



Capítulo 7

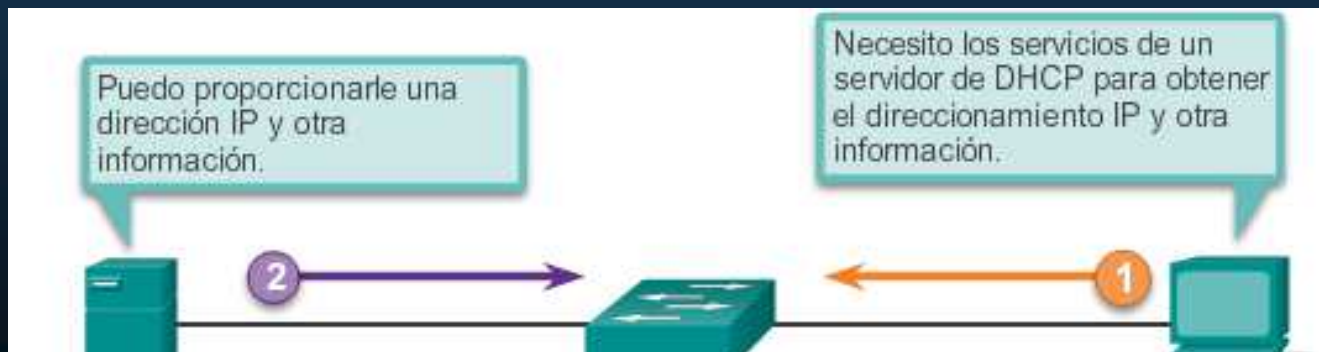
DHCPv4

<https://contenthub.netacad.com/srwe/7.1.1>

Conceptos de DHCPv4

• Cliente y Servidor DHCPv4

- DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica.
- Un servidor dedicado DHCPv4 es escalable y fácil de administrar.
 - Para SOHO, un router Cisco puede brindar un servidor DHCPv4 integrado.
 - Dinámicamente arrenda direcciones IPv4 de un pool, por un periodo limitado (administrable de 24 horas a una semana).
 - Cuando el arrendamiento termina la IPv4 regresa al pool.
- Los clientes arrendan su configuración IPv4 del servidor.
 - Al finalizar el arrendamiento, debe solicitar uno nuevo.



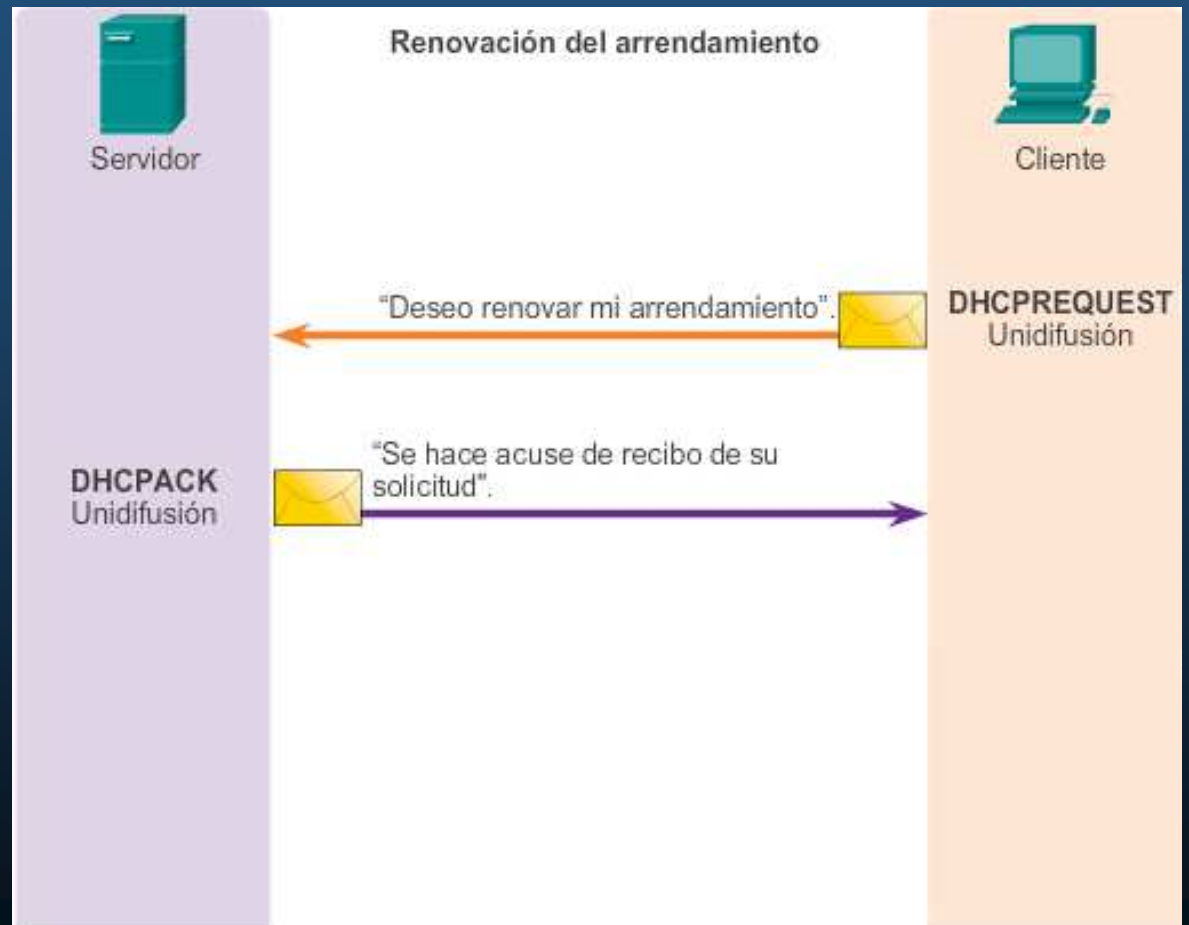
El arrendamiento permite sobrellevar el agotamiento del pool cuando un cliente abandona la red, sin avisar.

Conceptos de DHCPv4

- Pasos para un Arrendamiento y Renovación

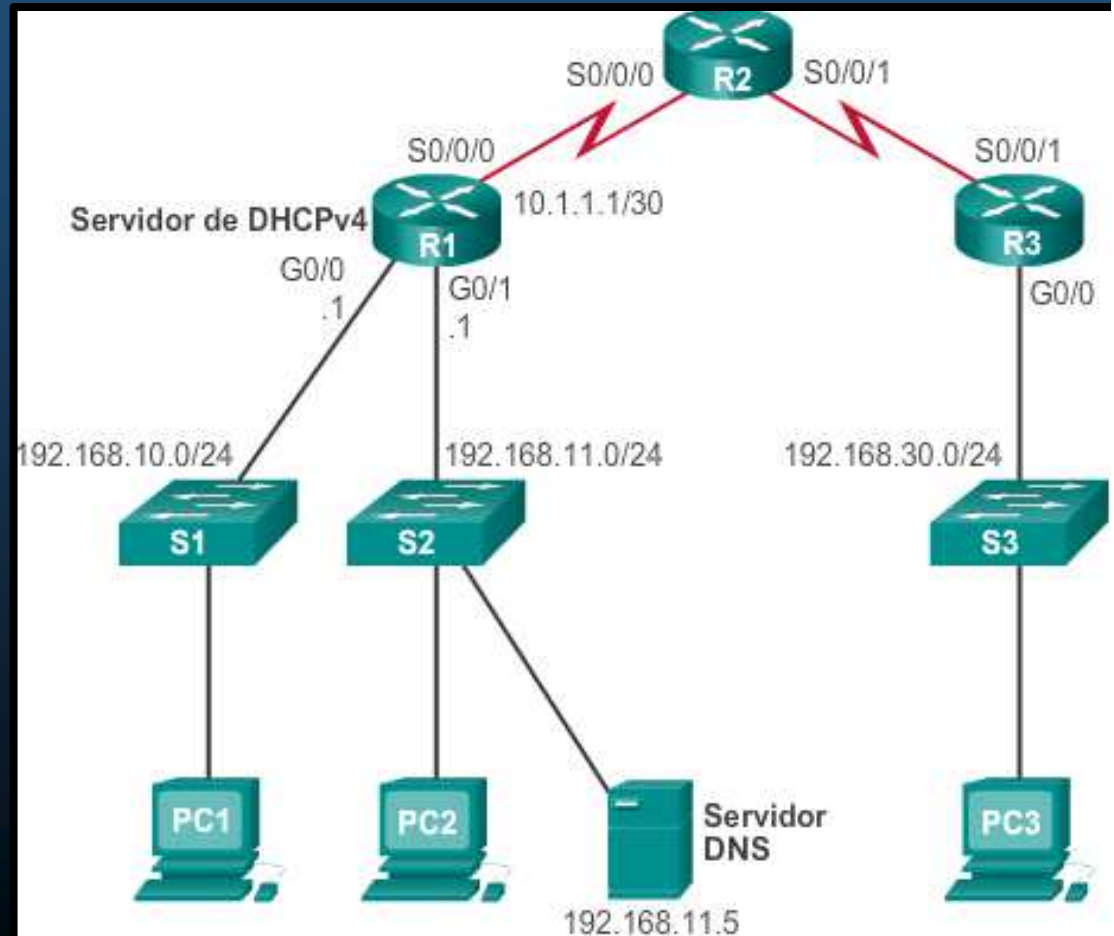
- Arrendamiento
 - 1. DHCP Discover (DHCPDISCOVER)
 - 2. DHCP Offer (DHCPOFFER)
 - 3. DHCP Request (DHCPREQUEST)
 - 4. DHCP Acknowledgment (DHCPACK)

- Renovación
 - 1. DHCP Request (DHCPREQUEST)
 - 2. DHCP Acknowledgment (DHCPACK)



Configurar un servidor DHCPv4 en IOS de Cisco

- Configuración de un servidor de DHCPv4 en IOS de Cisco
 - El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4.
 - **Paso 1.** Excluir direcciones IPv4
 - **Paso 2.** Definir el nombre de un pool DHCPv4
 - **Paso 3.** Configurar el pool DHCPv4.



Configurar un servidor DHCPv4 en IOS de Cisco

- Configuración de un servidor de DHCPv4 en IOS de Cisco
 - Paso 1. Excluir direcciones IPv4
 - (config)# ip dhcp excluded-address
 - Se puede excluir una única dirección o un rango de direcciones.
 - Generalmente, algunas IPv4s se reservan para su uso estático.
 - Por lo tanto, estas direcciones no deben asignarse por DHCP.

```
R1(config)# ip dhcp excluded-address low-address [high-address]
```

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9  
R1(config)# ip dhcp excluded-address 192.168.10.254
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Configuración de un servidor de DHCPv4 en IOS de Cisco
 - Paso 2. Configurar un pool de DHCPv4
 - Definir el nombre de un conjunto de direcciones a repartir.

```
R1(config)# ip dhcp pool pool-name  
R1(dhcp-config)#
```

```
R1(config)# ip dhcp pool LAN-POOL-1  
R1(dhcp-config)#
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Configuración de un servidor de DHCPv4 en IOS de Cisco
 - Paso 3. Configurar tareas específicas
 - Usar `network` para definir el rango de direcciones disponibles.
 - Usar `default-router` para definir el router de gateway predeterminado.

Tareas requeridas	Comando
Definir el conjunto de direcciones.	<code>network</code> número-red [máscara /longitud-prefijo]
Definir el router o gateway predeterminado.	<code>default-router</code> dirección [dirección2...dirección8]

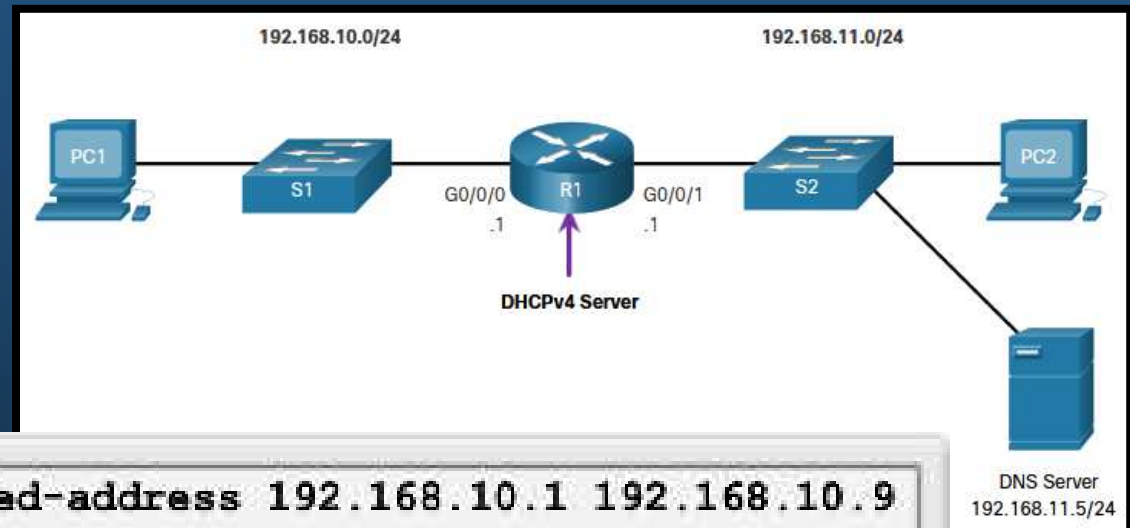
Tareas opcionales	Comando
Definir un servidor DNS.	<code>dns-server</code> dirección [dirección2...dirección8]
Definir el nombre de dominio.	<code>domain-name</code> dominio
Definir la duración de la concesión DHCP.	<code>lease</code> {días [horas] [minutos] infinito}
Definir el servidor WINS con NetBIOS.	<code>netbios-name-server</code> dirección [dirección2...dirección8]

Configurar un servidor DHCPv4 en IOS de Cisco

- Configuración de un servidor de DHCPv4 en IOS de Cisco

- Ejemplo de DHCPv4

- DHCPv4 configurado en R1, para la LAN 192.168.10.0/24.



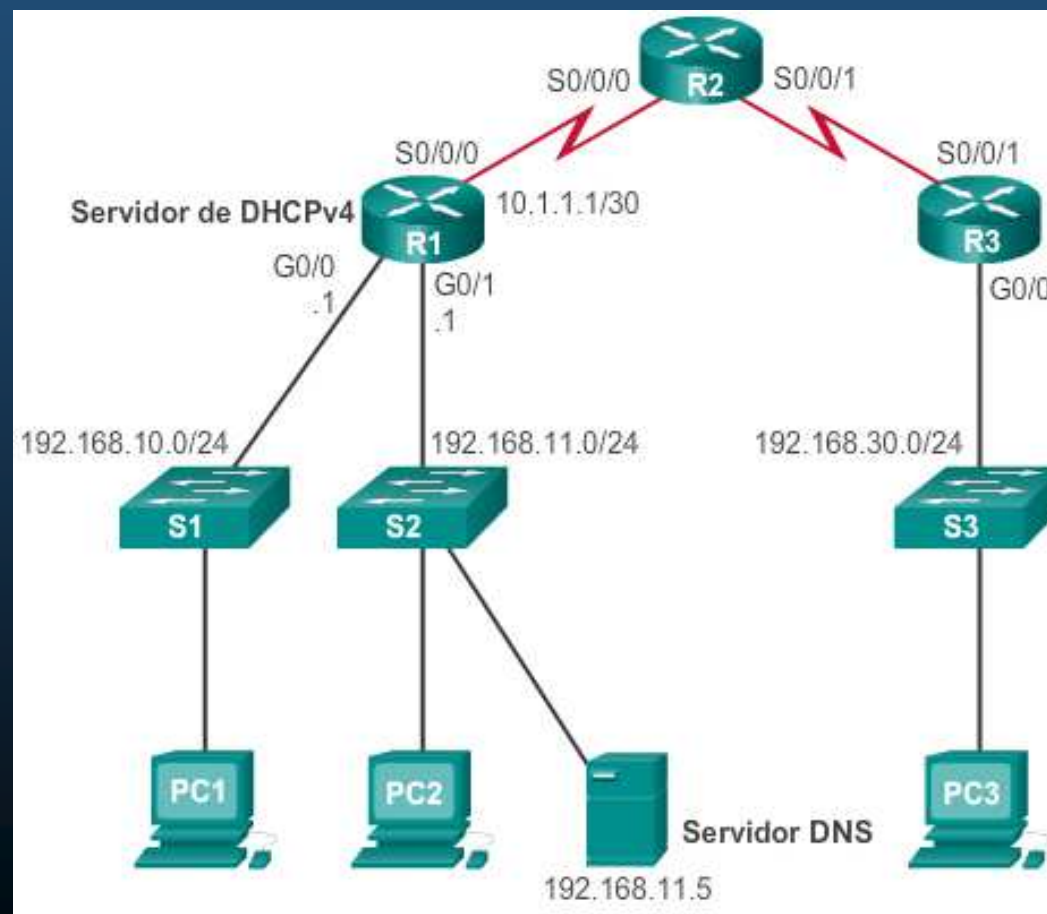
```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```


Configurar un servidor DHCPv4 en IOS de Cisco

- Comandos de Verificación de DHCPv4
 - Pueden utilizarse los siguientes comandos:
 - **show running-config | section dhcp**
 - Despliega los comandos con los que se configuró el router.
 - **show ip dhcp binding.**
 - Muestra lista de vinculaciones de IPv4 con la dirección MAC proporcionadas por DHCPv4.
 - **show ip dhcp server statistics,**
 - Verifica si el router recibe o envía los mensajes. Muestra conteos de la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

Configurar un servidor DHCPv4 en IOS de Cisco

- Verificar que DHCPv4 es Operacional
 - Ejemplo: se configuró R1 para que proporcione servicios DHCPv4. Dado que la PC1 no se encendió, no tiene una dirección IP.



Configurar un servidor DHCPv4 en IOS de Cisco

- Verificación de la Configuración de DHCPv4
 - `show running-config | section dhcp,`

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.11.254
ip dhcp pool LAN-POOL-1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
  domain-name example.com
ip dhcp pool LAN-POOL-2
  network 192.168.11.0 255.255.255.0
  default-router 192.168.11.1
  dns-server 192.168.11.5
  domain-name example.com
R1#
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Verificación de Vinculaciones y Estadísticas DHCPv4

- `show ip dhcp binding`.
Muestra lista de vinculaciones de IPv4 con la dirección MAC proporcionadas por DHCPv4.

- `show ip dhcp server statistics`,
Verifica si el router recibe o envía los mensajes. Muestra conteos de la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration  Type
                Hardware address/
                User name

R1# show ip dhcp server statistics
Memory usage      23543
Address pools     1
Database agents   0
Automatic bindings 0
Manual bindings   0
Expired bindings  0
Malformed messages 0
Secure arp entries 0

Message           Received
BOOTREQUEST       0
DHCPDISCOVER      0
DHCPREQUEST       0
DHCPDECLINE       0
DHCPRELEASE       0
DHCPIFORM         0

Message           Sent:
BOOTREPLY         0
DHCPOFFER         0
DHCPACK           0
DHCPNAK           0
R1#
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Verificar que el Cliente DHCPv4 recibió dirección IPv4
 - `ipconfig /all`
 - En una PC, despliega los parámetros TCP/IP arrendados.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration

Host Name . . . . . : ciscolab
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : example.com
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 00-05-9A-3C-7A-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.10.10
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Saturday, September 14, 2019 8:42:22AM
Lease Expires . . . . . : Sunday, September 15, 2019 8:42:22AM
Default Gateway . . . . . : 192.168.10.1
DHCP Server . . . . . : 192.168.10.1
DNS Servers . . . . . : 192.168.11.5
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Verificación de Vinculaciones y Estadísticas DHCPv4
 - Mismos comandos después de arrancar PC1 y PC2.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration    Type
                Hardware address/
                User name
192.168.10.10   0100.e018.5bdd.35  May 28 2013 01:06 PM Automatic
192.168.11.10   0100.b0d0.d817.e6  May 28 2013 01:10 PM Automatic

R1# show ip dhcp server statistics
Memory usage      25307
Address pools     2
Database agents   0
Automatic bindings 2
Manual bindings   0
Expired bindings  0
Malformed messages 0
Secure arp entries 0

Message           Received
BOOTREQUEST       0
DHCPDISCOVER      8
DHCPREQUEST       3
DHCPDECLINE       0
DHCPRELEASE       0
DHCPINFORM        0

Message           Sent
BOOTREPLY         0
DHCPOFFER         3
DHCPACK           3
DHCPNAK           0
R1#
```

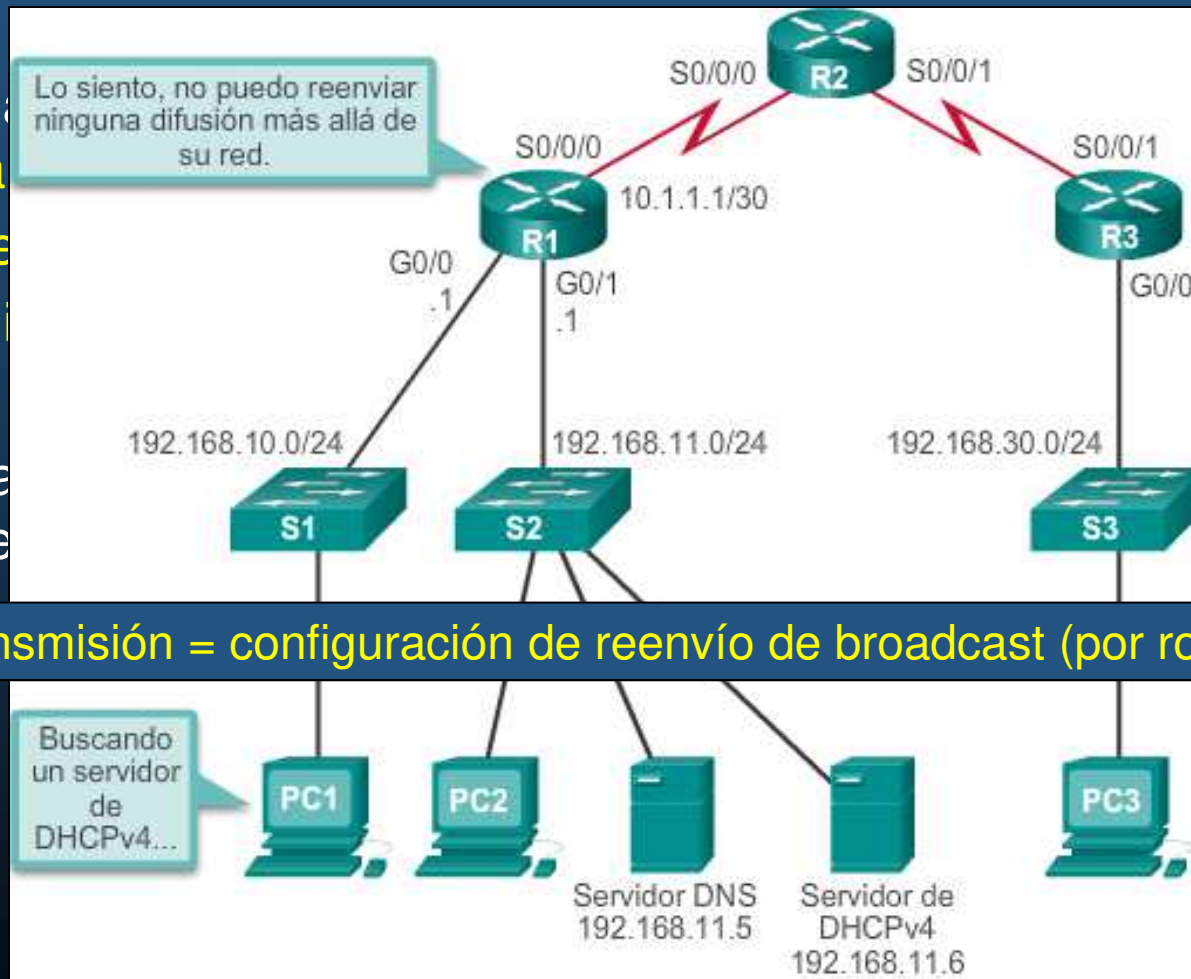
Configurar un servidor DHCPv4 en IOS de Cisco

- Deshabilitación de DHCPv4
 - Habilitado, de manera predeterminada. Deshabilitar con:
 - `(config)# no service dhcp`
 - Habilitar el proceso:
 - `(config)# service dhcp`
 - Si los parámetros no se configuran, habilitar el servicio no tiene ningún efecto.

Configurar un servidor DHCPv4 en IOS de Cisco

- Retransmisión de DHCPv4

- En una granja
- Se
- Cl
- Pa
- fre



dos en una

clientes con

Configurar un servidor DHCPv4 en IOS de Cisco

- Retransmisión de DHCPv4

- Una PC puede liberar su configuración IP (arrendamiento), con:

- `ipconfig /release`

```
C:\Users\Student> ipconfig /release
Windows IP Configuration
Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . :
    Default Gateway . . . . . :
```

Configurar un servidor DHCPv4 en IOS de Cisco

- Retransmisión de DHCPv4

- Una PC puede intentar renovar su arrendamiento de configuración IPv4 con:

- `ipconfig /renew`

```
C:\Users\Student> ipconfig /renew
Windows IP Configuration
An error occurred while renewing interface Ethernet0 : unable to connect to your DHCP
server. Request has timed out.
```

- Puede fallar si no se ha configurado adecuadamente la retransmisión.

Configurar un servidor DHCPv4 en IOS de Cisco

- Retransmisión de DHCPv4

- La interfaz en el router que retransmitirá la difusión se configura con:

- `(config-if)# ip helper-address DHPC-ip`

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<resultado omitido>
```

- Verificar la interfaz en el router que retransmite la difusión con:

- `# show ip interface <interface_id>`

Configurar un servidor DHCPv4 en IOS de Cisco

- Retransmisión de DHCPv4
 - Una PC puede verificar su arrendamiento de configuración IP, con:
 - `ipconfig /all`

```
C:\Users\Student> ipconfig /all
Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : example.com
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

Configurar un servidor DHCPv4 en IOS de Cisco

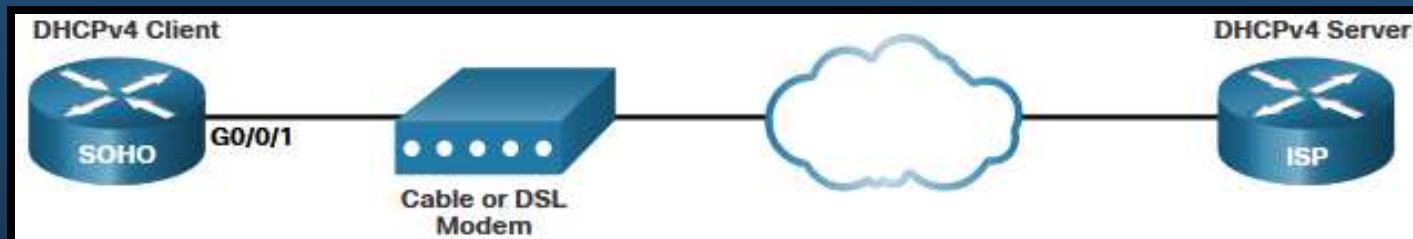
- Otros Servicios que usan Retransmisión de Broadcast.
 - DHCPv4 no es el único servicio que se retransmite.
 - `(config-if)# ip helper-address`
reenvía los siguientes ocho siguientes servicios UDP:
 - Puerto 37: Tiempo
 - Puerto 49: TACACS
 - Puerto 53: DNS
 - Puerto 67: cliente DHCP/BOOTP
 - Puerto 68: servidor de DHCP/BOOTP
 - Puerto 69: TFTP
 - Puerto 137: servicio de nombres NetBIOS
 - Puerto 138: servicio de datagrama NetBIOS

Configuración de cliente DHCPv4

- Configuración de un router como cliente DHCPv4

- Habrá ocasiones en que se deba arrendar una IP de un ISP:
 - Uso de interfaz Ethernet para conectarse a un cable módem o un módem DSL.

```
(config-if)# ip address dhcp.
```



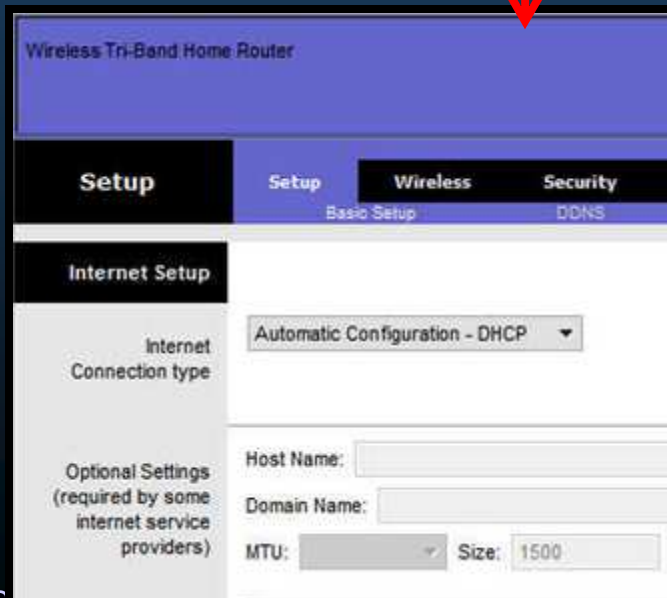
```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<resultado omitido>
```

Configuración de cliente DHCPv4

- Configuración de un router SOHO como cliente DHCPv4

- Un router como el Linksys EA6500 se configura mediante una interfáz web.
 - Por defecto la configuración WAN predeterminada establece:
 - Automatic Configuration - DHCP (Configuración automática, DHCP).

- PacketTracer presenta interface similar.



Resolución de Problemas de DHCPv4

- Tareas de problemas DHCPv4

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.	<code># show ip dhcp conflict</code>
Tarea 2 de la resolución de problemas:	Verificar la conectividad física.	<code># show interface <i>interfaz</i></code>
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv4 estática.	Si hay conectividad, no es culpa del DHCP
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.	Puede ser alguna configuración de puerto.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.	Si local y no remoto, checar redistribución.

Resolución de Problemas de DHCPv4

- Verificación de configuración DHCPv4

```
R1# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.11.6
 duplex auto
 speed auto
R1#

R1# show running-config | include no service dhcp
R1#
```

Si no está deshabilitado, significa que está activo

Resolución de Problemas de DHCPv4

- Depuración DHCPv4

```
R1(config)# access-list 100 permit udp any any eq 67
R1(config)# access-list 100 permit udp any any eq 68
R1(config)# end
R1# debug ip packet 100
IP packet debugging is on for access list 100
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
rcvd 2
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
stop process pak for forus packet
*IP: s=192.168.11.1 (local), d=255.255.255.255
(GigabitEthernet0/1), len 328, sending broad/multicast

<resultado omitido>

R1# debug ip dhcp server events
DHCPD: returned 192.168.10.11 to address pool LAN-POOL-1
DHCPD: assigned IP address 192.168.10.12 to client
0100.0103.85e9.87.
DHCPD: checking for expired leases.
DHCPD: the lease for address 192.168.10.10 has expired.
DHCPD: returned 192.168.10.10 to address pool LAN-POOL-1
```

Puertos comunes DHCP

Tráfico DHCP

Eventos DHCP

TAREA

(Sin Calificación)

7.4.1. Implementación de DHCPv4 en Packet Tracer

<https://contenthub.netacad.com/srwe/7.4.1>

La actividad práctica de éste capítulo, se integrará con la del capítulo 8.



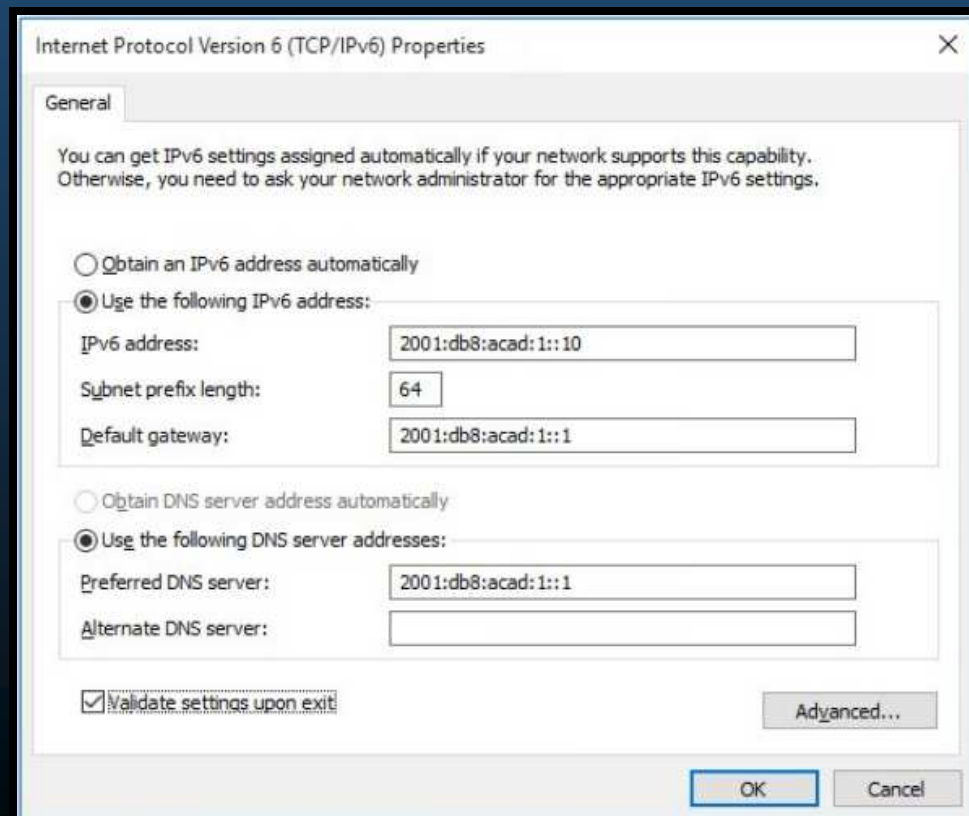
Capítulo 8

SLAAC & DHCPv6

<https://contenthub.netacad.com/srwe/8.1.1>

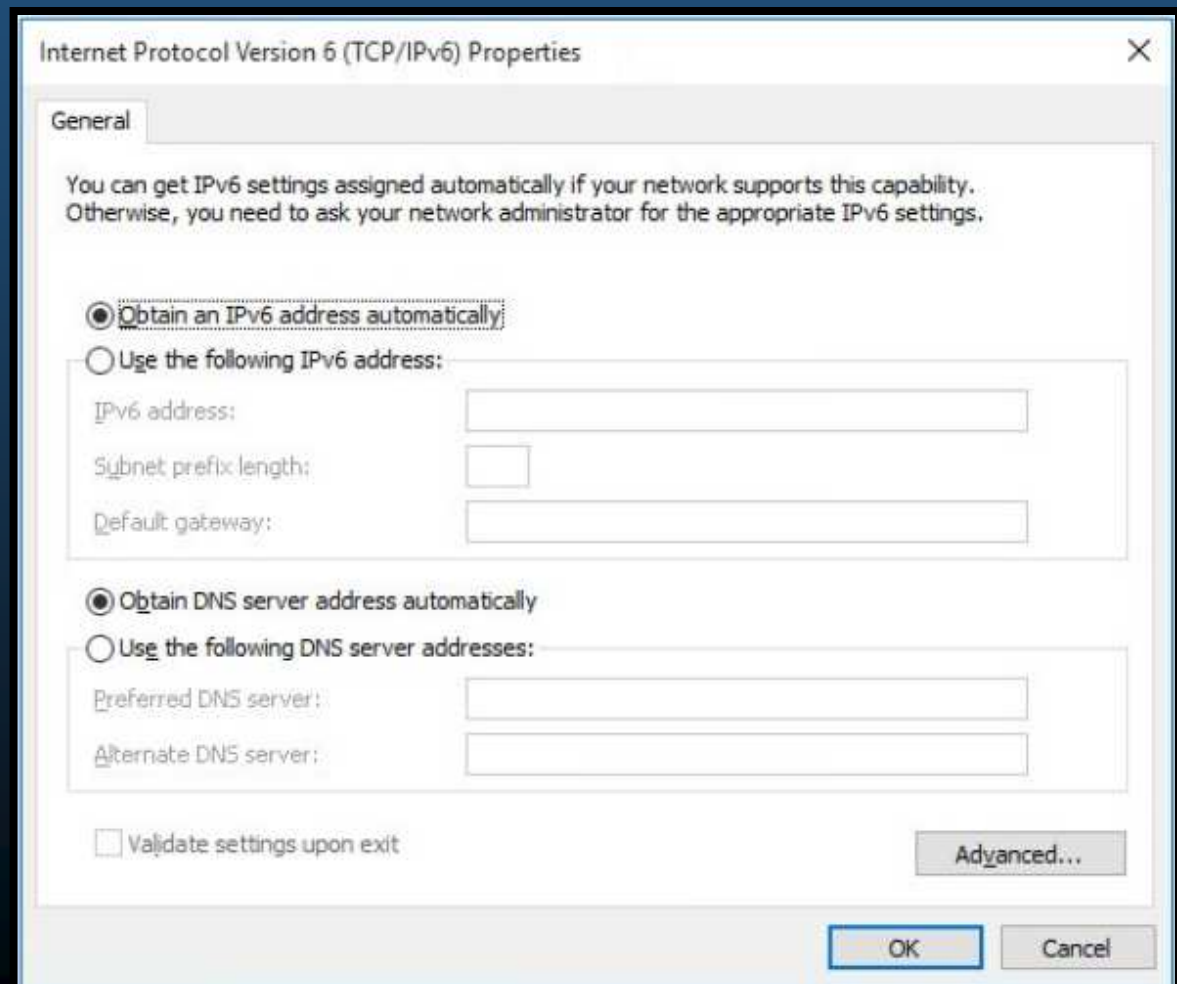
Configuración de Host IPv6

- Configuración de un host IPv6
 - Configuraciones GUA (Global Unicast Address) y LLAs (Local-Link Address).
 - En un Router Cisco:
 - `(config-if)# ipv6 address ipv6-address [/prefix-length] [local-link]`
 - En un host Windows:



Configuración de Host IPv6

- Configuración de un host IPv6
 - Configuraciones GUA Automática (Global Unicast Address)
 - En un host Windows:



Configuración de Host IPv6

- Direcciones Link-Local en un host IPv6
 - GUA automática implica uno de 3 métodos de RAs (Router Advertisements) de ICMPv6:
 - Un Router IPv6 envía RAs a su LAN sugiriendo a los hosts cómo obtener su configuración IPv6.
 - Las direcciones Link-local IPv6 se crean automáticamente cuando inicia el host.

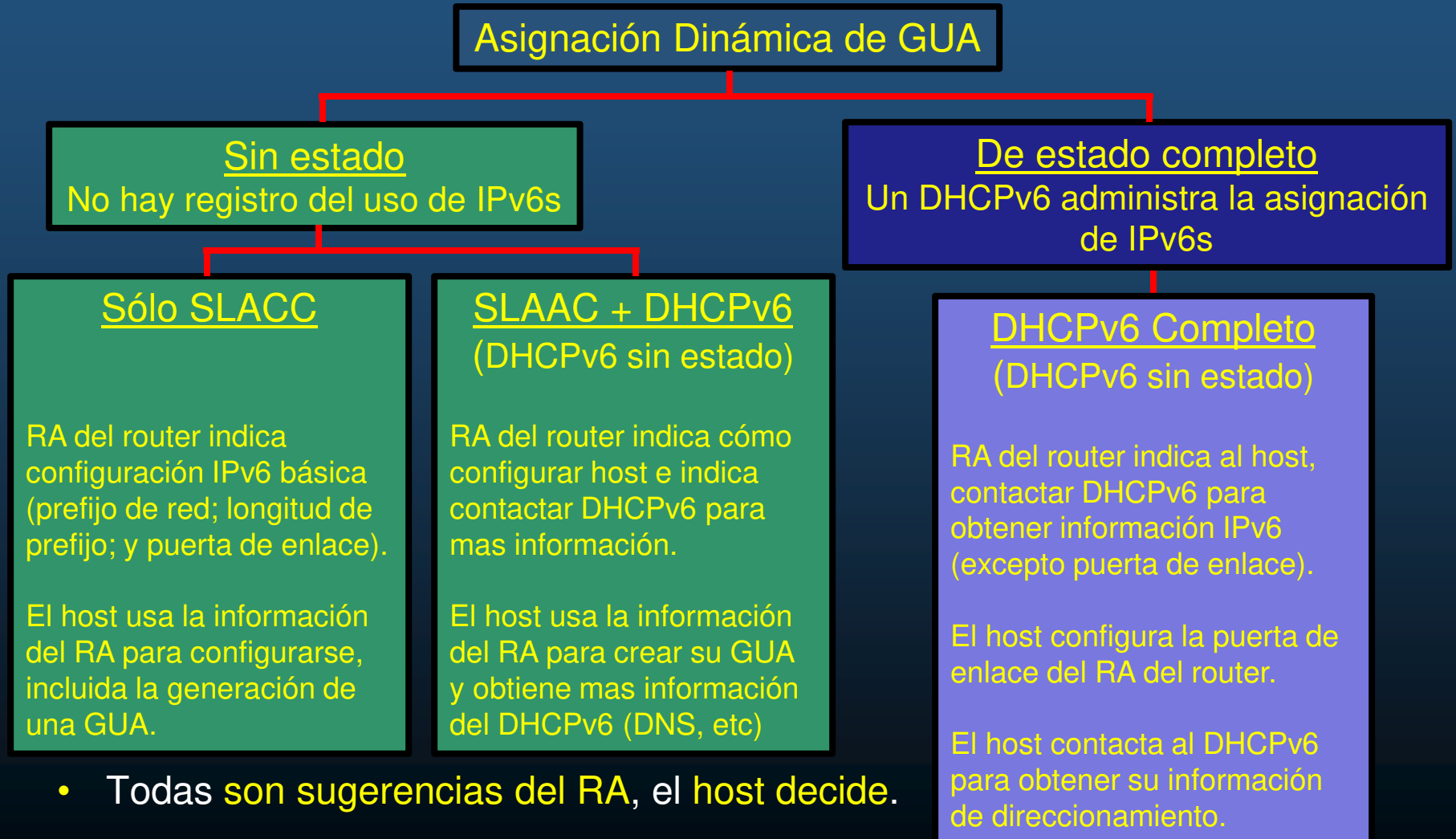
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . :
    Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
    IPv4 Address. . . . . : 169.254.202.140
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
```

- Aún si no hay GUA asignada.
- El signo % y un número subsecuente indican un ID de zona o ambiente
 - Utilizado por el S.O. para identificar la interface asociada.

Configuración de Host IPv6

- Asignación de GUA IPv6



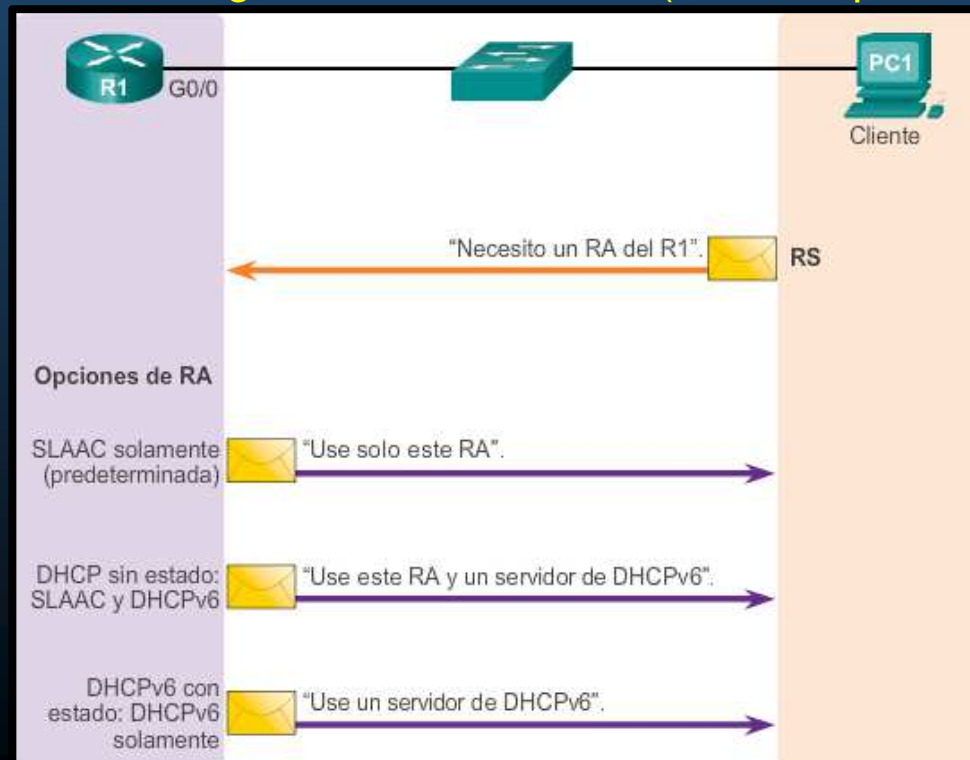
- Todas son sugerencias del RA, el host decide.

Configuración de Host IPv6

- Banderas de los mensajes RA

- La indicación de cómo deberá actuar el host está dada por 3 banderas:

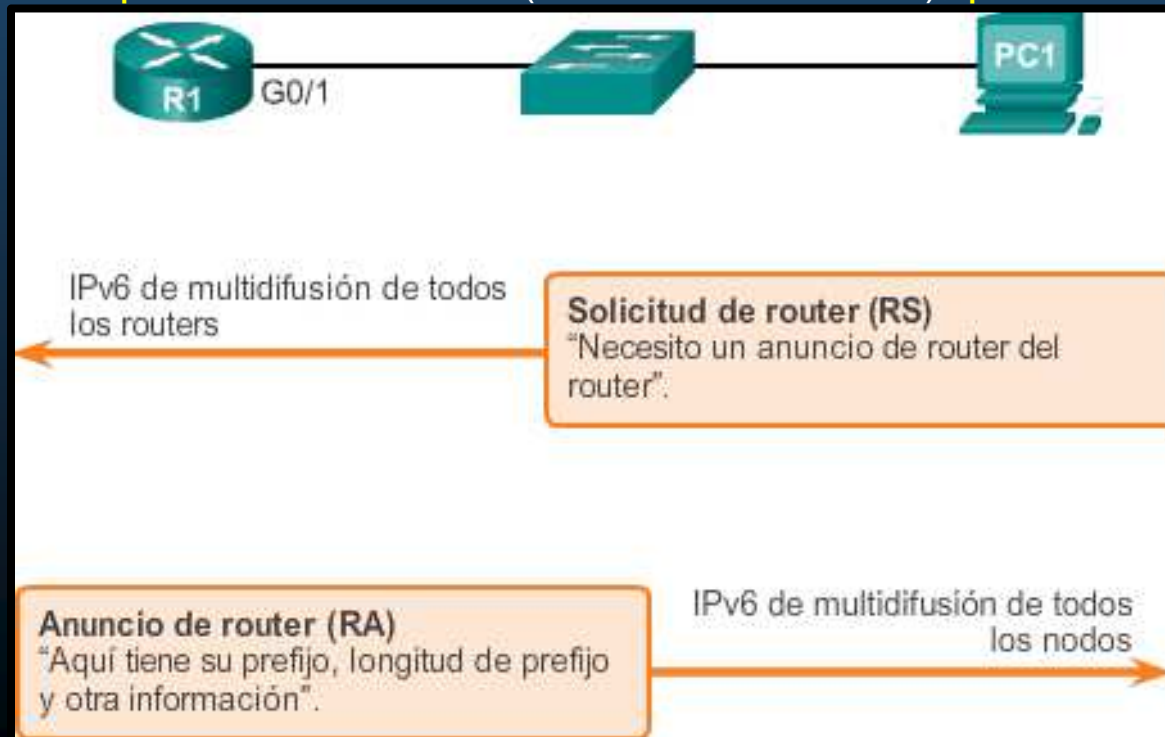
- A – Bandera de autoconfiguración de dirección (SLAAC para crear GUA)
- O – Bandera de más configuración disponible por DHCPv6.
- M – Bandera de configuración Administrada (DHCPv6 para GUA con Estado Total)



SLAAC

- Introducción a SLAAC.

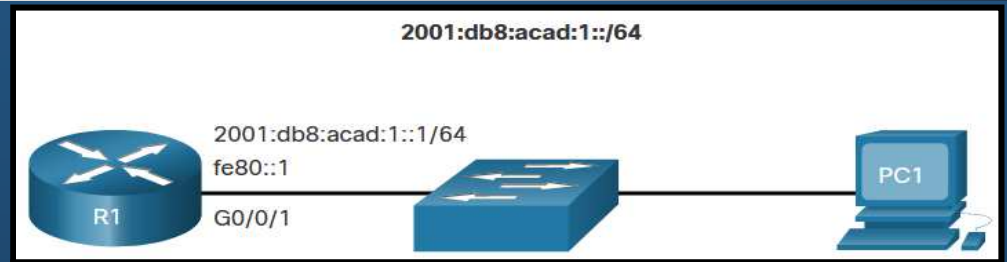
- SLAAC permite a hosts crear una GUA única sin DHCPv6.
 - Sin estado, no hay registro de que IPv6s están en uso/disponibles.
 - Usa mensajes RA de ICMPv6 para proveer información de direccionamiento a hosts.
 - Un host puede usar un RS (Router Solicitation), para solicitar un RA.



SLAAC

- **Habilitar SLAAC**

- **Verificar direccionamiento IPv6.**
 - Debe haber una IPv6 asignada a la interface donde habilitar SLAAC.
- El router debe **habilitar IPv6 para enviar RAs:**
- **Verificar SLAAC:**
 - El router debe **responder a las direcciones multicast: ff02::1 y ff02::2**



```
R1# show ipv6 interface G0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1
No Virtual link-local address(es):
Description: Link to LAN
Global unicast address(es):
  2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
(output omitted)
```

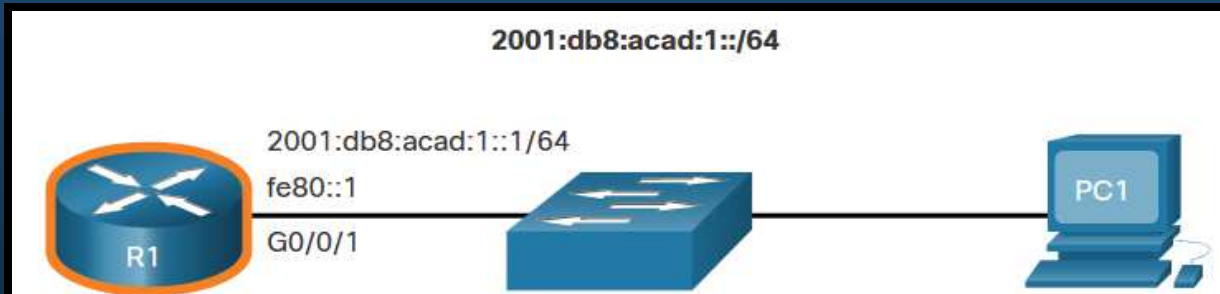
```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
```

```
R1# show ipv6 interface G0/0/1 | section Joined
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
R1#
```

SLAAC

- Mecanismo Sólo SLAAC

- Predeterminada Cisco al configurar `ipv6 unicast routing`
 - Tanto **M** como **O** están en 0 en el RA.
 - **A** está en 1, indicando al host autogenerar su **GUA** usando el prefijo del RA + **EUI-64**, o aleatoriamente.



La puerta de enlace solo puede ser obtenida desde RAs (Nunca del DHCP).

RA Message

Flag	value
A	1
O	0
M	0

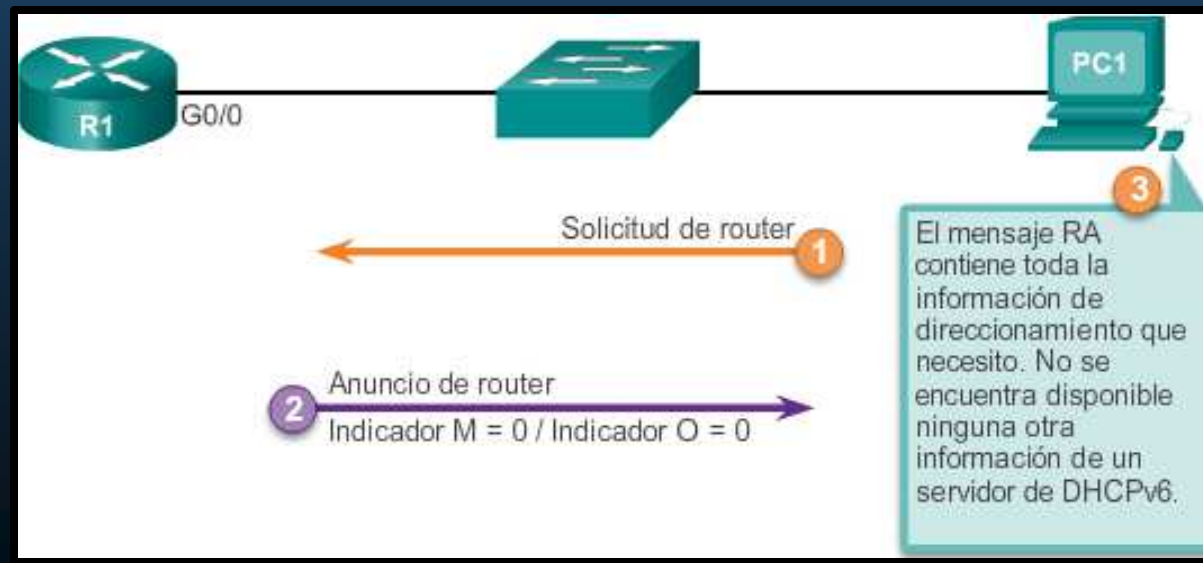
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . . :
    IPv6 Address. . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
    Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
    IPv4 Address. . . . . : 169.254.202.140
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1%6
C:\PC1>
```

SLAAC

- Mecanismo Sólo SLAAC

- Los Mensajes RA se configuran en una interfaz de un router.
 - Restablecer indicadores M y O a sus valores iniciales de 0 con:

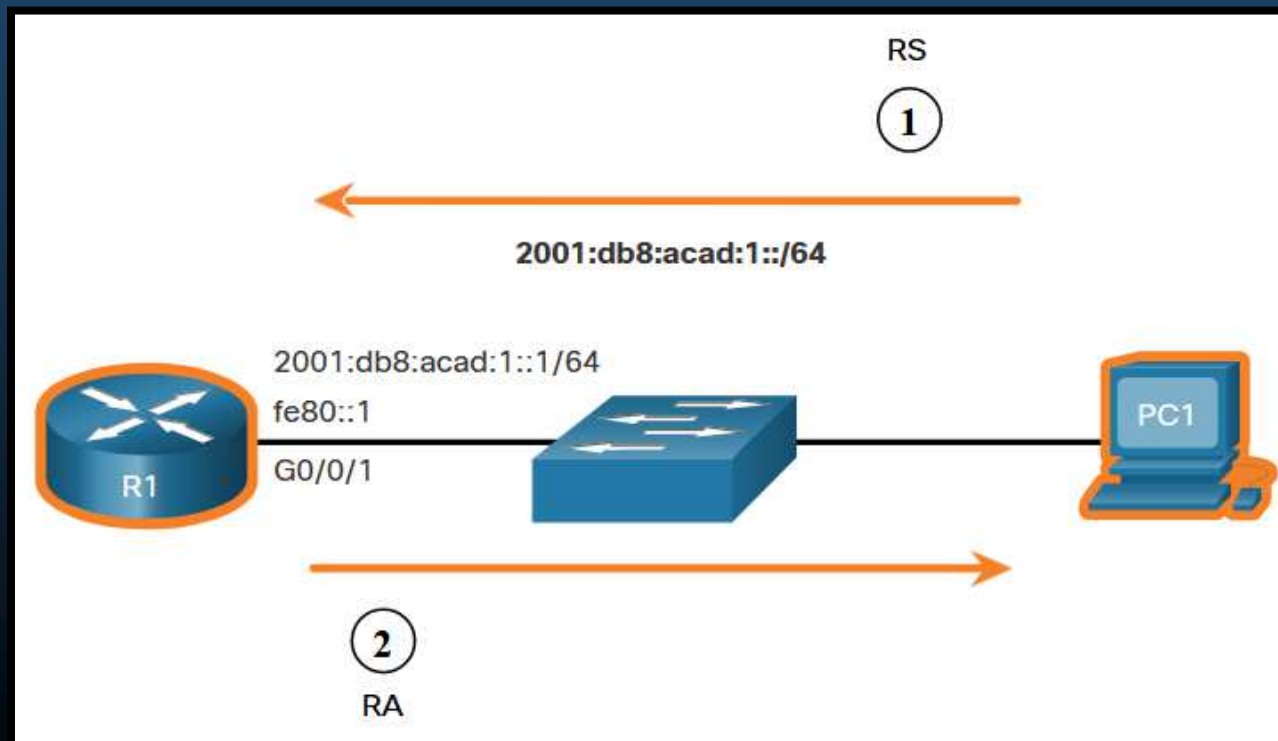
```
Router(config-if)# no ipv6 nd managed-config-flag  
Router(config-if)# no ipv6 nd other-config-flag
```



SLAAC

- **Mensajes RS de ICMPv6**

- Un router envía RAs cada 200s o cuando recibe un RS a la dirección ff02::1 (all-nodes-multicast).
- Un cliente que requiere auto-configurarse, envía RS a la dirección ff02::2 (all-routers-multicast).



SLAAC

- Proceso de un Host para Generar un ID de Interface.
 - Con SLAAC un host recibe el prefijo de subred de 64bits.
 - Necesario generar los 64 bits del ID interface:
 - Aleatoriamente: Método actualmente utilizado en Windows 10.

```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    IPv6 Address . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
    Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
    IPv4 Address. . . . . : 169.254.202.140
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1%6

C:\PC1>
```

- EUI-64: crea su ID de interface a partir de la MAC de 48 bits.
 - Inserta FFFE a la mitad de la MAC.
 - Actualmente en desuso por cuestiones de privacidad.

SLAAC

- **Detección de Direcciones Duplicadas.**
 - Al **generar ID de interface aleatorios**, pueden generarse **duplicados**.
 - Un **host** puede **verificar su nueva IP generada** es única.
 - **Proceso DAD** (Duplicate Address Detection).
 - Uso de **ICMPv6 para buscar vecinos**:
 - Mensaje **NS** (Neighbor Solicitation).
 - **Multicast** que **duplica 24 bits de** la dirección del **host**.
 - Si **nadie responde** con un **NA** (Neighbor Advertising)
 - Se considera la **IP** cómo **única**.
 - Si **alguien responde**, se **genera otra IPv6**
 - **Recomendado por IETF** en cualquier tipo de configuración (incluso manual).
 - Aunque **no es obligatorio**.
 - Aún así la **mayoría de los S.O.s lo realizan**.

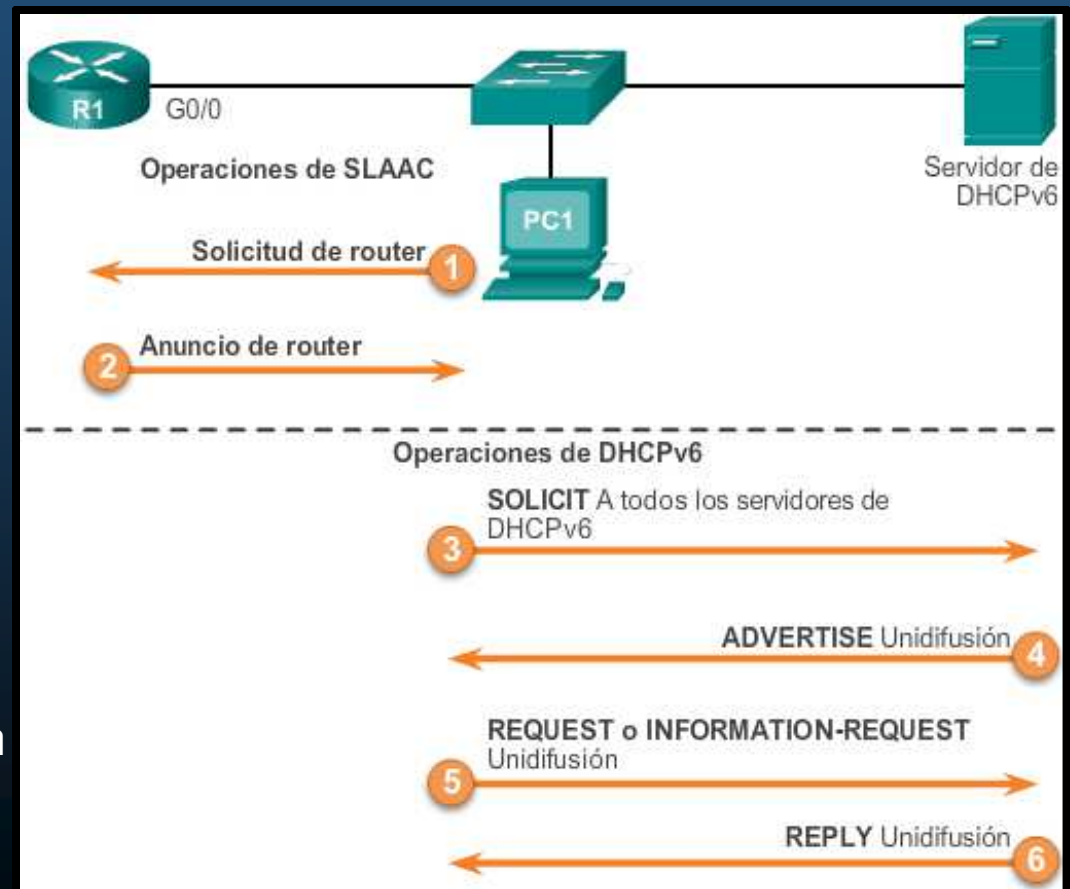
DHCPv6

- Pasos de Operación de DHCPv6

- Un servidor DHCPv6 escucha por el puerto 547 UDP y el cliente por el 546.

- Pasos para la operación de DHCPv6:

1. El host envía un RS.
2. El router responde con RA.
3. El host envía DHCPv6 SOLICIT.
4. El DHCPv6 responde con ADVERTISE.
5. El host responde al servidor DHCPv6.
6. El servidor DHCPv6 envía un REPLY.

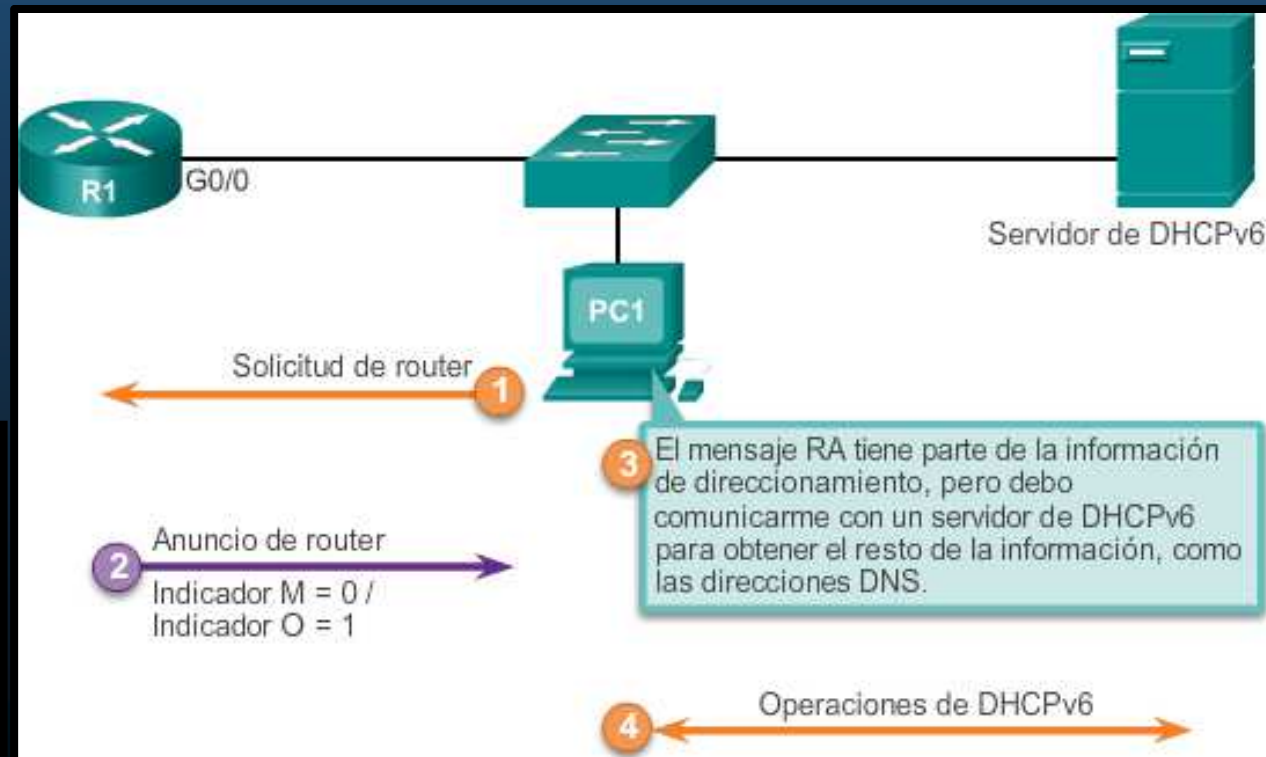


DHCPv6

- Operación de DHCPv6 Sin Estado.

- Usar información de RA, pero que hay más configuraciones disponibles.
 - O se configura en 1
 - indicador M se deja en 0

RA Message	
Flag	Value
A	1
O	1
M	0



DHCPv6

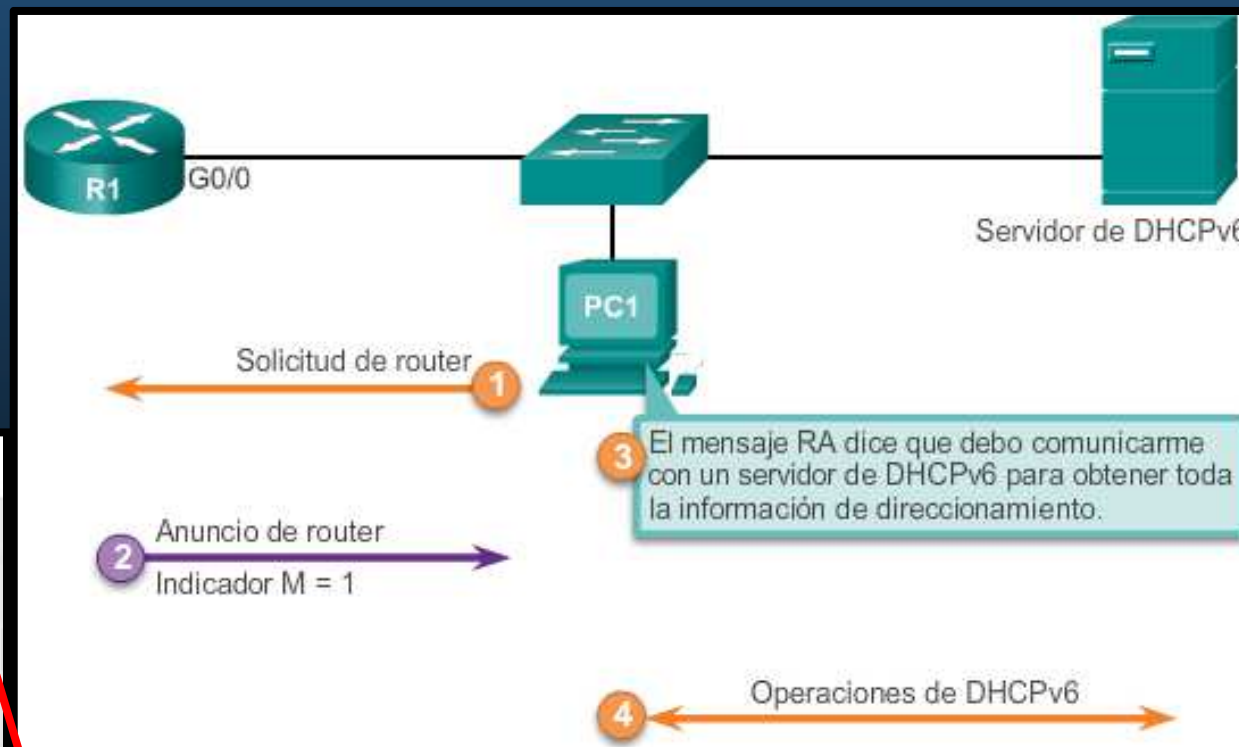
- **Habilitar DHCPv6 Sin Estado en una Interface.**
 - Usar información de RA, pero que hay más configuraciones disponibles.
 - O se configura en 1
 - Router(config-if)# ipv6 nd other-config-flag
 - indicador M se deja en 0
 - La salida muestra que el RA informará al host autoconfiguración sin estado:

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
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.
```

DHCPv6

- Opción de DHCPv6 con estado

- RA informa no utilizar su información sino obtener de un DHCPv6 con estado.
 - Indicador M señala utilizar DHCPv6.
 - Indicador O no interviene.



RA Message	
Flag	Value
A	0
O	0
M	1

Si A=1 y M=1 El S.O. generará su IPv6 y solicitará otra al DHCPv6

DHCPv6

- **Habilitar DHCPv6 con Estado en una Interface.**

- RA informa no utilizar su información sino obtener de un DHCPv6 con estado.

- Indicador M señala utilizar DHCPv6.

- Router(config-if)# ipv6 nd managed-config-flag

- Indicador O no interviene.

- La salida muestra que el RA informará al host autoconfiguración con estado:

```
R1(config)# int g0/0/1
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
  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.
```

Configurar un Servidor DHCPv6

- Roles de un Router DHCPv6.
 - En redes pequeñas puede no ser necesario implementar un Servidor DHCPv6 dedicado.
 - Los routers Cisco, pueden fungir cómo:
 - Servidor DHCPv6: Proveer IPv6 con o sin estado.
 - Cliente DHCPv6: Adquirir su IPv6 de un DHCPv6.
 - Agente de Retransmisión DHCPv6: Reenvío de tráfico cuando el DHCPv6 se encuentra en red diferente al cliente.

Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 sin estado
 - Cuatro pasos para configurar un router como servidor de DHCPv6:

Paso 1: habilitar el routing IPv6

```
Router(config)# ipv6 unicast-routing
```

Paso 2: configurar un pool de DHCPv6

```
Router(config)# ipv6 dhcp pool pool-name  
Router(config-dhcpv6)#
```

Paso 3: configurar los parámetros del pool

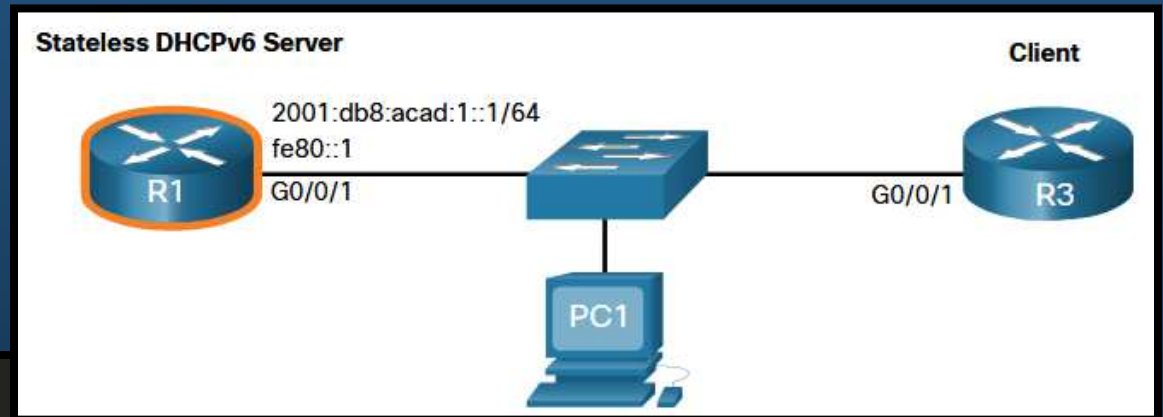
```
Router(config-dhcpv6)# dns-server dns-server-address  
Router(config-dhcpv6)# domain-name domain-name
```

Paso 4: configurar la interfaz DHCPv6

```
Router(config)# interface type number  
Router(config-if)# ipv6 dhcp server pool-name  
Router(config-if)# ipv6 nd other-config-flag
```

Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 sin estado
 - Ejemplo: Configurar servidor DHCPv6 sin estado.



```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:acad:1::254
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface GigabitEthernet0/0/1
R1(config-if)# description Link to LAN
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# no shut
R1(config-if)# end
```

Nota: PacketTracer solo soporta DHCPv6 sin estado en redes /64

Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 sin estado
 - Verificar que los clientes reciben información de direccionamiento IPv6.

```
C:\PC1> ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet0:

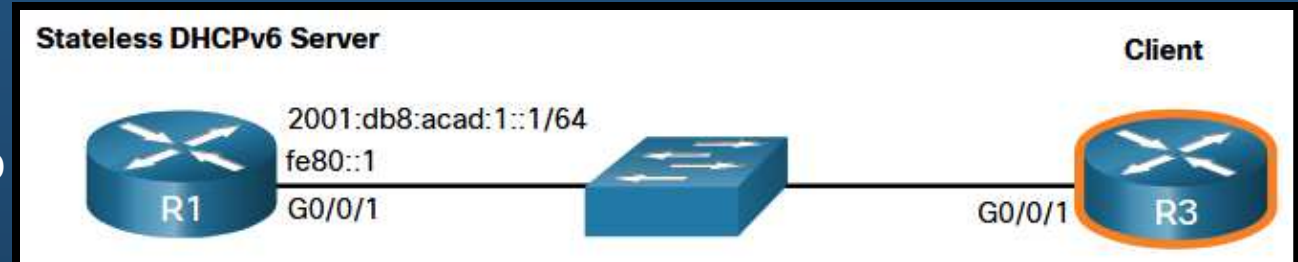
    Connection-specific DNS Suffix . : example.com
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-05-9A-3C-7A-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2001:db8:acad:1:1dd:a2ea:66e7 (Preferred)
    Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21 (Preferred)
    IPv4 Address. . . . . : 169.254.102.23 (Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1%6
    DHCPv6 IAID . . . . . : 318768538
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
    DNS Servers . . . . . : 2001:db8:acad:1::1
    NetBIOS over Tcpi. . . . . : Enabled
```

Configurar un Servidor DHCPv6

- Configuración de un Cliente de DHCPv6 sin Estado

- Un **router** también puede actuar como **cliente DHCPv6**.

- Habilitar enrutamiento IPv6.
- Configurar el Router cliente para generar LLA.
- Configurar el Router Cliente para usar SLAAC.
- Verificar que el Router Cliente recibe GUA.



```
R3(config)# ipv6 unicast-routing
```

```
R3(config)# interface g0/0/1
```

```
R3(config-if)# ipv6 enable
```

```
R3(config-if)# ipv6 address autoconfig
```

```
R3(config-if)# end
```

```
R3# show ipv6 interface brief
```

```
GigabitEthernet0/0/0 [up/up]
```

```
unassigned
```

```
GigabitEthernet0/0/1 [up/up]
```

```
FE80::2FC:BAFF:FE94:29B1
```

```
2001:DB8:ACAD:1:2FC:BAFF:FE94:29B1
```

```
Serial0/1/0 [up/up]
```

```
unassigned
```

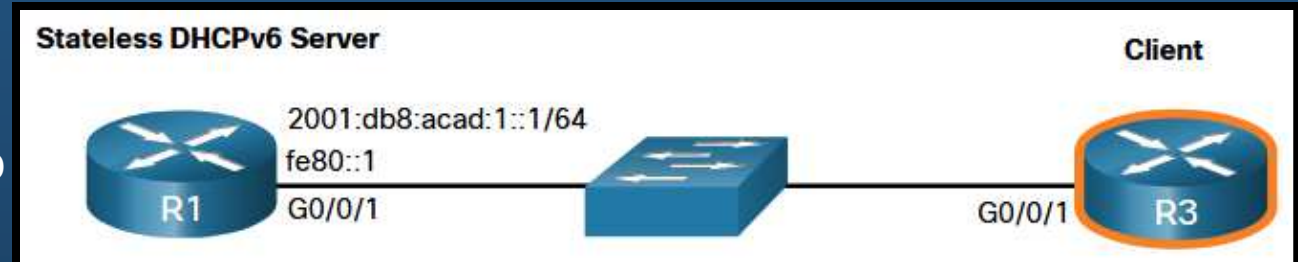
```
Serial0/1/1 [up/up]
```

```
unassigned
```

Configurar un Servidor DHCPv6

- Configuración de un Cliente de DHCPv6 sin Estado

- Un **router** también puede actuar como **cliente DHCPv6**.



- Habilitar enrutamiento IPv6.
- Configurar el Router cliente para generar LLA.
- Configurar el Router Cliente para usar SLAAC.
- Verificar que el Router Cliente recibe GUA.
- Verificar que el Router Cliente recibe información Adicional.

```
R3# show ipv6 dhcp interface g0/0/1
GigabitEthernet0/0/1 is in client mode
Prefix State is IDLE (0)
Information refresh timer expires in 23:56:06
Address State is IDLE
List of known servers:
  Reachable via address: FE80::1
  DUID: 000300017079B3923640
  Preference: 0
Configuration parameters:
  DNS server: 2001:DB8:ACAD:1::254
  Domain name: example.com
  Information refresh time: 0
Prefix Rapid-Commit: disabled
Address Rapid-Commit: disabled
```

Configurar un Servidor DHCPv6

- Verificación de DHCPv6 sin estado
 - Verificación del servidor de DHCPv6 sin estado
 - # show ipv6 dhcp pool
 - Cantidad de clientes es 0, por ser sin estado.
 - show running-config.



Configurar un Servidor DHCPv6

- Verificación de DHCPv6 sin estado
 - Verificación del cliente DHCPv6 sin estado
 - # `show ipv6 interface int-id`
 - Prefijo contenido en RA.
 - Host-id por EUI-64.

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is
FE80::32F7:DFE:FE25:2DE1
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:CAFE:1:32F7:DFE:FE25:2DE1, subnet is
2001:DB8:CAFE:1::/64 [EUI/CAL/PRE]
  valid lifetime 2591935 preferred lifetime 604735
Joined group address(es):
  FF02::1
  FF02::1:FE25:2DE1
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 NS retransmit interval is 1000 milliseconds
Default router is FE80::D68C:B5FF:FECE:A0C1 on
GigabitEthernet0/1
R3#
```


Configurar un Servidor DHCPv6

- Verificación de DHCPv6 sin estado

- Verificación del cliente DHCPv6 sin estado

- # debug ipv6 dhcp detail

- Muestra mensajes intercambiados entre el cliente y el servidor.

- R3 = Cliente (INFORMATION-REQUEST)

- Envía desde su link-local.

- Hacia todos los agentes de retransmisión y servidores de DHCPv6, FF02::1:2.

```
R3# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
R3#
*Feb  3 02:39:10.454: IPv6 DHCP: Sending INFORMATION-REQUEST
to FF02::1:2 on GigabitEthernet0/1
*Feb  3 02:39:10.454: IPv6 DHCP: detailed packet contents
*Feb  3 02:39:10.454:   src FE80::32F7:DFE:FE25:2DE1
*Feb  3 02:39:10.454:   dst FF02::1:2 (GigabitEthernet0/1)
*Feb  3 02:39:10.454:   type INFORMATION-REQUEST(11), xid
12541745
<resultado omitido>
*Feb  3 02:39:10.454: IPv6 DHCP: Adding server
FE80::D68C:B5FF:FECE:A0C1
*Feb  3 02:39:10.454: IPv6 DHCP: Processing options
*Feb  3 02:39:10.454: IPv6 DHCP: Configuring DNS server
2001:DB8:CAFE:AAAA::5
*Feb  3 02:39:10.454: IPv6 DHCP: Configuring domain name
example.com
*Feb  3 02:39:10.454: IPv6 DHCP: DHCPv6 changes state from
INFORMATION-REQUEST to IDLE (REPLY_RECEIVED) on
GigabitEthernet0/1
R3#
```

Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 con estado
 - Similar a configurar un servidor sin estado.
 - Incluye información de direccionamiento IPv6.

Paso 1: habilitar el routing IPv6

```
Router(config)# ipv6 unicast-routing
```

Paso 2: configurar un pool de DHCPv6

```
Router(config)# ipv6 dhcp pool pool-name  
Router(config-dhcpv6)#
```

Paso 3: configurar los parámetros del pool

```
Router(config-dhcpv6)# address prefix/length [lifetime  
valid-lifetime preferred-lifetime  
| infinite]  
Router(config-dhcpv6)# dns-server dns-server-address  
Router(config-dhcpv6)# domain-name domain-name
```

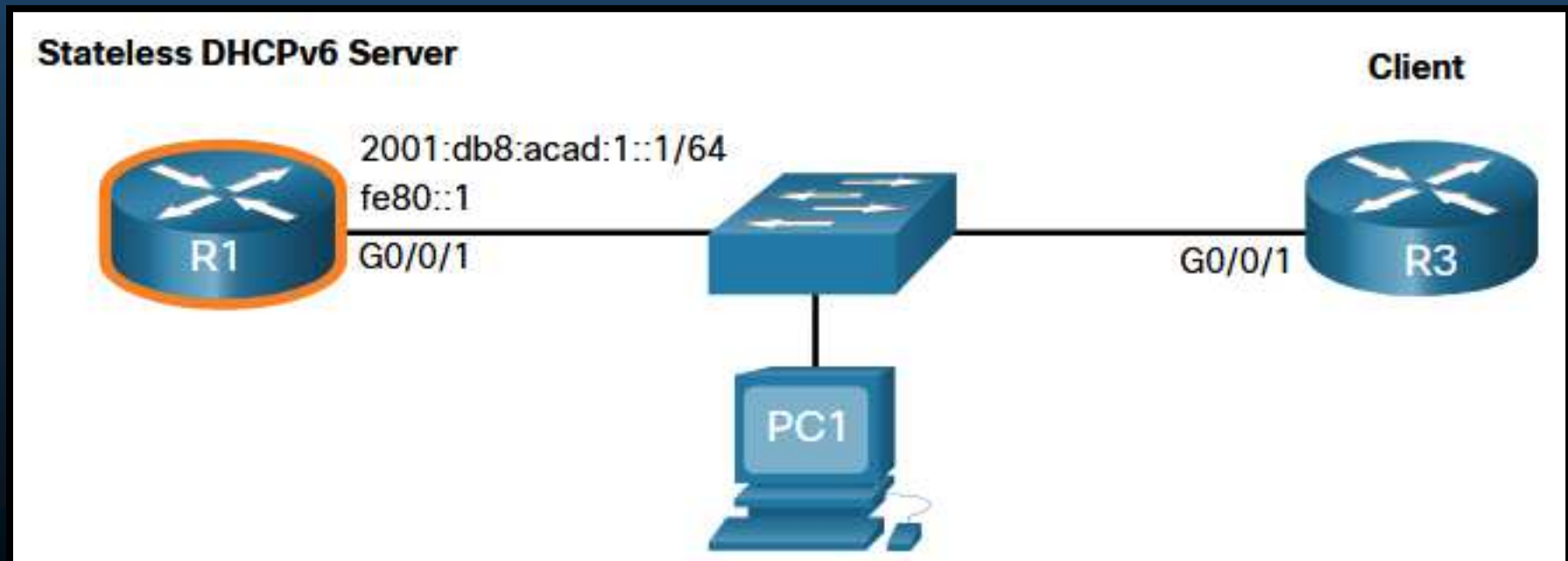
Paso 4: configurar la interfaz DHCPv6

```
Router(config)# interface type number  
Router(config-if)# ipv6 dhcp server pool-name  
Router(config-if)# ipv6 nd managed-config-flag
```

```
Router(config-if)# ipv6 nd prefix default no-autoconfig
```

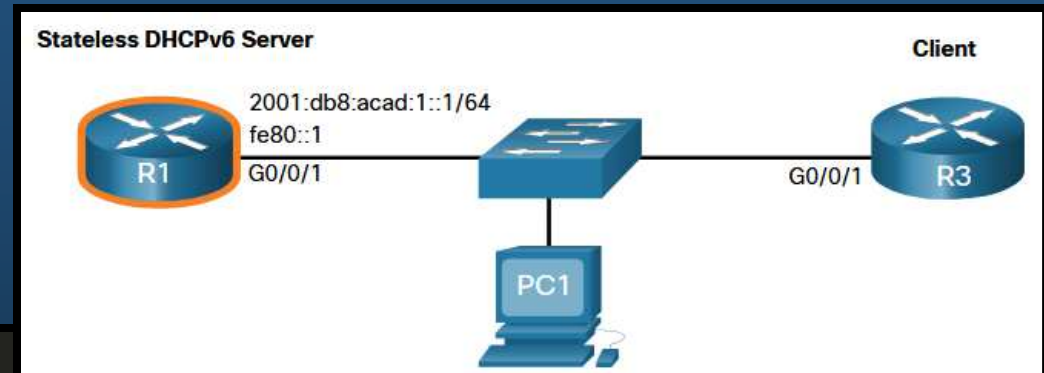
Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 con estado
 - Ejemplo de servidor de DHCPv6 con estado
 - No se especifica el gateway predeterminado,
 - El router **envia su dirección link-local** como el **gateway predeterminado**.
 - **R3** configurado como **cliente para verificar** DHCPv6 con estado.
 - Adicionalmente **deshabilita A**, para evitar duplicidad de IPv6 en el host.



Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 con estado
 - Ejemplo de servidor de DHCPv6 con estado

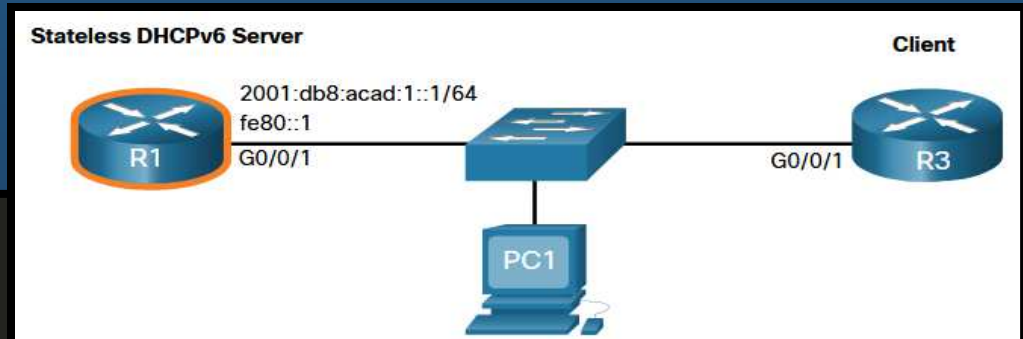


```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:db8:acad:1::/64
R1(config-dhcpv6)# dns-server 2001:4860:4860::8888
R1(config-dhcpv6)# domain-name example.com
R1(config)# interface GigabitEthernet0/0/1
R1(config-if)# description Link to LAN
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 nd prefix default no-autoconfig
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# no shut
R1(config-if)# end
```

Nota: Comando no disponible en PacketTracer

Configurar un Servidor DHCPv6

- Configuración de un router como servidor de DHCPv6 con estado
 - Ejemplo de cliente configurado mediante DHCPv6 con estado



```
C:\PC1> ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet0:

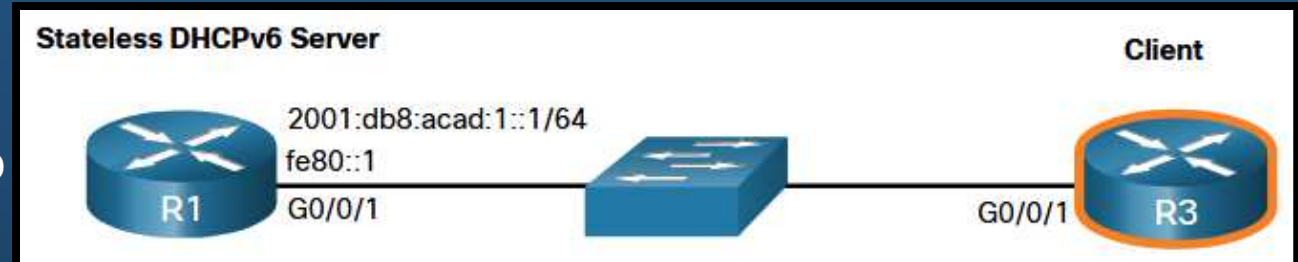
    Connection-specific DNS Suffix  . : example.com
    Description . . . . . : IntelI 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-05-9A-3C-7A-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv6 Address. . . . . : 2001:db8:acad:1a43c:fd28:9d79:9e42 (Preferred)
    Lease Obtained. . . . . : Saturday, September 27, 2019, 10:45:30 AM
    Lease Expires . . . . . : Monday, September 29, 2019 10:05:04 AM
    Link-local IPv6 Address . . . . . : fe80::192f:6fbc:9db:b749%6 (Preferred)
    Autoconfiguration IPv4 Address. . : 169.254.102.73 (Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1%6
    DHCPv6 IAID . . . . . : 318768538
    DHCPv6 Client DUID. . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
    DNS Servers . . . . . : 2001:4860:4860::8888
    NetBIOS over Tcpip. . . . . : Enabled
```

Configurar un Servidor DHCPv6

- Configuración de un Cliente de DHCPv6 Con Estado Completo

- Un **router** también puede actuar como **cliente DHCPv6**.

- Habilitar enrutamiento IPv6.
- Configurar el Router cliente para generar LLA.
- Configurar el Router Cliente para usar DHCPv6.
- Verificar que el Router Cliente recibe GUA.
- Verificar que el Router Cliente recibe información Adicional.



```
R3(config)# ipv6 unicast-routing
```

```
R3(config)# interface g0/0/1  
R3(config-if)# ipv6 enable
```

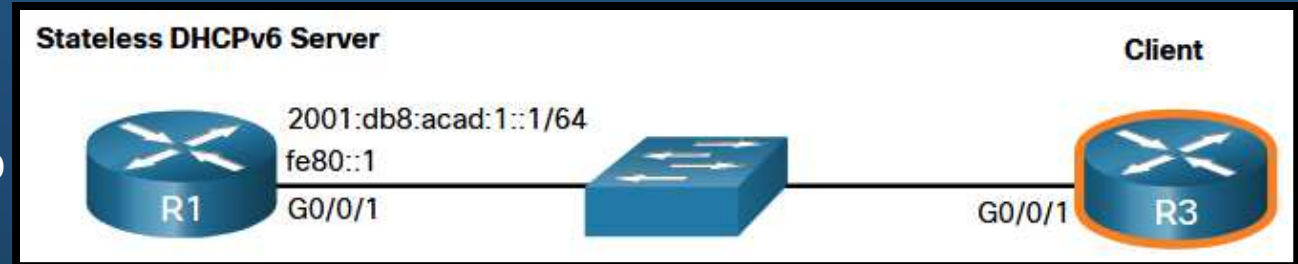
```
R3(config-if)# ipv6 address dhcp  
R3(config-if)# end
```

```
R3# show ipv6 interface brief  
GigabitEthernet0/0/0    [up/up]  
    unassigned  
GigabitEthernet0/0/1    [up/up]  
    FE80::2FC:BAFF:FE94:29B1  
    2001:DB8:ACAD:1:B4CB:25FA:3C9:747C  
Serial0/1/0             [up/up]  
    unassigned  
Serial0/1/1             [up/up]  
    unassigned
```

Configurar un Servidor DHCPv6

- Configuración de un Cliente de DHCPv6 Con Estado Completo

- Un **router** también puede actuar como **cliente DHCPv6**.

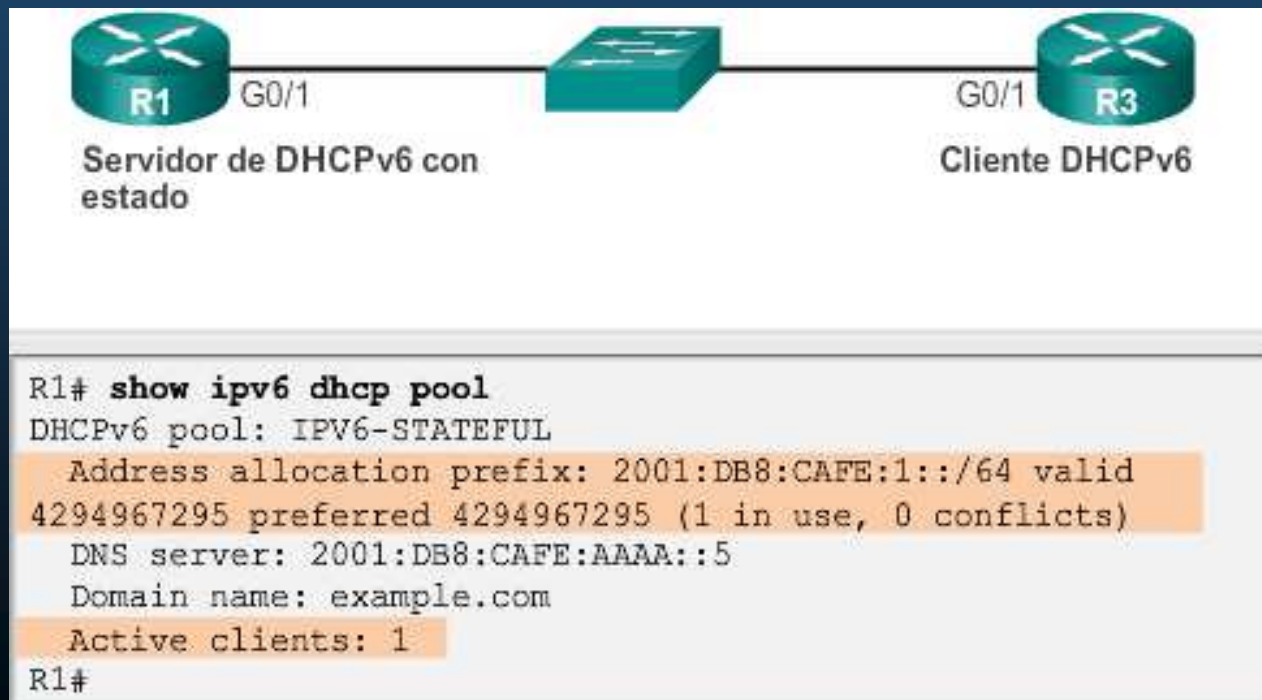


- Habilitar enrutamiento IPv6.
- Configurar el Router cliente para generar LLA.
- Configurar el Router Cliente para usar DHCPv6.
- Verificar que el Router Cliente recibe GUA.
- Verificar que el Router Cliente recibe información DHCPv6.

```
R3# show ipv6 dhcp interface g0/0/1
GigabitEthernet0/0/1 is in client mode
Prefix State is IDLE
Address State is OPEN
Renew for address will be sent in 11:56:33
List of known servers:
Reachable via address: FE80::1
DUID: 000300017079B3923640
Preference: 0
Configuration parameters:
IA NA: IA ID 0x00060001, T1 43200, T2 69120
Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C/128
        preferred lifetime 86400, valid lifetime 172800
        expires at Sep 29 2019 11:52 AM (172593 seconds)
DNS server: 2001:4860:4860::8888
Domain name: example.com
Information refresh time: 0
Prefix Rapid-Commit: disabled
Address Rapid-Commit: disabled
```

Configurar un Servidor DHCPv6

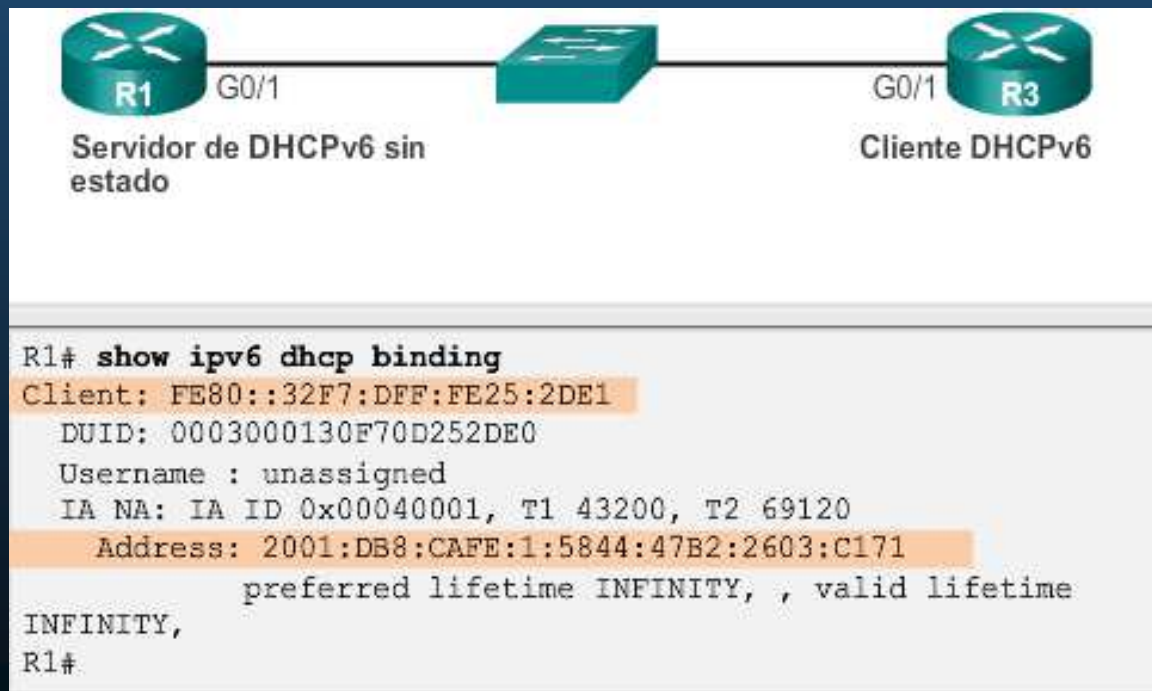
- Verificación de DHCPv6 con estado
 - Verifica parámetros del pool de DHCPv6
 - Cantidad de clientes activos 1, refleja cliente R3.
 - `show ipv6 dhcp pool`



Configurar un Servidor DHCPv6

- Verificación de DHCPv6 con estado

- Verificar vinculación automática entre dirección link-local del cliente y dirección asignada por el servidor.
 - `#show ipv6 dhcp binding`



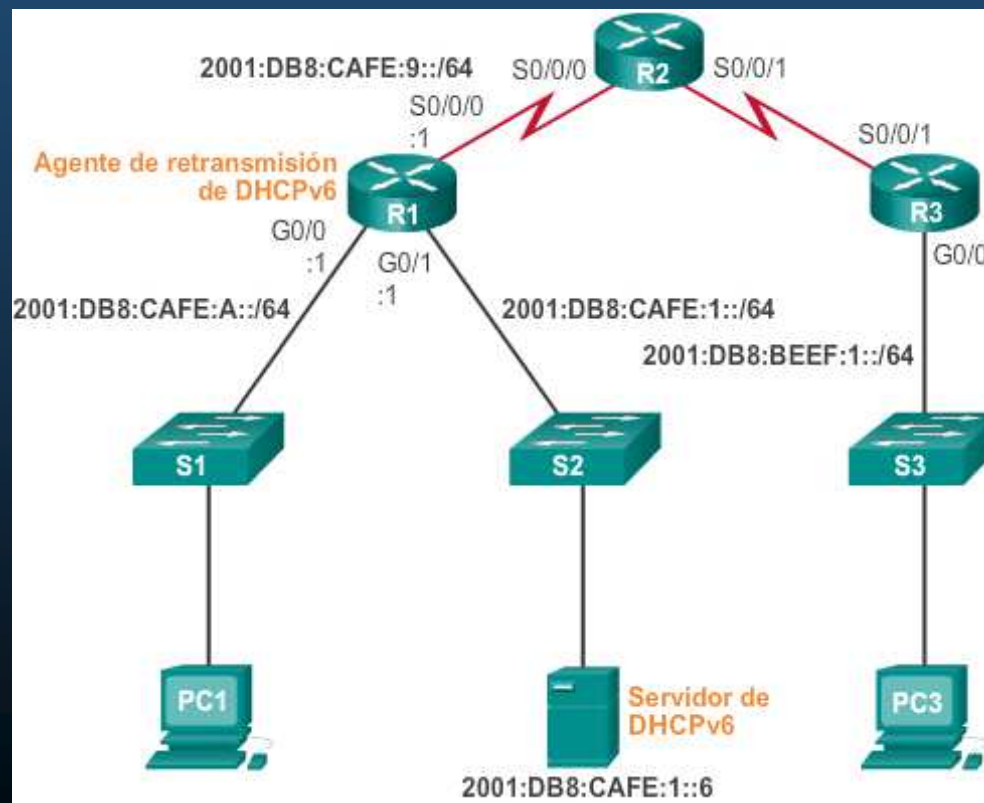
Configurar un Servidor DHCPv6

- Verificación de DHCPv6 con estado
 - Verificar dirección en cliente DHCPv6.
 - #show ipv6 interface

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::32F7:DFE:FE25:2DE1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:CAFE:1:5844:47B2:2603:C171, subnet is
2001:DB8:CAFE:1:5844:47B2:2603:C171/128
  Joined group address(es):
    FF02::1
    FF02::1:FF03:C171
    FF02::1:FF25:2DE1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  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::D68C:B5FF:FECE:A0C1 on
GigabitEthernet0/1
R3#
```

Configurar un Servidor DHCPv6

- Configuración de un router como agente de retransmisión DHCPv6
 - Servidor DHCPv6 en una red distinta al cliente
 - Router IPv6 puede retransmitir DHCPv6 similar a DHCPv4.



Configurar un Servidor DHCPv6

- Configuración de un router como agente de retransmisión DHCPv6

- (config-if)# `ipv6 dhcp relay destination dhcpv6-ip [interface_de_salida]`.

Nota: Comando no disponible en PacketTracer

- Verificación:

- # `show ipv6 dhcp interface`

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```

Resolución de Problemas DHCPv6

- Tareas de solución de problemas:

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.
Tarea 2 de la resolución de problemas:	Verificar el método de asignación.
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv6 estática.
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.

```
# show ipv6 dhcp conflict
```

```
# show ipv6 interface interfaz
```

Ausencia de conectividad con IP estática, implica problema diferente a DHCP

Si en otro puerto hay conectividad, hay alguna configuración errónea en el switch.

Si funciona local y no remoto, checar redistribución.

Resolución de Problemas DHCPv6

- Verificación de problemas DHCPv6:

Servicios DHCPv6 con estado

```
R1 (config)# ipv6 unicast-routing
R1 (config)# ipv6 dhcp pool IPV6-STATEFUL
R1 (config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite
R1 (config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1 (config-dhcpv6)# domain-name example.com
R1 (config-dhcpv6)# exit
R1 (config)# interface g0/1
R1 (config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1 (config-if)# ipv6 dhcp server IPV6-STATEFUL
R1 (config-if)# ipv6 nd managed-config-flag
```

Servicios DHCPv6 sin estado

```
R1 (config)# ipv6 unicast-routing
R1 (config)# ipv6 dhcp pool IPV6-STATELESS
R1 (config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1 (config-dhcpv6)# domain-name example.com
R1 (config-dhcpv6)# exit
R1 (config)# interface g0/1
R1 (config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1 (config-if)# ipv6 dhcp server IPV6-STATELESS
R1 (config-if)# ipv6 nd other-config-flag
```

Resolución de Problemas DHCPv6

- Verificación de problemas DHCPv6:

SLAAC

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::D68C:B5FF:FECE:A0C1
<resultado omitido>
Hosts use stateless autoconfig for addresses.
```

DHCPv6 sin estado

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::D68C:B5FF:FECE:A0C1
<resultado omitido>
Hosts use DHCP to obtain other configuration.
```

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::D68C:B5FF:FECE:A0C1
<resultado omitido>
Hosts use DHCP to obtain routable addresses.
```

Resolución de Problemas DHCPv6

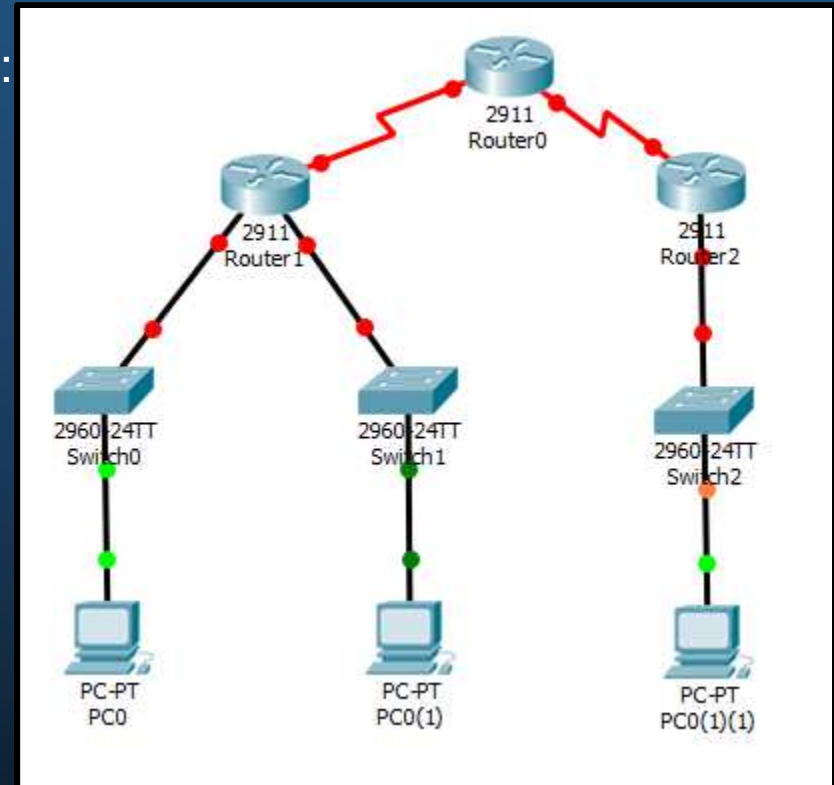
- Verificación de problemas DHCPv6:

```
R1# debug ipv6 dhcp detail
    IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from
FE80::32F7:DFE:FE25:2DE1 on GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:   src FE80::32F7:DFE:FE25:2DE1
(GigabitEthernet0/1)
*Feb  3 21:27:41.127:   dst FF02::1:2
*Feb  3 21:27:41.127:   type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:   option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:     elapsed-time 0
*Feb  3 21:27:41.127:   option CLIENTID(1), len 10
*Feb  3 21:27:41.127:     000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-
STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for
FE80::32F7:DFE:FE25:2DE1 in pool IPV6-STATEFUL
<resultado omitido>
```


Integración

- **Actividad Práctica de DHCPv4 + DHCPv6:**

- Armar la topología mostrada en la figura:
- Crear un esquema de direccionamiento, IPv4 mediante VLSM e IPv6 mediante subnetting.
- Configurar Router 1 como DHCPv4 para las 3 LANs.
- Configurar Router 0 como DHCPv6 con estado para LAN de Switch 2.
 - Si la actividad es en PacketTracer
 - Cambiar Router 0 por Router2
- Configurar Router 2 como DHCPv6 sin estado para LANs de Switch 0 y Switch 1.
 - Si la actividad es en PacketTracer, cambiar Router 2 por Router1
- Habilitar DHCP Relay donde sea necesario.





Capítulo 9

Conceptos de FHRP

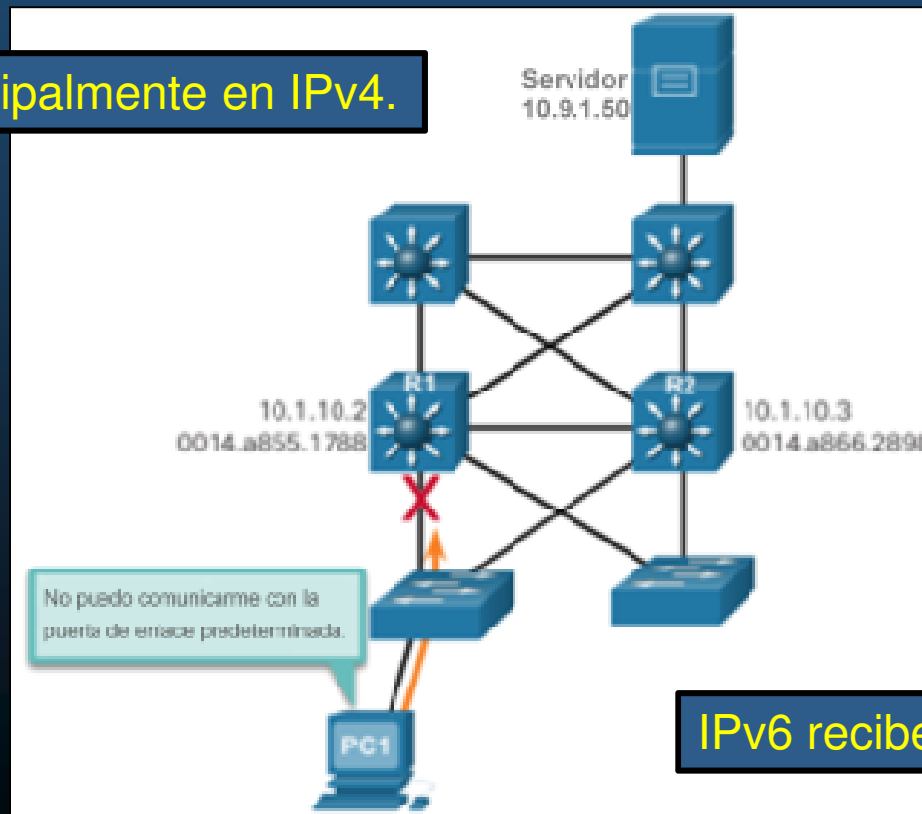
(First Hop Redundancy Protocols –
Protocolos de Redundancia de Primer Salto)

<https://contenthub.netacad.com/srwe/9.1.1>

Protocolos de Redundancia de Primer Salto

- Limitaciones de Puerta de Enlace Predeterminada.
 - En una LAN cada cliente recibe sólo un gateway, aunque haya mas.
 - Un host que pierde su puerta de enlace predeterminada, queda aislado.
 - Hace falta un mecanismo para brindar redundancia de Gateway.

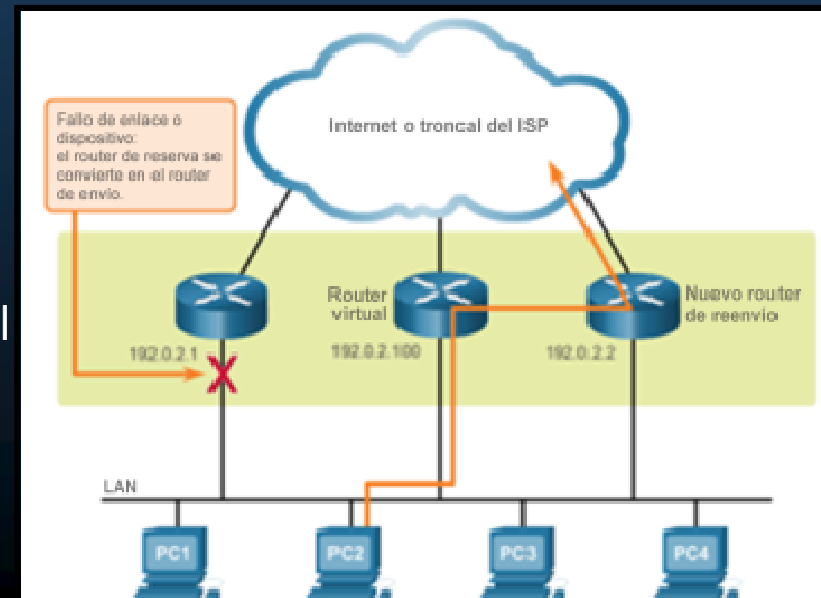
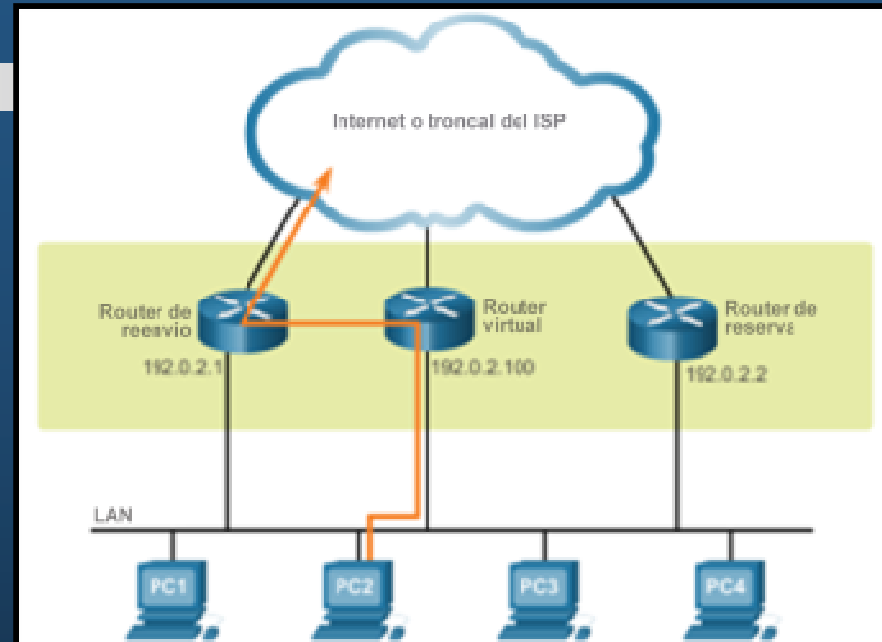
Problema principalmente en IPv4.



IPv6 recibe gateway por RAs.

Protocolos de Redundancia de Primer Salto

- Redundancia de Router.
 - Grupo de routers comparten IP y MAC virtuales (Gateway virtual).
 - Un protocolo determina:
 - Rol de routers re-envio y respaldo.
 - Transiciones entre roles.
- Pasos para la Redundancia de Router
 - Si falla el router activo.
 1. El de respaldo deja de ver saludos del activo.
 2. El router en espera se torna activo.
 3. Hosts no perciben interrupción en el servicio.



Protocolos de Redundancia de Primer Salto

- Opciones FHRP.

- Protocolo de Routing de Reserva Activa (HSRP).
 - Exclusivo de Cisco, permite conmutación por falla transparente para IPv4.
 - Un router de respaldo controla el estado operativo del grupo.
- HSRP para IPv6.
 - Funcionalidad de HSRP, pero para IPv6 (mediante direcciones link-local y RAs).
- Protocolo de Redundancia de Router Virtual versión 2 (VRRPv2).
 - No exclusivo, para IPv4.
 - Varios routers en una LAN con la misma IP virtual (maestro / respaldo).
- VRRPv3.
 - Evolución de VRRPv2, tanto para IPv4 cómo IPv6 con mas prestaciones.
- Protocolo de Balanceo de Carga de Puerta de Enlace (GLBP)
 - Exclusivo de Cisco, similar a HSRP y/o VRRP + Balanceo de Carga.
- GLBP para IPv6.
- Detección de Router ICMP (IRDP).
 - RFC 1256. Solución antigua.

HSRP

- Descripción General de HSRP.

- Los routers seleccionan al router **Activo**.
- Si falla el activo, el router en espera asume el rol de **activo**.

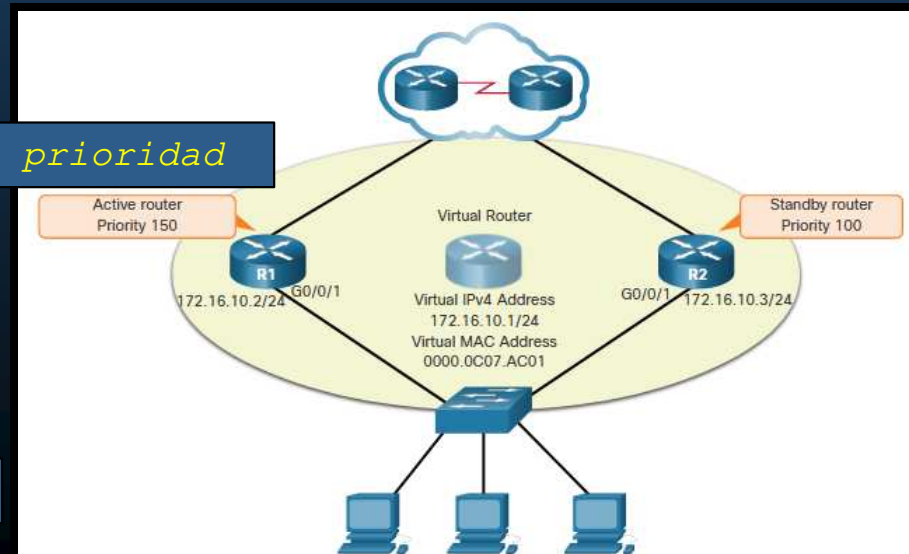
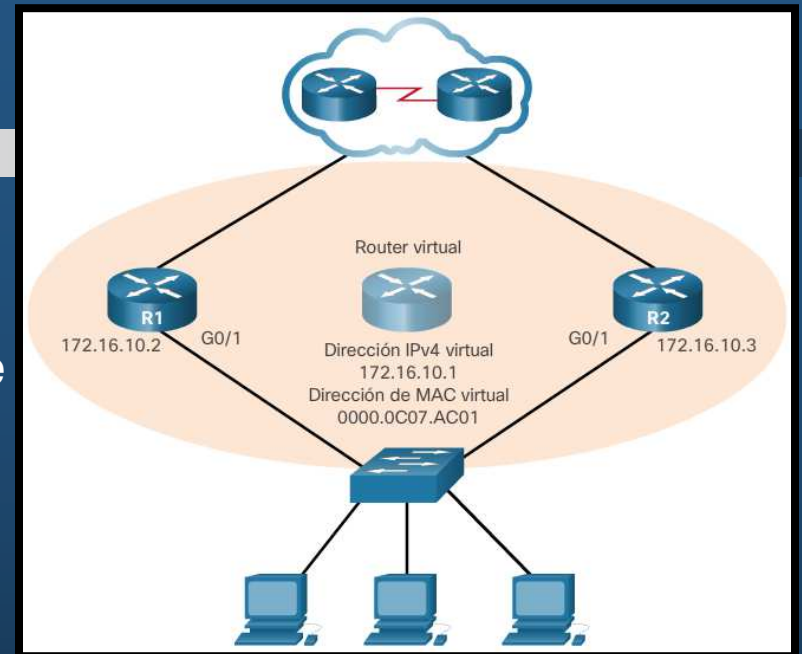
- Prioridad e Intento de Prioridad de HSRP.

- Los roles activo y en espera se determinan durante la elección HSRP.
 - Por defecto, el router con la IPv4 mas alta se elige como **activo**.
 - **Prioridad** (100 predeterminada) puede **alterar elección**:

```
(config-if)# standby priority prioridad
```

- Un **router activo se mantiene**, incluso si se agrega otro con mayor prioridad.
- **Forzar re-elección** con:

```
(config-if)# standby preempt
```



HSRP

- Estados y temporizadores de HSRP.

Estado	Definición
Inicial	Este estado se ingresa a través de un cambio de configuración o cuando una interfaz está disponible por primera vez.
Aprender	El router no ha establecido la dirección IP virtual y todavía no ha visto un mensaje de saludo del router activo. En este estado, el router espera para escuchar al router activo.
Escuchar	El router conoce la dirección IP virtual, pero el router no es el router activo ni el router de reserva. Escucha los mensajes de saludo de esos routers.
Hablar	El router envía mensajes de saludo periódicos y participa activamente en la elección de un router activo y/o de reserva.
En espera	El router es candidato a convertirse en el próximo router activo y envía mensajes de saludo periódicos.
Activo	El router actualmente reenvía paquetes que son enviados a la dirección MAC virtual del grupo. El router envía mensajes de saludo periódicos.

HSRP

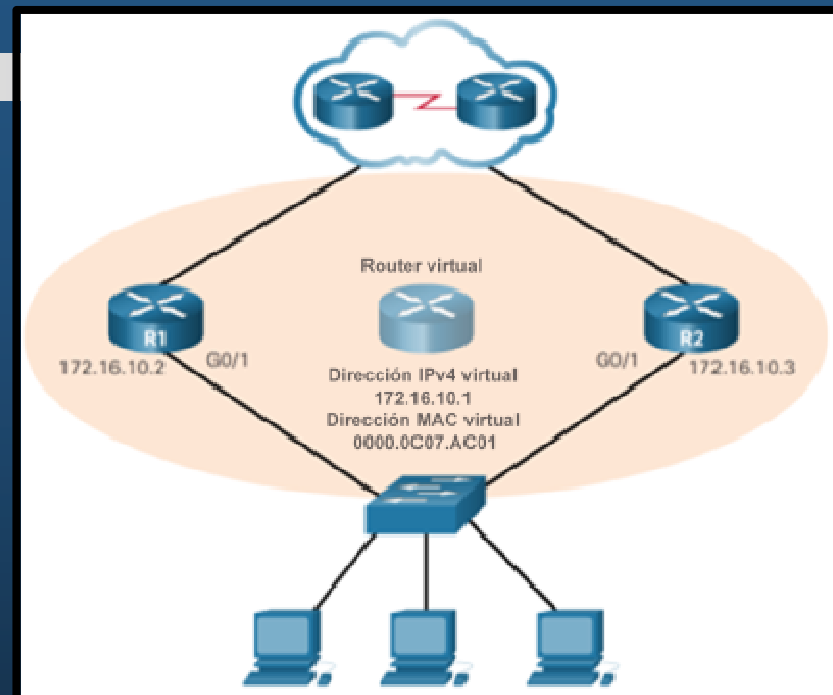
- Configuración de HSRP.

Comando	Definición
Router(config-if)# standby version 2	Configura el HSRP para usar la versión 2. La versión 1 de HSRP es la versión predeterminada.
Router(config-if)# standby [group-numberip-address]	Configura la dirección IP virtual de HSRP que utilizará el grupo especificado. Si no se configuró ningún grupo, entonces se asigna la dirección IP virtual al grupo 0.
Router(config-if)# standby [group-numberpriority [priority-value]	Configura el router activo deseado con una prioridad más alta que la prioridad predeterminada de 100. El rango es de 0 a 255. Si no se configura ninguna prioridad o si la prioridad es igual, tiene prioridad el router con la dirección IP más alta.
Router(config-if)# standby [group-numberpreempt	Configura un router para sustituir al router activo.

HSRP

- Ejemplo de configuración del HSRP.

```
R1(config)# int g0/1
R1(config-if)# ip add 172.16.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 172.16.10.1
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
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
R1(config-if)#
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1
state Speak -> Standby
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1
state Standby -> Active
```



```
R2(config)# int g0/1
R2(config-if)# ip add 172.16.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 1 ip 172.16.10.1
R2(config-if)# no shut
R2(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
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1
state Init -> Init
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1
state Speak -> Standby
```


HSRP

- Verificación del HSRP.
 - Verificar la **configuración** de HSRP: # **show standby**
 - Verificar el **estado** de HSRP: # **show standby brief**

```
R1# show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    12 state changes, last state change 0:04:54
  Virtual IP address is 172.16.10.1
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.519 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.10.3
  Priority 150 (configured 150)
  Group name is hsrp-Gig0/0-1 (default)
R1#
R1# show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State      Active          Standby          Virtual IP
Gig0/0         1   150 P Active    local           172.16.10.3     172.16.10.1
R1#
```

Integración

- Actividad Práctica.
 - Resuelva la actividad de PacketTracer encontrada en:
 - <https://contenthub.netacad.com/srwe/9.3.3>



Capítulo 10

Conceptos de Seguridad en una LAN

<https://contenthub.netacad.com/srwe/10.1.1>

Seguridad de Puntos Finales

- Ataques de Seguridad Actuales.

- Una búsqueda sobre “últimos ataques de red”, entregará varios artículos relacionados con:

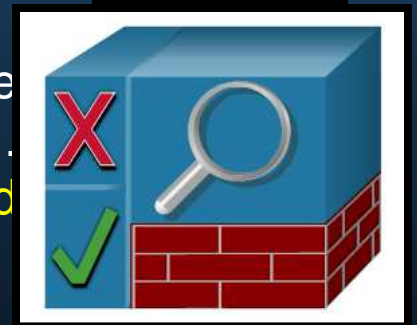
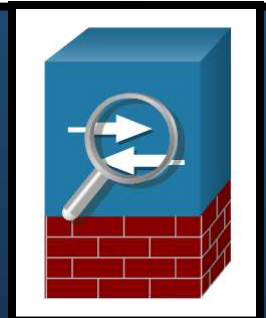
- Denegación de Servicios Distribuido (DDoS): Ataque coordinado de varios dispositivos (zombies), buscando degradar el acceso a recursos de una organización.
- Brecha de Datos: Ataque en el que los recursos de datos de una organización quedan comprometidos para el robo de información.
- Malware: Ataque en el que un host de alguna organización se infecta con software malicioso, causando múltiples problemas. Por ejemplo, el ransomware WannaCry, cifra los datos del equipo hasta que se realize un pago.



Seguridad de Puntos Finales

- **Dispositivos de Seguridad de Red.**

- Router Habilitado para VPN. Router que proporciona **conexión segura** entre redes remotas conectadas **por internet**.
- Cortafuegos de siguiente generación (NGFW). Proporciona **inspección de paquetes** con estado. Incluye Sistema de Prevención de Intrusos de Siguiete Generación (**NGIPS**) y Protección Avanzada contra Malware (**AMP**).
- Control de Acceso a la Red (NAC). Incluye un sistema de Autenticación, Autorización y Auditoría de cuentas (**AAA**). Maneja **políticas de seguridad** de usuarios en una gran **variedad de dispositivos**.

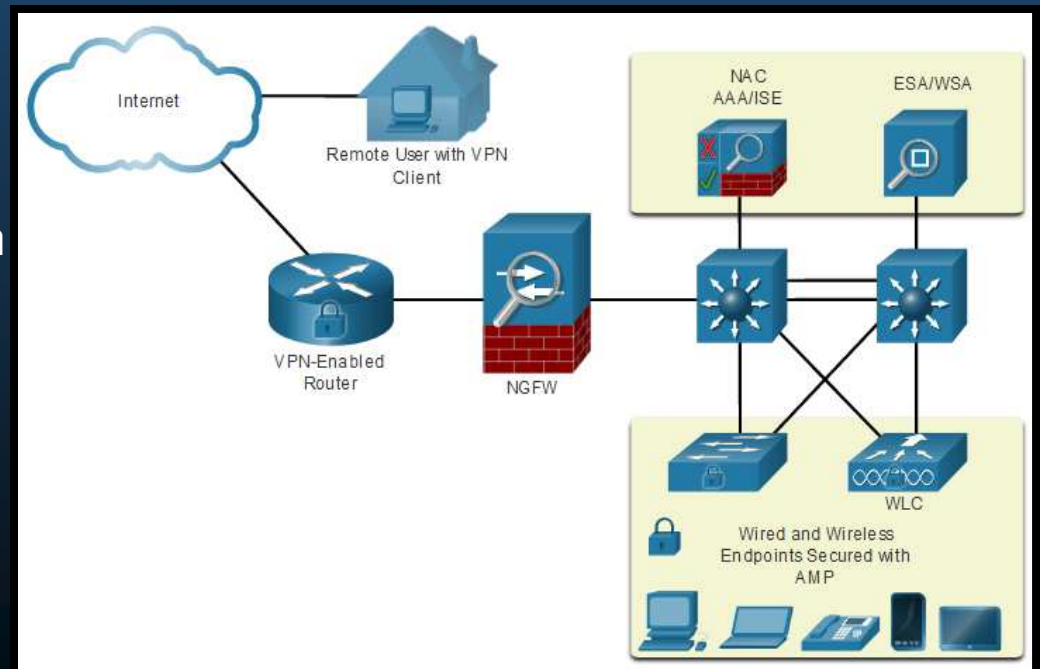


Seguridad de Puntos Finales

- Protección de Puntos Finales.

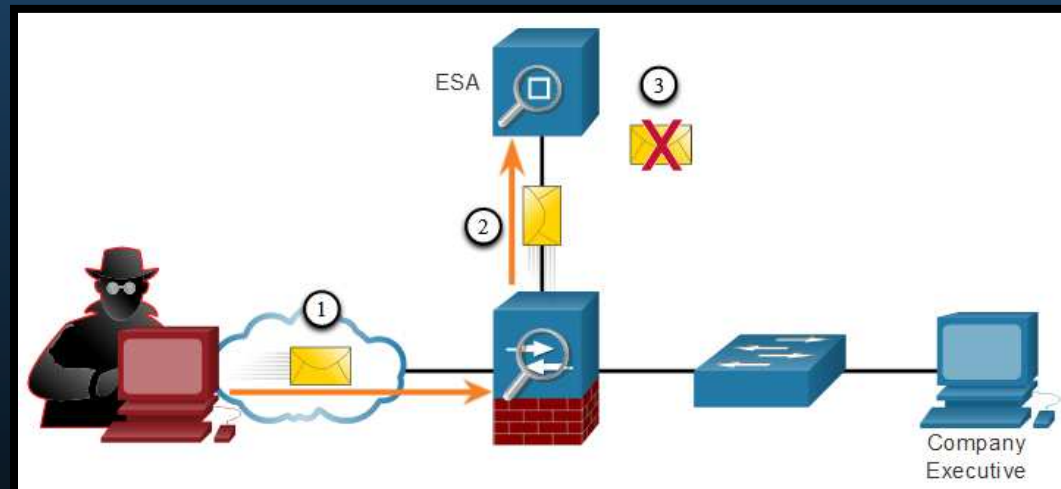
- Muchos ataques pueden originarse desde dentro de una red, si un host queda comprometido.
- Los puntos (dispositivos) finales, son susceptibles a malware, que puede llegar por correo o web.

- Seguridad típica:
 - Antivirus/Antimalware, Sistemas de Prevención de Intrusos para Host (HIPSs).
- Seguridad actual: AMP.



Seguridad de Puntos Finales

- Dispositivo de seguridad de correo electrónico (ESA) de Cisco.
 - Dispositivos de seguridad de contenido, realizan análisis de contenidos de e-mail o web.
 - Phishing es un ataque que intenta hacer pasar un email fraudulento por veraz, para recabar información de los usuarios.
 - Un ESA de Cisco, analiza el contenido de SMTP, actualiza base de datos de contenidos fraudulentos de Cisco Talos.

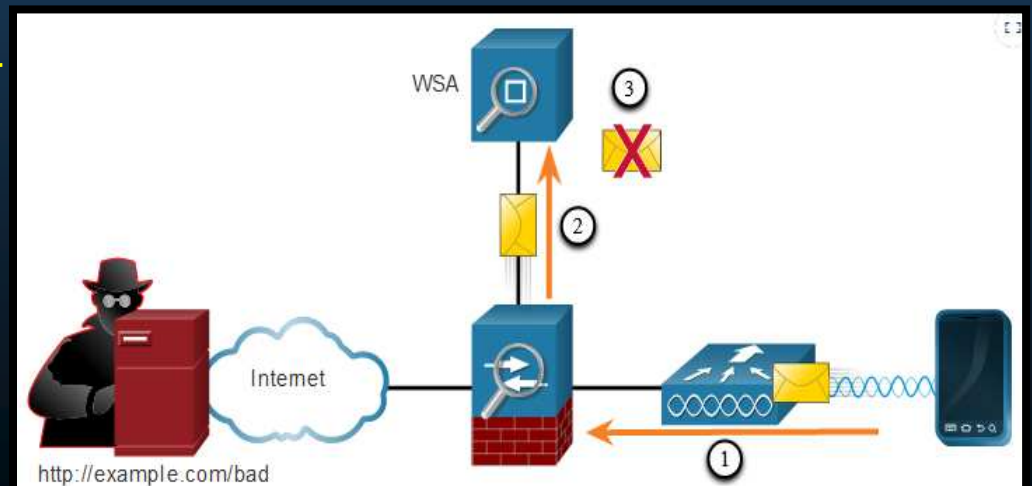


1. Se envía un ataque phishing a un dispositivo de red importante.
2. El firewall re-envía todo el tráfico al ESA.
3. El ESA analiza el e-mail, si es malware lo descarta.

Seguridad de Puntos Finales

- **Dispositivo de Seguridad Web (WSA) de Cisco.**
 - Tecnología de mitigación de amenazas basadas en web.
 - Ayuda a controlar el tráfico web.
 - Combina protección anti-malware y uso políticas de seguridad.
 - Reportes.
 - Controla completamente el acceso a internet.
 - Permite/Bloquea aplicaciones y características (chat, mensajería, video, etc...)
 - Administra listas negras y categorización de Urls.

1. Un usuario trata de conectar a un sitio web.
2. El firewall re-envía el sitio web al WSA.
3. El WSA evalúa la URL, la evalúa y determina si se descarga o descarta.



Control de Acceso

- Autenticación con una Contraseña Local.

- NAC proporciona servicios AAA.
- Existen varios métodos de autenticación y diferentes niveles de seguridad:
- Contraseña para acceso a VTYs (fácil de implementar / Inseguro / No administrado)

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

- SSH (Mas seguro / Local / Administrado a Nivel de Usuario)

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

- Limitaciones: Uso de base de datos local (difícil de escalar). Sin método de autenticación alternativa (si olvida la contraseña).

Control de Acceso

- Componentes AAA.

- AAA = Autenticación, Autorización y Auditoría de Cuentas.

- Similar al uso de una tarjeta de crédito.

- Identifica:

1. Quién puede usarla.

2. Cuanto puede gastar.

3. Lleva registro de gastos.



Authentication

Who are you?

Authorization

How much can you spend?

Accounting

What did you spend it on?

Account Number	Statement Closing Date	Current Amount Due
1234-567-890	01-31-01	\$278.50

JOE EMPLOYEE 456 SKYVIEW DRIVE HOMETOWN, USA 99900-1234		MAIL PAYMENT TO: THE BANK 132 VINE STREET ANYTOWN, USA 67900-0010
672919345 00178255000000003		

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01
Statement Date: 02-01-01	Payment Due Date: 03-01-01	
Closing Date: 01-31-01	Credit Limit: \$1,500.00	Credit Available: \$1221.50
New Balance: \$278.50	Minimum Payment Due: \$20.00	

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

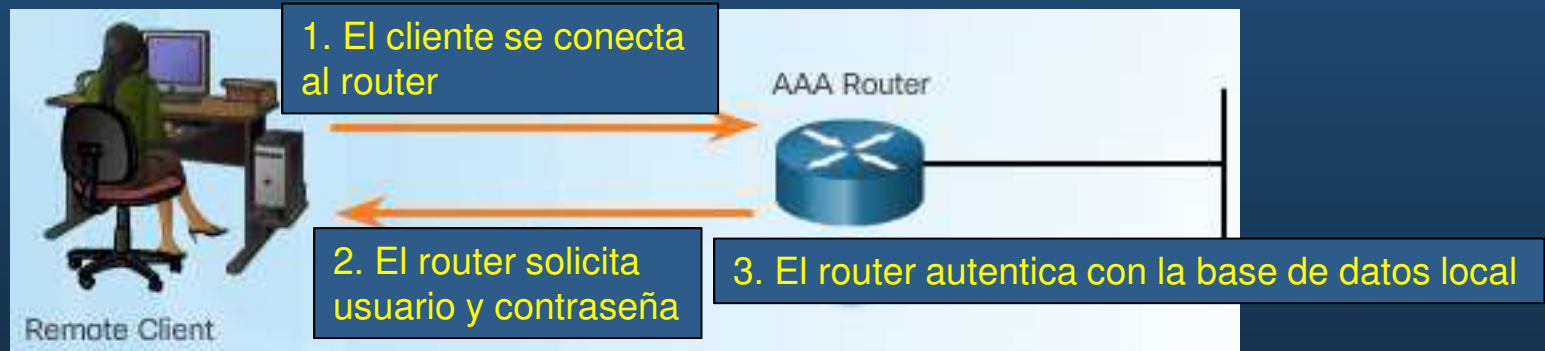
Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
76543210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

Control de Acceso

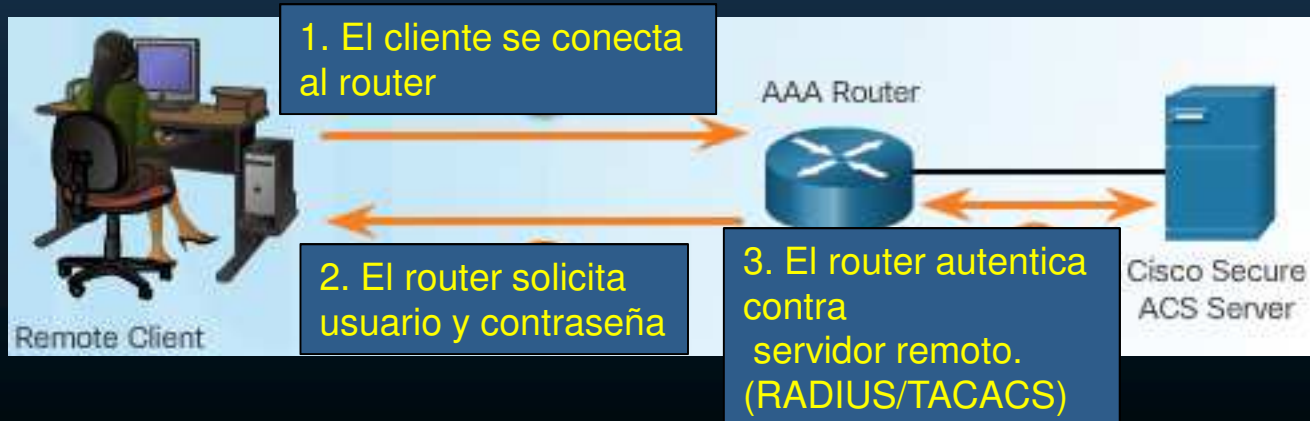
- Autenticación.

- Dos métodos principales mediante AAA:

- Local: Autenticación auto-contenida, ideal para redes pequeñas.



- Basado en Servidor: Ideal para desarrollos medianos/grandes



Control de Acceso

- Autorización.

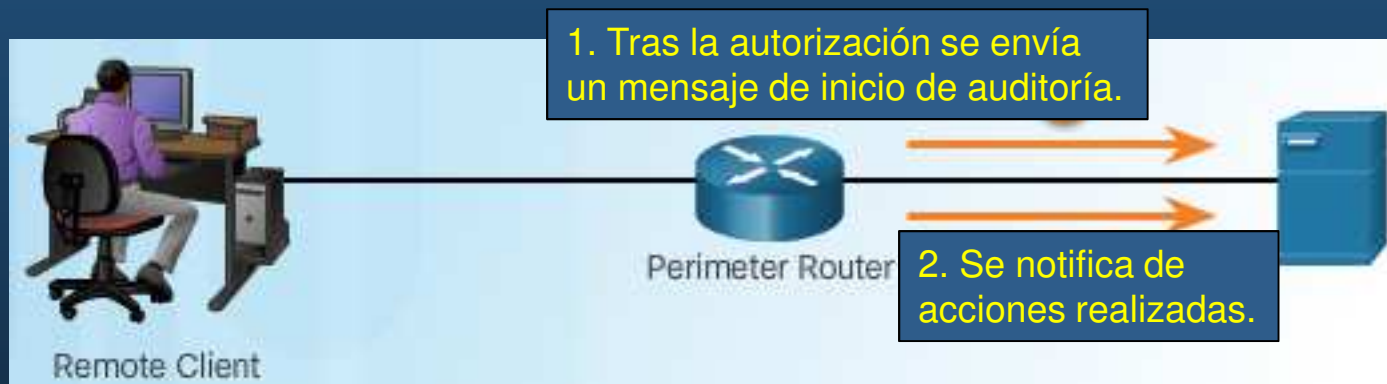
- Una vez **autenticado** se **determinan** las acciones y recursos autorizados.



- Este **proceso** es **automático** e **inmediato** a la **autenticación** y no requiere intervención del usuario.

Control de Acceso

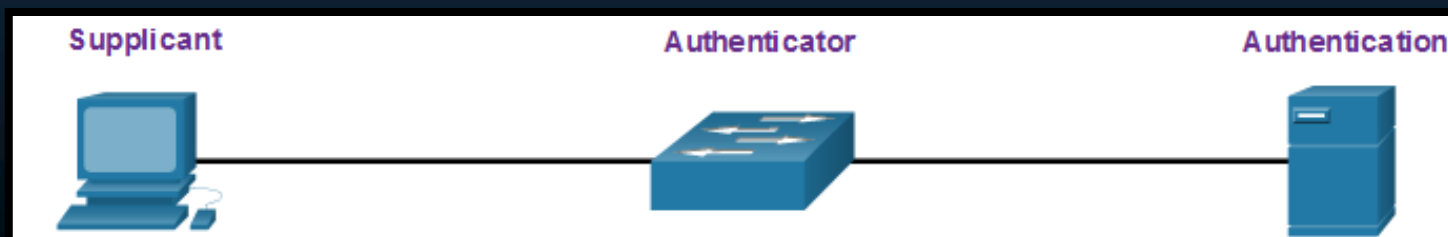
- Auditoría de Cuentas.
 - Colecta y reporta uso de datos.



- Brinda **mayor seguridad** que solo Autenticar y Autorizar.
- Genera logs de:
 - PPP, Telnet, SSH, EXEC, reboots, comandos, intentos de autenticación, autorización, etc.

Control de Acceso

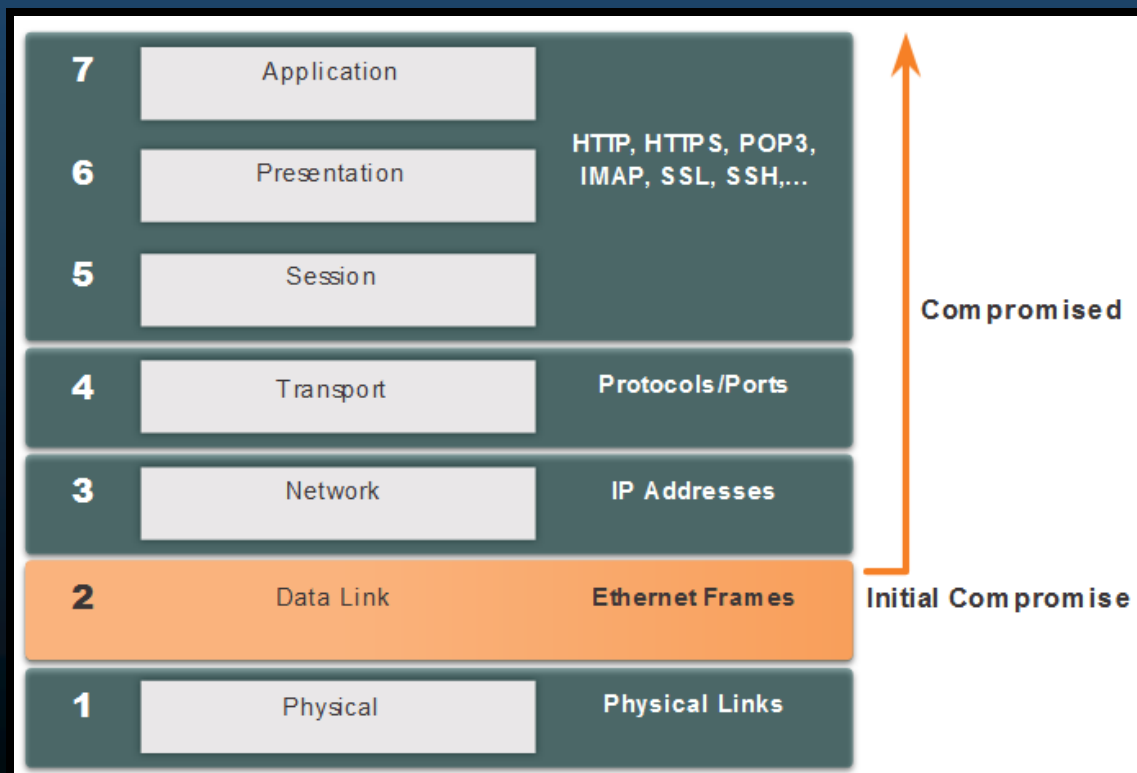
- 802.1X.
 - Estándar IEEE 802.1X. Protocolo de Autenticación y Control de Acceso Basado en Puerto.
 - Restringe estaciones de trabajo no autorizadas de conectarse a una LAN.
 - Un servidor de autenticación, autoriza a cada estación de trabajo conectada al switch, antes de que pueda acceder a la red.
 - Los dispositivos tienen roles específicos:
 - Cliente (Suplicante): Dispositivo con cliente software 802.1X para NIC o WNIC.
 - Switch (Autenticador): Intermediario entre cliente y servidor de autenticación. Envía solicitud de autenticación del cliente y respuesta del servidor.
 - Servidor de Autenticación: Valida la identidad del cliente y notifica al autenticador.



Amenazas de Seguridad de Capa 2

- Vulnerabilidades Capa 2.

- Las capas 3 o superiores del modelo OSI, usan VPNs, Firewalls e IPSs para protegerse.
- Sin embargo, si la capa 2 queda comprometida, el resto de capas se ven afectadas.
- Vgr; Un atacante captura tramas capa 2, tiene acceso a la información de todas las capas superiores (encapsuladas).



Amenazas de Seguridad de Capa 2

- Categorías de Ataques a Switches.
 - Ataques Capa 2:

Categoría	Ejemplos
Ataques a Tabla MAC	Incluye ataques de inundación de direcciones MAC.
Ataques a VLAN	Incluye saltos de VLAN y ataques de doble etiquetado de VLAN. También incluye ataques entre dispositivos en una VLAN común.
Ataques a DHCP	Incluye hambruna DHCP y ataques de suplantación de DHCP.
Ataques a ARP	Incluye suplantación de ARP y ataques de envenenamiento por ARP.
Ataques de Suplantación de Direcciones	Incluye suplantación de ARP y ataques de envenenamiento por ARP.
Ataques a STP	Incluye ataques de manipulación del protocolo Spanning Tree.

Amenazas de Seguridad de Capa 2

- Técnicas de mitigación de Ataques a Switches.

- Mitigación de Ataques Capa 2.

Solución	Descripción
Seguridad de puerto.	Previene tipos de ataques como, inundación de MACs y hambruna de DHCP.
DHCP Snooping.	Previene la hambruna de DHCP y los ataques de suplantación de DHCP.
La inspección dinámica de ARP (DAI)	Previene la falsificación de ARP y los ataques de envenenamiento por ARP.
IP Source Guard (IPSG)	Evita los ataques de suplantación de direcciones IP y MAC.

- Cualquiera de estas medidas no serán efectivas, si no se aseguran primero los protocolos de administración como: Syslog, SNMP, TFTP, FTP, etc...
 - Usar variante segura de protocolos.
 - Usar administración offline de ser posible
 - Tener una VLAN exclusiva para administración.
- Usar ACLs para evitar tráfico indeseado.

Ataque a la Tabla de Direcciones MAC

- Revisión de la Operación de un Switch.
 - Para tomar decisiones de re-envío, un switch construye una tabla (Tabla de Direcciones MAC), basada en la información de MAC origen de las tramas recibidas.

```
S1# show mac address-table dynamic
      Mac Address Table
-----
Vlan  Mac Address      Type        Ports
----  -
  1    0001.9717.22e0    DYNAMIC    Fa0/4
  1    000a.f38e.74b3    DYNAMIC    Fa0/1
  1    0090.0c23.ceca    DYNAMIC    Fa0/3
  1    00d0.ba07.8499    DYNAMIC    Fa0/2
S1#
```


Ataque a la Tabla de Direcciones MAC

- Inundación de Tabla de Direcciones MAC.

- La tabla MAC tiene tamaño fijo, al desbordarse, el switch inunda.
 - Un atacante puede bombardear al switch con direcciones MAC falsas, para forzarlo a inundar esa VLAN.
 - Al inundar el switch, un atacante puede capturar el tráfico de la VLAN, no destinado a él.



1. El atacante conectado a la VLAN 10 usa **macof** para generar tráfico con direcciones **MAC aleatorias**.
2. Tras un corto periodo de tiempo el **switch llena su tabla MAC**.
3. Con la tabla MAC llena, el switch comienza a **inundar** tráfico unicast.
4. El atacante utiliza un **sniffer** para capturar tramas de los dispositivos en la **VLAN**.

Ataque a la Tabla de Direcciones MAC

- Mitigación de Ataques a la Tabla de Direcciones MAC.
 - Switch Catalyst 6500 almacena hasta 132,000 direcciones en su tabla MAC.
 - macof puede desbordarla en pocos segundos.

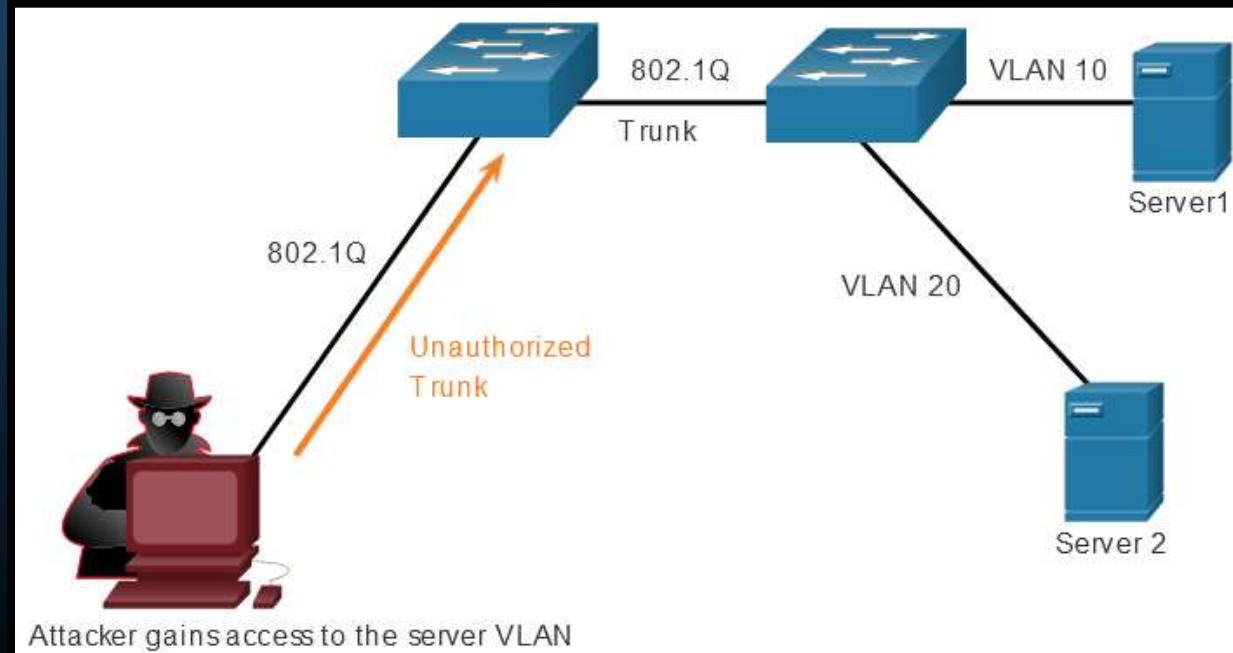
```
# macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S
1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0)
win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0)
win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S
1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S
1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S
1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0)
win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S
605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S
2128143986:2128143986(0) win 512
```

- Para mitigar el ataque se requiere habilitar seguridad de puerto.
 - Sólo permitir un número finito de direcciones MAC por puerto.

Ataque a VLAN y DHCP

- Ataques VLAN Hopping (Salto de VLAN).

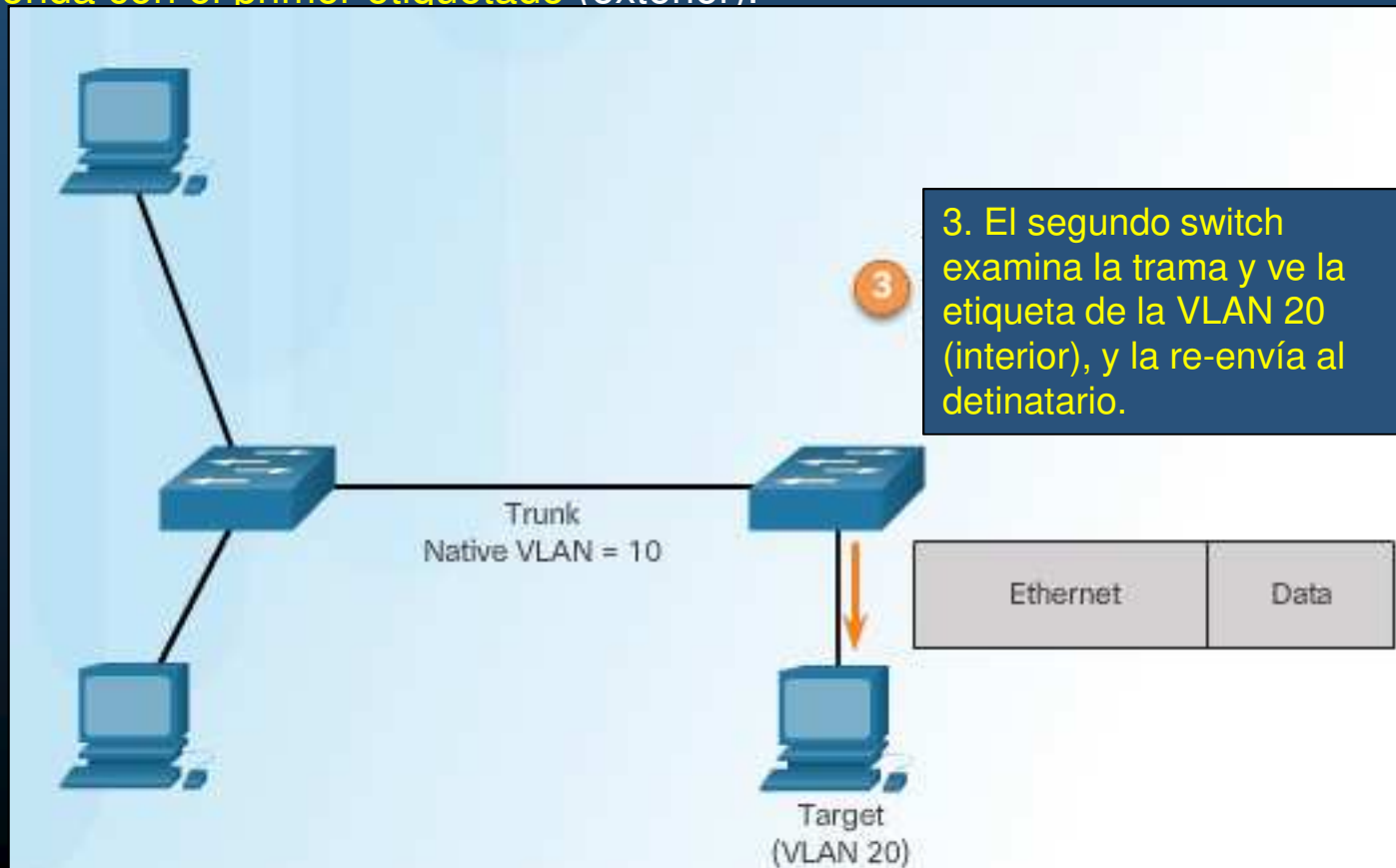
- Permite ver tráfico de una VLAN en otra (sin el uso de un router).
 - Asume la característica de troncal automático por defecto en los switches.
 - El atacante configura un host para fingir ser un switch
 - Usa señalizaciones 802.1Q y de protocolo de enlace dinámico (DTP) para entablar un troncal (enviar y recibir tramas de y hacia cualquier VLAN).
 - El atacante introduce un host que finge ser un switch, con el cual entablar el troncal.



Ataque a VLAN y DHCP

- **Ataque de Doble Etiquetado (Encapsulación) de VLAN.**

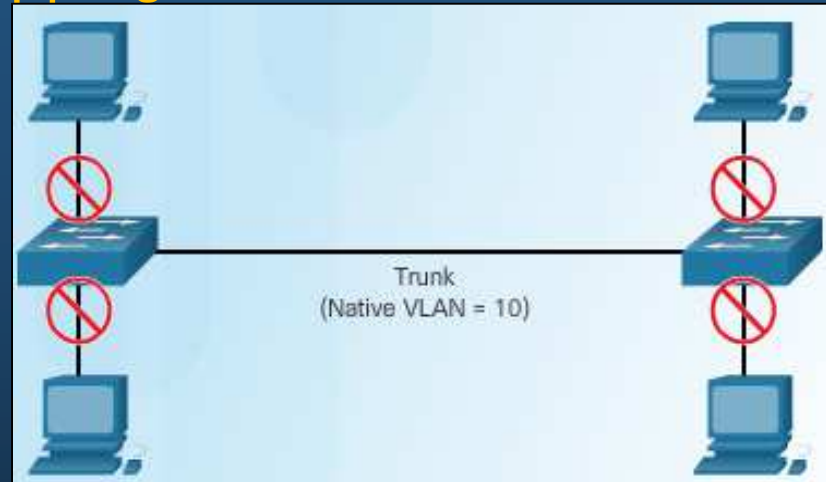
- La mayoría de los switches asumen una sola encapsulación de etiquetas VLAN.
- Un doble etiquetado puede permitir a una trama alcanzar la VLAN del segundo etiquetado (interior), siempre y cuando atraviese por un troncal y la VLAN nativa corresponda con el primer etiquetado (exterior).




Ataque a VLAN y DHCP

- Mitigación de Ataques VLAN Hopping.

- Deshabilitar troncales en puertos de **acceso** (`switchport mode access`).
- Deshabilitar troncales automáticos (DTP). (`switchport non-negotiate`).
- Habilitar **troncales manualmente**. (`switchport mode trunk`).
- Usar la **VLAN nativa solo en los troncales y un valor no usual**. (`switchport trunk native vlan vlan`).
- Deshabilitar puertos **no utilizados** (`shutdown`).

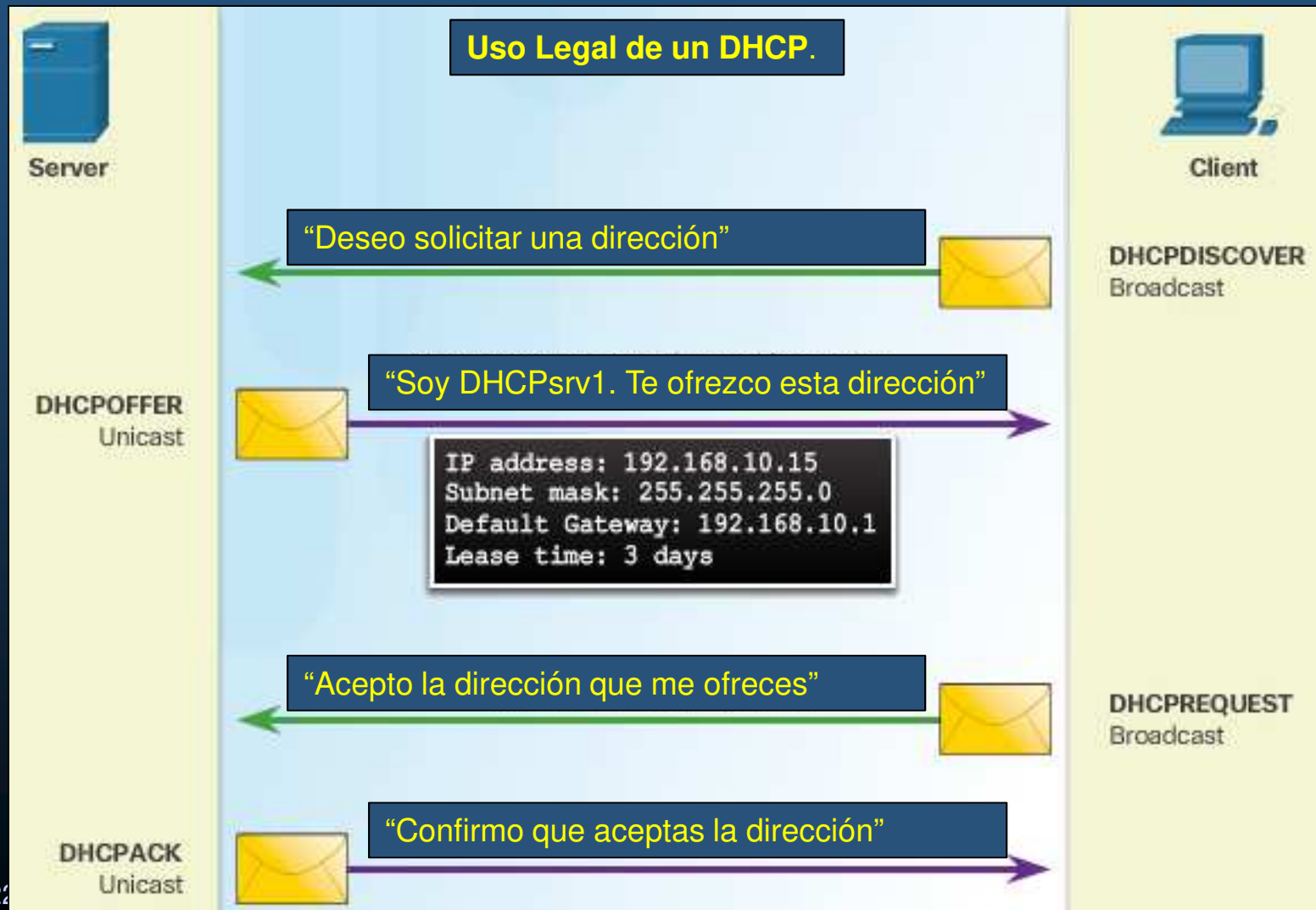


- Ejemplo: 

```
S1(config)# interface range f0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range f0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range f0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# exit
S1(config)#
```

Ataque a VLAN y DHCP

- Mensajes DHCP.



Ataque a VLAN y DHCP

- Ataques DHCP.
 - DHCP Starvation (Hambruna).
 - Busca generar DoS, dejando incomunicados a los hosts de la red.
 - Atacante envía muchos DHCP Discoverys.
 - Servidor envía muchos (si no es que todos sus) DHCP Offers.
 - Atacante solicita aceptar todas las ofertas (DHCP Request).
 - Servidor registra todas las ofertas aceptadas (DHCP ACK)
 - Una herramienta para realizar estas acciones es Gobbler
 - Busca consumir la totalidad de las Ips disponibles en un DHCP.



Ataque a VLAN y DHCP

- Ataques DHCP.
 - Ataque DHCP Spoofing (falso).
 - Servidor DHCP ilegítimo proporciona parámetros de configuración falsos.
 - Puerta de enlace predeterminada errónea (inexistente o proxy ilegítimo).
 - DNSs erróneos (incorrectos / inexistentes / webs ilegítimas).
 - Dirección IP errónea (inválida → DoS).
 - En una topología con 2 DHCPs (Legítimo/Ilegítimo)
 - Ambos reciben el DHCP Discovery del Cliente DHCP.
 - Ambos generan un DHCP Offer.
 - El cliente difundirá en un DHCP Request, que acepta la primer configuración que le llegue.
 - El Servidor DHCP cuya oferta haya llegado primero al cliente, enviará un acuse de recibo.
 - Un DHCP ilegítimo colocado estratégicamente, puede llegar a ganar todas las Ofertas.

Ataque a VLAN y DHCP

- Ataques DHCP.
 - Ataque DHCP Spoofing (falso).
 - Topología con 2 DHCPs (Legítimo/Ilegítimo)

El Servidor DHCP cuya oferta llegó primero al cliente, enviará un acuse de recibo.



Ataque a VLAN y DHCP

- **Ataques ARP.**

Un atacante puede enviar falsos ARP Reply Gratuitos (El RFC, indica que un ARP Reply no solicitado, debe considerarse igual de válido). Se establece como puente para ataque MITM. (Envenenamiento ARP).

ARP Cache on PC-A	
IP Address	MAC Address
192.168.10.1	EE:EE:EE:EE:EE:EE

ARP Cache on R1	
IP Address	MAC Address
192.168.10.10	EE:EE:EE:EE:EE:EE

IP: 192.168.10.10
MAC: AA:AA:AA:AA:AA:AA



ARP Reply:
192.168.10.1 has EE:EE:EE:EE:EE:EE

ARP Reply:
192.168.10.10 has
EE:EE:EE:EE:EE:EE

IP: 192.168.10.254
MAC: EE:EE:EE:EE:EE:EE



Múltiples herramientas disponibles:
Dsniff, Cain & Abel, Ettercap, Yersinia,...

IP: 192.168.10.1
MAC: A1:A1:A1:A1:A1:A1



ICMPv6 implementa prevención ARP
Replay falsos

Mitigación de ataques ARP requiere DAI (Inspección Dinámica de ARP) Donde el switch permite solo los ARP Replays que correspondan con un ARP Request.

ARP Cache on Attacker Host	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

Ataque a VLAN y DHCP

- **Ataque de Suplantación de Direcciones (Address Spoofing).**
 - Un atacante puede **falsear** tanto **IPs** como **MACs**.
 - **Falseo de una MAC,**
 - Un atacante **enviar tramas** a un switch **con MAC origen de Equipo atacado**.
 - El **switch re-envía** el **tráfico** destinado al host atacado **al atacante**.
 - El **atacante debe mantener** esa entrada en la **tabla CAM**.
(**tráfico legal** (desde el host atacado) **regresaría la CAM a su estado legal**)
 - **Envía tramas falseadas** constantemente.
 - **No hay mecanismo** en **Capa 2** para **prevenirlo**.
 - **Falseo de una IP.**
 - El **atacante utiliza** una **ip de otro host** o una **ip aleatoria**.
 - **Difícil de mitigar.**
 - Especialmente cuando se usa en la subred a la que pertenece.
 - **Requiere Protector de origen IP** (IP Source Guard - **IPSG**).
 - **Mantiene Reglas por puerto, por VLAN** (PVACL) en el switch
 - **Basadas en asociaciones IP-MAC-puerto.**

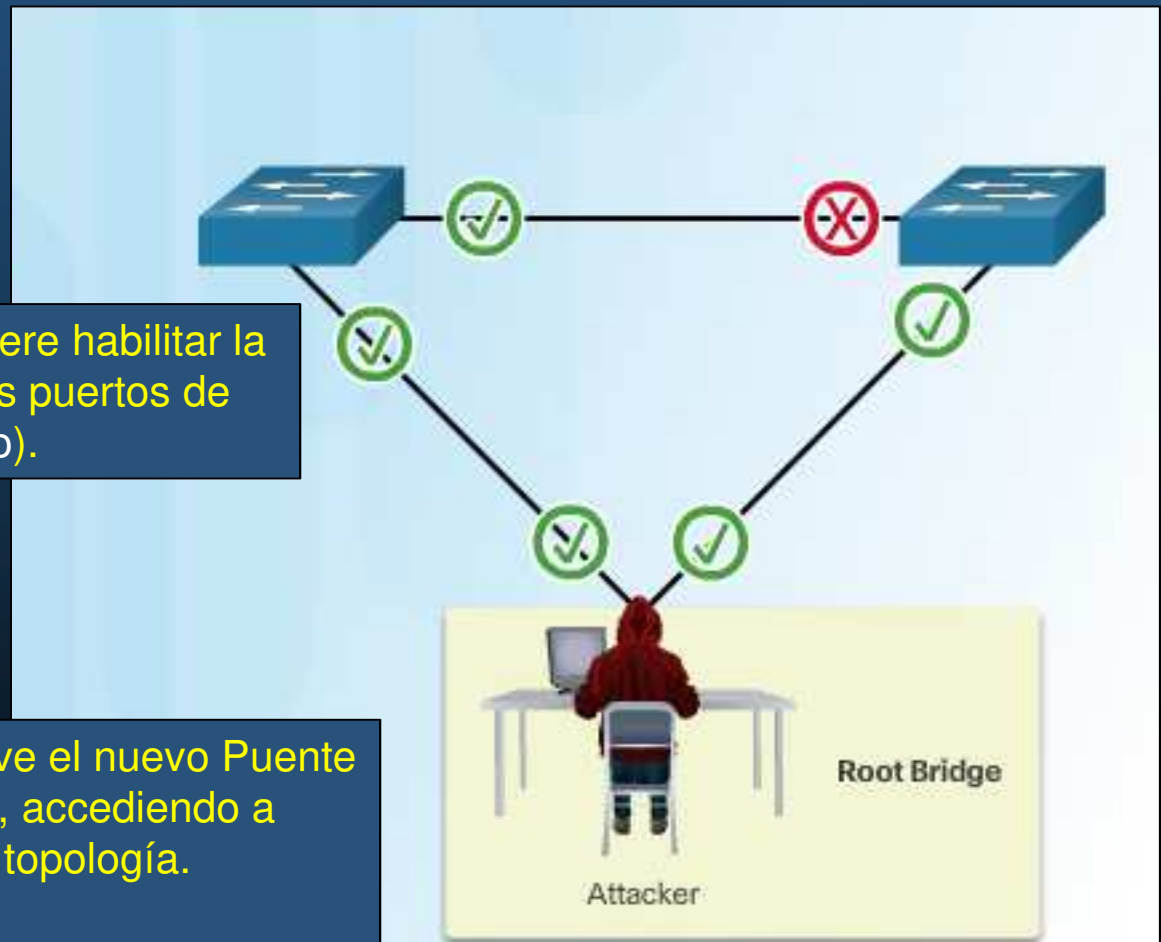
Ataque a VLAN y DHCP

- Ataques por Manipulación de STP.

- Un atacante puede fingir su host como Puesto Raíz y capturar todo el tráfico.

Para mitigar estos ataques se requiere habilitar la seguridad BPDU Guard en todos los puertos de acceso (mas adelante en este curso).

El atacante se vuelve el nuevo Puesto Raíz (prioridad = 0), accediendo a todo el tráfico de la topología.



Ataque a VLAN y DHCP

- Reconocimiento CDP.

- Cisco Discovery Protocol (CDP), descubre dispositivos Cisco en enlaces capa 2.
 - Habilitado de manera predeterminada.
 - Útil a administradores de red al configurar y solucionar problemas.
 - Transmisiones de datos de dispositivos sin cifrar.

- Dirección IP
- Versión del IOS
- Plataforma
- Capacidades
- VLAN nativa.

- Puede ser utilizado con fines maliciosos.
 - Falsear dispositivos
 - Conocer datos de dispositivos reales

- Deshabilitar si no se usa
- Lo mismo con LLDP.

The screenshot shows a Wireshark capture of CDP traffic. The top table lists two CDP packets. The bottom pane shows the details of a CDP packet, including fields like Version, TTL, Checksum, Device ID, Software Version, and Addresses. Two blue boxes with red arrows point to configuration commands: one for disabling CDP and another for disabling LLDP.

```
(config)# no cdp run
(config-if)# no cdp enable

(config)# no lldp run
(config-if)# no lldp transmit
(config-if)# no lldp receive
```

Integración

- Quiz (opcional).
 - Resuelva el Quiz encontrada en:
 - <https://contenthub.netacad.com/srwe/10.6.2>



Capítulo 11

Configuración de Seguridad en Switch

<https://contenthub.netacad.com/srwe/11.1.1>

Implementar Seguridad de Puertos

- **Asegurar Puertos No Utilizados.**
 - Importante **asegurar puertos antes de** poner un switch en **producción.**
 - Prevenir acceso no autorizado deshabilitando puertos no utilizados con:

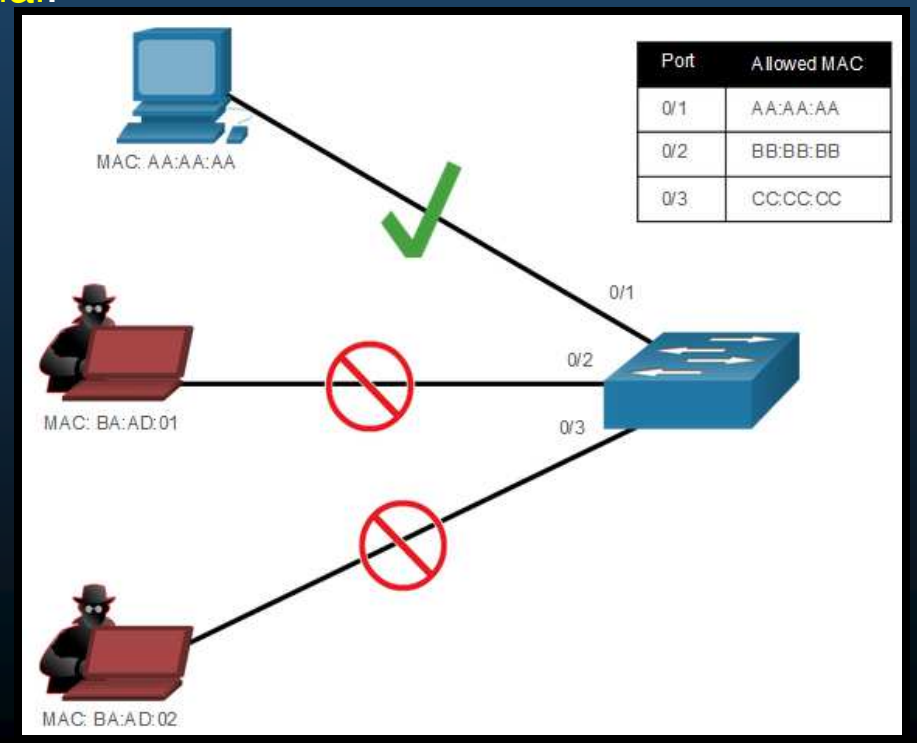
```
Switch(config)# interface range type module/first-number - last-number  
Switch(config-f)# shutdown
```

- *Ejemplo:*

```
S1(config)# interface range fa0/8 - 24  
S1(config-if-range)# shutdown  
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down  
(output omitted)  
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down  
S1(config-if-range)#
```


Implementar Seguridad de Puertos

- Mitigar Ataques a la Tabla de Direcciones MAC.
 - Seguridad de Puerto: Evita desbordamiento de tabla de direcciones MAC.
 - Limita el número de direcciones MAC permitidas en cada puerto.
 - Especificadas de forma manual.
 - Aprendidas dinámicamente, conforme se detecta tráfico.
 - Previene accesos no autorizados a la red.



Implementar Seguridad de Puertos

- **Habilitar Seguridad de Puerto.**
 - Solo puede habilitarse en puertos de acceso o troncales estáticos.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

- **Desplegar configuraciones actuales de seguridad de puerto con:**

- `#show port-security <int_id>`

```
S1# show port-security interface f0/1
Port Security                : Enabled
Port Status                   : Secure-shutdown
Violation Mode                : Shutdown
Aging Time                    : 0 mins
Aging Type                     : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 1
Total MAC Addresses           : 0
Configured MAC Addresses      : 0
Sticky MAC Addresses          : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0
S1#
```

Implementar Seguridad de Puertos

- Habilitar Seguridad de Puerto.
 - Pueden especificarse mas parámetros para seguridad de puerto:

```
S1(config-if)# switchport port-security ?
aging          Port-security aging commands
mac-address    Secure mac address
maximum        Max secure addresses
violation      Security violation mode
<cr>
S1(config-if)# switchport port-security
```

Implementar Seguridad de Puertos

- Limitar y Aprender Direcciones MAC.

- Establecer cantidad de direcciones MAC permitidas (1 por defecto):

```
Switch(config-if) # switchport port-security maximum value
```

- El máximo depende del modelo del switch:

- Configurar MACs manualmente:

```
Switch(config-if) # switchport port-security mac-address mac-address
```

- Indicar aprender de manera dinámica (las primeras que generen tráfico)
 - Habilitado por defecto, pero cada reinicio fuerza re-aprendizaje.
 - Para establecer persistencia (tras-reinicio):

```
Switch(config-if) # switchport port-security mac-address sticky
```

Implementar Seguridad de Puertos

- Limitar y Aprender Direcciones MAC.

- Ejemplo:

```
S1# show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 4
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

```
S1# show port-security address
```

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	aaaa.bbbb.1234	SecureConfigured	Fa0/1	-

```
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

```
S1#
```

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
```

Implementar Seguridad de Puertos

- Envejecimiento de la Seguridad de Puerto.
 - Dos posibilidades de eliminación de MACs aseguradas en puerto:
 - **Absolute**: Son eliminadas tras el tiempo especificado.
 - **Inactivity**: Son eliminadas solo si están inactivas el tiempo especificado.
 - Incrementar el tiempo de envejecimiento asegura que las MACs aseguradas anteriores permanezcan, incluso mientras se agregan nuevas.

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Parámetro	Descripción
<code>static</code>	Habilita el envejecimiento para las direcciones seguras configuradas estáticamente en este puerto.
<code>time <i>time</i></code>	Especifica el tiempo de envejecimiento (0 a 1440 minutos). Si el tiempo es 0, el envejecimiento está deshabilitado para este puerto.
<code>type absolute</code>	Establece el tiempo de envejecimiento absoluto. Las direcciones seguras caducan después del tiempo (en minutos) especificado y se eliminan de la lista de direcciones seguras.
<code>type inactivity</code>	Establezce el tipo de envejecimiento de inactividad. Las direcciones seguras caducan solo si no hay tráfico de datos desde la dirección de origen segura durante el tiempo especificado.

Implementar Seguridad de Puertos

- Envejecimiento de la Seguridad de Puerto.
 - Ejemplo: Configuración de tiempo de envejecimiento a 10 minutos de inactividad y verificación:

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Restrict
Aging Time              : 10 mins
Aging Type              : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
```

Implementar Seguridad de Puertos

- **Modos de Violación de Seguridad de Puerto.**

- Si la **dirección origen** llegada al puerto **difiere de las MACs aseguradas**, ocurre una **violación de puerto**.
- Para **especificar el modo de violación** utilice:

```
Switch(config-if)# switchport port-security violation { protect | restrict | shutdown }
```

Modo	Descripción
shutdown (default)	El puerto pasa al estado de error deshabilitado, apaga el LED y envía un mensaje de registro del sistema. Incrementa el contador de violaciones. El administrador debe volver a habilitarlo (<code>shutdown + no shutdown</code>).
restrict	El puerto descarta paquetes con direcciones de origen desconocidas hasta que elimine un número suficiente de direcciones MAC seguras. Este modo hace que el contador de infracción de seguridad se incremente y genera mensaje de syslog.
protect	El menos seguro. El puerto descarta paquetes con direcciones de origen MAC desconocidas hasta que elimine un número suficiente de direcciones MAC seguras. No se envía ningún mensaje de syslog.

Implementar Seguridad de Puertos

- Modos de Violación de Seguridad de Puerto.
 - Comparación de los modos:

Modo de Violación	Descarta Tráfico Ofensivo	Envía Mensaje Syslog	Incrementa Contador de Violaciones	Apaga el Puerto
protect	Si	No	No	No
restrict	Si	Si	Si	No
shutdown (default)	Si	Si	Si	Si

- Ejemplo de cambio del modo de violación

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
```

```
S1# show port-security interface f0/1
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Restrict
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
S1#
```

Implementar Seguridad de Puertos

- Puertos en Estado “error-disabled”.
 - Un puerto en este estado, **no envía ni recibe tráfico**, pero:
 - **Envía mensajes a la consola**

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18,
putting Fa0/18 in err-disable state
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 000c.292b.4c75 on port FastEthernet0/18.
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18,
changed state to down
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

- **show interface** lo identifica como **err-disabled**
- **show port-security** indica **secure-shutdown**

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/18
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
(output omitted)
S1#
```

Implementar Seguridad de Puertos

- Puertos en Estado “error-disabled”.
 - El administrador debe **determinar que causó el error**.
 - Una vez **resuelto, re-habilitar** el puerto usando:
 - `(config-if)# shutdown`
 - `(config-if)# no shutdown`

```
S1(config)# interface fa0/18
S1(config-if)# shutdown
*Sep 20 07:11:18.845: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to
administratively down
S1(config-if)# no shutdown
*Sep 20 07:11:32.006: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up
*Sep 20 07:11:33.013: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/18, changed state to up
S1(config-if)#
```

Implementar Seguridad de Puertos

- Verificar Seguridad de Puerto.
 - Desplegar configuraciones de seguridad de puerto en todas las interfaces:

```
S1# show port-security
Secure Port   MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)      (Count)
-----
    Fa0/1           1             0             0             Shutdown
    Fa0/2           1             0             0             Shutdown
    Fa0/3           1             0             0             Shutdown
(output omitted)
    Fa0/24          1             0             0             Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
Switch#
```

Implementar Seguridad de Puertos

- Verificar Seguridad de Puerto.
 - Desplegar configuraciones de seguridad de puerto en una interfaz específica:

```
S1# show port-security interface fastethernet 0/18
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode                : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0025.83e6.4b01:1
Security Violation Count     : 0
S1#
```

Implementar Seguridad de Puertos

- Verificar Seguridad de Puerto.
 - Verificar Direcciones MAC Aprendidas:

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

- Verificar Direcciones MAC Aseguradas:

```
S1# show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports      Remaining Age
        (mins)
-----
1       0025.83e6.4b01   SecureDynamic       Fa0/18     -
1       0025.83e6.4b02   SecureSticky        Fa0/19     -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Mitigar Ataques de VLAN

- Ataques de VLAN.

- Tres principales ataques:

- Suplantación de mensajes DTP. El host atacante hace pasar un host por un switch para establecer un enlace troncal. Logrando enviar tráfico con etiquetado de VLAN, al switch, que entregará los paquetes al destino.
 - Introducción de un switch no autorizado habilitando enlaces troncales. El atacante puede acceder a todas las VLANs en el switch atacado, desde el interruptor no autorizado.
 - Salto de VLAN. Es un ataque de doble etiquetado (o doble encapsulado). Este ataque aprovecha la forma en que funciona el hardware en la mayoría de los conmutadores.

Mitigar Ataques de VLAN

- Pasos para Mitigar Ataques VLAN Hopping (Salto de VLAN).

1. Establecer puertos de acceso.

2. Deshabilitar puertos no utilizados.

3. Establecer troncales manuales.

4. Deshabilitar auto negociación de troncales por DTP.

5. Establecer una VLAN Nativa diferente a la 1.

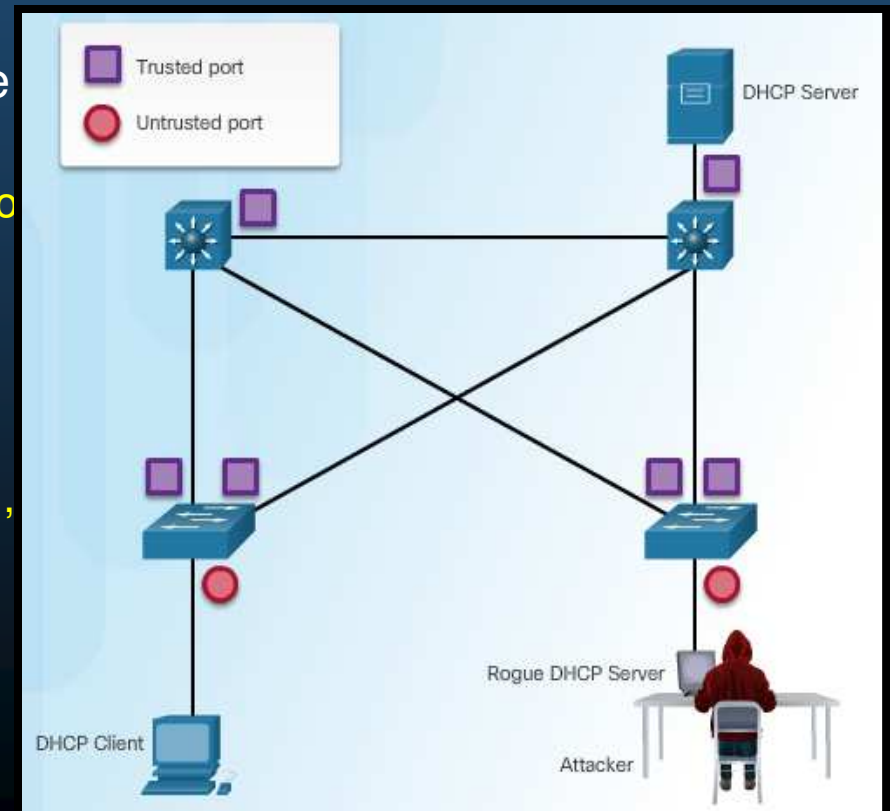
```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```


Mitigar Ataques DHCP

- Ataques de DHCP.
 - DHCP Starvation (Hambruna). Busca generar DoS, con clientes falsos.
 - Se mitiga con seguridad de puerto (una MAC por cada solicitud DHCP).
 - Suplantación de identidad de DHCP (Spoofing). Mas complicado...
 - Si utiliza diferentes MACs por una misma interfáz → Seguridad de Puerto.
 - Puede utilizar su MAC en trama, con diferente MAC en DHCP Request.
 - Seguridad de Puerto Inefectivo.
 - Mitigar con detección de DHCP en puertos de confianza (DHCP Snooping).

Mitigar Ataques DHCP

- **DHCP Snooping** (Detección de DHCP en puertos de confianza).
 - Define 2 tipos de puertos.
 - **Confiables**: Puertos por los que se accede a un **servidor DHCP Legítimo**.
 - **No confiables**: Puertos para **hosts** donde no debería haber servidor DHCP.
 - Limita DHCP Discoverys por puerto.
 - Crea **B.D. de asociaciones DHCP**, para que el switch pueda **filtrar** tráfico DHCP.
 - **MAC** del cliente, **Dir. IP**, **Tiempo de préstamo**, **tipo de asociación**, **Num. de VLAN**, **Interfáz**.
 - **Switch analiza** tráfico DHCP y **desecha** si:
 - **Identifica** tráfico de **DHCP no autorizado**, en puerto no confiable.
 - **Mensajes** de clientes **DHCP no-autorizados**, o diferentes a las registradas en la **BD**.
 - Es **retransmisión DHCP** (opción 82) en un **puerto no confiable**.
 - **MAC** de la trama **no coincide con MAC** del **DHCP Request**.



Mitigar Ataques DHCP

- Pasos para Implementar DHCP Snooping.

- Use los siguientes pasos para configurar DHCP Snooping:

1. Habilitar DHCP Snooping.

```
S(conf)# ip dhcp snooping
```

2. Configurar puertos confiables.

```
S(conf-if)# ip dhcp snooping trust
```

3. Limitar cantidad de DHCP Discoverys permitidos en puertos no confiables.

```
S(conf-if)# ip dhcp snooping limit rate
```

4. Habilitar DHCP Snooping x VLAN.

```
S(conf)# ip dhcp snooping vlan
```

Mitigar Ataques DHCP

- Ejemplo de Configuración de DHCP Snooping.



```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
S1 (config) circuit-id default format: vlan-mod-port
S1 (config) remote-id: 0cd9.96d2.3f80 (MAC)
S1 (config) Option 82 on untrusted port is not allowed
S1 (config) Verification of hwaddr field is enabled
S1 (config) Verification of giaddr field is enabled
S1 (config) DHCP snooping trust/rate is configured on the following Interfaces:
S1 (config)
S1 (config) Interface          Trusted      Allow option  Rate limit (pps)
S1 (config) -----          -
S1 (config) FastEthernet0/1      yes         yes           unlimited
S1 (config) Custom circuit-ids:
S1 (config) FastEthernet0/5      no          no            6
S1 (config) Custom circuit-ids:
S1 (config) FastEthernet0/6      no          no            6
S1 (config) Custom circuit-ids:
S1 (config)
S1 (config) <output omitted>
```



• Mitigar opción 82.

```
S1# show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)  Type           VLAN  Interface
-----
00:03:47:B5:9F:AD  192.168.10.10  193185     dhcp-snooping  5     FastEthernet0/5
```

Mitigar Ataques ARP

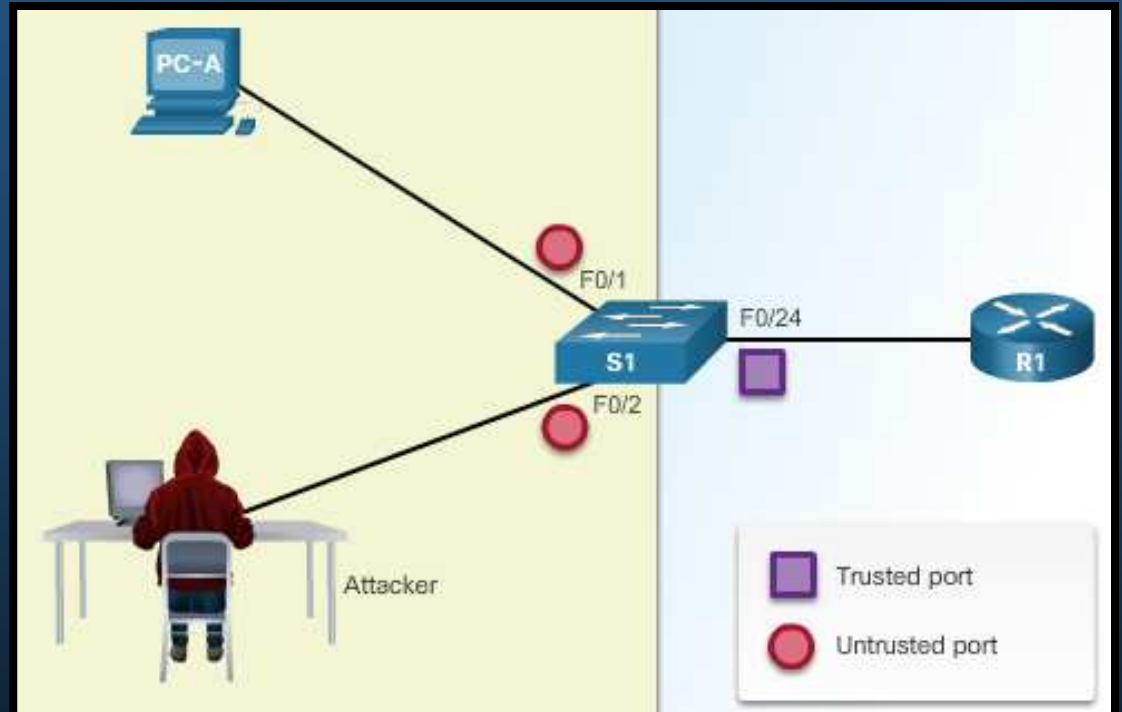
- Inspección Dinámica de ARP (DAI)
 - En un ataque ARP, el atacante envía ARP Reply Gratuitos y Falsos.
 - Se establece como puente para ataque MITM (Man In The Middle).
 - Se mitiga con DAI.
 - Requiere DHCP Snooping.
 - Utiliza B.D. de asociaciones MAC-IP.
 - Acciones de DAI:
 - Permite solo los ARP Replays, que correspondan con un ARP Request, por VLAN.
 - Intercepta todos los ARP Requests y Repls de puertos no confiables.
 - Verifica que los paquetes correspondan con una asociación IP-MAC válida.
 - Desecha y registra ARP Repls inválidos.
 - Establece interface en error-disabled si se excede el número de paquetes ARP configurado.

Mitigar Ataques ARP

- Guías para Implementar DAI.

- Pautas:

- Implementar **DHCP Snooping** globalmente.
 - Habilitar **DHCP Snooping** por VLANs.
 - Habilitar **DAI** por VLANs.
 - Configurar interfaces **confiables** considerando tanto DHCP Snooping como Inspección ARP.
 - Puertos de **acceso** = **No confiables**
 - Puertos hacia **otros dispositivos de red** = **Confiables**



Mitigar Ataques ARP

- Ejemplo de Configuración de DAI.

```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
ip       Validate IP addresses
src-mac  Validate source MAC address
```

```
S1(config)# ip arp inspection validate src-mac
```

```
S1(config)# ip arp inspection validate dst-mac
```

```
S1(config)# ip arp inspection validate ip
```

```
S1(config)#
```

```
S1(config)# do show run | include validate
```

```
ip arp inspection validate ip
```

```
S1(config)#
```

```
S1(config)# ip arp inspection validate src-mac dst-mac ip
```

```
S1(config)#
```

```
S1(config)# do show run | include validate
```

```
ip arp inspection validate src-mac dst-mac ip
```

```
S1(config)#
```

¡Cuidado! Cada entrada sobre-escribe la anterior

```
config)# ip dhcp snooping
```

```
config)#
```

```
config)# ip dhcp snooping vlan 10
```

```
config)# ip arp inspection vlan 10
```

```
config)#
```

```
config)# interface fa0/24
```

```
config-if)# ip dhcp snooping trust
```

```
config-if)# ip arp inspection trust
```

```
S1(config-if)#
```

- Adicionalmente DAI puede verificar direcciones IP y MAC origen y destino.
- **S(conf)# ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
 - **src-mac**: Verifica MAC origen en trama contra MAC origen en ARP.
 - **dst-mac**: Verifica MAC destino en trama contra MAC destino en ARP.
 - **ip**: Verifica IP en busca de errores o valores inesperados.

Mitigar Ataques STP

- **PortFast y BPDU Guard.**

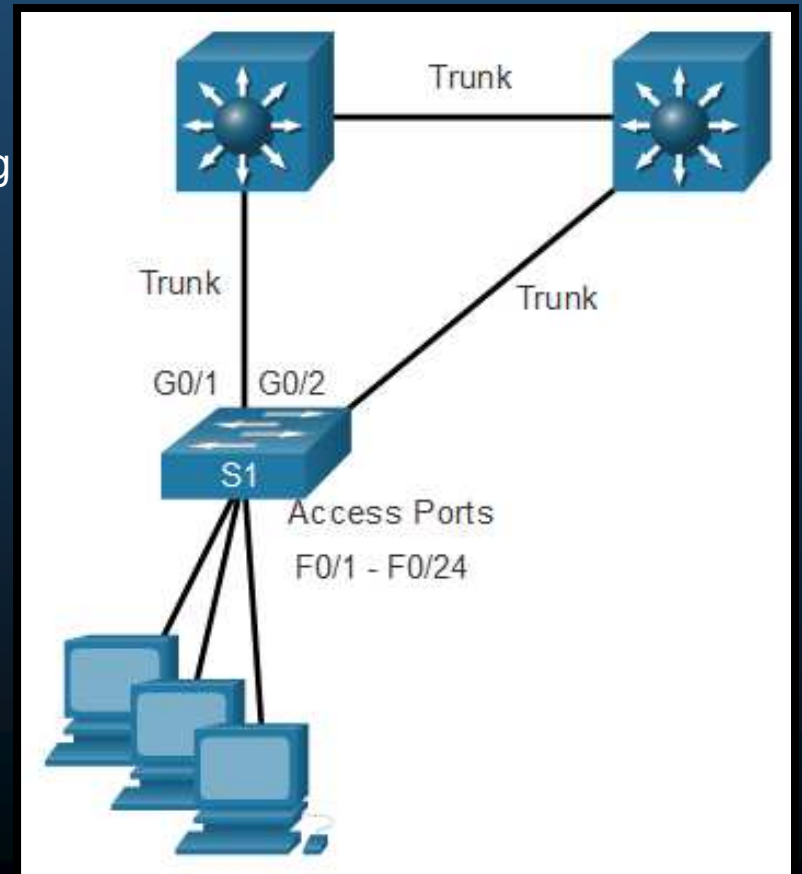
- Un atacante puede manipular el STP al fingir su host, como Puesto Raíz y capturar todo el tráfico de la red.

- Para mitigar existe:

- **PortFast:** Cambia de estado de bloqueo a re- envío. Sin pasar por Listening ó Learning
 - Aplicar solo a puertos de usuario (acceso).

- **BPDU Guard:** Deshabilita puertos que reciban BPDUs.
 - Aplicar a puertos de usuario PortFast para evitar inserción de Switches Espurios.

- En la figura FA0/1-24 deberíasn implementar: PortFast yBPDU Guard.



Mitigar Ataques STP

- Configuración de PortFast.

- Permite que los Hosts puedan conectarse a la Red mas rápido de lo normal. (Antes de que STP converja)
 - Pasa de estado de bloqueo a re-envío. Sin pasar por Listening ó Learning.
 - Aplicar solo a puertos de usuario (acceso).

Habilitar PortFast en todos los puertos:

```
S(config)# spanning-tree portfast default
```

Habilitar PortFast en una interface determinada:

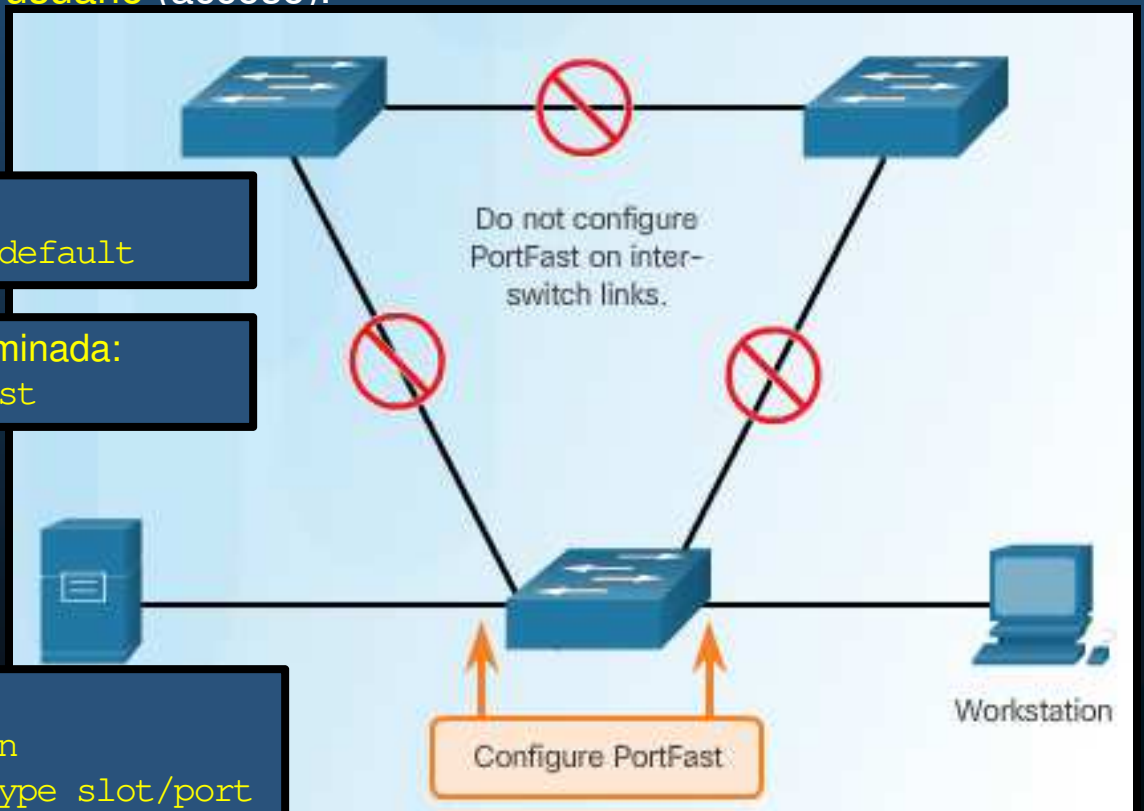
```
S(config-if)# spanning-tree portfast
```

- Su uso en troncales puede provocar bucles STP.

Verificar si PortFast está habilitado:

```
S# show running-config | begin span
```

```
S# show running config interface type slot/port
```



Mitigar Ataques STP

- Ejemplo de Configuración PortFast.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
  host. Connecting hubs, concentrators, switches, bridges, etc... to this
  interface when portfast is enabled, can cause temporary bridging loops.
  Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
  have effect when the interface is in a non-trunking mode
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all
  should now disable portfast explicitly on switched ports
  switches and bridges as they may create temporary bridging
S1(config)# exit
```

```
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
S1#
```

Mitigar Ataques STP

- Configurar BPDU Guard.

- BPDU Guard **coloca** el puerto en estado **error-disabled**, al recibir BPDUs.
 - **Protege** Puertos **PortFast** para que **no intervengan** en convergencia **STP**.
 - **Evita** que **se agreguen switches** adicionales a la topología.



Habilitar BPDU Guard en todos los puertos PortFast:

```
S(config)# spanning-tree
```

Habilitar BPDU Guard en un puerto:

```
S(config-if)# spanning-tree
```

```
Switch# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short
Name          Blocking Listening Learning Forwarding STP Active
-----
1 VLAN        0          0          0          1          1

<output omitted>
```

```
%SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port F0/1 with BPDU Guard enabled. Disabling port.
%PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putting F0/1 in err-disable state
```

Mitigar Ataques STP

- Ejemplo de Configuración BPDU Guard.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID          is enabled
Portfast Default            is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default          is disabled
EtherChannel misconfig guard is enabled
UplinkFast                  is disabled
BackboneFast                is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

Integración

- **Actividad Práctica.**

- **Retome su Topología** creada en el **capítulo 6** y **añada** lo siguiente:
 - **Implemente** donde resulte conveniente **y justifique**:
 - **Seguridad de Puerto**
 - Implemente lo necesario para **mitigar ataques VLAN**
 - Implemente lo necesario para **mitigar ataques DHCP**
 - Implemente lo necesario para **mitigar ataques ARP**
 - Implemente lo necesario para **mitigar ataques STP**
 - Incluya **etiquetas de texto** en su topología donde **describa y justifique sus implementaciones.**



Capítulo 12

Conceptos de WLANs

<https://contenthub.netacad.com/srwe/12.1.1>

Introducción a la tecnología inalámbrica

- Beneficios de lo Inalámbrico.

- Las personas requieren movilidad mediante varios dispositivos, como computadoras de escritorio y portátiles, tablet PC y smartphones. Deseo de viajar y llevar con ellas su conexión a la red.
- Existen muchas infraestructuras diferentes (LAN cableada, redes de proveedores de servicios) ofrecen movilidad limitada;
- LAN inalámbrica (WLAN) movilidad versátil en entornos empresariales.
- La capacidad móvil permite que un dispositivo inalámbrico mantenga el acceso a Internet sin perder la conexión.

Introducción a la tecnología inalámbrica

- **Tipos de Redes inalámbricas**
 - **Redes de área personal inalámbrica (WPAN):** tienen alcance de pocos metros (6m a 9m). En WPAN, son dispositivos con Bluetooth o ZigBee habilitado. Basadas en estándar IEEE 802.15y frecuencia de 2.4GHz.
 - **LAN inalámbricas (WLAN):** tiene alcance de 90 m. aprox., como para una sala, un hogar, una oficina e incluso un campus. Basadas en estándar IEEE 802.11 y frecuencia de 2.4GHz y 5GHz.
 - **Redes inalámbricas de área metropolitana (WMAN):** Provee conectividad inalámbrica en áreas geográficas mas grandes, como una ciudad o distrito. Usan frecuencias bajo licencia.
 - **Redes de área amplia inalámbrica (WWAN):** tiene un alcance de kilómetros, implica comunicaciones para una nación o global, mediante retransmisiones de microondas que usan igualmente frecuencias bajo licencia.

Introducción a la tecnología inalámbrica

- Tecnologías inalámbricas



Wi MAX:

- ✓ Estándar IEEE 802.16, denominado “WiMAX”.
- ✓ Utiliza topología de punto a multipunto para proporcionar acceso celular de banda ancha.
- ✓ Se usa como alternativa a las tecnologías de cable y DSL.
- ✓ Admite velocidades de hasta 1 Gb/s a distancias hasta 50km.
- ✓ Uso de torres similares a las celulares.

Introducción a la tecnología inalámbrica

- Estándares 802.11

El estándar de **WLAN IEEE 802.11** define cómo se usa la **RF** en las **bandas de frecuencia ISM** sin licencia para la **capa física** y la **subcapa MAC** de los enlaces inalámbricos.

- **802.11** (1997), banda de 2,4 GHz y velocidades de hasta 2 Mb/s.
 - Uso de **antena** para **transmitir y recibir** señales inalámbricas.
- **IEEE 802.11a** (1999), banda de 5 GHz y velocidades de hasta 54 Mb/s. Área de cobertura menor y menos efectivo al penetrar estructuras. **No interoperable con 802.11b y 802.11g.**
- **IEEE 802.11b** (1999), banda de 2,4 GHz y velocidades de hasta 11 Mb/s. Mayor alcance y **pueden penetrar mejor las estructuras edilicias que 802.11a.**
- **IEEE 802.11g** (2003), banda de frecuencia **de 2,4 GHz** y velocidades de hasta 54 Mb/s. **Compatible con 802.11b.** Al admitir un **cliente 802.11b**, se reduce el ancho de banda general.

Introducción a la tecnología inalámbrica

- Estándares 802.11

- **IEEE 802.11n** (2009), bandas de frecuencia de 2,4 GHz y 5 GHz, (dispositivo de doble banda). Velocidades desde 150 Mb/s hasta 600 Mb/s, alcance de hasta 70 m (0,5 mi). Requieren varias antenas con tecnología de múltiple entrada múltiple salida (MIMO). Compatible con 802.11a/b/g.
- **IEEE 802.11ac** (2013), banda de frecuencia de 5 GHz, velocidades desde 450 Mb/s hasta 1,3 Gb/s (1300 Mb/s). Tecnología MIMO. Compatible con 802.11a/n.
- **IEEE 802.11ax** (2019) conocido como “HEW” (High-Efficiency Wireless), Solución Wi-Fi de bandas en 2,4 GHz, 5 GHz, Mejorar el rendimiento promedio, multiplicándolo hasta por 4, permite a más usuarios trabajar en un mismo punto de acceso simultáneamente, ya que soporta hasta 6,97 Gbps trabajando en ocho flujos espaciales. Posibilidad de uso de bandas entre 1GHz y 7GHz si están disponibles.

Introducción a la tecnología inalámbrica

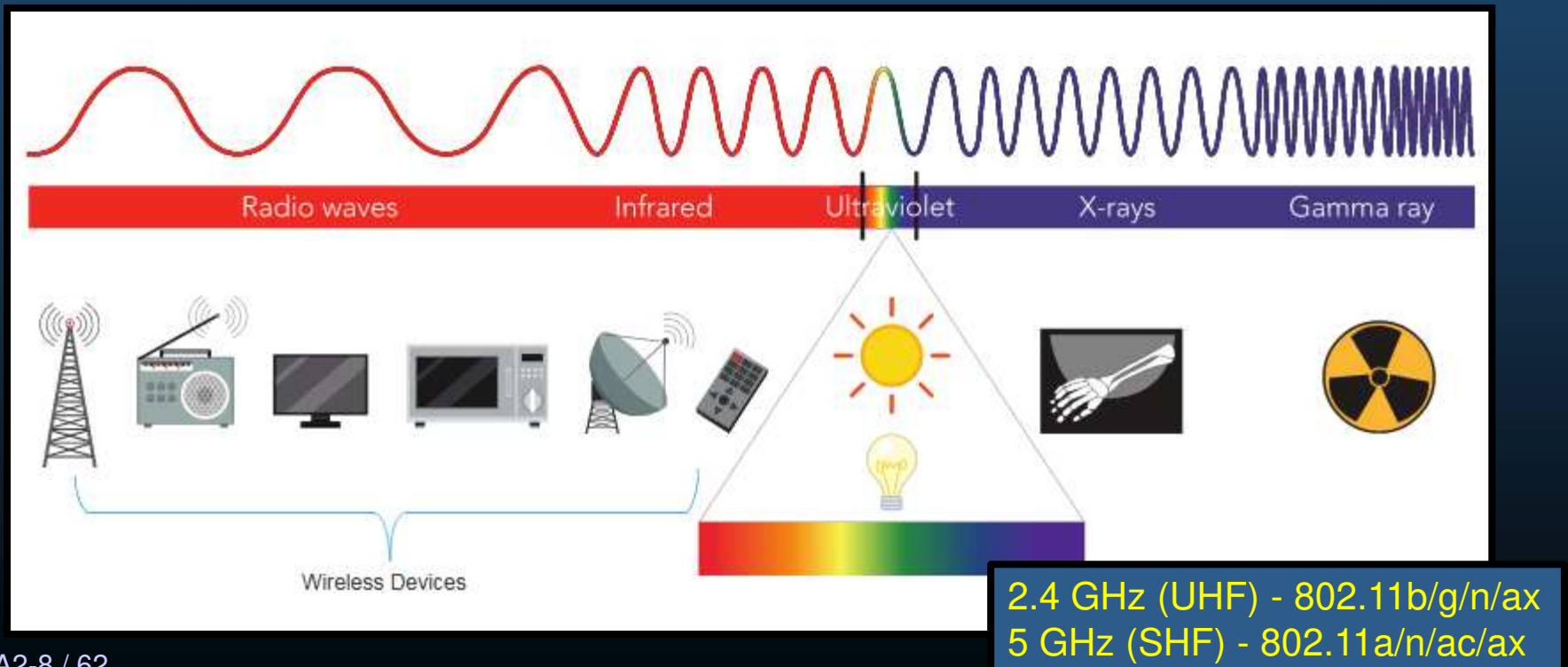
- Estándares 802.11

Estandar IEEE	Velocidad Máxima	Frecuencias	Compatibilidad
802.11	2 Mb/s	2.4 GHz	---
802.11a	54 Mb/s	5 GHz	---
802.11b	11 Mb/s	2.4 GHz	---
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz y 5GHz	802.11a/b/g
802.11ac	1.3 Gb/s	5 GHz	802.11a/n
802.11ax	11 Gb/s	1 GHz - 7 GHz	802.11a/b/g/n/ac

Introducción a lo Inalámbrico

- Radio Frecuencias.

- Los dispositivos inalámbricos operan en el rango del espectro electromagnético.
 - Las WLAN operan principalmente en los 2.4GHz y los 5GHz.
 - Los dispositivos WLAN cuentan con emisores/receptores sintonizados en dichas frecuencias.



Introducción a lo Inalámbrico

- **Organizaciones de Estándares Inalámbricos.**

- Los **estándares aseguran la interoperabilidad** entre dispositivos de diferentes marcas.

- **ITU** (International Telecommunication Union): **regula el uso del espectro de frecuencias de radio y orbitas satelitales.** Específicamente la ITU-R (Radiocomunicación).



- **IEEE**: Especifica **cómo modular radiofrecuencias para transmitir información.** Manteniendo las familias de **estándares 802.**



- **Wi-Fi Alliance**: Asociación global dedicada a la promoción, crecimiento y aceptación de WLANs. Buscan mejorar la interoperabilidad de productos basados en estándares 802.11 y **certifican a los productos y vendedores que cumplen cabalmente los estándares.**



Componentes de WLANs

- NIC inalámbrico

La mayoría de los dispositivos de red inalámbricos requieren un adaptador de red inalámbrico (NIC inalámbrico) para conectarse a una red inalámbrica.

- Tecnología de red inalámbrica
- Dispositivos de red inalámbricos

Las tarjetas de red inalámbricas se conectan a un puerto de red en un dispositivo de red. Si un dispositivo de red no tiene un puerto de red, se puede usar un adaptador de red inalámbrico (NIC inalámbrico) para conectarse a una red inalámbrica.

Si un dispositivo de red no tiene un puerto de red, se puede usar un adaptador de red inalámbrico (NIC inalámbrico) para conectarse a una red inalámbrica.

Adaptadores USB inalámbricos



Adaptador mini-USB de doble banda Wireless-AC Wi-Fi Linksys AE6000 802.11ac de 2,4 GHz o 5 GHz



Adaptador USB N de doble banda de alto rendimiento Linksys AE3000

ente:

s

smisor, un

de usar un

ANs

Red doméstica típica



Router inalámbrico Cisco Linksys EA6500 802.11ac



En las pequeñas empresas y los hogares, los routers inalámbricos desempeñan la función de punto de acceso, switch Ethernet y router.

Como lo siguiente:

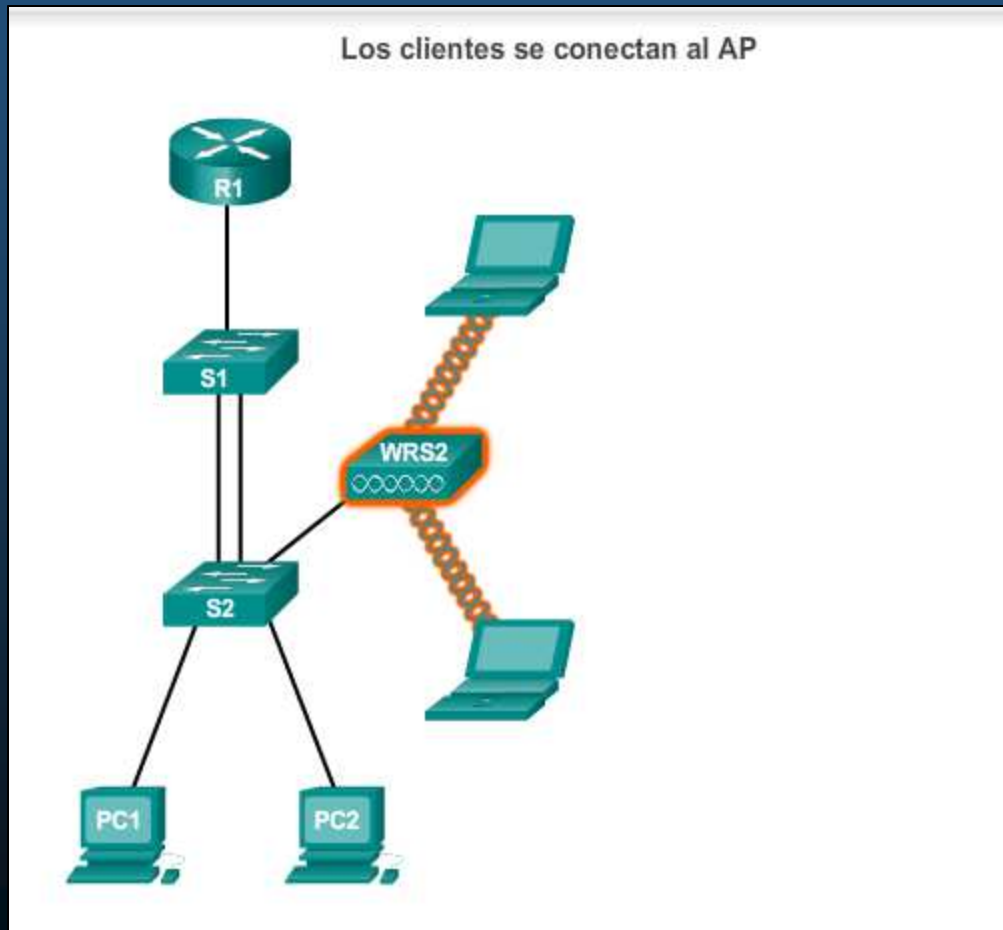
802.11a/b/g/n/ac/ax.

Tiene características avanzadas:

- ✓ Acceso de alta velocidad.
- ✓ Diseño óptimo para transmitir video.
- ✓ Compatibilidad con IPv6,
- ✓ Compatibilidad con QoS,
- ✓ Fácil configuración mediante Wi-Fi WPS.
- ✓ Puertos USB

Componentes de WLANs

- Puntos de Acceso (APs) Inalámbricos.



Los clientes inalámbricos usan la NIC inalámbrica para detectar los AP cercanos que anuncian su SSID.

Los clientes después intentan asociarse y autenticarse con un AP.

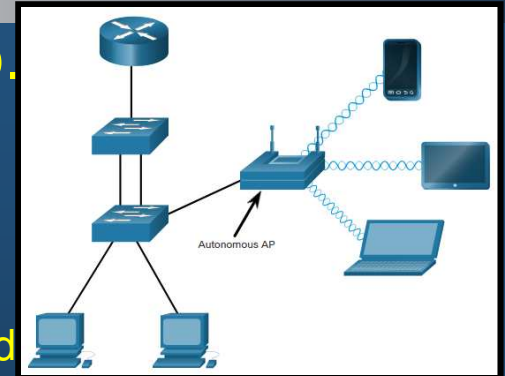
Después de la autenticación, los usuarios inalámbricos tienen acceso a los recursos de la red.

Componentes de WLANs

- **Categorías de Puntos de Acceso Inalámbrico.**

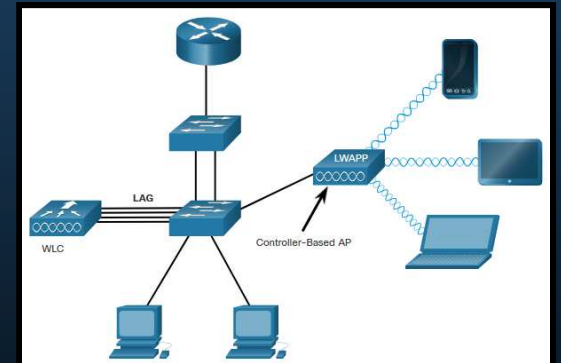
- **AP autónomos**

- También denominados “AP pesados”,
- Se configuran mediante la CLI de Cisco o una GUI.
- Son útiles cuando solo se requiere un par de AP en la red.
- Se pueden controlar varios AP mediante los servicios de dominio inalámbrico (WDS)
- Se pueden administrar mediante el motor de soluciones de LAN inalámbricas (WLSE) CiscoWorks.



- **AP basados en controladores**

- AP Ligeros (LAPs) ó basados en controladores administrados desde un controlador (WLC), mediante el protocolo LWAPP.
- Útiles cuando se requieren muchos APs en la red.
- Cada que se agregan más AP, el controlador WLAN lo configura y administra automáticamente.
- WLC usa 4 puertos agregados (LAG) similar a Etherchannel, pero no usa LACP ni PaGP.



Componentes de WLANs

- Antenas inalámbricas

Cisco desarrolló antenas para condiciones específicas: física, distancia y estética.

La mayoría de los APs pueden usar:

- **Antenas Wi-Fi omnidireccionales:** antenas dipolos básicas (antenas de goma). Cobertura de 360°. Ideal para casas, cuartos de conferencias y exteriores.
- **Antenas Wi-Fi direccionales:** concentran la señal de radio en un sentido determinado (Yagi y Parabólicas). Proveen señales mas fuertes en una dirección y reducida en otras.
- **Antenas MIMO:** antena de Múltiples Entradas y Múltiples Salidas, usa varias antenas para incrementar disponibilidad y ancho de banda para diferentes estándares IEEE 802.11. Hasta 8 antenas.



Componentes de WLANs

- Antenas inalámbricas

Varias antenas inalámbricas Cisco

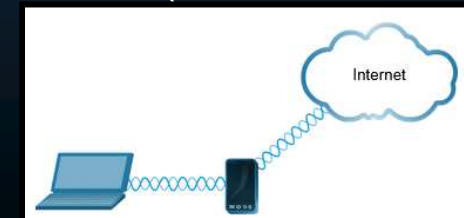
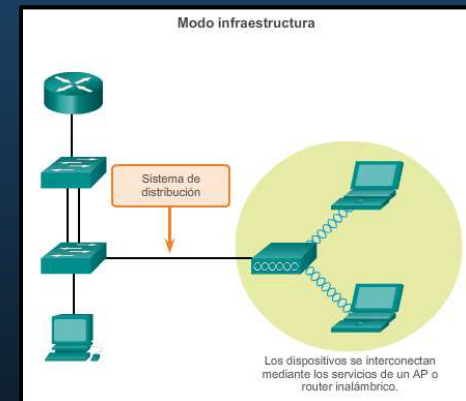
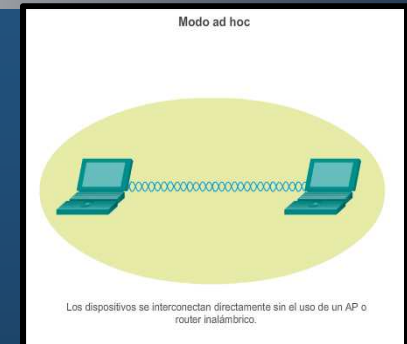


Operación de una WLAN

- Modos de topología inalámbrica 802.11

Dos modos de topología inalámbrica:

- **Modo ad hoc:** dos dispositivos se conectan de manera inalámbrica (IBSS) sin la ayuda de un dispositivo de infraestructura, como un router o un AP inalámbrico. (Bluetooth y Wi-Fi Direct)
- **Modo de infraestructura:** los clientes inalámbricos se conectan mediante un router o un AP inalámbrico, quienes se conectan a su vez a la infraestructura de la red mediante el sistema de distribución (DS) cableado (Ethernet).
- **Enlazado (Tethering):** variante de ad-hoc, donde un dispositivo móvil (con acceso a datos celulares), actúa como punto de enlace (router Wi-Fi), para brindar salida a Internet (hotspot) a otros dispositivos.



Operación de una WLAN

- **Modo infraestructura**
 - Dos componentes básicos de topología:
 - Conjunto de servicios básicos (BSS)
 - Conjunto de servicios extendidos (ESS).
- **Conjunto de servicios básicos (BSS)**
 - Un único AP interconecta todos los clientes inalámbricos asociados.
 - BSA es el área de cobertura real (BSA y BSS suelen usarse indistintamente).
 - La MAC del AP identifica cada BSS y se denomina “identificador del conjunto de servicios básicos” (BSSID).
 - BSSID es el nombre formal del BSS y siempre se asocia a un único AP.

Operación de una WLAN

- BSS

Resumen del conjunto de servicios básicos



Resumen de BSS

Modo de topología WLAN	Infraestructura
Topología inalámbrica 802.11	conjunto de servicios básicos (BSS)
Cantidad de AP	1
Área de cobertura de 802.11	Área de servicios básicos (BSA)

Se muestran **dos BSS**. Los **círculos** representan el **área de cobertura** dentro de la que los **clientes inalámbricos del BSS** pueden **permanecer comunicados**. Se denomina “**área de servicios básicos**” (BSA). Si un **cliente sale de su BSA**, ya **no se puede comunicar directamente**.

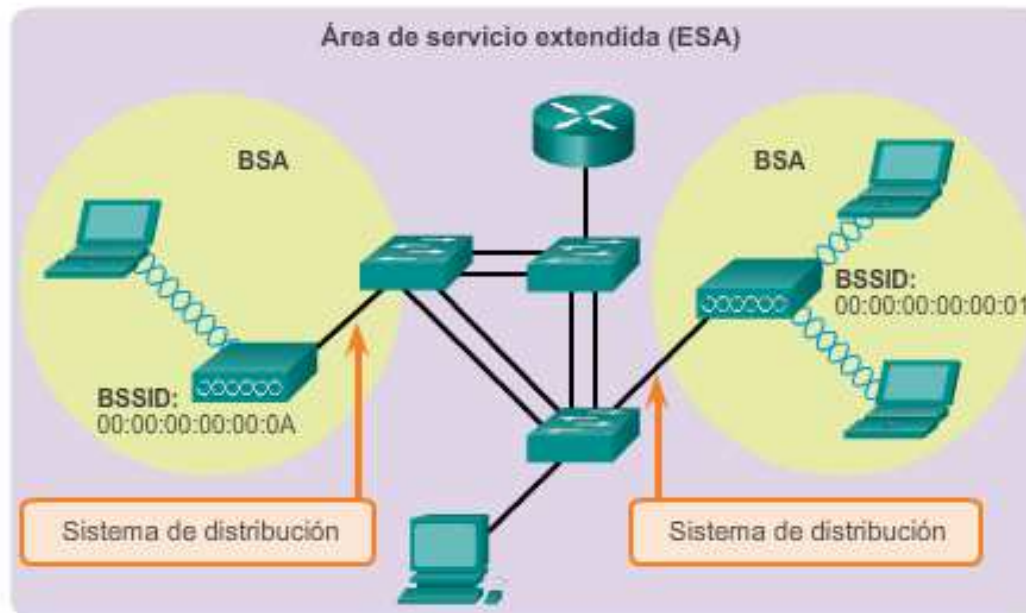
Operación de una WLAN

- ESS
 - **Conjunto de servicios extendidos (ESS)**
 - Un **ESS** es la unión de **dos o más BSS interconectados** mediante un sistema de distribución (**DS**) por cable.
 - Los **clientes inalámbricos en una BSA** ahora se pueden comunicar con los clientes inalámbricos en **otra BSA dentro del mismo ESS**.
 - Los **clientes con conexión inalámbrica móvil** se pueden trasladar de una **BSA a otra (dentro del mismo ESS)** y se pueden conectar sin inconvenientes.
 - Cada **ESS se identifica mediante un SSID** y, en un **ESS**, cada **BSS se identifica mediante su BSSID**.

Operación de una WLAN

- ESS

Resumen del conjunto de servicios extendidos



Resumen de ESS

Modo de topología WLAN	Infraestructura
Topología inalámbrica 802.11	conjunto de servicios extendidos (ESS)
Cantidad de AP	2 o más
Área de cobertura de 802.11	Área de servicio extendida (ESA)

El área rectangular representa el área de cobertura dentro de la que los miembros de un ESS se pueden comunicar.

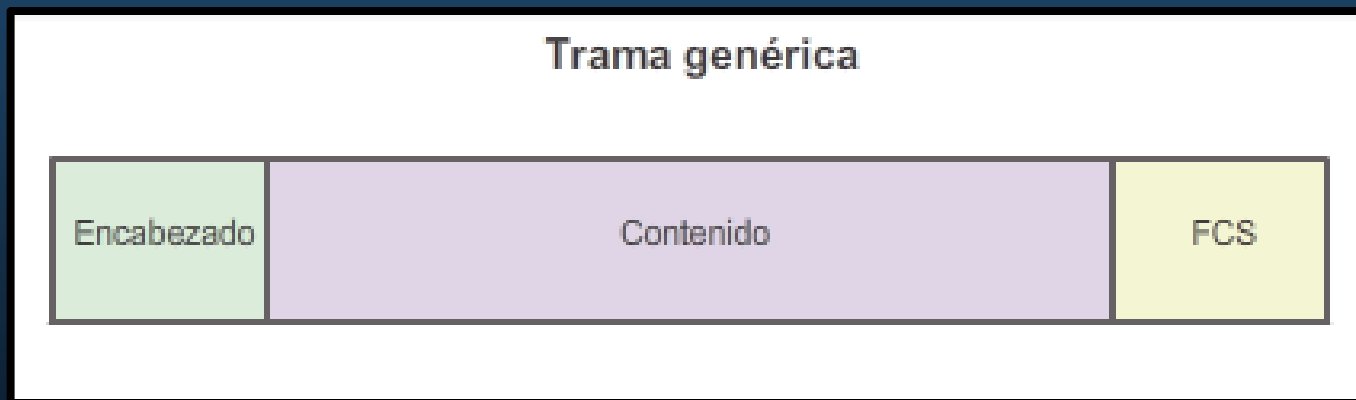
Esta área se denomina “área de servicios extendidos” (ESA).

Una ESA a menudo involucra varios BSS en configuraciones superpuestas o separadas.

Operación de una WLAN

- Trama 802.11 inalámbrica

Todas las tramas de capa 2 constan de un **encabezado**, un **contenido** y una **sección FCS**.



Operación de una WLAN

- Trama 802.11 inalámbrica

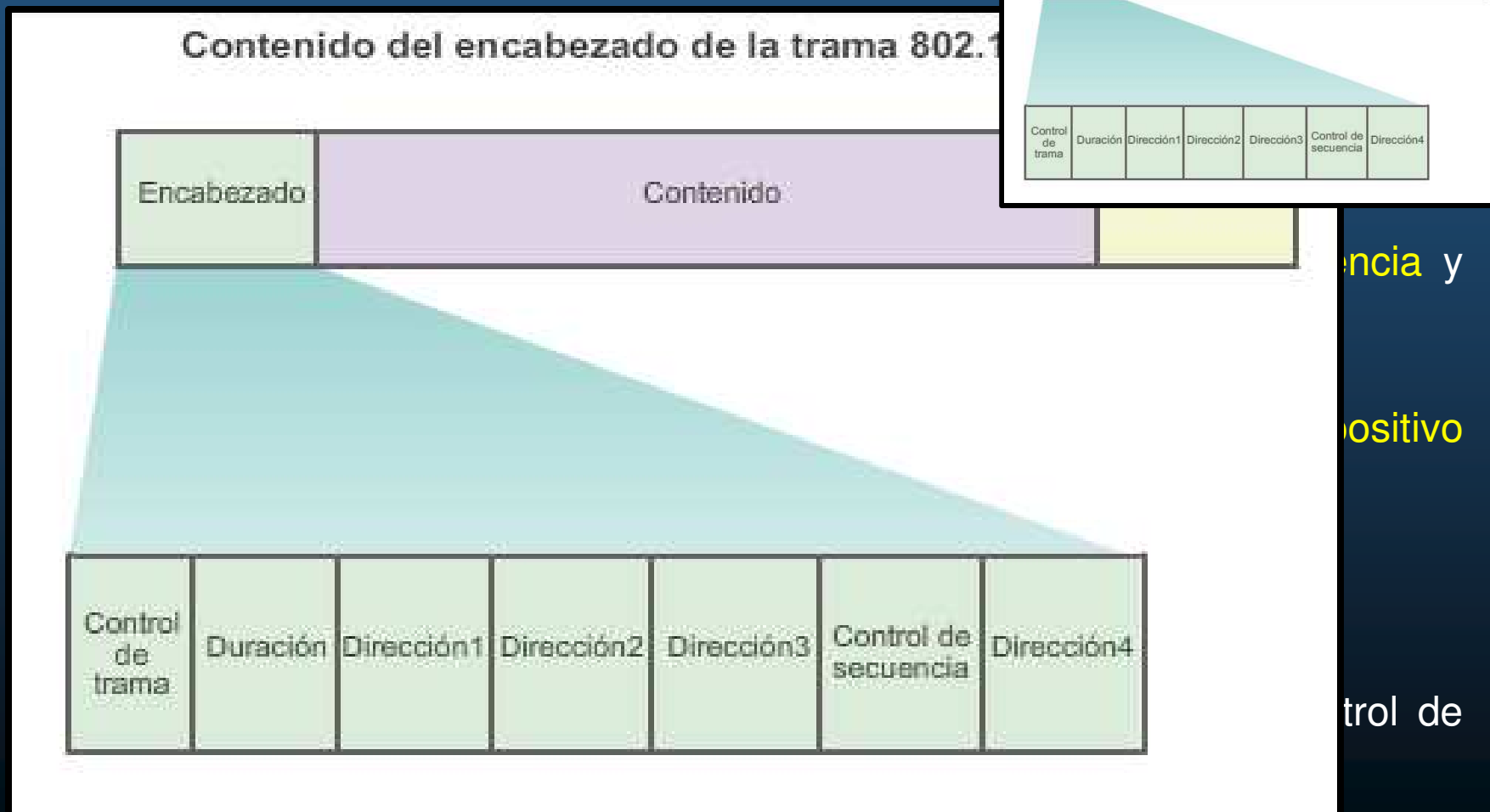
Las tramas 802.11 inalámbricas contienen los siguientes campos:



- **Control de trama:** identifica el tipo de trama inalámbrica y contiene la versión del protocolo, el tipo de trama, de dirección, la administración de energía y la configuración de seguridad.
- **Duración:** se usa para indicar la duración restante necesaria para recibir la siguiente transmisión de tramas.
- **Dirección 1:** contiene la dirección MAC del dispositivo o AP receptor inalámbrico (destino final en la red).
- **Dirección 2:** contiene la dirección MAC del dispositivo o AP transmisor inalámbrico (nodo que inició la trama).

Operación de una WLAN

- Trama 802.11 inalámbrica



encia y
ositivo
trol de

Operación de una WLAN

- CSMA/CA (Acceso múltiple por detección de portadora y prevención de colisiones)

Las WLAN IEEE 802.11 usan el protocolo MAC CSMA/CA.

Los sistemas Wi-Fi son configurados en modo half-dúplex, creando un problema, ya que un cliente inalámbrico no puede oír mientras envía y no es posible detectar una colisión.

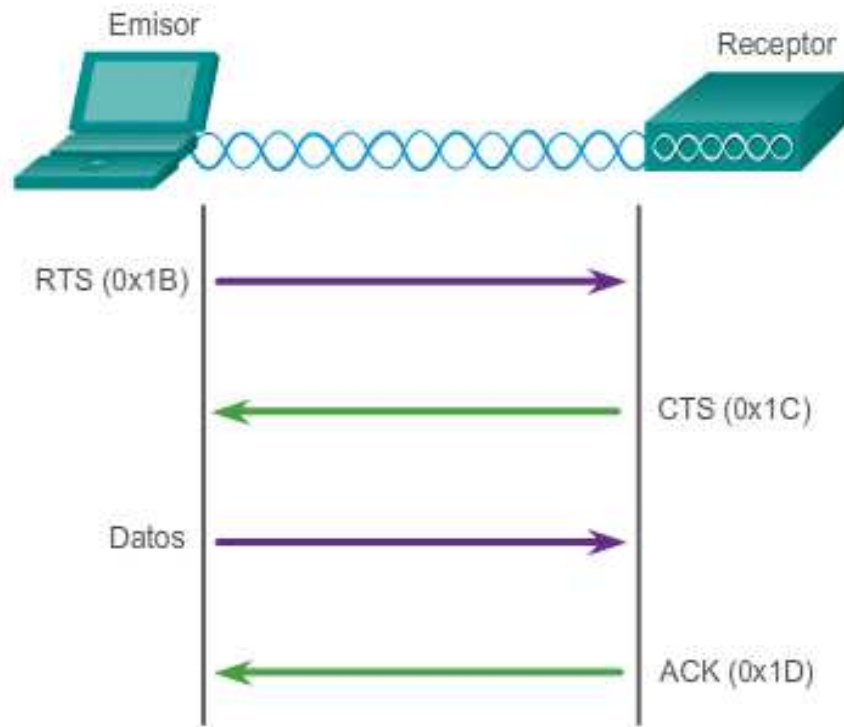
El IEEE desarrolló una manera de prevención de colisiones denominado “función de coordinación distribuida” (DCF). Un cliente inalámbrico transmite solo si el canal está libre. Todas las transmisiones se confirman; si no recibe un acuse de recibo, supone que ocurrió una colisión y lo vuelve a intentar.

Los clientes inalámbricos y los AP usan las tramas de control RTS y CTS para facilitar la transferencia de datos.

Operación de una WLAN

- CSMA/CA

Uso de las tramas de control para la transferencia de datos



Cuando un cliente inalámbrico envía datos:

- ✓ Evalúa los medios para determinar si otros dispositivos los están usando.
- ✓ Si no, envía una trama RTS al AP, trama que se usa para solicitar acceso dedicado al medio de RF durante un período específico.
- ✓ Si está disponible, otorga al cliente inalámbrico acceso al medio de RF mediante el envío de una trama CTS de la misma duración.
- ✓ Todos los dispositivos ceden los medios al nodo transmisor para la transmisión.

La trama de control CTS incluye el período durante el que se le permite transmitir al nodo transmisor.

Operación de una WLAN

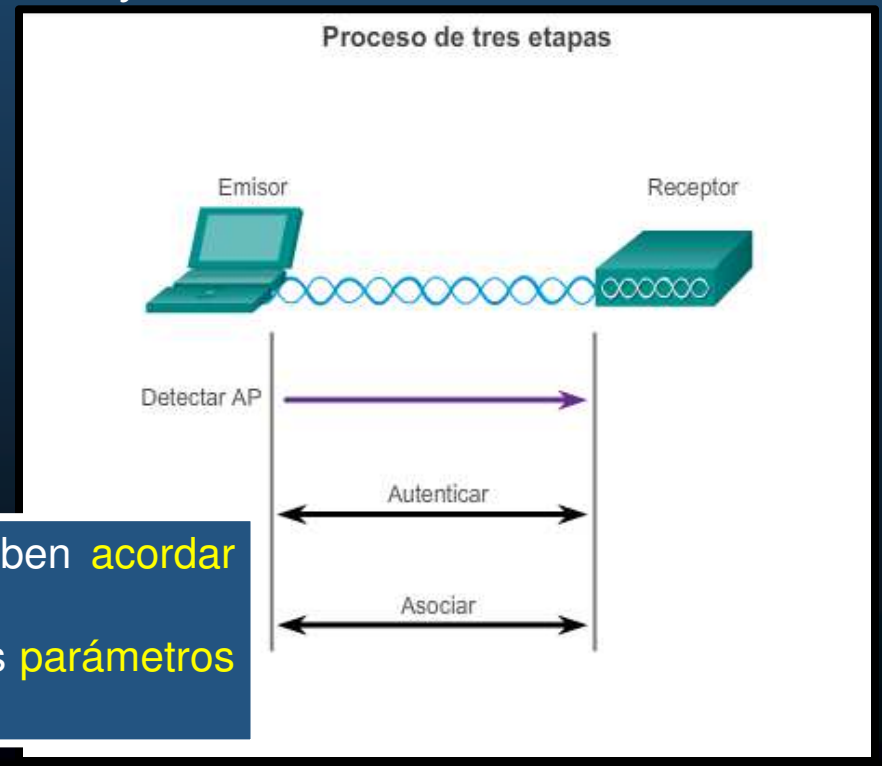
- Asociación de puntos de acceso y clientes inalámbricos

Los dispositivos inalámbricos que se comunican en una red, se deben **asociar a un AP o un router inalámbrico**.

Parte proceso 802.11 es **descubrir una WLAN y conectarse a esta**.

Los dispositivos inalámbricos usan las **tramas de administración** para completar el siguiente **proceso de tres etapas**:

- Descubrir nuevos AP inalámbricos.
- Autenticar con el AP.
- Asociarse al AP.



Para asociarse, un cliente inalámbrico y un AP deben acordar parámetros específicos.

Para permitir la negociación, se deben configurar los parámetros en el AP y posteriormente en el cliente.

Operación de una WLAN

- **Parámetros de asociación**

Los parámetros inalámbricos configurables comunes incluyen lo siguiente:

- **SSID:** un SSID es un **identificador único**, los nombres tienen una longitud de 2 a 32 caracteres.
- **Password (Contraseña):** necesaria para **autenticarse** con el **AP**. Las contraseñas se denominan “clave de seguridad”.
- **Network mode (Modo de red):** se refiere a los **estándares de WLAN** 802.11a/b/g/n/ac/ad. Los **AP** y los **routers** inalámbricos pueden funcionar en modo **Mixed (Mixto)**.
- **Security mode (Modo de seguridad):** la configuración de los parámetros de seguridad, como **WEP, WPA o WPA2**.
- **Channel settings (Configuración de canales):** se refiere a las **bandas de frecuencia** que se usan para transmitir datos inalámbricos.

Operación de una WLAN

- **Detección de AP**

Los dispositivos inalámbrico detectan un AP o un router inalámbrico y se conectan a este.

Los clientes inalámbricos se conectan al AP mediante un proceso de análisis (sondeo).

Este proceso se realiza de la siguiente manera :

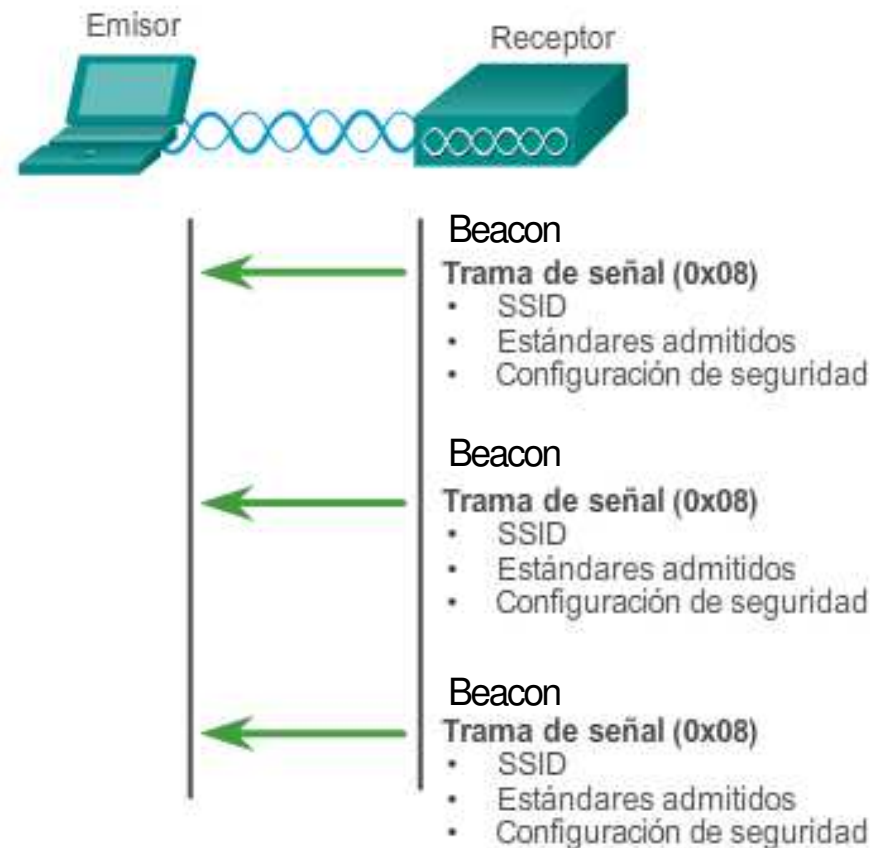
- **Modo pasivo:** el AP envía periódicamente tramas de señal de difusión que contienen el SSID, los estándares admitidos y la configuración de seguridad. El propósito es permitir que se descubran redes y que AP existen en un área determinada.
- **Modo activo:** los clientes inalámbricos deben conocer el nombre del SSID. El cliente inalámbrico inicia el proceso al transmitir. La solicitud de sondeo incluye el nombre del SSID y los estándares admitidos.

Operación de una WLAN

- Detección de AP
 - **Modo pasivo**

Se muestra cómo funciona el modo pasivo con el AP que transmite por difusión una trama de señal con determinada frecuencia.

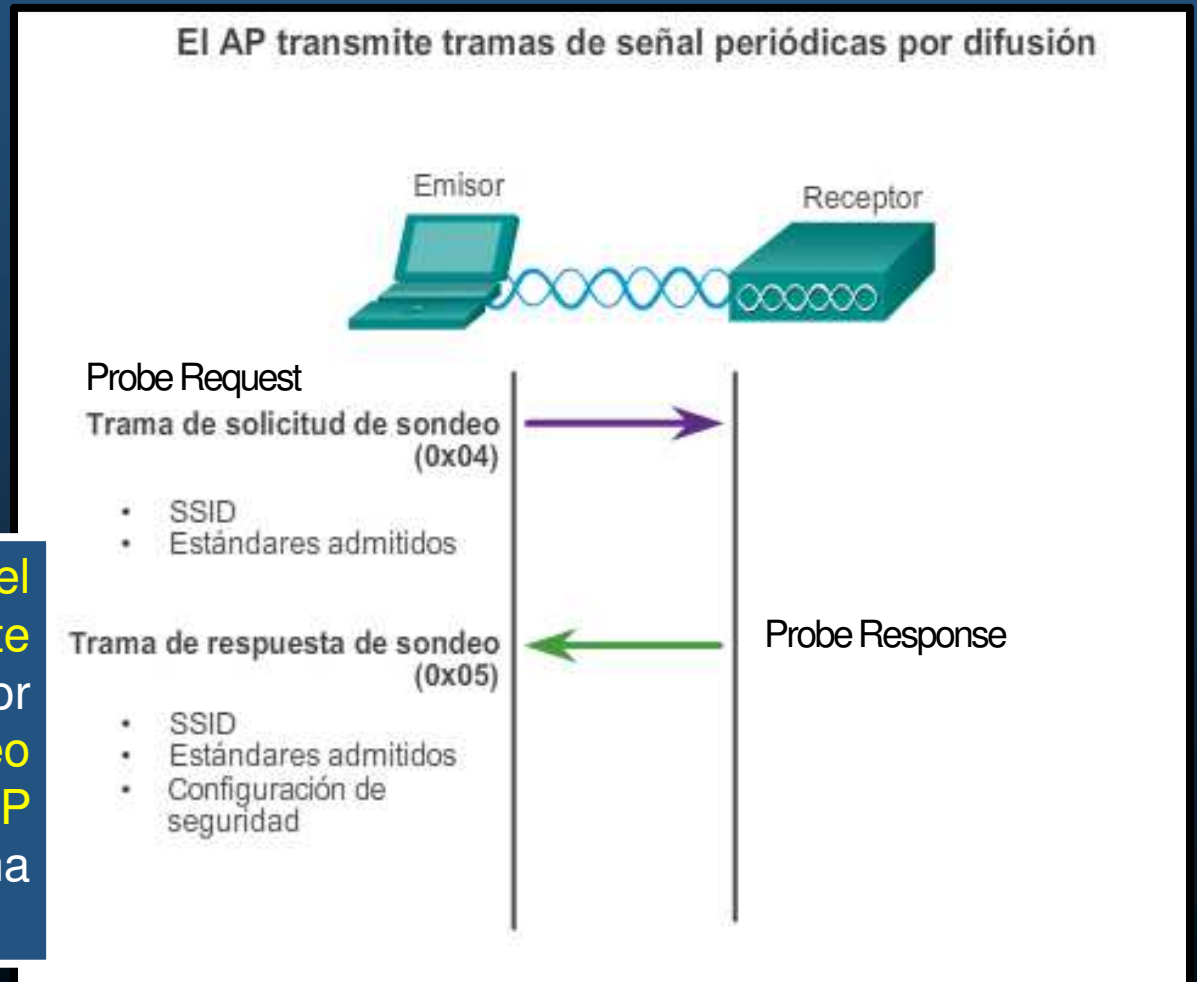
Los dispositivos cliente escuchan un AP



Operación de una WLAN

- Detección de AP
 - **Modo activo**

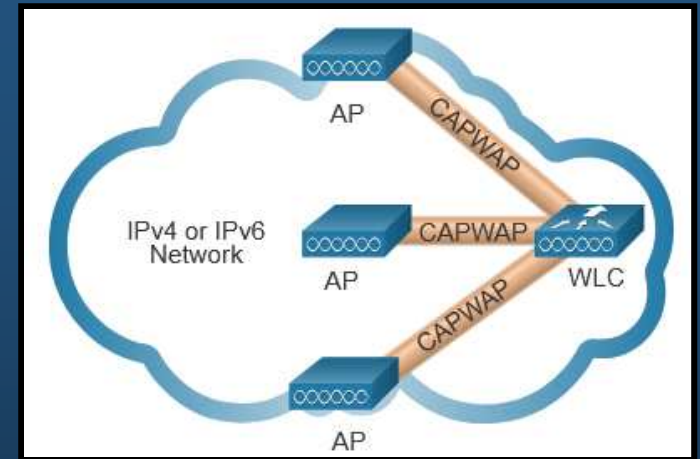
Se muestra cómo funciona el modo activo con un cliente inalámbrico que transmite por difusión una solicitud de sondeo para un SSID específico. El AP con ese SSID responde con una trama de respuesta de sondeo.



Operación CAPWAP

- **Introducción a CAPWAP.**

- Protocolo **Estándar IEEE.**
- **Habilita un WLC** par administrar múltiples **Aps.**
- Responsable de la **encapsulación del tráfico de clientes** entre un **AP** y el **WLC.**
- Basado en LWAPP, pero con **seguridad** en al **Protocolo de Capa de Transporte de Datagramas (DTLS)**
 - Establece **túneles** en puertos **UDP.**
- Puede Operar en **IPv4 e IPv6.**
 - Uso de **puertos 5246 y 5247.**
 - **Múltiples protocolos IP** utilizados en cabeceras.
 - **IPv4** usa protocolo IP **17**
 - **IPv6** usa protocolo IP **136**



Operación CAPWAP

- **Arquitectura MAC Dividida.**

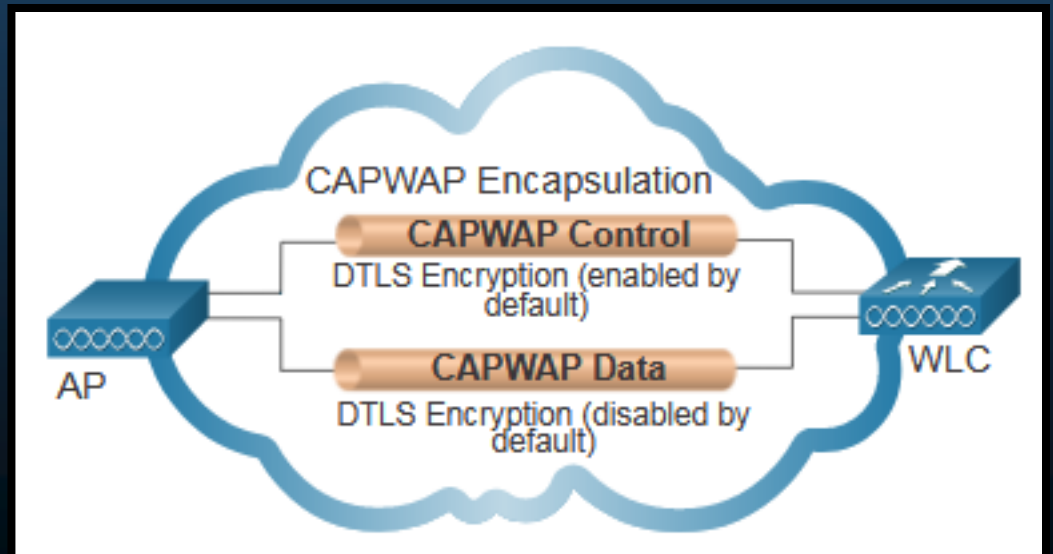
- Le **permite** a CAPWAP **realiza tareas** comunes de los APs y **distribuir las** entre dos componentes funcionales:

- **Funciones MAC AP**
- **Funciones MAC WLC**

Funciones MAC AP	Funciones MAC WLC
Beacons y Respuestas Probe	Autenticación
Acuses de recibo y retransmisión de paquetes.	Asociación y re-asociación de clientes vagabundos (roaming).
Encolado de tramas y manejo de prioridades de paquetes.	Traducción de tramas de otros protocolos
Cifrado / descifrado de datos de capa MAC	Terminación del tráfico 802.11 en una iterfaz cableada

Operación CAPWAP

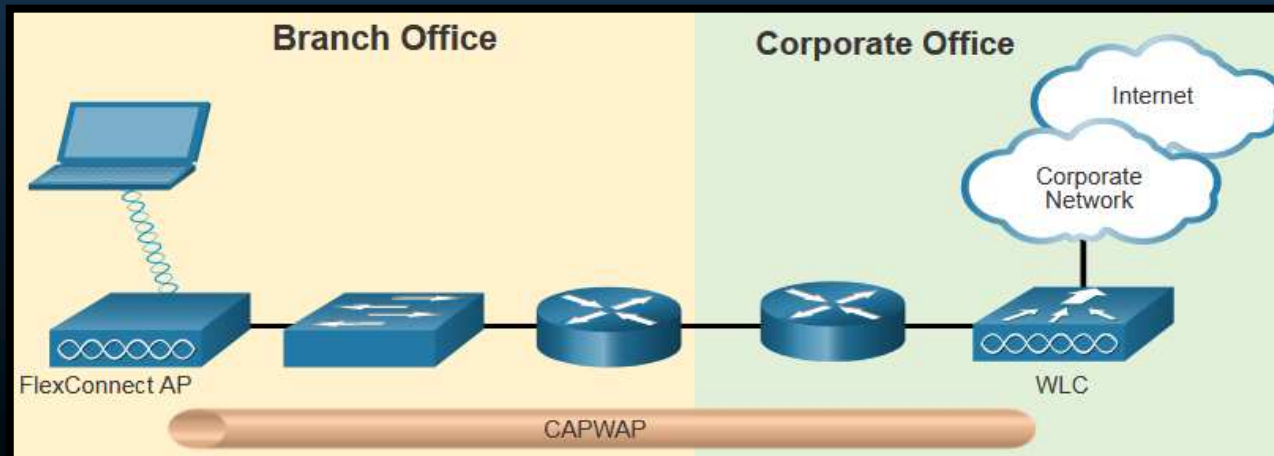
- Cifrado DTLS.
 - DTLS: Protocolo que brinda seguridad entre AP y WLC.
 - Habilitado por defecto para asegurar canales de administración y control CAPWAP.
 - Previene ataques MITM.
 - Deshabilitado por defecto para canales de datos.
 - Cifrado opcional .
 - Se habilita por AP.
 - Requiere licencias en el WLC.



Operación CAPWAP

- Aps FlexConnect.

- Solución Inalámbrica para empresas matrices con sucursales.
- Permite configurar control de accesos inalámbricos en sucursales, desde la matriz, a través de un enlace WAN.
- Dos modos de operación:
 - Conectado: El WLC es alcanzable desde el AP via tuneles CAPWAP.
 - Solitario: El WLC no es alcanzable. El AP asume algunas funciones del WLC, cómo conmutación local de datos del cliente y autenticación local.



Administración de Canales

- Saturación de canales de frecuencia

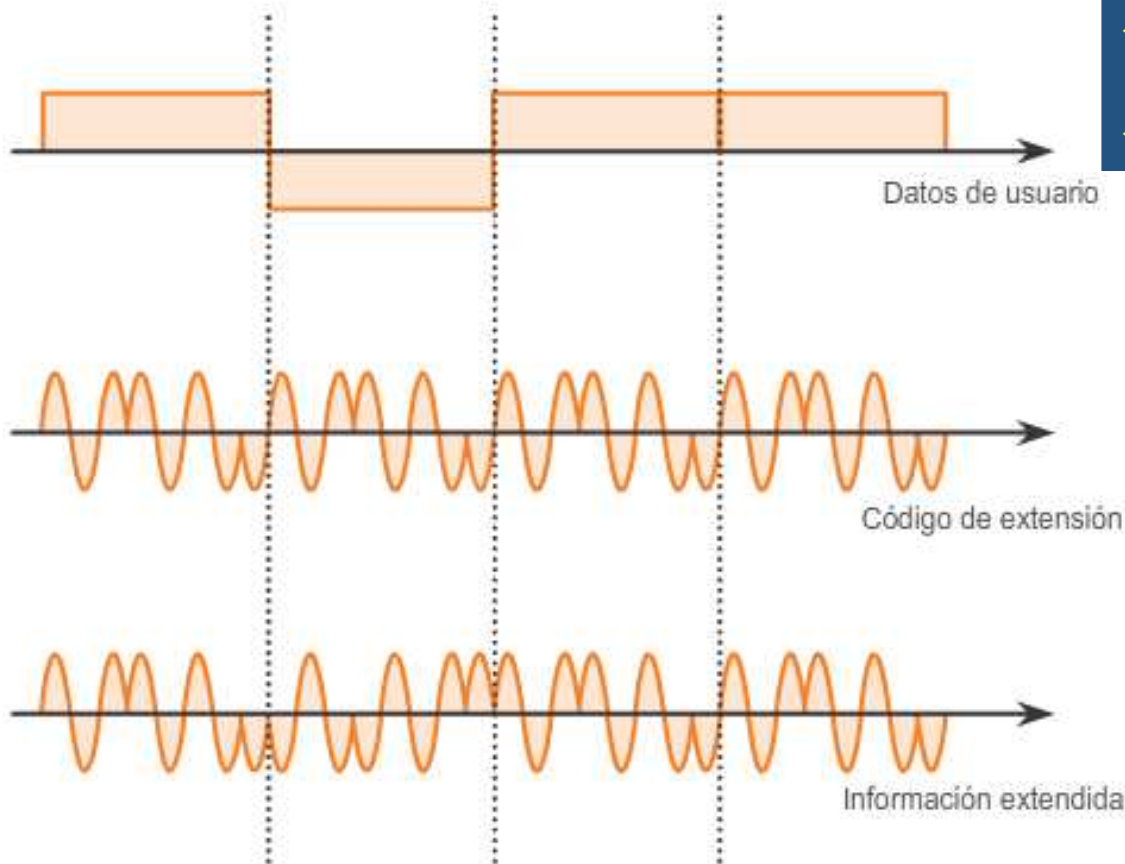
Es habitual asignar las frecuencias como rangos. Estos rangos después se dividen en rangos más pequeños denominados “canales”.

Si la demanda de un canal específico es demasiado alta, es probable que ese canal se sobresature. La saturación de un medio inalámbrico deteriora la calidad de la comunicación.

Administración de Canales

- Saturación de canales de frecuencia

Ejemplo de DSSS

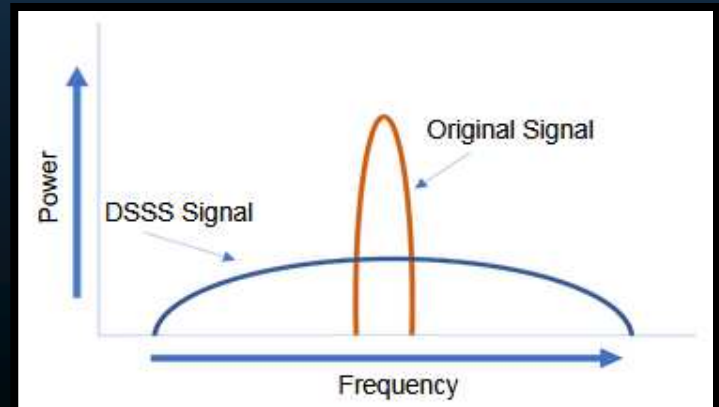


Usos:

- ✓ Teléfonos inalámbricos que operan en 900 MHz, 2,4 GHz y 5,8 GHz.
- ✓ Redes de telefonía móvil con CDMA.
- ✓ Redes GPS con CDMA.

Usa una **banda de frecuencia** resistente a la interferencia.

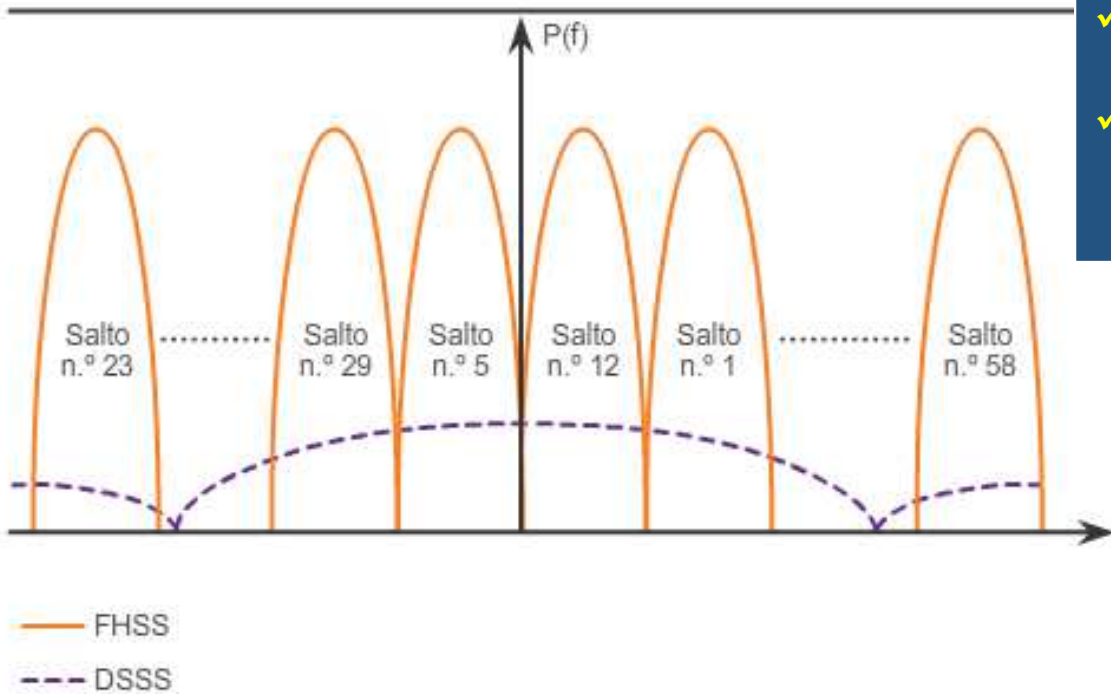
El "ruido fabricado" conocido como



Administración de Canales

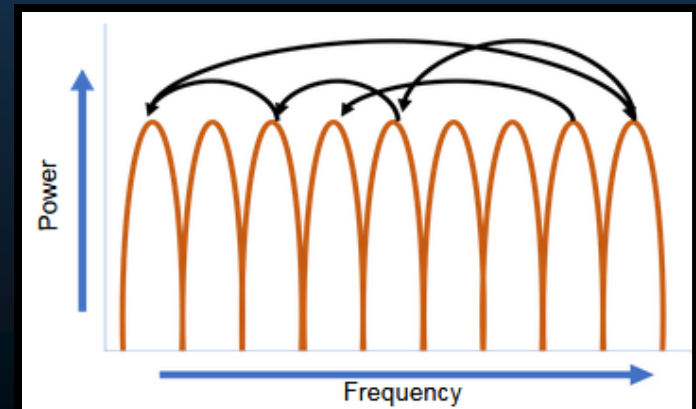
- Saturación de canales de frecuencia

Ejemplo de FHSS



Usos de FHSS:

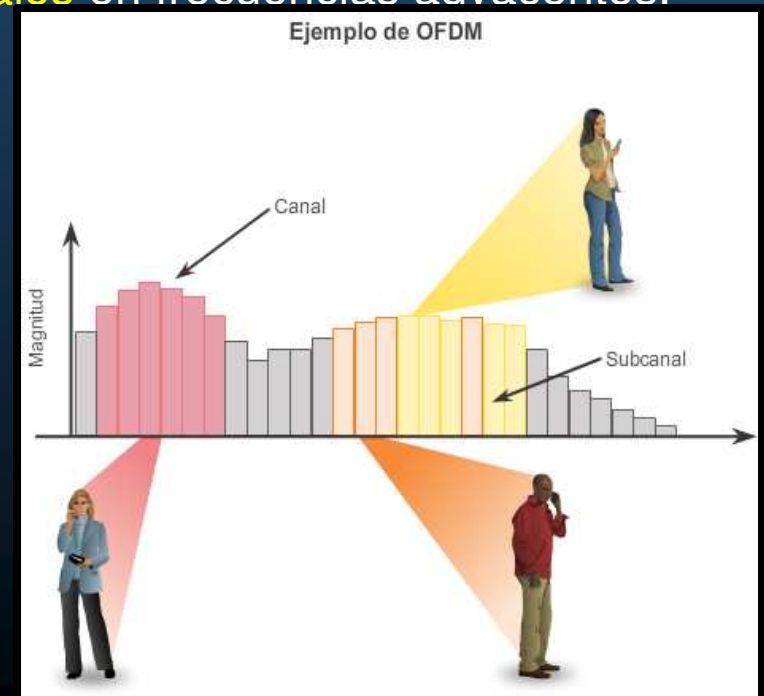
- ✓ Los walkie-talkies.
- ✓ Teléfonos inalámbricos de 900 MHz también usan FHSS.
- ✓ Bluetooth usa una variante de FHSS.
- ✓ El estándar 802.11 original también usa FHSS.



Administración de Canales

- Saturación de canales de frecuencia
 - Multiplexación por división de frecuencia ortogonal (OFDM):
 - Es un subconjunto de la **multiplexación** por división de frecuencia en el que **un único canal usa varios subcanales** en frecuencias adyacentes.
 - OFDM puede **maximizar la eficacia espectral** sin causar interferencia en los canales adyacentes.
 - OFDM usa **subcanales**.

Una serie de sistemas de comunicación, incluidos los estándares 802.11a/g/n/ac/ax, usa OFDM.



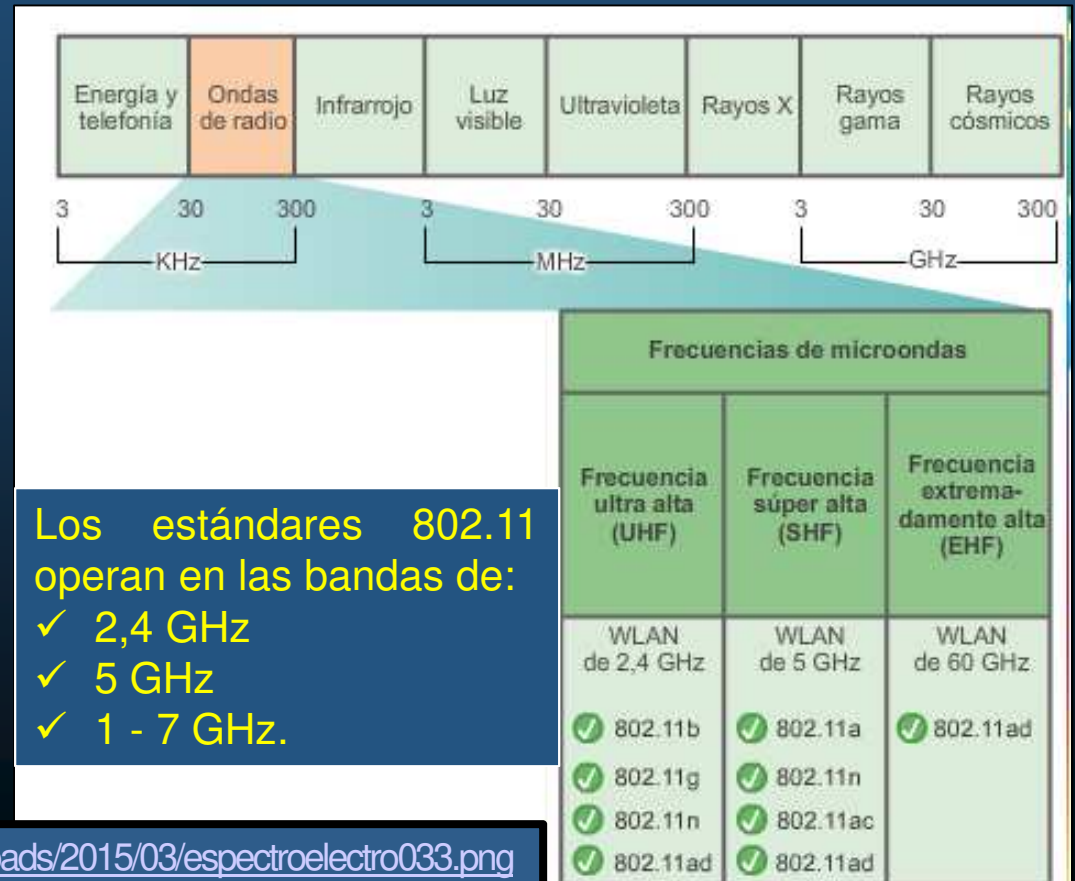
Administración de Canales

- Selección de canales

Los estándares IEEE 802.11b/g/n operan en las frecuencias de microondas del espectro de radio.

Los estándares IEEE 802.11b/g/n operan en el espectro de 2,4 GHz a 2,5 GHz.

Los estándares 802.11a/n/ac operan en la banda de 5 GHz, que está regulada en mayor medida.



Los estándares 802.11 operan en las bandas de:

- ✓ 2,4 GHz
- ✓ 5 GHz
- ✓ 1 - 7 GHz.

Administración de Canales

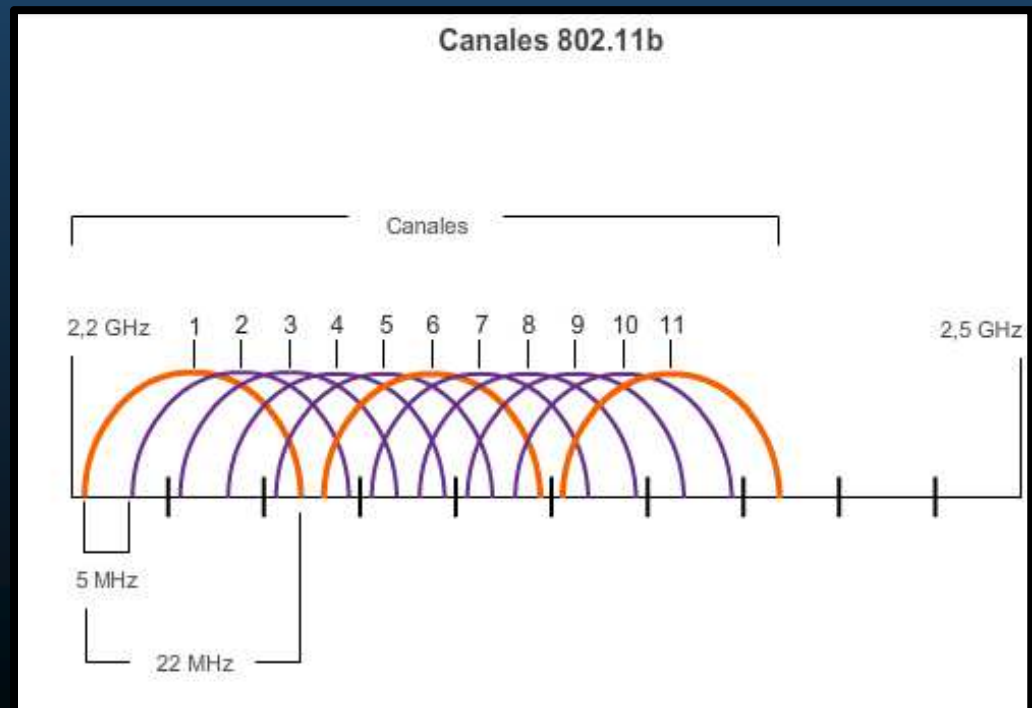
- Selección de canales

La banda de 2,4 GHz se subdivide en varios canales.

El ancho de banda general combinado es de 22 MHz, y cada canal está separado por 5 MHz.

El estándar 802.11b identifica 11 canales para América del Norte.

El ancho de banda de 22 MHz, en combinación con la separación de 5 MHz entre las frecuencias, produce una superposición entre los canales sucesivos.



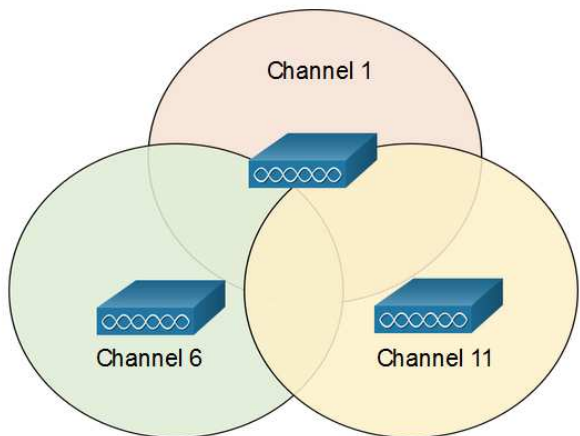
Administración de Canales

- Selección de canales

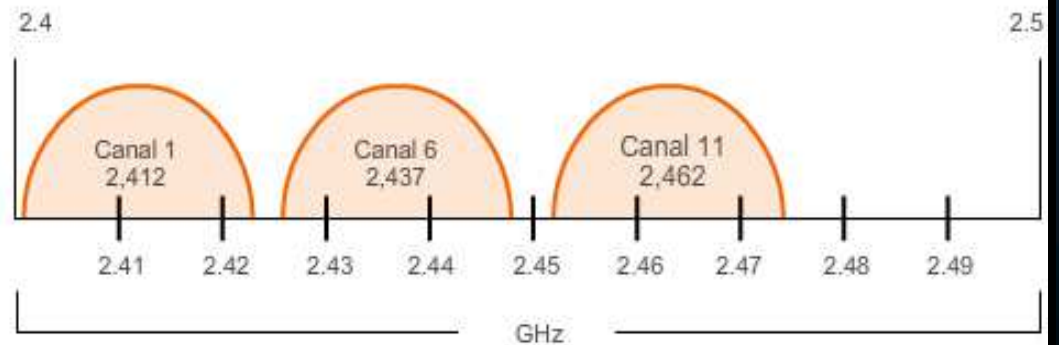
La **interferencia ocurre** cuando una **señal no deseada** se **superpone** a un canal reservado para una señal deseada, lo que causa una posible distorsión.

La **solución** a la interferencia es **usar canales** que no se **superpongan**.

Los canales 1, 6 y 11 son canales 802.11b no superpuestos.



Ancho de canal 802.11b (DSSS) de 22 MHz



Administración de Canales

- Selección de canales

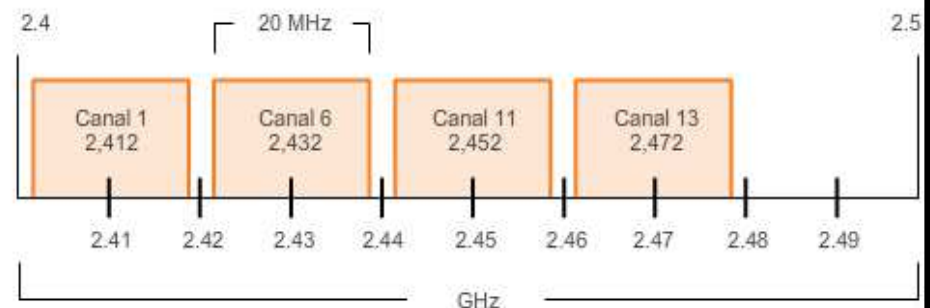
Para las **WLAN** que requieren varios **AP**, se recomienda usar **canales no superpuestos**. Si existen tres AP adyacentes, use los **canales 1, 6 y 11**.

Si **existen solo dos**, seleccione aquellos dos que estén separados por **cinco canales**, como los canales **5 y 10**.

A medida que las WLAN empresariales migran a **802.11n**, pueden usar canales en una banda de **5 GHz más grande** y **menos poblada**, lo que **reduce la “denegación de servicio (DoS) accidental”**.

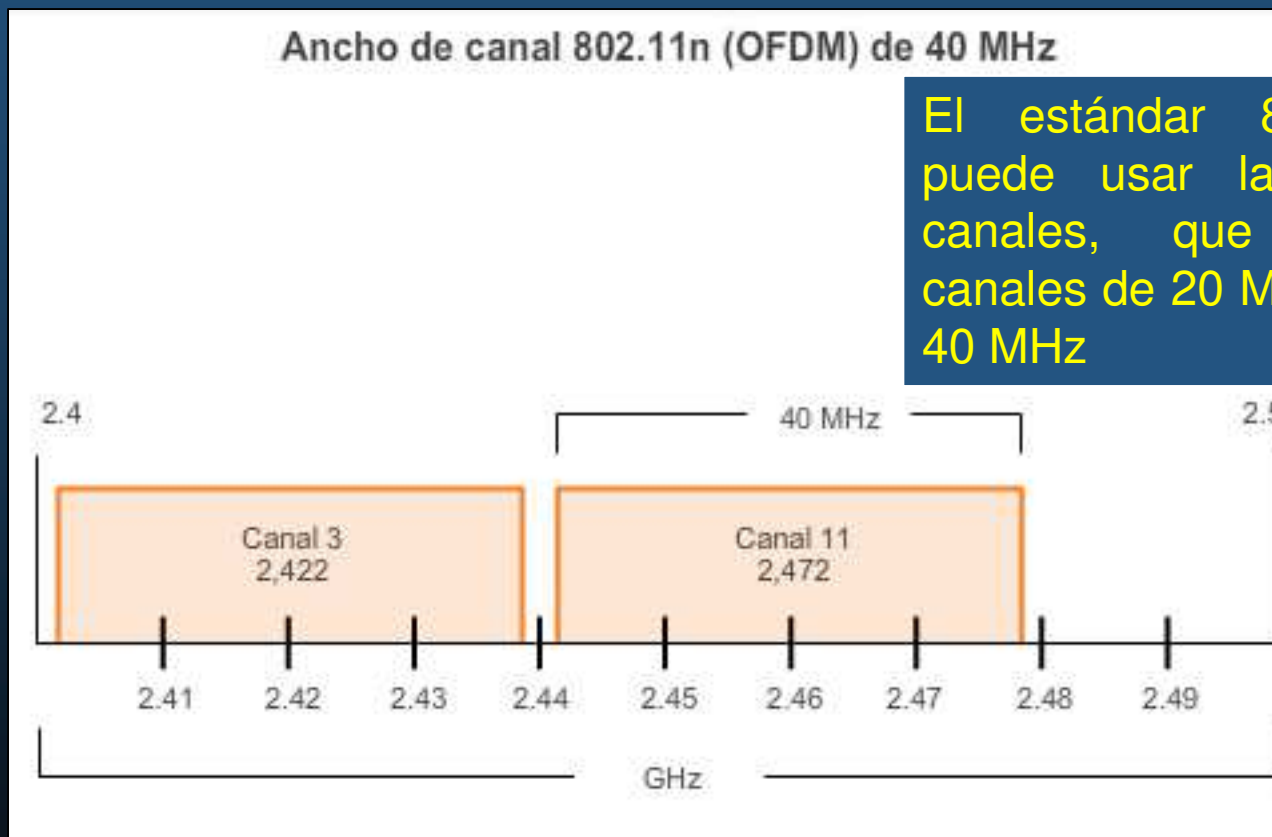
Ancho de canal 802.11g/n (OFDM) de 20 MHz

El estándar 802.11n usa OFDM y puede admitir cuatro canales no superpuestos.



Administración de Canales

- Selección de canales

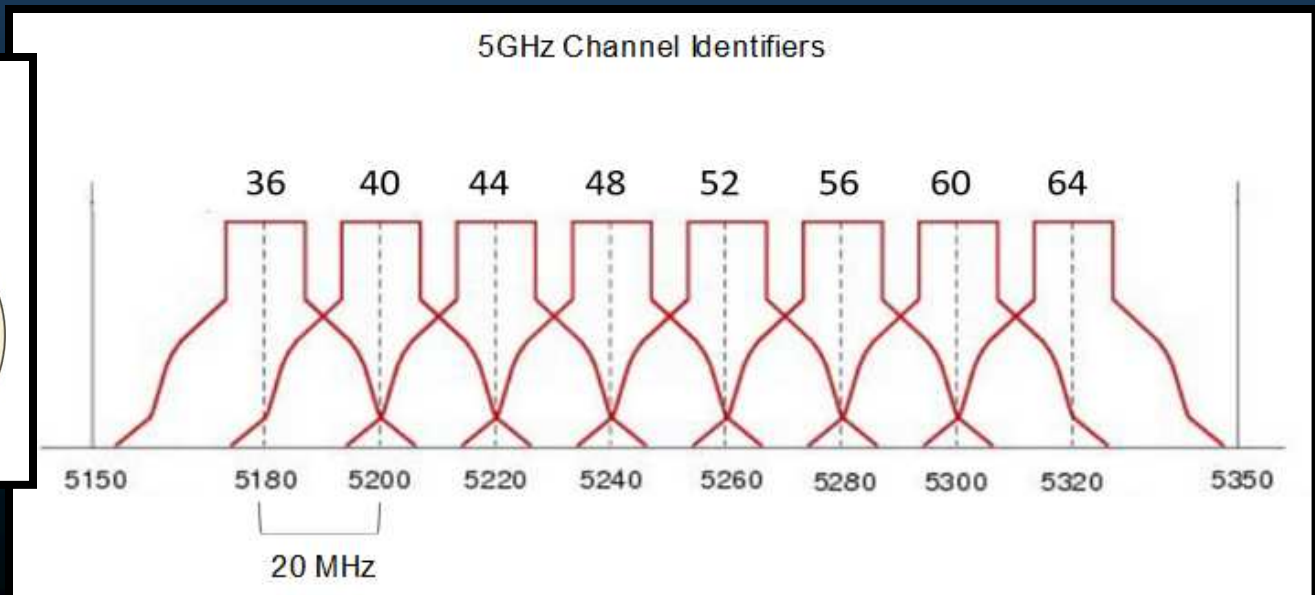
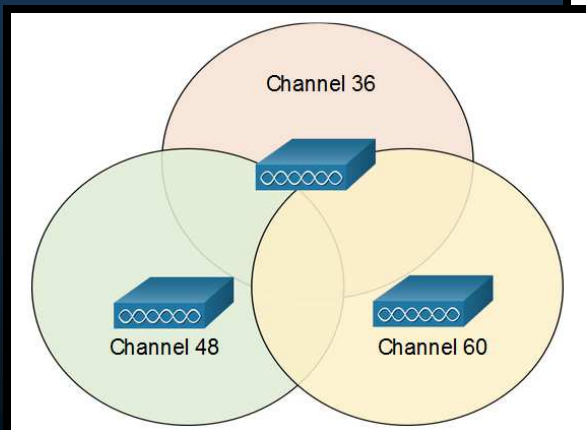


El estándar 802.11n también puede usar la vinculación de canales, que combina dos canales de 20 MHz en canales de 40 MHz

Administración de Canales

- Selección de Canales.

- Para los 5 GHz (802.11a / n / ac), hay 24 canales.
- La banda de 5 GHz se divide en tres secciones.
- Cada canal está separado del siguiente canal por 20 MHz.
- Aunque hay una ligera superposición, los canales no interfieren entre sí.
- Puede proporcionar una transmisión de datos más rápida.
- Preferible elegir canales sin traslape.

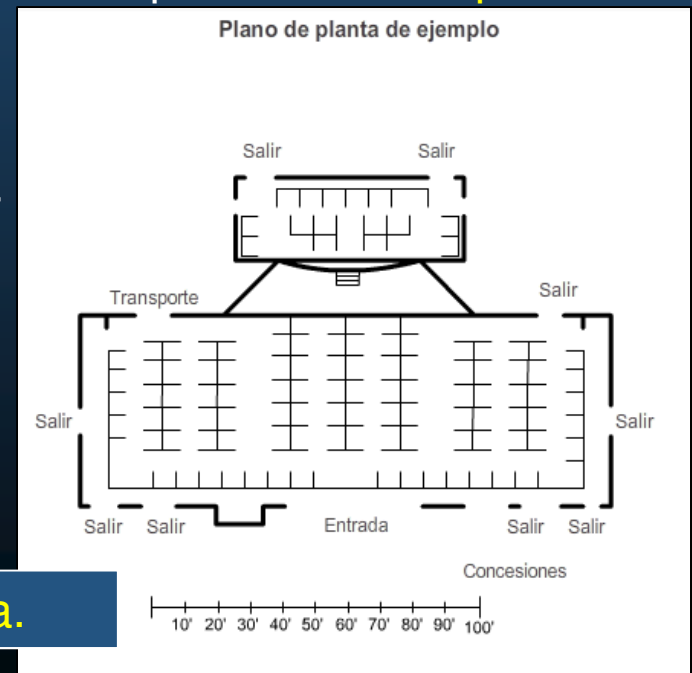


Administración de Canales

- Planificación de una implementación de WLAN

Las WLAN pueden abarcar desde instalaciones relativamente simples a diseños intrincados y muy complejos.

El número de usuarios que una WLAN puede admitir depende de la disposición geográfica de la instalación, incluidos el número de personas y dispositivos que pueden caber en un espacio, las velocidades de datos que esperan los usuarios, el uso de canales no superpuestos por parte de varios AP en un ESS y la configuración de energía de transmisión.



Plano de Ejemplo: Planta Baja.

Administración de Canales

- Planificación de una implementación de WLAN

El **área de cobertura circular** aproximada es importante, pero existen algunas recomendaciones adicionales:

- Si los **AP** deben usar un **cableado** existente **señale** estas ubicaciones **en el mapa**.
- **Posicione** los **AP** por encima de las **obstrucciones**.
- Posicione los **AP** **en forma vertical**, en el centro de cada área de cobertura.
- Coloque los **AP** en las **ubicaciones** en las que se espera **que estén** los **usuarios**.

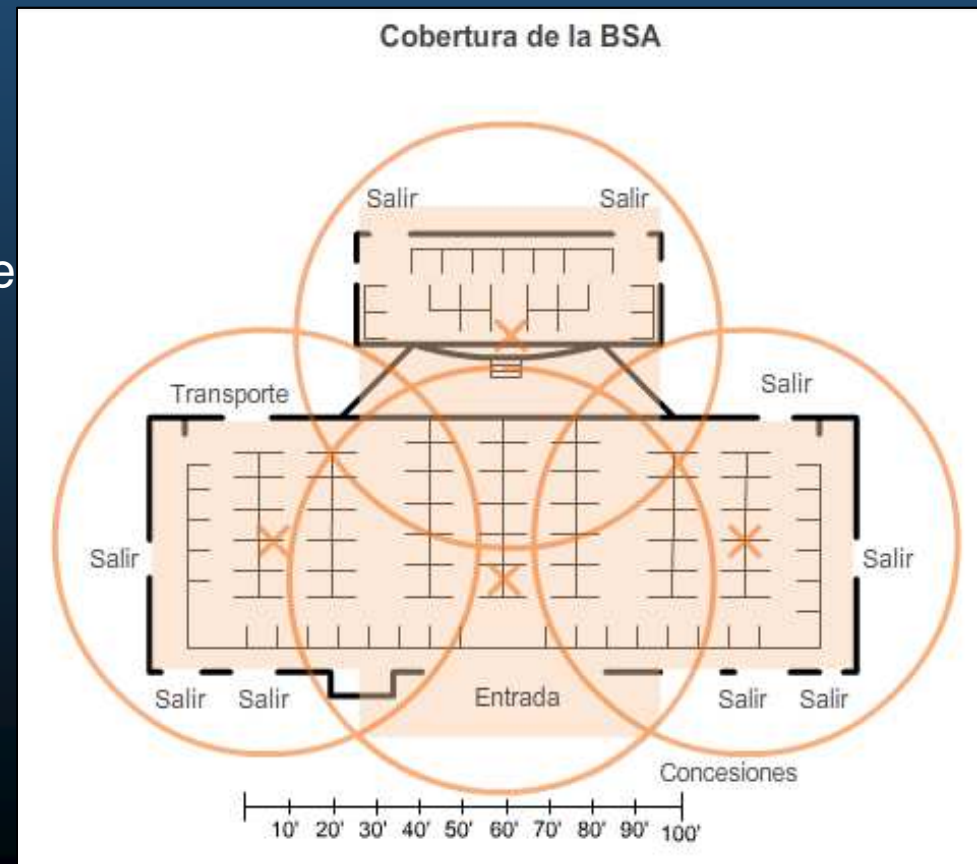
Administración de Canales

- Planificación de una implementación de WLAN

Las **BSA** representan el **área de cobertura** proporcionada por **un único canal**.

En un **ESS**, debe haber una superposición del **10 % al 15 %** entre las **BSA**.

Con una **superposición del 15 %** entre las **BSA**, un **SSID** y **canales no superpuestos** (es decir, una celda en el canal 1 y la otra en el canal 6), **se puede crear capacidad móvil**.



Amenazas en WLANs

- Seguridad de una LAN inalámbrica.
 - Amenazas inalámbricas comunes.



Ataques por denegación de servicio

Los servicios de las WLAN se pueden ver comprometidos accidentalmente o debido a intentos malintencionados. Existen varias soluciones según el origen del DoS.

Amenazas en WLANs

- **Ataque de DoS.**

- **Dispositivos mal configurados.**

Los errores de configuración pueden deshabilitar la WLAN.

- Un **usuario malintencionado interfiere** en la comunicación inalámbrica intencionalmente.

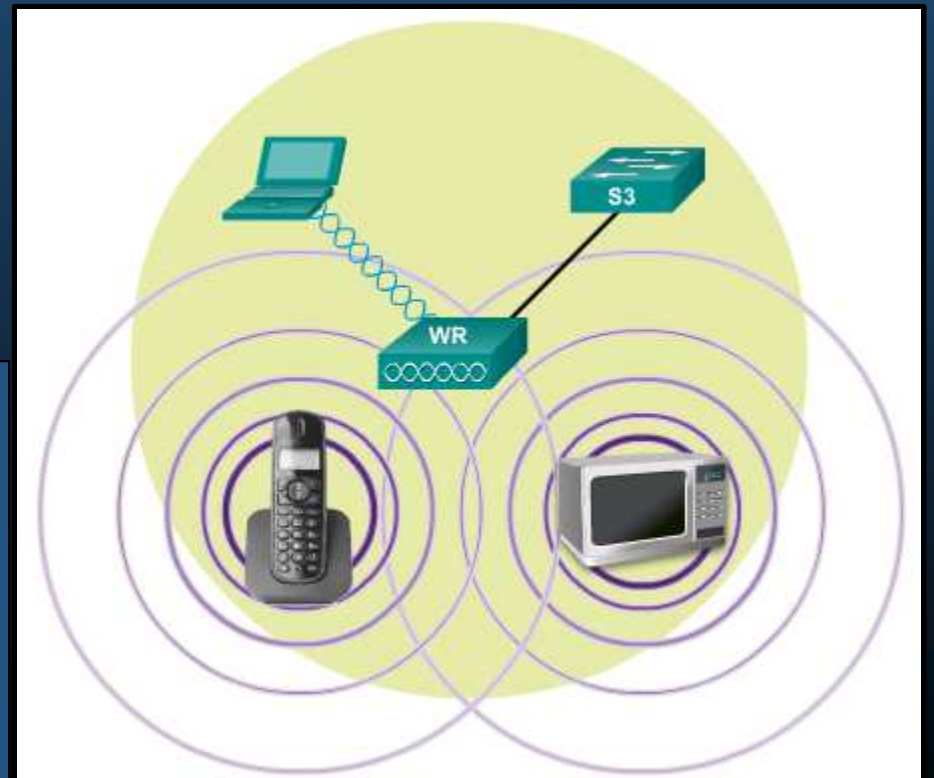
Deshabilita la red inalámbrica por completo o a tal punto que ningún dispositivo legítimo pueda acceder al medio.

- **Interferencia accidental.**

Las WLAN operan en las bandas de frecuencia sin licencia.

La banda de 2.4 GHz es más proclive a la interferencia que la banda de 5 GHz.

Solo ocurre cuando se agrega otro dispositivo inalámbrico.



Amenazas en WLANs

- Ataques DoS a las Tramas de administración.
 - Se pueden manipular para crear varios tipos de ataque DoS.
 - Los dos tipos de ataques comunes incluyen lo siguiente:
 - Ataque de desconexión suplantada.

Un atacante envía una serie de comandos de “desasociación” a los clientes inalámbricos dentro de un BSS.

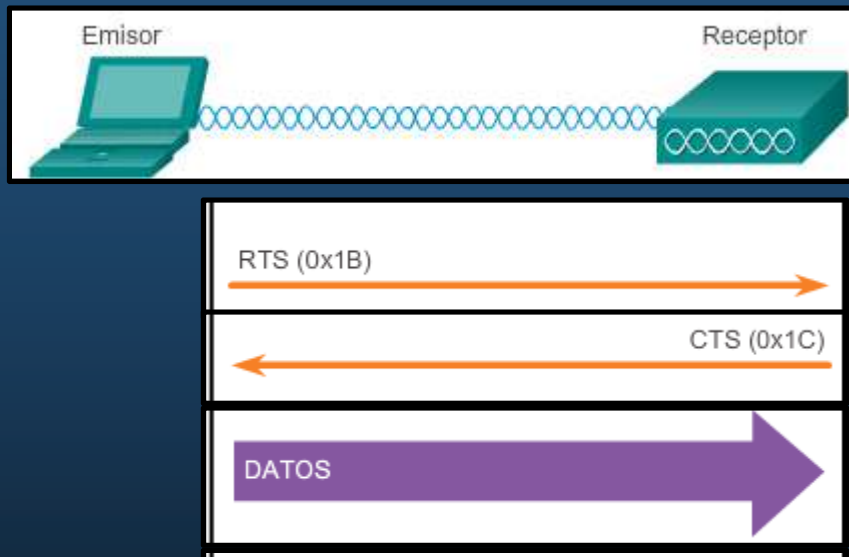
- Saturación con CTS.

Un atacante aprovecha el método de contienda CSMA/CA para monopolizar el ancho de banda y denegar el acceso de todos los demás clientes inalámbricos al AP.

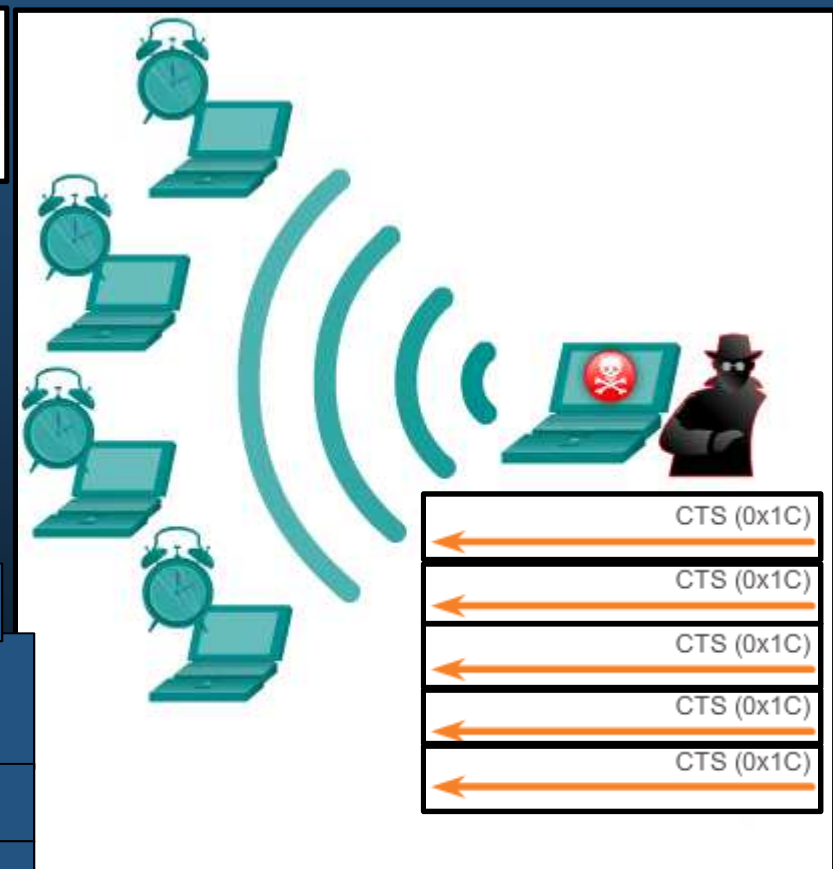
Amenazas en WLANs

- Ataques DoS a las Tramas de administración.

Funcionamiento normal con CSMA/CA



Ataque DoS de saturación con CTS.



Soluciones Cisco para Mitigar Ataques DoS.

Protección de tramas de administración (MFP).

Cisco Adaptive Wireless IPS.

Estándar 802.11i basado en MFP y 802.11w (para manipulación de tramas).

Amenazas en WLANs

- **Aps No Autorizados** = AP o router inalámbrico que:
 - Se **conectó** a una **red** empresarial **sin autorización** explícita o **en contra** de la política de la empresa.
 - Un **atacante** lo **conectó** o **habilitó** para **capturar datos** de clientes, como las direcciones MAC de los clientes (inalámbricos y cableados).

The screenshot shows the Cisco WLC configuration interface for Rogue Policies. The left sidebar shows the navigation tree with 'Rogue Policies' selected under 'Wireless Protection Policies'. The main content area is titled 'Rogue Policies' and includes the following settings:

- Rogue Detection Security Level:** Radio buttons for Low, High (selected), Critical, and Custom.
- Rogue Location Discovery Protocol:** MonitorModeAps (dropdown).
- Expiration Timeout for Rogue AP and Rogue Client entries:** 1200 Seconds.
- Validate rogue clients against AAA:** Enabled (checkbox).
- Validate rogue AP against AAA:** Enabled (checkbox).
- Polling Interval:** 0 Seconds.
- Validate rogue clients against MSE:** Enabled (checkbox).
- Detect and report Ad-Hoc Networks:** Enabled (checkbox).
- Rogue Detection Report Interval (10 to 300 Sec):** 30.
- Rogue Detection Minimum RSSI (-70 to -128):** -128.
- Rogue Detection Transient Interval (0, 120 to 1800 Sec):** 300.
- Rogue Client Threshold (0 to disable, 1 to 256):** 0.
- Rogue containment automatic rate selection:** Enabled (checkbox).

The **Auto Contain** section includes:

- Auto Containment Level:** Auto (dropdown).
- Auto Containment only for Monitor mode APs:** Enabled (checkbox).
- Auto Containment on FlexConnect Standalone:** Enabled (checkbox).
- Rogue on Wire:** Enabled (checkbox).
- Using our SSID:** Enabled (checkbox).
- Valid client on Rogue AP:** Enabled (checkbox).
- AdHoc Rogue AP:** Enabled (checkbox).

Un WLC puede implementar políticas contra Aps No Autorizados y combinar con un de monitorización.

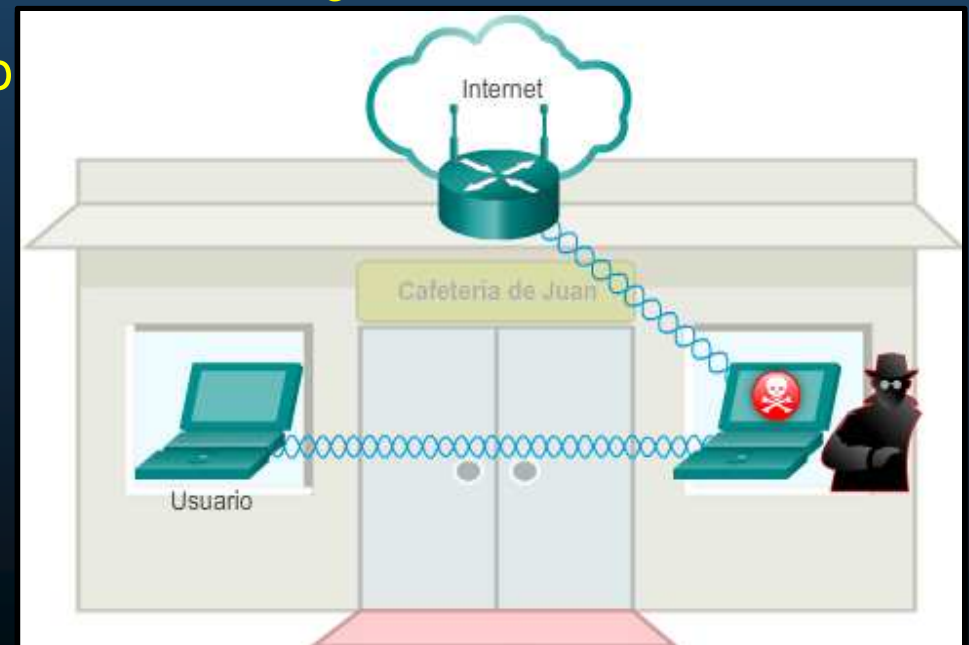
Amenazas en WLANs

- **Ataque Man-In-The-Middle (MITM)**

- Ataque **WMITM** común «Ataque con AP de red intrusa».
- Atacante **introduce AP no autorizado** con el mismo **SSID**.
 - Los **clientes detectan dos APs**.
 - Los **mas cercanos al intruso se asociarán a éste**.
 - El **AP intruso recibe los datos y los re-envía al AP legítimo**.

- Para las **WLAN** de empresas **Cisco** **proporciona** herramientas para administradores como un **sistema de prevención de intrusión inalámbrica (IPS)**.

- Estas herramientas incluyen **escáneres** que identifican las **redes ad hoc** y los **AP no autorizados**.
- Un **AP** que está más ocupado de lo normal **avisa** al administrador sobre posible **tráfico no autorizado**.



Seguridad en WLANs

- Encubrimiento SSID y filtrado de direcciones MAC
 - Ocultamiento de SSID.
 - Los AP y algunos routers inalámbricos permiten que se deshabilite la trama de señal del SSID.



Seguridad en WLANs

- Encubrimiento SSID y filtrado de direcciones MAC
 - Filtrado de direcciones MAC.
 - Un administrador puede permitir o denegar el acceso inalámbrico a los clientes de forma manual según la dirección MAC del hardware físico.

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

Wireless Tri-Band Home Router HomeRouter-PT-AC

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Guest Network Wireless MAC Filter Advanced Wireless Settings

Wireless MAC Filter

Wireless Port: 2.4G

Enabled Disabled

Prevent PCs listed below from accessing the wireless network

Permit PCs listed below to access wireless network

Wireless Client List

MAC 01:	00:D0:97:39:06:A6	MAC 26:	00:00:00:00:00:00
MAC 02:	00:E0:A3:7A:26:2B	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00

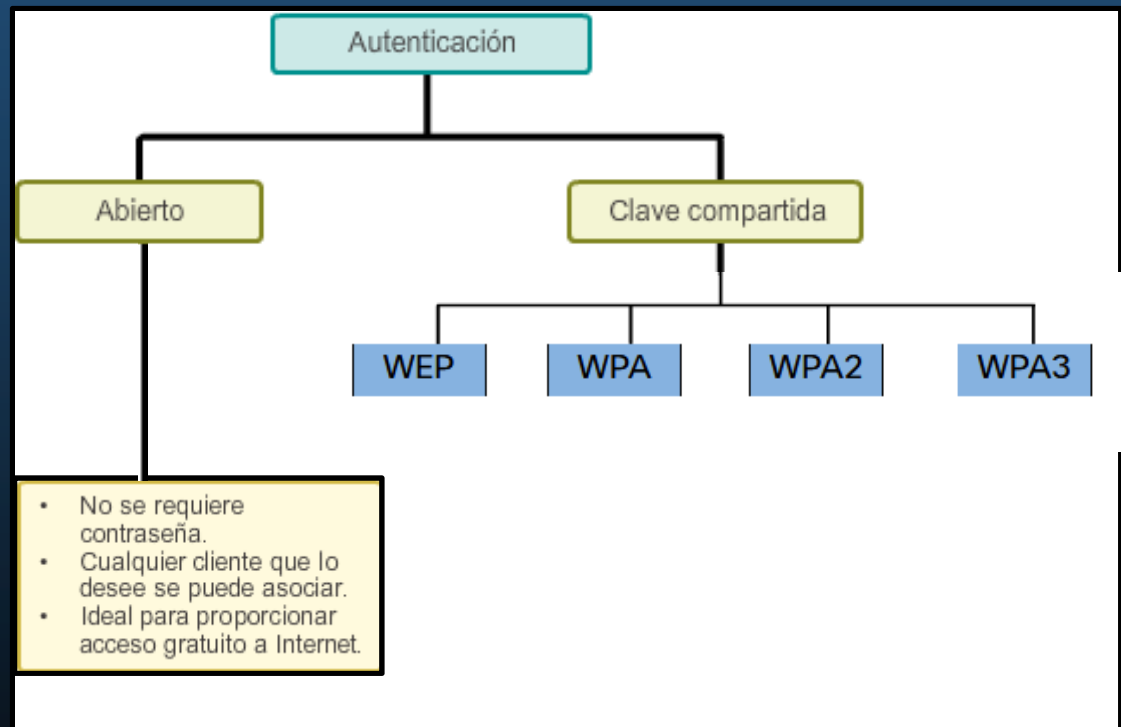
Access Resolution

MAC Address filter list

Help...

Seguridad en WLANs

- Sistemas de autenticación y cifrado (802.11 original).
 - Autenticación de sistema abierto.
 - Autenticación mediante clave compartida.



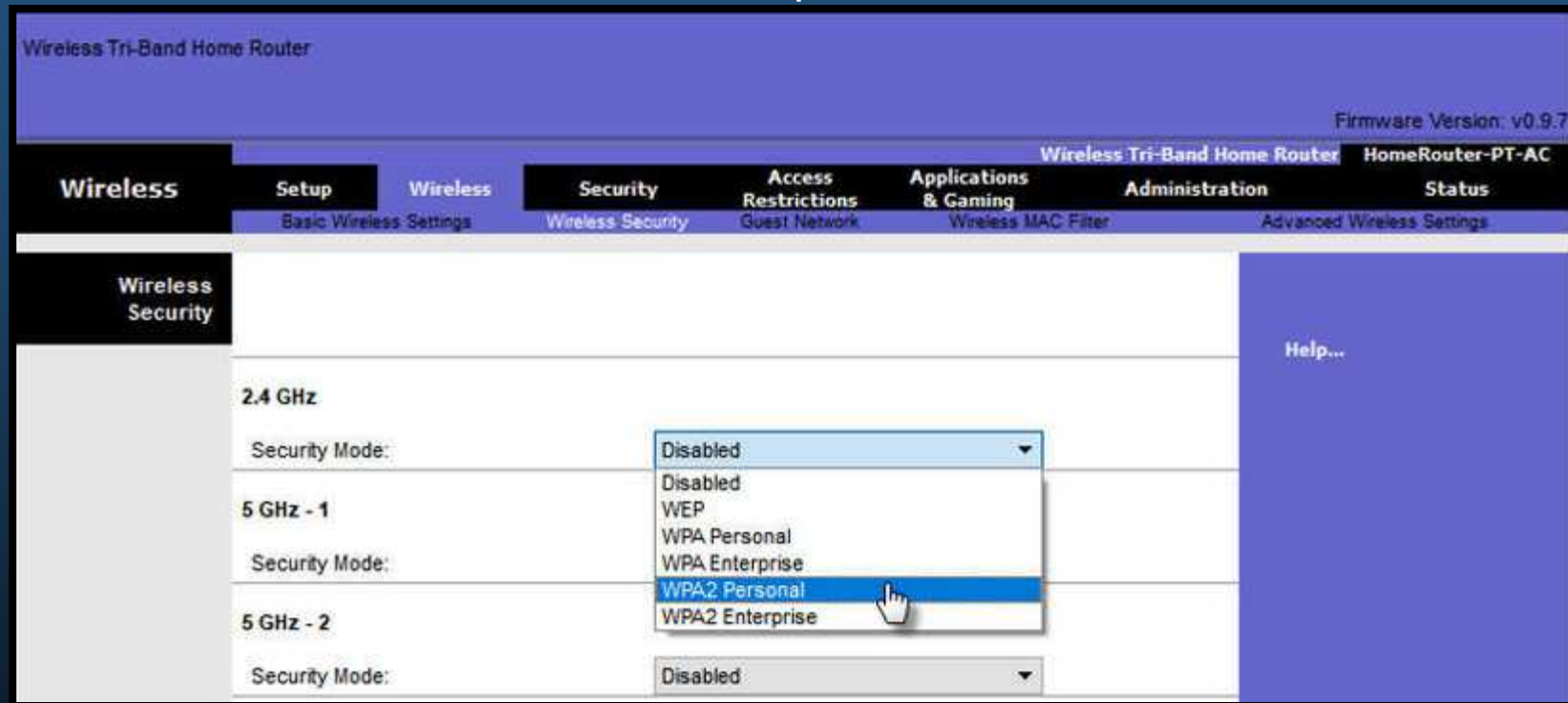
Seguridad en WLANs

- **Métodos de Autenticación Mediante Clave Compartida**
 - Existen **cuatro técnicas de autenticación mediante clave compartida.**

Método de Autenticación	Descripción
Privacidad equivalente por cable (WEP)	Especificación 802.11 original, diseñada para proteger datos utilizando cifrado Rivest Cipher 4 (RC4) con una clave estática que nunca cambia al intercambiar paquetes. Fácil de hackear. No se recomienda y no debe usarse.
Acceso protegido a Wi-Fi (WPA)	Estándar de Wi-Fi Alliance. Usa WEP, pero asegura los datos con cifrado del Protocolo de integridad de clave temporal (TKIP). Cambia la clave para cada paquete. Difícil de hackear.
WPA2	Estándar actual para proteger redes inalámbricas. Utiliza Estándar de cifrado avanzado (AES). El mejor protocolo de cifrado actual.
WPA3	Próxima generación de seguridad Wi-Fi. Utiliza los últimos métodos de seguridad, no permiten protocolos heredados obsoletos y requieren el uso de marcos de administración protegidos (PMF). Sin embargo, aún no están disponibles.

Seguridad en WLANs

- Autenticación de un Usuario en Casa.
 - Usualmente usan WPA / WPA2 para autenticarse.



- **Personal:** Uso de Llave Pre-Compartida (PSK)
- **Enterprise:** Uso de un servidor RADIUS mediante 802.1x, con el Protocolo de Autenticación Extensible (EAP)

Seguridad en WLANs

- Autenticación en la Empresa
 - El modo de seguridad “Enterprise” requiere un servidor RADIUS con autenticación, autorización y Administración de cuentas (AAA).
 - Dirección IP del servidor RADIUS.
 - Dirección del servidor RADIUS a la que se puede llegar.
 - Números de puerto UDP.
 - Asignados oficialmente 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS ò 1645 y 1646.
 - Clave compartida.
 - Autentica el AP con el servidor RADIUS.
 - No es un parámetro que se debe configurar en una STA. Solo se requiere en el AP para autenticar con el servidor RADIUS.
 - El proceso de inicio de sesión 802.1X usa EAP para comunicarse con el AP y el servidor RADIUS.

Seguridad en WLANs

- Autenticación en la Empresa

The image displays two overlapping screenshots of a wireless router's configuration interface. The top screenshot shows the 'Wireless Security' page for a 'Wireless Tri-Band Home Router' (Firmware Version: v0.9.7). The 'Wireless Security' section is expanded, showing settings for the 2.4 GHz network. The 'Security Mode' is set to 'WPA2/WPA Mixed Enterprise', and the 'Encryption' is set to 'TKIP'. The 'RADIUS Server' is set to '10', and the 'RADIUS Port' is set to '1812'. The 'Shared Secret' is set to 'cisco12345'. The 'Key Renewal' is set to '30'. The 5 GHz - 1 network is also visible, with 'Security Mode' set to 'WPA2/WPA Mixed Enterprise' and 'Encryption' set to 'TKIP'. The bottom screenshot shows the 'Wireless' configuration page for the same router. The '2.4 GHz network' is enabled, and the '5 GHz network' is also enabled. The '2.4 GHz network' settings are: Network: Enabled, Network name (SSID): Home-Net, RADIUS server: 10.10.10.10, RADIUS port: 1812, Shared key: cisco12345, Network mode: Mixed, Security mode: WPA2/WPA Mixed Enterprise, Channel width: Auto, and Channel: Auto. The '5 GHz network' settings are: Network: Enabled, Network name (SSID): Home-Net, Password: 666-6725, Network mode: Mixed, Security mode: WPA2/WPA Mixed Personal, Channel width: 80 MHz, and Channel: 103 - 5.755 GHz.

Seguridad en WLANs

- **WPA3**

- No disponible a la fecha de redacción del presente material.
- WPA2 ya no se considera seguro (Usar WPA3 cuando esté disponible).
- WPA3 tiene cuatro formas:
 - WPA3-Personal: Frustra ataques de “hand-shake” mediante Autenticación Simultánea Simultánea (SAE), especificada en IEEE 802.11-2016.
 - WPA3-Enterprise: Utiliza autenticación 802.1X / EAP de 192 bits y elimina la combinación de protocolos de seguridad para 802.11 anteriores. Se adhiere a la Suite de Algoritmos de Seguridad Nacional Comercial (CNSA) usado en redes Wi-Fi de alta seguridad.
 - Redes Abiertas: No utilizan ninguna autenticación. Utilizan el cifrado inalámbrico oportunista (OWE) para cifrar todo el tráfico inalámbrico.
 - Incorporación del Internet de las Cosas (IoT): WPA2 incluyó Configuración Protegida de Wi-Fi (WPS) para incorporar rápidamente dispositivos sin configuración. WPS es vulnerable (no se recomienda). Los dispositivos IoT no tienen GUI para configurarlos, y necesitan una forma fácil de conectarse. El Protocolo de Aprovisionamiento de Dispositivos (DPP) busca cubrir esta necesidad. Cada dispositivo tiene una clave pública codificada (QR estampado en el dispositivo). El administrador de red escanea el código QR y rápidamente conectar el dispositivo. Busca reemplazar a WPS con el tiempo.

Integración

- Verifique su comprensión de los conceptos de WLAN

Realice el quizz del capítulo 12
(opcional)

<https://contenthub.netacad.com/srwe/12.8.2>



Capítulo 13

Configuración de WLANs

<https://contenthub.netacad.com/srwe/13.1.1>

El Router Inalámbrico

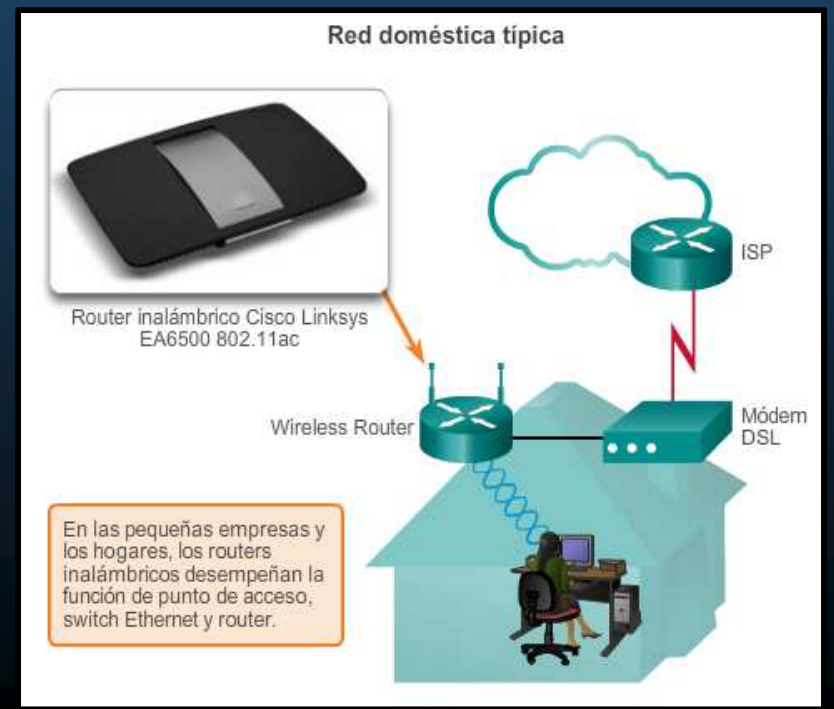
- Router doméstico (para trabajador a distancia) inalámbrico.

- Denominados **routers integrados**, son pequeños y cuentan con los siguientes componentes:
 - **Punto de acceso**: proporciona **acceso inalámbrico 802.11 a/b/g/n/ac (/ax)**.
 - **Switch**: proporciona un **switch Ethernet 10/100/1000, full-duplex**, de cuatro puertos para conectar dispositivos por cable.
 - **Router**: proporciona un **gateway** predeterminado para la conexión a otras infraestructuras de la red.



Características de routers Inalámbricos (varían dependiendo del modelo):

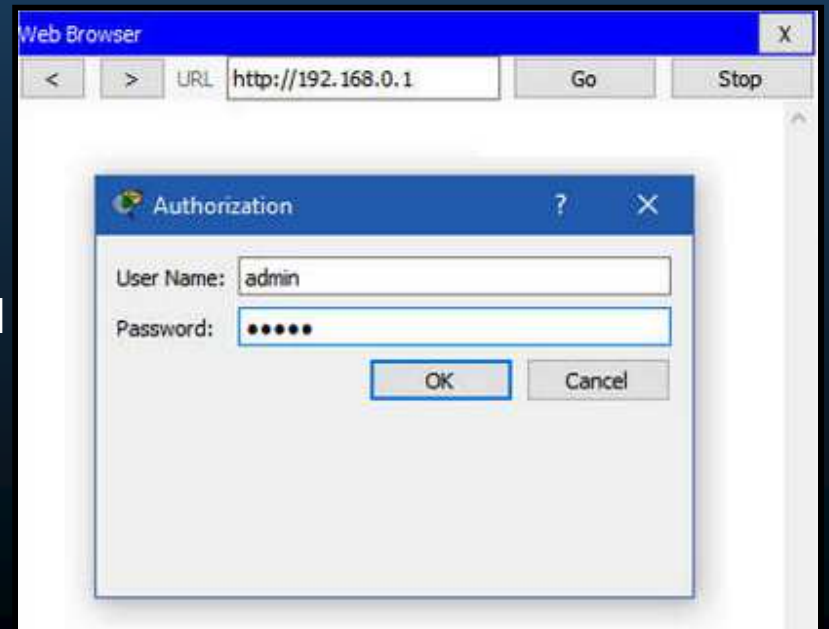
- ✓ Seguridad WLAN.
- ✓ Servicios DHCP.
- ✓ Traducción de Direcciones de Red (NAT)
- ✓ Compatibilidad con IPv6,
- ✓ Compatibilidad con QoS,
- ✓ Fácil configuración mediante Wi-Fi WPS.
- ✓ Puertos USB



El Router Inalámbrico

- Iniciar Sesión en el Router Inalámbrico.

- La mayoría vienen de fábrica, pre-configurados con algunos servicios cómo: acceso inalámbrico, DHCP, PAT, entre otros.
- Sus configuraciones por defecto (IP, usuario y contraseña), se encuentran disponibles en internet (Inseguras).
 - Nombre de usuario y contraseña en PacketTracer: admin/admin
 - Prioritario cambiarlas.
- Para acceder a su GUI de configuración:
 - Conectar un equipo a la LAN del router.
 - Abrir un navegador web.
 - Escribir la dirección IP del router inalámbrico.
 - Disponible en la documentación del dispositivo (varia según el modelo)
 - En P.T. 192.168.0.1
 - Escribir usuario y contraseña cuando se solicite.



El Router Inalámbrico

- Configuración de Red Básica.
 1. Iniciar sesión en el router inalámbrico.
 - Se abre una GUI con pestañas y menús para navegar la configuración y guardarla.

The screenshot displays the configuration interface for a Wireless Tri-Band Home Router. The browser address bar shows the URL `http://192.168.0.1/index.asp`. The page title is "Wireless Tri-Band Home Router" with a firmware version of v0.9.7. The navigation menu includes "Setup", "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Setup" section is expanded to show "Basic Setup".

Internet Setup

- Internet Connection type: Automatic Configuration - DHCP
- Optional Settings (required by some internet service providers):
 - Host Name: [text input]
 - Domain Name: [text input]
 - MTU: [dropdown] Size: 1500

Network Setup

- Router IP:
 - IP Address: 192 - 168 - 0 - 1
 - Subnet Mask: 255.255.255.0
- DHCP Server Settings:
 - DHCP Server: Enabled Disabled
 - DHCP Reservation: [button]
 - Start IP Address: 192.168.0. [text input: 100]
 - Maximum number of Users: [text input: 50]

El Router Inalámbrico

- Configuración de Red Básica.
 2. Cambiar datos de administración por defecto.
 - Varía en cada modelo.
 - En el ejemplo: Pestaña Administration > Management > Router Access
 - Solo admite cambiar contraseña.

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

Administration Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Management

Router Access

Router Password:

Re-enter to confirm:

Web Access

Web Utility Access: HTTP HTTPS

Web Utility Access via Wireless: Enabled Disabled

Remote Access

Remote Management: Enabled Disabled

Web Utility Access: HTTP

Remote Upgrade: Enabled

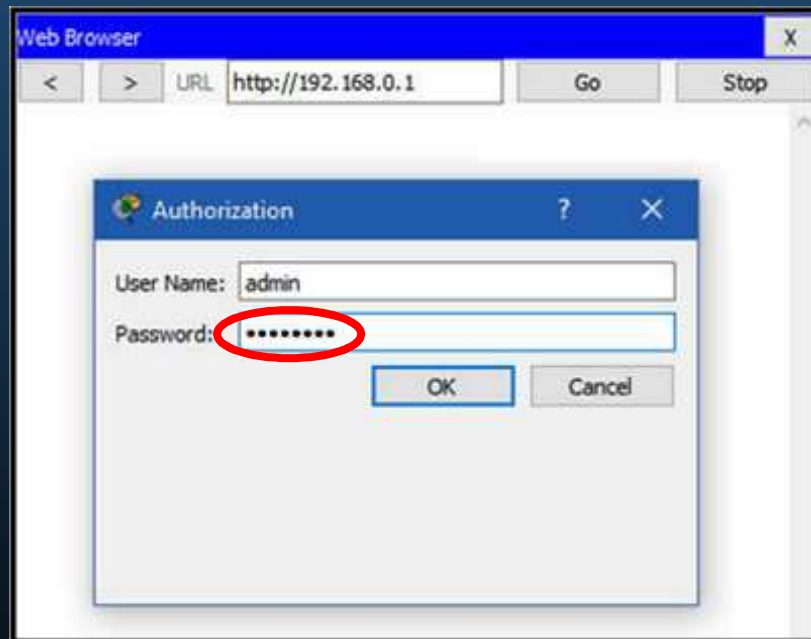
Tras cada cambio en la configuración, faltaría guardar los cambios, usualmente un botón "Save" al final de la página.

El Router Inalámbrico

- Configuración de Red Básica.

3. Iniciar sesión con las nuevas credenciales.

- Tras cambiar las credenciales de administración, se cierra sesión en la GUI.
- Necesario volver a Autenticarse



El Router Inalámbrico

- Configuración de Red Básica.
 4. Cambiar la dirección de red del DHCP.
 - Puede implementarse con cualquier direccionamiento privado.
 - Ajustar a las necesidades particulares (Ejemplo: 10.0.0.1)

The screenshot shows the configuration page for a Wireless Tri-Band Home Router. The browser address bar shows the URL `http://192.168.0.1/index.asp`. The page title is "Wireless Tri-Band Home Router" and the firmware version is "v0.9.7". The navigation menu includes "Setup" (highlighted with a red circle), "Wireless", "Security", "Access Restrictions", "Applications & Gaming", "Administration", and "Status". The "Internet Setup" section shows "Automatic Configuration - DHCP" selected. The "Network Setup" section (highlighted with a red rectangle) shows the "Router IP" settings: IP Address: 10.10.10.1 and Subnet Mask: 255.255.255.0. The "DHCP Server Settings" section shows "DHCP Server" set to "Enabled", "Start IP Address" set to 192.168.0.100, and "Maximum number of Users" set to 50. A "Help..." link is visible on the right side of the page.

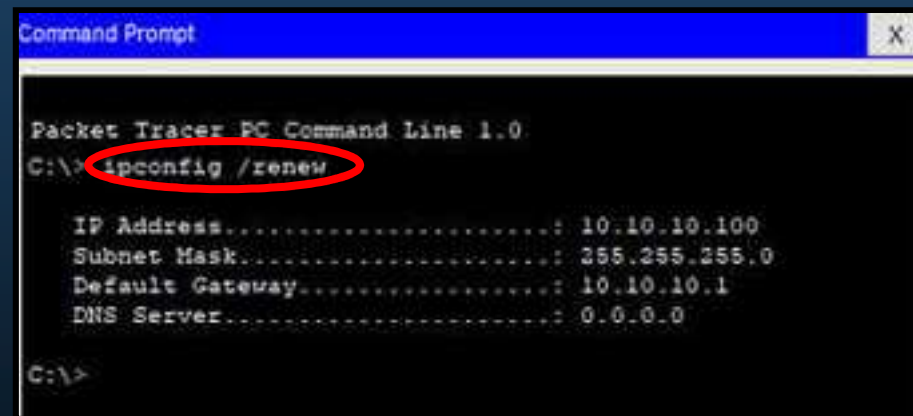
Faltaría guardar los cambios, usualmente un botón "Save" al final de la página.

El Router Inalámbrico

- Configuración de Red Básica.

- 5. Renovar la dirección IP.

- Una vez cambiada la IP del DHCP se perderá acceso a la GUI.
 - Necesario renovar la asociación con el cliente DHCP:
 - En Windows abrir una terminal cmd y utilizar `ipconfig /renew`.



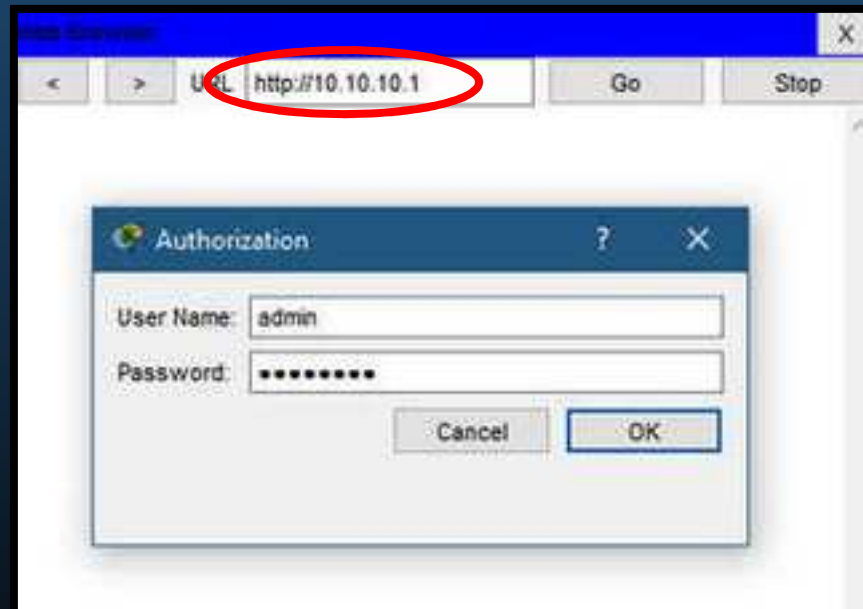
```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\> ipconfig /renew
IP Address. . . . . : 10.10.10.100
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . : 10.10.10.1
DNS Server. . . . . : 0.0.0.0
C:\>
```

El Router Inalámbrico

- Configuración de Red Básica.

6. Iniciar sesión con la nueva IP.

- Tras cambiar la IP del DHCP se perdió acceso a la GUI.
- Necesario volver a Autenticarse utilizando la nueva IP.



El Router Inalámbrico

- Configuración Inalámbrica Básica.

1. Verificar las configuraciones por defecto.

- Configuraciones inalámbricas por defecto: modo, nombre de red (SSID), canal, etc.
- Necesario ajustar a las necesidades particulares.

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

HomeRouter-PT-AC

Wireless Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings

2.4 GHz

Network Mode: Auto

Network Name (SSID): Default

SSID Broadcast: Enabled Disabled

Standard Channel: 1-2.412GHz

Channel Bandwidth: Auto

5 GHz - 2

Network Mode: Auto

Network Name (SSID): Default

SSID Broadcast: Enabled Disabled

Standard Channel: Auto

Channel Bandwidth: Auto

El Router Inalámbrico

- Configuración Inalámbrica Básica.

2. Cambiar el modo de red.

- Algunos routers inalámbricos permiten **cambiar el estándar IEEE 802.11 a usar.**
- El ejemplo elige **Legacy**, para dar **compatibilidad a todos los estándares soportados.**

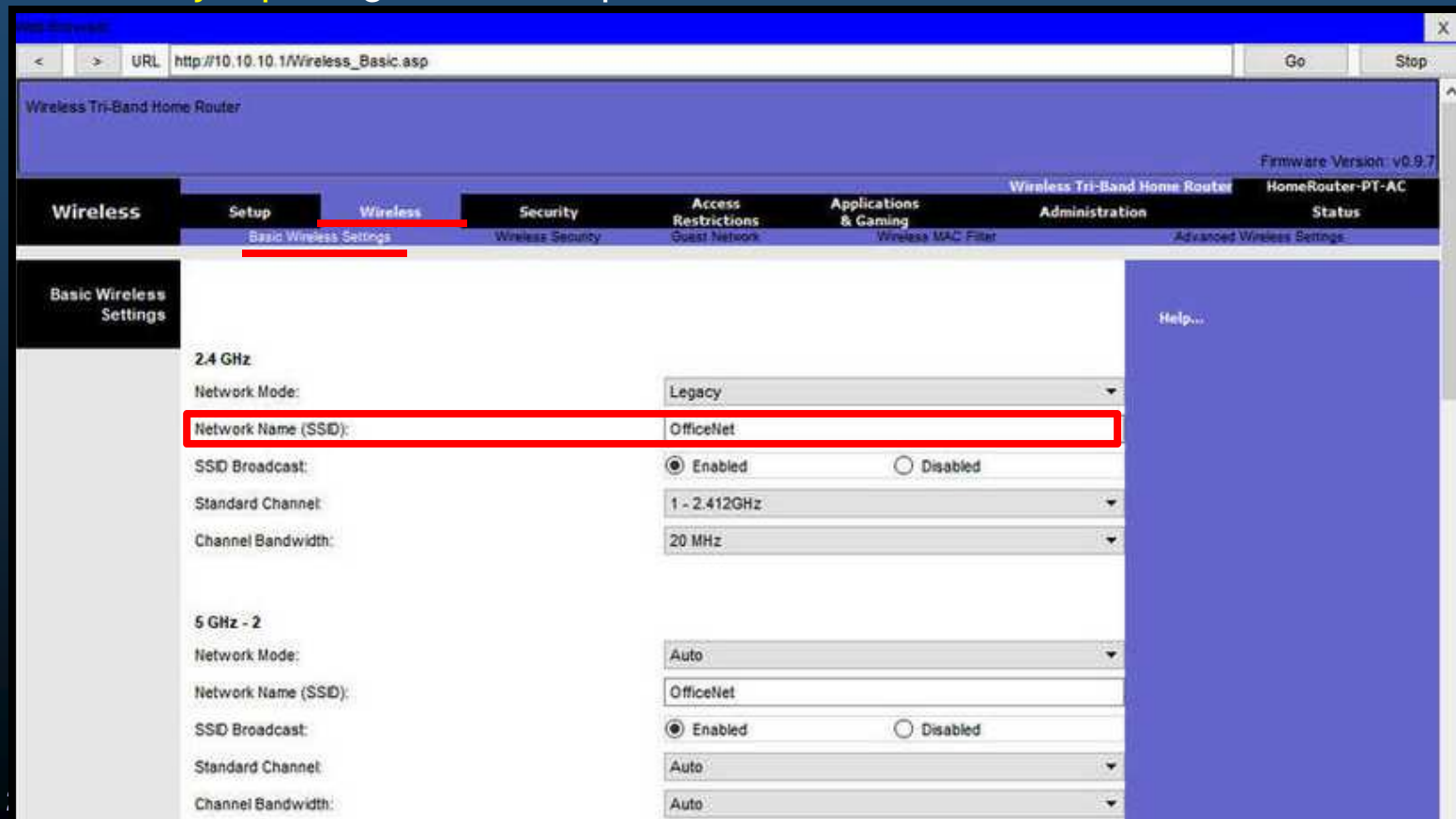
The screenshot shows the configuration interface for a 'Wireless Tri-Band Home Router'. The browser address bar displays 'http://10.10.10.1/Wireless_Basic.asp'. The page has a navigation menu with tabs for 'Wireless', 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. Under the 'Wireless' tab, there are sub-tabs: 'Basic Wireless Settings', 'Wireless Security', 'Guest Network', and 'Wireless MAC Filter'. The 'Basic Wireless Settings' section is highlighted with a red box. It contains settings for two frequency bands: 2.4 GHz and 5 GHz - 2. The 2.4 GHz section includes 'Network Mode' (set to 'Legacy'), 'Network Name (SSID)', 'SSID Broadcast', 'Standard Channel' (set to '1 - 2.412GHz'), and 'Channel Bandwidth' (set to 'Auto'). The 5 GHz - 2 section includes 'Network Mode' (set to 'Auto'), 'Network Name (SSID)' (set to 'Default'), 'SSID Broadcast' (with 'Enabled' selected), 'Standard Channel' (set to 'Auto'), and 'Channel Bandwidth' (set to 'Auto').

El Router Inalámbrico

- Configuración Inalámbrica Básica.

- 3. Configurar el SSID.

- Algunos routers inalámbricos utilizan **por defecto** la **marca del producto**.
 - El **ejemplo** elige **OfficeNet**, para identificar la red inalámbrica.



El Router Inalámbrico

- Configuración Inalámbrica Básica.

- 4. Configurar el canal.

- Por defecto los dispositivos tienen un canal configurado.
 - Traslapes en los canales inalámbricos pueden causar DoS.

The screenshot shows the configuration page for a Wireless Tri-Band Home Router. The page is titled "Basic Wireless Settings" and is divided into two sections: "2.4 GHz" and "5 GHz - 2". The "2.4 GHz" section is currently selected. The "Standard Channel" dropdown menu is open, showing a list of channels from 1 to 10. Channel 6 (2.437GHz) is highlighted. The "Channel Bandwidth" is set to "Auto". The "5 GHz - 2" section is also visible, with "Standard Channel" set to "Auto" and "Channel Bandwidth" set to "Auto".

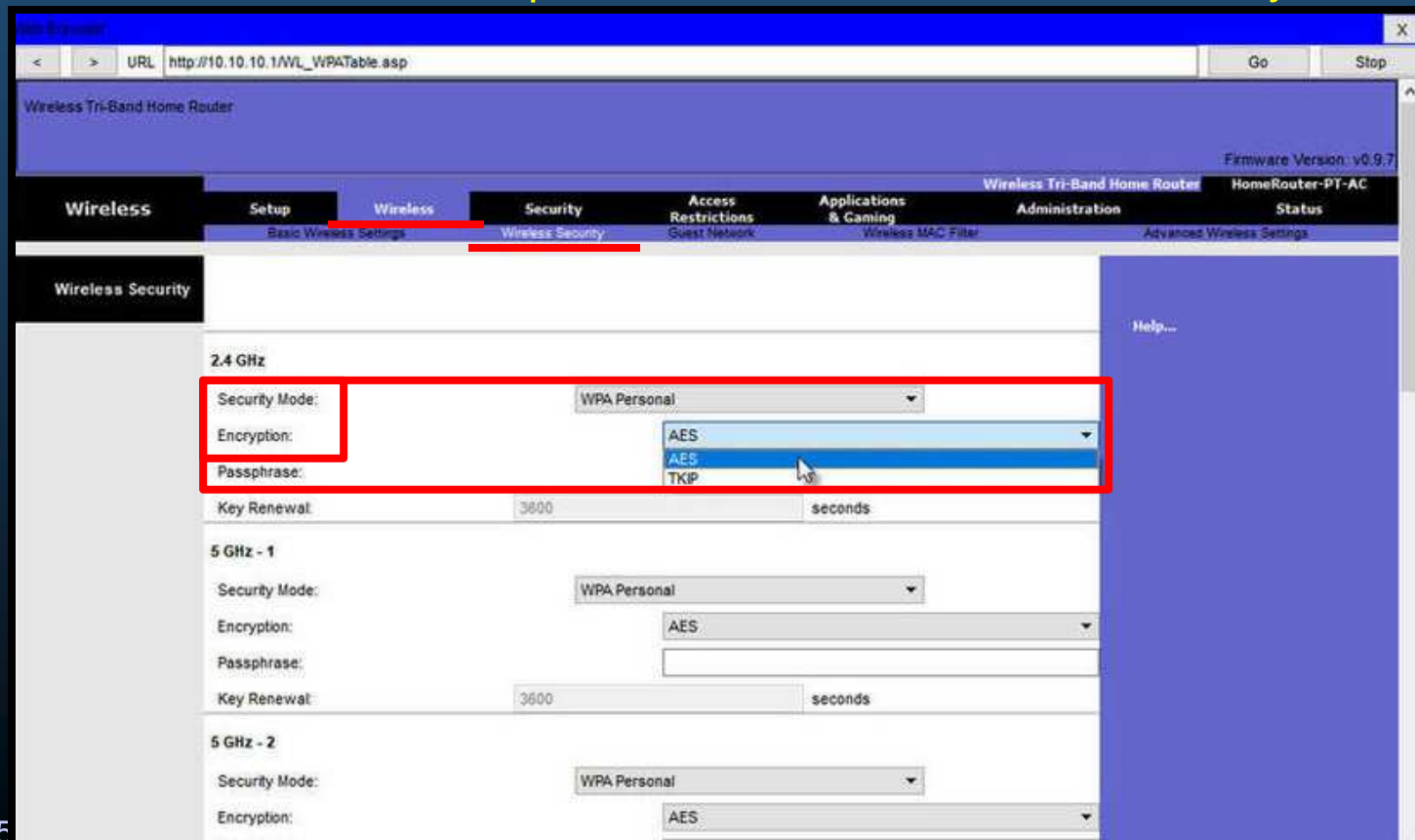
Channel	Frequency
1	2.412GHz
2	2.417GHz
3	2.422GHz
4	2.427GHz
5	2.432GHz
6	2.437GHz
7	2.442GHz
8	2.447GHz
9	2.452GHz
10	2.457GHz

El Router Inalámbrico

- Configuración Inalámbrica Básica.

- 5. Configurar el modo de seguridad.

- Puede tener alguna configuración por defecto.
 - Mientras no esté disponible WPA3 se debería utilizar WPA2 y AES.



El Router Inalámbrico

- Configuración Inalámbrica Básica.

- 6. Configurar la frase de paso.

- Usadas por WPA2 para entornos pequeños sin necesidad de un servidor.
 - Empresas grandes deberían utilizar un servidor de autenticación.

The screenshot shows the configuration page for a Wireless Tri-Band Home Router. The page is titled "Wireless Security" and displays settings for three wireless bands: 2.4 GHz, 5 GHz - 1, and 5 GHz - 2. Each band has a "Security Mode" dropdown set to "WPA Personal" and an "Encryption" dropdown set to "AES". The "Passphrase" field for each band is set to "cisco123". The "Key Renewal" field is set to "3600 seconds". The "Passphrase" field for the 2.4 GHz band is highlighted with a red box.

El Router Inalámbrico

- Configurar una Red en Malla Inalámbrica (WMN).
 - Para cubrir áreas de mas de 45m en interiores o 90m en exteriores, se pueden agregar APs en una topología de malla inalámbrica.

Mismas configuraciones, pero en diferente canal (sin traslape).

Algunos vendedores facilitan la configuración de WMNs mediante aplicaciones para dispositivos móviles.

El Router Inalámbrico

- **NAT para IPv4.**

- La pestaña **Status** muestra **información de direccionamiento** y configuración de **Internet** con el que se realiza NAT a la LAN privada (no enrutable en Internet), para poder salir a Internet.

Con NAT una red privada (local), traduce su direccionamiento por una IP pública (global). El proceso se revierte al regresar el tráfico.

Usualmente por defecto utiliza cliente DHCP.

The screenshot shows the web interface of a Wireless-N Broadband Router. The 'Status' tab is selected and circled in red. The interface displays the following information:

Router Information	Value
Firmware Version:	v0.93.3
Current Time:	Not Available
Internet MAC Address:	000D.BDA6.3001
Host Name:	
Domain Name:	

Internet Connection	Value
Connection Type:	Automatic Configuration - DHCP
Internet IP Address:	209.165.201.11
Subnet Mask:	255.255.255.0
Default Gateway:	209.165.201.1
DNS1:	64.100.0.100
DNS2:	
DNS3:	
MTU:	1500
DHCP Lease Time:	1 days 0:0:0

Buttons for 'IP Address Release' and 'IP Address Renew' are visible at the bottom of the Internet Connection section.

Puede re-configurarse manualmente en:
Setup > Internet Setup.
(ver diapositiva 4)

El Router Inalámbrico

- **Calidad en el Servicio.**

- Permite **garantizar** que ciertos tipos de tráfico tengan **mayor prioridad** que otros.
- Algunos routers permiten especificar prioridades por puertos específicos.
 - Usualmente en “Configuraciones Avanzadas” y/o “Bandwith Control”

Basic Advanced Cancel Apply

Advanced Home QoS Setup

#	Qos Policy	Priority	Description
1	IP Phone	High	IP Phone applications
2	Counter Strike	High	Online Gaming Counter Strike
3	Netflix	High	Online Video Streaming Netflix
4	FTP	Medium	FTP Applications
5	WWW	Medium	WWW Applications
6	Gnutella	Low	Gnutella Applications
7	SMTP	Medium	SMTP Applications

Edit Delete Delete All

Add Priority Role

El Router Inalámbrico

- **Re-envío de Puertos.**

- Un router Inalámbrico usualmente bloquea el tráfico TCP/UDP a la red interna, para prevenir accesos no autorizados.
- Si un puerto se requiere abierto, el reenvío de puertos puede permitirlo.
 - Cuando el tráfico alcanza el router, éste determina a quién debe re-enviar ese tráfico en base al puerto destino.

Wireless Tri-Band Home Router

Firmware Version: v0.9.7

Applications & Gaming | Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Single Port Forwarding

Internal Port	Protocol	To IP Address	Enabled	Help...	
---	---	10.10.10. 0	<input type="checkbox"/>		
---	---	10.10.10. 0	<input type="checkbox"/>		
---	---	10.10.10. 0	<input type="checkbox"/>		
---	---	10.10.10. 0	<input type="checkbox"/>		
---	---	10.10.10. 0	<input type="checkbox"/>		
---	---	10.10.10. 0	<input type="checkbox"/>		
Web Server	80	80	TCP	10.10.10. 50	<input type="checkbox"/>
---	0	0	Both	10.10.10. 0	<input type="checkbox"/>

Port Triggering, habilita nuevos re-envíos del tráfico generado a un nuevo puerto, derivados de una comunicación ya establecida (en otro puerto).

El ejemplo habilita el re-envío del tráfico HTTP que llegue al router, al host local 10.10.10.50

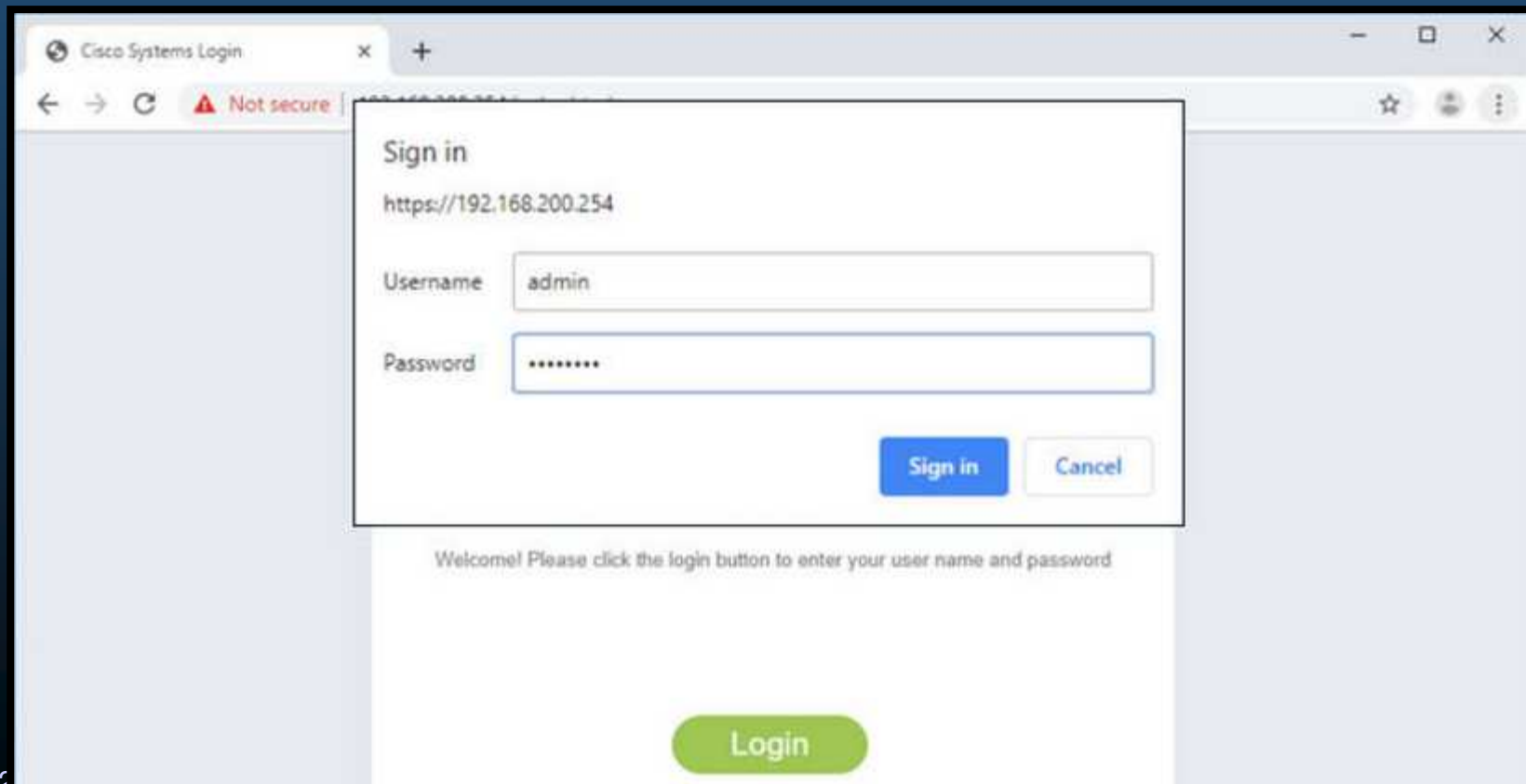
Configurar una WLAN Básica desde un WLC

- Topología para WLC.
 - AP1 es un AP basado en controlador ó ligero (no requiere configuración inicial).
 - Usará WLAPP para comunicarse con el WLC de quien recibirá configuraciones y administración.

Device	Interface	IP Address	Subnet Mask
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	DHCP	
WLC	Management	192.168.200.254	255.255.255.0
AP1	Wired 0	192.168.200.3	255.255.255.0
PC-A	NIC	172.16.1.254	255.255.255.0
PC-B	NIC	DHCP	
Wireless Laptop	NIC	DHCP	

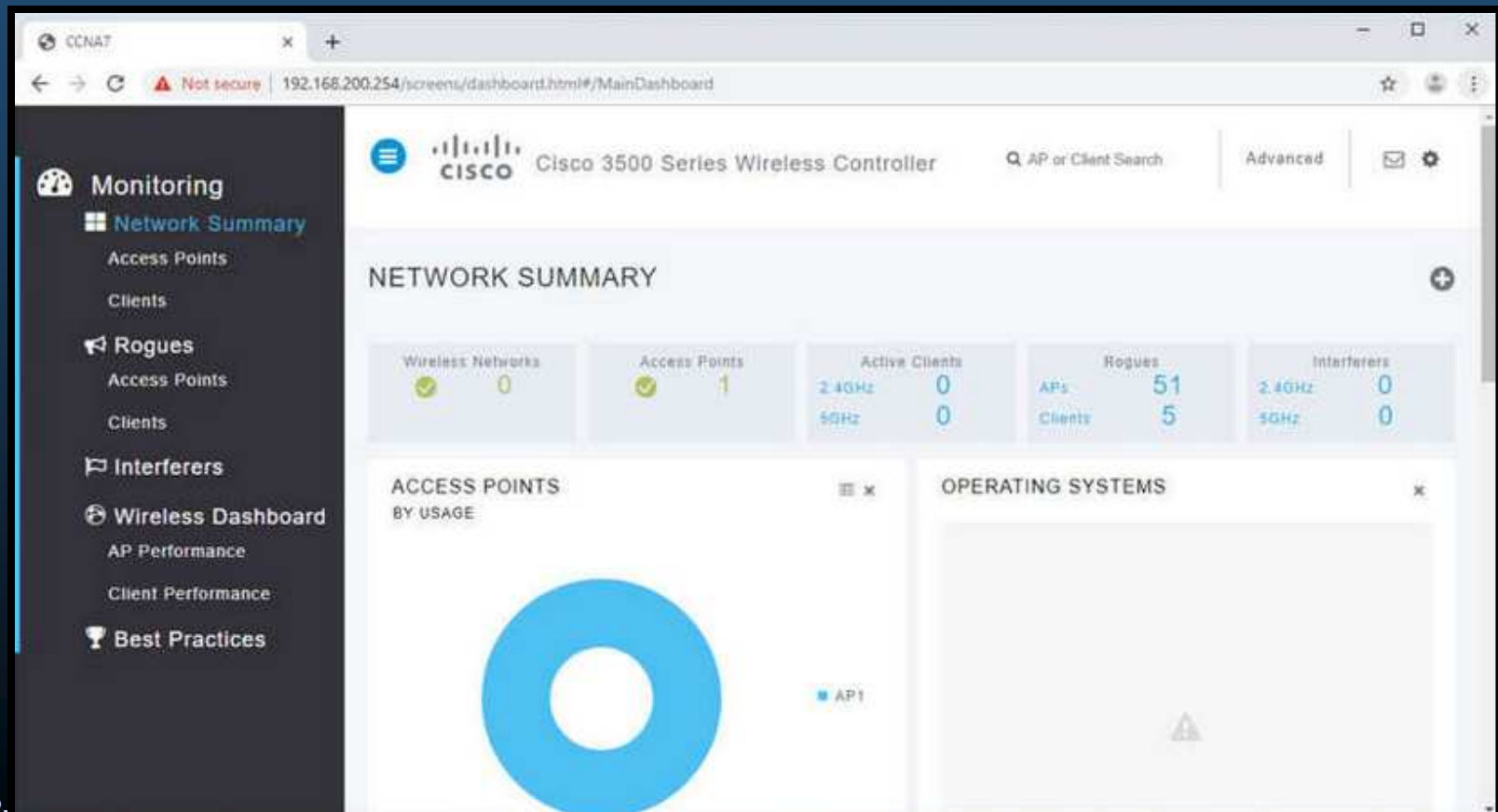
Configurar una WLAN Básica desde un WLC

- Iniciar sesión en el WLC.
 - Similar a un router inalámbrico.
 - Ingresar IP en el navegador e introducir credenciales por defecto.
 - El ejemplo muestra la GUI de un Cisco 3504 (192.168.200.254/admin/admin)



Configurar una WLAN Básica desde un WLC

- Iniciar sesión en el WLC.
 - Tras iniciar sesión se muestra la sección “Network Summary” con:
 - Redes inalámbricas configuradas, APs asociados, clientes activos, incluso Aps, no autorizados.



The screenshot displays the Cisco 3500 Series Wireless Controller dashboard. The browser address bar shows the URL 192.168.200.254/screens/dashboard.html#/MainDashboard. The dashboard features a left-hand navigation menu with categories like Monitoring, Rogues, Interferers, and Wireless Dashboard. The main content area is titled "NETWORK SUMMARY" and includes a summary table and two charts.

Wireless Networks	Access Points	Active Clients	Rogues	Interferers
0	1	2.4GHz: 0 5GHz: 0	APs: 51 Clients: 5	2.4GHz: 0 5GHz: 0

Below the summary table, there are two charts: "ACCESS POINTS BY USAGE" (a donut chart showing 1 AP) and "OPERATING SYSTEMS" (a chart with a warning icon).

Configurar una WLAN Básica desde un WLC

- Ver Información de APs.
 - Ir en el menú Izquierdo a: Access Points
 - Despliega información de desempeño, IP utilizada, información CDP (si habilitado).

The screenshot displays the 'ACCESS POINT VIEW' page for AP1. On the left is a navigation menu with 'Monitoring' selected, containing 'Network Summary', 'Access Points', 'Clients', 'Rogues', 'Interferers', 'Wireless Dashboard', and 'Best Practices'. The main content is divided into 'GENERAL' and 'PERFORMANCE SUMMARY' sections.

GENERAL

AP Name: AP1
Location: default location

MAC Address: 2c:4f:52:60:37:e8
IP Address: 192.168.200.3
CDP / LLDP: Switch, FastEthernet0/1
Ethernet Speed: 100 Mbps
Model / Domain: AIR-AP1815I-B-K9 / 802.11bg-A
802.11a-B
Power status: PoE/Full Power
Serial Number: FCW2320NGDH
Groups: AP Group: default-group, Flex Group: default-flex-group
Mode / Sub-mode: Local / Not Configured
Max Capabilities: 802.11n 2.4GHz, 802.11ac 5GHz
Spatial Streams - 2 (2.4GHz), 2 (5.0GHz)
Max. Data Rate - 144 Mbps(2.4GHz), 367 Mbps(5.0GHz)
Fabric: Disabled

PERFORMANCE SUMMARY

	2.4GHz	5GHz
Number of clients	1	0
Channels	11	(100, 104, 108, 112)
Configured Rate	Min: 1 Mbps, Max: 144 Mbps	Min: 6 Mbps, Max: 367 Mbps
Usage Traffic	709.4 MB	231.1 KB
Throughput	2.1 KB	0
Transmit Power	20 dBm	20 dBm
Noise	-90	-93 -95 -95 -95
Channel Utilization	9%	1%
Interference	7%	1%
Traffic	2%	0%
Air Quality	-	-
Admin Status	Enabled	Enabled
Clean Air Status	Not applicable	Not applicable

Configurar una WLAN Básica desde un WLC

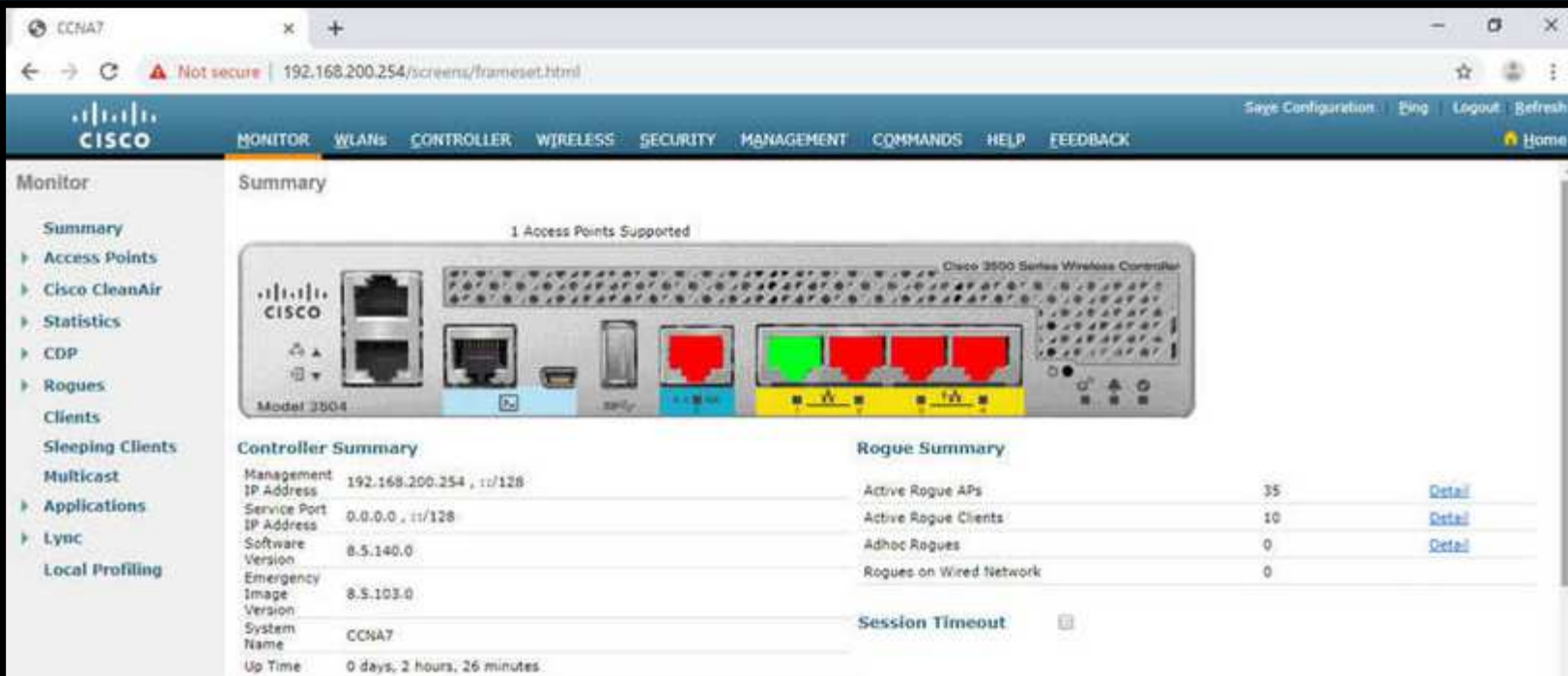
- Ver Información de APs.
 - El AP de la figura anterior es un Cisco Aironet 1815i (ver model/domain)
 - Soporta administración por CLI.
 - Permite verificar conectividad por ping

```
AP1# ping 192.168.200.1
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1069812.242/1071814.785/1073817.215 ms
AP1# ping 192.168.200.254
Sending 5, 100-byte ICMP Echos to 192.168.200.254, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1055820.953/1057820.738/1059819.928 ms
AP1# show interface wired 0
wired0    Link encap:Ethernet  HWaddr 2C:4F:52:60:37:E8
          inet addr:192.168.200.3  Bcast:192.168.200.255  Mask:255.255.255.255
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:2478  errors:0  dropped:3  overruns:0  frame:0
          TX packets:1494  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:80
          RX bytes:207632 (202.7 KiB)  TX bytes:300872 (293.8 KiB)
AP1#
```

Configurar una WLAN Básica desde un WLC

- Configuraciones Avanzadas.

- La mayoría de WLCs vienen con configuraciones por defecto.
 - Un administrador usualmente requiere realizar configuraciones avanzadas.
 - Necesario hacer clic en “Advanced” en esquina superior derecha (ver diapositiva 22)
 - Ello desplegará el resumen de configuraciones avanzadas:



The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The browser address bar indicates the URL `192.168.200.254/screens/frameset.html`. The interface includes a navigation menu on the left with options like Monitor, Summary, Access Points, and Statistics. The main content area displays the 'Summary' page, which includes a visual representation of the controller hardware and a table of configuration details.

Controller Summary		Rogue Summary	
Management IP Address	192.168.200.254, 11/128	Active Rogue APs	35
Service Port IP Address	0.0.0.0, 11/128	Active Rogue Clients	10
Software Version	8.5.140.0	Adhoc Rogues	0
Emergency Image Version	8.5.103.0	Rogues on Wired Network	0
System Name	CCNA7		
Up Time	0 days, 2 hours, 26 minutes		

Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.
 - Los WLCs tienen puertos físicos e interfaces virtuales similares a SVIs en switches.
 - Cada interfaz transporta tráfico a una WLAN por una VLAN diferente.
 - Un WLC Cisco 3504 soporta 150 APs y 4096 VLANs pero solo tiene 5 puertos físicos.
 - Cada puerto es como un troncal que puede llevar tráfico de múltiples VLANs.

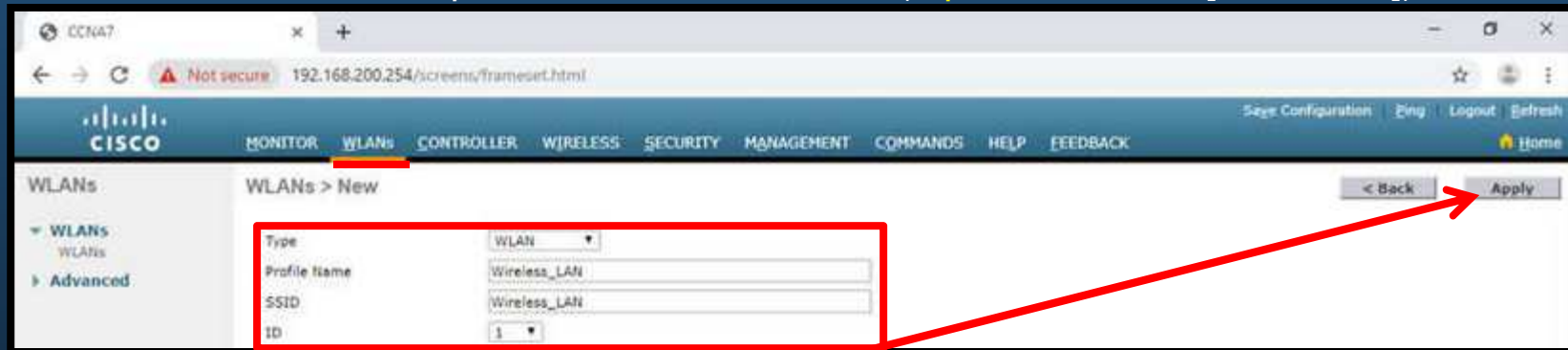


Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.

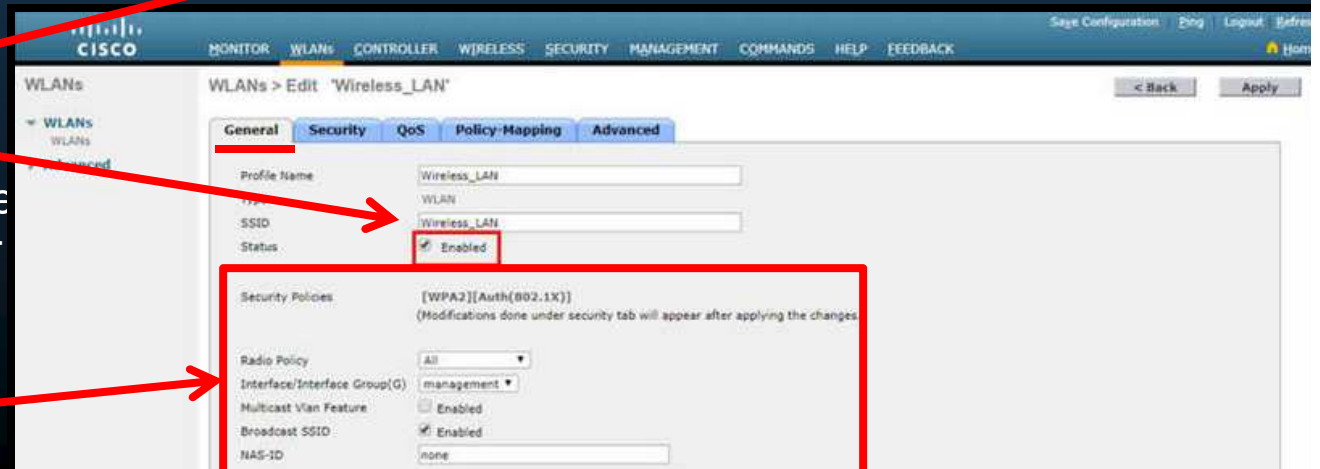
1. Crear una WLAN.

- Ir a “Advanced > WLAN”.
- Establecer parámetros de la WLAN (Tipo / SSID / ID [de WLAN]).



2. Aplicar y Habilitar la WLAN

- Tras hacer clic en “Apply”, es necesario habilitar la red antes de que sea accedida por los usuarios o configurar mas parámetros.

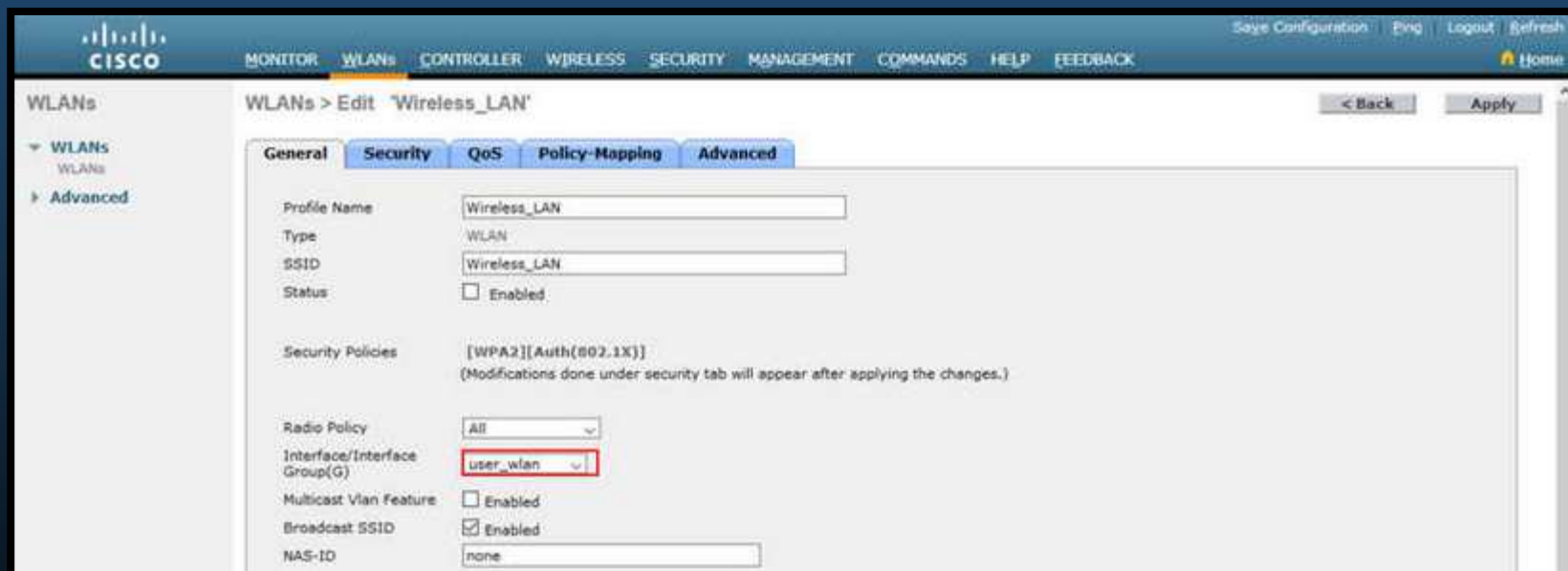


Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.

3. Elegir la interfáz.

- Necesario especificar la interfáz que llevará el tráfico de la WLAN.
- Cómo crear interfaces se trata mas adelante en este curso.

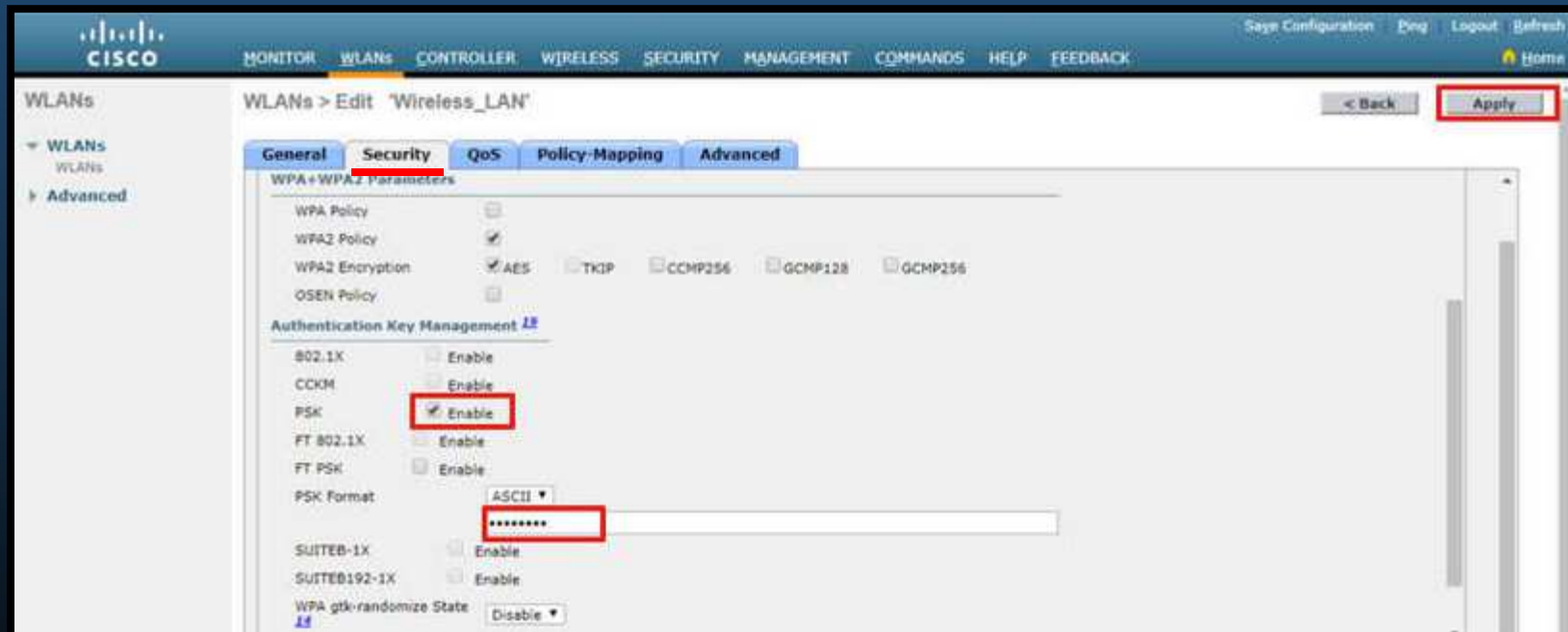


Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.

4. Asegurar la WLAN.

- Ir a la pestaña “Security”.
- Establecer parámetros de Seguridad (WPA / Autenticación / Frase) y Aplicar.



Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.
 5. Verificar si la WLAN es operacional.
 - Ir a “WLANs” en el menu izquierdo.
 - Aparecerá una lista de WLANs configuradas y sus parámetros.



The screenshot shows the Cisco WLC configuration interface for WLANs. The left sidebar has a tree view with 'WLANs' selected and highlighted with a red box. The main content area displays a table of configured WLANs. The table has columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. One WLAN is listed with ID 1, Type WLAN, Profile Name Wireless_LAN, WLAN SSID Wireless_LAN, Admin Status Enabled, and Security Policies [WPA2][Auth(PSK)].

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Wireless_LAN	Wireless_LAN	Enabled	[WPA2][Auth(PSK)]

Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.

6. Monitorear una WLAN.

- Ir al resumen de monitoreo “Monitor” en el menu superior.
- Desde ahí se pueden verificar los clientes asociados a las WLANs.

The screenshot shows the Cisco WLC Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'MONITOR' tab is selected. The left sidebar contains a 'Monitor' menu with options like Summary, Access Points, Cisco CleanAir, Statistics, CDP, Rogues, Clients, Sleeping Clients, Multicast, Applications, Lync, and Local Profiling. The main content area is titled 'Summary' and features a hardware image of a Cisco 3504 Wireless Controller. Below the image are two summary tables: 'Controller Summary' and 'Rogue Summary'. The 'Controller Summary' table lists management and service IP addresses, software and emergency image versions, system name, up time, system time, redundancy mode, and internal temperature. The 'Rogue Summary' table shows zero active rogue APs, clients, and rogues on the wired network. At the bottom right, a 'Top WLANs' table is highlighted with a red box, showing one WLAN named 'Wireless_LAN' with 1 client.

Profile Name	# of Clients
Wireless_LAN	1

Configurar una WLAN Básica desde un WLC

- Configurar una WLAN.

7. Ver Detalles de Clientes Inalámbricos.

- Haga clic en “Clients” en el menú izquierdo.
- Aparecerá una lista de Clientes asociados y sus parámetros.



The screenshot shows the Cisco Wireless LAN Controller (WLC) GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The left sidebar is expanded to show 'Clients' under the 'Monitor' section. The main content area displays the 'Clients' page with a table of wireless clients. The table has columns for Client MAC Addr, IP Address(Ipv4/Ipv6), AP Name, WLAN Profile, and WLAN SSID. One client is listed with MAC address 00:12:0c:37:7c:d7, IP address 192.168.5.2, AP Name AP1, WLAN Profile Wireless_LAN, and WLAN SSID Wireless_LAN.

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID
00:12:0c:37:7c:d7	192.168.5.2	AP1	Wireless_LAN	Wireless_LAN

Configurar una WLAN con WPA2 Empresarial en el WLC

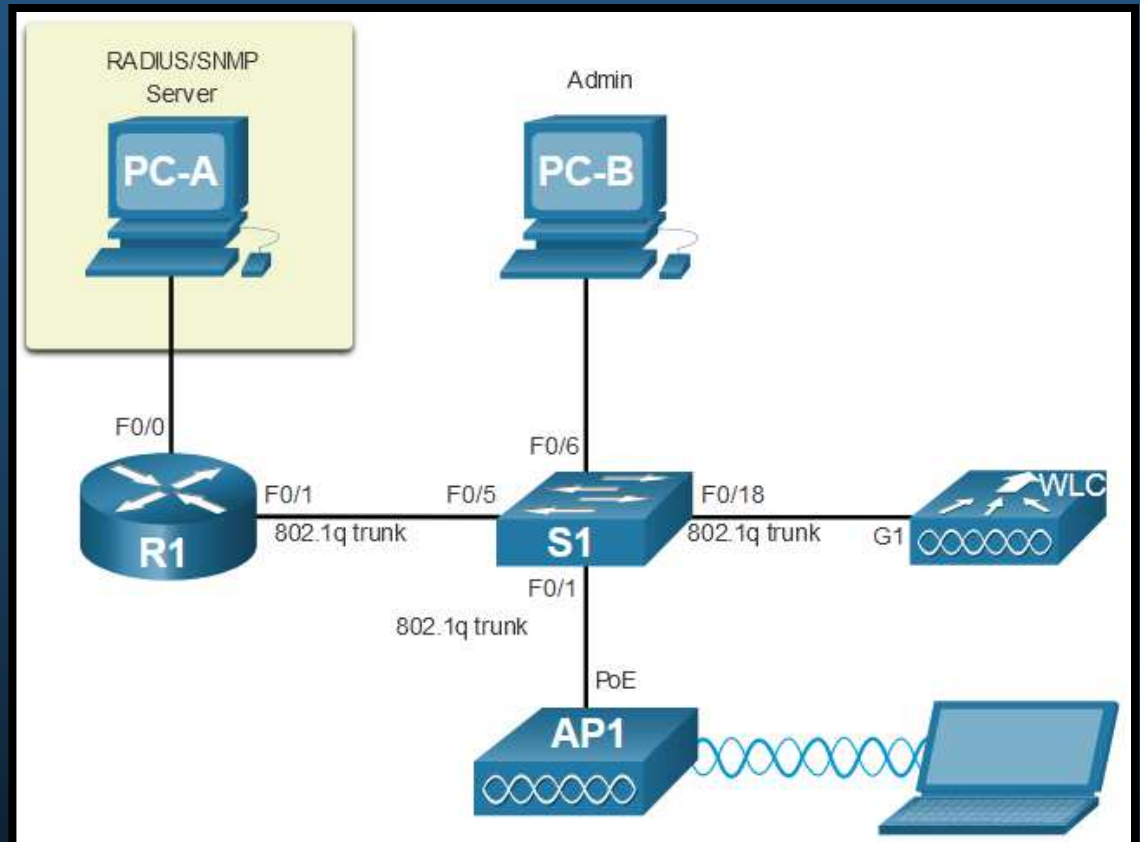
- **SNMP y RADIUS.**

- PC-A corre tanto un servidor de **Protocolo de Administración de Red Simple (SNMP)**, como **Servicio de Autenticación Remota de Usuarios por Llamada (RADIUS)**.

- **SNMP** monitorea la red.
- **RADIUS** proporciona servicios **AAA**, en lugar de una **PSK** para WPA.

- Los **usuarios inalámbricos** con autenticación **WPA2 Empresarial**, deben **ingresar su nombre de suario y contraseña**, que serán **verificados por RADIUS**, con lo que se podrá **rastrear su actividad**.

- **SNMP y RADIUS** quedan fuera del alcance de este curso.

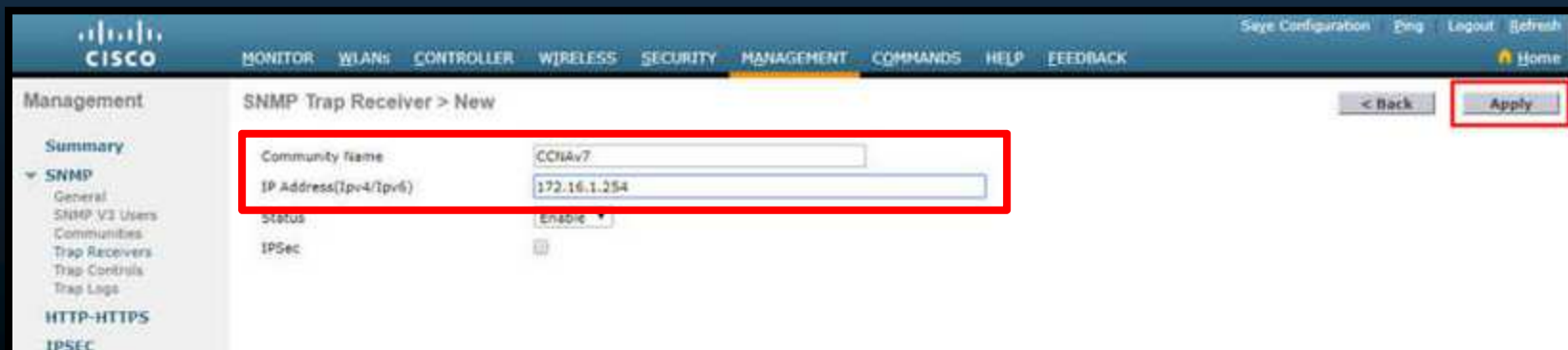


Configurar una WLAN con WPA2 Empresarial en el WLC

- Configurar Información de un Servidor SNMP.
 - En la GUI del WLC, hacer clic en la pestaña “MANAGEMENT”, y “SNMP” en el menú izquierdo, posteriormente la opción “Trap Receivers” y finalmente en el botón “New”.



- Ahí se deberá ingresar : “Community Name” e “IP” del servidor SNMP y dar clic en “Apply” .



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configurar Información de un Servidor RADIUS.

- En la GUI del WLC, hacer clic en la pestaña “SECURITY”, y “RADIUS” en el menú izquierdo, posteriormente la opción “Authentication” y finalmente en el botón “New”.



- Ahí se deberá ingresar : “IP” y “Shared Secrets” (contraseña para utilizada entre WLC y servidor) de RADIUS y dar clic en “Apply” .



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configurar Información de un Servidor RADIUS.
 - Tras dar clic en “Apply”, se mostrará la lista de servidores RADIUS configurados.



The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar shows the navigation menu with 'RADIUS' selected under 'AAA'. The main content area displays the configuration for a RADIUS server with the following settings:

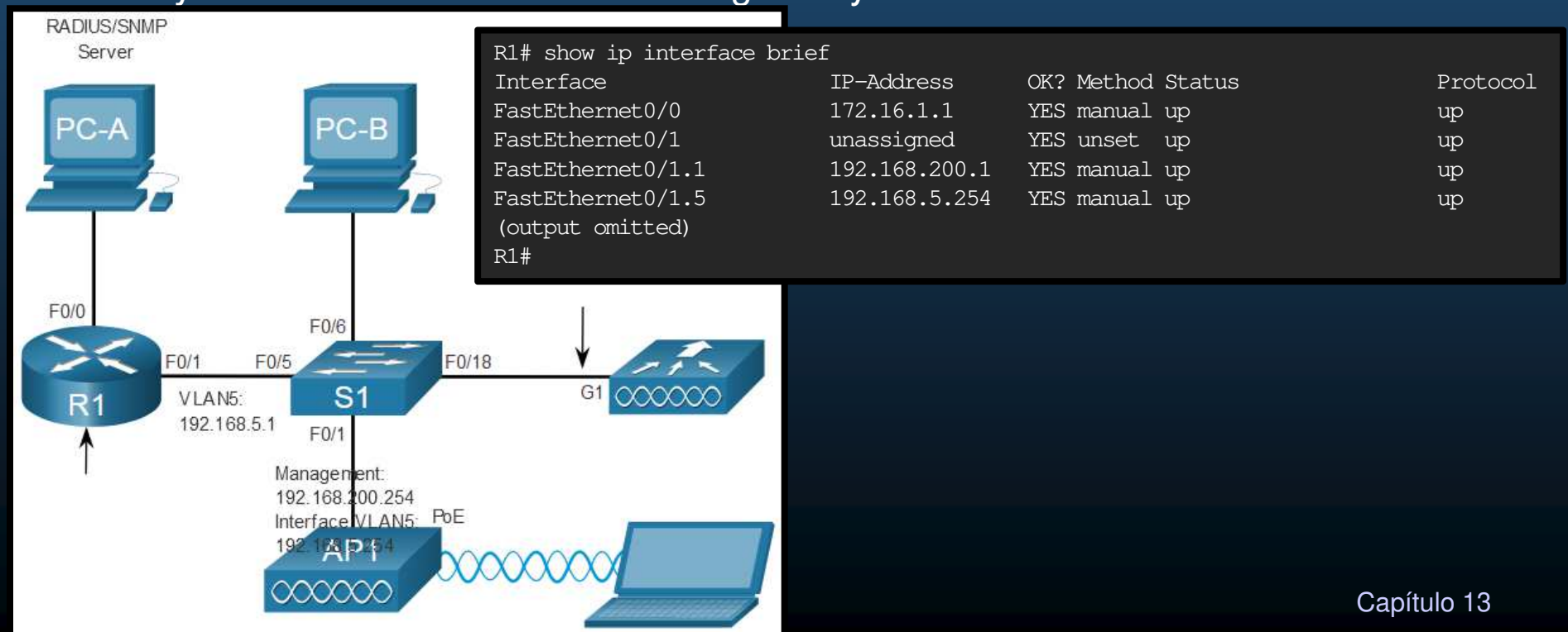
- Auth Called Station ID Type: AP MAC Address/SSID
- Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- MAC Delimiter: Hyphen
- Framed MTU: 1300

Below the configuration fields is a table of configured RADIUS servers:

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	172.16.1.254	1812	Disabled	Enabled

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración con Direcccionamiento en la VLAN 5.
 - Cada WLAN en un WLC requiere su propia interfáz.
 - Cada puerto físico del WLC puede configurarse para soportar múltiples WLANs.
 - Los puertos físicos también se pueden agregar para crear enlaces de alta velocidad.
 - En la topología de ejemplo se muestra un AP en la VLAN 5 (192.168.5.0/24) donde R1 ya cuenta con una subinterfáz configurada y activa en dicha VLAN.



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una nueva Interfáz.

1. Crear una nueva Interfáz.

- Clic en **CONTROLLER > Interfaces > New**

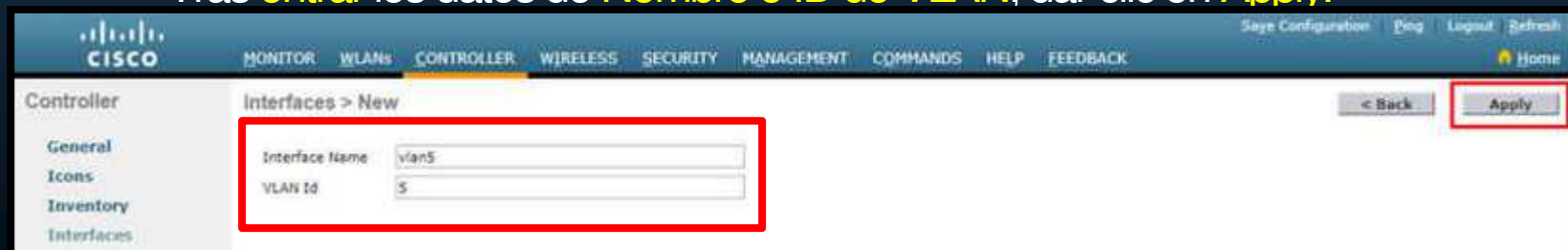


The screenshot shows the Cisco WLC Controller configuration page. The 'CONTROLLER' tab is selected in the top navigation bar. In the left sidebar, 'Interfaces' is highlighted. The main content area displays a table of existing interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.200.254	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-boot	untagged	0.0.0.0	Static	Not Supported	
service-portal	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

2. Configurar la VLAN.

- Tras **entrar** los datos de **Nombre e ID de VLAN**, dar clic en **Apply**.



The screenshot shows the 'Interfaces > New' configuration page. The 'CONTROLLER' tab is selected. The form contains the following fields:

- Interface Name:
- VLAN Id:

The 'Apply' button is highlighted in the bottom right corner.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una nueva Interfáz.

3. Configurar el puerto y dirección de interfáz.

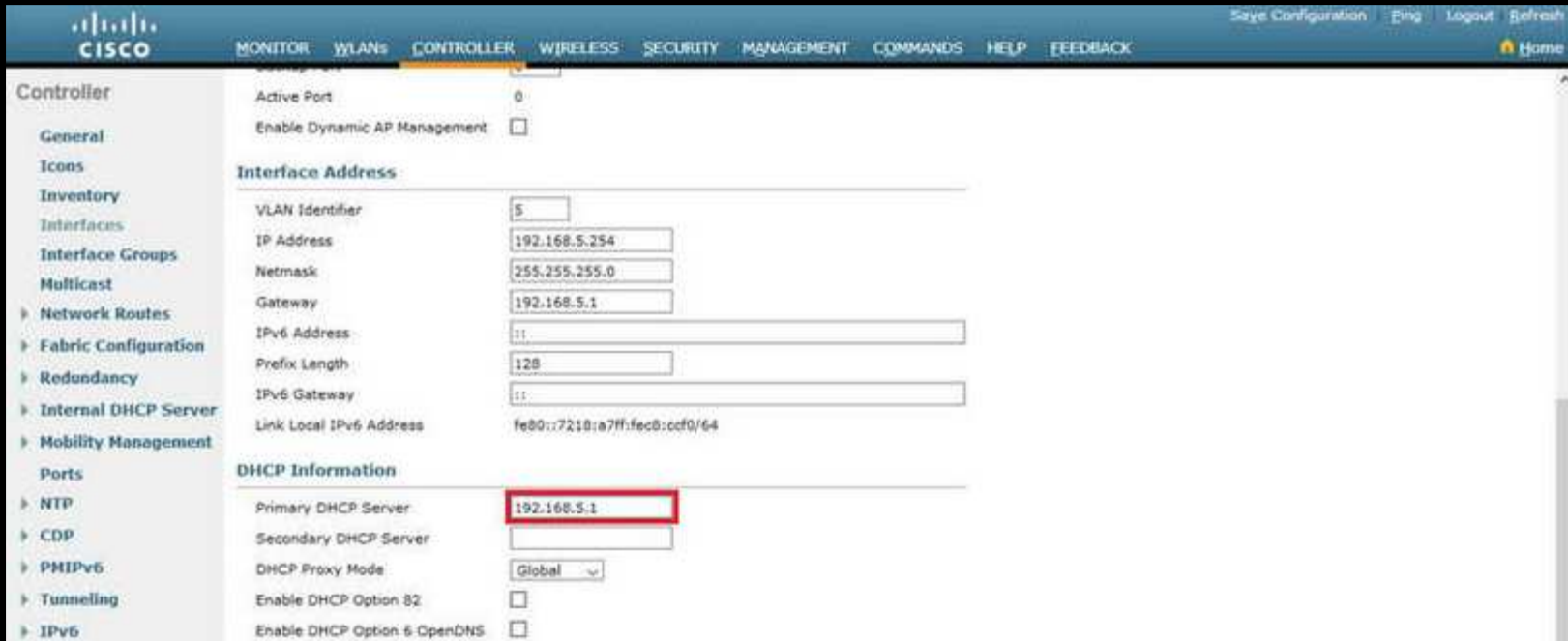
- Clic en **CONTROLLER > Interfaces > Edit**
- Configurar el número de puerto físico, ID de VLAN y Direcccionamiento IP.

The screenshot shows the Cisco WLC configuration page for an interface. The page is titled "Interfaces > Edit" and has a navigation menu on the left with categories like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PMIPv6, Tunneling, IPv6, mDNS, and Advanced. The main content area is divided into sections: General Information, Configuration, Physical Information, and Interface Address. The Physical Information section has a red box around the Port Number field, which is set to 1. The Interface Address section has a red box around the IP Address, Netmask, and Gateway fields, which are set to 192.168.5.254, 255.255.255.0, and 192.168.5.1 respectively. The General Information section shows the Interface Name as vlan5 and the MAC Address as 70:18:a7:c8:ccf1. The Configuration section shows Guest Lan, Quarantine, and Quarantine Vlan Id as 0, and NAS-ID as none.

Section	Field	Value
General Information	Interface Name	vlan5
	MAC Address	70:18:a7:c8:ccf1
Configuration	Guest Lan	<input type="checkbox"/>
	Quarantine	<input type="checkbox"/>
	Quarantine Vlan Id	0
	NAS-ID	none
Physical Information	Port Number	1
	Backup Port	0
	Active Port	1
	Enable Dynamic AP Management	<input type="checkbox"/>
Interface Address	VLAN Identifier	5
	IP Address	192.168.5.254
	Netmask	255.255.255.0
	Gateway	192.168.5.1

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una nueva Interfaz.
 4. Configurar dirección del servidor DHCP.
 - En CONTROLLER > Interfaces > Edit
 - Deslice la página hacia abajo hasta encontrar las configuraciones de DHCP.



The screenshot shows the Cisco WLC configuration page for an interface. The page is titled "Controller" and has a navigation menu on the left with options like General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PMIPv6, Tunneling, and IPv6. The main content area is divided into sections: "Interface Address" and "DHCP Information". The "Interface Address" section includes fields for VLAN Identifier (5), IP Address (192.168.5.254), Netmask (255.255.255.0), Gateway (192.168.5.1), IPv6 Address (::), Prefix Length (128), IPv6 Gateway (::), and Link Local IPv6 Address (fe80::7218:a7ff:fec8:ccf0/64). The "DHCP Information" section includes fields for Primary DHCP Server (192.168.5.1), Secondary DHCP Server, DHCP Proxy Mode (Global), Enable DHCP Option 82, and Enable DHCP Option 6 OpenDNS. The Primary DHCP Server field is highlighted with a red box.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una nueva Interfáz.

5. Aplique Cambios y Confirme.

- En CONTROLLER > Interfaces > Edit
- Concluida la configuración, deslice la página hacia arriba y de clic en Apply y luego confirme con Ok.



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una nueva Interfáz.

6. Verifique las Interfaces.

- En CONTROLLER > Interfaces
- La nueva interfáz se debería mostrar en la lista.



The screenshot shows the Cisco WLC web interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected. On the left, a sidebar menu shows 'Controller' with various sub-menus like 'General', 'Icons', 'Inventory', 'Interfaces', etc. The main content area is titled 'Interfaces' and displays a table of configured interfaces. The 'vlan5' interface is highlighted with a red box.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.200.254	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-port	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
user_wlan	10	192.168.10.254	Dynamic	Disabled	::/128
virtual	N/A	1.1.1.1	Static	Not Supported	
vlan5	5	192.168.5.254	Dynamic	Disabled	::/128

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración del Ámbito DHCP.
 1. Crear un nuevo ámbito DHCP.
 - Similar a un pool DHCP.
 - Hacer clic en **Internal > DHCP Server > DHCP Scope > New...**

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'CONTROLLER' tab is selected. On the left, a sidebar menu shows 'Internal DHCP Server' highlighted with a red box and a circled '1'. Below it, 'DHCP Scope' is also highlighted with a red box and a circled '2'. In the main content area, the 'DHCP Scopes' table is visible, with a 'New...' button highlighted by a red box and a circled '3'. The table contains one entry:

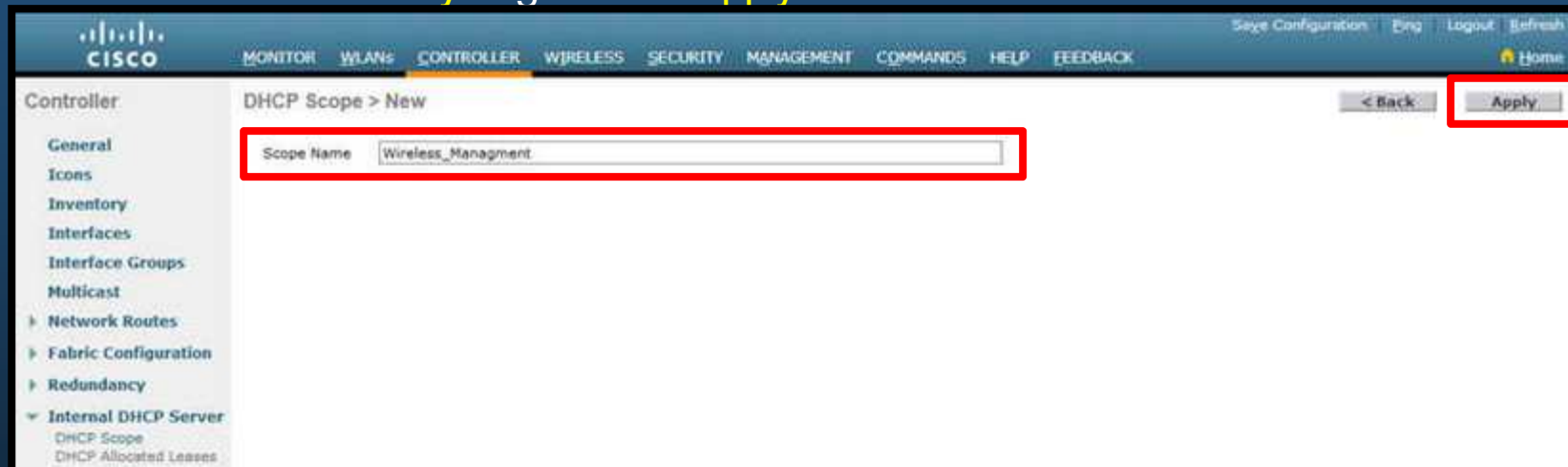
Scope Name	Address Pool	Lease Time	Status
dev@fire-mount	192.168.1.3 - 192.168.1.14	10 m	Enabled

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración del Ámbito DHCP.

2. Dar nombre al ámbito DHCP.

- De un nombre y haga clic en **Apply**.



3. Verifique el nuevo ámbito DHCP.

- Tras hacer clic en **Apply** a un nuevo ámbito DHCP, se muestra la lista de ámbitos.

The screenshot shows the Cisco WLC configuration interface displaying the list of DHCP Scopes. The table below shows the details of the newly created scope, "Wireless_Management", which is highlighted with a red box. The table also shows an existing scope, "dvs@-dhcp-manag".

Scope Name	Address Pool	Lease Time	St
Wireless_Management	0.0.0.0 - 0.0.0.0	1 d	Di
dvs@-dhcp-manag	192.168.1.3 - 192.168.1.14	1 d	En

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración del Ámbito DHCP.
 4. Configure y habilite el nuevo ámbito DHCP.
 - En la pantalla anterior, seleccione el ámbito deseado y clic en “Edit”.
 - Configure el pool, y demás parámetros de red para el DHCP:
 - El router por defecto corresponde a la subinterfáz para R1.

The screenshot shows the Cisco WLC configuration interface for a DHCP Scope. The page title is "DHCP Scope > Edit". The left sidebar shows the navigation menu with "Internal DHCP Server" selected. The main content area contains the following fields:

Scope Name	Wireless_Managment	
Pool Start Address	192.168.200.240	
Pool End Address	192.168.200.249	
Network	192.168.200.0	
Netmask	255.255.255.0	
Lease Time (seconds)	86400	
Default Routers	192.168.200.1	0.0.0.0
DNS Domain Name		
DNS Servers	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0
Status	Enabled	

Red boxes highlight the Pool Start Address, Pool End Address, Network, Netmask, Default Routers, and Status fields.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración del Ámbito DHCP.
 5. Verificar el ámbito DHCP habilitado.
 - La GUI regresa a “DHCP Scopes”, donde puede verificarse que el ámbito esté asignado.



Scope Name	Address Pool	Lease Time	Status
Wireless_Management	192.168.200.240 - 192.168.200.249	1 d	Enabled
dau0-dhcp-mgmt	192.168.1.3 - 192.168.1.14	1 d	Enabled

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una WLAN con WPA2 Empresarial.
 - Por defecto las WLAN creadas en un WLC usan WPA2 + AES con 802.1x + RADIUS
 - Anteriormente se configuró la IP del servidor RADIUS
 - Falta crear interfáz a la VLAN 5
- 1. Crear una nueva WLAN.
 - Clic en “WLAN” y luego “Go”.



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una WLAN con WPA2 Empresarial.

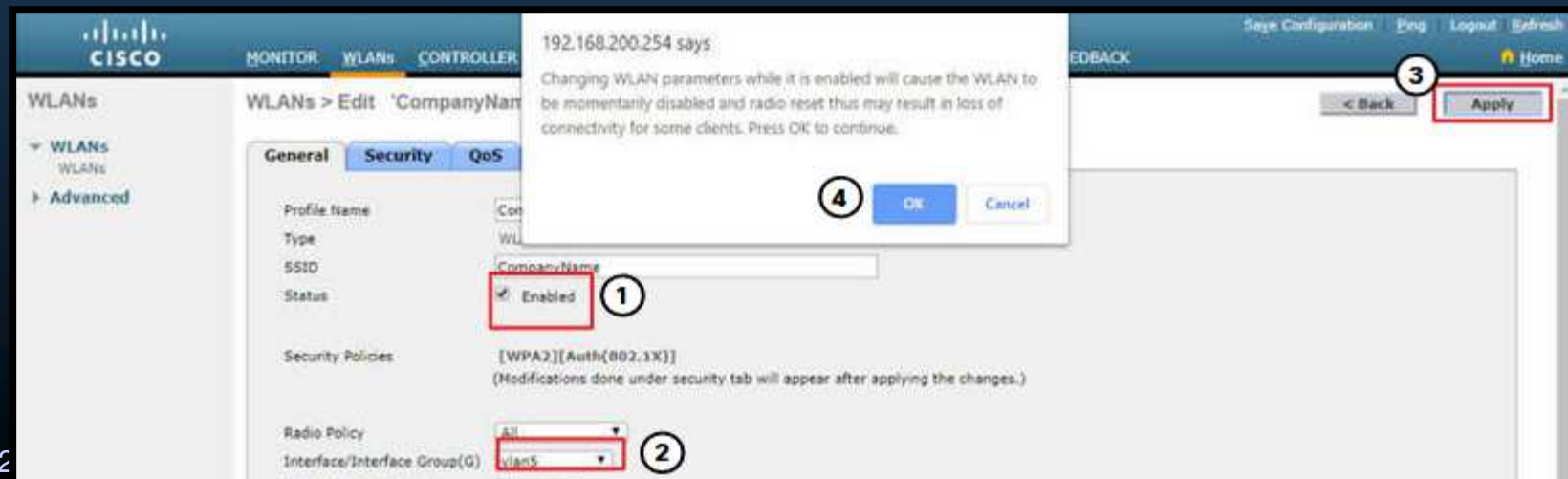
2. Configurar la WLAN y el SSID.

- Rellenar SSID e ID consistente con la configuración (5), clic en **Apply**.



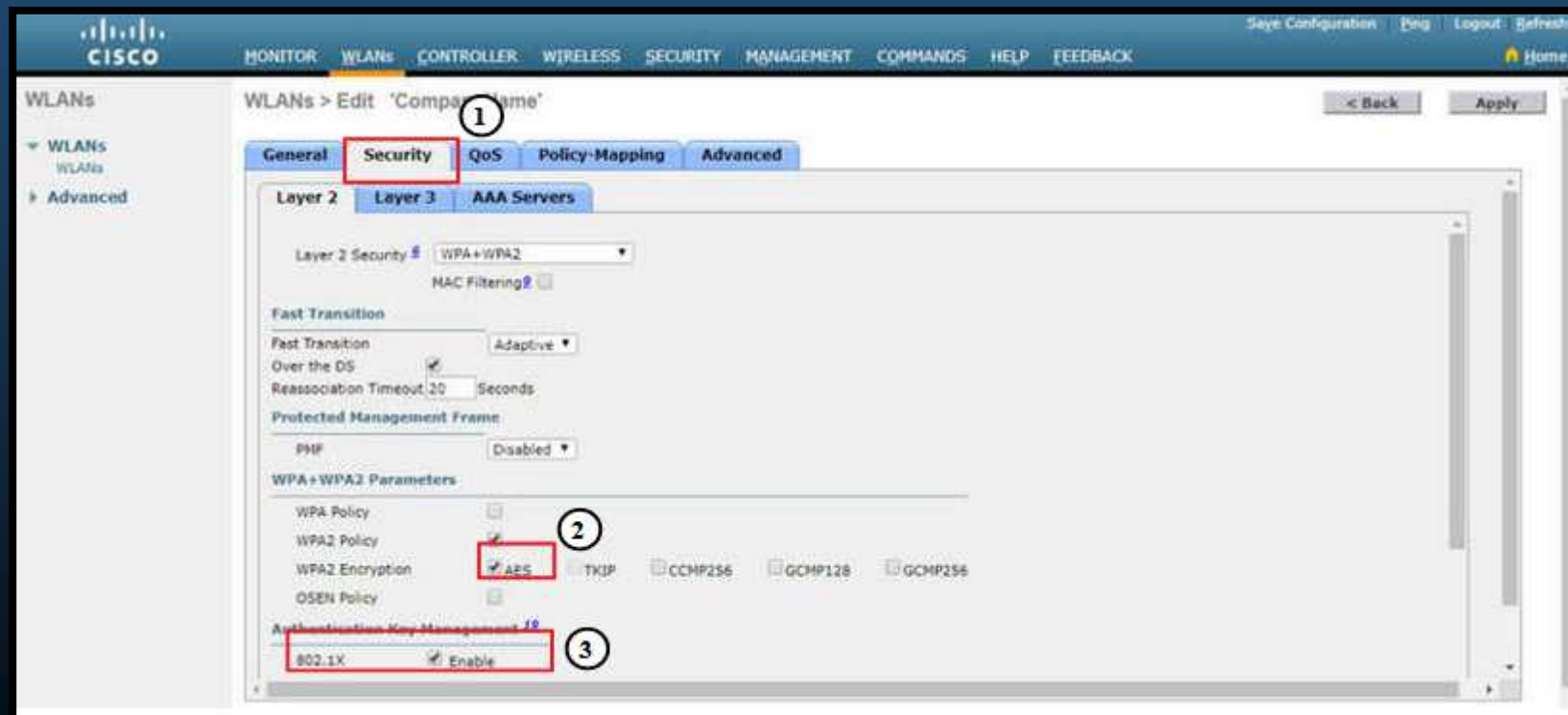
3. Habilite la WLAN para la VLAN 5.

- La VLAN debe asociarse con la VLAN correcta (Habilitar, elegir interfáz, aplicar y confirmar).



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una WLAN con WPA2 Empresarial.
 4. Verificar configuraciones AES y 802.1x por defecto.
 - Clic en pestaña “Security > Layer 2”, para la nueva WLAN.
 - Configurar WPA2 con AES y habilitar 802.1x entre WLC y RADIUS



Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una WLAN con WPA2 Empresarial.

- 5. Configurar el servidor RADIUS.

- Clic en pestaña “Security > AAA Servers”,.
 - En la lista desplegable elija el servidor RADIUS configurado previamente.

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'CompanyName'. The 'Security' tab is selected, and the 'AAA Servers' sub-tab is active. The 'AAA Servers' section is highlighted with a red box and a circled '1'. Below this, the 'RADIUS Servers' section is visible, with the 'Authenticating Servers' column highlighted by a red box and a circled '2'. The first server is configured with IP 10.173.16.1 and Port 1812. The 'Apply' button is highlighted with a red box and a circled '3'. The 'Interim Update' checkbox is checked, and the 'Interim Interval' is set to 0 seconds.

Server	Authenticating Servers	Accounting Servers
Server 1	10.173.16.1 Port: 1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

Configurar una WLAN con WPA2 Empresarial en el WLC

- Configuración de una WLAN con WPA2 Empresarial.
 6. Verifique que la nueva WLAN esté disponible.
 - Clic en la opción “WLANs”, en el menú de la izquierda.
 - En la lista desplegable deberían aparecer las 2 WLANs creadas previamente.



The screenshot displays the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'WLANs' menu item is highlighted. The main content area shows a table of WLANs with the following data:

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Wireless_LAN	Wireless_LAN	Enabled	[WPA2][Auth(PSK)]
2	WLAN	CompanyName	CompanyName	Enabled	[WPA2][Auth(802.1X)]

Configurar una WLAN con WPA2 Empresarial en el WLC

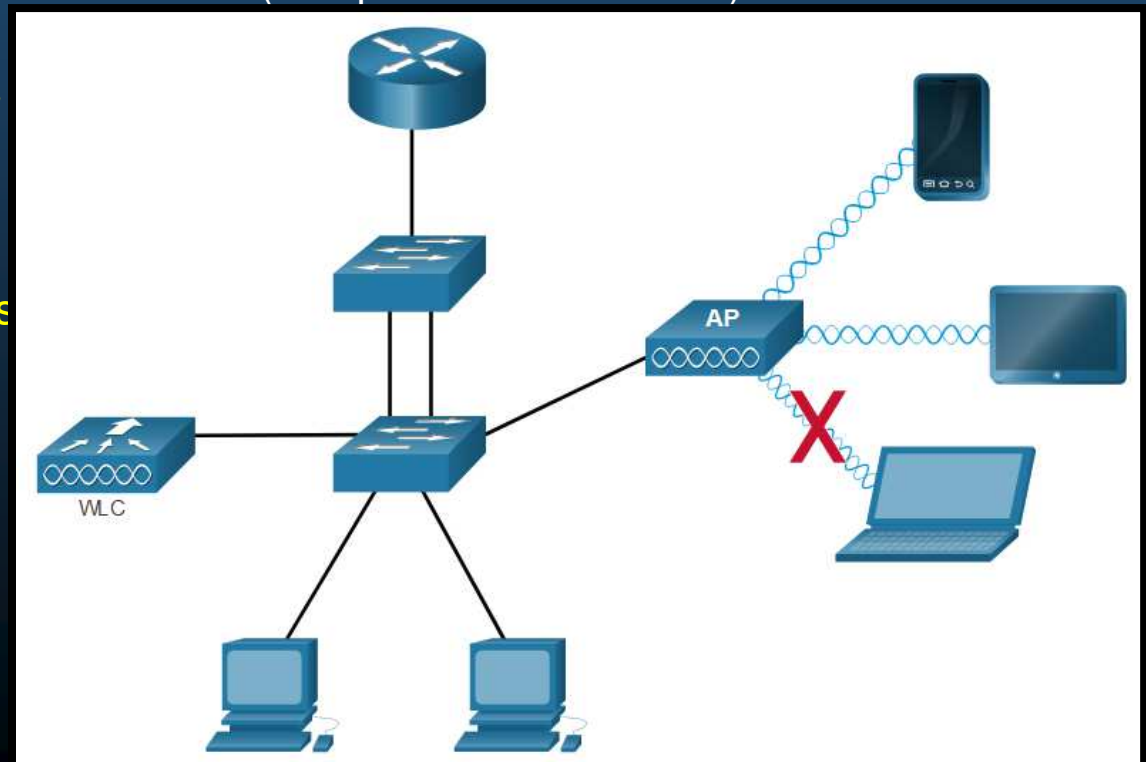
- Resolución de Problemas de WLAN.

- Metodología:

Paso	Título	Descripción
1	Identifique el problema	Si bien las herramientas se pueden utilizar en este paso, una conversación con el usuario a menudo es muy útil.
2	Establezca una teoría de las causas probables	Intente establecer una teoría de las causas probables. A menudo produce más de unas pocas causas probables del problema.
3	Pruebe la teoría para determinar la causa	Pruebe teorías para determinar la causa del problema. Un técnico a menudo aplicará un procedimiento rápido para probar y ver si resuelve el problema. Si un procedimiento rápido no corrige el problema, investigue más a fondo.
4	Establezca un plan de acción para resolver el problema e implemente la solución	Después de haber determinado la causa exacta del problema, establezca un plan de acción para resolver el problema e implementar la solución.
5	Verifique la funcionalidad completa del sistema e implemente medidas preventivas	Después de que haya corregido el problema, verifique la funcionalidad completa y, si corresponde, implemente medidas preventivas.
6	Documente los hallazgos, acciones y resultados	Finalmente, documente sus hallazgos, acciones y resultados. Esto es muy importante para futuras referencias.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Los Clientes Inalámbricos no Conectan.
 - Implementar un proceso de eliminación.
 - Si un cliente inalámbrico no conecta.
 - Confirme la configuración del PC con ipconfig
 - Verifique si recibió configuración IP por DHCP o si tiene IP estática.
 - Confirme conectividad con la red cableada (a los puertos LAN del router).
 - Reinstale los drivers en el cliente ó pruebe una WNIC diferente.
 - Si la WNIC funciona, verifique el modo de seguridad y configuraciones de cifrado . Si las configuraciones no concuerdan, reconfigure.



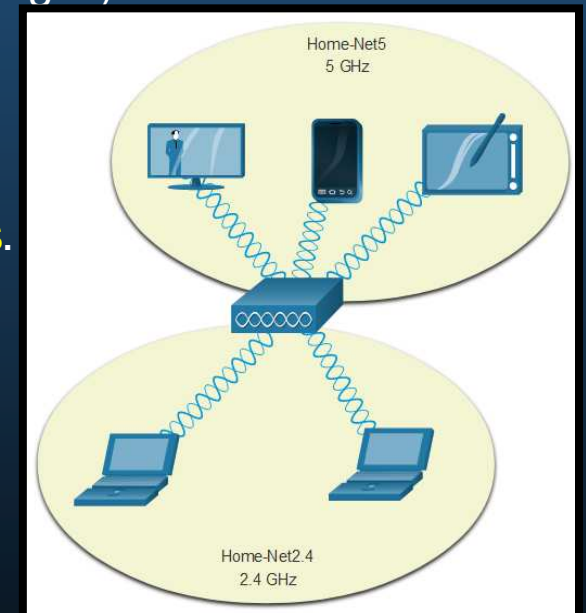
Configurar una WLAN con WPA2 Empresarial en el WLC

- Los Clientes Inalámbricos no Conectan.
 - Si el cliente inalámbrico funciona correctamente pero conecta pobremente.
 - Verifique la distancia entre PC y AP.
 - Verifique que el software cliente detecte canal correcto y SSID.
 - Verifique la presencia de otros dispositivos en el área que operen a 2.4GHz
 - Asegúrese que todos los dispositivos estén correctamente colocados.
 - Finalmente inspeccione la red cableada, en búsqueda de enlaces defectuosos o faltantes.
 - Si nada de lo anterior presenta problema, probablemente algo esté mal con el AP o su configuración.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Diagnosticar Cuando la Red está Lenta.

- Para **optimizar** e incrementar el ancho de banda **802.11 de banda dual**:
 - **Actualice sus clientes inalámbricos.** Dispositivos 802.11 b/g/n pueden alentar redes mas recientes. Cuando un **cliente no cumple** con **estándares recientes**, **forza la red entera a trabajar en al estándar del dispositivo** (mas antiguo).
 - **Divida el tráfico.** Desde 802.11n el tráfico en las **bandas de 2.4GHz y 5GHz**, se divide en **redes separadas**.
 - El **ancho de banda se comparte con WLANAs cercanas**.
 - Banda de **2.4GHz** :
 - **Para tráfico no sensible al tiempo:** (web, email, descargas)
 - Banda de **5GHz** .
 - **Para tráfico sensible al tiempo:** Streaming
 - **Banda de frecuencia menos saturada**, que cuenta con **mas canales**, por lo que **estará mas libre de interferencias**.
 - **Mas sensible a obstrucciones que 2.4GHz** (menores distancias de **cobertura**).



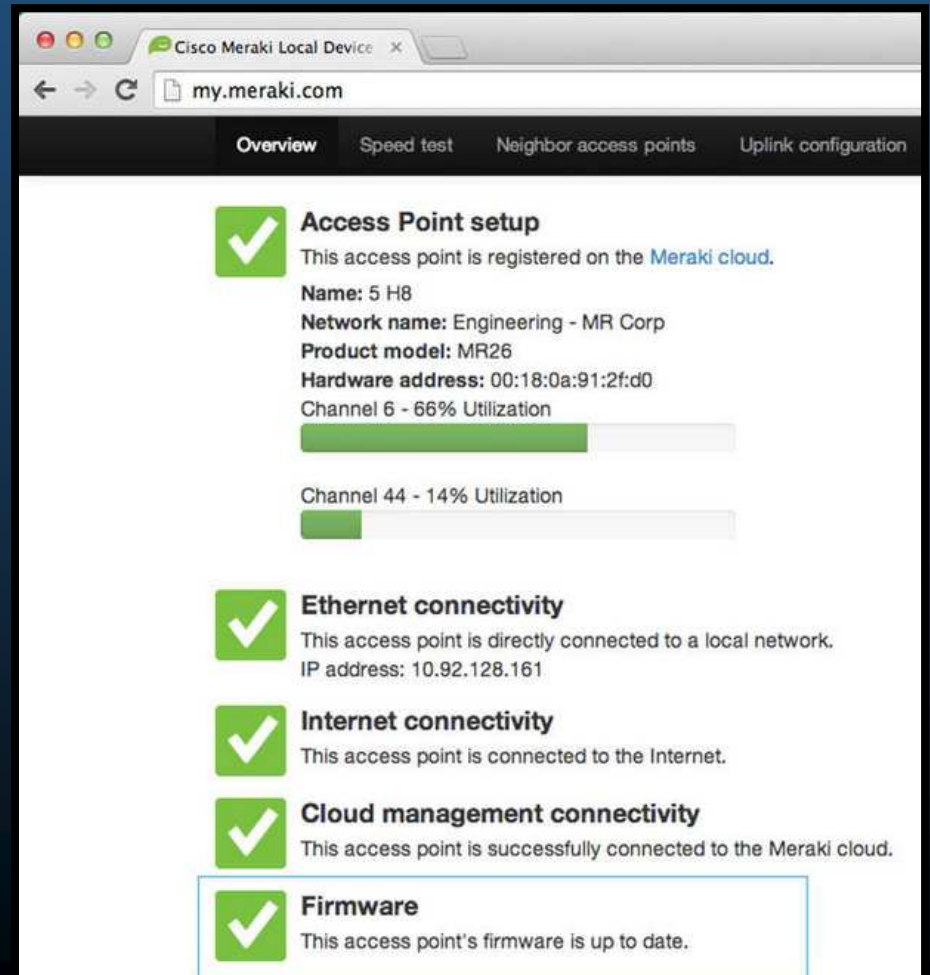
Configurar una WLAN con WPA2 Empresarial en el WLC

- **Actualizar Firmware.**

- La mayoría de APs o WLCs ofrecen actualizaciones de Firmware.

- Contienen correcciones a múltiples problemas y vulnerabilidades de seguridad.
- Verificar continuamente por nuevas actualizaciones.

- En un AP Cisco Meraki, puede hacerse esta y otras gestiones desde la nube.



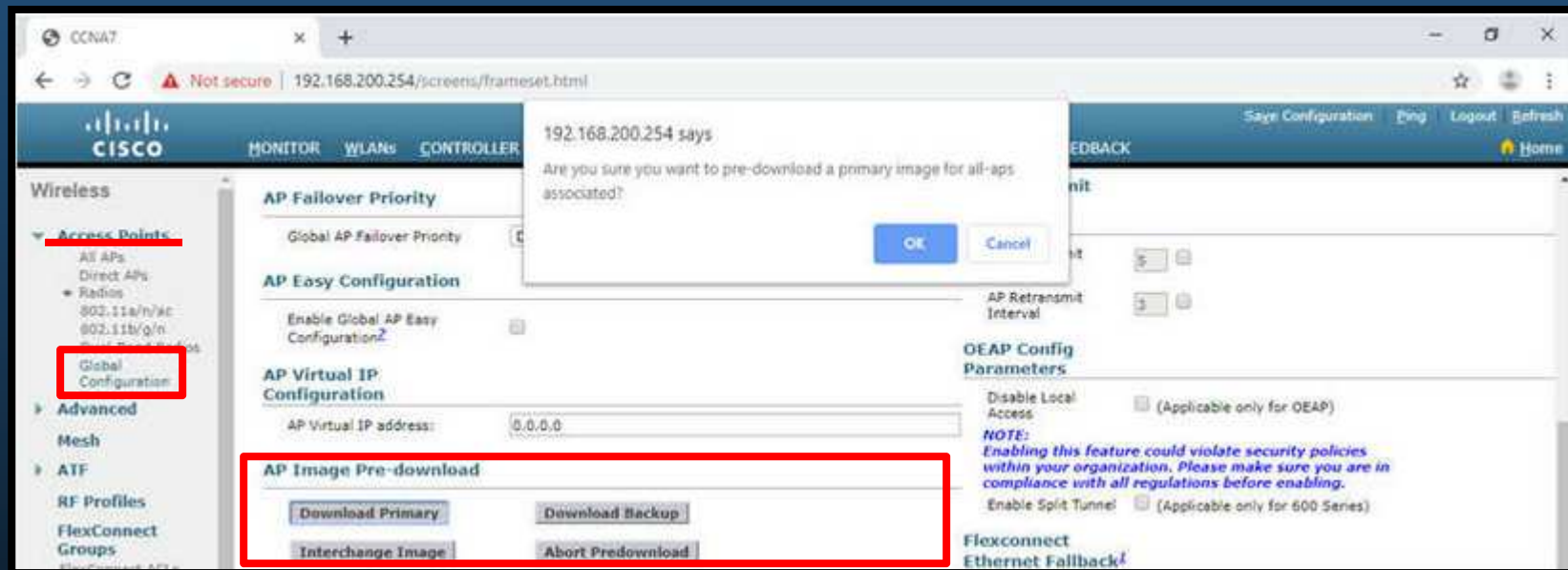
The screenshot shows a web browser window with the URL `my.meraki.com`. The page displays the status of a Cisco Meraki access point. The navigation bar includes links for Overview, Speed test, Neighbor access points, and Uplink configuration. The main content area shows several status checks, each with a green checkmark icon:

- Access Point setup**: This access point is registered on the Meraki cloud. Details include Name: 5 H8, Network name: Engineering - MR Corp, Product model: MR26, and Hardware address: 00:18:0a:91:2f:d0. Channel utilization is shown as Channel 6 - 66% and Channel 44 - 14%.
- Ethernet connectivity**: This access point is directly connected to a local network. IP address: 10.92.128.161.
- Internet connectivity**: This access point is connected to the Internet.
- Cloud management connectivity**: This access point is successfully connected to the Meraki cloud.
- Firmware**: This access point's firmware is up to date.

Configurar una WLAN con WPA2 Empresarial en el WLC

- Actualizar Firmware.

- En un WLC, debería haber manera de actualizar el firmware de todos sus APs.
- Primero se debe descargar el firmware adecuado para cada AP.



- En un Cisco 3504: Pestaña **WIRELESS** > **Access Points** del menú izquierdo > submenú **Global Configuration**. Deslizar hasta el final de la página hasta **AP Image Pre-download**.

Integración

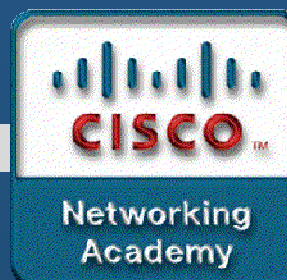
- Realice en PacketTracer, la actividad:

Configuración de una WLAN (se calificará)

En esta actividad ud, deberá **configurar** una **red inalámbrica con un router doméstico** y una red **basada en WLC**. Implementar **WPA2-PSK y WPA2 Personal**

<https://contenthub.netacad.com/srwe/13.5.1>

En esta ocasión no les dejo una actividad libre, puesto que en éste capítulo del curso de Cisco no se explica todo lo necesario para realizar una configuración desde cero. Adicionalmente a la actividad, no olviden incluir un párrafo con su aplicación creativa.



Capítulo 14

Conceptos de Enrutamiento

<https://contenthub.netacad.com/srwe/14.1.2>

Determinación de una Ruta

- Las Dos Funciones de un Router
 - Las funciones principales de un router son las siguientes:
 - Determinar la mejor ruta para enviar paquetes.
 - Los switches conectan dispositivos en una red y los routers conectan redes en una internet. Es necesario un mecanismo para identificar a por que interfaces se conectan las diferentes redes (Tabla de enrutamiento).
 - Reenviar paquetes a su destino.
 - El router usa la tabla de routing para buscar la mejor ruta hacia esa red. Incluye la interfaz que se debe usar para reenviar los paquetes a cada red conocida.
 - Un router puede recibir un paquete encapsulado en un tipo de trama de enlace de datos y reenviarlo por una interfaz que usa otro tipo de trama de enlace de datos.

Determinación de una Ruta

- Ejemplo de las Funciones del Router.

- R1 recibe el paquete encapsulado en una trama de Ethernet.
- Desencapsula el paquete y **usa la dirección IP de destino para buscar una dirección de red en su tabla de routing.**

```
R1# show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

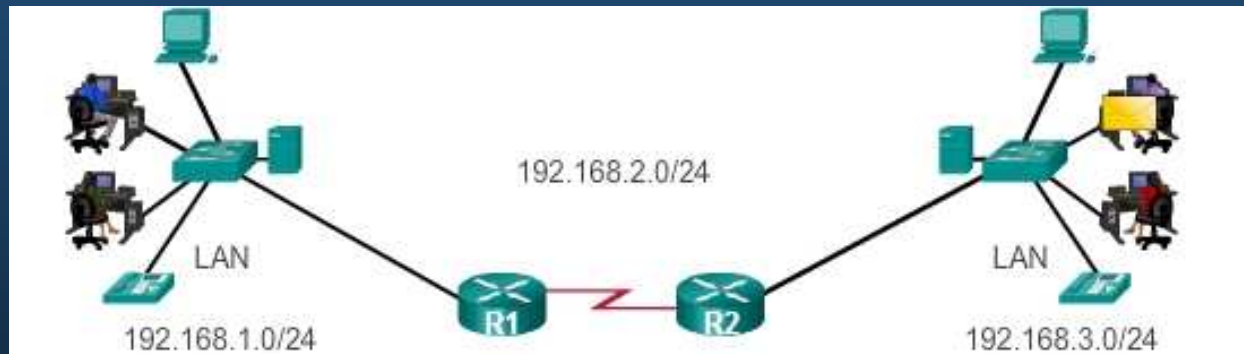
Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Los routers utilizan la tabla de routing como un mapa para descubrir la mejor ruta para una red determinada.

Determinación de una Ruta

- Los routers eligen las mejores rutas.
 - Luego de encontrar una dirección de red de destino en la tabla de enrutamiento, R1 encapsula el paquete dentro de una trama PPP y reenvía el paquete a R2. El R2 realiza un proceso similar.



Determinación de una Ruta

- La Mejor Ruta está Dada por la Mejor Coincidencia.
 - Se busca la mejor coincidencia de bits entre la dirección IP destino de cada paquete y las entradas de la tabla de enrutamiento.
 - La coincidencia debe ser de izquierda a derecha.
 - Para ser considerada, deben coincidir al menos los bits de la longitud del prefijo de la ruta en la tabla de enrutamiento.
 - Pues un paquete IP solo lleva dirección, no prefijo.
 - La ruta con el mayor número de bits equivalentes del extremo izquierdo, es siempre la ruta preferida.

Determinación de una Ruta

- Ejemplo de Mejor Coincidencia en IPv4.

- Un paquete con la IP Destino: 172.16.0.10, llega a un router con 3 entradas en su tabla de enrutamiento, de las cuales, 172.16.0.0/26 es la mejor coincidencia.

Dirección IPv4 Destino		Dirección en Binario
172.16.0.10		10101100.00010000.00000000.00001010
Entrada de Ruta	Prefijo/ Longitud de Prefijo	Dirección en Binario
1	172.16.0.0/12	10101100.00010000.00000000.00001010
2	172.16.0.0/18	10101100.00010000.00000000.00001010
3	172.16.0.0/26	10101100.00010000.00000000.00001010

Determinación de una Ruta

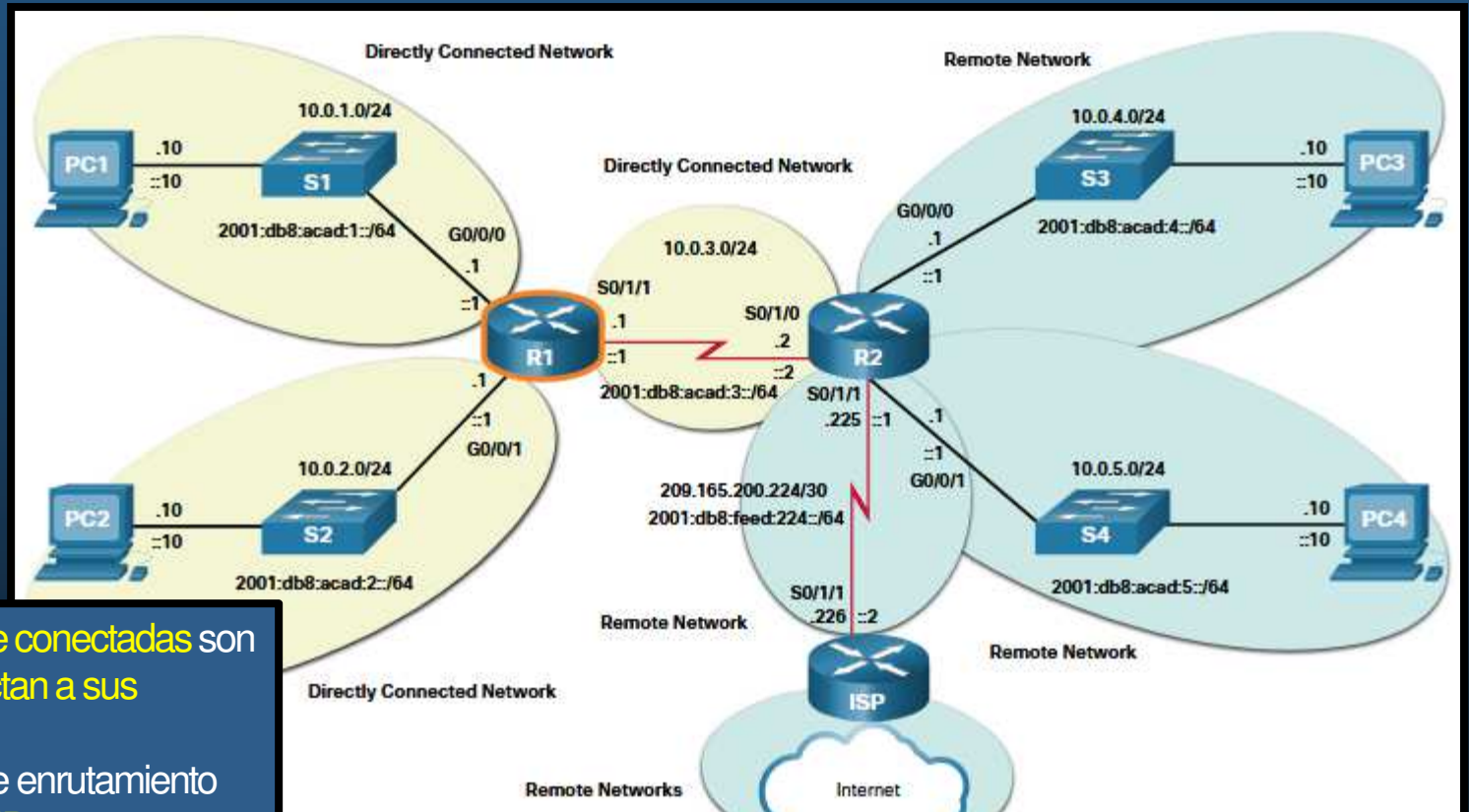
- Ejemplo de Mejor Coincidencia en IPv6.
 - Un paquete con la IP Destino: **2001:db8:c000::99**, llega a un router con 3 entradas en su tabla de enrutamiento, de las cuales, **2001:db8:c000::/48** es la mejor coincidencia.

Dirección IPv6 Destino		
2001:db8:c000::99		
Entrada de Ruta	Prefijo/ Longitud de Prefijo	Longitud de la coincidencia
1	2001:db8:c000::/40	40 bits
2	2001:db8:c000::/48	48 bits (mejor coincidencia)
3	2001:db8:c000:5555::/64	No coinciden los 64 bits

Determinación de una Ruta

- Construcción de una Tabla de Enrutamiento.

- Visto desde R1.



Las **redes directamente conectadas** son las redes que se conectan a sus interfaces activas.

Se añaden a la tabla de enrutamiento cuando se configura n IP , mascara y no shutdown.

La **ruta por defecto** especifica el siguiente salto para las redes que no están en la tabla de enrutamiento . Tiene una longitud de preijo de 0 (no necesita coincidir ningún bit).

Las **redes remotas** son las redes que no conectadas a sus interfaces.

Se aprenden de 2 formas:

Estáticas, se configuran manualmente.

Dinámicas, aprendidas por protocolos de enrutamiento.

Reenvío de Paquetes

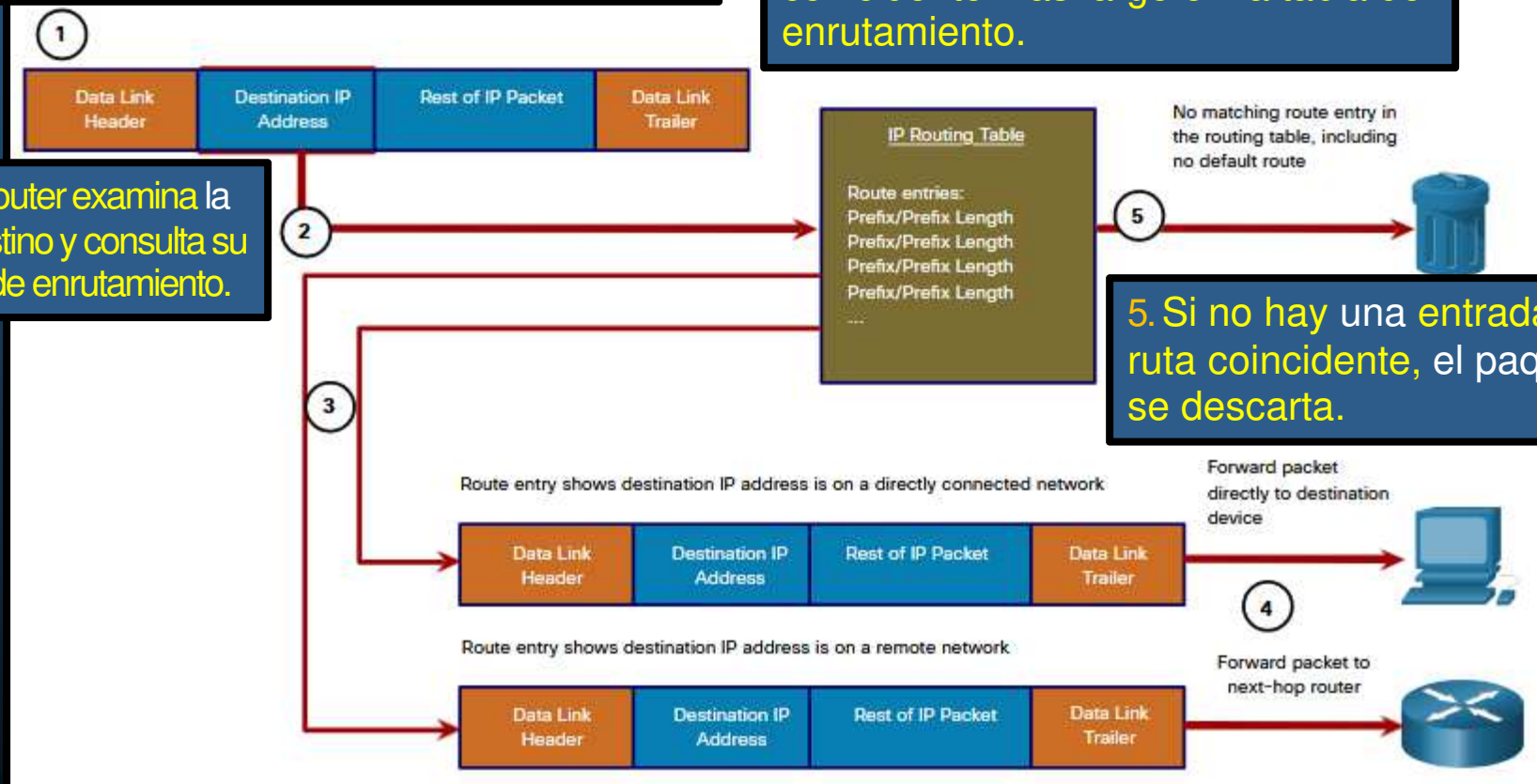
Proceso de Decisión de Reenvío de Paquetes.

1. La trama con un paquete IP encapsulado llega a la interfaz de entrada.

3. El router encuentra el prefijo coincidente más largo en la tabla de enrutamiento.

2. El router examina la IP destino y consulta su tabla de enrutamiento.

5. Si no hay una entrada de ruta coincidente, el paquete se descarta.



4. El router encapsula el paquete en un nuevo marco y lo reenvía desde la interfaz de salida. El destino podría ser un dispositivo final o un enrutador de siguiente salto.

Reenvío de Paquetes

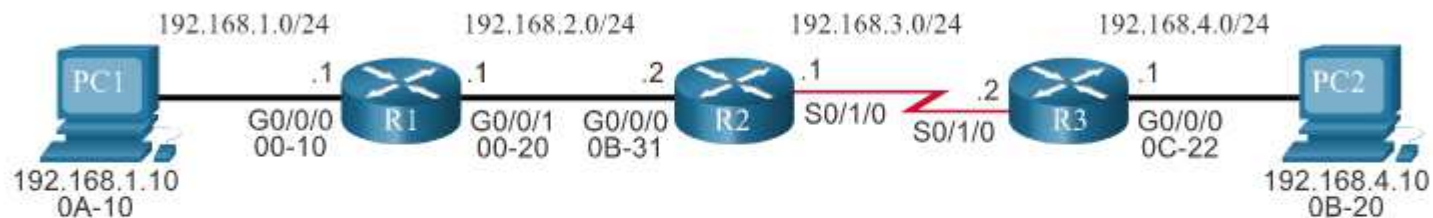
- **Proceso de Decisión de Reenvío de Paquetes.**
 - **Tras determinar la mejor ruta un router puede:**
 - **Reenviar el paquete a un dispositivo en una red conectada directamente.**
 - La **interfaz de salida** se encuentra indicada en la **entrada de ruta**.
 - Debe realizar un **nuevo encapsulado capa 2**.
 - Debe **determinar la dirección destino de capa de enlace**.
 - Vgr; **IPv4** se apoya en **ARP** de forma similar, **IPv6** en **ICMPv6**
 - **Reenviar el paquete a un router de siguiente salto.**
 - La **red destino es remota**.
 - La **dirección del siguiente salto** se indica en la **entrada de ruta**.
 - Debe **determinar la dirección destino de capa de enlace**.
 - Este proceso **variará dependiendo del tipo de redes de capa 2**.
 - **Desechar el paquete:** **no hay coincidencias** en la tabla de enrutamiento.
 - Si **no hay coincidencia** entre IP destino y un prefijo en la tabla de enrutamiento, **y si no hay una ruta predeterminada**, el paquete **se descartará**.

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada para la interfaz saliente.

PC1 tiene un paquete para PC2



Layer 2 Data Link Frame

Packet's Layer 3 data

Caché ARP para PC1

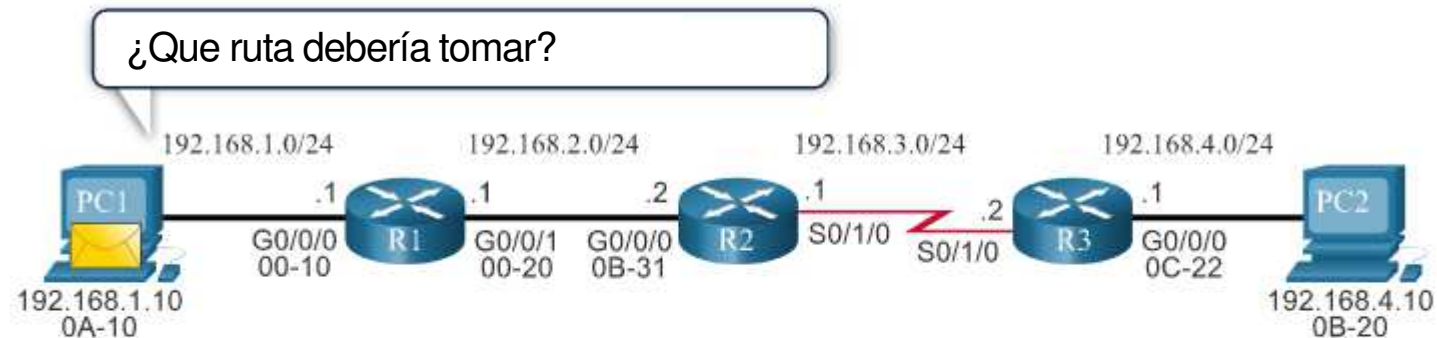
IP Address MAC Address

192.168.1.1 00-10

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada para la interfaz saliente.



Layer 2 Data Link Frame

Packet's Layer 3 data

Caché ARP para PC1

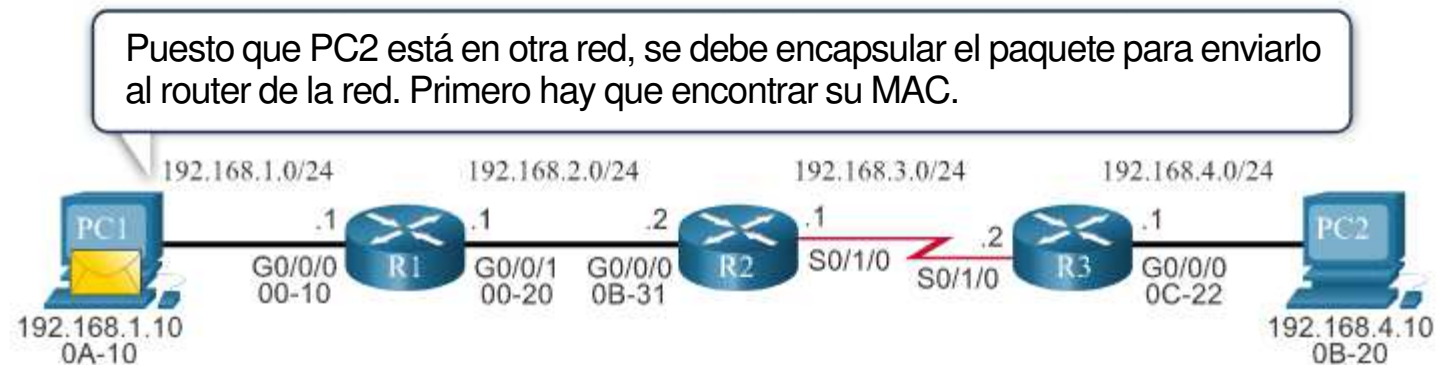
IP Address MAC Address

192.168.1.1 00-10

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada para la interfaz saliente.



Layer 2 Data Link Frame

Packet's Layer 3 data

Source IP	Dest. IP	IP fields	Data
192.168.1.10	192.168.4.10		

Caché ARP para PC1

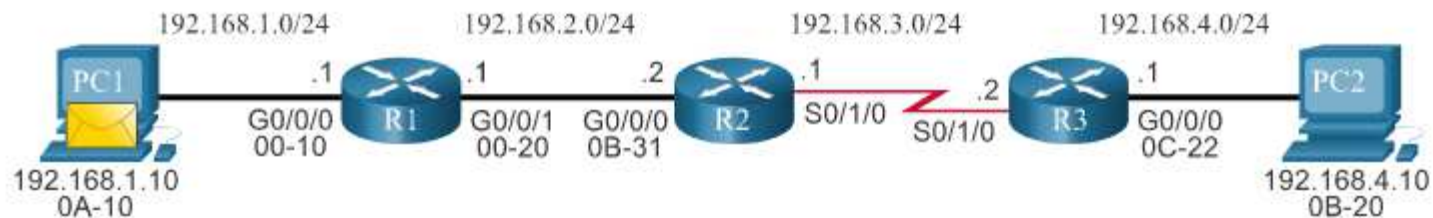
IP Address MAC Address

192.168.1.1 00-10

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada para la interfaz saliente.



Layer 2 Data Link Frame

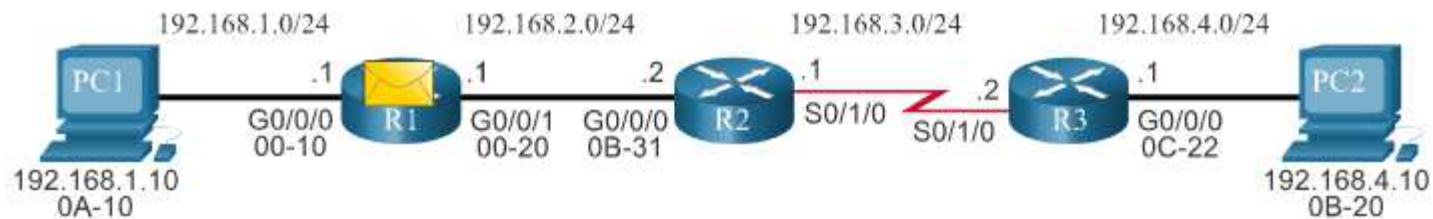
Layer 2 Data Link Frame			Packet's Layer 3 data				
Dest. MAC	Source MAC	Type	Source IP	Dest. IP	IP fields	Data	Trailer
00-10	0A-10	0x800	192.168.1.10	192.168.4.10			

Caché ARP para PC1

IP Address	MAC Address
192.168.1.1	00-10

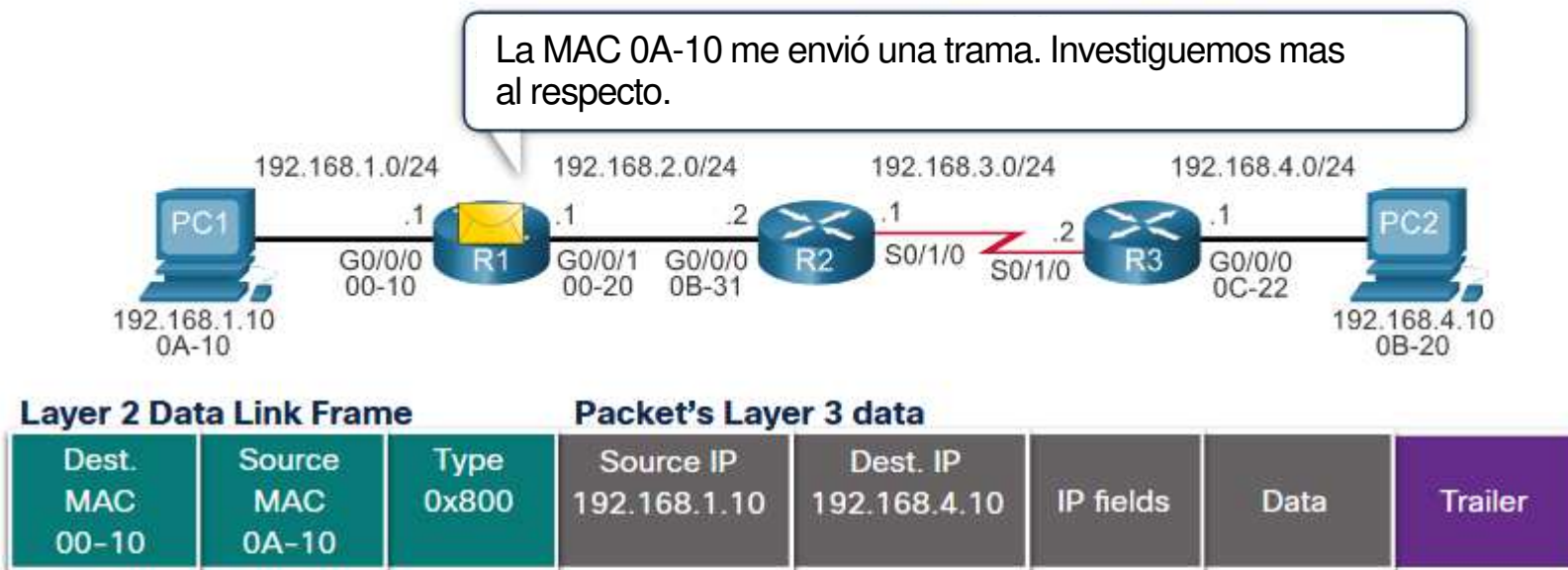
Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**
 - Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada para la interfaz saliente.



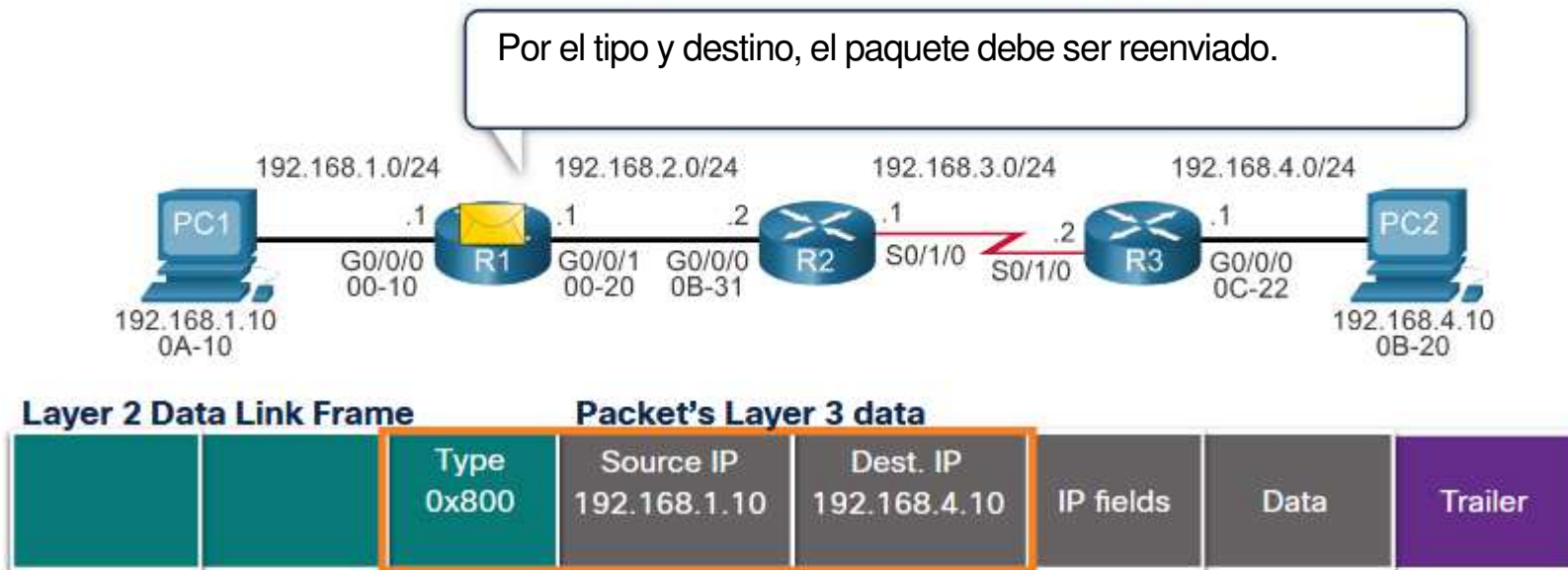
Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.



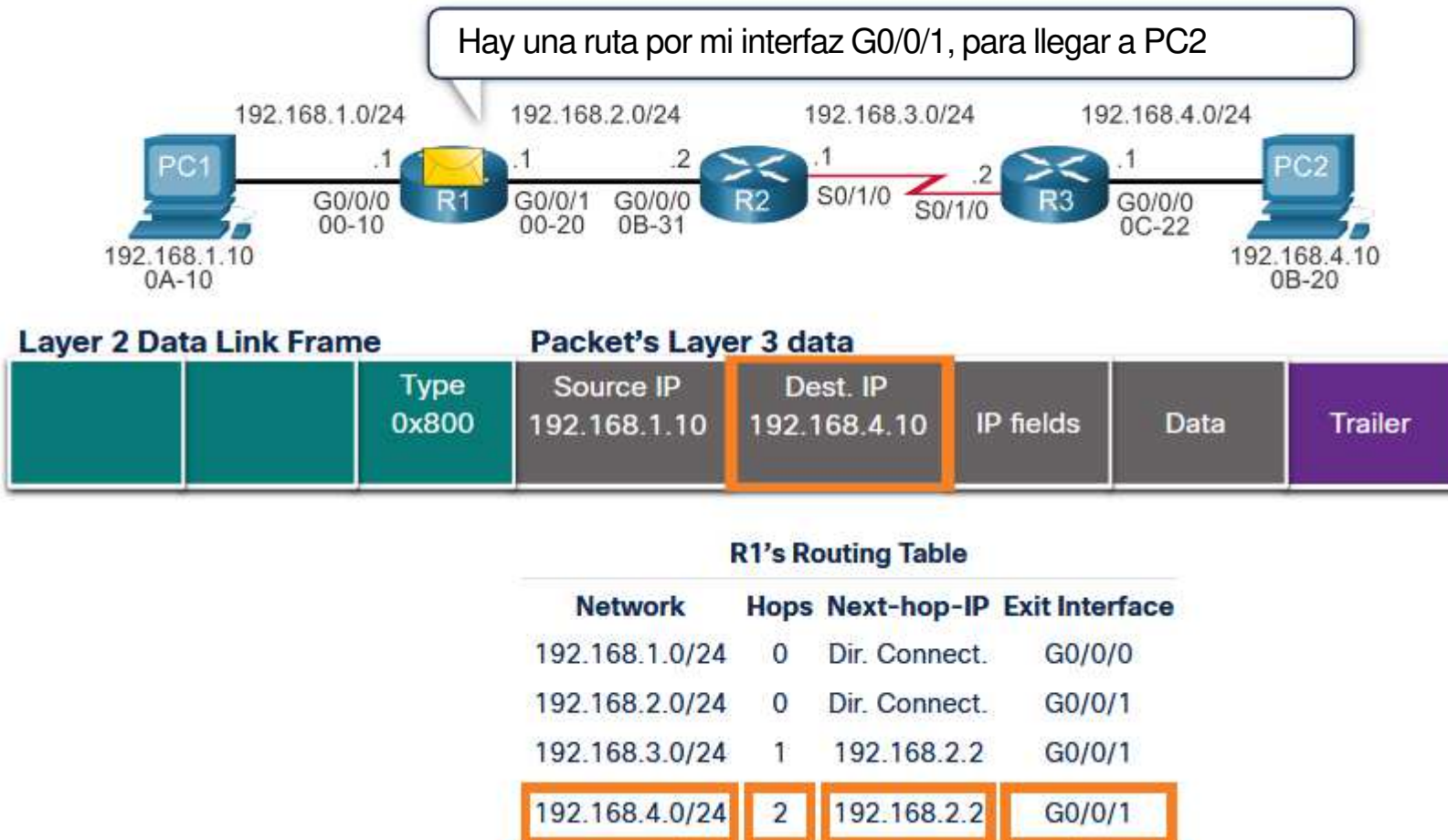
Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.



Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.

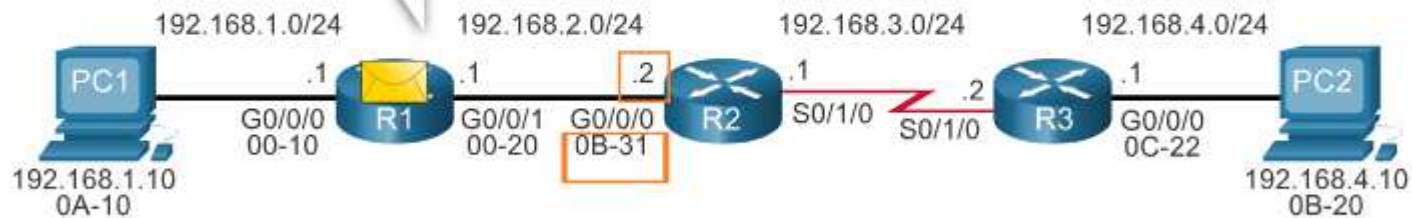


Reenvío de Paquetes

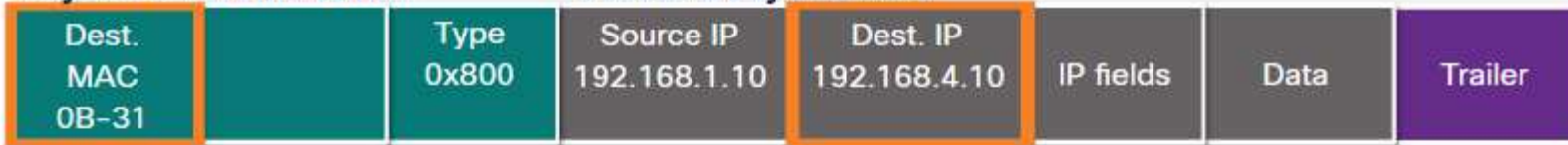
- Reenvío de Paquetes de Extremo a Extremo.

Necesario reconstruir la trama.

ARP indica que PC2 se puede alcanzar mediante 0B-31



Layer 2 Data Link Frame



Packet's Layer 3 data

R1's ARP Cache

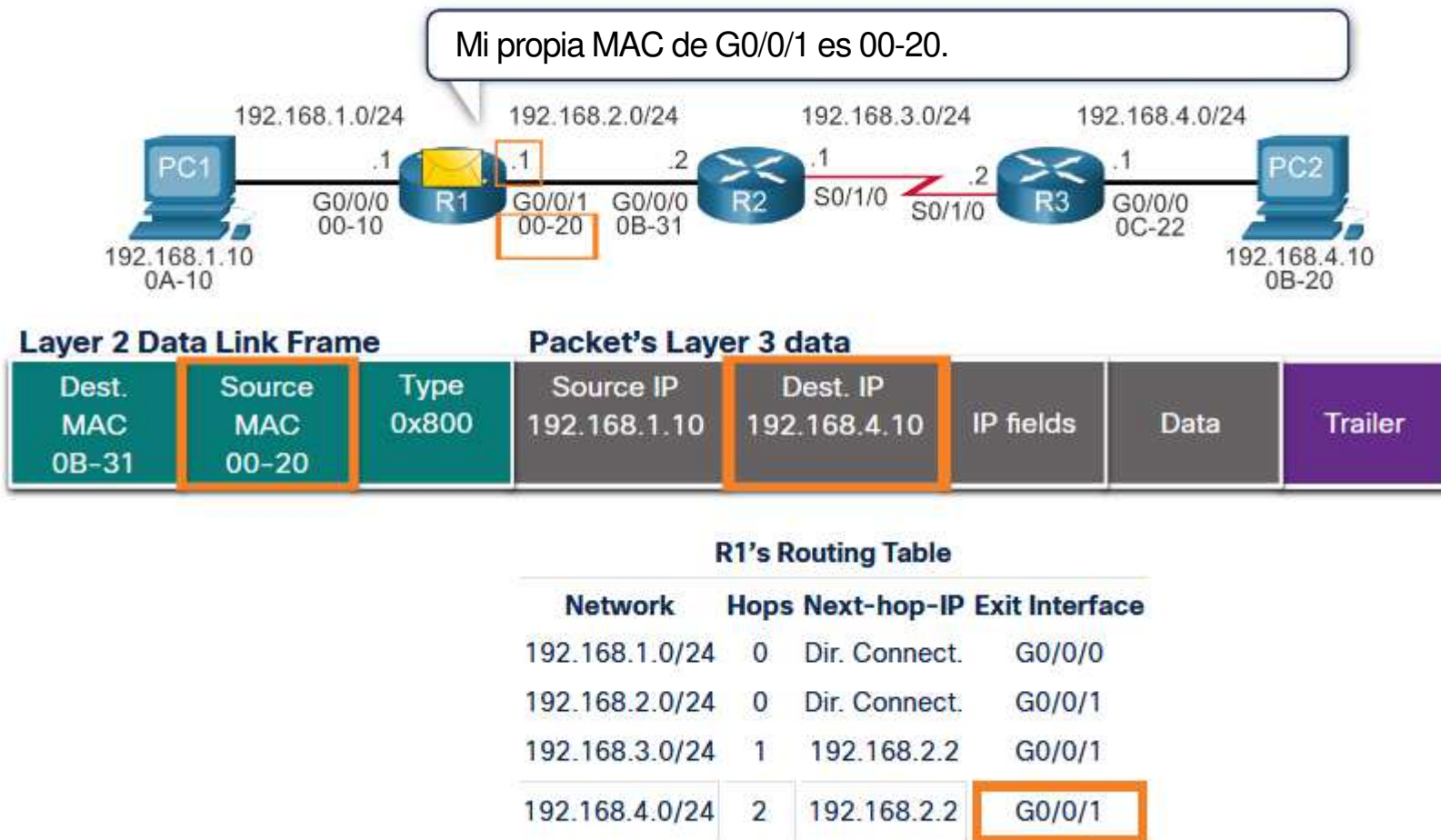
IP Address	MAC Address
192.168.2.2	0B-31

R1's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	0	Dir. Connect.	G0/0/0
192.168.2.0/24	0	Dir. Connect.	G0/0/1
192.168.3.0/24	1	192.168.2.2	G0/0/1
192.168.4.0/24	2	192.168.2.2	G0/0/1

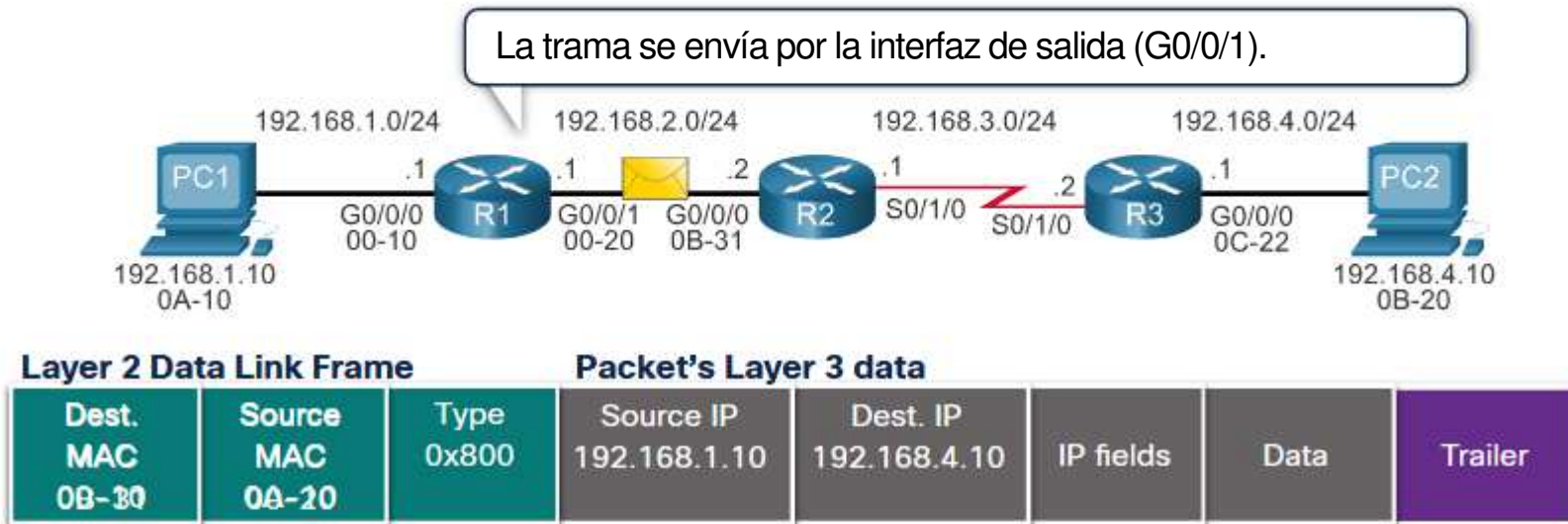
Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.



Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.

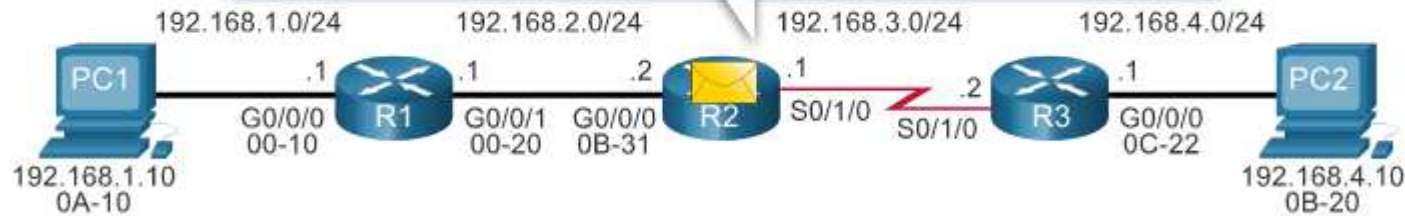


Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.

Me llega una trama a mi MAC, investigando:

Al ver el tipo de trama y dirección IP destino deduzco que el paquete requiere ser reenviado.



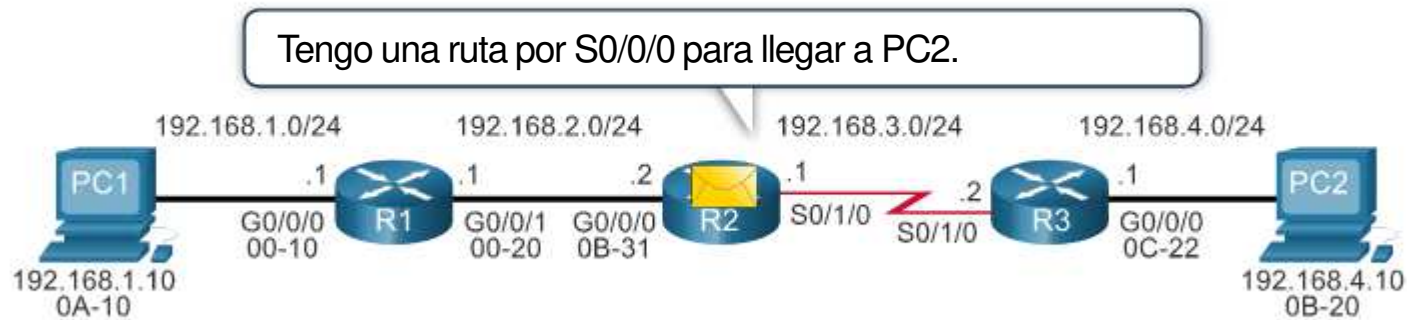
Dest MAC 0B-31	Source MAC 00-20	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
----------------------	------------------------	---------------	---------------------------	--------------------------	-----------	------	---------

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	G0/0/0
192.168.2.0/24	0	Dir. Connect.	G0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.168.3.2	S0/0/0

Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.



Dest MAC 0B-31	Source MAC 00-20		Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
----------------------	------------------------	--	---------------------------	--------------------------	-----------	------	---------

R3's Routing Table

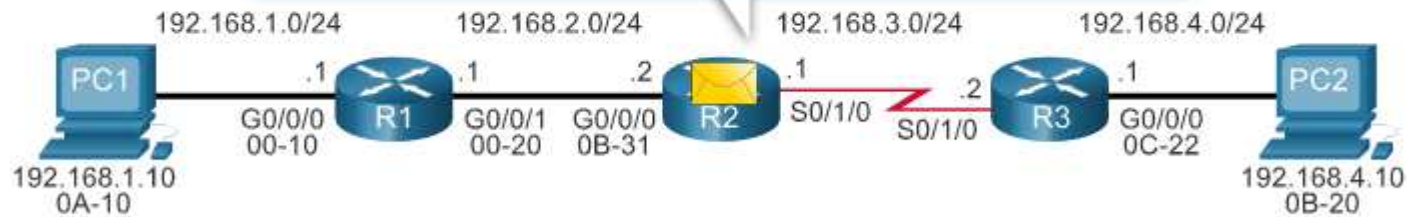
Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	G0/0/0
192.168.2.0/24	0	Dir. Connect.	G0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.168.3.2	S0/0/0

Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.

Necesario reconstruir la trama.

El paquete se enviará por un enlace serial, por lo que se coloca la dirección de broadcast como destino.



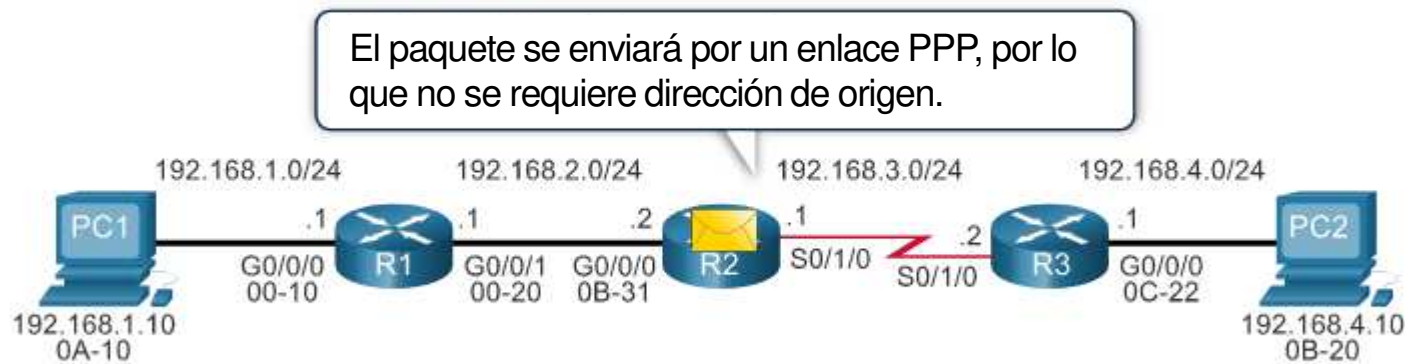
Address 0x8F 0B-31	Control 0x00 00-20	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
--------------------------	--------------------------	---------------	---------------------------	--------------------------	-----------	------	---------

R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	G0/0/0
192.168.2.0/24	0	Dir. Connect.	G0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.168.3.2	S0/0/0

Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.



Address 0x8F 0B-31	Control 0x00 00-20	Type 0x800	Source IP 192.168.1.10	Dest. IP 192.168.4.10	IP fields	Data	Trailer
--------------------------	--------------------------	---------------	---------------------------	--------------------------	-----------	------	---------

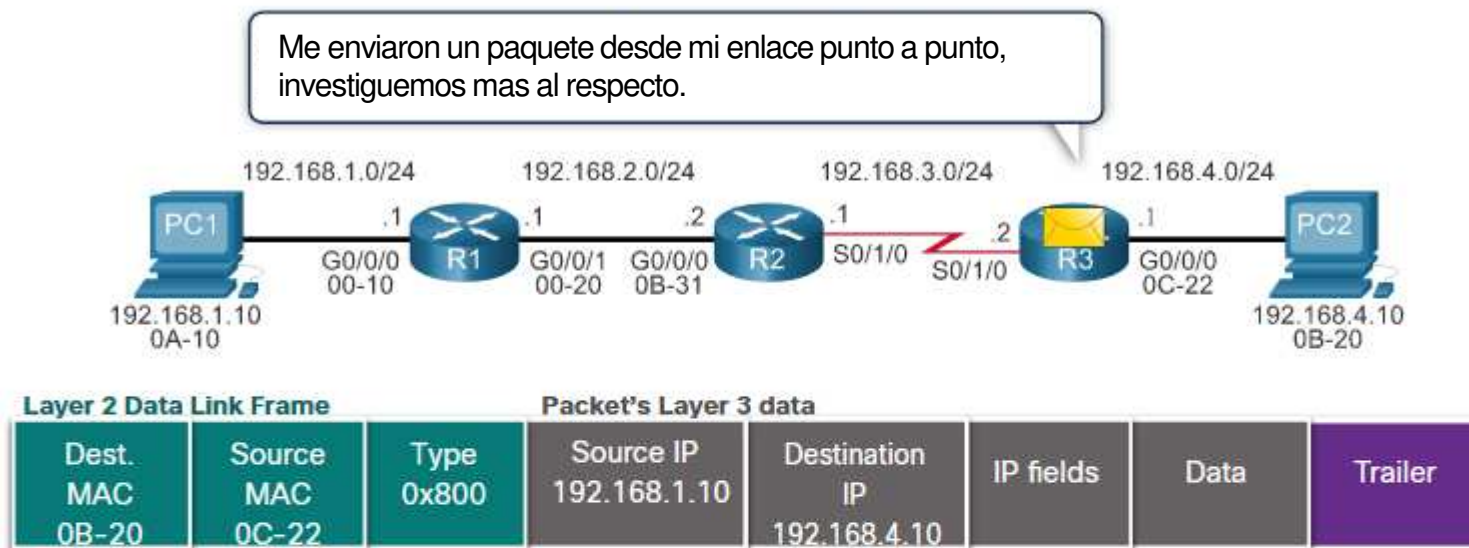
R3's Routing Table

Network	Hops	Next-hop-IP	Exit Interface
192.168.1.0/24	1	192.168.3.1	G0/0/0
192.168.2.0/24	0	Dir. Connect.	G0/0/0
192.168.3.0/24	0	Dir. Connect.	S0/0/0
192.168.4.0/24	1	192.168.3.2	S0/0/0

Reenvío de Paquetes

- Reenvío de Paquetes de Extremo a Extremo.

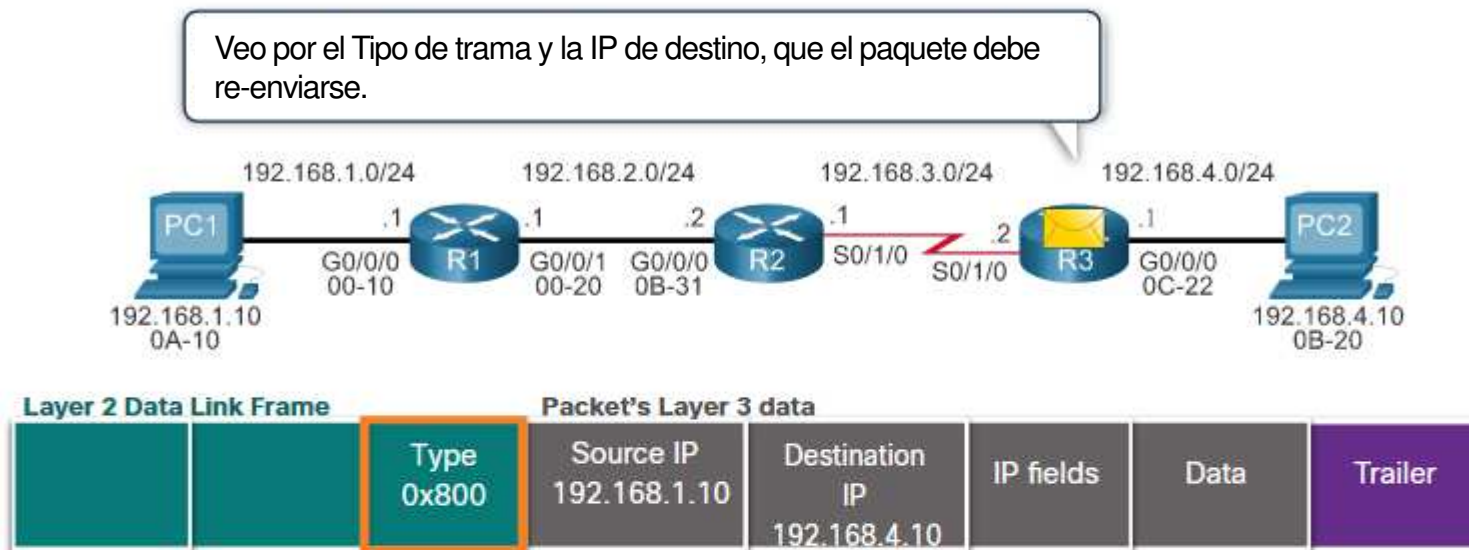
- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada.



Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada.

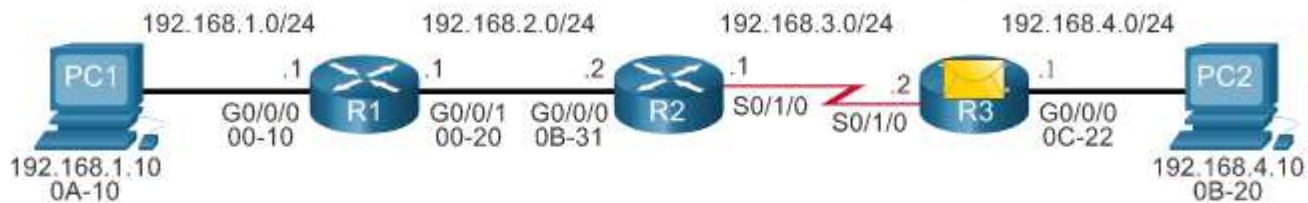


Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada.

Tengo una ruta por Fa0/0 para llegar a PC2.



R3's Routing Table

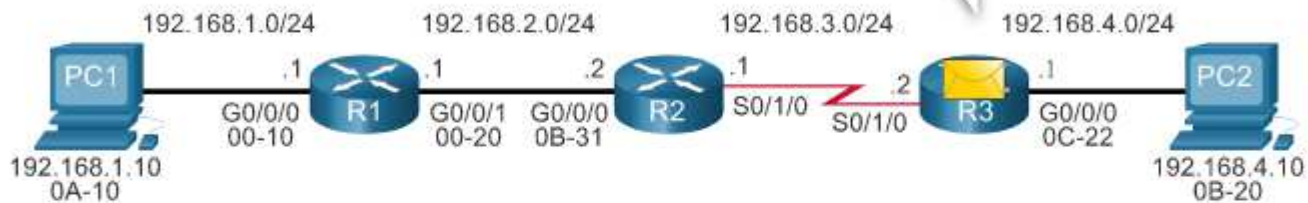
Network	Hops	Next-Hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Direct Connect	S0/0/0
192.168.4.0/24	0	Direct Connect	Fa0/0

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada.

Necesario reconstruir la trama.
Mi tabla ARP dice que la PC2 usa la MAC 0B-20. Enviémoslo.



Layer 2 Data Link Frame			Packet's Layer 3 data				
Dest. MAC 0B-20	Source MAC 0C-22	Type 0x800	Source IP 192.168.1.10	Destination IP 192.168.4.10	IP fields	Data	Trailer

IP Address	MAC Address
192.168.4.10	0B-20

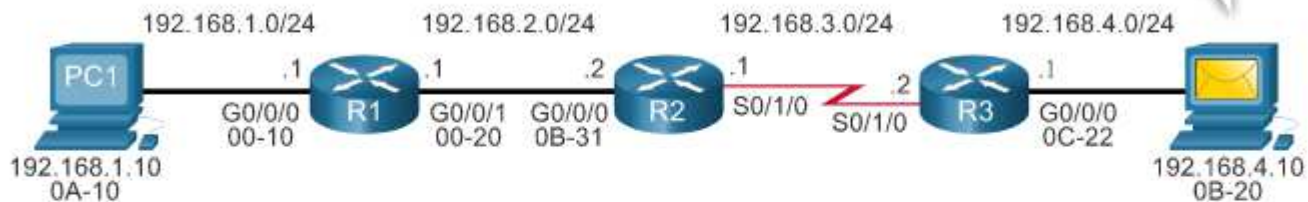
Network	Hops	Next-Hop-IP	Exit Interface
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Direct Connect	S0/0/0
192.168.4.0/24	0	Direct Connect	Fa0/0

Reenvío de Paquetes

- **Reenvío de Paquetes de Extremo a Extremo.**

- Es responsabilidad del reenvío de paquetes, encapsularlos en la trama apropiada.

Oh mira, enviaron una trama a mi MAC, veamos que trae.
El paquete indica en la IP destino que es para mi.

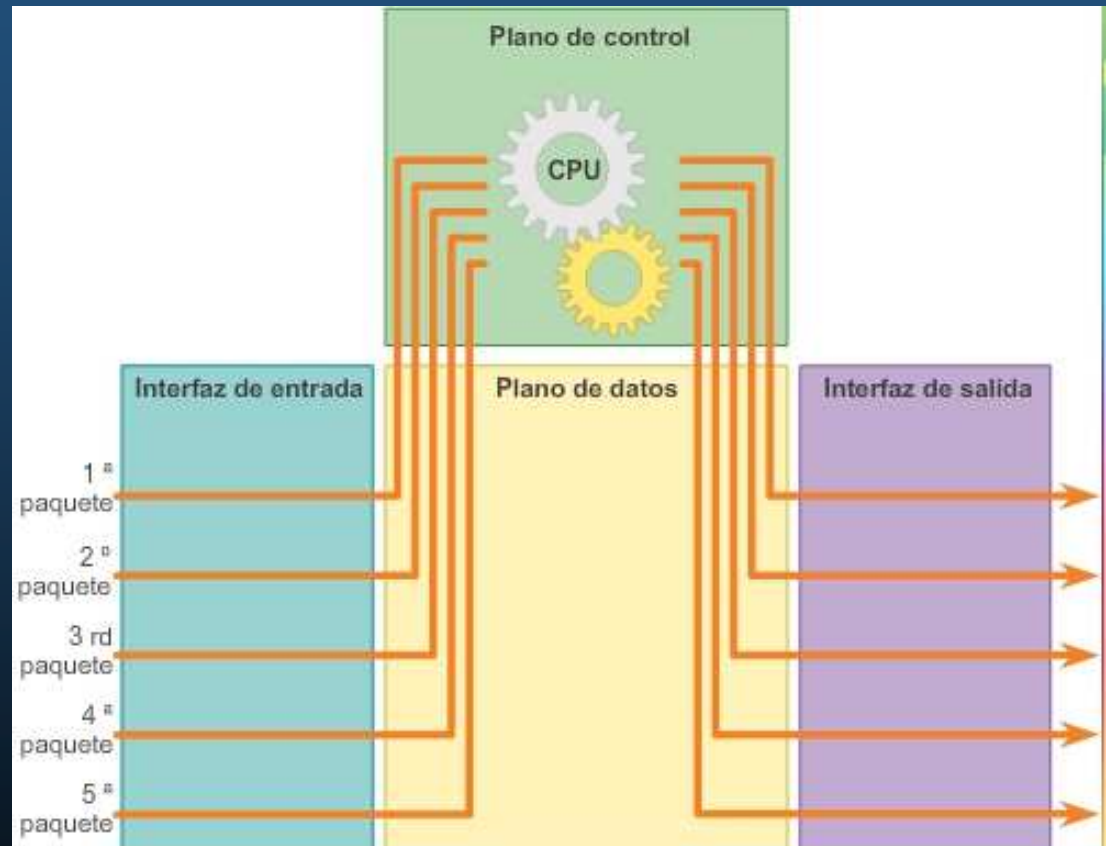


Layer 2 Data Link Frame

Layer 2 Data Link Frame			Packet's Layer 3 data				
Dest. MAC	Source MAC	Type	Source IP	Destination IP	IP fields	Data	Trailer
0B-20	0C-22	0x800	192.168.1.10	192.168.4.10			

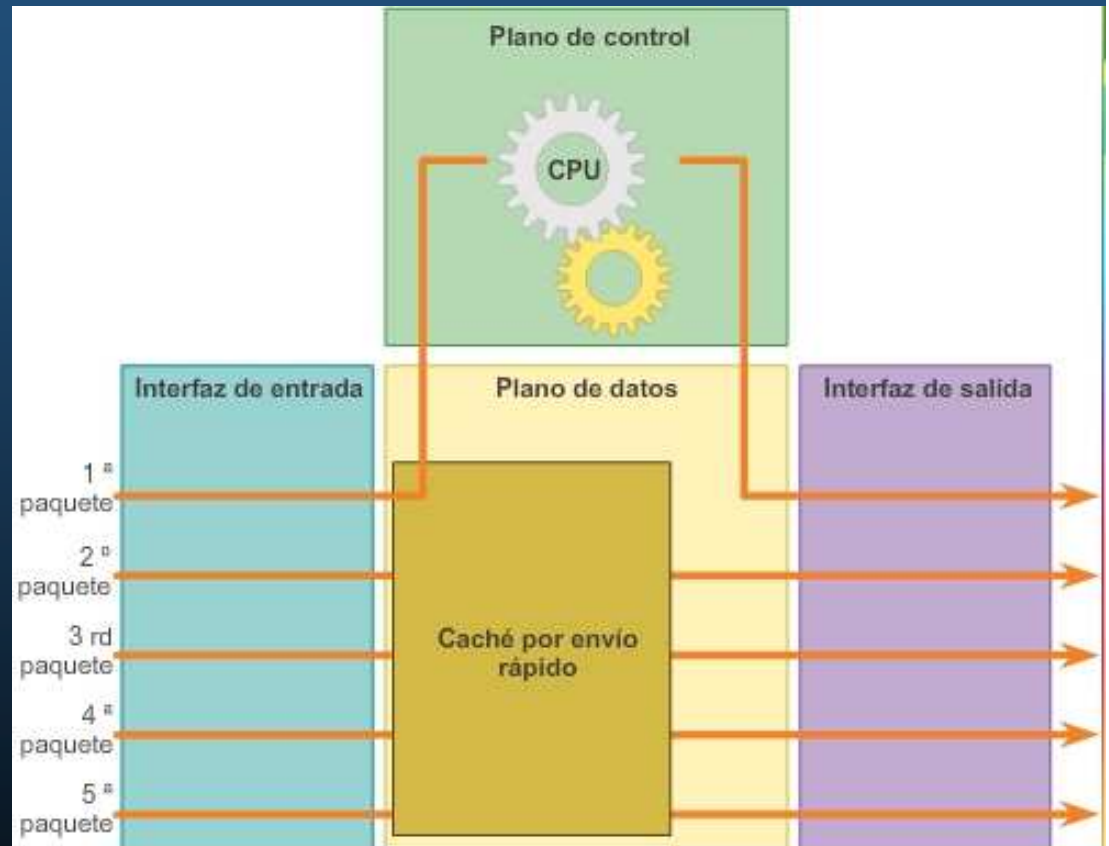
Reenvío de Paquetes

- Mecanismos de reenvío de paquetes.
- Switching de procesos:
Reenvío antiguo:
 - Paquete llega,
 - Reenvía a plano de control,
 - Checa dirección destino contra entradas de la tabla de routing,
 - Elige interfaz de salida,
 - Reenvía el paquete.



Reenvío de Paquetes

- Mecanismos de reenvío de paquetes.
- **Switching Rápido:**
Caché de switching rápido con información de siguiente salto.
 - Paquete llega y busca en caché.
 - Si existe, reenvía.
 - No existe, aplica reenvío antiguo a la interfaz de salida.
 - Y almacena información en caché para usarla después.



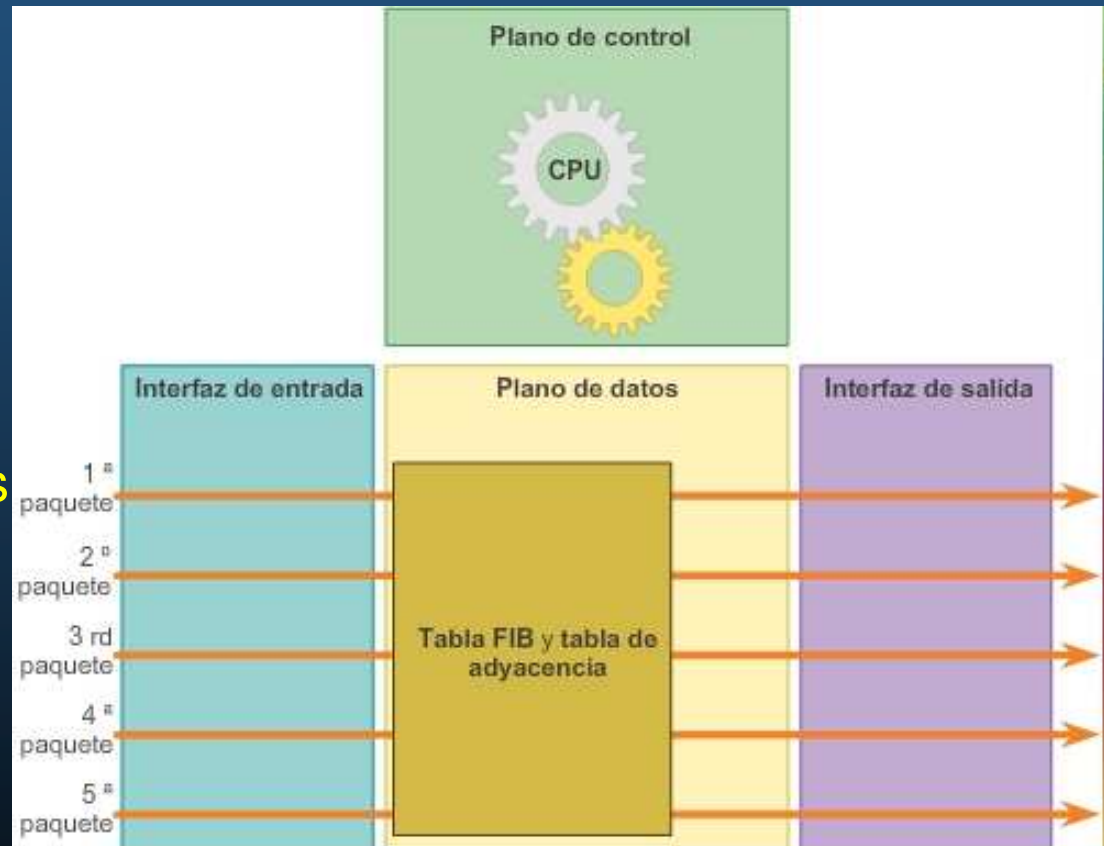
Reenvío de Paquetes

- Mecanismos de reenvío de paquetes.
- Cisco Express Forwarding (CEF):

- Arma base de información de reenvío (FIB) y una tabla de adyacencia.

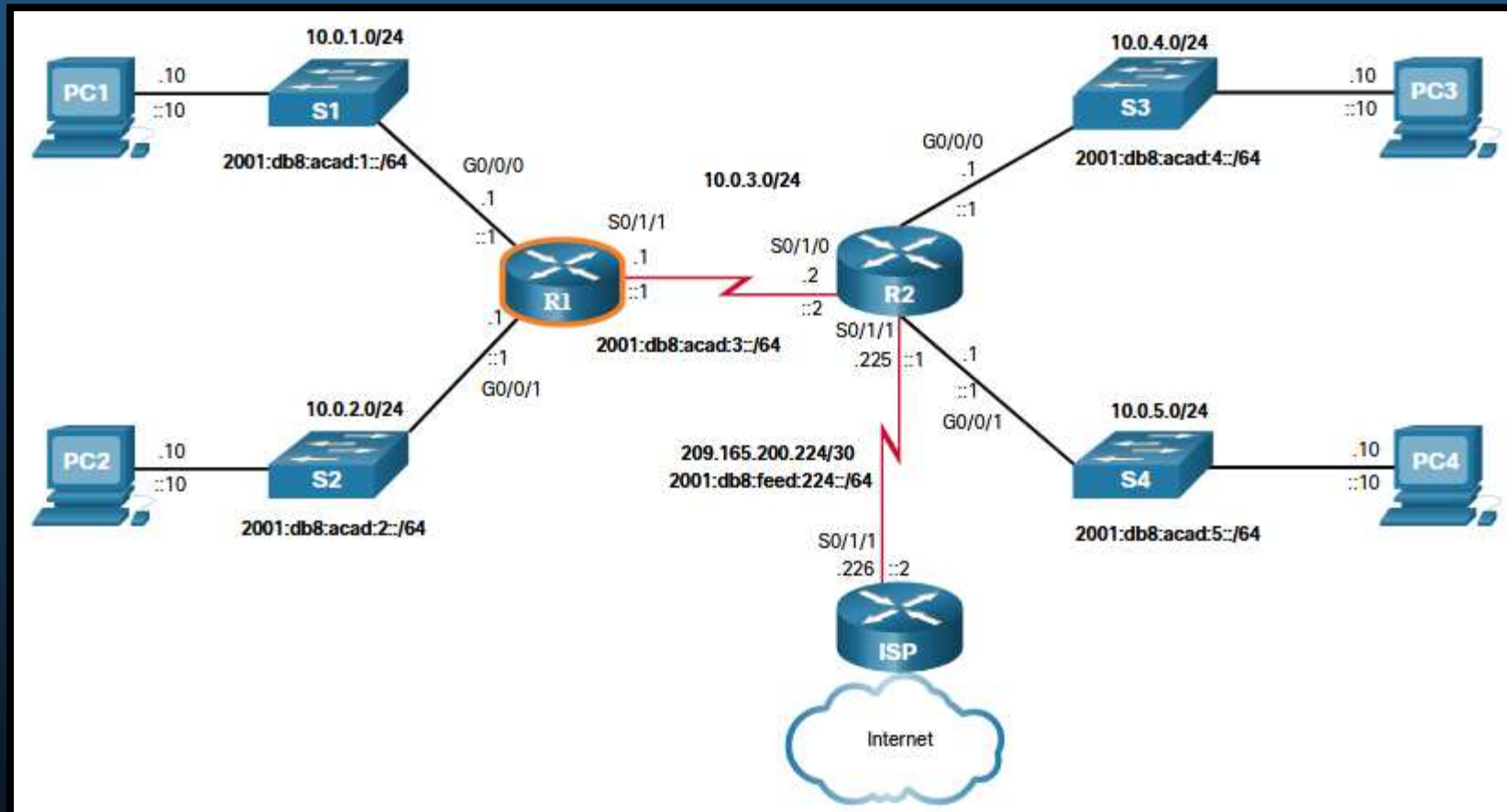
- Entradas se activan por cambios en la topología de la red.

- Converge una red, la FIB y las tablas de adyacencia contienen información para reenviar un paquete.



Revisión de la Configuración Básica de un Router

- Topología.



- Se usa la topología mostrada para revisar la configuración de un router y su verificación .

Revisión de la Configuración Básica de un Router

- Comandos de Configuración.

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config)#
```


Revisión de la Configuración Básica de un Router

- Comandos de Configuración.

```
R1(config)# ipv6 unicast-routing
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 10.0.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1:a link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 10.0.2.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1:b link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 10.0.3.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1:c link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

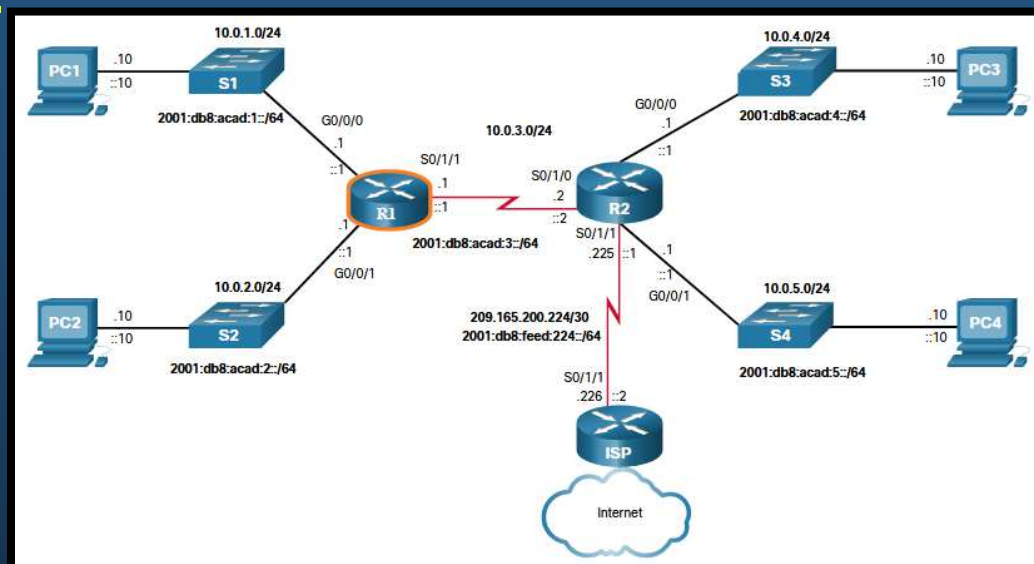
Revisión de la Configuración Básica de un Router

- Comandos de Verificación.
 - En cada caso es posible reemplazar **ip** por **ipv6**.
 - `show ip interface brief`
 - `show running-config interface interface-type number`
 - `show interfaces`
 - `show ip interface`
 - `show ip route`
 - `ping`

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- `show ip interface brief`



```
R1# show ip interface brief
```

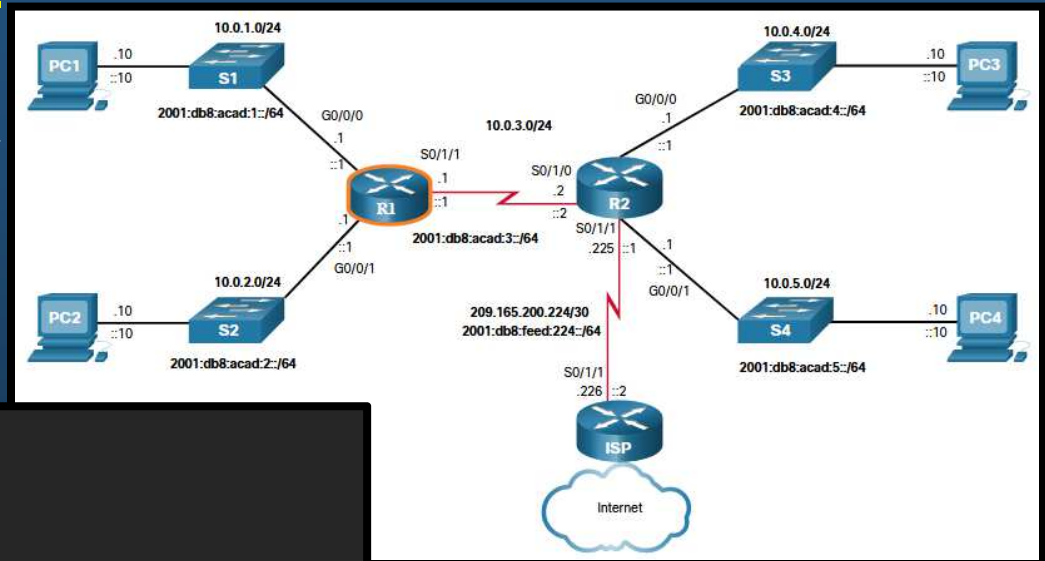
Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	10.0.1.1	YES	manual	up	up
GigabitEthernet0/0/1	10.0.2.1	YES	manual	up	up
Serial0/1/0	unassigned	YES	unset	administratively down	down
Serial0/1/1	10.0.3.1	YES	manual	up	up
GigabitEthernet0	unassigned	YES	unset	down	down

```
R1#
```

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- show ipv6 interface brief

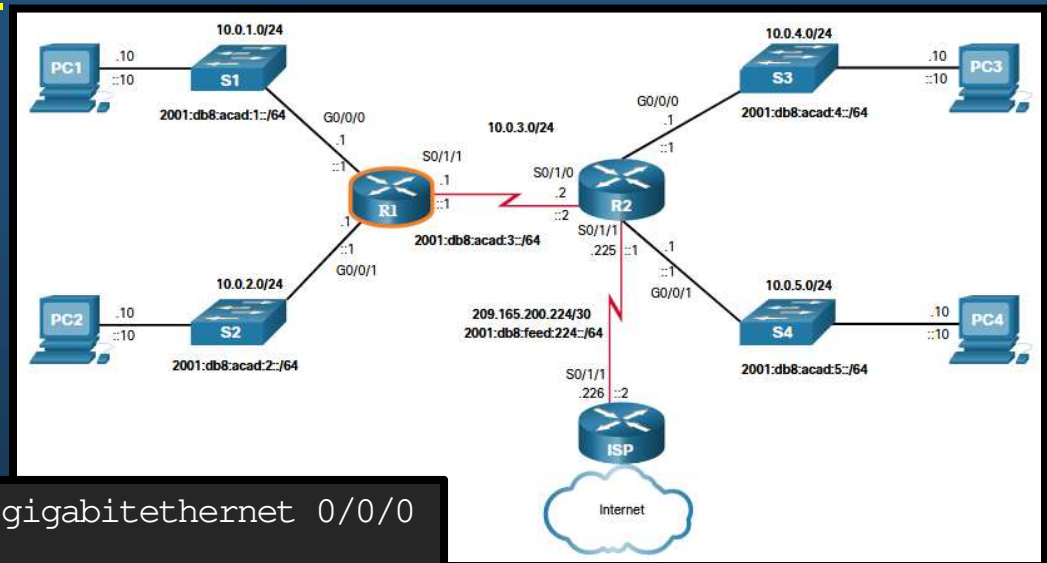


```
R1# show ipv6 interface brief
GigabitEthernet0/0/0    [up/up]
    FE80::1:A
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1    [up/up]
    FE80::1:B
    2001:DB8:ACAD:2::1
Serial0/1/0              [administratively down/down]
    unassigned
Serial0/1/1              [up/up]
    FE80::1:C
    2001:DB8:ACAD:3::1
GigabitEthernet0        [down/down]
    unassigned
R1#
```

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- `show running-config interface interface-type number`



```
R1# show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 189 bytes
!
interface GigabitEthernet0/0/0
  description Link to LAN 1
  ip address 10.0.1.1 255.255.255.0
  negotiation auto
  ipv6 address FE80::1:A link-local
  ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

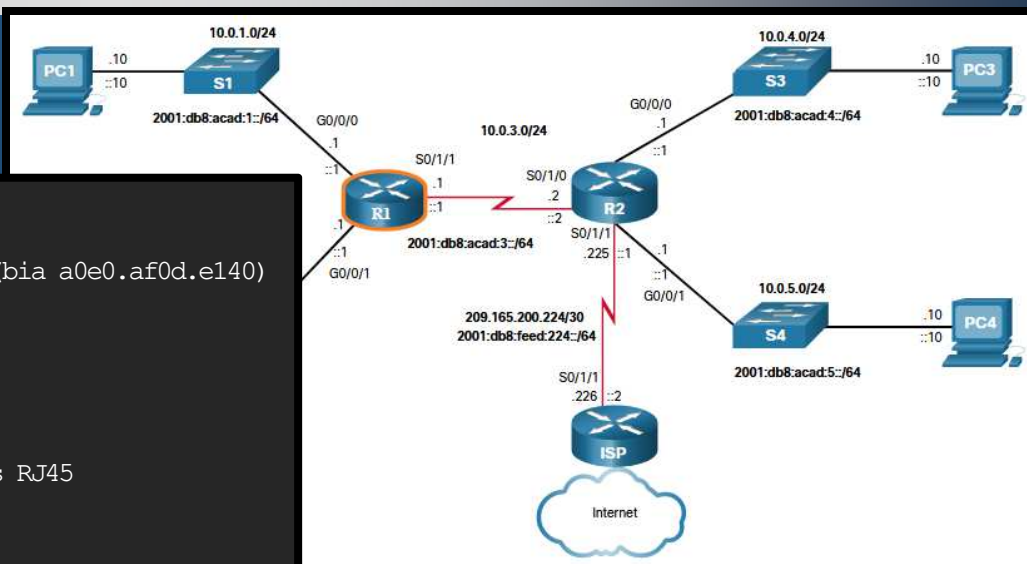
Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- show interfaces**

```
R1# show interfaces gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia a0e0.af0d.e140)
  Internet address is 10.0.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    57793 packets input, 10528767 bytes, 0 no buffer
    Received 19711 broadcasts (0 IP multicasts)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 36766 multicast, 0 pause input
    10350 packets output, 1280030 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      0 unknown protocol drops
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

R1#

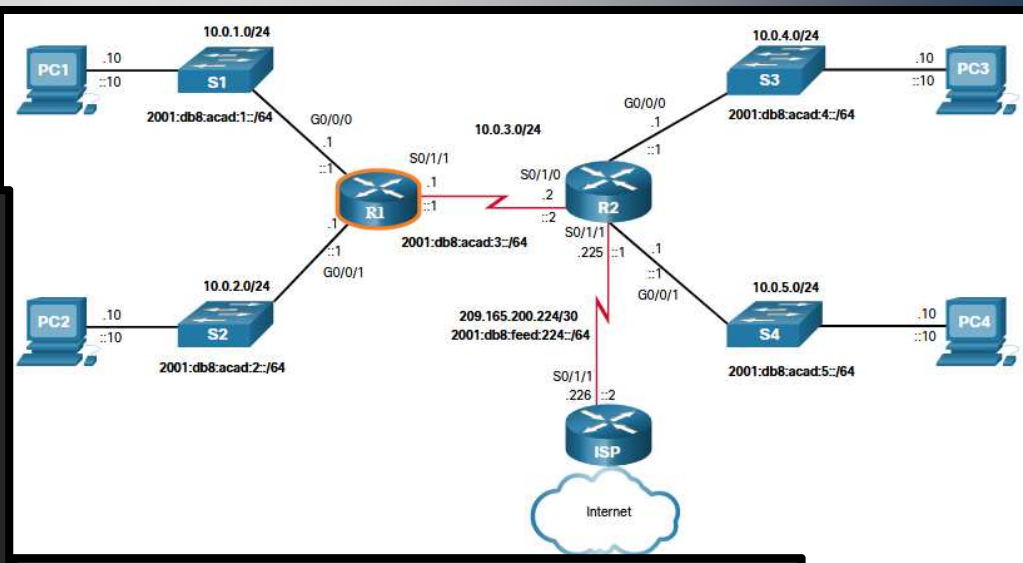


Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- show ip interface**

```
R1# show ip interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 10.0.1.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Multicast reserved groups joined: 224.0.0.5 224.0.0.6
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
  Topology "base", operation state is UP
...
```



```
...
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
IPv4 WCCP Redirect outbound is disabled
IPv4 WCCP Redirect inbound is disabled
IPv4 WCCP Redirect exclude is disabled
```

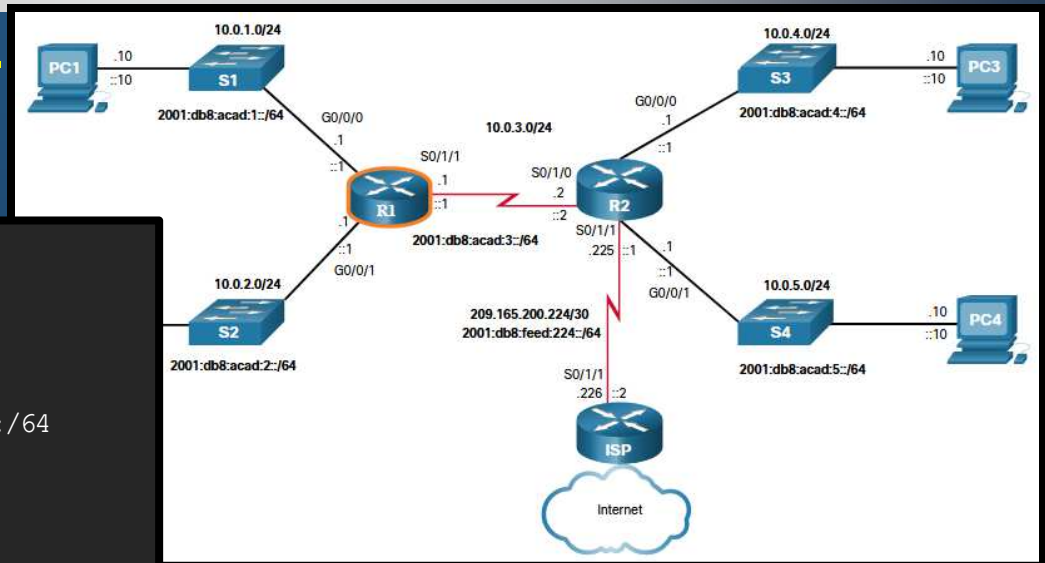
R1#

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.
 - `show ipv6 interface`

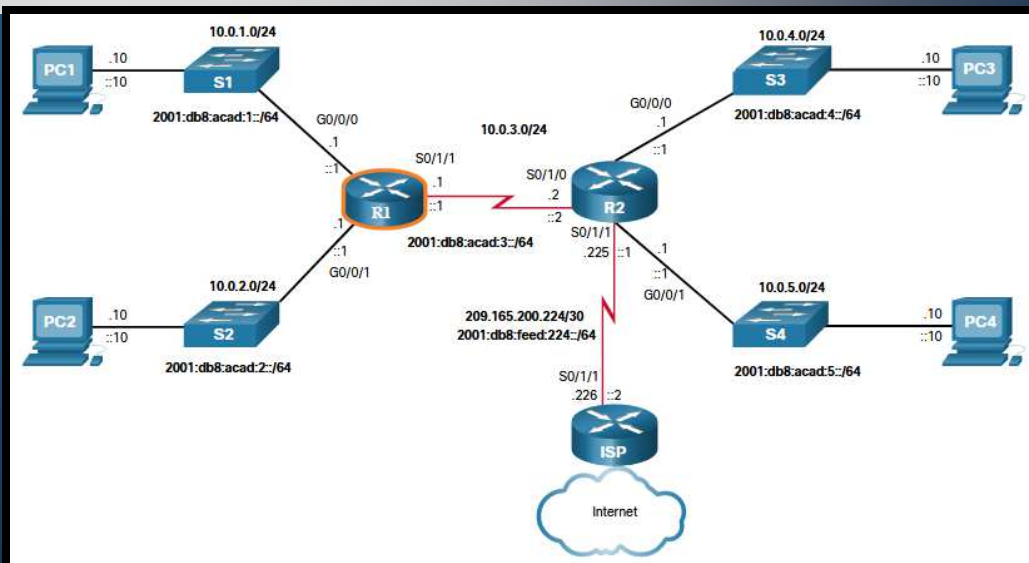
```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::1:A
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::5
  FF02::6
  FF02::1:FF00:1
  FF02::1:FF01:A
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.
```

R1#



Revisión de la Configuración Básica de un Router

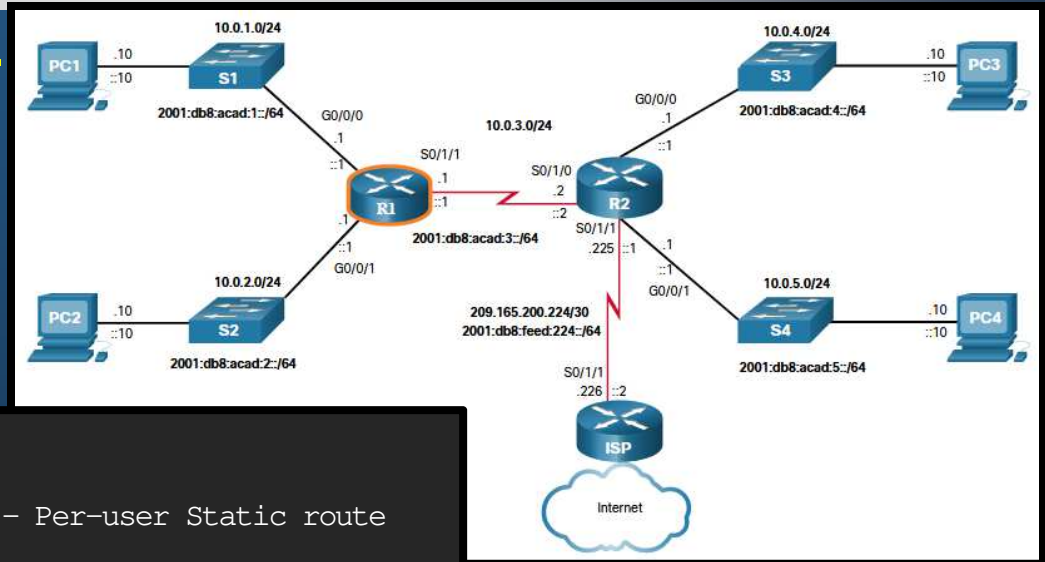
- Comandos de Verificación.
 - `show ip route`



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(Output omitted)
Gateway of last resort is not set
  10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L       10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C       10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L       10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C       10.0.3.0/24 is directly connected, Serial0/1/1
L       10.0.3.1/32 is directly connected, Serial0/1/1
R1#
```

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.
 - `show ipv6 route`

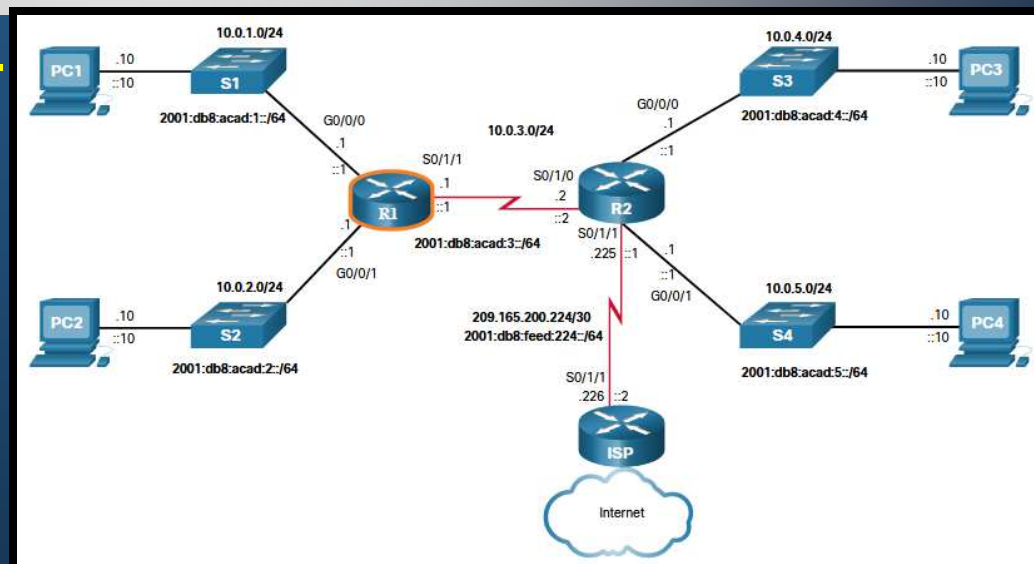


```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)
C 2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
   via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
   via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
   via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
   via Serial0/1/1, receive
L FF00::/8 [0/0]
   via Null0, receive
R1#
```

Revisión de la Configuración Básica de un Router

- Comandos de Verificación.

- ping



```
R1# ping 10.0.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms
R1# ping 2001:db8:acad:3::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:3::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/2 ms
R1#
```

Revisión de la Configuración Básica de un Router

- Filtrado de la Salida de Comandos.
 - `show` puede filtrarse con (|) y uno de los siguientes modificadores:
 - section: muestra la sección completa que comienza con la expresión de filtrado.
 - include: incluye todas las líneas de salida que coinciden con la expresión de filtrado.
 - exclude: excluye todas las líneas de salida que coinciden con la expresión de filtrado.
 - begin: muestra todas las líneas de salida desde un punto determinado, comenzando con la línea que coincide con la expresión de filtrado.

Revisión de la Configuración Básica de un Router

- Filtrado de la Salida de Comandos.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 121A0C0411044C
 login
 transport input telnet ssh
R1#
R1# show ipv6 interface brief | include up
GigabitEthernet0/0/0 [up/up]
GigabitEthernet0/0/1 [up/up]
Serial0/1/1 [up/up]
R1#
R1# show ip interface brief | exclude unassigned
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 192.168.10.1 YES manual up up
GigabitEthernet0/0/1 192.168.11.1 YES manual up up
Serial0/1/1 209.165.200.225 YES manual up up
R1#
R1# show ip route | begin Gateway
Gateway of last resort is not set
 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L   192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
 192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L   192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/1/1
L   209.165.200.225/32 is directly connected, Serial0/1/1
R1#
```

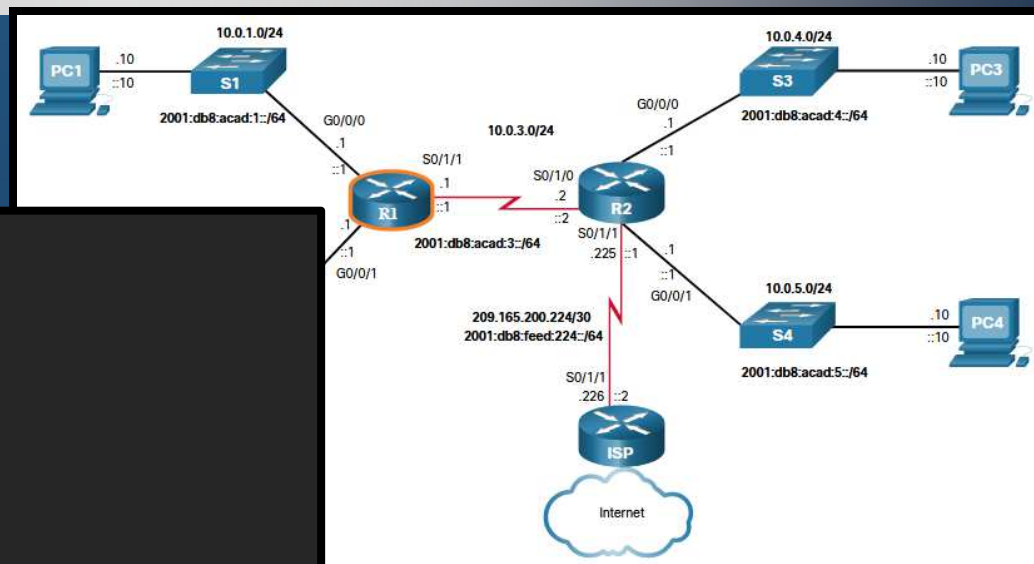


Tabla de Enrutamiento IP

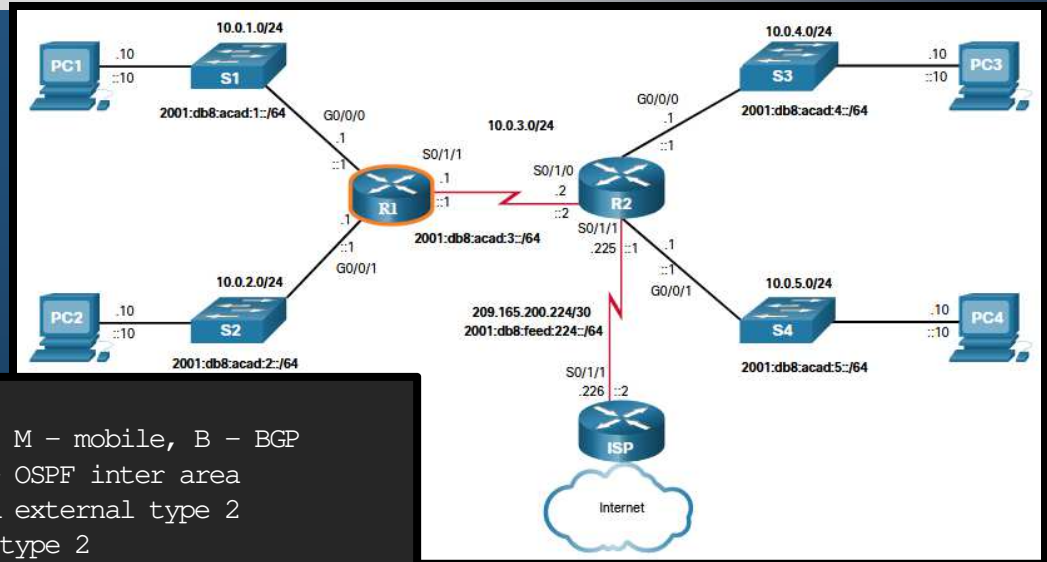
- Orígenes de Ruta.

- La tabla de enrutamiento contiene una lista de rutas hacia redes conocidas.
 - Incluye prefijos y sus longitudes
- Su origen puede provenir de cualquiera de los siguientes orígenes:
 - Redes directamente conectadas
 - Rutas estáticas
 - Protocolos de Enrutamiento Dinámico.
- El origen de cada ruta se identifica por un código:
 - L: dirección asignada a una interfaz del router. Le permite determinar si un paquete está destinado a su interfaz (no requiere reenviarlo).
 - C: red conectada directamente.
 - S: ruta estática creada para llegar a una red específica.
 - O - red aprendida dinámicamente desde otro enrutador utilizando el protocolo de enrutamiento OSPF.
 - * - Esta ruta es candidata para una ruta predeterminada.

Tabla de Enrutamiento IP

- Orígenes de Ruta.

- Ejemplo: R1# show ip route



```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

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

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

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
```

```
a - application route
```

```
+ - replicated route, % - next hop override, p - overrides from PfR
```

```
Gateway of last resort is 10.0.3.2 to network 0.0.0.0
```

```
O*E2 0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
```

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
```

```
C 10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
```

```
L 10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
```

```
C 10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
```

```
L 10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
```

```
C 10.0.3.0/24 is directly connected, Serial0/1/1
```

```
L 10.0.3.1/32 is directly connected, Serial0/1/1
```

```
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
```

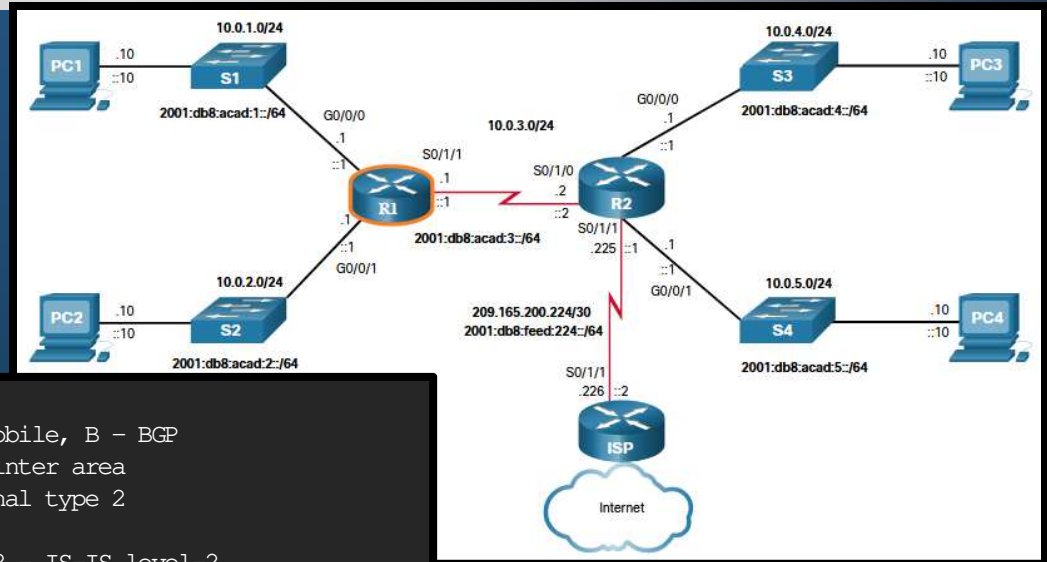
```
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
```

```
R1#
```

Tabla de Enrutamiento IP

- Orígenes de Ruta.

- Ejemplo: R2# show ip route



```
R2# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

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

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

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

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

```
S* 0.0.0.0/0 [1/0] via 209.165.200.226
```

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
```

```
O 10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
```

```
O 10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
```

```
C 10.0.3.0/24 is directly connected, Serial0/1/0
```

```
L 10.0.3.2/32 is directly connected, Serial0/1/0
```

```
C 10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
```

```
L 10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
```

```
C 10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
```

```
L 10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
```

```
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 209.165.200.224/30 is directly connected, Serial0/1/1
```

```
L 209.165.200.225/32 is directly connected, Serial0/1/1
```

```
R2#
```

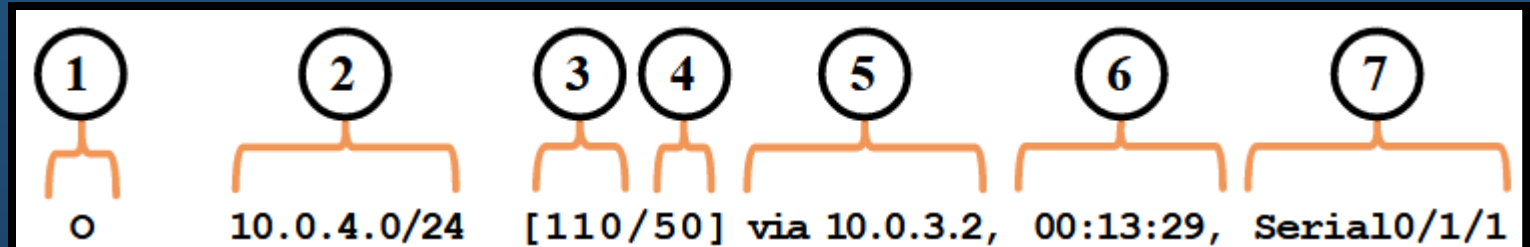

Tabla de Enrutamiento IP

- Principios de la Tabla de Enrutamiento.
 - Cada enrutador toma su decisión solo, con la información de su tabla de enrutamiento.
 - R1 solo puede reenviar usando su propia tabla de enrutamiento.
 - R1 no conoce las rutas en las tablas de enrutamiento de otros routers (cómo, R2).
 - La información en una tabla de enrutamiento no necesariamente coincide con la de otro router.
 - El que R1 tenga una ruta a una red a través de R2, no significa que R2 conozca esa misma red.
 - La información de enrutamiento sobre una ruta no proporciona información de enrutamiento para el retorno.
 - R1 recibe un paquete para PC1 desde PC3. El que R1 sepa reenviar el paquete a su destino (por G0/0/0) no significa que sepa reenviar paquetes de respuesta desde PC1 a PC3.

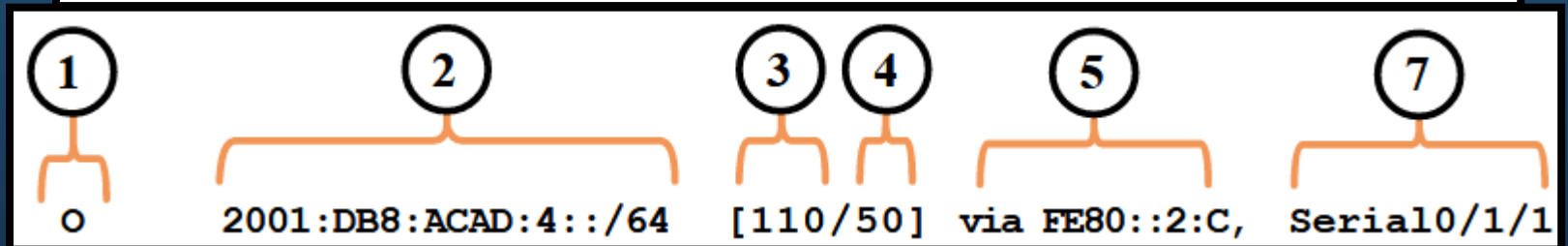
Tabla de Enrutamiento IP

- Entradas de la Tabla de Enrutamiento.

- IPv4



- IPv6



- 1. Origen de la ruta:** identifica cómo se aprendió la ruta.
- 2. Red de destino** (prefijo y longitud del prefijo): identifica la dirección de la red remota.
- 3. Distancia administrativa:** confiabilidad de la ruta. Valores más bajos, preferibles.
- 4. Métrica:** costo para llegar a la red remota. Valores más bajos, preferibles.
- 5. Next-hop:** dirección IP del siguiente enrutador al que se reenviará el paquete.
- 6. Marca de tiempo de ruta:** tiempo que ha pasado desde que se aprendió la ruta.
- 7. Interfaz de salida:** interfaz de salida para que los paquetes salientes lleguen a su destino final.

Tabla de Enrutamiento IP

- Interfaces Directamente Conectadas.
 - Para ser aprendida, se deben cumplir con los siguientes requisitos:
 - Se le debe **asignar** una dirección **IPv4 o IPv6** válida.
 - Se debe **activar** mediante el comando: **no shutdown**.
 - Debe recibir una señal **portadora** de otro dispositivo (router, switch, host, etc.).
 - Interfaz **activa**, implica **red incorporada a tabla de routing incluyendo**:
 - **Origen de ruta**: Modo en que se descubrió la ruta.
 - “C” Red **Conectada** directamente y
 - “L” Dirección IP de la **interfaz local del router**.
 - **Red de destino**: direcciones de la **red / interfaz**.
 - **Interfaz de salida**: Por la que se configuró la IP.

Tabla de Enrutamiento IP

- Interfaces Directamente Conectadas.
 - Ejemplo:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(Output omitted)
C      10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L      10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
R1#
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)

C  2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
R1#
```

Tabla de Enrutamiento IP

- Rutas Estáticas.

- Se configuran de forma **manual**.
- Ruta **explícita** entre redes.
- No se **actualizan automáticamente**.
- No **interfieren** con el **ancho de banda** de los enlaces.
- Se identifican en la tabla de routing con el código "S"

- Ruta estática **a una red específica**

- `(config)# ip[v6] route prefijo long-pref {siguiente-salto | int-salida}`

- Ruta estática **predeterminada**

- `(config)# ip route 0.0.0.0 0.0.0.0 {siguiente-salto | int-salida}`
- `(config)# ip route ::/0 {siguiente-salto | int-salida}`

Tabla de Enrutamiento IP

- **Rutas Estáticas.**

- Enrutan hacia y desde redes stub (extremo final). Red a la que se accede por una única ruta, y el enrutador solo tiene un vecino.
 - Cualquier red conectada a R1 solo tendría una forma de llegar a otros destinos (R2 o más allá de R2).
 - 10.0.1.0/24 y 10.0.2.0/24 son redes stub y R1 es un router stub.

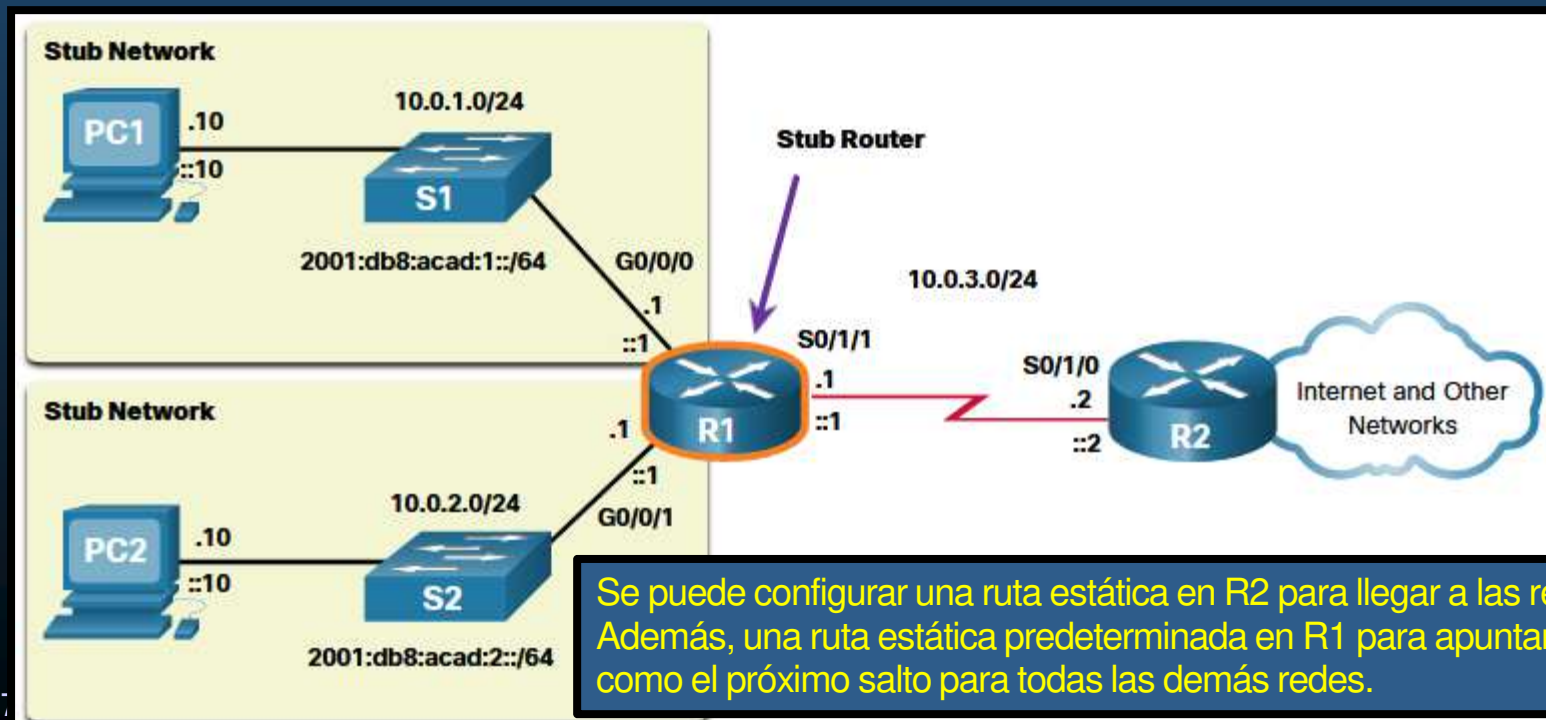
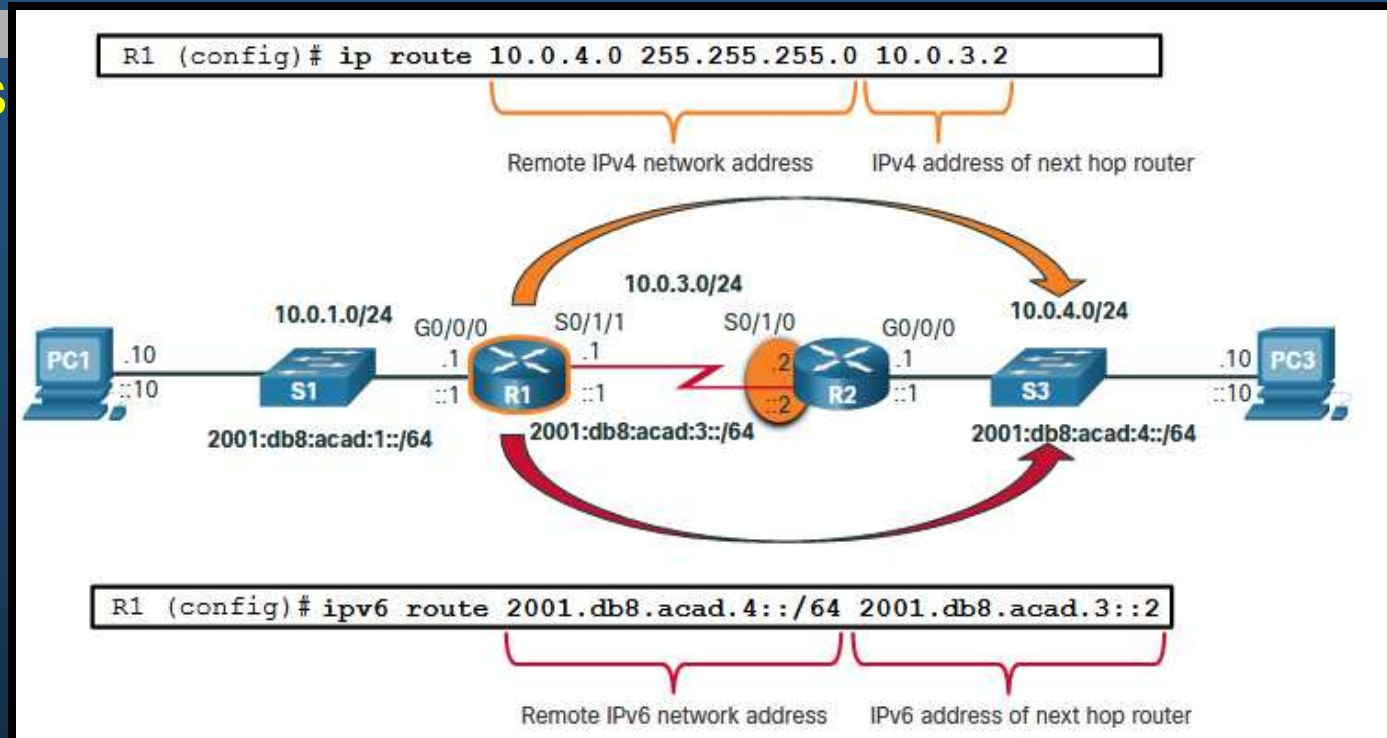


Tabla de Enrutamiento IP

- Rutas Estáticas en la Tabla de Enrutamiento IP.

- Considere la configuración de la siguiente topología:

- Ello generará las **entradas estáticas** mostradas en la **tabla de enrutamiento**:



```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(output omitted)
```

```
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
```

```
S      10.0.4.0/24 [1/0] via 10.0.3.2
```

```
R1# show ipv6 route static
```

```
IPv6 Routing Table - default - 8 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(output omitted)
```

```
S      2001:DB8:ACAD:4::/64 [1/0]
         via 2001:DB8:ACAD:3::2
```

Tabla de Enrutamiento IP

- **Protocolos** de enrutamiento dinámico

- **Compartir información** sobre conexión de redes remotas.
- **Detección** de redes y el **mantenimiento** de las **tablas de routing**.
- Identifica **redes descubiertas** por un **protocolo** de routing dinámico **específico**.
- **Convergen** una vez que **finalizan el intercambio y actualización** sus tablas de routing.

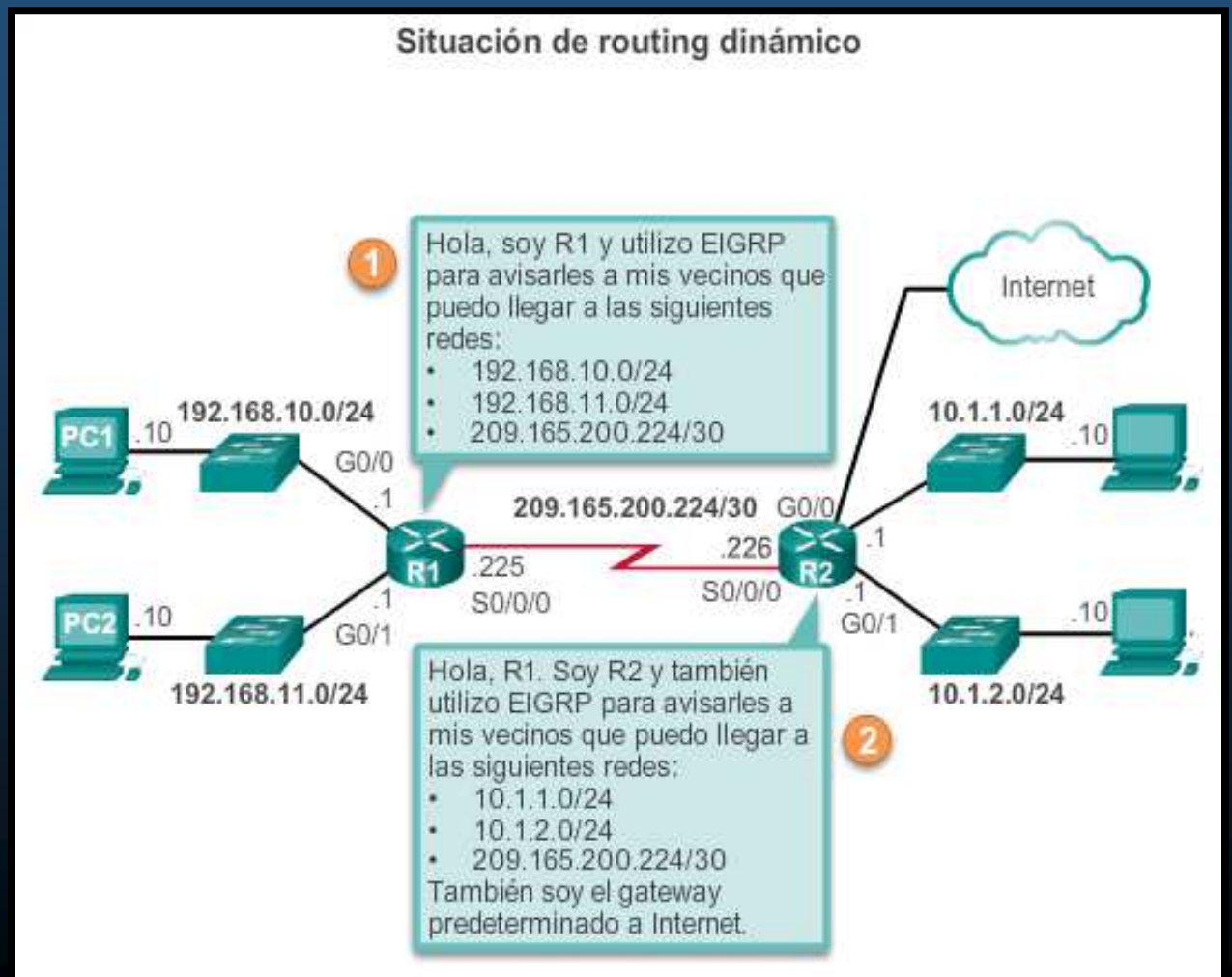


Tabla de Enrutamiento IP

- Protocolos de Enrutamiento Dinámico.
 - Permiten a los routes compartir información sobre sus redes remotas.

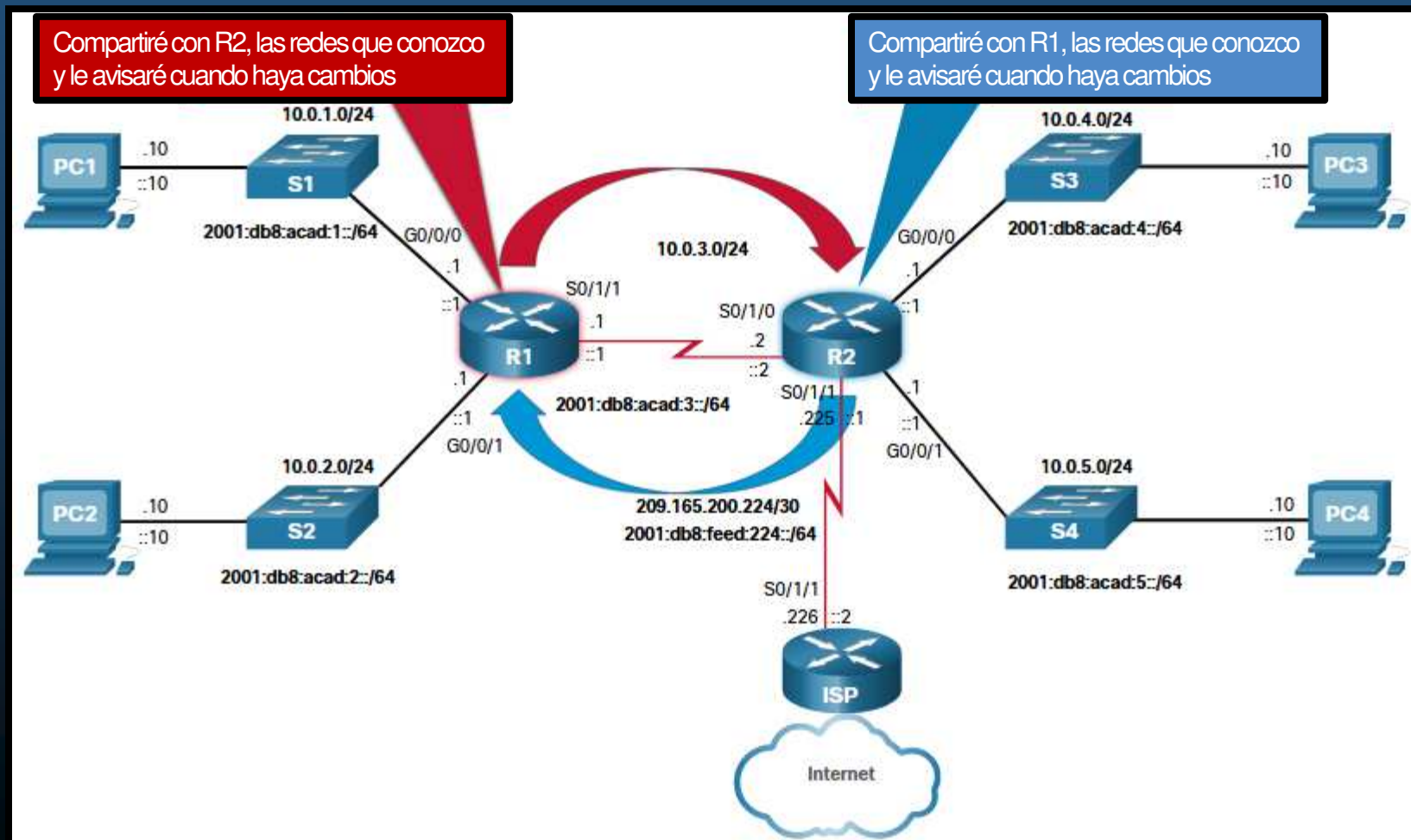


Tabla de Enrutamiento IP

- **Protocolos de Enrutamiento Dinámico en la Tabla de Enrutamiento IP.**
 - Considere que en lugar de realizar la **configuración estática de la topología**, se utiliza **OSPF como protocolo de enrutamiento dinámico**.
 - Ello generará las **entradas dinámicas mostradas en la tabla de enrutamiento**:

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
(output omitted for brevity)
O       10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O       10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O       2001:DB8:ACAD:4::/64 [110/50]
       via FE80::2:C, Serial0/1/1
O       2001:DB8:ACAD:5::/64 [110/50]
       via FE80::2:C, Serial0/1/1
```

Tabla de Enrutamiento IP

- Ruta por Defecto (Predeterminada).
 - Similar a un gateway en un host.
 - Define el siguiente salto a utilizar cuando no hay otras coincidencias en la tabla de enrutamiento.
 - Puede aprenderse estáticamente o por protocolos de enrutamiento dinámico.
 - Permite reducir el tamaño de las tablas de enrutamiento.
 - Consta de sólo ceros en el prefijo y la longitud.
 - IPv4: 0.0.0.0 /0
 - IPv6: ::/0
 - Útil cuando un router sólo tiene redes directamente conectadas y una salida al ISP.

Tabla de Enrutamiento IP

- Ruta por Defecto (Predeterminada).

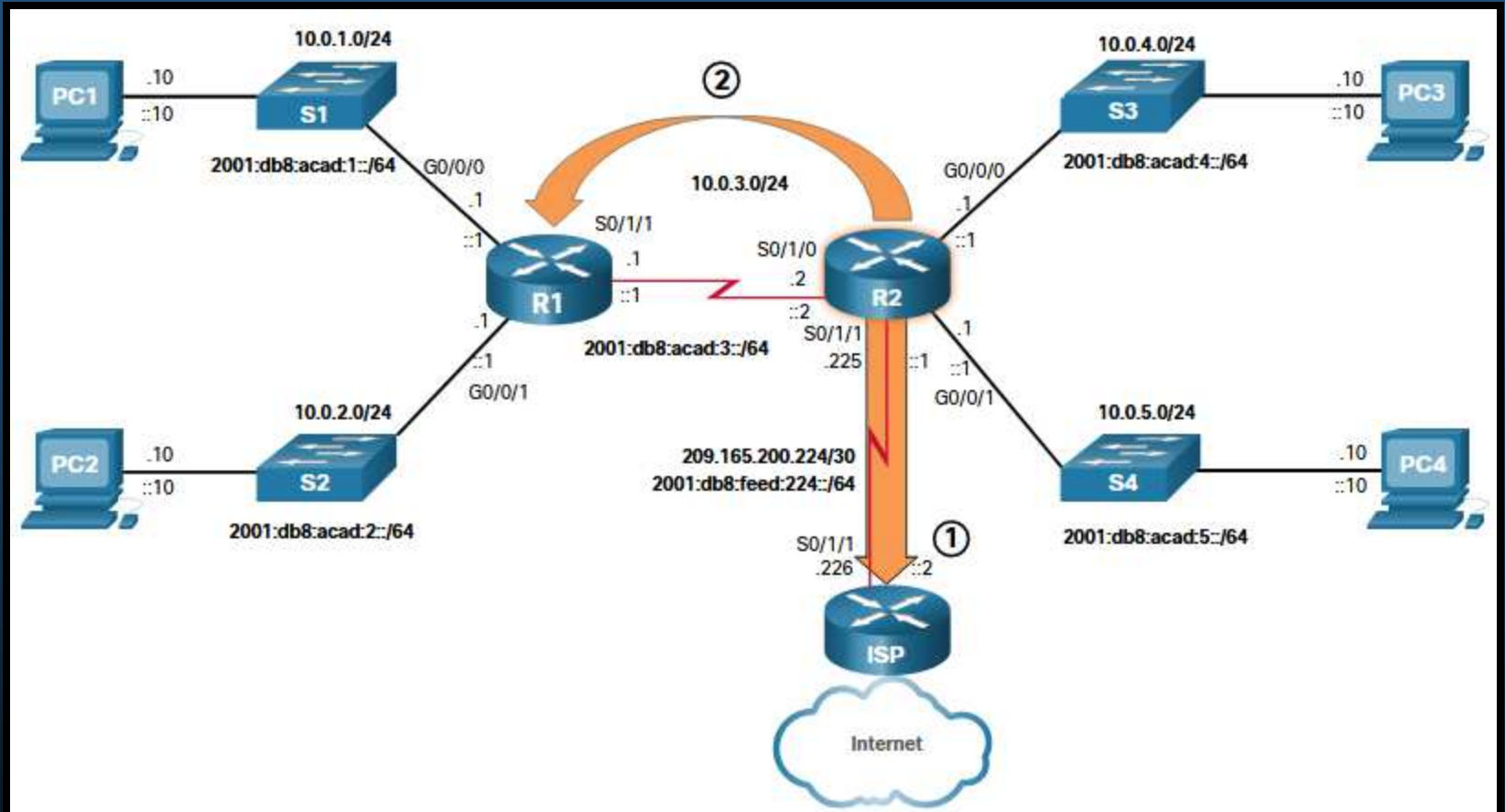


Tabla de Enrutamiento IP

- Ruta por Defecto (Predeterminada).
 - La imagen muestra la tabla de enrutamiento de R2:

```
R2# show ip route
(Output omitted)
S*    0.0.0.0/0 [1/0] via 209.165.200.226
R2#
R2# show ipv6 route
(Output omitted)
S     ::/0 [1/0]
      via 2001:DB8:FEED:224::2
R2#
```

Tabla de Enrutamiento IP

- Estructura de una Tabla de Enrutamiento IPv4.
 - Aún utiliza estructura ClassFull (direccionamiento de principios de los 80s).
 - Aunque ya no se usan clases, se mantiene la estructura para buscar coincidencias.
 - Dos niveles:
 - Justificado: Ruta padre, red ClassFull.
 - Indentado: Ruta hija, subred de una red ClassFull, directamente conectada, local.
 - Incluye información de origen y re-envío.

```
Router# show ip route
(Output omitted)
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.12.0/30 is directly connected, Serial0/0/0
L    192.168.12.1/32 is directly connected, Serial0/0/0
  192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.13.0/30 is directly connected, Serial0/0/1
L    192.168.13.1/32 is directly connected, Serial0/0/1
  192.168.23.0/30 is subnetted, 1 subnets
O    192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
Router#
```

Tabla de Enrutamiento IP

- Estructura de una Tabla de Enrutamiento IPv6.
 - Cada entrada tiene el mismo formato y alineación (nunca se definieron clases IPv6).

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
    via FE80::2:C, Serial0/0/1
C   2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/1/1, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/1/1, receive
O   2001:DB8:ACAD:4::/64 [110/50]
    via FE80::2:C, Serial0/1/1
O   2001:DB8:ACAD:5::/64 [110/50]
    via FE80::2:C, Serial0/1/1
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

Tabla de Enrutamiento IP

- **Distancia Administrativa (AD).**
 - **Confiabilidad** de una ruta en base a:
 - **Origen o protocolo de enrutamiento.**
 - **Una ruta para una red específica, solo puede aparecer una vez en la tabla de enrutamiento.**
 - **Pueden haber más de un origen y/o camino** para alcanzar dicha red.
 - Usualmente solo se debería utilizar un protocolo de enrutamiento por enrutador.
 - Hay excepciones, y varios protocolos podrían conocer las mismas redes y diferentes caminos para llegar a ellas.
 - **La AD determina la ruta a instalar en la tabla de enrutamiento.**
 - **La más baja** o más confiable.

Origen de la Ruta	Distancia Administrativa
Directamente Conectada	0
Ruta Estática	1
Ruta Sumarizada EIGRP	5
BGP Externo	20
EIGRP Interno	90
OSPF	110
IS-IS	115
RIP	120
EIGRP Externo	170
BGP Interno	200

Enrutamiento Estático y Dinámico.

- Estático vs. Dinámico.
 - Usos de Enrutamiento Estático:
 - Para **rutas predeterminadas** hacia el ISP.
 - Para **rutas fuera del dominio** no aprendidas por ningún protocolo.
 - Para **forzar administrativamente una ruta** a una red.
 - Para **enrutar redes stub**.
 - Usos de enrutamiento Dinámico:
 - Para **redes** considerablemente **grandes**.
 - Para cuando **cambios en la topología requieren** determinar una **nueva ruta**.
 - Para **escalabilidad**, aprender nuevas rutas conforme crece la red.

Enrutamiento Estático y Dinámico.

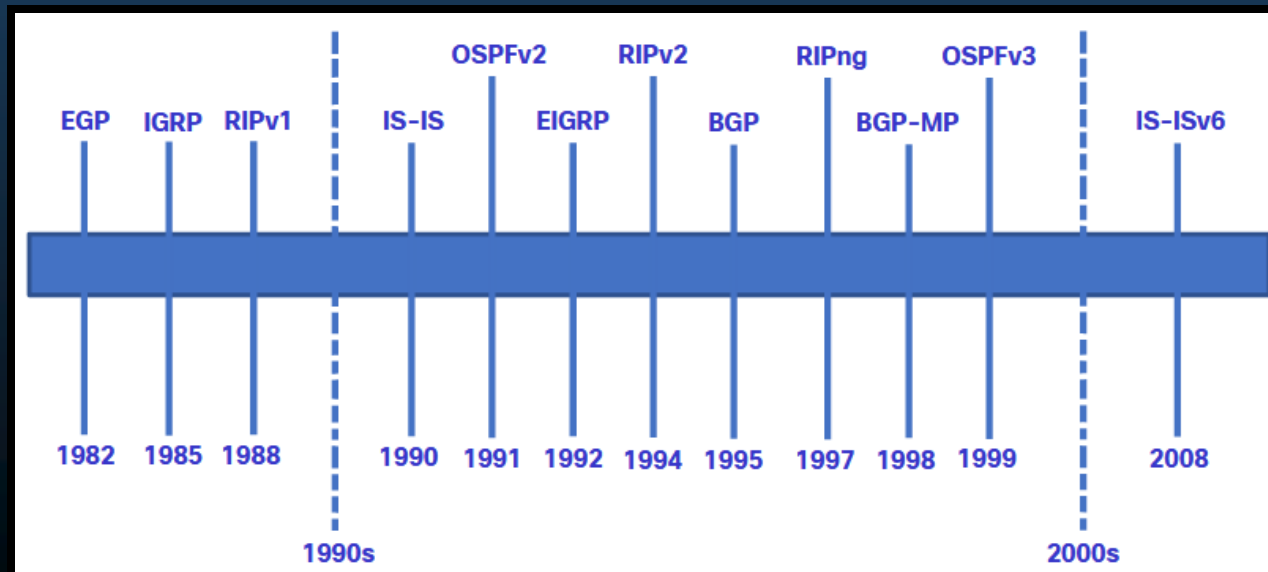
- Estático vs. Dinámico.

Característica	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Independiente del tamaño de la red	Aumenta con el tamaño de la red
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere intervención del administrador
Escalabilidad	Adecuado para topologías de red simples a complejas	Adecuado para topologías simples
Seguridad	La seguridad debe configurarse	La seguridad es inherente
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	No se necesitan recursos adicionales
Previsibilidad de ruta	La ruta depende de la topología y el protocolo de enrutamiento utilizado	Definido explícitamente por el administrador

Enrutamiento Estático y Dinámico.

• Evolución del Enrutamiento Dinámico.

- Uno de los primeros: **RIP** (finales de los 80s), surge de investigaciones ARPANET.
 - Se actualiza a **RIPv2** y **RIPng** (no adecuado para redes grandes)
- **OSPF**, **IS-IS**, **IGRP** de Cisco (Actualmente **EIGRP**), surgen para soportar redes mas complejas.
- Se dividen dominios de enrutamiento en Sistemas Autónomos (AS), y surge la necesidad de un protocolo para enrutar entre ellos.
 - **BGP** (sucesor de EGP)



Enrutamiento Estático y Dinámico.

- Evolución del Enrutamiento Dinámico.
 - Protocolos de Gateway interior: enrutan dentro de un AS.
 - Protocolos de Gateway exterior: enrutan fuera de los ASs.
 - El direccionamiento IP evoluciona y se requieren nuevos protocolos para IPv6.
 - El tipo de algoritmo utilizado para determinar la mejor ruta los categoriza como>
 - Vector Distancia, Estado de Enlace y Vector Ruta

Protocolos de Gateway interior			Protocolos de Gateway exterior		
	Vector Distancia		Estado de Enlace		Vector Ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP p' IPv6	OSPFv3	IS-IS p' IPv6	BGP-MP

Enrutamiento Estático y Dinámico.

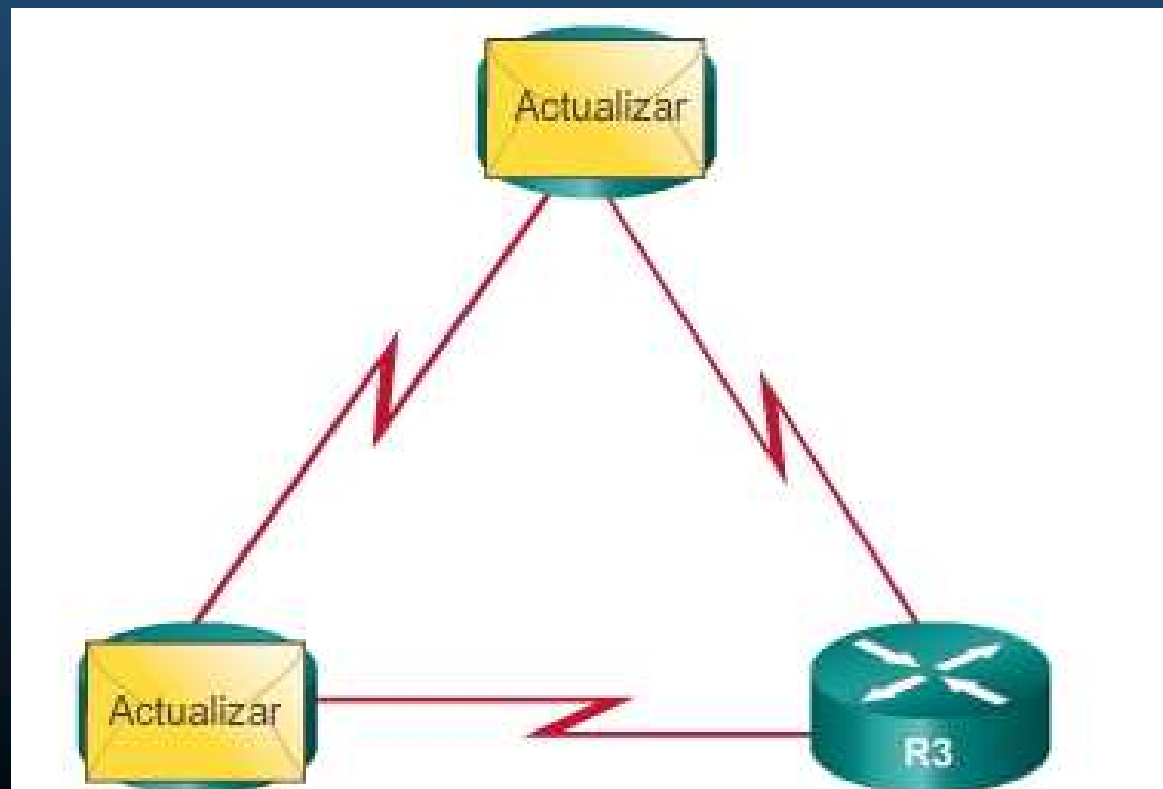
- **Conceptos de Protocolos de Enrutamiento Dinámico.**
 - Un protocolo de enrutamiento dinámico es un conjunto de procesos, algoritmos y mensajes, usados para intercambiar información de enrutamiento y poblar la tabla de enrutamiento con las mejores rutas.
 - Propósito:
 - Descubrir redes remotas.
 - Mantener información actualizada.
 - Elegir la mejor ruta a las redes destino.
 - Encontrar una nueva ruta si la actual ya no está disponible.
 - Componentes:
 - Estructuras de datos. Para sus operaciones. Almacenadas en RAM.
 - Mensajes de Protocolo de Enrutamiento: para sus tareas como descubrir vecinos, intercambiar rutas , etc.
 - Algoritmo: Lista finita de pasos para realizar la tarea de intercambiar información de enrutamiento y determinar la mejor ruta.

Enrutamiento Estático y Dinámico.

- **Función de los protocolos de routing dinámico**
 - Determinar **la mejor ruta hacia cada red** y agregarla a la tabla de routing.
 - **Intercambian información** ante un **cambio en la topología**.
 - **Obtener información sobre nuevas redes y rutas alternativas** si hay una falla.
 - Aligerar carga administrativa.
 - **Implica** el costo de **dedicar recursos del router a la operación del protocolo**, tiempo de CPU y ancho de banda del enlace de red.

Enrutamiento Estático y Dinámico.

- Función de los protocolos de routing dinámico.
 - Los protocolos de enrutamiento permiten a los routers **compartir** dinámicamente información sobre redes remotas y **ofrecen** automáticamente esta información a sus propias **tablas de enrutamiento**.



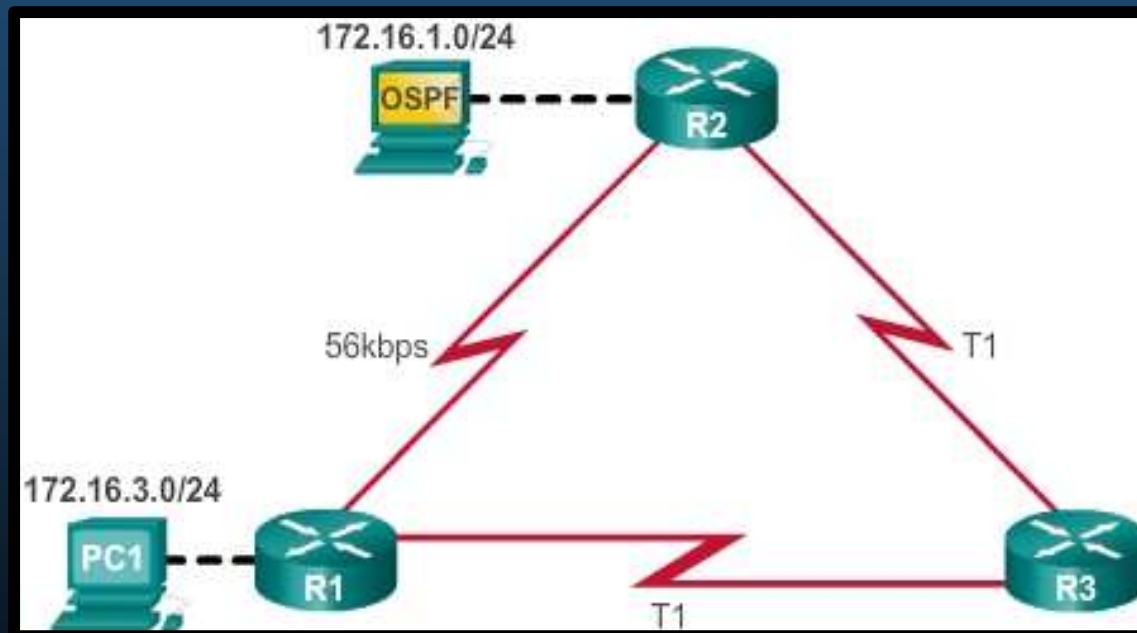
Enrutamiento Estático y Dinámico.

- Mejor Ruta

- Antes de ofrecer rutas a la tabla de enrutamiento un protocolo de enrutamiento dinámico debe determinar la mejor ruta a cada red.
 - Evaluar si hay múltiples rutas a la red (diferente interfaz de salida).
 - Elegir la mejor en base a la menor métrica de distancia a la red.
 - Cada protocolo utiliza diferentes reglas y características para sus métricas.
 - Protocolo de información de routing (RIP):
 - Conteo de saltos.
 - Protocolo OSPF (Open Shortest Path First):
 - Ancho de banda acumulativo de origen a destino.
 - Protocolo de routing de gateway interior mejorado (EIGRP):
 - Ancho de banda, retraso, carga, confiabilidad.

Enrutamiento Estático y Dinámico.

- Mejor Ruta
 - 56 kbps vs T1 = 1.544 Mbps



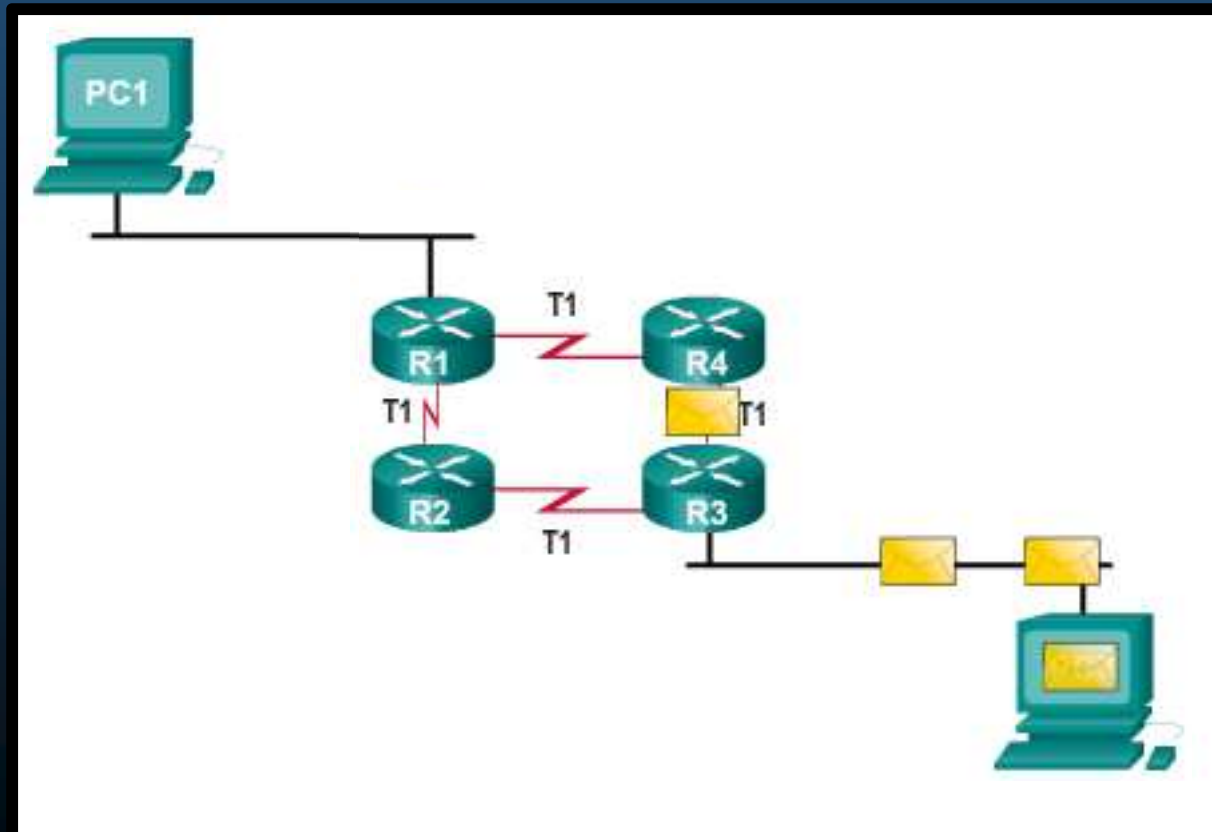
Determinación de Ruta.

- **Balanceo de Carga.**

- Cuando un router tiene dos o más rutas a un destino con iguales métricas, el enrutador alterna los paquetes utilizando ambas rutas por igual.
 - La tabla de enrutamiento tiene la red de destino único, con múltiples interfaces de salida.
- Si se configura correctamente, el balanceo de carga puede aumentar el rendimiento de la red.
- El equilibrio de carga de igual costo se implementa:
 - Automáticamente mediante protocolos de enrutamiento dinámico.
 - Con rutas estáticas, cuando hay varias rutas estáticas a la misma red de destino utilizando diferentes interfaces de salida (ó siguiente salto).
- Solo EIGRP admite el equilibrio de carga de costos desiguales (fuera del alcance de este curso).

Determinación de Ruta.

- Balanceo de Carga.
 - Dos rutas a un destino, misma métrica.



Integración

- Verifique su comprensión sobre “Conceptos de Enrutamiento”:

Realice el Quiz
(opcional)

<https://contenthub.netacad.com/srwe/14.6.2>



Capítulo 15

Enrutamiento Estático

<https://contenthub.netacad.com/srwe/15.1.1>

Rutas Estáticas

- Tipos de Rutas Estáticas

- Independientemente del protocolo IP disponible las rutas estáticas se clasifican en:

- Rutas Estáticas **Estándar**.
- Rutas Estáticas **por Defecto**.
- Rutas Estáticas **Flotantes**.
- Rutas Estáticas **de Resumen**.

- Las rutas estáticas se configuran utilizando las formas de los comandos:

- `ip route`
- `ipv6 route`

Rutas Estáticas

- **Opciones de Siguiete Salto.**

- Al configurar una ruta estática, dependiendo de la manera de determinar el siguiete salto, se denominan:
 - Ruta de Siguiete Salto: Sólo se especifica la IP de siguiete salto.
 - Ruta Estática Directamente Conectada: Sólo se especifica la interfaz de salida.
 - Ruta Completamente Especificada: se especifican IP de siguiete salto e interfaz de salida.
 - Requeridas en para rutas por redes de acceso compartido.

Rutas Estáticas

- Comando para Rutas Estáticas IPv4.

- Las rutas estáticas se configuran con el comando ip route de configuración global.

```
Router(config)# ip route network-address subnet-mask { ip-address | exit-intf [ip-address] }  
[distance]
```

Descripción	Parámetros
network-address	Identifica la dirección de la red destino remota a agregar a la tabla de enrutamiento.
subnet-mask	Identifica la máscara de subred de la red remota . Se puede modificar para resumir un grupo de redes en una ruta estática de resumen.
ip-address	Identifica la dirección del enrutador del siguiente salto. Para redes de difusión (como, Ethernet). Genera búsqueda recursiva, el router debe buscar la interfaz de salida.
exit-intf	Identifica la interfaz de salida para reenviar paquetes. Crea una ruta estática conectada directamente. Normalmente para redes punto a punto.
exit-intf ip-address	Crea una ruta estática completamente especificada porque especifica la interfaz de salida y la dirección IPv4 del siguiente salto.
distance	Opcional. Puede asignar un valor de distancia administrativa entre 1 y 255. Para configurar rutas estáticas flotantes con una distancia administrativa más alta que otras.

Rutas Estáticas

- Comando para Rutas Estáticas IPv6.

- Las rutas estáticas IPv6 se configuran con el comando `ipv6 route` de configuración global.

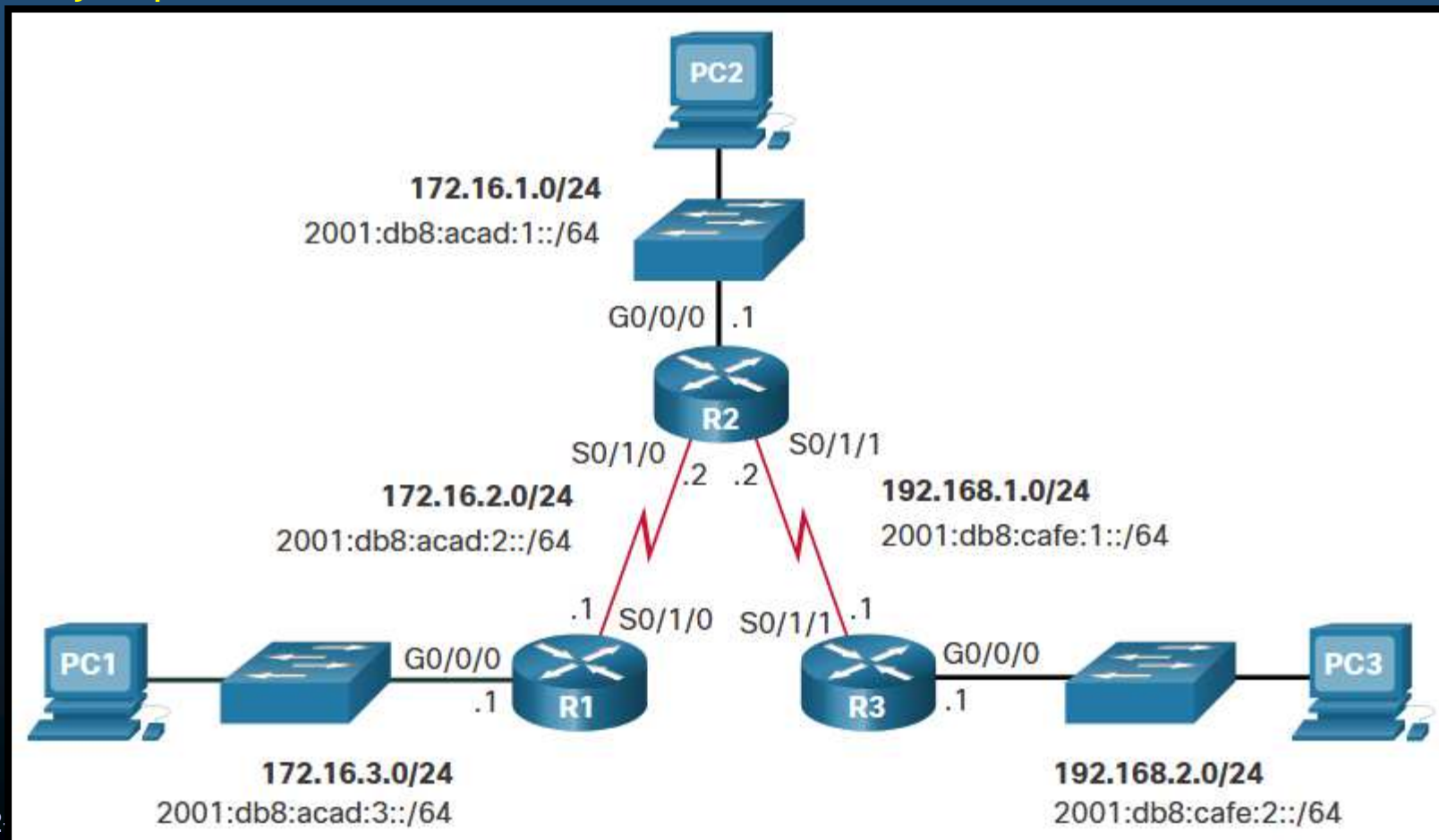
```
Router(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-address | exit-intf  
[ipv6-address]} [distance]
```

Descripción	Parámetros
<code>ipv6-prefix</code>	Identifica el prefijo de la red destino remota a agregar a la tabla de enrutamiento.
<code>/prefix-length</code>	Identifica la longitud del prefijo de la red remota .
<code>ipv6-address</code>	Identifica la dirección del enrutador del siguiente salto. Para redes de difusión (como, Ethernet). Genera búsqueda recursiva, el router debe buscar la interfaz de salida.
<code>exit-intf</code>	Identifica la interfaz de salida para reenviar paquetes. Crea una ruta estática conectada directamente. Normalmente para redes punto a punto.
<code>exit-intf ipv6-address</code>	Crea una ruta estática completamente especificada porque especifica la interfaz de salida y la dirección IPv6 del siguiente salto.
<code>distance</code>	Opcional. Puede asignar un valor de distancia administrativa entre 1 y 255. Para configurar rutas estáticas flotantes con una distancia administrativa más alta que otras.

Rutas Estáticas

- Topología Dual Stack.

- La imagen muestra la **topología** considerada **para** desarrollar los **ejemplos** subsecuentes:



Rutas Estáticas

- Tablas de Enrutamiento IPv4 Iniciales.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
R1#
```

```
R2# show ip route | begin Gateway
Gateway of last resort is not set
    172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.2/32 is directly connected, Serial0/1/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/1/1
L       192.168.1.2/32 is directly connected, Serial0/1/1
R2#
```

```
R3# show ip route | begin Gateway
Gateway of last resort is not set
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/1/1
L       192.168.1.1/32 is directly connected, Serial0/1/1
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0/0
L       192.168.2.1/32 is directly connected, GigabitEthernet0/0/0
R3#
```

Rutas Estáticas

- Tablas de Enrutamiento IPv4 Iniciales.
 - Cada router conoce sólo sus redes directamente conectadas.
 - Por ende:
 - R1 puede hacer ping a R2.

```
R1# ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
```

- R1 no puede hacer ping a R3.

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Rutas Estáticas

- Tablas de Enrutamiento IPv6 Iniciales.

```
R1# show ipv6 route | begin C
C   2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
    via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

```
R3# show ipv6 route | begin C
C   2001:DB8:CAFE:1::/64 [0/0]
    via Serial0/1/1, directly connected
L   2001:DB8:CAFE:1::1/128 [0/0]
    via Serial0/1/1, receive
C   2001:DB8:CAFE:2::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   2001:DB8:CAFE:2::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R3#
```

```
R2# show ipv6 route | begin C
C   2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::2/128 [0/0]
    via Serial0/1/0, receive
C   2001:DB8:CAFE:1::/64 [0/0]
    via Serial0/1/1, directly connected
L   2001:DB8:CAFE:1::2/128 [0/0]
    via Serial0/1/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R2#
```

Rutas Estáticas

- Tablas de Enrutamiento IPv6 Iniciales.
 - Cada router conoce sólo sus redes directamente conectadas.
 - E igualmente:
 - R1 puede hacer ping a R2.

```
R1# ping 2001:db8:acad:2::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

- R1 no puede hacer ping a R3.

```
R1# ping 2001:DB8:cafe:2::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:2::1, timeout is 2 seconds:
% No valid route for destination
Success rate is 0 percent (0/1)
```

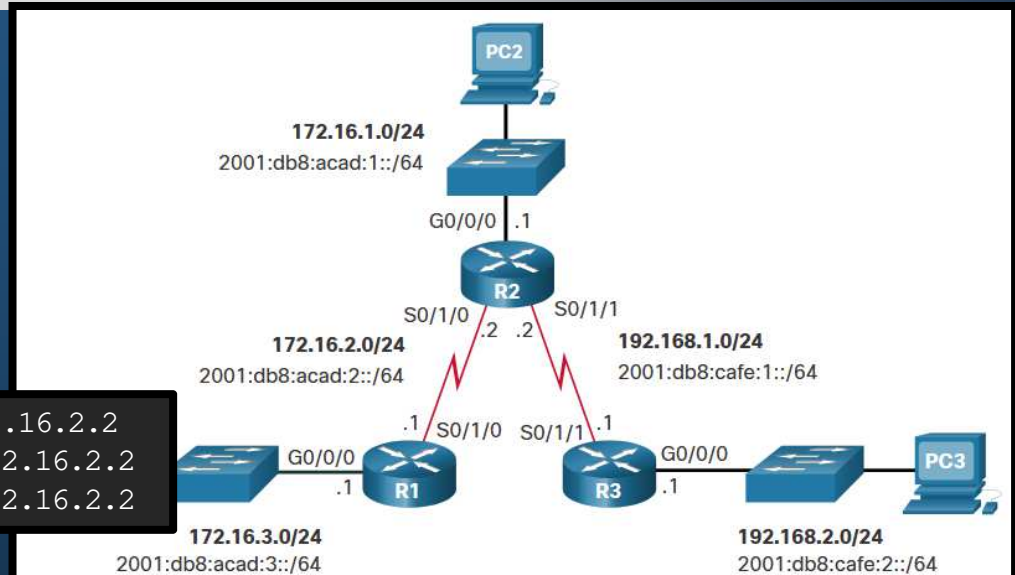
Configurar Rutas Estáticas

- Rutas Estáticas IPv4 de Siguiente Salto.

- Configuración de R1 con las rutas estáticas a las redes remotas.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

- La tabla de enrutamiento de R1, ahora tiene rutas para las redes remotas.



```
R1# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S       192.168.1.0/24 [1/0] via 172.16.2.2
S       192.168.2.0/24 [1/0] via 172.16.2.2

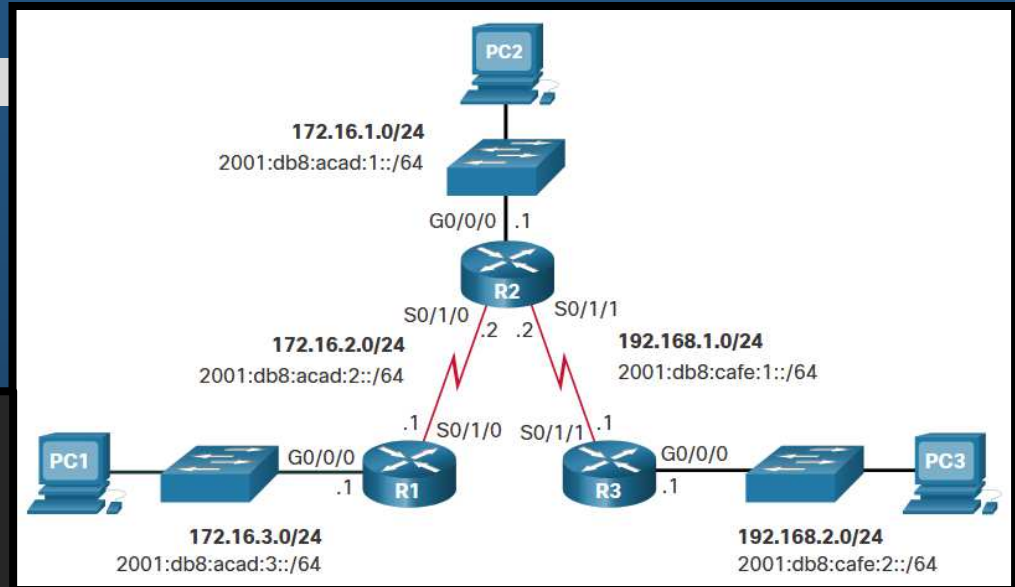
R1#
```

Configurar Rutas Estáticas

- Rutas Estáticas IPv6 de Siguiente Salto.
 - Configuración de R1 con las rutas estáticas a las redes remotas.

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route 2001:db8:acad:1::/64
2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:1::/64
2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:2::/64
2001:db8:acad:2::2
```

- La tabla de enrutamiento de R1, ahora tiene rutas para las redes remotas.



```
R1# show ipv6 route
...
S 2001:DB8:ACAD:1::/64 [1/0]
  via 2001:DB8:ACAD:2::2
C 2001:DB8:ACAD:2::/64 [0/0]
  via Serial0/1/0, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
  via Serial0/1/0, receive
C 2001:DB8:ACAD:3::/64 [0/0]
  via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
  via GigabitEthernet0/0/0, receive
S 2001:DB8:CAFE:1::/64 [1/0]
  via 2001:DB8:ACAD:2::2
S 2001:DB8:CAFE:2::/64 [1/0]
  via 2001:DB8:ACAD:2::2
L FF00::/8 [0/0]
  via Null0, receive
```


Configurar Rutas Estáticas

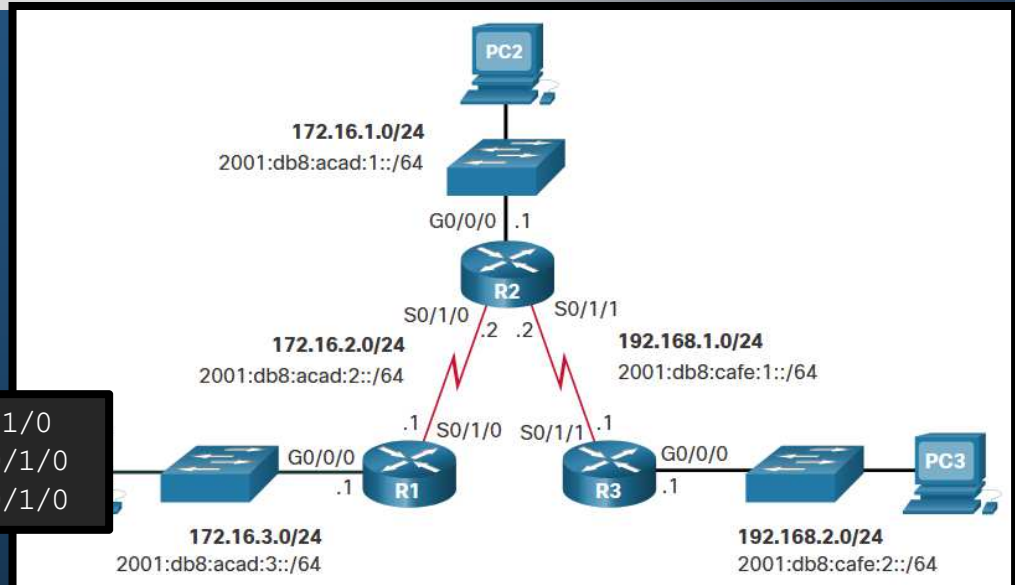
- Rutas Estáticas IPv4 Directamente Conectadas.

- Configuración de R1 con las rutas conectadas a las redes remotas.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.2.0 255.255.255.0 s0/1/0
```

- La tabla de enrutamiento de R1, ahora tiene rutas para las redes remotas.

- Se recomienda utilizar rutas de siguiente salto.
- Las rutas conectadas se recomienda para redes punto a punto.



```
R1# show ip route | begin Gateway
Gateway of last resort is not set
172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S    172.16.1.0/24 is directly connected, Serial0/1/0
C    172.16.2.0/24 is directly connected, Serial0/1/0
L    172.16.2.1/32 is directly connected, Serial0/1/0
C    172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L    172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S    192.168.1.0/24 is directly connected, Serial0/1/0
S    192.168.2.0/24 is directly connected, Serial0/1/0
```

Configurar Rutas Estáticas

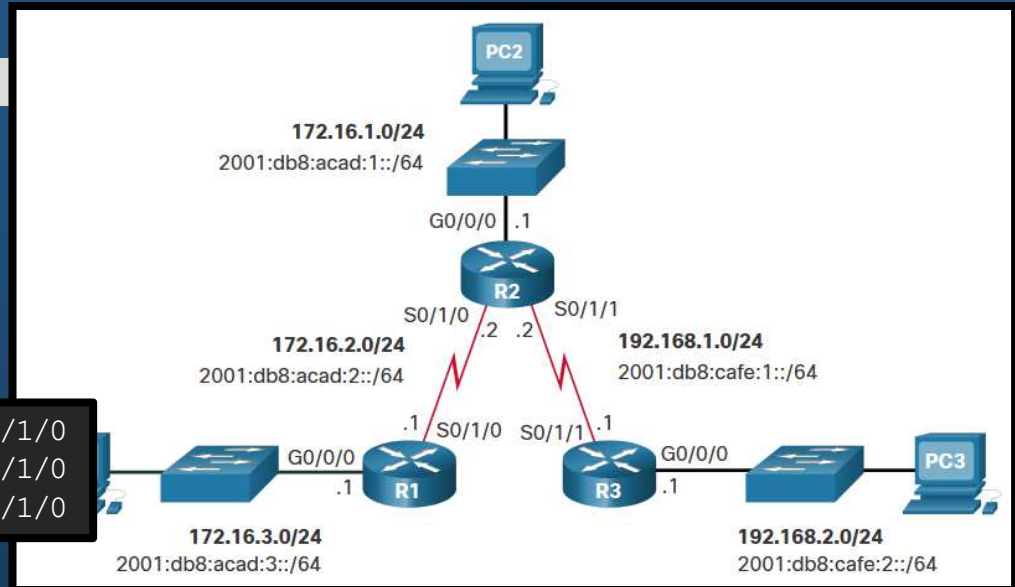
- **Rutas Estáticas IPv6 Directamente Conectadas.**

- Configuración de R1 con las rutas estáticas a las redes remotas.

```
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:2::/64 s0/1/0
```

- La **tabla de enrutamiento de R1**, ahora tiene rutas para las redes remotas.

- Se recomienda utilizar **rutas de siguiente salto**.
- Las **rutas conectadas** se recomienda **para redes punto a punto**.

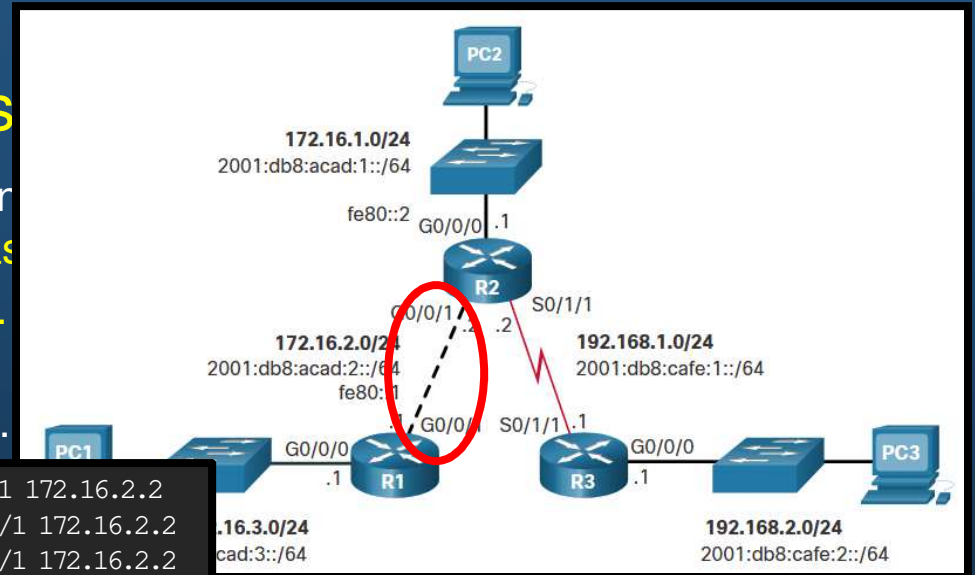


```
R1# show ipv6 route
...
S 2001:DB8:ACAD:1::/64 [1/0]
  via Serial0/1/0, directly connected
C 2001:DB8:ACAD:2::/64 [0/0]
  via Serial0/1/0, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
  via Serial0/1/0, receive
C 2001:DB8:ACAD:3::/64 [0/0]
  via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
  via GigabitEthernet0/0/0, receive
S 2001:DB8:CAFE:1::/64 [1/0]
  via Serial0/1/0, directly connected
S 2001:DB8:CAFE:2::/64 [1/0]
  via Serial0/1/0, directly connected
L FF00::/8 [0/0]
  via Null0, receiveIPv6 Routing Table - default - 8 entries
R1#
```

Configurar Rutas Estáticas

- **Rutas Estáticas IPv4 Completamente Especificadas**

- Para redes de acceso múltiple se deben usar rutas completamente especificadas
- Si el enlace de R1 a R2 fuese Ethernet.
 - Configuración de R2 con rutas especificadas a las redes remotas.



```
R1(config)# ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
```

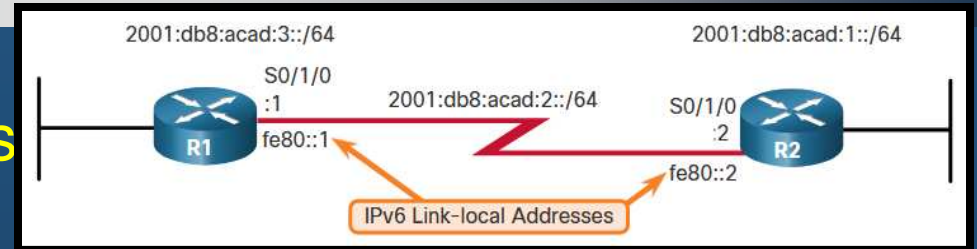
- La **tabla de enrutamiento de R1**, ahora tiene rutas para las redes remotas.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
C       172.16.2.0/24 is directly connected, GigabitEthernet0/0/1
L       172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S       192.168.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
S       192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
```

Configurar Rutas Estáticas

- Rutas Estáticas IPv6 Completamente Especificadas

- Cuando una ruta estática IPv6 utiliza una dirección link-local como siguiente salto, se requieren rutas completamente especificadas
- Configuración de R1 con las rutas completamente especificadas a la red remotas.



```
R1(config)# ipv6 route 2001:db8:acad:1::/64 fe80::2
%Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2
```

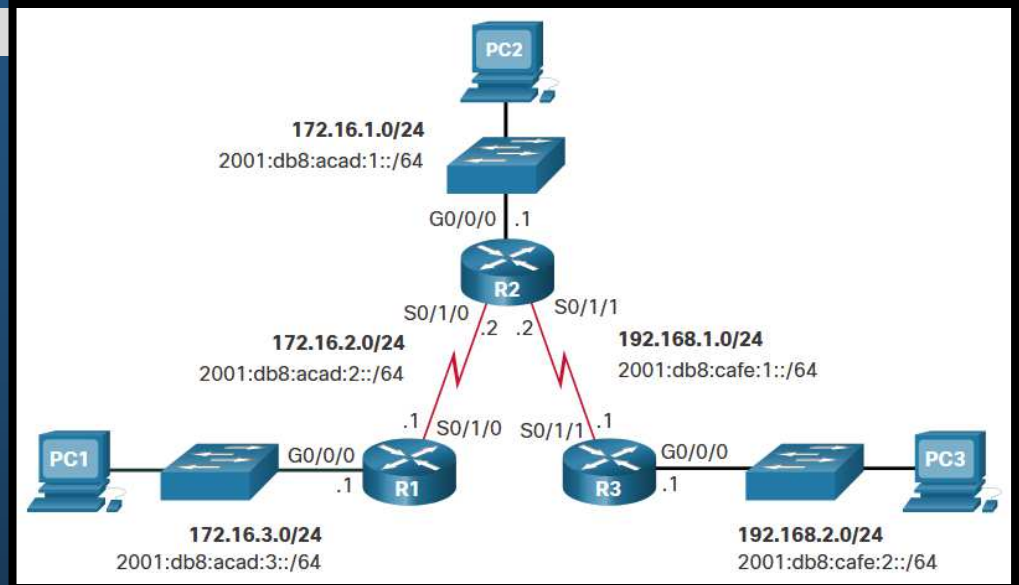
- Las direcciones link-local no son únicas, se pueden repetir en cada red, por lo que es indispensable especificar la interfaz de salida.
- La siguiente figura muestra la salida de la tabla de enrutamiento completamente especificada.

```
R1# show ipv6 route static | begin 2001:db8:acad:1::/64
S 2001:DB8:ACAD:1::/64 [1/0]
  via FE80::2, Seria0/1/0
```

Configurar Rutas Estáticas

- **Verificar Rutas Estáticas.**

- **Comandos disponibles:**
 - `show ip route static`
 - `show ip route network`
 - `show running-config | section ip route`
- **Para Ipv6 reemplace ip por ipv6.**
- **Mostrar sólo rutas estáticas**



```
R1# show ip route static | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S    172.16.1.0/24 [1/0] via 172.16.2.2
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

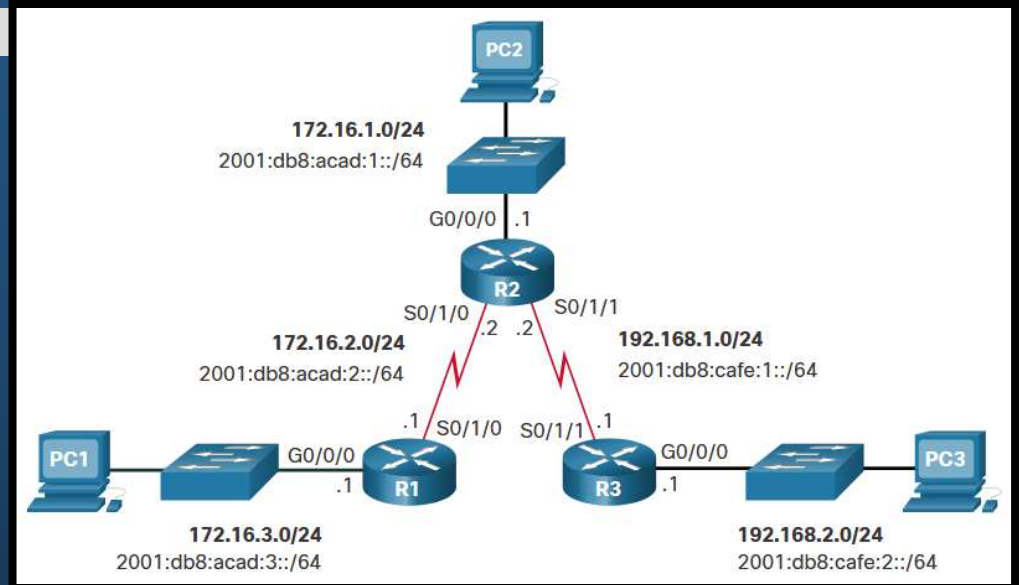
- **Desplegar una red específica**

```
R1# show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
    * 172.16.2.2
      Route metric is 0, traffic share count is 1
R1#
```

Configurar Rutas Estáticas

- **Verificar Rutas Estáticas.**

- **Comandos disponibles:**
 - `show ip route static`
 - `show ip route network`
 - `show running-config | section ip route`
- **Para Ipv6 reemplace ip por ipv6.**
- **Desplegar Configuración de Rutas Estáticas IPv4.**



```
R1# show running-config | section ip route
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1#
```

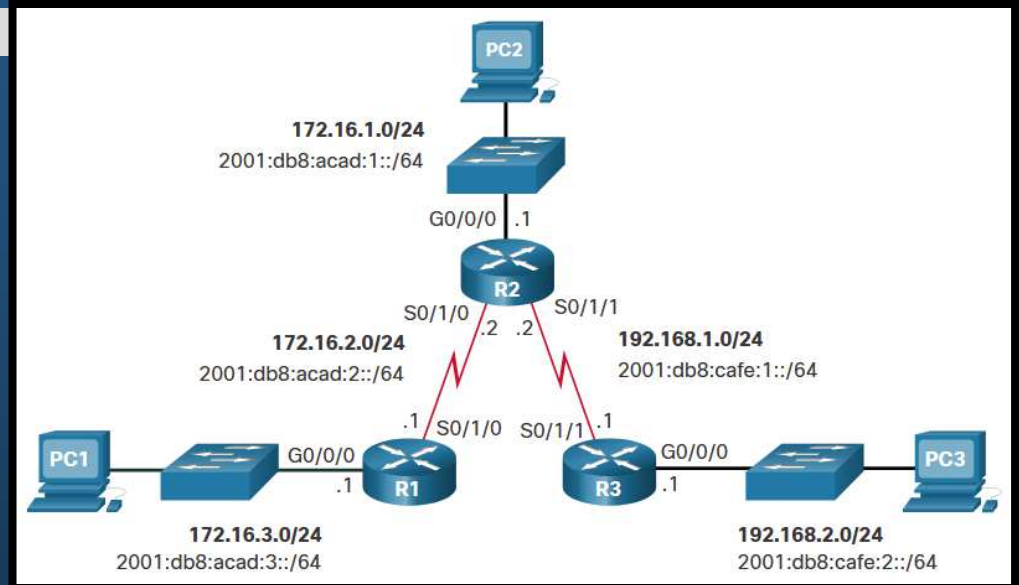
- **Desplegar sólo rutas estáticas**

```
R1# show ipv6 route static
...
S 2001:DB8:ACAD:1::/64 [1/0]
  via 2001:DB8:ACAD:2::2
S 2001:DB8:CAFE:1::/64 [1/0]
  via 2001:DB8:ACAD:2::2
S 2001:DB8:CAFE:2::/64 [1/0]
  via 2001:DB8:ACAD:2::2
R1#
```

Configurar Rutas Estáticas

- **Verificar Rutas Estáticas.**

- **Comandos disponibles:**
 - `show ip route static`
 - `show ip route network`
 - `show running-config | section ip route`
- **Para Ipv6 reemplace ip por ipv6.**
- **Desplegar una red IPv6 específica.**



```
R1# show ipv6 route 2001:db8:cafe:2::  
Routing entry for 2001:DB8:CAFE:2::/64  
Known via "static", distance 1, metric 0  
Route count is 1/1, share count 0  
Routing paths:  
  2001:DB8:ACAD:2::2  
    Last updated 00:23:55 ago  
R1#
```

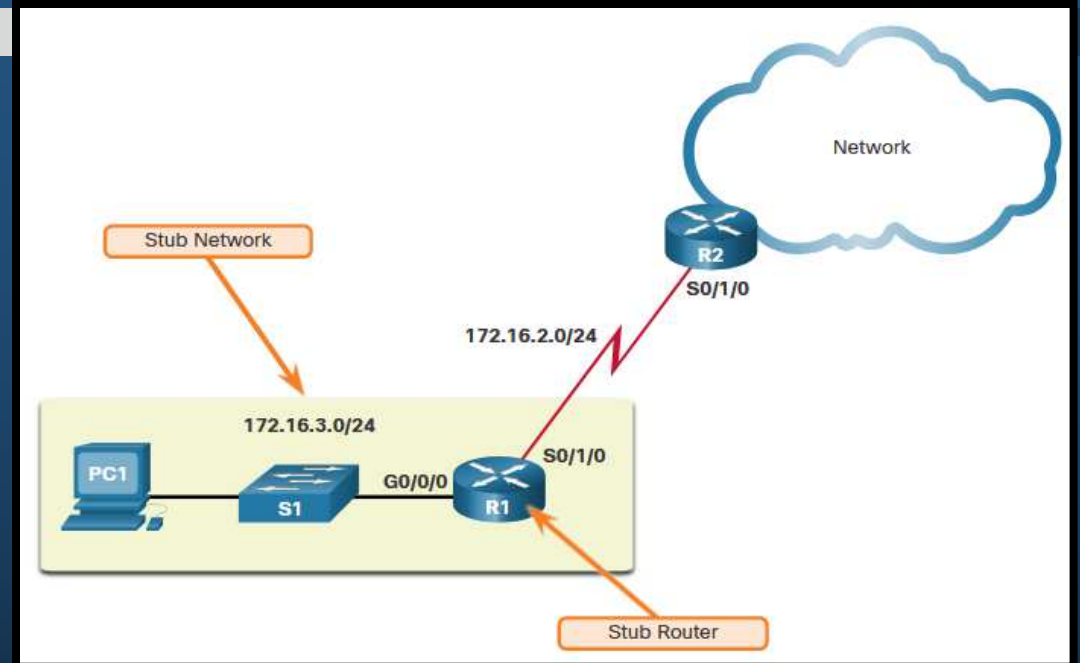
- **Desplegar Configuración de Rutas Estáticas IPv6.**

```
R1# show running-config | section ipv6 route  
ipv6 route 2001:DB8:ACAD:1::/64  
2001:DB8:ACAD:2::2  
ipv6 route 2001:DB8:CAFE:1::/64  
2001:DB8:ACAD:2::2  
ipv6 route 2001:DB8:CAFE:2::/64  
2001:DB8:ACAD:2::2  
R1#
```


Configurar Rutas Estáticas Predeterminadas

- Rutas Estáticas Predeterminadas.

- Representan todas las redes que no se encuentren ya, en la tabla de enrutamiento.
- No requiere coincidencia de ningún bit.
 - Mascara y longitud = 0.
- Útiles al conectar router de extremo a un ISP, o routers stub.



- Comando disponible para IPv4:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

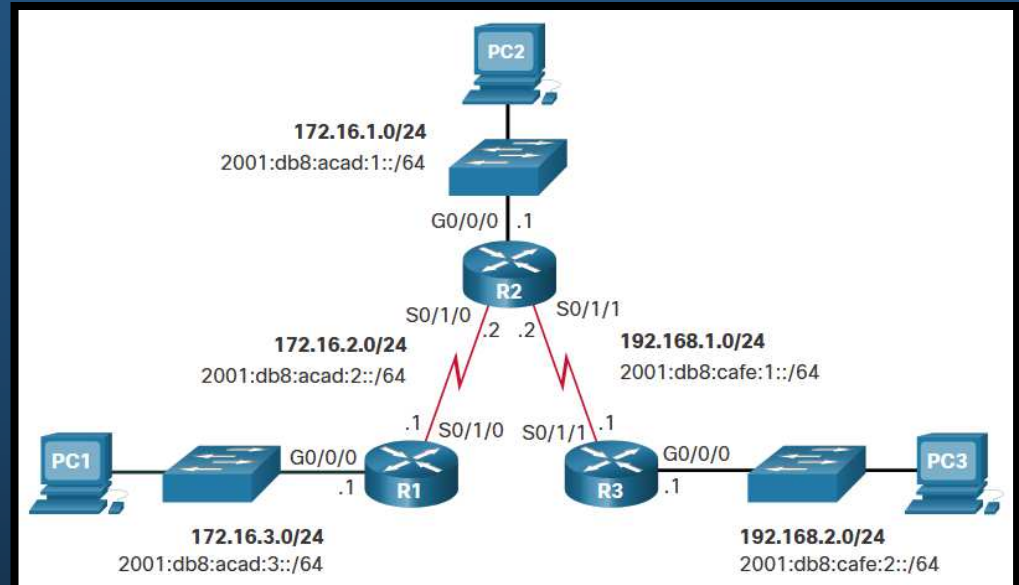
- Para Ipv6:

```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```


Configurar Rutas Estáticas Predeterminadas

- Configurar Rutas Estáticas Predeterminadas.

- En el ejemplo, R1 podría configurarse con 3 rutas estáticas para las redes remotas o con una sola ruta predeterminada.



- Para IPv4:

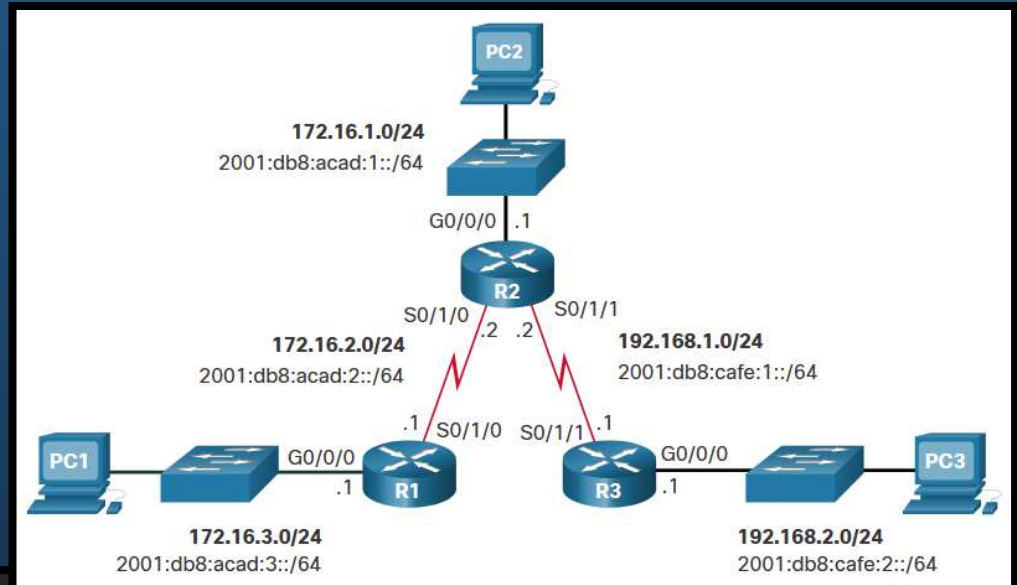
```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

- Para IPv6:

```
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
```

Configurar Rutas Estáticas Predeterminadas

- Verificar Rutas Estáticas Predeterminadas.
 - Siguiendo el ejemplo, R1 podría verificar sus rutas predeterminadas.
- Para IPv4:



```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override
```

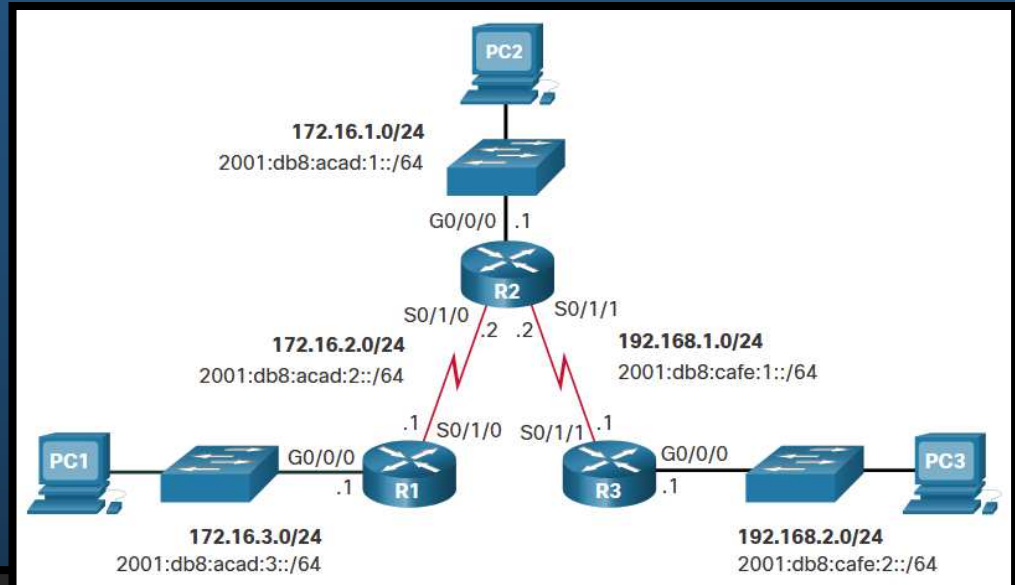
```
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
```

```
S* 0.0.0.0/0 [1/0] via 172.16.2.2
```

```
R1#
```

Configurar Rutas Estáticas Predeterminadas

- Verificar Rutas Estáticas Predeterminadas.
 - Siguiendo el ejemplo, R1 podría verificar sus rutas predeterminadas.
- Para IPv6:



```
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S    ::/0 [1/0]
    via 2001:DB8:ACAD:2::2

R1#
```

Configurar Rutas Estáticas Flotantes

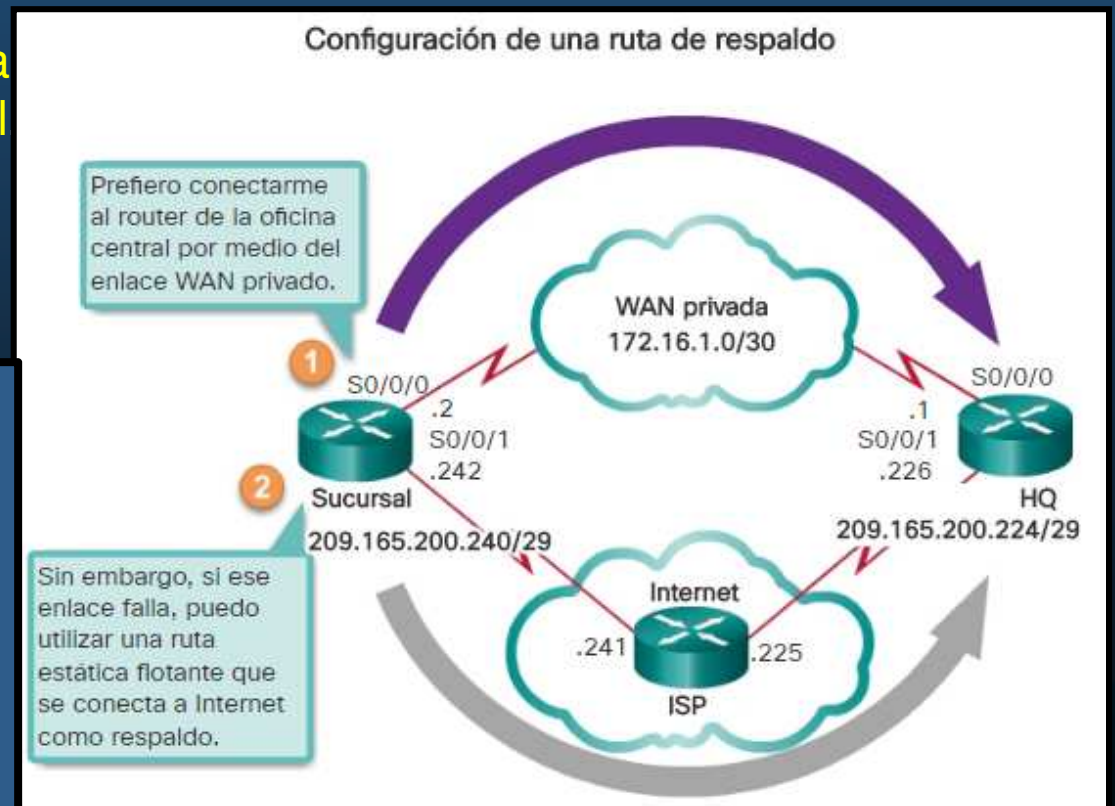
- Rutas Estáticas Flotantes.

- Rutas estáticas que se utilizan para proporcionar una ruta de respaldo, en caso de falla en la ruta principal.
 - Se utilizan únicamente cuando la ruta principal no está disponible.
 - Se configura con una Distancia Administrativa mayor a la ruta principal
 - En la tabla de enrutamiento, sólo se instalan las rutas de menor AD.

Por defecto, las rutas estáticas tienen una AD de 1, por lo que se prefieren a las de los protocolos de enrutamiento dinámico.

EIGRP = 90
OSPF = 110
IS-IS = 115

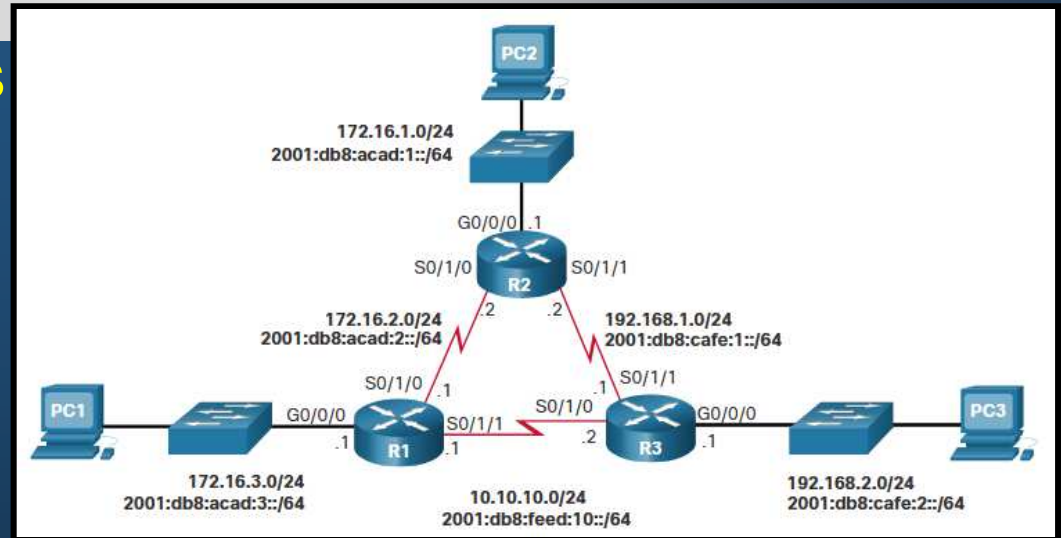
Sin embargo, la AD en una ruta estática puede ser cambiada deliberadamente.



Configurar Rutas Estáticas Flotantes

- Configurar Rutas Estáticas Flotantes.

- En el ejemplo, R1 prefiere a R2 cómo siguiente salto para llegar a redes remotas, con opción para utilizar R3 en caso de que el enlace entre R1 y R2 falle.



```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
R1(config)# ipv6 route ::/0 2001:db8:feed:10::2 5
```

- Para verificar ruta utilizada y configuradas:

```
R1# show ip route static | begin Gateway
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
```

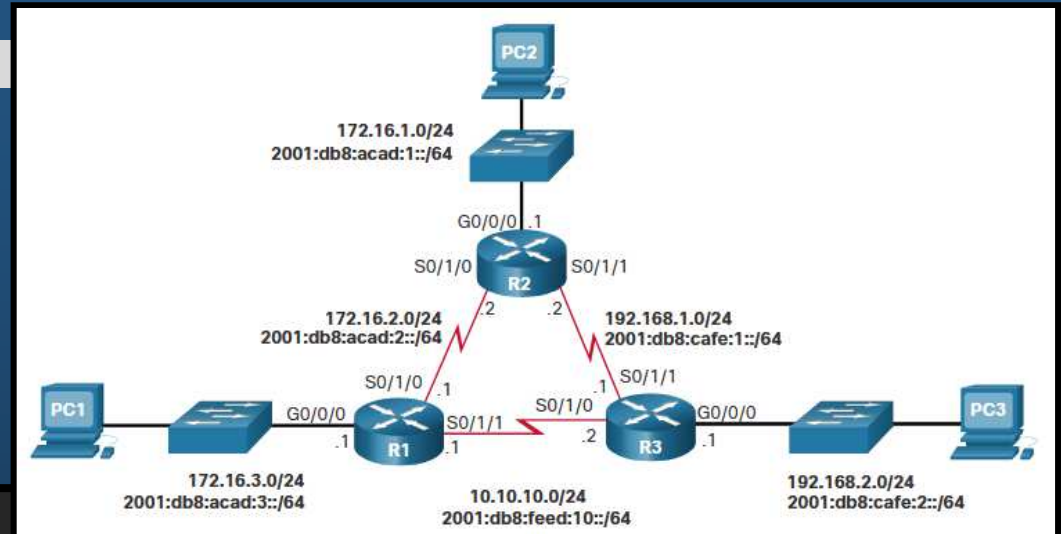
```
S* 0.0.0.0/0 [1/0] via 172.16.2.2
R1# show ipv6 route static | begin S :
S ::/0 [1/0]
via 2001:DB8:ACAD:2::2
R1#
```

```
R1# show run | include ipv6 route
ipv6 route ::/0 2001:db8:feed:10::2 5
ipv6 route ::/0 2001:db8:acad:2::2
R1#
```

Configurar Rutas Estáticas Flotantes

- Probar Rutas Estáticas Flotantes.

- En el ejemplo, para simular una falla en el enlace entre R1 y R2, se deshabilitan las interfaces seriales de R2.



```
R2(config)# interface s0/1/0
R2(config-if)# shut
*Sep 18 23:36:27.000: %LINK-5-CHANGED: Interface Serial0/1/0, changed state to administratively down
*Sep 18 23:36:28.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
R2(config-if)# interface s0/1/1
R2(config-if)# shut
*Sep 18 23:36:41.598: %LINK-5-CHANGED: Interface Serial0/1/1, changed state to administratively down
*Sep 18 23:36:42.598: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down
```

- Para verificar error R1 emite mensajes y las rutas utilizadas cambian:

```
R1#
*Sep 18 23:35:48.810: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to down
R1#
*Sep 18 23:35:49.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
R1# show ip route static | begin Gateway
Gateway of last resort is 10.10.10.2 to network 0.0.0.0
S*   0.0.0.0/0 [5/0] via 10.10.10.2
R1# show ipv6 route static | begin ::
S   ::/0 [5/0]
      via 2001:DB8:FEED:10::2
R1#
```

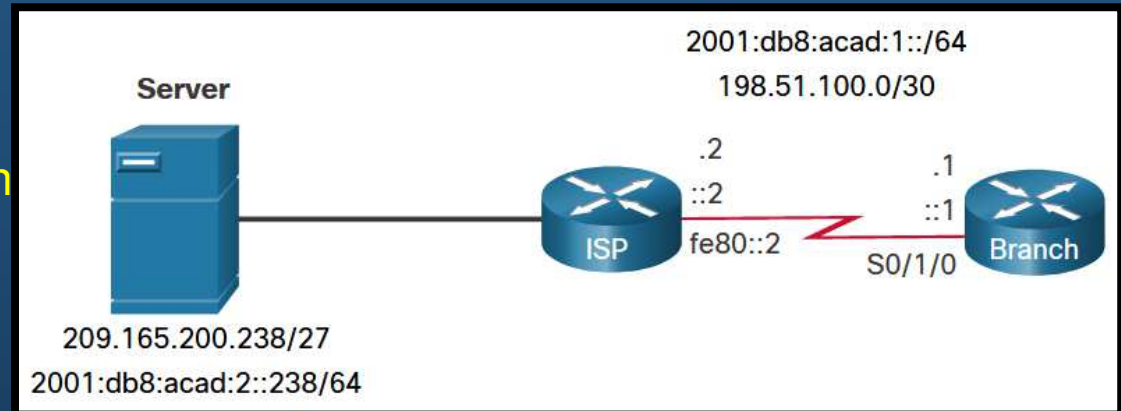
Configurar Rutas Estáticas de Host

- Rutas de Host.
 - Rutas con mascara /32 (IPv4) o /128 (IPv6).
 - Tres maneras de añadirla a la tabla de enrutamiento:
 - Automáticamente al configurar una IP en una interfaz.
 - Configurada como ruta estática.
 - Automáticamente obtenida por otros métodos (mas adelante en este curso).

Configurar Rutas Estáticas de Host

- Rutas de Host.

- Instalada automáticamente al configurar una interfaz en el router.
- Ayuda a determinar si el tráfico va dirigido al router o se debe re-enviar.
- Se marca con una L en la tabla de enrutamiento.



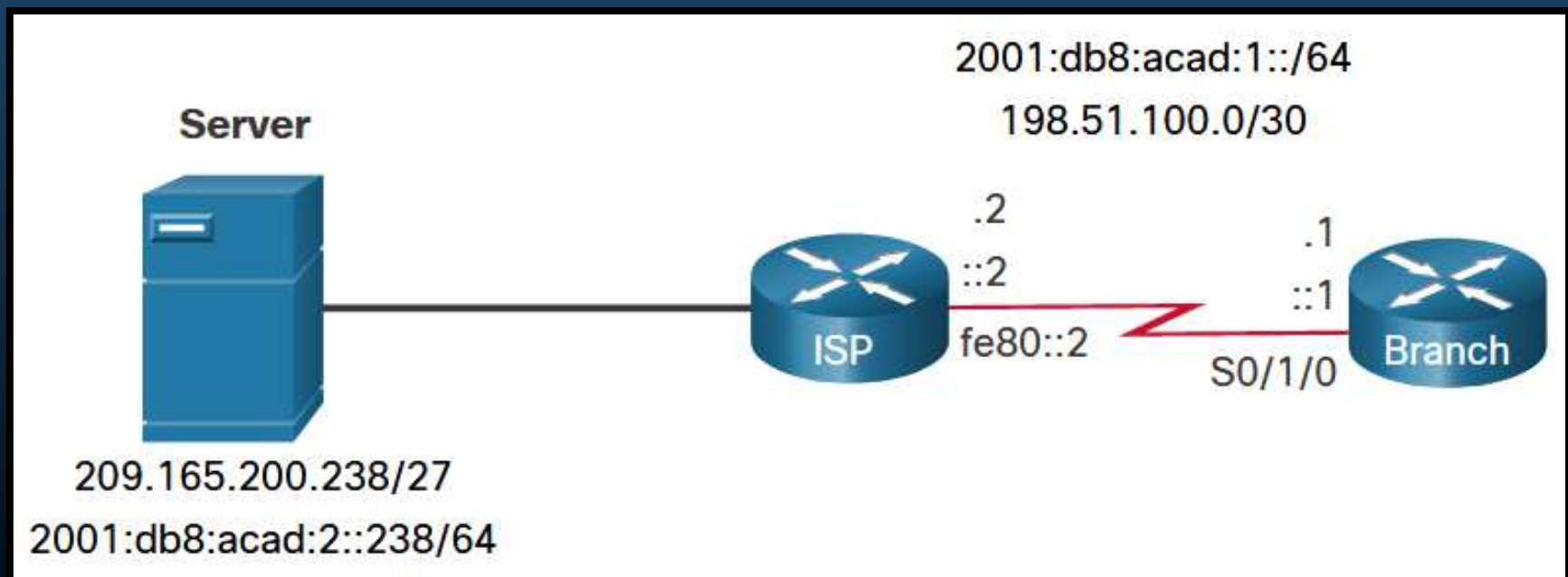
```
Branch# show ip route | begin Gateway
Gateway of last resort is not set
    198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       198.51.100.0/30 is directly connected, Serial0/1/0
L       198.51.100.1/32 is directly connected, Serial0/1/0
Branch# show ipv6 route | begin ::
C       2001:DB8:ACAD:1::/64 [0/0]
        via Serial0/1/0, directly connected
L       2001:DB8:ACAD:1:::1/128 [0/0]
        via Serial0/1/0, receive
L       FF00::/8 [0/0]
        via Null0, receive
```


Configurar Rutas Estáticas de Host

- Rutas de Host Estáticas.

- Pueden configurarse manualmente para redirigir el tráfico a un destino específico (como el servidor en la figura).

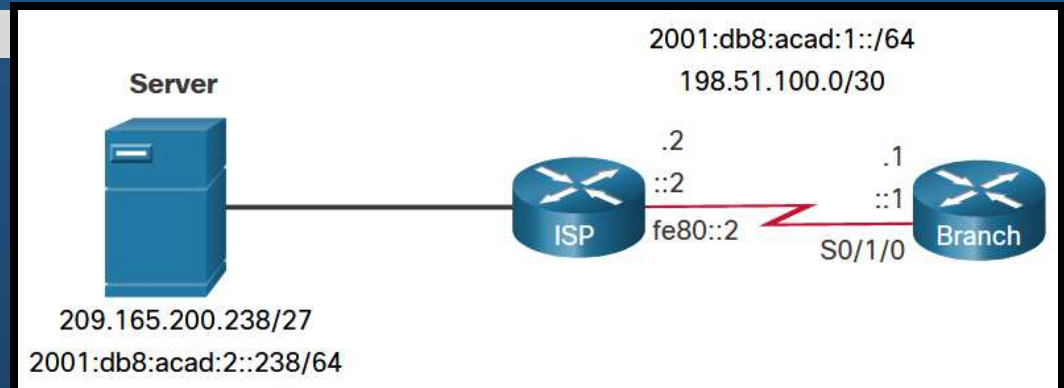
- Utilizará una red destino /32 para IPv4 o longitud de prefijo /128 para IPv6.



Configurar Rutas Estáticas de Host

- Configurar y Verificar Rutas de Host Estáticas.

- Ejemplo de configuración en router Branch.



```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2
Branch(config)# exit
Branch#
```

- Verificación de que las rutas configuradas se encuentran activas:

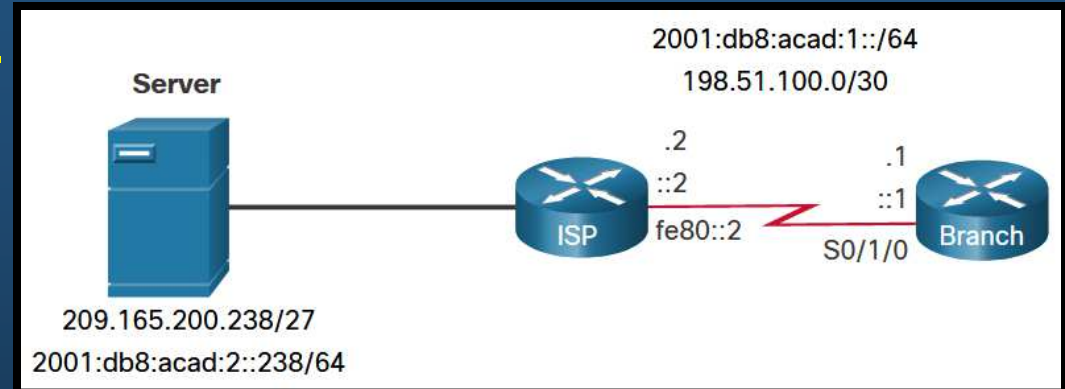
```
Branch# show ip route | begin Gateway
Gateway of last resort is not set
  198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       198.51.100.0/30 is directly connected, Serial0/1/0
L       198.51.100.1/32 is directly connected, Serial0/1/0
S       209.165.200.0/32 is subnetted, 1 subnets
S       209.165.200.238 [1/0] via 198.51.100.2
Branch# show ipv6 route
(Output omitted)
C       2001:DB8:ACAD:1::/64 [0/0]
        via Serial0/1/0, directly connected
L       2001:DB8:ACAD:1::1/128 [0/0]
        via Serial0/1/0, receive
S       2001:DB8:ACAD:2::238/128 [1/0]
        via 2001:DB8:ACAD:1::2
```

```
Branch#
```

Configurar Rutas Estáticas de Host

- Configurar y Verificar Rutas de Host Estáticas IPv6 con Local-Link cómo Siguiendo Salto.

- Ejemplo de configuración en router Branch.



- Necesario incluir la interfaz de salida:

```
Branch(config)# no ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 serial 0/1/0 fe80::2
Branch# show ipv6 route | begin ::
C 2001:DB8:ACAD:1::/64 [0/0]
  via Serial0/1/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
  via Serial0/1/0, receive
S 2001:DB8:ACAD:2::238/128 [1/0]
  via FE80::2, Serial0/1/0
Branch#
```

Integración

- **Configure Rutas Estáticas y Predeterminadas IPv4 e IPv6.**

Realice la Actividad Práctica del Módulo 15
Incluya una **aplicación creativa** para los temas.
(Se calificará)

<https://contenthub.netacad.com/srwe/15.6.1>



Capítulo 16

Diagnóstico de Problemas de Enrutamiento Estático

<https://contenthub.netacad.com/srwe/16.1.1>

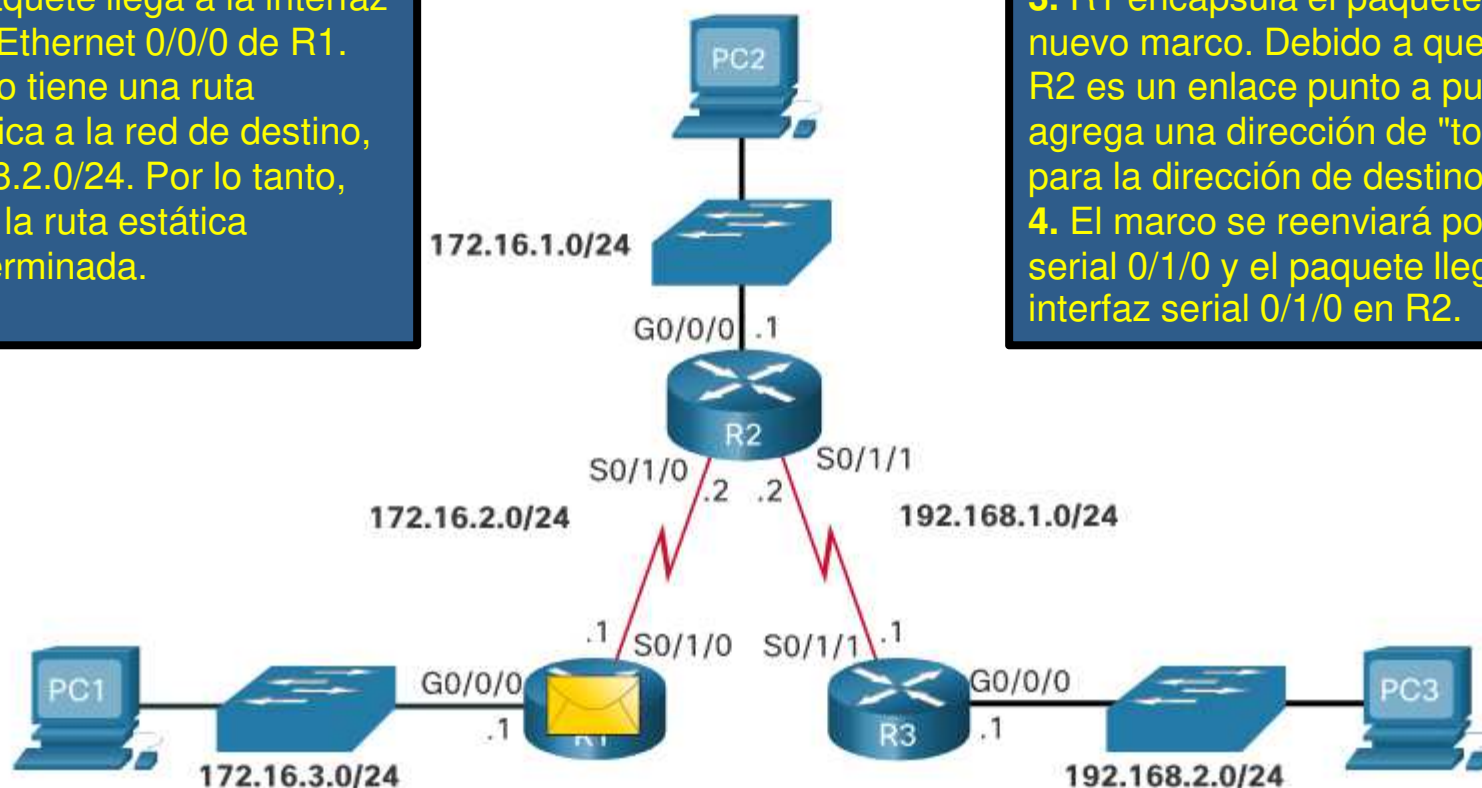
Procesamiento de Paquetes con Rutas Estáticas

- Rutas Estáticas y Re-envío de Paquetes.

- Antes de entrar a la resolución de problemas, se revisará el re-envío de paquetes con rutas estáticas:

1. El paquete llega a la interfaz GigabitEthernet 0/0/0 de R1.
2. R1 no tiene una ruta específica a la red de destino, 192.168.2.0/24. Por lo tanto, R1 usa la ruta estática predeterminada.

3. R1 encapsula el paquete en un nuevo marco. Debido a que el enlace a R2 es un enlace punto a punto, R1 agrega una dirección de "todos los 1s" para la dirección de destino de Capa 2.
4. El marco se reenviará por la interfaz serial 0/1/0 y el paquete llegará a la interfaz serial 0/1/0 en R2.

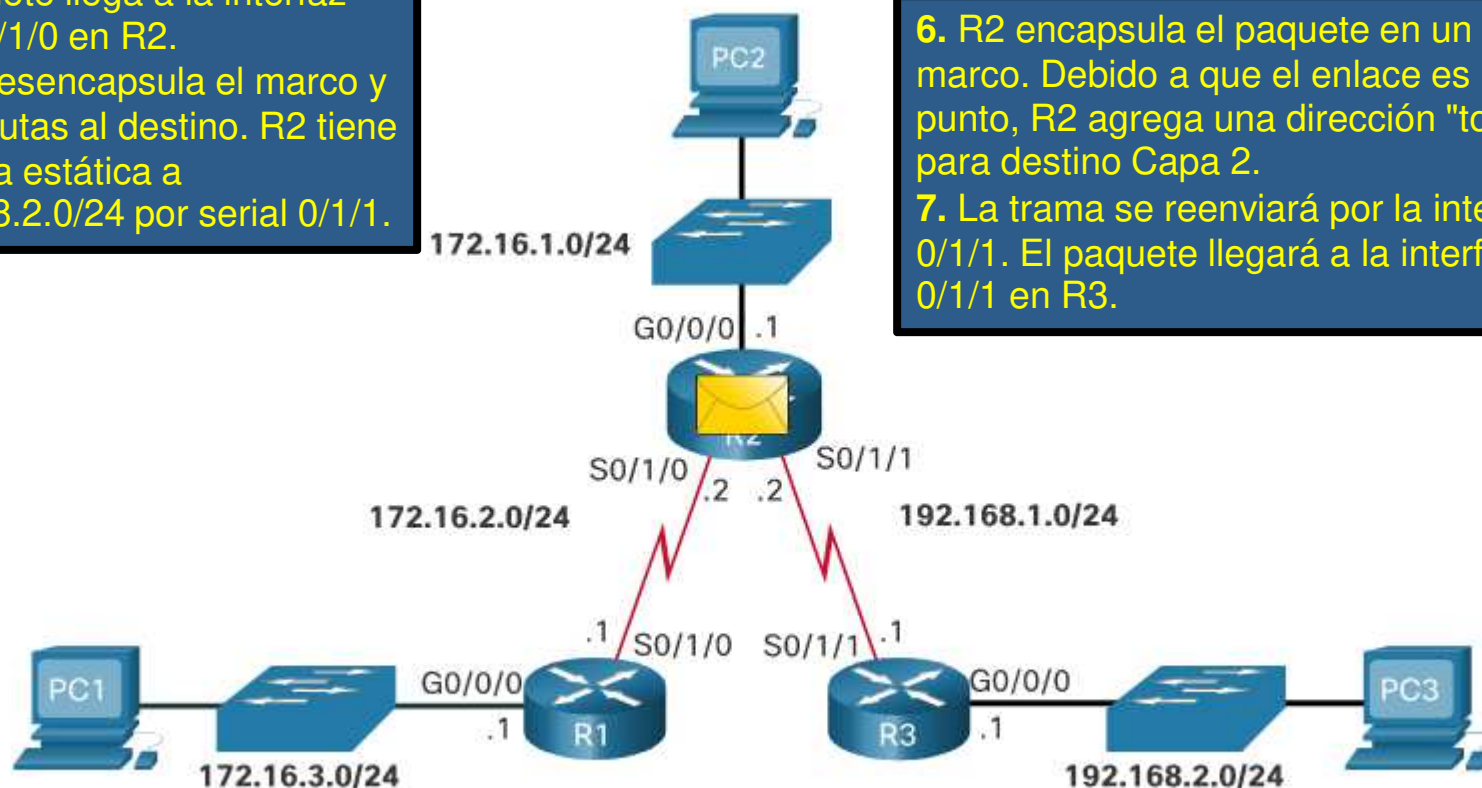


Procesamiento de Paquetes con Rutas Estáticas

- Rutas Estáticas y Re-envío de Paquetes.

- Antes de entrar a la resolución de problemas, se revisará el re-envío de paquetes con rutas estáticas:

El paquete llega a la interfaz serial 0/1/0 en R2.
5. R2 desencapsula el marco y busca rutas al destino. R2 tiene una ruta estática a 192.168.2.0/24 por serial 0/1/1.



6. R2 encapsula el paquete en un nuevo marco. Debido a que el enlace es punto a punto, R2 agrega una dirección "todos 1s" para destino Capa 2.
7. La trama se reenviará por la interfaz serial 0/1/1. El paquete llegará a la interfaz serial 0/1/1 en R3.

Procesamiento de Paquetes con Rutas Estáticas

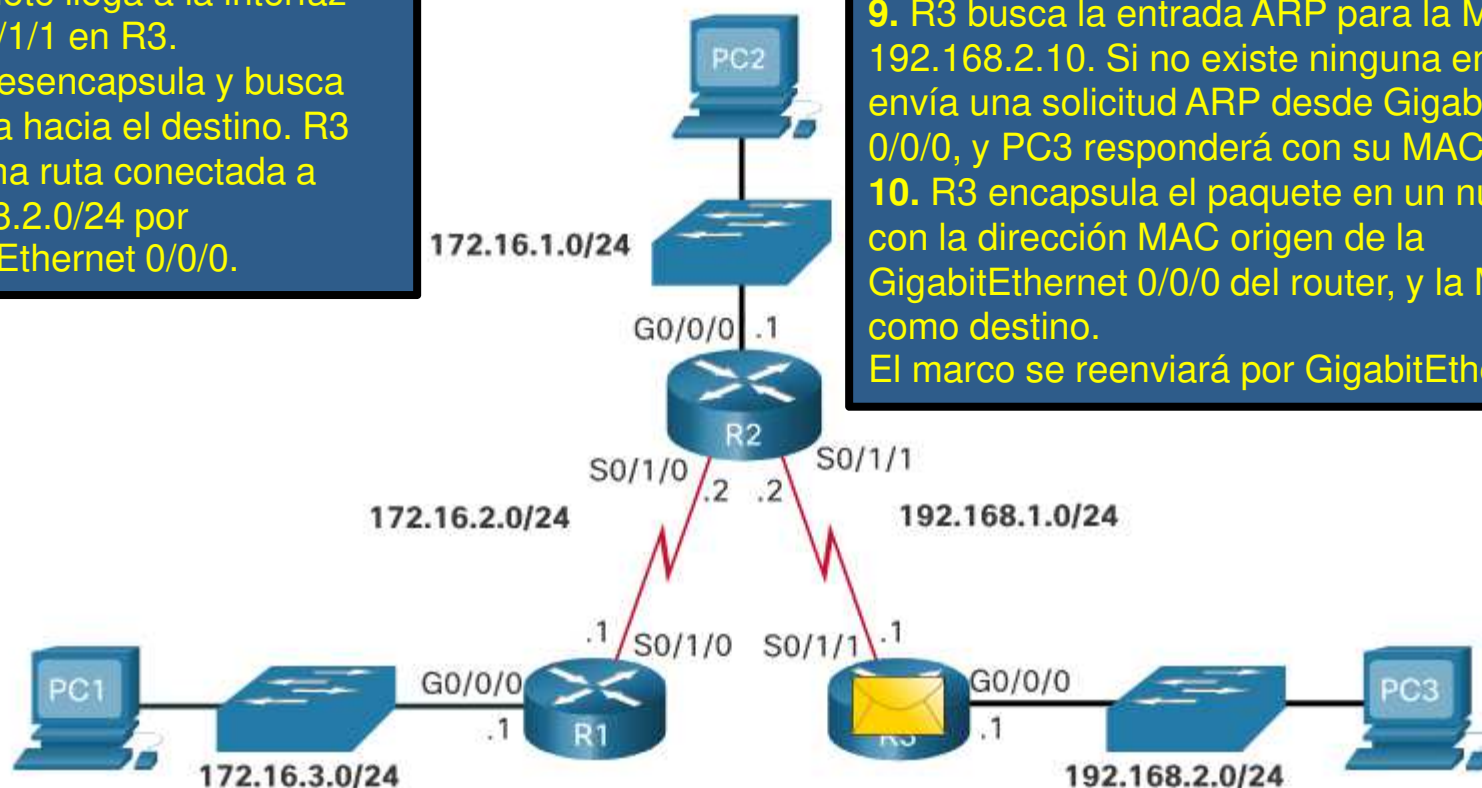
- Rutas Estáticas y Re-envío de Paquetes.

- Antes de entrar a la resolución de problemas, se revisará el re-envío de paquetes con rutas estáticas:

El paquete llega a la interfaz serial 0/1/1 en R3.

8. R3 desencapsula y busca una ruta hacia el destino. R3 tiene una ruta conectada a 192.168.2.0/24 por GigabitEthernet 0/0/0.

9. R3 busca la entrada ARP para la MAC de 192.168.2.10. Si no existe ninguna entrada, R3 envía una solicitud ARP desde GigabitEthernet 0/0/0, y PC3 responderá con su MAC.
10. R3 encapsula el paquete en un nuevo marco con la dirección MAC origen de la GigabitEthernet 0/0/0 del router, y la MAC de PC3 como destino. El marco se reenviará por GigabitEthernet 0/0/0.

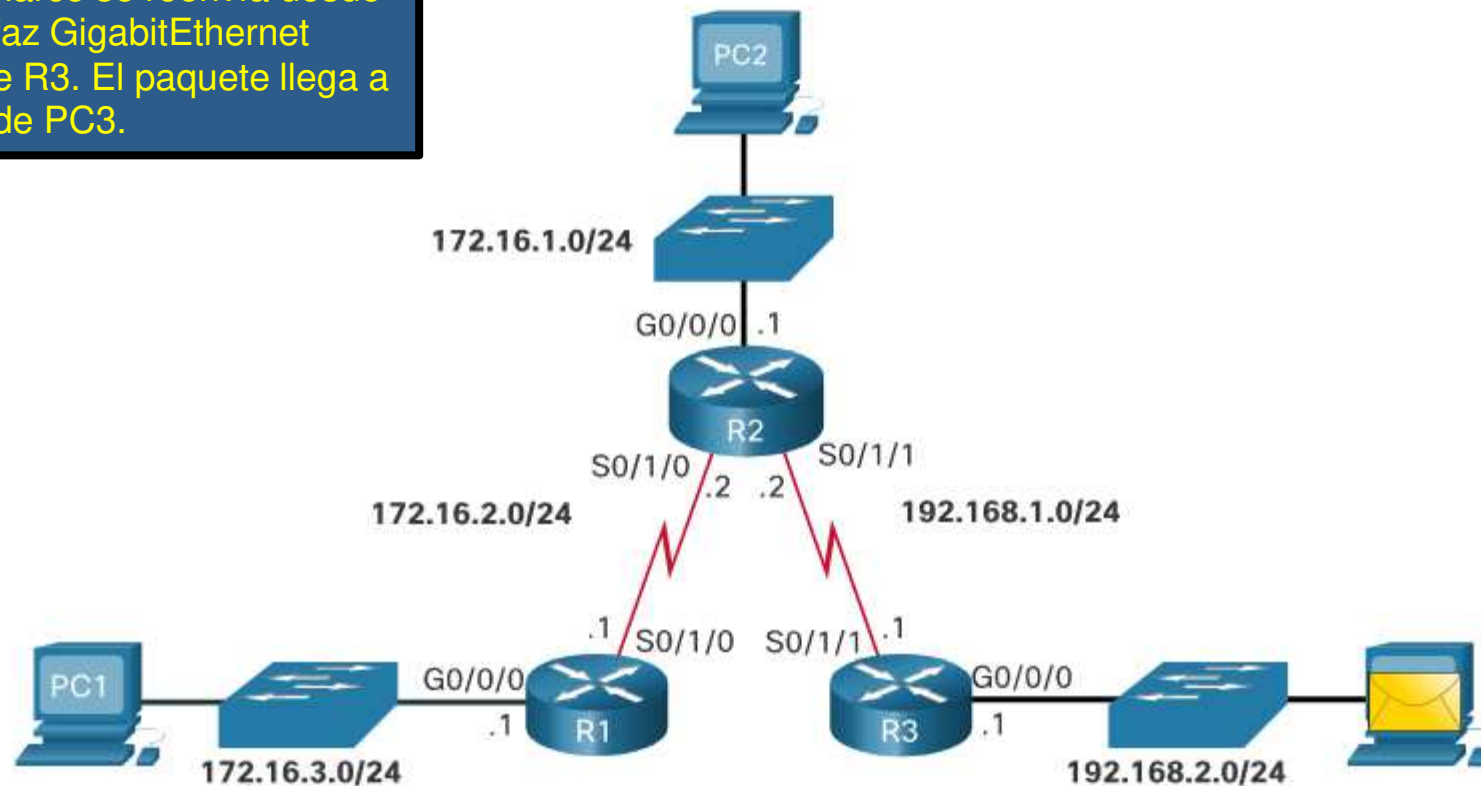


Procesamiento de Paquetes con Rutas Estáticas

- Rutas Estáticas y Re-envío de Paquetes.

- Antes de entrar a la resolución de problemas, se revisará el re-envío de paquetes con rutas estáticas:

11. El marco se reenvía desde la interfaz GigabitEthernet 0/0/0 de R3. El paquete llega a la NIC de PC3.

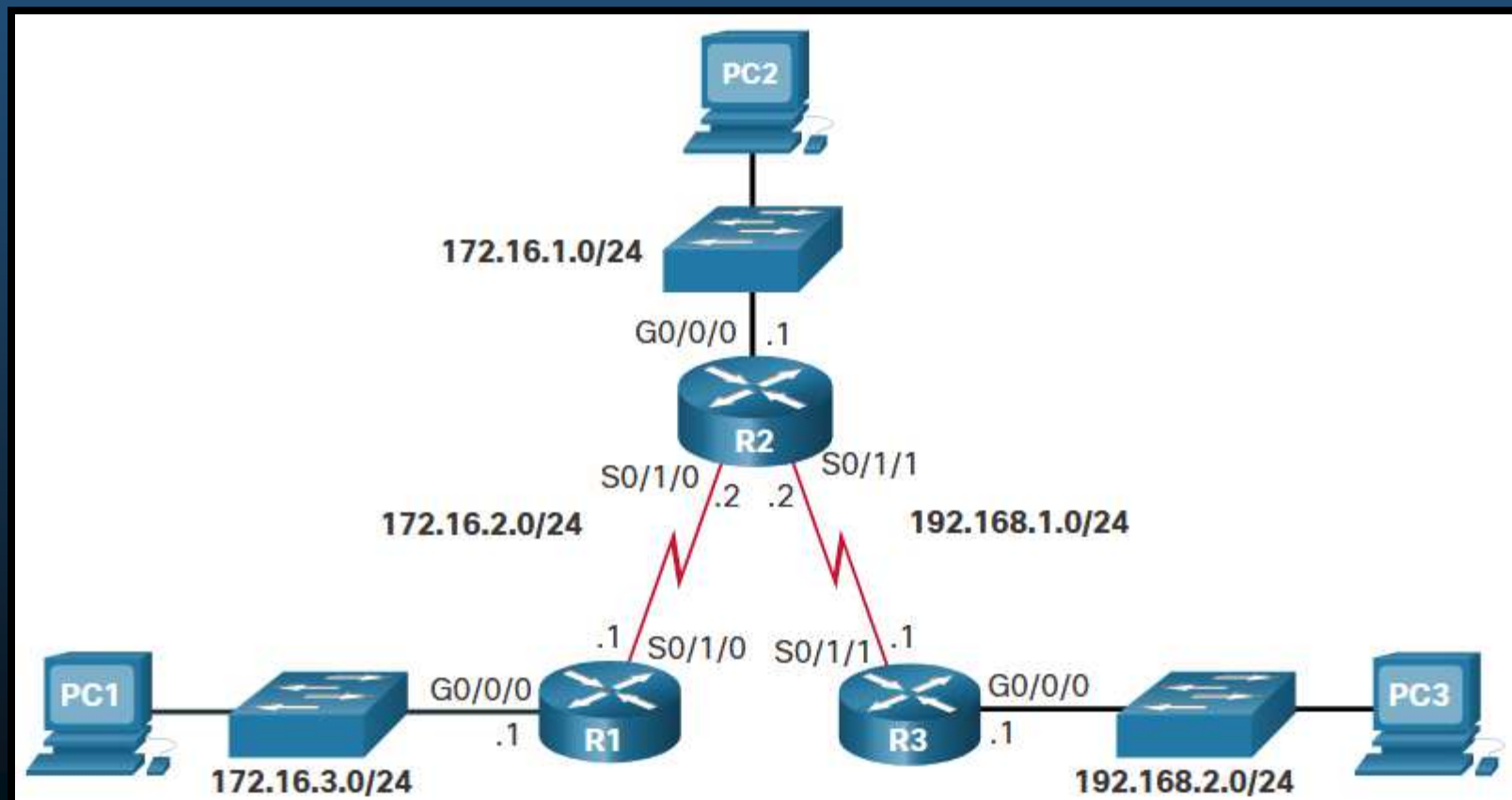


Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Cambios en la Red.
 - Todas las redes son susceptibles a fallos:
 - Fallo de una interfaz.
 - Pérdida de conexión con el ISP.
 - Enlaces sobresaturados.
 - Errores de configuración de algún administrador.
 - Cuando hay un cambio en la red, puede haber pérdidas de comunicación.
 - Es responsabilidad de los administradores resolver el problema.
 - Existen herramientas para aislar problemas de enrutamiento.
 - **ping**
 - **tracert**
 - **show ip route**
 - **show ip interface brief**
 - **show cdp neighbors detail**

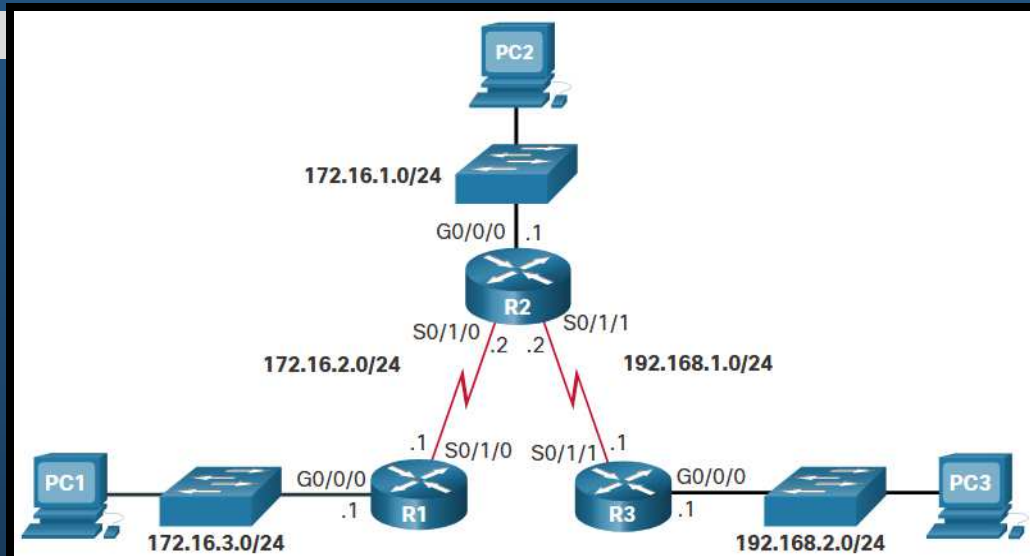
Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Comandos Comunes para Diagnóstico de Problemas.
 - Topología de ejemplo para diagnóstico de problemas:



Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Comandos Comunes para Diagnóstico de Problemas.
 - Un router puede realizar un ping extendido para especificar el origen de un paquete.

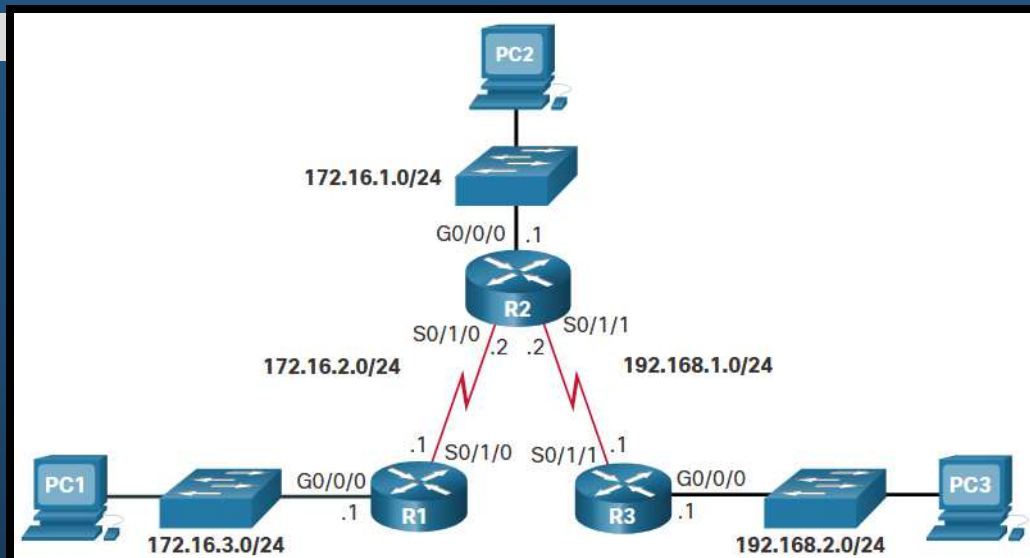


```
R1# ping 192.168.2.1 source 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
R1#
```

- El ejemplo **verifica** el **enrutamiento de 172.16.3.0 a 172.16.2.0**.

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Comandos Comunes para Diagnóstico de Problemas.
 - **traceroute** utiliza ICMP para contar los saltos a un destino.

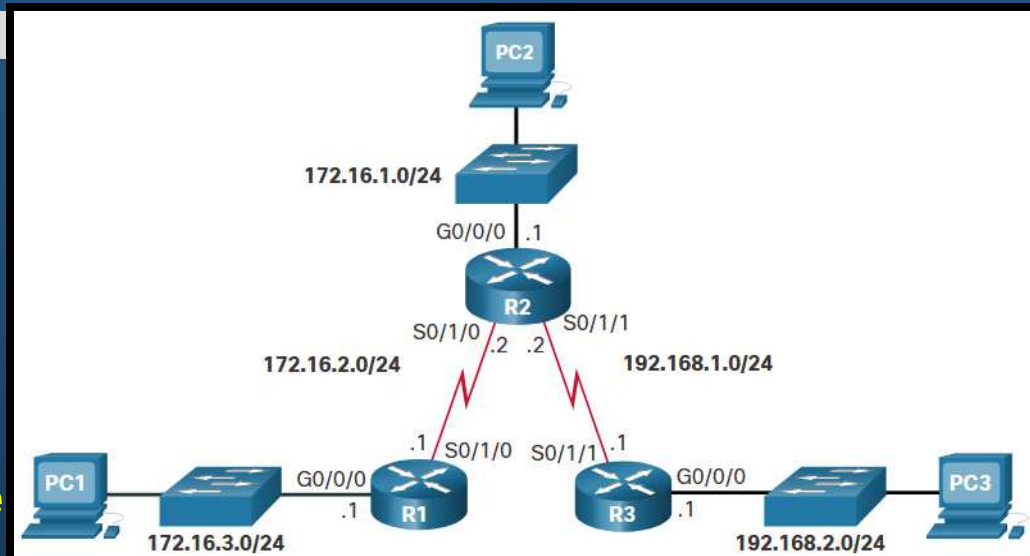


```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.2.2 1 msec 2 msec 1 msec
 2 192.168.1.1 2 msec 3 msec *
R1#
```

- El **ejemplo** muestra el resultado de un **traceroute** de R1 a la LAN de R3.

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

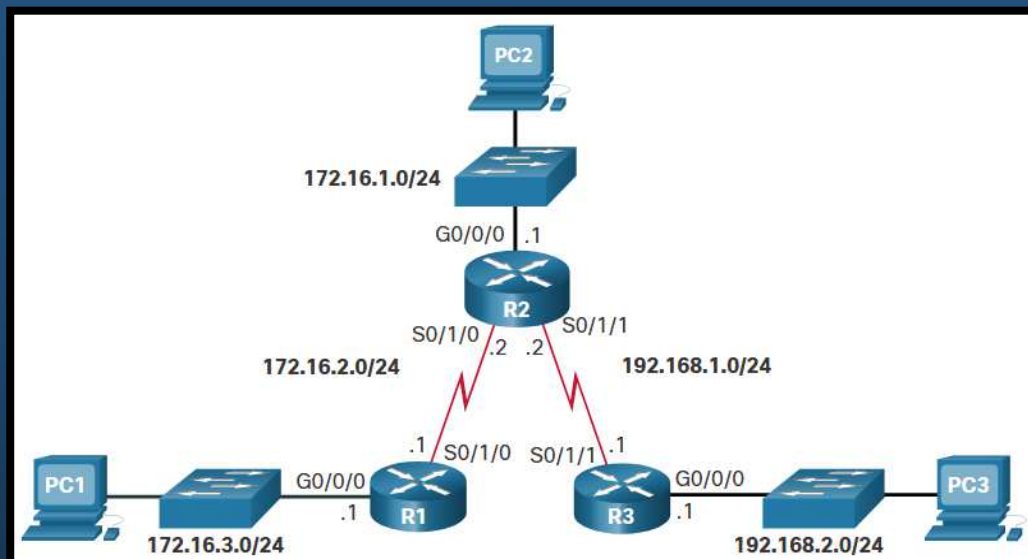
- Comandos Comunes para Diagnóstico de Problemas.
 - Show ip route.
 - El ejemplo despliega la tabla de enrutamiento de R1.



```
R1# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.1.0/24 [1/0] via 172.16.2.2
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.1/32 is directly connected, Serial0/1/0
C       172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S       192.168.1.0/24 [1/0] via 172.16.2.2
S       192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Comandos Comunes para Diagnóstico de Problemas.
 - **show ip interface brief.**
 - El ejemplo despliega el estado resumido de las interfaces de R1.



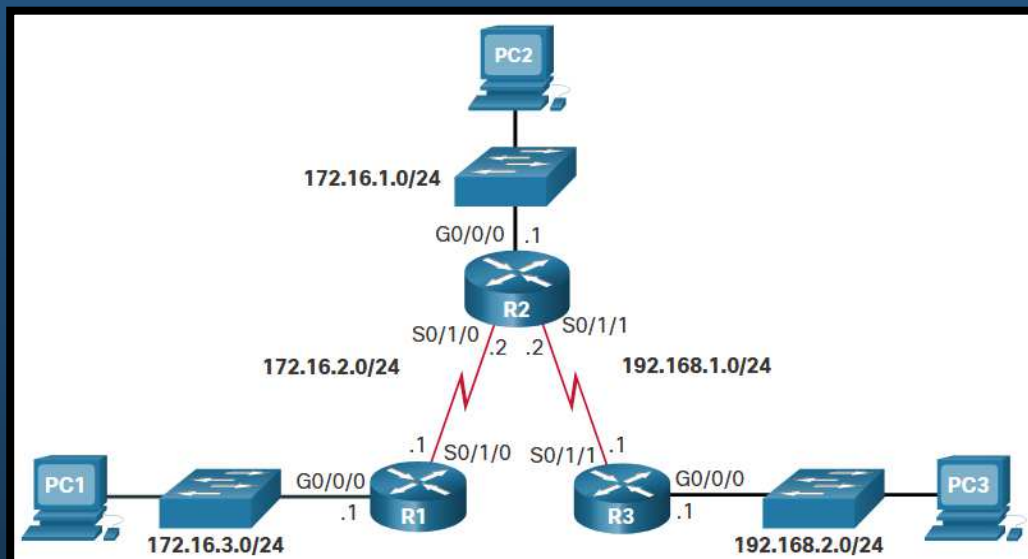
```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	172.16.3.1	YES	manual	up	up
GigabitEthernet0/0/1	unassigned	YES	unset	up	up
Serial0/1/0	172.16.2.1	YES	manual	up	up
Serial0/1/1	unassigned	YES	unset	up	up

```
R1#
```

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Comandos Comunes para Diagnóstico de Problemas.
 - **show cdp neighbors.**
 - El ejemplo despliega la lista de vecinos Cisco de R1.

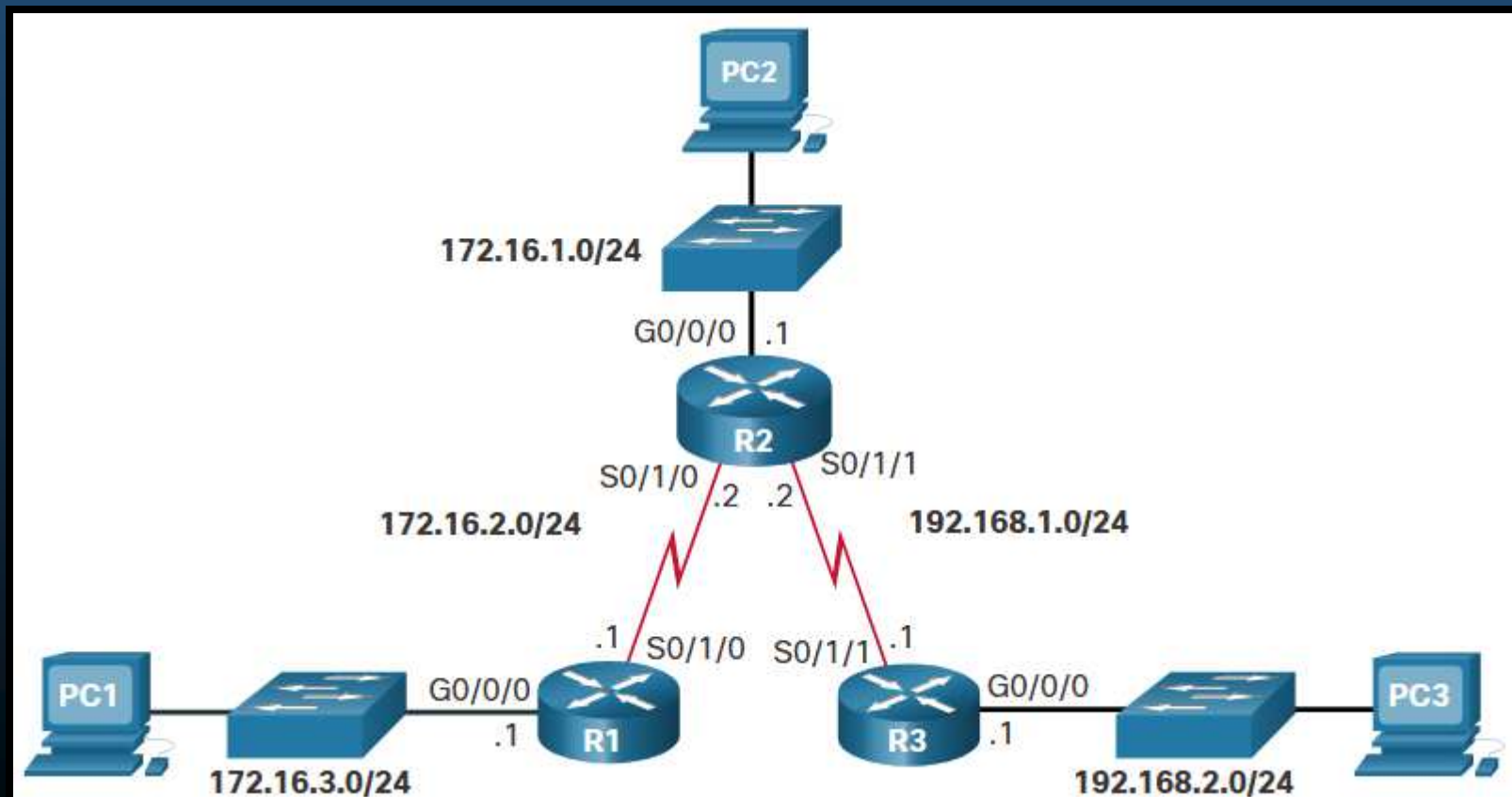


```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
Switch            Gig 0/0/1      129        S I         WS-C3560-  Fas 0/5
R2                Ser 0/1/0      156        R S I       ISR4221/K  Ser 0/1/0
R3                Ser 0/1/1      124        R S I       ISR4221/K  Ser 0/1/0
Total cdp entries displayed : 3
R1#
```

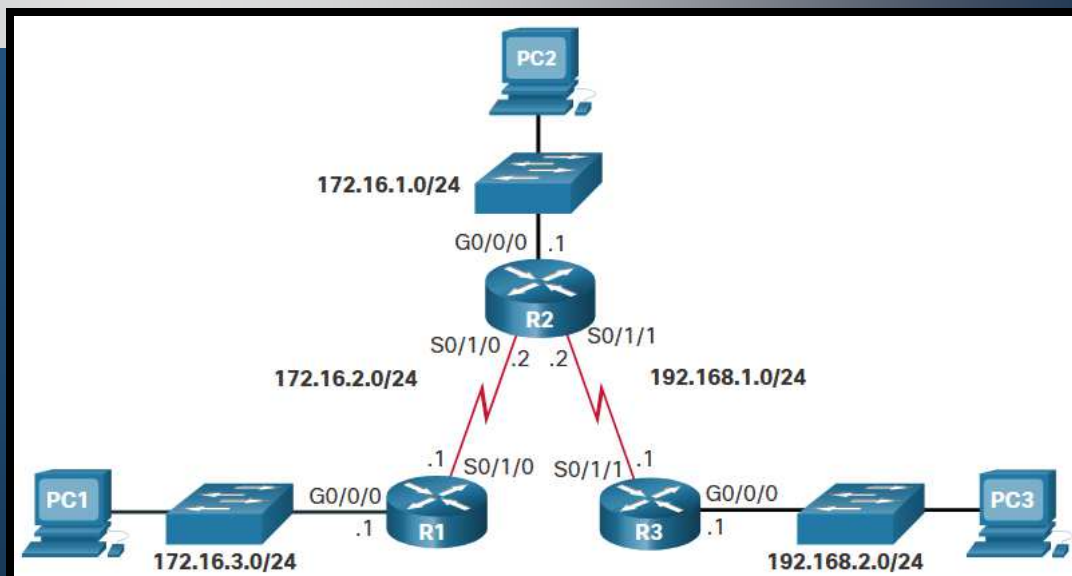

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Resolver un Problema de Conectividad.
 - Encontrar un error de enrutamiento estático es un proceso sencillo si se utilizan las herramientas de manera metódica.
 - Considere la siguiente topología de ejemplo, donde PC1 no puede acceder a la LAN de R3:



Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

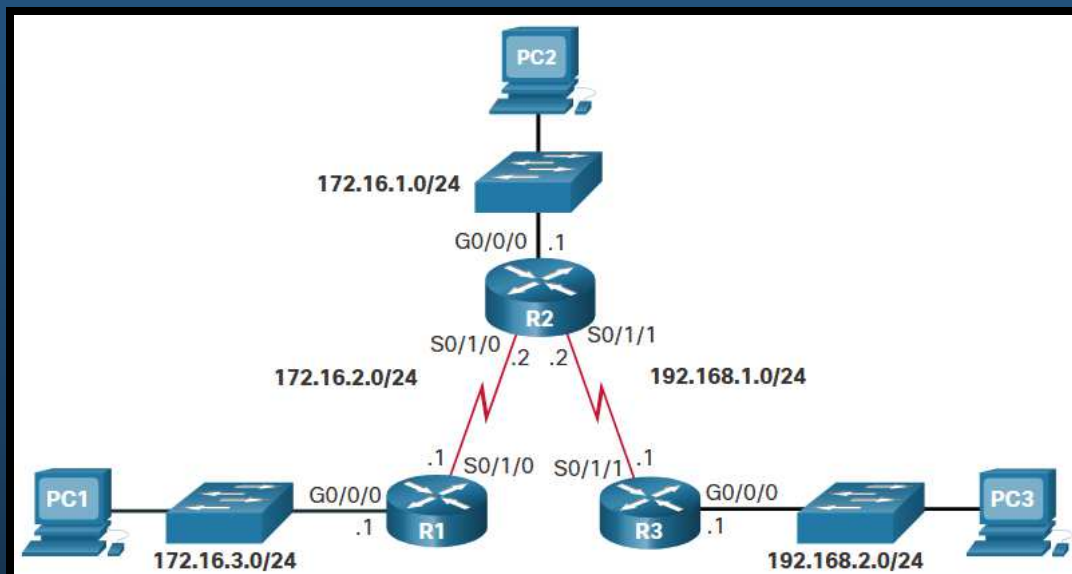
- Resolver un Problema de Conectividad.
 - Hacer ping a la LAN remota desde el router accesible.
 - El ejemplo hace ping desde R1 (desde LAN) en lugar de PC1 y no hay conectividad.



```
R1# ping 192.168.2.1 source g0/0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
.....
Success rate is 0 percent (0/5)
```

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

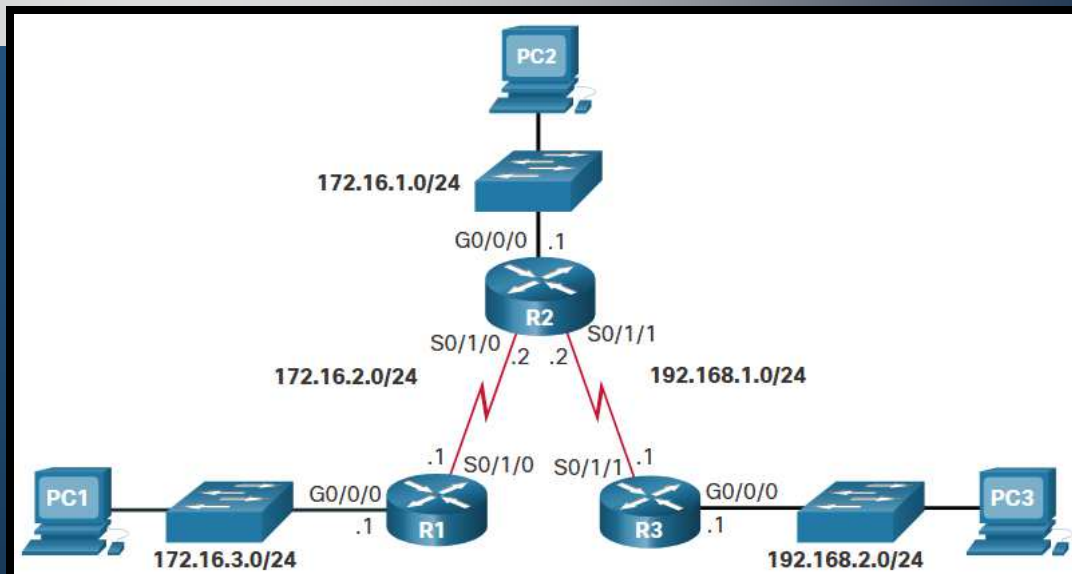
- Resolver un Problema de Conectividad.
 - Hacer ping al siguiente salto.
 - El ejemplo hace ping desde R1 a R2 y es exitoso.



```
R1# ping 172.16.2.2
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 = 3/3/4 ms
```

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Resolver un Problema de Conectividad.
 - Hacer ping a la LAN remota desde el router.
 - El ejemplo hace ping desde R1 (interfaz WAN) y hay conectividad.



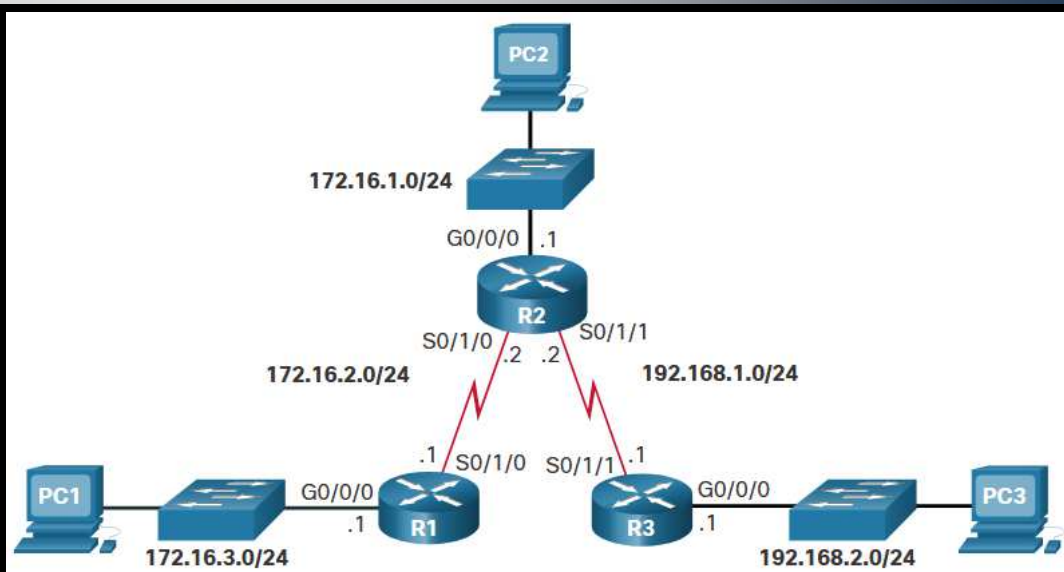
```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
```

- R1 puede hacer ping a LAN de R3, pero no así la LAN de R1.

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Resolver un Problema de Conectividad.

- Verificar las tablas de enrutamiento.
- El ejemplo muestra la tabla de enrutamiento de R2.

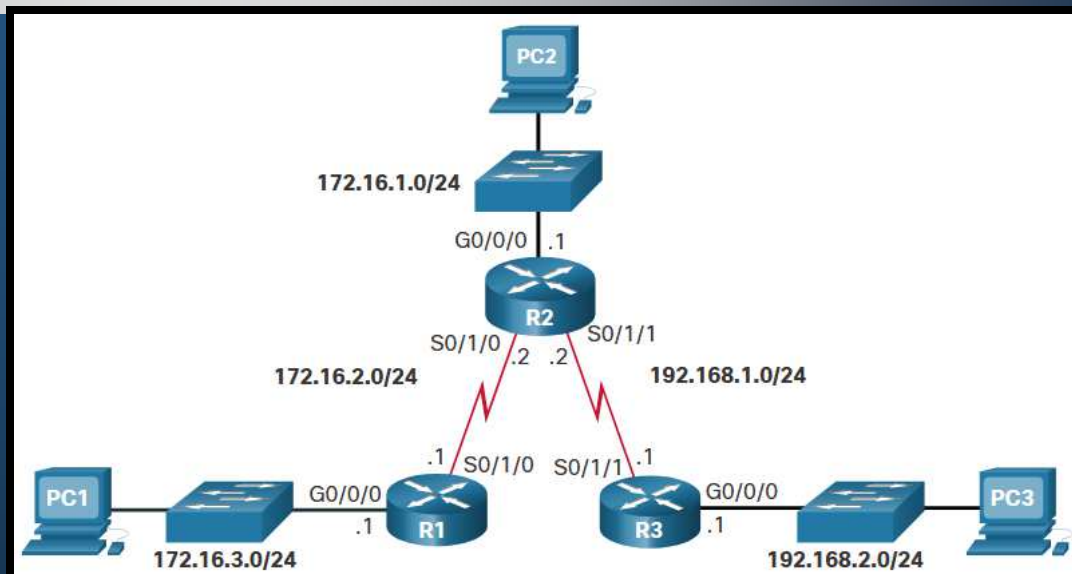


```
R2# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.2/32 is directly connected, Serial0/1/0
S       172.16.3.0/24 [1/0] via 192.168.1.1
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/1/1
L       192.168.1.2/32 is directly connected, Serial0/1/1
S       192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Resolver un Problema de Conectividad.

- Corregir las tablas de enrutamiento.
- El ejemplo corrige la tabla de enrutamiento de R2.

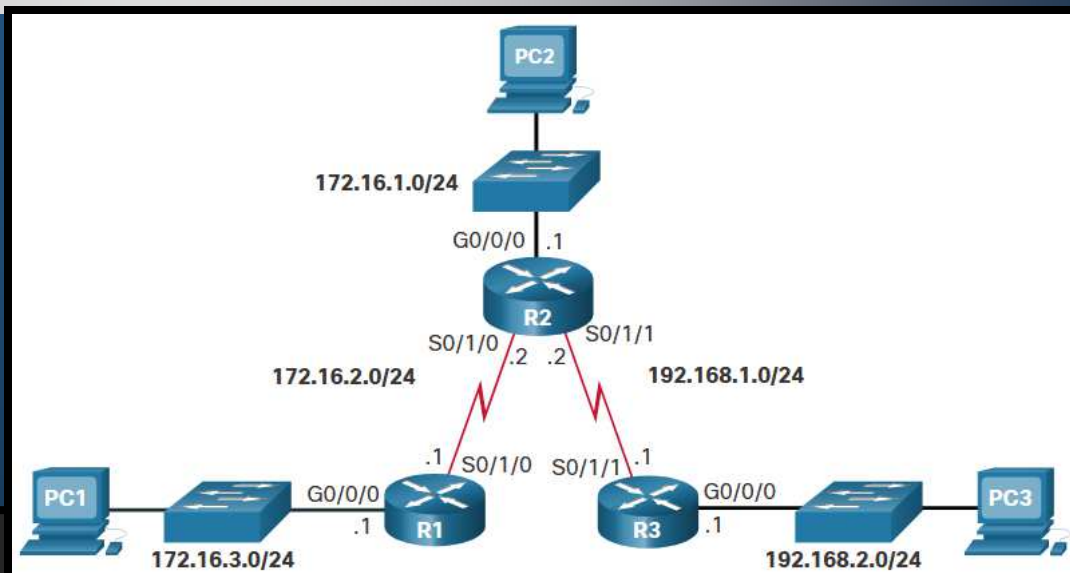


```
R2# show running-config | include ip route
ip route 172.16.3.0 255.255.255.0 192.168.1.1
ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2#
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# no ip route 172.16.3.0 255.255.255.0 192.168.1.1
R2(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#
```

- Remover la ruta errónea y añadir la corregida

Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

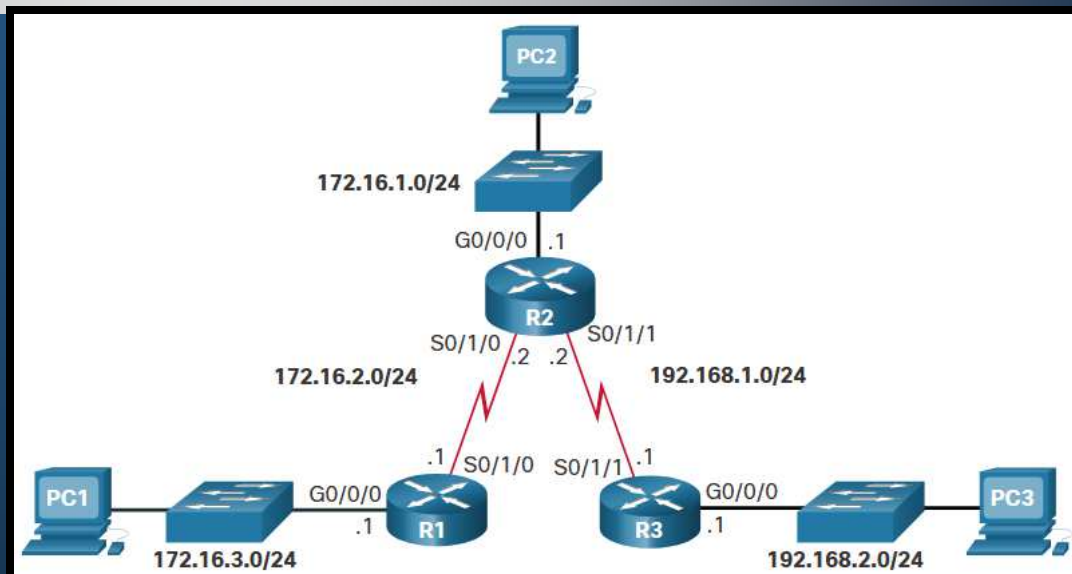
- Resolver un Problema de Conectividad.
 - Verificar las tablas de enrutamiento corregidas.
 - El ejemplo verifica la tabla de enrutamiento de R2.



```
R2# show ip route | begin Gateway
Gateway of last resort is not set
  172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C       172.16.2.0/24 is directly connected, Serial0/1/0
L       172.16.2.2/32 is directly connected, Serial0/1/0
S       172.16.3.0/24 [1/0] via 172.16.2.1
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial0/1/1
L       192.168.1.2/32 is directly connected, Serial0/1/1
S       192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```


Diagnóstico de Problemas con Rutas Estáticas IPv4 Predeterminadas

- Resolver un Problema de Conectividad.
 - Verificar la conectividad.
 - El ejemplo verifica el ping desde la LAN de R1 a la LAN de R3.



```
R1# ping 192.168.2.1 source g0/0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

- Ping exitoso, problema resuelto.

FIN

- Fin del Curso.



Gracias Totales.