPv6.com
```

- c. Asigne una dirección de servidor DNS.

```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
```

```
R1(config-dhcpv6)# exit
```

- d. Asigne el pool de DHCPv6 a la interfaz.

```
R1(config)# interface g0/1
```

```
R1(config-if)# ipv6 dhcp server IPV6POOL-A
```

- e. Establezca la detección de redes (ND) DHCPv6 other-config-flag.

```
R1(config-if)# ipv6 nd other-config-flag
```

```
R1(config-if)# end
```

Paso 2: verificar la configuración de DHCPv6 en la interfaz G0/1 del R1.

Use el comando **show ipv6 interface g0/1** para verificar que la interfaz ahora forme parte del grupo IPv6 de multidifusión de todos los servidores de DHCPv6 (FF02::1:2). La última línea del resultado de este comando **show** verifica que se haya establecido other-config-flag.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
```

```
Hosts use stateless autoconfig for addresses.
```

```
Hosts use DHCP to obtain other configuration.
```

Paso 3: ver los cambios realizados en la red en la PC-A.

Use el comando **ipconfig /all** para revisar los cambios realizados en la red. Observe que se recuperó información adicional, como la información del nombre de dominio y del servidor DNS, del servidor de DHCPv6. Sin embargo, las direcciones IPv6 de unidifusión global y link-local se obtuvieron previamente mediante SLAAC.

```
Adaptador de Ethernet Conexión de área local:
    Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
    Descripción . . . . . : Conexión de red Intel(R) PRO/1000 MT
    Dirección física. . . . . : 00-0C-29-E3-23-17
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
    Vínculo: dirección IPv6 local. . . : fe80::e8ed:811c:3215:5bc2%11<Preferido>
    Dirección IPv4. . . . . : 192.168.96.139<Preferido>
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . : fe80::1%11
    IAID DHCPv6 . . . . . : 234884137
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
    Servidores DNS. . . . . : 2001:db8:acad:a::abcd
    NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.localdomain:
    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . : ccna-statelessDHCPv6.com
    Descripción . . . . . : Adaptador ISATAP de Microsoft
    Dirección física. . . . . : 00-00-00-00-00-00-E0
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . : sí
```

Paso 4: ver los mensajes RA en Wireshark.

Desplácese hasta el último mensaje RA que se muestra en Wireshark y expándalo para ver la configuración de indicadores ICMPv6. Observe que el indicador Other configuration (Otra configuración) está establecido en 1.

Filter: **ipv6.dst==ff02::1** Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
191	190.005980	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
422	383.803033	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
696	581.355847	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1
877	776.644829	fe80::1	ff02::1	ICMPv6	118	Router Advertisement from d4:8c:b5:ce:a0:c1

Frame 877: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)

Ethernet II, Src: d4:8c:b5:ce:a0:c1 (d4:8c:b5:ce:a0:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)

Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)

Internet Control Message Protocol v6

- Type: Router Advertisement (134)
- Code: 0
- Checksum: 0x17d6 [correct]
- Cur hop limit: 64
- Flags: 0x40
 - 0... .. = Managed address configuration: Not set
 - 1... .. = Other configuration: Set**
 - ..0. = Home Agent: Not set
 - ...0 0... = Prf (Default Router Preference): Medium (0)
 - 0.. = Proxy: Not set
 -0. = Reserved: 0
- Router lifetime (s): 1800
- Reachable time (ms): 0
- Retrans timer (ms): 0
- ICMPv6 Option (Source link-layer address : d4:8c:b5:ce:a0:c1)
- ICMPv6 Option (MTU : 1500)
- ICMPv6 Option (Prefix information : 2001:db8:acad:a::/64)

Paso 5: verificar que la PC-A no haya obtenido su dirección IPv6 de un servidor de DHCPv6.

Use los comandos **show ipv6 dhcp binding** y **show ipv6 dhcp pool** para verificar que la PC-A no haya obtenido una dirección IPv6 del pool de DHCPv6.

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

Paso 6: restablecer la configuración de red IPv6 de la PC-A.

- Desactive la interfaz F0/6 del S1.

Nota: la desactivación de la interfaz F0/6 evita que la PC-A reciba una nueva dirección IPv6 antes de que usted vuelva a configurar el R1 para DHCPv6 con estado en la parte 4.

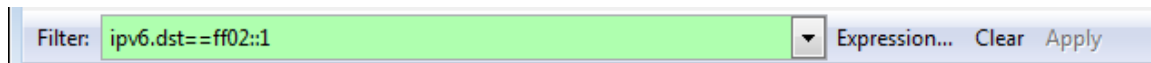
```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

- Detenga la captura de tráfico con Wireshark en la NIC de la PC-A.
- Restablezca la configuración de IPv6 en la PC-A para eliminar la configuración de DHCPv6 sin estado.
 - Abra la ventana Propiedades de conexión de área local, desactive la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y haga clic en **Aceptar** para aceptar el cambio.
 - Vuelva a abrir la ventana Propiedades de conexión de área local, haga clic para habilitar la casilla de verificación **Protocolo de Internet versión 6 (TCP/IPv6)** y, a continuación, haga clic en **Aceptar** para aceptar el cambio.

Parte 4: configurar la red para DHCPv6 con estado

Paso 1: preparar la PC-A.

- Inicie una captura del tráfico en la NIC con Wireshark.
- Filtre la captura de datos para ver solo los mensajes RA. Esto se puede realizar mediante el filtrado de paquetes IPv6 con una dirección de destino FF02::1, que es la dirección de solo unidifusión del grupo de clientes.



Paso 2: cambiar el pool de DHCPv6 en el R1.

- Agregue el prefijo de red al pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64
```

- Cambie el nombre de dominio a **ccna-statefulDHCPv6.com**.

Nota: debe eliminar el antiguo nombre de dominio. El comando **domain-name** no lo reemplaza.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

- Verifique la configuración del pool de DHCPv6.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in
  use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 0
```

- Ingrese al modo de depuración para verificar la asignación de direcciones de DHCPv6 con estado.

```
R1# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

Paso 3: establecer el indicador en G0/1 para DHCPv6 con estado.

Nota: la desactivación de la interfaz G0/1 antes de realizar cambios asegura que se envíe un mensaje RA cuando se activa la interfaz.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```

Paso 4: habilitar la interfaz F0/6 en el S1.

Ahora que configuró el R1 para DHCPv6 con estado, puede volver a conectar la PC-A a la red activando la interfaz F0/6 en el S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

Paso 5: verificar la configuración de DHCPv6 con estado en el R1.

- Emita el comando **show ipv6 interface g0/1** para verificar que la interfaz esté en el modo DHCPv6 con estado.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:2
  FF02::1:FF00:1
  FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use DHCP to obtain routable addresses.
Hosts use DHCP to obtain other configuration.
```

- En el símbolo del sistema de la PC-A, escriba **ipconfig /release6** para liberar la dirección IPv6 asignada actualmente. Luego, escriba **ipconfig /renew6** para solicitar una dirección IPv6 del servidor de DHCPv6.
- Emita el comando **show ipv6 dhcp pool** para verificar el número de clientes activos.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
  Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in
  use, 0 conflicts)
  DNS server: 2001:DB8:ACAD:A::ABCD
  Domain name: ccna-StatefulDHCPv6.com
  Active clients: 1
```

- d. Emita el comando **show ipv6 dhcp binding** para verificar que la PC-A haya recibido su dirección IPv6 de unidifusión del pool de DHCP. Compare la dirección de cliente con la dirección IPv6 link-local en la PC-A mediante el comando **ipconfig /all**. Compare la dirección proporcionada por el comando **show** con la dirección IPv6 que se indica con el comando **ipconfig /all** en la PC-A.

```
R1# show ipv6 dhcp binding
Client: FE80::D428:7DE2:997C:B05A
DUID: 0001000117F6723D000C298D5444
Username : unassigned
IA NA: IA ID 0x0E000C29, T1 43200, T2 69120
Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE
preferred lifetime 86400, valid lifetime 172800
expires at Mar 07 2013 04:09 PM (171595 seconds)
```

```
Adaptador de Ethernet Conexión de área local:
Sufijo DNS específico para la conexión. . : ccna-StatefulDHCPv6.com
Descripción . . . . . : Conexión de red Intel(R) PRO/1000
MT
Dirección física. . . . . : 00-0C-29-E3-23-17
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferido>
Concesión obtenida. . . . . : jueves, 05 de septiembre de 2013
16:07:59
La concesión expira . . . . . : jueves, 05 de septiembre de 2013
16:38:03
Dirección IPv6 . . . . . : 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferido>
Vínculo: dirección IPv6 local. . . : fe80::d428:7de2:997c:b05a%11<Preferido>
Dirección IPv4. . . . . : 192.168.96.139<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . : fe80::1%11
IAID DHCPv6 . . . . . : 234884137
DUID de cliente DHCPv6. . . . . : 00-01-00-01-19-A7-DD-BE-00-0C-29-E3-23-17
Servidores DNS. . . . . : 2001:db8:acad:a::abcd
NetBIOS sobre TCP/IP. . . . . : habilitado
```

- e. Emita el comando **undebg all** en el R1 para detener la depuración de DHCPv6.

Nota: escribir **u all** es la forma más abreviada de este comando y sirve para saber si quiere evitar que los mensajes de depuración se desplacen hacia abajo constantemente en la pantalla de la sesión de terminal. Si hay varias depuraciones en proceso, el comando **undebg all** las detiene todas.

```
R1# u all
Se ha desactivado toda depuración posible
```

- f. Revise los mensajes de depuración que aparecieron en la pantalla de terminal del R1.

1) Examine el mensaje de solicitud de la PC-A que solicita información de red.

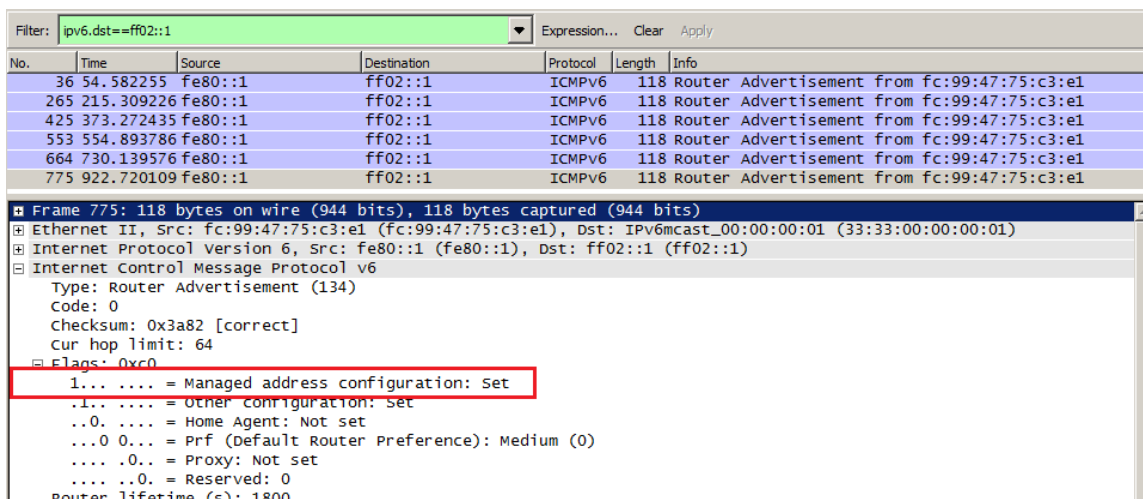
```
*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on GigabitEthernet0/1
*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.775: dst FF02::1:2
*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238
*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2
*Mar 5 16:42:39.775: elapsed-time 6300
*Mar 5 16:42:39.775: option CLIENTID(1), len 14
```

2) Examine el mensaje de respuesta enviado a la PC-A con la información de red DHCP.

```
*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on
GigabitEthernet0/1
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.779: src FE80::1
*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```

Paso 6: verificar DHCPv6 con estado en la PC-A.

- Detenga la captura de Wireshark en la PC-A.
- Expanda el mensaje RA más reciente que se indica en Wireshark. Verifique que se haya establecido el indicador **Managed address configuration** (Configuración de dirección administrada).



- Cambie el filtro en Wireshark para ver solo los paquetes **DHCPv6** escribiendo **dhcpv6** y, a continuación, haga clic en **Apply** (Aplicar). Resalte la última respuesta DHCPv6 de la lista y expanda la información de DHCPv6. Examine la información de red DHCPv6 incluida en este paquete.

Filter: dhcpv6		Expression... Clear Apply				
No.	Time	Source	Destination	Protocol	Length	Info
250	443.078236	fe80::d428:7de2:997:ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
267	475.083284	fe80::d428:7de2:997:ff02::1:2		DHCPv6	146	Solicit XID: 0x2b2a8e CID: 0001000117f6723d000c2
425	656.281211	fe80::d428:7de2:997:ff02::1:2		DHCPv6	146	Solicit XID: 0xc86c32 CID: 0001000117f6723d000c2
429	656.282249	fe80::1	fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Advertise XID: 0xc86c32 CID: 0001000117f6723d000c2
460	657.292018	fe80::d428:7de2:997:ff02::1:2		DHCPv6	188	Request XID: 0xc86c32 CID: 0001000117f6723d000c2
462	657.292638	fe80::1	fe80::d428:7de2:997:ff02::1:2	DHCPv6	191	Reply XID: 0xc86c32 CID: 0001000117f6723d000c298
Ethernet II, Src: fc:99:47:75:c3:e1 (Fc:99:47:75:c3:e1), Dst: Vmware_be:6c:89 (00:50:56:be:6c:89)						
Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: fe80::d428:7de2:997c:b05a (fe80::d428:7de2:997c:b05a)						
User Datagram Protocol, Src Port: dhcpv6-server (547), Dst Port: dhcpv6-client (546)						
DHCPv6						
Message type: Reply (7)						
Transaction ID: 0xc86c32						
Server Identifier: 00030001fc994775c3e0						
Client Identifier: 0001000117f6723d000c298d5444						
Identity Association for Non-temporary Address						
Option: Identity Association for Non-temporary Address (3)						
Length: 40						
Value: 0e000c290000a8c000010e000005001820010db8acad000a...						
IAID: 0e000c29						
T1: 43200						
T2: 69120						
IA Address: 2001:db8:acad:a:b55c:8519:8915:57ce						
DNS recursive name server						
Option: DNS recursive name server (23)						
Length: 16						
Value: 2001:db8:acad:000a:0000:0000:0000:abcd						
DNS servers address: 2001:db8:acad:a:abcd						
Domain Search List						
Option: Domain Search List (24)						
Length: 25						
Value: 1363636e612d537461746566756c44484350763603636f6d...						
DNS Domain Search List						
Domain: ccna-StatefulDHCPv6.com						

Reflexión

- ¿Qué método de direccionamiento IPv6 utiliza más recursos de memoria en el router configurado como servidor de DHCPv6: DHCPv6 sin estado o DHCPv6 con estado? ¿Por qué?

DHCPv6 usa más recursos de memoria – DHCPv6 con estado requiere que el router guarde dinámicamente el estado de información acerca de los clientes, DHCPv6 sin estado los clientes no necesita servidor para obtener información de las direcciones, así que no necesitan ser guardadas.

- ¿Qué tipo de asignación dinámica de direcciones IPv6 recomienda Cisco: DHCPv6 sin estado o DHCPv6 con estado?

Cisco recomienda la versión DHCPv6 sin estado cuando implementa y desarrolla redes en IPv6 sin un registro de red cisco, (CNR).

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	Interfaz Ethernet #1	Interfaz Ethernet n.º 2	Interfaz serial #1	Interfaz serial n.º 2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de IOS de Cisco para representar la interfaz.				

CONCLUSIONES

Durante todos los trabajos colaborativos, aunque individualmente realizados tambien se creó integración y esfuerzo que nos permitió el desarrollo de cada una de las practicas presentadas, todo esto conllevando a un aprendizaje mutuo y trabajo incansable para lograr los objetivos propuestos.

Se lograron las metas aprendiendo con el simulador Packet Tracer de Cisco, donde realizamos configuraciones de una forma practica e interactiva y bastante real que nos permite tener mas claro al momento de llevar esto a un ambiente laboral dado que hay muy poca diferencia para con los equipos físicos de Cisco donde se aplicara todo este conocimiento y practica realizadas.

Teniendo en cuenta que Cisco es una de las empresas mejor ubicadas en cuanto a equipos de redes y telecomunicaciones se refiere, es para nosotros una herramienta de muchísimo valor el poder demostrar que el aprendizaje obtenido durante este diplomado nos permitirá abrir puertas para poder continuar con el mismo y así forjar mejor nuestro futuro laboral.

REFERENCIAS BIBLIOGRAFICAS Y CIBERGRAFIA

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación.

Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

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

Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de:

<https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y

Conmutación. Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>