

Capacitación de certificación de Huawei

HCIA-Datacom
Ingeniero de Datacom
Guía de laboratorio

V1.0



Huawei Technologies Co., Ltd.

Copyright Huawei Technologies Co., Ltd. 2020. Todos los derechos reservados.

Ninguna parte del presente documento podrá ser reproducida o transmitida de cualquier forma o por cualquier medio sin el previo consentimiento por escrito de Huawei Technologies Co., Ltd.

Marcas y permisos



otras marcas comerciales de Huawei pertenecen a Huawei Technologies Co., Ltd.

Todas las otras marcas y nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Los productos, servicios y funciones adquiridos se estipulan en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, servicios y funciones descritos en este documento no se encuentren dentro del alcance de compra o de uso. A menos que se especifique otra cosa en el contrato, todas las declaraciones, información y recomendaciones que figuran en el presente documento se proporcionan "tal cual" sin garantías, garantías o representaciones de ningún tipo, ya sean explícitas o implícitas.

La información contenida en este documento está sujeta a cambios sin previo aviso. Se ha hecho todo lo posible en la elaboración de este documento para garantizar la exactitud de los contenidos, pero todas las declaraciones, informaciones y recomendaciones contenidas en el presente documento no constituyen garantía de ningún tipo, expresa o implícita.

Huawei Technologies Co., Ltd.

Domicilio: Base industrial de Huawei
Bantian, Longgang.
Shenzhen 518129
People's Republic of China

Sitio web: <https://e.huawei.com/>



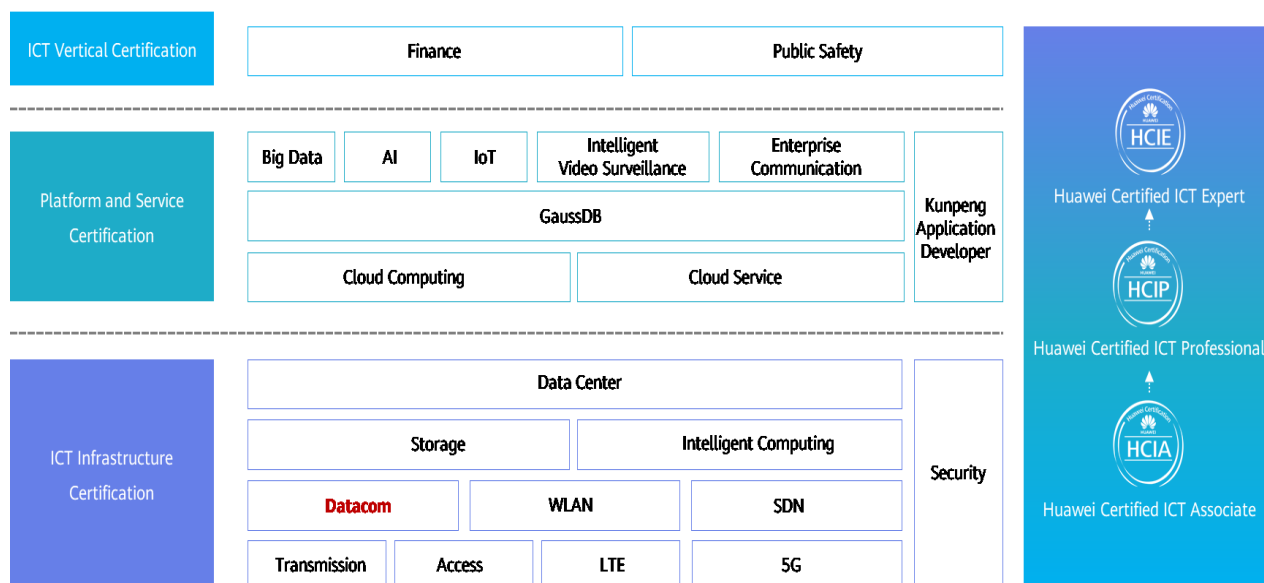
Sistema de certificación de Huawei

La Certificación de Huawei sigue la estrategia de desarrollo "plataforma + ecosistema", que es una nueva arquitectura colaborativa de infraestructura de TIC basada en "Cloud-Pipe-Terminal". Huawei ha establecido un sistema de certificación completo que consta de tres categorías: certificación de infraestructura de TIC, certificación de plataforma y servicio y certificación vertical de TIC. Es el único sistema de certificación que cubre todos los campos técnicos de las TIC en la industria. Huawei ofrece tres niveles de certificación: Huawei Certified TCI Associate (Huawei), Huawei Certified TCI Professional (Huawei) y Huawei Certified TCI Expert (Huawei). La Certificación de Huawei cubre todos los campos de las TIC y se adapta a la tendencia de la industria de convergencia de las TIC. Con su sistema líder de desarrollo de talentos y sus normas de certificación, se ha comprometido a fomentar nuevos talentos en TIC en la era digital y a construir un ecosistema sólido de talentos en TIC.

Huawei Certified TCI Associate-Datacom (HCIA-Datacom) ha sido diseñado para los ingenieros de primera línea de Huawei y para cualquiera que desee comprender los productos y tecnologías de datacom de Huawei. La certificación HCIA-Datacom cubre los principios de enrutamiento y conmutación, los principios básicos de WiFi, los conceptos básicos de seguridad de red, gestión de red y los conceptos básicos de O&M, NDS y programabilidad y automatización.

El sistema de certificación de Huawei presenta la industria, fomenta la innovación e imparte conocimientos de última generación en la esfera de la comunicación de datos.

Certificación



Acerca de este documento

Introducción

Este documento es un curso de capacitación en certificación HCIA-Datacom y está destinado a los alumnos que van a tomar el examen HCIA-Datacom o lectores que quieran entender los principios de enrutamiento y conmutación, los principios básicos de la red WiFi, los conceptos básicos de seguridad de la red, Gestión de red y conceptos básicos de O&M, RDS y programabilidad y automatización.

Antecedentes necesarios

Este curso es para la certificación básica de Huawei. Para entender mejor este curso, familiarícese con los siguientes requisitos:

- Conocimientos informáticos básicos
- Conocimiento básico de la comunicación de datos

Convenciones de símbolos



—————
Cable Ethernet



- - - - -
Cable Serial



Entorno de laboratorio

Descripción de la Red

Este entorno de laboratorio está destinado a ingenieros de datacom que se están preparando para el examen HCIA-Datacom. Cada entorno de laboratorio incluye dos switches (no compatible con PoE), dos switches PoE, dos puntos de acceso inalámbricos (AP) y dos routers.

Requerimientos del dispositivo

Para cumplir con los requerimientos de ejercicio, las configuraciones recomendadas del entorno son las siguientes:

La siguiente tabla enumera los dispositivos requeridos:

Nombre del dispositivo	Modelo de dispositivo	Versión de software
Cambiar	CloudEngine S5731-H24T4XC	V200R019C00 o posterior
Switch PoE	CloudEngine S5731-H24P4XC	V200R019C00 o posterior
PA	AirEngine 5760-10	V200R009 o posterior
Router	NetEngine AR651C	V300R019 o posterior



La información de puerto, salida y configuración de los dispositivos en este documento se proporciona en base a la topología recomendada. La información real puede variar según el entorno del laboratorio.



Contenido

Acerca de este documento	3
1. Básicos de VRP y configuración de Huawei	11
1.1. Introducción.....	错误!未定义书签。
1.1.1. Acerca de este laboratorio.....	11
1.1.2. Objetivos.....	11
1.1.3. Topología de redes	11
1.2. Configuración del laboratorio	12
1.2.1. Configuración Roadmap	错误!未定义书签。
1.2.2. Procedimiento de configuración.....	12
1.3. Verificación.....	18
1.4. Referencia de configuración	18
1.5. Verificación.....	错误!未定义书签。
1.6. Apéndice	18
2. Creación de una red IP interconectada	20
2.1. Laboratorio 1: Dirección y enrutamiento IPv4.....	20
2.1.1. Introducción.....	错误!未定义书签。
2.1.1.1. Acerca de este laboratorio.....	20
2.1.1.2. Objetivos.....	20
2.1.1.3. Topología de networking.....	21
2.1.2. Configuración de laboratorio.....	21
2.1.2.1. Configuración Roadmap.....	错误!未定义书签。
2.1.2.2. Procedimiento de configuración.....	21
2.1.3. Verificación	31
2.1.4. Referencia de configuración.....	31
2.1.5. Quiz	32
2.2. Laboratorio 2: Enrutamiento de OSPF	33
2.2.1. Introducción	错误!未定义书签。
2.2.1.1. Acerca de este laboratorio	33
2.2.1.2. Objetivos	33
2.2.1.3. Topología de redes.....	33



2.2.2. Configuración del laboratorio.....	34
2.2.2.1. Configuración Roadmap.....	错误!未定义书签。
2.2.2.2. Procedimiento de configuración.....	34
2.2.3. Verificación	40
2.2.4. Referencia de configuración.....	40
2.2.5. Quiz	41
3 Creación de una red Ethernet conmutada	42
3.1. Laboratorio 1: Configuración básica de Ethernet y VLANs	42
3.1.1 . Introducción	错误!未定义书签。
3.1.1.1. Acerca de este laboratorio	42
3.1.1.2. Objetivos.	42
3.1.1.3. Topología de networking.....	43
3.1.2. Configuración de laboratorio.....	43
3.1.2.1. Configuración Roadmap.....	错误!未定义书签。
3.1.2.2. Procedimiento de configuración.....	43
3.1.3. Verificación	49
3.1.4. Referencia de configuración.....	49
3.1.5. Quiz	50
3.2. Laboratorio 2: Árbol de expansión	52
3.2.1. Introducción	错误!未定义书签。
3.2.1.1. Acerca de este laboratorio	52
3.2.1.2. Objetivos.	52
3.2.1.3. Topología de networking.....	52
3.2.2. Configuración de laboratorio.....	53
3.2.2.1. Configuración Roadmap.....	错误!未定义书签。
3.2.2.2. Procedimiento de configuración.....	53
3.2.3. Verificación	60
3.2.4. Referencia de configuración.....	61
3.2.5. Quiz	62
3.3. Laboratorio 3: Agregación de enlaces Ethernet	63
3.3.1. Introducción	63
3.3.1.1. Acerca de este laboratorio	63
3.3.1.2. Objetivos.	63
3.3.1.3. Topología de networking.....	63
3.3.2. Configuración de laboratorio.....	64
3.3.2.1. Configuración Roadmap.....	错误!未定义书签。



3.3.2.2. Procedimiento de configuración.....	64
3.3.3. Verificación	70
3.3.4. Referencia de configuración.....	70
3.3.5. Quiz	71
3.4. Laboratorio 4: Comunicación entre VLAN	72
3.4.1. Introducción	错误!未定义书签。
3.4.1.1. Acerca de este laboratorio	72
3.4.1.2. Objetivos.....	72
3.4.1.3. Topología de networking.....	72
3.4.2. Configuración de laboratorio.....	73
3.4.2.1. Configuración Roadmap.....	错误!未定义书签。
3.4.2.2. Procedimiento de configuración.....	73
3.4.3. Verificación	76
3.4.4. Referencia de configuración.....	76
3.4.5. Quiz	77
4 Conceptos básicos de seguridad de red y acceso a la red.....	78
4.1. Laboratorio 1: Configuración de LCA	78
4.1.1. Introducción	错误!未定义书签。
4.1.1.1. Acerca de este laboratorio	78
4.1.1.2. Objetivos.	78
4.1.1.3. Topología de networking.....	78
4.1.2. Configuración de laboratorio.....	79
4.1.2.1. Configuración Roadmap.....	错误!未定义书签。
4.1.2.2. Procedimiento de configuración.....	79
4.1.3. Verificación	83
4.1.4. Referencia de configuración (método 1).....	83
4.1.5. Referencia de configuración (método 2).....	84
4.1.6. Quiz	85
4.2. Laboratorio 2: Configuración local de AAA.....	87
4.2.1. Introducción	错误!未定义书签。
4.2.1.1. Acerca de este laboratorio	87
4.2.1.2. Objetivos.	876
4.2.1.3. Topología de networking.....	87
4.2.2. Configuración de laboratorio.....	88
4.2.2.1. Configuración Roadmap.....	错误!未定义书签。
4.2.2.2. Procedimiento de configuración.....	88



4.2.3. Verificación	90
4.2.4. Referencia de configuración.....	90
4.2.5. Quiz	错误!未定义书签。
4.3. Laboratorio 3: Configuración de NAT	91
4.3.1. Introducción	错误!未定义书签。
4.3.1.1. Acerca de este laboratorio	91
4.3.1.2. Objetivos.....	91
4.3.1.3. Topología de networking.....	92
4.3.2. Configuración de laboratorio.....	92
4.3.2.1. Configuración Roadmap.....	错误!未定义书签。
4.3.2.2. Procedimiento de configuración.....	92
4.3.3. Verificación	97
4.3.4. Referencia de configuración.....	97
4.3.5. Quiz	98
5 Configuración básica de aplicaciones y servicios de red	99
5.1. Laboratorio 1: Configuración de FTPComment.....	99
5.1.1. Introducción	错误!未定义书签。
5.1.1.1. Acerca de este laboratorio	99
5.1.1.2. Objetivos.....	99
5.1.1.3. Topología de networking.....	99
5.1.2. Configuración de laboratorio.....	100
5.1.2.1. Configuración Roadmap.....	错误!未定义书签。
5.1.2.2. Procedimiento de configuración.....	100
5.1.3. Verificación	103
5.1.4. Referencia de configuración.....	104
5.1.5. Quiz	错误!未定义书签。
5.2. Laboratorio 2: Configuración de DHCP	106
5.2.1. Introducción	错误!未定义书签。
5.2.1.1. Acerca de este laboratorio	106
5.2.1.2. Objetivos.....	106
5.2.1.3. Topología de networking.....	106
5.2.2. Configuración de laboratorio.....	107
5.2.2.1. Configuración Roadmap.....	错误!未定义书签。
5.2.2.2. Procedimiento de configuración.....	107
5.2.3. Verificación	109
5.2.3.1. Muestra las direcciones IP y las rutas de R1 y R3.....	1098



5.2.3.2. Muestra la asignación de direcciones en R2.....	110
5.2.4. Referencia de configuración.....	111
5.2.5. Quiz	错误!未定义书签。
Creación de una red local inalámbrica (WLAN).....	113
6.1. Introducción.....	错误!未定义书签。
6.1.1. Acerca de este laboratorio.....	113
6.1.2. Objetivos.....	113
6.1.3. Topología de networking	113
6.1.4. Planificación de datos.....	114
6.2. Configuración de laboratorio	115
6.2.1. Configuración Roadmap	错误!未定义书签。
6.2.2. Procedimiento de configuración.....	115
6.3. Verificación.....	122
6.4. Referencia de configuración	122
6.5. Quiz	错误!未定义书签。
6.6 Apéndice	125
7. Creación de una red IPv6.....	127
7.1. Introducción.....	错误!未定义书签。
7.1.1. Acerca de este laboratorio.....	127
7.1.2. Objetivos.....	127
7.1.3. Topología de networking	127
7.2. Configuración de laboratorio	128
7.2.1. Configuración Roadmap	错误!未定义书签。
7.2.2. Procedimiento de configuración.....	128
7.3. Verificación.....	135
7.4. Referencia de configuración	135
7.5. Quiz	错误!未定义书签。
8. Conceptos básicos de programación y automatización de redes.....	138
8.1. Introducción.....	错误!未定义书签。
8.1.1. Acerca de este laboratorio.....	138
8.1.2. Objetivos.....	138
8.1.3. Topología de networking	138
8.2. Configuración de laboratorio	139
8.2.1. Configuración Roadmap	错误!未定义书签。
8.2.2. Procedimiento de configuración.....	139



8.2.3. Interpretación del código	141
8.3. Verificación.....	143
8.4. Referencia de configuración	143
8.5. Quiz	错误!未定义书签。
9. Configuración de una red de campus.....	145
9.1. Información de referencia	145
9.2. Introducción.....	错误!未定义书签。
9.2.1. Acerca de este laboratorio.....	145
9.2.2. Objetivos.....	146
9.2.3. Topología de networking	146
9.3. Tareas de laboratorio.....	146
9.3.1. Recolección y análisis de requerimientos.....	146
9.3.2. Planificación y diseño	148
9.3.3. Aplicación.....	158
9.3.4. Red de O&M.....	163
9.3.5. Optimización de la red.....	165
9.4. Verificación.....	165
9.5. Referencia de configuración	165
9.6. Quiz	错误!未定义书签。
Respuestas de referencia	187



1

Fundamentos de configuración y VRPs de Huawei

1.1 Introducción

1.1.1 Acerca de este laboratorio

En esta actividad de laboratorio, se aprenden las operaciones básicas del sistema de VRPs de Huawei mediante la configuración de los dispositivos de Huawei.

1.1.2 Objetivos.

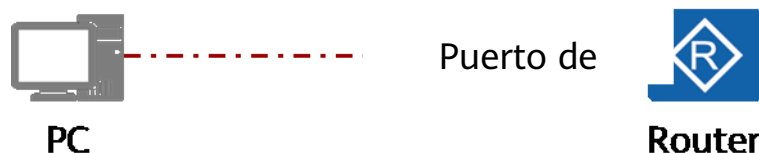
Una vez completada esta tarea, podrá:

- Comprender el significado de las vistas de la línea de comandos y cómo acceder y salir de las vistas de la línea de comandos
- Comprender los comandos comunes
- Comprender cómo usar la ayuda en línea de la línea de comandos
- Aprenda a negar un comando
- Aprenda a usar las teclas de acceso directo de la línea de comandos

1.1.3 Topología de networking

Como se muestra en el siguiente diagrama de networking, el router es un router nuevo sin ninguna configuración. El ordenador se conecta al puerto de consola del router a través de un cable serie. Se debe inicializar el router.

Figure 1-1 Topología de laboratorio para entender el sistema operativo del VRPName





1.2 Configuración de laboratorio

1.2.1 Configuración Roadmap

1. Configuraciones básicas completas, como el nombre del dispositivo y la dirección IP de la interfaz del router.
2. Guarde las configuraciones.
3. Reinicie el dispositivo.

1.2.2 Procedimiento de configuración

Step 1 Inicie sesión en la interfaz de usuario de cliente del router a través del puerto de consola.

Los detalles no se proporcionan aquí.

Step 2 Muestra la información básica del dispositivo.

Muestra información sobre la versión del dispositivo.

```
<Huawei> versión de pantalla
Software de plataforma de enrutamiento versátil de Huawei
Software de VPR (R), Versión 5.160 (AR651C V300R019C00SPC100)
Copyright (C) 2011-2016 HUAWEI Tech Co., LDA
El tiempo de actividad del router AR651C de Huawei es de 0 semanas, 0 días, 0 horas y 53 minutos.
Información sobre la version 0 de BKP:
1. Versión de PCB : AR01BAK2C VER.B
2. En caso de apoyar a los PoE : No
3. Tipo de tarjeta : AR651C
4. Cantidad de ranuras de la MPU : 1
5. Cantidad de ranuras LPU : 1
```

Step 3 Configuraciones básicas completas de dispositivos.

Cambie el nombre del router a **Datacom-Router**.

```
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
Ha ingresado la vista del sistema desde la vista del usuario.
[Huawei]sysname Datacom-Router
[Datacom-Router]
El nombre del dispositivo se ha cambiado a Datacom-Router.
```

Los dispositivos de Huawei ofrecen una amplia variedad de funciones y comandos de consulta y configuración relacionados. Los comandos están disponibles en diferentes vistas de comandos según las funciones de los comandos. Para utilizar una función, primero ingrese la vista de comandos correspondiente y luego ejecute los comandos correspondientes.

Ingrese a la vista de la interfaz y configure la dirección IP de la interfaz.

```
[Datacom-Router]inter //Press Tab to complete the command.
[Datacom-Router]interface // "interface" is the only optional keyword.
```



```
[Datacom-Router]interface g //Press Tab to complete the command.  
[Datacom-Router]interface GigabitEthernet // "GigabitEthernet" is the only optional keyword.  
[Datacom-Router]interface GigabitEthernet 0/0/1 //Enter the complete command.
```

Introduzca las primeras letras de una keyword en un comando y pulse Tab para mostrar una keyword completa. Las primeras letras, sin embargo, deben identificar la keyword de forma única. Si no identifican una keyword específica, presione Tab continuamente hasta que aparezca la keyword deseada. Por ejemplo:

Cuando se introduce **inter** y se pulsa Tab, sólo el comando de **interface** comienza con **inter**. Por lo tanto, el comando se autocompleta como **interface**. El comando no cambia si pulsa Tab varias veces.

```
[Datacom-Router-GigabitEthernet00/1]  
Se muestra la vista de la interfaz GigabitEthernet0/ 0/ 1.  
[Datacom-Router-GigabitEthernet0/0/1]i?  
icmp <Group> icmp command group  
igmp Specify parameters for IGMP  
ip <Group> ip command group  
ipsec Specify IPSec(IP Security) configuration information  
ipv6 <Group> ipv6 command group  
isis Configure interface parameters for ISIS
```

Si introduce sólo el primer o los primeros caracteres de una keyword de comando, puede utilizar la función de ayuda contextual para obtener todas las keywords que comienzan con un carácter o cadena de caracteres. También se mostrará el significado de cada keyword. Por ejemplo:

En la vista de la interfaz GigabitEthernet0, ingrese i y un signo de interrogación (?) para mostrar las opciones de todos los comandos comenzando con i en la vista actual. Puede presionar Tab para completar el comando de manualmente ingrese el comando completo de acuerdo con la información de ayuda. En la información anterior, **icmp** e **igmp** son keywords, **<Group> icmp command group** y **Specify parameters for IGMP** son las descripciones de las keywords.

```
[Datacom-Router-GigabitEthernet0/0/1]ip ?  
accounting <Group> accounting command group  
address <Group> address command group  
binding Enable binding of an interface with a VPN instance  
fast-forwarding Enable fast forwarding  
forward-broadcast Specify IP directed broadcast information  
netstream IP netstream feature  
verify IP verify
```

Al introducir algunas keywords de un comando y un signo de interrogación (?) separados por un espacio, se muestran todas las keywords asociadas a este comando, así como descripciones simples. Por ejemplo:

Si introduce **ip**, un espacio y un signo de interrogación (?), se muestran todos los comandos que contienen la keyword **ip** y las descripciones correspondientes.

```
[Datacom-Router-GigabitEthernet0/0/1]ip address ?  
IP_ADDR<X.X.X.X> IP address  
bootp-alloc IP address allocated by BOOTP  
dhcp-alloc IP address allocated by DHCP
```



unnumbered	Share an address with another interface
[Datacom-Router-GigabitEthernet0/0/1]ip address 192.168.1.1 ?	
INTEGER<0-32>	Length of IP address mask
IP_ADDR<X.X.X.X>	IP address mask
[Datacom-Router-GigabitEthernet0/0/1]ip address 192.168.1.1 24 ?	
sub	Indicate a subordinate address
<cr>	Please press ENTER to execute command

<cr> indica que no existe ninguna keyword o parámetro en esta posición. Pulse Enter para ejecutar el comando.

```
[Datacom-Router-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#
```

El comando **display this** muestra la configuración en ejecución en la vista actual. Los argumentos efectivos establecidos en sus predeterminados no se muestran. Tampoco se muestran argumentos configurados que no se han comprometido correctamente. Este comando se utiliza para verificar la configuración.

No es necesario introducir keywords completas si los caracteres introducidos pueden coincidir con una keyword única en la vista actual. Esta función mejora la eficiencia. Por ejemplo:

El comando **dis this** se puede ejecutar en una interfaz porque sólo el comando **display this** coincide con los caracteres introducidos en la vista actual. Del mismo modo, también se puede ejecutar el comando **dis cu** o **d cu** porque son equivalentes al comando **display current-configuration**.

```
[Datacom-Router-GigabitEthernet0/0/1]quit
```

El comando **quit** devuelve un dispositivo desde la vista actual a una vista de nivel inferior. Si la vista actual es la vista de usuario, este comando sale del sistema.

Negar la configuración de la dirección IP porque la dirección IP debe ser firmada para interfaz GigabitEthernet 0/0/2.

```
[Datacom-Router]interface GigabitEthernet 0/0/1
[Datacom-Router-GigabitEthernet0/0/1]undo ip address
```

Para ello, debe anular la configuración de dirección IP de GigabitEthernet0/0/1. De lo contrario, se produce un conflicto de direcciones IP y la configuración falla.

Para anular un comando, utilice la keyword **undo** con el comando. Por lo general, se utiliza un comando undo para restablecer una configuración predeterminada, deshabilitar una función o eliminar una configuración. Casi toda línea de comandos tiene un comando de deshacer correspondiente.

```
[Datacom-Router]interface GigabitEthernet 0/0/2
[Datacom-Router-GigabitEthernet0/0/2]ip address 192.168.1.1 24
[Datacom-Router-GigabitEthernet0/0/2]quit
```

Muestra la configuración actual del dispositivo.



```
[Datacom-Router]display current-configuration
[V200R003C00]
#
sysname Datacom-Router
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent
#
clock timezone China-Standard-Time minus 08:00:00
#
portal local-server load portalpage.zip
#
drop illegal-mac alarm
#
set cpu-usage threshold 80 restore 75
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %$%$K8m.Nt84DZ}e#<0`8bmE3Uw}%$%$
 local-user admin service-type http
#
---- More ----
```

Cuando la información no puede ser mostrada completamente en una pantalla, el sistema se detendrá para que pueda ver la información. Si ---- **More** ----- se muestra en la parte inferior de la salida de comandos, puede

1. Presione Ctrl+C o Ctrl+Z para detener la ejecución de la pantalla o de los comandos.
2. Presione la barra de espacio para mostrar la siguiente pantalla.
3. Presione Enter para mostrar la siguiente línea.

Step 4 Guardar la configuración actual del dispositivo.

Volver a la vista de usuario.

```
[Datacom-Router]
<Datacom-Router>
```

Además del comando **quit**, también puede:

1. Ejecute el comando **return** para volver a la vista de usuario desde cualquier vista.
2. Presione Ctrl+Z para volver a la vista del usuario desde cualquier vista.

Guardar la configuración. *// Entrar y para confirmar.*

```
<Datacom-Router>save
The current configuration will be written to the device.
Are you sure to continue? .(y/n)[n]:y                               //Enter y to confirm.
```




It will take several minutes to save configuration file, please wait.....

Configuration file had been saved successfully

Note: The configuration file will take effect after being activated

La configuración actual se ha guardado correctamente.

Los cambios de configuración se deben guardar en el archivo de configuración para sobrevivir al reinicio del sistema. Puede ejecutar el comando **save** para guardar la configuración actual en la ruta predeterminada y sobrescribir el archivo de configuración original. También puede ejecutar el comando **save configuration-file** para guardar la configuración actual en un archivo especificado en el dispositivo de almacenamiento. Este comando no afecta al archivo de configuración de inicio actual del sistema.

Compare la configuración en ejecución con la configuración en el archivo de configuración de inicio.

```
<Datacom-Router>compare configuration
```

The current configuration is the same as the next startup configuration file.

La configuración en ejecución es la misma que en el archivo de configuración de inicio.

Step 5 Realizar operaciones en el sistema de archivos.

Lista todos los archivos en el directorio actual.

```
<Datacom-Router>dir
```

Directory of flash:/

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	22,622	Feb 20 2020	10:35:18	mon_file.txt
2	-rw-	737	Feb 20 2020	10:38:36	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	783	Jul 10 2018	14:46:16	default_local.cer
5	-rw-	0	Sep 11 2017	00:00:54	brdxpon_snmp_cfg.efs
6	drw-	-	Sep 11 2017	00:01:22	update
7	drw-	-	Sep 11 2017	00:01:48	shelldir
8	drw-	-	Sep 21 2019	17:14:24	localuser
9	drw-	-	Sep 15 2017	04:35:52	dhcp
10	-rw-	509	Feb 20 2020	10:38:40	private-data.txt
11	-rw-	2,686	Dec 19 2019	15:05:18	mon_lpu_file.txt
12	-rw-	3,072	Dec 18 2019	18:15:54	Boot_LogFile

510,484 KB total available (386,456 KB free)

vrpcfg.zip: archivo de configuración La extensión del nombre de archivo de configuración debe ser .cfg o .zip.

ar651c- v300r019c00Sspc100.cc: system software La extensión del nombre de archivo del software del sistema debe ser .cc.

Guardar la configuración en ejecución y nombrar el archivo de configuración test.cfg.

```
<Datacom-Router>save test.cfg
```

Are you sure to save the configuration to test.cfg? (y/n)[n]y

//Enter y to confirm.

It will take several minutes to save configuration file, please wait.....



Configuration file had been saved successfully
Note: The configuration file will take effect after being activated

Lista todos los archivos en el directorio actual de nuevo.

```
<Datacom-Router>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	22,622	Feb 20 2020	10:35:18	mon_file.txt
2	-rw-	737	Feb 20 2020	10:38:36	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	783	Jul 10 2018	14:46:16	default_local.cer
5	-rw-	0	Sep 11 2017	00:00:54	brdxpon_snmp_cfg.efs
6	drw-	-	Sep 11 2017	00:01:22	update
7	drw-	-	Sep 11 2017	00:01:48	shelldir
8	drw-	-	Sep 21 2019	17:14:24	localuser
9	drw-	-	Sep 15 2017	04:35:52	dhcp
10	-rw-	1,404	Feb 20 2020	11:55:17	test.cfg
11	-rw-	509	Feb 20 2020	11:55:18	private-data.txt
12	-rw-	2,686	Dec 19 2019	15:05:18	mon_lpu_file.txt
13	-rw-	3,072	Dec 18 2019	18:15:54	Boot_LogFile

510,484 KB total available (386,452 KB free)

El archivo de configuración se ha guardado correctamente.

Configure el archivo como el archivo de configuración de inicio.

```
<Datacom-Router>startup saved-configuration test.cfg
This operation will take several minutes, please wait.....
Info: Succeeded in setting the file for booting system
```

Muestra el archivo de configuración de inicio.

```
<Datacom-Router>display startup
```

MainBoard:

Startup system software:	flash:/ ar651c- v300r019c00Sspc100.cc
Next startup system software:	flash:/ ar651c- v300r019c00Sspc100.cc
Backup system software for next startup:	null
Startup saved-configuration file:	flash:/vrpcfg.zip
Next startup saved-configuration file:	flash:/test.cfg
Startup license file:	null
Next startup license file:	null
Startup patch package:	null
Next startup patch package:	null
Startup voice-files:	null
Next startup voice-files:	null

El comando **display startup** muestra el software del sistema y los archivos de configuración, licencia, parche y voz.

Borrar el archivo de configuración.

```
<Datacom-Router>reset saved-configuration
This will delete the configuration in the flash memory.
The device configuratio
```



```
ns will be erased to reconfigure.  
Are you sure? (y/n)[n]:y //Enter y to confirm.  
Clear the configuration in the device successfully.
```

Step 6 Reinicie el dispositivo.

```
<<Datacom-Router>reboot  
Info: The system is comparing the configuration, please wait.  
System will reboot! Continue ? [y/n]:y //Enter y to confirm.  
Info: system is rebooting ,please wait..  
El sistema se está reiniciando.  
<Datacom-Router>  
El dispositivo se reinicia.
```

-----Final

1.3 Verificación

Los detalles no se proporcionan aquí.

1.4 Referencia de configuración

Los detalles no se proporcionan aquí.

1.5 Quiz

1. Familiarizese con las teclas de función del sistema VRP de Huawei de acuerdo a la sección 2.6.
2. En el paso 5, se ejecuta el comando **reset saved-configuration** para eliminar la configuración. ¿Por qué se mantiene la configuración después de reiniciar el dispositivo?

1.6 Apéndice

Table 1-1 Teclas de función del sistema

Tecla	Función
<Ctrl+A>	Mueve el cursor al principio de la línea actual.
<Ctrl +B>	Mueve el cursor hacia atrás un carácter.
<Ctrl +C >	Detiene la ejecución de las funciones actuales.
<Ctrl +D >	Borra el carácter en el que se encuentra el cursor.



Tecla	Función
<Ctrl +E >	Mueve el cursor hasta el final de la última línea.
<Ctrl +F >	Mueve el cursor un carácter hacia delante.
<Ctrl +H >	Borra el carácter a la izquierda del cursor.
<Ctrl +K >	Finaliza la conexión de una llamada saliente durante el establecimiento de la conexión.
<Ctrl +N> o la tecla de flecha hacia abajo	Muestra el siguiente comando en el historial de comandos.
< Ctrl + N > o la tecla de flecha hacia arriba	Muestra el comando anterior en el historial de comandos.
<Ctrl +T >	Entra un signo de interrogación (?).
<Ctrl +>	Borra la cadena de caracteres (palabra) a la izquierda del cursor.
<Ctrl +X >	Borra todos los caracteres a la izquierda del cursor.
<Ctrl +Y >	Borra el carácter en el cursor y todos los caracteres a la derecha del cursor.
<Ctrl +Z >	Vuelve a la vista de usuario.
<Ctrl + J>	Detiene o redirige las conexiones entrantes.
<Esc +B >	Mueve el cursor hacia atrás una cadena de caracteres (palabra).
<Esc+D>	Elimina una cadena de caracteres (palabra) a la derecha del cursor.
<Esc+F>	Mueve el cursor hacia delante una cadena de caracteres (palabra).



2 Creación de una red IP interconectada

2.1 Laboratorio 1: direccionamiento y enrutamiento IPv4

2.1.1 Introducción

2.1.1.1 Acerca de este laboratorio

Internet Protocol version 4 (IPv4) es un protocolo central de la suite de protocolos PCT /ip y funciona en la capa de Internet en el modelo PCT /ip o en la capa de red en el modelo de Interconexión de Sistema Abierto (ISO). La capa de red proporciona la transmisión de datos sin conexión. Cada datagrama de IPs se transmite de forma independiente, eliminando la necesidad de establecer una conexión antes de enviar los datagramas de IPs.

El enrutamiento es el elemento básico de las redes de comunicación de datos. Es el proceso de selección de rutas en una red a lo largo de la cual se envían paquetes desde un origen a un destino.

En esta actividad de laboratorio, configurará las direcciones IPv4 y las rutas estáticas IPv4, y entenderá los principios básicos de enrutamiento en el proceso.

2.1.1.2 Objetivos.

Una vez completada esta tarea, podrá:

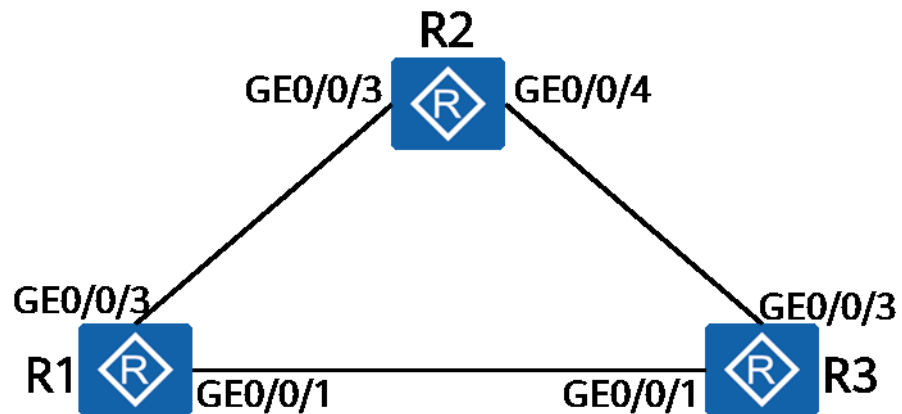
- Aprender a configurar una dirección IPv4 en una interfaz
- Comprender las funciones y los significados de las interfaces de bucle de retorno.
- Comprender cómo se generan las rutas directas.
- Aprender a configurar rutas estáticas y a comprender las condiciones para que las rutas estáticas surtan efecto.
- Aprender cómo probar la conectividad de la capa de red mediante la herramienta ping.
- Aprender a configurar rutas estáticas y entender sus escenarios de aplicación



2.1.1.3 Topología de redes

R1, R2 y R3 son gateways de sus redes. Es necesario configurar estos gateways para conectar estas redes.

Figure 2-1 Topología de laboratorio para direccionamiento y enrutamiento IPv4



2.1.2 Configuración del laboratorio

2.1.2.1 Configuración Roadmap

1. Configurar direcciones IP para las interfaces de los routers.
2. Configurar rutas estáticas para interconectar los routers.

2.1.2.2 Procedimiento de configuración

Step 1 Completa configuración básica del dispositivo.

Nombrar los dispositivos.

Los detalles no se proporcionan aquí.

Step 2 Muestra la dirección IP de la interfaz actual y la tabla de enrutamiento del router.

Muestra el estado de la interfaz en el router (R1 en este ejemplo).

```
[R1]display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 5
The number of interface that is UP in Protocol is 1
The number of interface that is DOWN in Protocol is 10
```



Interfaz	IP Dirección/Mascara	F í sico	Protocolo
GigabitEthernet0/0/1	unassigned	up	down
GigabitEthernet0/0/2	unassigned	up	down
GigabitEthernet0/0/3	unassigned	up	down

El comando **display IP interface brief** muestra información breve sobre las direcciones IP de la interfaz, incluidas las direcciones Ip, las máscaras de subred, el estado físico, el estado del protocolo de capa de enlace y la cantidad de interfaces en diferentes estados.

GigabitEthernet0/0/1 y GigabitEthernet0/0/3 en R1 no están configurados con direcciones IPs. Por lo tanto, el campo Dirección IP/Mask se encuentra en estado no asignado, el campo Protocolo se encuentra en estado down y el campo Físico en estado up.

Muestra la tabla de enrutamiento en el router (en este ejemplo, R1).

```
[[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 4      Routes :
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

InLoopBack0 es una interfaz de bucle de retorno predeterminada.

InLoopBack0 utiliza la dirección fija de bucle de retorno 127.0.0.1/para recibir paquetes de datos destinados al host donde reside InLoopBack0. La dirección IP de la interfaz InLoopBack0 no puede ser cambiada o anunciada utilizando un protocolo de enrutamiento.

Step 3 Configurar IPs para las interfaces físicas.

Configure las direcciones IP para las interfaces físicas de acuerdo con la siguiente tabla.

Table 2-1 Direcciones IPs de las interfaces físicas

Router	Interfaz	Mascara / Dirección IP
R1	GigabitEthernet0/0/1	10.0.13.1/24 y 24 de abril de 2001
	GigabitEthernet0/0/3	10.0.12.1/24
R2	GigabitEthernet0/0/3	10.0.12.2/24 y 24.
	GigabitEthernet0/0/4	10.0.23.2 y 24.
R3	GigabitEthernet0/0/1	10.0.13.3/24 y 24 de abril de 2001



	GigabitEthernet0/0/3	10.0.23.3 y 24.
--	----------------------	-----------------

```
< R1>system-view
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.0.13.1 24
[R1-GigabitEthernet0/0/1]quit
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R1-GigabitEthernet0/0/3]quit
```

```
<R2>system-view
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
<R3>system-view
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.13.3 24
[R3-GigabitEthernet0/0/1]quit
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.0.23.3 24
[R3-GigabitEthernet0/0/3]quit
```

Utilice la herramienta de ping para probar la conectividad.

```
[R1]ping 10.0.12.2
PING 10.0.12.2: 56 data bytes, press CTRL_C to break
Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=70 ms
Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=50 ms
Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=40 ms
Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=30 ms
Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=50 ms

--- 10.0.12.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 30/48/70 ms

[R1]ping 10.0.13.3
PING 10.0.13.3: 56 data bytes, press CTRL_C to break
Reply from 10.0.13.3: bytes=56 Sequence=1 ttl=255 time=50 ms
Reply from 10.0.13.3: bytes=56 Sequence=2 ttl=255 time=60 ms
Reply from 10.0.13.3: bytes=56 Sequence=3 ttl=255 time=50 ms
Reply from 10.0.13.3: bytes=56 Sequence=4 ttl=255 time=30 ms
Reply from 10.0.13.3: bytes=56 Sequence=5 ttl=255 time=30 ms

--- 10.0.13.3 ping statistics ---
5 packet(s) transmitidos
5 packet(s) recibidos
```




0.00% paquetes perdidos
round-trip min/avg/max = 30/44/60 ms

Muestra la tabla de enrutamiento de R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 10      Routes : 10

Destination/Mask    Proto    Pre  Cost    Flags  NextHop    Interface
-----
10.0.12.0/24        Direct   0    0        D    10.0.12.1   GigabitEthernet0/0/3
10.0.12.1/32        Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/3
10.0.12.255/32      Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/3
10.0.13.0/24        Direct   0    0        D    10.0.13.1   GigabitEthernet0/0/1
10.0.13.1/32        Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/1
10.0.13.255/32      Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/1
127.0.0.0/8         Direct   0    0        D    127.0.0.1   InLoopBack0
127.0.0.1/32        Direct   0    0        D    127.0.0.1   InLoopBack0
127.255.255.255/32  Direct   0    0        D    127.0.0.1   InLoopBack0
255.255.255.255/32  Direct   0    0        D    127.0.0.1   InLoopBack0
```

El resultado del comando anterior muestra que se generan automáticamente tres rutas directas para cada interfaz una vez configuradas las direcciones IP de las interfaces, que son

1. Ruta a la red donde reside la interfaz
2. La ruta del host a la interfaz
3. La ruta del host a la dirección de difusión de la red donde reside la interfaz.

Una ruta de host es una ruta con una máscara de 32 bits.

Step 4 Cree una interfaz de bucle de retorno.

Configure la interfaz de bucle de retorno de acuerdo con la siguiente tabla.

Table 2-2 Direcciones IPs de las interfaces de bucle de retorno

Router	Interfaz	Mascara / Direccion IP
R1	LoopBack0	10.0.1.1/32
R2	LoopBack0	10.0.1.2 /32
R3	LoopBack0	10.0.1.3 /32

Las interfaces de bucle invertido son interfaces lógicas configuradas manualmente y no existen físicamente. Las interfaces lógicas se pueden utilizar para intercambiar datos. Una interfaz de bucle de retorno siempre está activa en la

capa física y en la capa de enlace a menos que se cierre manualmente. Por lo general, una interfaz de bucle de retorno utiliza una máscara de 32 bits. Las interfaces de Loopback se utilizan para los siguientes fines:

1. Se utiliza como dirección para identificar y gestionar el router
2. Utilizado como identificador de Router en OSPF
3. Usado para mejorar la confiabilidad de la red

En esta actividad de laboratorio, las interfaces de bucle de retorno se utilizan para simular clientes.

```
[R1]interface LoopBack0
[R1-LoopBack0]ip address 10.0.1.1 32
[R2]interface LoopBack0
[R2-LoopBack0]ip address 10.0.1.2 32
[R3]interface LoopBack0
[R3-LoopBack0]ip address 10.0.1.3 32
```

Muestra la tabla de enrutamiento en el router (R1 en este ejemplo).

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
          Destinations : 11          Routes : 11

Destination/Mask    Proto    Pre  Cost    Flags  NextHop    Interface
-----
      10.0.1.1/32    Direct   0     0        D    127.0.0.1    LoopBack0
      10.0.12.0/24    Direct   0     0        D    10.0.12.1    GigabitEthernet0/0/3
      10.0.12.1/32    Direct   0     0        D    127.0.0.1    GigabitEthernet0/0/3
      10.0.12.255/32  Direct   0     0        D    127.0.0.1    GigabitEthernet0/0/3
      10.0.13.0/24    Direct   0     0        D    10.0.13.1    GigabitEthernet0/0/1
      10.0.13.1/32    Direct   0     0        D    127.0.0.1    GigabitEthernet0/0/1
      10.0.13.255/32  Direct   0     0        D    127.0.0.1    GigabitEthernet0/0/1
      127.0.0.0/8     Direct   0     0        D    127.0.0.1    InLoopBack0
      127.0.0.1/32    Direct   0     0        D    127.0.0.1    InLoopBack0
      127.255.255.255/32 Direct   0     0        D    127.0.0.1    InLoopBack0
      255.255.255.255/32 Direct   0     0        D    127.0.0.1    InLoopBack0
```

Se han generado rutas directas.

Pruebe la conectividad entre las interfaces de bucle de retorno.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.1.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
```



Utilizando el comando **ping - a source-ip-address destination-ip-address** para especificar las direcciones IP de origen y de destino de los paquetes ping. En este punto, el router no tiene una ruta a la dirección IP de destino. Por lo tanto, la operación de ping falla.

Step 5 Configure rutas estáticas.

En R1, configure una ruta a las interfaces loopback0 de R2 y R3.

```
[R1]IP route-static 10.0.1.2 32 10.0.12.2
[R1]IP route-static 10.0.1.3 32 10.0.13.3
```

Muestra la tabla de enrutamiento de R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 13      Routes : 13

Destination/Mask    Proto    Pre  Cost    Flags NextHop         Interface
-----
10.0.1.1/32        Direct   0    0        D    127.0.0.1       LoopBack0
10.0.1.2/32        Static   60    0        RD   10.0.12.2       GigabitEthernet0/0/3
10.0.1.3/32        Static   60    0        RD   10.0.13.3       GigabitEthernet0/0/1
10.0.12.0/24       Direct   0    0        D    10.0.12.1       GigabitEthernet0/0/3
10.0.12.1/32       Direct   0    0        D    127.0.0.1       GigabitEthernet0/0/3
10.0.12.255/32     Direct   0    0        D    127.0.0.1       GigabitEthernet0/0/3
10.0.13.0/24       Direct   0    0        D    10.0.13.1       GigabitEthernet0/0/1
10.0.13.1/32       Direct   0    0        D    127.0.0.1       GigabitEthernet0/0/1
10.0.13.255/32     Direct   0    0        D    127.0.0.1       GigabitEthernet0/0/1
127.0.0.0/8        Direct   0    0        D    127.0.0.1       InLoopBack0
127.0.0.1/32       Direct   0    0        D    127.0.0.1       InLoopBack0
127.255.255.255/32 Direct   0    0        D    127.0.0.1       InLoopBack0
255.255.255.255/32 Direct   0    0        D    127.0.0.1       InLoopBack0
```

Las rutas estáticas configuradas se agregan a la tabla de enrutamiento de IPs.

Probar conectividad.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 10.0.1.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss
The loopback0 interface of R2 still cannot be pinged because R2 does not have a route to the loopback0 interface of R1.
```

En R2, añade una ruta a LoopBack0 de R1.

```
[R2]ip route-static 10.0.1.1 32 10.0.12.1
```



Prueba conectividad.

```
<R1>ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=60 ms
  Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=50 ms
  Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=30 ms

--- 10.0.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 10/36/60 ms
```

Loopback0 en R1 puede comunicarse con loopback0 en R2.

Configurar otras rutas necesarias.

```
[R2]ip route-static 10.0.1.3 32 10.0.23.3
[R3]ip route-static 10.0.1.1 32 10.0.13.1
[R3]ip route-static 10.0.1.2 32 10.0.23.2
```

Prueba la conectividad entre las interfaces loopback0 de los routers en referencia a la descripción del proceso.

Step 6 Configure una ruta de R1 a R2 a través de R3 como ruta de respaldo desde LoopBack0 de R1 a LoopBack0 de R2.

Configurar rutas estáticas en R1 y R2.

```
[R1]ip route-static 10.0.1.2 32 10.0.13.3 preference 100
[R2]ip route-static 10.0.1.1 32 10.0.23.3 preference 100
```

Muestra las tablas de enrutamiento de R1 y R2.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 13          Routes : 13

Destination/Mask    Proto    Pre  Cost    Flags  NextHop    Interface
-----
10.0.1.1/32         Direct   0    0        D    127.0.0.1   LoopBack0
10.0.1.2/32         Static   60    0        RD   10.0.12.2   GigabitEthernet0/0/3
10.0.1.3/32         Static   60    0        RD   10.0.13.3   GigabitEthernet0/0/1
10.0.12.0/24        Direct   0    0        D    10.0.12.1   GigabitEthernet0/0/3
10.0.12.1/32        Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/3
10.0.12.255/32      Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/3
10.0.13.0/24        Direct   0    0        D    10.0.13.1   GigabitEthernet0/0/1
10.0.13.1/32        Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/1
10.0.13.255/32      Direct   0    0        D    127.0.0.1   GigabitEthernet0/0/1
127.0.0.0/8         Direct   0    0        D    127.0.0.1   InLoopBack0
127.0.0.1/32        Direct   0    0        D    127.0.0.1   InLoopBack0
127.255.255.255/32  Direct   0    0        D    127.0.0.1   InLoopBack0
255.255.255.255/32  Direct   0    0        D    127.0.0.1   InLoopBack0
```



```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Tables: Public
```

```
Destinations : 13      Routes : 13
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Static	60	0	RD	10.0.12.1	GigabitEthernet0/0/3
10.0.1.2/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.3/32	Static	60	0	RD	10.0.23.3	GigabitEthernet0/0/4
10.0.12.0/24	Direct	0	0	D	10.0.12.2	GigabitEthernet0/0/3
10.0.12.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.23.0/24	Direct	0	0	D	10.0.23.2	GigabitEthernet0/0/4
10.0.23.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4
10.0.23.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

La ruta estática con un valor de preferencia de 100 no se agrega a la tabla de enrutamiento.

Cierre la interfaz GigabitEthernet0/warp 0/warp 3 en las rutas 1 y 2 para invalidar la ruta con la prioridad más alta.

```
[R1]interface GigabitEthernet0/0/3
[ R1-GigabitEthernet0/0/3]shutdown
```

Muestra la tabla de enrutamiento en R1 y R2. El resultado del comando muestra que las rutas con menor prioridad se activan cuando se invalidan las rutas con mayor prioridad.

```
[R1]display IP routing-table
Route Flags: R - relay, D - download to fib
```

```
-----
Routing Tables: Public
```

```
Destinations : 10      Routes : 10
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.2/32	Static	100	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0



```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 10          Routes : 10

Destination/Mask    Proto   Pre  Cost   Flags NextHop         Interface
-----
 10.0.1.1/32        Static  100   0       RD   10.0.23.3        GigabitEthernet0/0/4
 10.0.1.2/32        Direct   0     0       D   127.0.0.1         LoopBack0
 10.0.1.3/32        Static   60    0       RD   10.0.23.3        GigabitEthernet0/0/4
 10.0.23.0/24       Direct   0     0       D   10.0.23.2        GigabitEthernet0/0/4
 10.0.23.2/32       Direct   0     0       D   127.0.0.1         GigabitEthernet0/0/4
 10.0.23.255/32     Direct   0     0       D   127.0.0.1         GigabitEthernet0/0/4
 127.0.0.0/8        Direct   0     0       D   127.0.0.1         InLoopBack0
 127.0.0.1/32       Direct   0     0       D   127.0.0.1         InLoopBack0
127.255.255.255/32  Direct   0     0       D   127.0.0.1         InLoopBack0
255.255.255.255/32  Direct   0     0       D   127.0.0.1         InLoopBack0
```

En este caso, la ruta estática original pasa a ser inválida y se activa la ruta estática de menor prioridad.

Probar conectividad.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=254 time=80 ms
  Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=254 time=60 ms
  Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=254 time=60 ms
  Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=254 time=110 ms
  Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=254 time=80 ms

--- 10.0.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
 round-trip min/avg/max = 60/78/110 ms
```

Trace la ruta de los paquetes de datos.

```
[R1]tracert -a 10.0.1.1 10.0.1.2

tracert to 10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 10.0.13.3 40 ms 30 ms 50 ms

 2 10.0.23.2 80 ms 80 ms 60 ms
```

El comando **tracert** muestra la ruta de los paquetes desde el origen hasta el destino.

El resultado del comando muestra que los paquetes de datos pasan a través de GigabitEthernet0/0/1 y GigabitEthernet0/0/3 de R3 y luego se reenvían a GigabitEthernet0/weddon/weddon/weddon4.



En algunos entornos de laboratorio, es posible que los dispositivos no respondan a los paquetes ICMP por razones de seguridad. Por lo tanto, los resultados pueden variar. Para finalizar la operación tracert, puede presionar Ctrl + bondyC.

Step 7 Configure las rutas predeterminadas para conectar la interfaz LoopBack0 de R1 y la interfaz LoopBack0 de R2.

Restaure las interfaces y elimine las rutas configuradas.

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]undo shutdown
[R1-GigabitEthernet0/0/3]quit
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.12.2
[R1]undo ip route-static 10.0.1.2 255.255.255.255 10.0.13.3 preference 100
```

Muestra la tabla de enrutamiento de R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 12      Routes : 12

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
10.0.1.1/32         Direct   0    0              D    127.0.0.1        LoopBack0
10.0.1.3/32         Static   60    0             RD    10.0.13.3        GigabitEthernet0/0/1
10.0.12.0/24        Direct   0    0              D    10.0.12.1        GigabitEthernet0/0/3
10.0.12.1/32        Direct   0    0              D    127.0.0.1        GigabitEthernet0/0/3
10.0.12.255/32      Direct   0    0              D    127.0.0.1        GigabitEthernet0/0/3
10.0.13.0/24        Direct   0    0              D    10.0.13.1        GigabitEthernet0/0/1
10.0.13.1/32        Direct   0    0              D    127.0.0.1        GigabitEthernet0/0/1
10.0.13.255/32      Direct   0    0              D    127.0.0.1        GigabitEthernet0/0/1
127.0.0.0/8         Direct   0    0              D    127.0.0.1        InLoopBack0
127.0.0.1/32        Direct   0    0              D    127.0.0.1        InLoopBack0
127.255.255.255/32  Direct   0    0              D    127.0.0.1        InLoopBack0
255.255.255.255/32  Direct   0    0              D    127.0.0.1        InLoopBack0
```

R no tiene una ruta a LoopBack0 (10.1.1.2 /32) de R2.

Configure una ruta predeterminada en R1.

```
[R1]IP route-static 0.0.0.0 0 10.0.12.2
```

Muestra la tabla de enrutamiento de R1.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 13      Routes : 13

Destination/Mask    Proto    Pre  Cost           Flags NextHop         Interface
-----
0.0.0.0/0           Static   60    0             RD    10.0.12.2        GigabitEthernet0/0/3
10.0.1.1/32         Direct   0    0              D    127.0.0.1        LoopBack0
```



10.0.1.3/32	Static	60	0	RD	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

La ruta predeterminada ha sido activada.

Pruebe la conectividad entre el bucle de retorno 0 de R1 y el bucle de retorno 0 de R2.

```
[R1]ping -a 10.0.1.1 10.0.1.2
PING 10.0.1.2: 56 data bytes, press CTRL_C to break
  Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=50 ms
  Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=30 ms
  Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=20 ms
  Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=40 ms
  Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=20 ms

--- 10.0.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 20/32/50 ms
```

LoopBack0 de R1 puede comunicarse con LoopBack0 de R2.

----Fin

2.1.3 Verificación

Se pueden ejecutar los comandos ping y tracert para probar la conectividad entre las interfaces loopback0 en diferentes dispositivos.

2.1.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.1 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
```




```
ip route-static 0.0.0.0 0.0.0.0 10.0.12.2
ip route-static 10.0.1.3 255.255.255.255 10.0.13.3
#
return
```

Configuración en R2

```
#
sysname R2
#
interface GigabitEthernet0/0/3
ip address 10.0.12.2 255.255.255.0
#
interface GigabitEthernet0/0/4
ip address 10.0.23.2 255.255.255.0
#
interface LoopBack0
ip address 10.0.1.2 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.12.1
ip route-static 10.0.1.1 255.255.255.255 10.0.23.3 preference 100
ip route-static 10.0.1.3 255.255.255.255 10.0.23.3
#
return
```

Configuración en R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet00/3
ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
ip address 10.0.1.3 255.255.255.255
#
ip route-static 10.0.1.1 255.255.255.255 10.0.13.1
ip route-static 10.0.1.2 255.255.255.255 10.0.23.2
#
return
```

2.1.5 Quiz

1. ¿En qué situaciones se agregará la ruta estática configurada a la tabla de ruteo ip? ¿Se puede agregar una ruta a la tabla de enrutamiento IP si el próximo salto configurado no es alcanzable?
2. En el paso 3, si el argumento -a no se especifica durante la prueba de conectividad entre las interfaces de bucle de retorno, ¿cuál es la dirección IP de origen de los paquetes ICMP? - ¿Por qué?



2.2 Laboratorio 2: enrutamiento OSPF

2.2.1 Introducción

2.2.1.1 Acerca de este laboratorio

El protocolo Open Shortest Path First es un protocolo de enlace de puerta de enlace interior desarrollado por el Grupo de trabajo de ingeniería de Internet. Actualmente, se utiliza la versión 2 de OSPF (RFC 2328) para IPv4. Como protocolo de estado de enlace, OSPF tiene las siguientes ventajas:

- Transmisión de paquetes multicast para reducir la carga en los switches que no ejecutan OSPF
- Enrutamiento entre dominios sin clase (IDC)
- Balanceo de carga entre rutas de igual costo
- Autenticación de paquetes

Con las ventajas anteriores, la OSPF es ampliamente aceptada y utilizada como un IGP.

En la actividad de laboratorio, usted entenderá las configuraciones y principios básicos de OSPF mediante la configuración de OSPF de una sola área.

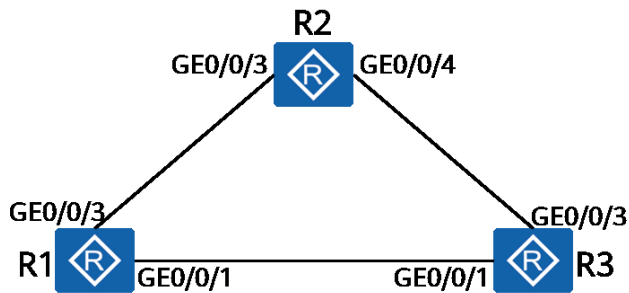
2.2.1.2 Objetivos

Una vez completada esta tarea, podrá:

- Aprenda los comandos básicos de OSPF
- Obtenga información sobre cómo verificar el estado de funcionamiento de OSPF.
- Aprenda a controlar la selección de rutas mediante costes
- Comprender el anuncio de rutas predeterminadas en OSPF
- Aprenda a configurar la autenticación OSPF

2.2.1.3 Topología de networking

R1, R2 y R3 son gateways de sus redes. Se debe configurar OSPF para habilitar la conectividad entre las redes.

**Figure 2-2** Topología de laboratorio para configurar OSPF

2.2.2 Configuración de laboratorio

2.2.2.1 Configuración Roadmap

1. Cree procesos OSPF en los dispositivos y habilite OSPF en las interfaces.
2. Configure la autenticación OSPF.
3. Configure OSPF para anunciar rutas predeterminadas.
4. Controle la selección de rutas de OSPF utilizando los costos.

2.2.2.2 Procedimiento de configuración

Step 1 Completa configuración básica del dispositivo.

Siga los pasos 1, 2, 3 y 4 del laboratorio 1 para nombrar los routers y configurar las direcciones IP de las interfaces física y de bucle de retorno.

Muestra la tabla de enrutamiento en el router (R1 en este ejemplo).

```
[R1]display ip routing-table
```

Route Flags: R - relay, D - download to fib

Routing Tables: Public

Destinations : 11 Routes : 11

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

En este punto, sólo existen rutas directas en el dispositivo.

Step 2 Complete la configuración básica del OSPF.

Crear un proceso OSPF.

```
[R1]ospf 1
```

Los parámetros de OSFF sólo se pueden configurar después de crear un proceso OSFF. Soporta múltiples procesos independientes en un dispositivo. El intercambio de rutas entre diferentes procesos OSPF es similar al intercambio entre diferentes protocolos de enrutamiento. Puede especificar un Id. de proceso al crear un proceso OSPF. Si no se especifica ningún Id. de proceso, se utiliza el Id. de proceso predeterminado 1.

Cree un área OSPF y especifique las interfaces en las que se debe habilitar OSPF.

```
[R1-ospf-1]area 0
```

El comando de **area** crea un área OSPF y muestra la vista de área OSPF.

```
[R1-ospf-1-area-0.0.0.0]network 10.0.12.1 0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.13.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0
```

El comando **network** *network-address wildcard-mask* especifica las interfaces en las que se habilitará OSPF. La función OSPF puede ejecutarse en una interfaz solo cuando se cumplen las dos condiciones siguientes:

1. La longitud de la máscara de la dirección IP de la interfaz no es menor que la especificada en el comando **network**. La OSPF utiliza una máscara inversa. Por ejemplo, 0.0.0.255 indica que la longitud de la máscara es de 24 bits.
2. La dirección de la interfaz debe estar dentro del rango de red especificado en el comando **network**.

En este ejemplo, se puede habilitar OSPF en las tres interfaces y todas se agregan al área 0.

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.0.23.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.0.1.2 0.0.0.0
```

Si la máscara de comodín del comando **network** es 0 y la dirección IP de la interfaz es la misma que la especificada en el comando **network-address**, la interfaz también ejecuta OSPF.

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.13.3 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 10.0.23.3 0.0.0.0
[R3-ospf-1-area-0.0.0.0]network 10.0.1.3 0.0.0.0
```

Step 3 Muestra el estado de la OSPF.

Muestra la información de vecinos OSPF.



```
[R1]display ospf peer

      OSPF Process 1 with Router ID 10.0.1.1
        Neighbors

Area 0.0.0.0 interface 10.0.13.1(GigabitEthernet0/0/1)'s neighbors
Router ID: 10.0.1.3      Address: 10.0.13.3
State: Full  Mode:Nbr is Master  Priority: 1
DR: 10.0.13.3  BDR: 10.0.13.1  MTU: 0
Dead timer due in 36 sec
Retrans timer interval: 0
Neighbor is up for 00:00:30
Authentication Sequence: [ 0 ]

      Neighbors

Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/3)'s neighbors
Router ID: 10.0.1.2      Address: 10.0.12.2
State: Full  Mode:Nbr is Master  Priority: 1
DR: 10.0.12.2  BDR: 10.0.12.1  MTU: 0
Dead timer due in 39 sec
Retrans timer interval: 4
Neighbor is up for 00:00:28
Authentication Sequence: [ 0 ]
```

El comando **display ospf peer** muestra información sobre vecinos en cada área de OSPF. La información incluye el área a la que pertenece el vecino, el identificador del router del vecino, el estado del vecino, DR, y DR.

Muestra las rutas aprendidas de OSPF.

```
[R1]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
-----
Public routing table : OSPF
      Destinations : 3      Routes : 4

OSPF routing table status : <Active>
      Destinations : 3      Routes : 4

Destination/Mask    Proto  Pre  Cost    Flags  NextHop    Interface
-----
10.0.1.2/32         OSPF   10   1        D     10.0.12.2   GigabitEthernet0/0/3
10.0.1.3/32         OSPF   10   1        D     10.0.13.3   GigabitEthernet0/0/1
10.0.23.0/24        OSPF   10   2        D     10.0.13.3   GigabitEthernet0/0/1
                   OSPF   10   2        D     10.0.12.2   GigabitEthernet0/0/3

OSPF routing table status : <Inactive>
      Destinations : 0      Routes : 0
```

Step 4 Configure la autenticación OSPF.

Configure la autenticación de la interfaz en R1.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ospf authentication-mode md5 1 cipher HCIA-Datcom
```



```
[R1]interface GigabitEthernet0/0/3
[R1- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datcom
[R1- GigabitEthernet0/0/3]display this
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher foCQTYsq-4.A\^38y!DVwQ0#
#
```

La contraseña se muestra en texto cifrado cuando se visualiza la configuración porque cipher significa texto cifrado.

Muestra los vecinos OSPF.

```
[R1]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.1
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
---------	-----------	-------------	-------

Total Peer(s): 0

La autenticación no está configurada en otros routers. Por lo tanto, la autenticación falla y no hay vecinos disponibles.

Configurando autenticación de interfaz en R2.

```
[R2]interface GigabitEthernet0/0/3
[R2- GigabitEthernet0/0/3]ospf authentication-mode md5 1 cipher HCIA-Datcom
[R2]interface GigabitEthernet0/0/4
[R2- GigabitEthernet0/0/4]ospf authentication-mode md5 1 cipher HCIA-Datcom
```

Muestra los vecinos OSPF en R2.

```
[R2]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.2
Peer Statistic Information
```

Area Id	Interface	Neighbor id	State
0.0.0.0	GigabitEthernet0/0/3	10.0.1.1	Full

Total Peer(s): 1

R2 ha establecido una relación de vecindad con R1.

Configure la autenticación de área en R3.

```
[D3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]authentication-mode md5 1 cipher HCIA-Datcom
```

Muestra vecinos OSPF en R3.

```
[R3]display ospf peer brief
```

```
OSPF Process 1 with Router ID 10.0.1.3
Peer Statistic Information
```



Area ID	Interfaz	Neighbor id	Estado
0.0.0.0	GigabitEthernet0/0/1	10.0.1.1	Full
0.0.0.0	GigabitEthernet0/0/3	10.0.1.2	Full

Total Peer(s): 2

R3 ha establecido una relación de vecindad con R1 y R2. Nota: La autenticación de interfaces OSFF y la autenticación de áreas implementan la autenticación de paquetes OSFF en interfaces OSFF.

Step 5 Supongamos que R1 es la salida de todas las redes. Por lo tanto, R1 anuncia la ruta predeterminada a OSPF.

Anuncie la ruta predeterminada en R1.

```
[R1]ospf
[R1-ospf-1]default-route-advertise always
```

El comando **default-route-advertise** anuncia la ruta predeterminada a un área de OSPF común. Si no se especifica el argumento **always**, la ruta predeterminada se anuncia a otros Routers sólo cuando hay rutas predeterminadas no OSPF activas en la tabla de enrutamiento del Router local. En este ejemplo, no existe ninguna ruta predeterminada en la tabla de enrutamiento local. Por lo tanto, es necesario utilizar el argumento **always**.

Muestra las tablas de enrutamiento de IPs de R2 y R3.

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public

Destinations : 15 Routes : 16

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	O_ASE	150	1	D	10.0.12.1	GigabitEthernet0/0/3
10.0.1.1/32	OSPF	10	1	D	10.0.12.1	GigabitEthernet0/0/3
10.0.1.2/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.3/32	OSPF	10	1	D	10.0.23.3	GigabitEthernet0/0/4
10.0.12.0/24	Direct	0	0	D	10.0.12.2	GigabitEthernet0/0/3
10.0.12.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	OSPF	10	2	D	10.0.12.1	GigabitEthernet0/0/3
	OSPF	10	2	D	10.0.23.3	GigabitEthernet0/0/4
10.0.23.0/24	Direct	0	0	D	10.0.23.2	GigabitEthernet0/0/4
10.0.23.2/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4
10.0.23.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/4
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

```
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
```

Routing Tables: Public



Destinations : 15		Routes : 16				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	O_ASE	150	1	D	10.0.13.1	GigabitEthernet0/0/1
10.0.1.1/32	OSPF	10	1	D	10.0.13.1	GigabitEthernet0/0/1
10.0.1.2/32	OSPF	10	1	D	10.0.23.2	GigabitEthernet0/0/3
10.0.1.3/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.12.0/24	OSPF	10	2	D	10.0.23.2	GigabitEthernet0/0/3
	OSPF	10	2	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.0/24	Direct	0	0	D	10.0.13.3	GigabitEthernet0/0/1
10.0.13.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.23.0/24	Direct	0	0	D	10.0.23.3	GigabitEthernet0/0/3
10.0.23.3/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.23.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

R2 y R3 han aprendido la ruta predeterminada.

Step 6 Cambie los valores de coste de las interfaces en R1 para que el bucle de retorno 0 en R1 pueda alcanzar el bucle de retorno 0 en R2 a través de R3.

De acuerdo con la tabla de enrutamiento de R1, el costo de la ruta de R1 a LoopBack0 de R2 es 1, y el costo de la ruta de R1 a R2 por R3 es 2. Por lo tanto, solo se debe cambiar el costo de la ruta de R1 a LoopBack0 de R2 para garantizar que el valor sea mayor que 2.

```
[R1]interface GigabitEthernet0/0/3
[R1- GigabitEthernet0/0/3]ospf costo 10
```

Muestra la tabla de enrutamiento de R1.

[R1]display ip routing-table						
Route Flags: R - relay, D - download to fib						

Routing Tables: Public						
Destinations : 14		Routes : 14				
Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.1.1/32	Direct	0	0	D	127.0.0.1	LoopBack0
10.0.1.2/32	OSPF	10	2	D	10.0.13.3	GigabitEthernet0/0/1
10.0.1.3/32	OSPF	10	1	D	10.0.13.3	GigabitEthernet0/0/1
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.23.0/24	OSPF	10	2	D	10.0.13.3	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0



```
255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0
```

En este caso, el siguiente salto de la ruta de R1 a LoopBack0 en R2 es GigabitEthernet0/0/1 en R3.

Verifique el resultado mediante la emisión de comandos Tracert.

```
[R1]tracert -a 10.0.1.1 10.0.1.2
```

```
tracert to 10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break
```

```
1 10.0.13.3 40 ms 50 ms 50 ms
```

```
2 10.0.23.2 60 ms 110 ms 70 ms
```

----Fin

2.2.3 Verificación

1. Prueba la conectividad entre interfaces en diferentes dispositivos utilizando Ping.
2. Apague las interfaces para simular fallas de enlace y verifique los cambios en las tablas de enrutamiento.

2.2.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
interface GigabitEthernet0/0/1
ip address 10.0.13.1 255.255.255.0
ospf authentication-mode md5 1 cipher %^%#`f*R'6q/RMq(+5*g(sP~SB8oQ49;%7WE:07P7X:W%^%#
#
interface GigabitEthernet0/0/3
ip address 10.0.12.1 255.255.255.0
ospf cost 10
ospf authentication-mode md5 1 cipher %^%#]e)pBf~7B0.FM~U;bRAVgE$U>%X;>T\M\tLIYRj2%^%#
#
interface LoopBack0
ip address 10.0.1.1 255.255.255.255
#
ospf 1
default-route-advertise always
area 0.0.0.0
network 10.0.1.1 0.0.0.0
network 10.0.12.0 0.0.0.255
network 10.0.13.0 0.0.0.255
#
return
```

Configuración en R2

```
#
sysname R2
```



```
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#z+72ZaTk2+v/g7E~AmR"NFYAKC>LZ8~Y`["**Gh=&%^%#
#
interface GigabitEthernet0/0/4
 ip address 10.0.23.2 255.255.255.0
 ospf authentication-mode md5 1 cipher %^%#=#2jEBu!{&UYoB*(RDVLc5t~<1B_a-PwC$WH%jQ3%^%#
#
interface LoopBack0
 ip address 10.0.1.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.0.1.2 0.0.0.0
  network 10.0.12.2 0.0.0.0
  network 10.0.23.2 0.0.0.0
#
return
```

Configuración en R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
 ip address 10.0.13.3 255.255.255.0
#
interface GigabitEthernet0/0/3
 ip address 10.0.23.3 255.255.255.0
#
interface LoopBack0
 ip address 10.0.1.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  authentication-mode md5 1 cipher %^%#Rl<:SVln1M>[Gk"v/OeSEW|:0:4*h;b|-d:N"s{>%^%#
  network 10.0.1.3 0.0.0.0
  network 10.0.13.3 0.0.0.0
  network 10.0.23.3 0.0.0.0
#
return
```

2.2.5 Quiz

1. En el paso 6, ¿cuál es la ruta para que R2 devuelva los paquetes ICMP a R1? Intente explicar la razón.

3

Creación de una red Ethernet conmutada

3.1 Laboratorio 1: Configuración básica de Ethernet y VLANs

3.1.1 Introducción

3.1.1.1 Acerca de este laboratorio

La tecnología Ethernet permite la comunicación de datos a través de medios compartidos a través de Carrier Sense Multiple Access/Collision Detection (CSMA/CD). Cuando una red Ethernet tiene un gran número de hosts, la colisión se convierte en un problema serio y puede conducir a tormentas de difusión. Esto puede degradar el rendimiento de la red o incluso provocar una falla total. El uso de switches para conectar las LAN puede mitigar las colisiones, pero la difusión todavía puede plantear un problema.

Para aliviar las tormentas de difusión, la tecnología VLAN divide una LAN física en varias VLAN, de modo que los dominios de difusión sean más pequeños. Los hosts dentro de una VLAN sólo pueden comunicarse directamente con los hosts de la misma VLAN. Deben utilizar un router para comunicarse con los hosts de otras VLAN.

En esta actividad de laboratorio, se explica cómo configurar las VLANs en los switches de Huawei.

3.1.1.2 Objetivos.

Una vez completada esta tarea, podrá:

- Aprender a crear una VLAN
- Aprenda a configurar puertos de acceso, troncales e híbridos.
- Aprender a configurar las VLAN en función de los puertos
- Aprender a configurar las VLAN según las direcciones MAC
- Obtenga información sobre cómo ver la tabla de direcciones MAC e información de VLANs.

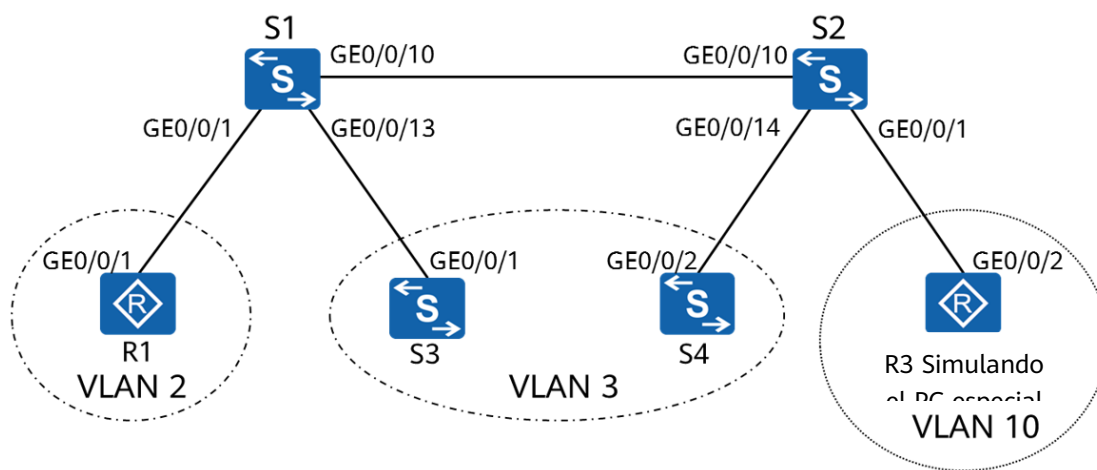


3.1.1.3 Topología de networking

Una empresa debe dividir una red de capa 2 en varias VLAN según los requerimientos del servicio. Además, la VLAN 10 requiere un mayor nivel de seguridad y solo se pueden agregar equipos específicos a la VLAN 10.

Para cumplir con este requerimiento, se pueden asignar puertos de usuario de servicios idénticos en S1 y S2 a la misma VLAN, y se pueden asignar puertos con direcciones MACs especificadas en S28 a una VLAN.

Figure 3-1 Topología de laboratorio para configuración de VLANs



3.1.2 Configuración de laboratorio

3.1.2.1 Configuración Roadmap

1. Cree una VLAN.
2. Configure una VLAN basada en puertos.
3. Configure una VLAN basada en direcciones MAC.

3.1.2.2 Procedimiento de configuración

Step 1 Configure los nombres de los puertos S1 y S2 y deshabilite los puertos innecesarios.

Nombra los dispositivos.

Los detalles no se proporcionan aquí.

Apagar GE0/0/11 Y GE0/0/12 on S1. Este paso sólo se aplica al entorno descrito en *HCIA-Datacom Lab Construction Guide V1.0*.

```
[S1] interface Gigabit Ethernet 0/0/11
[S1-GigabitEthernet0/0/11]
[S1-GigabitEthernet0/0/11] quit
```



```
[S1]interface Gigabit Ethernet 0/0/12
[S1-GigabitEthernet0/0/12 ]1
[S1-GigabitEthernet0/0/12 ]quit
```

Apagar GE0/0/11 and GE0/0/12 on S2.

```
[S2]interface GigabitEthernet 0/0/11
[S2-GigabitEthernet0/0/11]shutdown
[S2-GigabitEthernet0/0/11]quit
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
[S2-GigabitEthernet0/0/12]quit
```

Step 2 Configure las direcciones IP del dispositivo.

Configure las direcciones IP para R1 y R3 en 10.1.2.1/24 y 10.1.10.1/24, respectivamente.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1 IP address 10.1.2.1 24
```

```
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]IP address 10.1.10.1 24
```

Configure las direcciones IP de S3 y S4 en 10.1.3.1/24 y 10.1.3.2/24, respectivamente. (Para el escenario 1, S3 y S4 soportan la conmutación de interfaces de capa 2 a interfaces de capa 3).

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]undo portswitch
The interface changes to Layer 3 mode.
```

El comando **undo portswitch** cambia el modo de operación de las interfaces Ethernet del modo Capa 2 al modo Capa 3.

```
[S3-GigabitEthernet0/0/1]ip address 10.1.3.1 24
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]undo portswitch
[S4-GigabitEthernet0/0/2]ip address 10.1.3.2 24
```

Configure las direcciones IP de VLANIF3 en S3 y S4 en 10.1.3.1/24 y 10.1.3.2/24, respectivamente. (Para el escenario 2, S3 y S4 no soportan la conmutación de interfaces de Capa 2 a interfaces de Capa 3).

1. Crear VLAN 3 en S3 y S4.

```
[S3]vlan 3
[S3-vlan3]
```

```
[S4]vlan 3
[S4-vlan3]
```



2. Configurar puertos en S3 y S4 como puertos de acceso y asignarlos a las VLAN correspondientes.

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]port link-type access
[S3-GigabitEthernet0/0/1]port default vlan 3
[S3-GigabitEthernet0/0/1]quit
```

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]port link-type access
[S4-GigabitEthernet0/0/2]port default vlan 3
[S4-GigabitEthernet0/0/2]quit
```

3. # Crear interfaces VLANIF y configurar direcciones IP.

```
[S3] interfaz Vlanif 3
```

El comando **interface vlanif** *vlan-id* crea una interfaz VLANIF y muestra la vista de la interfaz VLANIF.

```
[S3-Vlanif3]ip address 10.1.3.1 24
```

```
[S4] interface Vlanif 3
[S4-Vlanif3]ip address 10.1.3.2 24
```

Step 3 Crear una VLAN.

Crear VLAN 2, 3 y 10 en S1 y S2.

```
[S1]vlan batch 2 to 3 10
Info: This operation may take a few seconds. Please wait for a moment...done.
VLANs 2, 3, and 10 are created successfully.
```

El comando **vlan** *vlan-id* crea una vlan y muestra la vista de la vlan. Si la VLAN existe, se visualiza la VLAN.

El comando **vlan batch** {*vlan-id1* [**to** *vlan-id2*]} crea VLAN por lotes.

```
[S2]vlan batch 2 to 3 10
```

Step 4 Configure las VLAN basadas en puertos.

Configure los puertos de usuario en S3 y S4 como puertos de acceso y asíguelos a las VLAN correspondientes.

```
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
```

El comando **port link-type** {**access** | **hybrid** | **trunk**} especifica el tipo de vínculo de una interfaz, que puede ser Access, Trunk o Hybrid.

```
[S1-GigabitEthernet0/0/1]port default vlan 2
```

El comando **port default vlan** *vlan-id* configura la Vlan default de una interfaz y asigna la interfaz a la Vlan.

```
[S1-GigabitEthernet0/0/1]quit
```



```
[S1]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3
[S1-GigabitEthernet0/0/13]quit
```

```
[S2]interface GigabitEthernet0/0/14
[S2-GigabitEthernet0/0/14]port link-type access
[S2-GigabitEthernet0/0/14]port default vlan 3
[S2-GigabitEthernet0/0/14]quit
```

Configure los puertos que conectan S1 y S2 como puertos troncales y permita que pasen solo los paquetes de VLAN 2 y VLAN 3.

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
```

El comando **port trunk allow-pass vlan** asigna un puerto troncal a las VLAN especificadas.

```
[ S1-GigabitEthernet0/0/10]under port trunk allow-pass vlan 1
```

El comando **undo port trunk allow-pass** vlan elimina un puerto troncal de las VLAN especificadas.

Por defecto, la VLAN 1 se encuentra en la lista permitida. Si la Vlan 1 no se utiliza para ningún servicio, se debe eliminar por motivos de seguridad.

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port link-type trunk
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3
[S2-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

Step 5 Configure las VLAN basadas en direcciones MAC.

Como se muestra en el diagrama de networking, R3simula un ordenador de servicio especial. Supongamos que la dirección Mac del ordenador es a008-6fe1-0c46. Se espera que el ordenador se conecte a la red a través de cualquiera de las plataformas GigabitEthernet0/0/1, GigabitEthernet0/0/2, y GigabitEthernet0/0/3 en S2 y transmitir datos a través de VLAN 10.

Configure S2 para asociar la mac-address del ordenador con la vlan 10.

La pertenencia a la VLAN depende de las direcciones MACs de origen de los paquetes, y las etiquetas de VLAN se agregan en consecuencia. Este método de asignación de VLANs es independiente de la ubicación, proporcionando un mayor nivel de seguridad y flexibilidad.

```
[S2]vlan 10
[S2-vlan10]mac-vlan mac-address a008-6fe1-0c46
```

El comando **mac-vlan mac-address** asocia una mac-address a una vlan.



Set GigabitEthernet0/0/1, GigabitEthernet0/0/2, y GigabitEthernet0/0/3 en S2 a puertos híbridos y configurarlos para permitir el paso de paquetes de VLAN basadas en direcciones MAC.

En los puertos de acceso y troncales, la asignación de VLANs basada en direcciones MAC sólo se puede utilizar cuando la VLAN es la misma que la VPID. Por lo tanto, se recomienda configurar la asignación de VLAN basada en direcciones MAC en un puerto híbrido para recibir paquetes sin etiquetas de varias VLAN.

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]port link-type hybrid
[S2-GigabitEthernet0/0/1]port hybrid untagged vlan 10
```

El comando **port hybrid untagged vlan** asigna un puerto híbrido a las VLAN especificadas para permitir el paso de tramas sin etiquetar.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
[S2-GigabitEthernet0/0/2]port link-type hybrid
[S2-GigabitEthernet0/0/2]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]port link-type hybrid
[S2-GigabitEthernet0/0/3]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/3]quit
```

Configure los puertos que conectan S1 y S2 para permitir que pasen los paquetes de la VLAN 10.

Los puertos deben permitir el paso de tramas etiquetadas de varias VLAN. Por lo tanto, los puertos se pueden configurar como puertos troncales.

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/10]quit
```

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 10
[S2-GigabitEthernet0/0/10]quit
```

Configure S2 y habilite la asignación de VLANs basada en direcciones MACs en GE0/0/1, GE0/0/2, y GE0/0/3.

Para habilitar un puerto para reenviar paquetes basados en asociaciones entre direcciones MACs y VLAN, se debe ejecutar el comando **mac-vlan enable**.

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1] mac-vlan enable
```

El comando **mac-vlan enable** habilita la asignación de VLANs basada en direcciones MAC en un puerto.

```
[S2-GigabitEthernet0/0/1]quit
[S2]interface GigabitEthernet0/0/2
```




```
[S2-GigabitEthernet0/0/2]mac-vlan enable
[S2-GigabitEthernet0/0/2]quit
[S2]interface GigabitEthernet0/0/3
[S2-GigabitEthernet0/0/3]mac-vlan enable
[S2-GigabitEthernet0/0/3]quit
```

Step 6 Muestra la información de configuración.

Muestra la información de la VLAN en el switch.

```
[S1]display vlan
```

El comando **display vlan** muestra información sobre las VLAN.

El comando **display vlan verbose** muestra información detallada sobre una VLAN especificada, incluyendo ID, tipo, descripción y estado de la VLAN, estado de la función de estadísticas de tráfico, puertos en la VLAN, y modo en el que se asignan los puertos a la VLAN.

The total number of vlans is : 4

```
-----
U: Up;          D: Down;          TG: Tagged;      UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan;  *: Management-vlan;
-----
```

VID	Type	Ports
1	common	UT: GE0/0/2(D) GE0/0/6(D) GE0/0/11(D) GE0/0/16(D) GE0/0/20(D) GE0/0/24(D)
		GE0/0/3(D) GE0/0/7(D) GE0/0/12(D) GE0/0/17(D) GE0/0/21(D)
		GE0/0/4(D) GE0/0/8(D) GE0/0/14(D) GE0/0/18(D) GE0/0/22(D)
		GE0/0/5(D) GE0/0/9(D) GE0/0/15(D) GE0/0/19(D) GE0/0/23(D)
2	common	UT: GE0/0/1(U)
		TG: GE0/0/10(U)
3	common	UT: GE0/0/13(U)
		TG: GE0/0/10(U)
10	common	TG: GE0/0/10(U)

VID	Status	Property	MAC-LRN	Statistics	Description
1	enable	default	enable	disable	VLAN 0001
2	enable	default	enable	disable	VLAN 0002
3	enable	default	enable	disable	VLAN 0003
10	enable	default	enable	disable	VLAN 0010

```
[S2]display vlan
```

The total number of vlans is : 4

```
-----
U: Up;          D: Down;          TG: Tagged;      UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan;  *: Management-vlan;
-----
```



VID	Type	Ports
1	common	UT: GE0/0/1(U) GE0/0/2(D) GE0/0/3(D) GE0/0/4(D) GE0/0/5(D) GE0/0/6(D) GE0/0/7(D) GE0/0/8(D) GE0/0/9(D) GE0/0/11(D) GE0/0/12(D) GE0/0/13(D) GE0/0/15(D) GE0/0/16(D) GE0/0/17(D) GE0/0/18(D) GE0/0/19(D) GE0/0/20(D) GE0/0/21(D) GE0/0/22(D) GE0/0/23(D) GE0/0/24(D)
2	common	TG: GE0/0/10(U)
3	common	UT: GE0/0/14(U) TG: GE0/0/10(U)
10	common	UT: GE0/0/1(U) GE0/0/2(D) GE0/0/3(D) TG: GE0/0/10(U)

VID	Status	Property	MAC-LRN	Statistics	Description
1	enable	default	enable	disable	VLAN 0001
2	enable	default	enable	disable	VLAN 0002
3	enable	default	enable	disable	VLAN 0003
10	enable	default	enable	disable	VLAN 0010

Muestra la configuración de la VLAN basada en direcciones MAC en el switch.

```
[S2]display mac-vlan vlan 10
```

MAC Address	MASK	VLAN	Priority
00e0-fc1c-47a7	ffff-ffff-ffff	10	0

Total MAC VLAN address count: 1

El comando **display mac-vlan** muestra la configuración de la asignación de VLANs basada en direcciones MACs.

3.1.3 Verificación

Probar la conectividad del dispositivo y verificar la configuración de VLANs.

1. Haga ping en S4 desde S3 y asegúrese de que la operación de ping se realice con éxito.
2. Haga ping a otros dispositivos desde R1 y asegúrese de que la operación de ping falla.
3. Haga ping de R1 a R3, capture paquetes en el enlace entre S1 y S2 y asegúrese de que la operación de ping falla pero se pueden capturar tramas de datos con etiqueta de Vlan 10.
4. Ejecute el comando **display mac-address verbose** en S1 y S2 para verificar las tablas de direcciones MACs en los switches.

3.1.4 Referencia de configuración

Configuración en S1



```
#
sysname S1
#
vlan batch 2 to 3 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
interface GigabitEthernet0/0/11
 shutdown
#
interface GigabitEthernet0/0/12
 shutdown
#
interface GigabitEthernet0/0/13
 port link-type access
 port default vlan 3
#
return
```

Configuración en S2

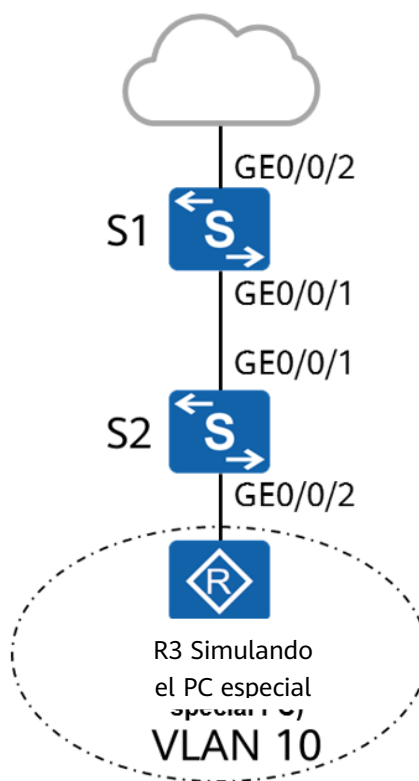
```
#
sysname S2
#
vlan batch 2 to 3 10
#
vlan 10
 mac-vlan mac-address a008-6fe1-0c46 priority 0
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/2
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/3
 port link-type hybrid
 port hybrid untagged vlan 10
 mac-vlan enable
#
interface GigabitEthernet0/0/10
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 2 to 3 10
#
```



```
interface GigabitEthernet0/0/11
shutdown
#
interface GigabitEthernet0/0/12
shutdown
#
interface GigabitEthernet0/0/14
port link-type access
port default vlan 3
#
return
```

3.1.5 Quiz

1. Como se muestra en la siguiente figura, para garantizar la seguridad de la información de un servicio especial, solo algunas PC especiales pueden acceder a la red a través de la VLAN 10. ¿Cómo se puede implementar este requerimiento en S1?





3.2 Laboratorio 2: Árbol de expansión

3.2.1 Introducción

3.2.1.1 Acerca de este laboratorio

En una red Ethernet conmutada, se utilizan enlaces redundantes para implementar el backup de enlaces y mejorar la disponibilidad de la red. Sin embargo, los enlaces redundantes pueden producir bucles, provocando tormentas de difusión y una tabla inestable de direcciones MAC, deteriorando o incluso interrumpiendo las comunicaciones. Para evitar bucles, la AEE introdujo el Protocolo de Árbol de Expansión (PTS).

El PTS definido en IEEE802.1D ha evolucionado al Protocolo Rápido de Árbol de Expansión (PTR) definido en IEEE802.1W, y al Protocolo Multiple de Árbol de Expansión (PTMS) definido en IEEE802.1S.

En esta actividad de laboratorio, usted aprenderá la configuración básica de STPs y entender sus principios y algunas características de RSTPs.

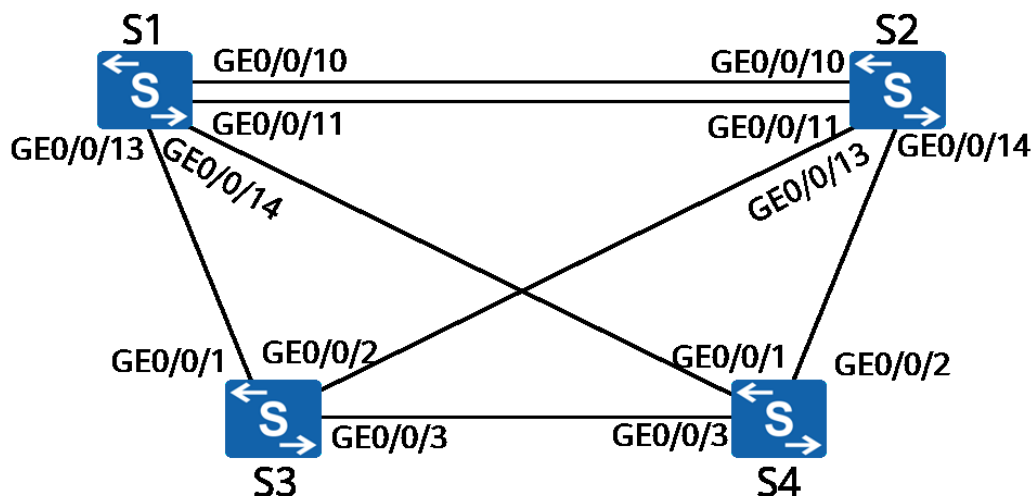
3.2.1.2 Objetivos.

Una vez completada esta tarea, podrá:

- Aprenda a habilitar y deshabilitar STP/RSTP
- Aprenda a cambiar el modo de transferencia automática de un switch
- Aprenda a cambiar las prioridades de los puentes para controlar la elección del puente raíz
- Aprenda a cambiar las prioridades de los puertos para controlar la elección del puerto raíz y el puerto designado
- Aprenda cómo cambiar los costos de los puertos para controlar la elección del puerto raíz y el puerto designado
- Aprenda a configurar puertos de borde
- Aprenda a habilitar y deshabilitar el protocolo RSTP

3.2.1.3 Topolog í a de networking

Una empresa debe implementar enlaces redundantes en su red conmutada de capa 2 para mejorar la disponibilidad de la red. Mientras tanto, la compañía también necesita desplegar PTS para evitar que los enlaces redundantes formen bucles y causen tormentas de difusión y aleteo de direcciones MAC.

**Figure 3-2** Topología de laboratorio para configurar PTS

3.2.2 Configuración de laboratorio

3.2.2.1 Configuración Roadmap

1. Habilitar PTS.
2. Cambiar las prioridades del puente para controlar la elección del puente raíz.
3. Modifique los parámetros del puerto para determinar el rol del puerto.
4. Cambie el protocolo a STPR.
5. Configure los puertos de borde.

3.2.2.2 Procedimiento de configuración

Step 1 # Cierre los puertos innecesarios. Este paso sólo se aplica al entorno descrito en HCIA-Datcom Lab Construction Guide V1.0.

Apagar el GigabitEthernet0/0/12 between S1 and S2.

```
[S1 ]interface Gigabit Ethernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
```

```
[S2]interface GigabitEthernet 0/0/12
[S2-GigabitEthernet0/0/12]shutdown
```

Step 2 Habilitar PTS.

Habilite PTS globalmente.

```
< S1>system-view
Enter system view, return user view with Ctrl+Z.
[S1]stp enable
```



El comando **stp enable** habilita STPs, RSTPs o MSTPs en un dispositivo de conmutación o en un puerto. Por defecto, STP, RSTP o MSTP se habilitan en los switches.

Cambie el modo de árbol de expansión a PTS.

```
[S1]stp mode stp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

El comando **stp mode {mstp | rstp | stp}** configura el modo de operación del protocolo de árbol de expansión en un dispositivo de conmutación. Por defecto, el dispositivo de conmutación funciona en modo MSTP. El modo de árbol de expansión del dispositivo actual se ha cambiado a PTS.

```
[S2]stp mode stp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S3]stp mode stp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S4]stp mode stp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

Muestra el estado del árbol de expansión. S1 se utiliza como ejemplo.

```
[S1]display stp
```

-----[CIST Global Info][Mode STP]-----

```
CIST Bridge           :32768.4c1f-cc33-7359           //Bridge ID of the device.
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :32768.4c1f-cc10-5913 / 20000     //ID and path cost of the current root
bridge.
CIST RegRoot/IRPC     :32768.4c1f-cc33-7359 / 0
CIST RootPortId       :128.14
BPDU-Protection       :Disabled
TC or TCN received    :47
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:0m:38s
Number of TC          :15
Last TC occurred      :GigabitEthernet0/0/14
```

La información mostrada también incluye información de estado del puerto, que no se incluye en la salida anterior.

Muestra la breve información sobre el árbol de esparcimiento en cada interruptor.

```
[[S1]display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	DESI	FORWARDING	NONE



0	GigabitEthernet0/0/11	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE

[[S2]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/11	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE

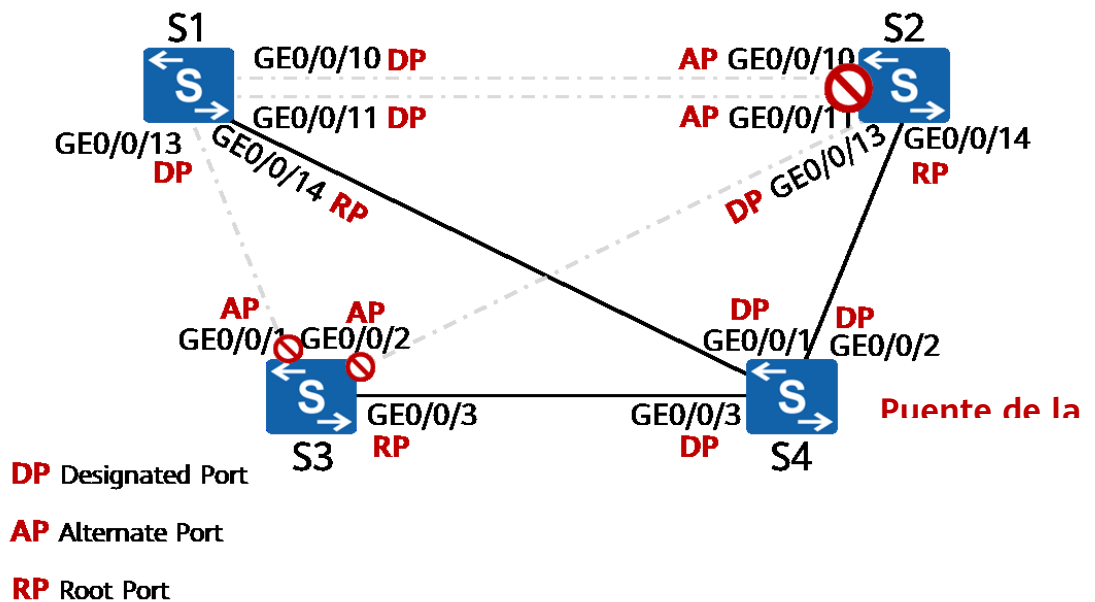
[S3]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE

Según la ID del puente raíz y la información del puerto de cada switch, la topología actual es la siguiente:



La línea de puntos indica que el enlace no reenvía datos de servicio.



Esta topología es solo de referencia y puede no ser la misma que la topología real del árbol de expansión en el entorno del laboratorio.

Step 3 Modifique los parámetros del dispositivo para que S1 sea el puente raíz y S2 sea el puente raíz secundario.

Cambie las prioridades del puente de S1 y S2.

```
[ S1 ] stp root primary
```

Debido a la importancia del puente raíz, el switch con alto rendimiento y jerarquía de red se elige generalmente como puente raíz. Sin embargo, la prioridad de dicho dispositivo puede no ser tan alta. Por lo tanto, es necesario establecer una alta prioridad para el switch para que el switch pueda ser elegido como el root bridge. El comando `stp root` configura el switch como un puente raíz o un puente raíz secundario de un árbol de expansión.

- El comando **stp root primary** especifica un switch como dispositivo de conmutación raíz. En este caso, el valor de prioridad del switch es 0 en el árbol de expansión y no se puede cambiar la prioridad.
- El comando **stp root secondary** especifica un switch como el secondary root bridge. En este caso, el valor de prioridad del switch es 4096 y no se puede cambiar la prioridad.

```
[ S2 ] stp root secondary
```

Muestra el estado de STPs en S1.

```
[ S1 ] display stp
```

```
-----[CIST Global Info][Mode STP]-----
```

```
CIST Bridge           :0      .4c1f-cc33-7359           //Bridge ID of the device.
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0      .4c1f-cc33-7359 / 0         //ID and path cost of the current root
bridge
CIST RegRoot/IRPC     :0      .4c1f-cc33-7359 / 0
CIST RootPortId       :0.0
BPDU-Protection       :Disabled
CIST Root Type        :Primary root
TC or TCN received    :84
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:1m:44s
Number of TC          :21
Last TC occurred      :GigabitEthernet0/0/10
```

En este caso, la id. de puente de S1 es la misma que la id. de puente raíz, y el costo de la ruta raíz es 0, lo que indica que S1 es el puente raíz de la red actual.

Muestra la breve información del estado de los STPs en todos los dispositivos.

```
[S1] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/11	DESI	FORWARDING	NONE



0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	DESI	FORWARDING	NONE

[S2]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/11	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	DESI	FORWARDING	NONE

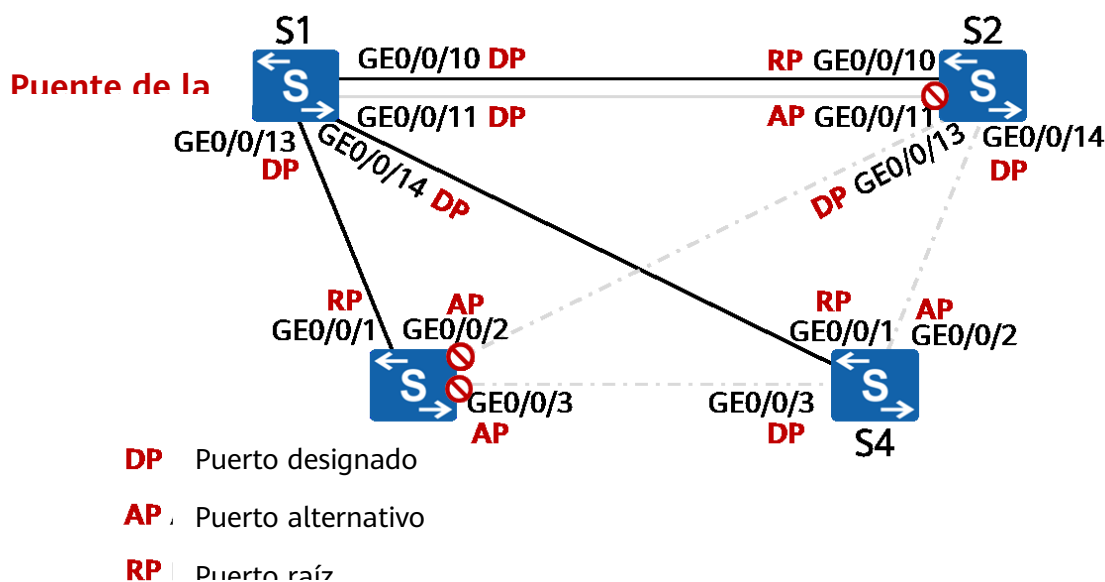
[S3]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/3	ALTE	DISCARDING	NONE

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/3	DESI	FORWARDING	NONE

Según la identificación del puente raíz y la información del puerto de cada switch, la topología actual es la siguiente:



Step 4 Modifique los parámetros del dispositivo para que GigabitEthernet0/0/2 de S4 sea el puerto raíz.

Muestra la información de PTS en S4.



```
[S4]display stp
-----[CIST Global Info][Mode STP]-----
CIST Bridge           :32768.4c1f-cc10-5913
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0 .4c1f-cc33-7359 / 20000
CIST RegRoot/IRPC     :32768.4c1f-cc10-5913 / 0
CIST RootPortId       :128.1
BPDU-Protection       :Disabled
TC or TCN received    :93
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:9m:5s
Number of TC          :18
Last TC occurred      :GigabitEthernet0/0/1
```

El costo de la ruta raíz de S4 a S1 es de 20000.

Cambie el costo de PTS de GigabitEthernet 0/0/1 en S4 a 50000.

```
[S4]interface GigabitEthernet 0/0/1
[S4-GigabitEthernet0/0/1]stp cost 50000
```

Muestra la breve información del estado de los STPs.

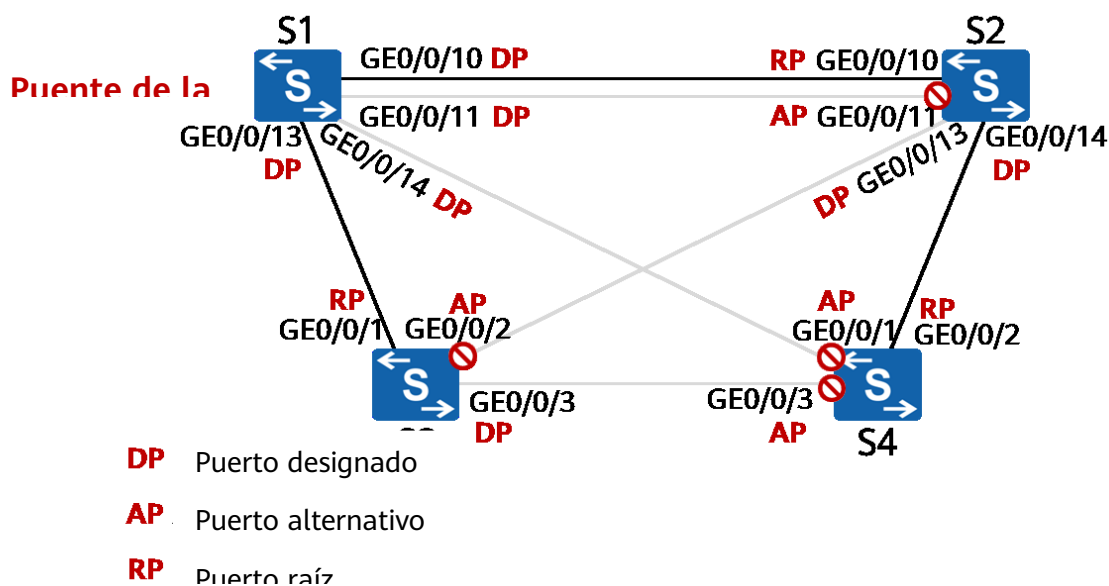
```
[S4]display stp brief
MSTID  Port                Role    STP State    Protection
0      GigabitEthernet0/0/1 ALTE    DISCARDING   NONE
0      GigabitEthernet0/0/2 ROOT    FORWARDING   NONE
0      GigabitEthernet0/0/3 ALTE    DISCARDING   NONE
```

GigabitEthernet0/0/2 en S4 se ha convertido en el puerto raíz.

Muestra la información actual del estado de los STPs.

```
[S4]display stp
-----[CIST Global Info][Mode STP]-----
CIST Bridge           :32768.4c1f-cc10-5913
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :0 .4c1f-cc33-7359 / 40000 //Root path cost = 20000 + 20000 = 40000
CIST RegRoot/IRPC     :32768.4c1f-cc10-5913 / 0
CIST RootPortId       :128.2
BPDU-Protection       :Disabled
TC or TCN received    :146
TC count per hello    :0
STP Converge Mode     :Normal
Time since last TC    :0 days 0h:2m:25s
Number of TC          :20
Last TC occurred      :GigabitEthernet0/0/2
```

La topología actual es la siguiente:



Step 5 Cambie el modo de árbol de expansión a RSTP.

Cambie el modo de árbol de expansión en todos los dispositivos.

```
[S1]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S2]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S3]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S4]stp mode rstp
```

Info: This operation may take a few seconds. Please wait for a moment...done.

Muestra el estado del árbol de esparcimiento. S1 se utiliza como ejemplo.

```
[S1]display stp
```

```
-----[CIST Global Info][Mode RSTP]-----
```

```
CIST Bridge           :0 .4c1f-cc33-7359
Config Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times          :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC        :0 .4c1f-cc33-7359 / 0
CIST RegRoot/IRPC     :0 .4c1f-cc33-7359 / 0
CIST RootPortId       :0.0
BPDU-Protection       :Disabled
CIST Root Type        :Primary root
TC or TCN received    :89
TC count per hello    :0
```



```
STP Converge Mode      :Normal
Time since last TC     :0 days 0h:0m:44s
Number of TC           :27
Last TC occurred       :GigabitEthernet0/0/11
```

Una vez cambiado el modo, la topología del árbol de esparcimiento no se ve afectada.

Step 6 Configure los puertos de borde.

GigabitEthernet 0/0/10-0/0/24 de S3 se conectan sólo a terminales y se deben configurar como puertos de borde.

```
[S3]interface range GigabitEthernet 0/0/10 to GigabitEthernet 0/0/24
```

Un dispositivo proporciona múltiples puertos Ethernet, muchos de los cuales tienen la misma configuración. Configurarlos uno por uno es tedioso y propenso a errores. Una manera fácil es agregar estos puertos a un grupo de puertos y configurar el grupo. El sistema ejecutará automáticamente los comandos en todos los puertos del grupo.



Esta función puede no estar disponible en algunos productos.

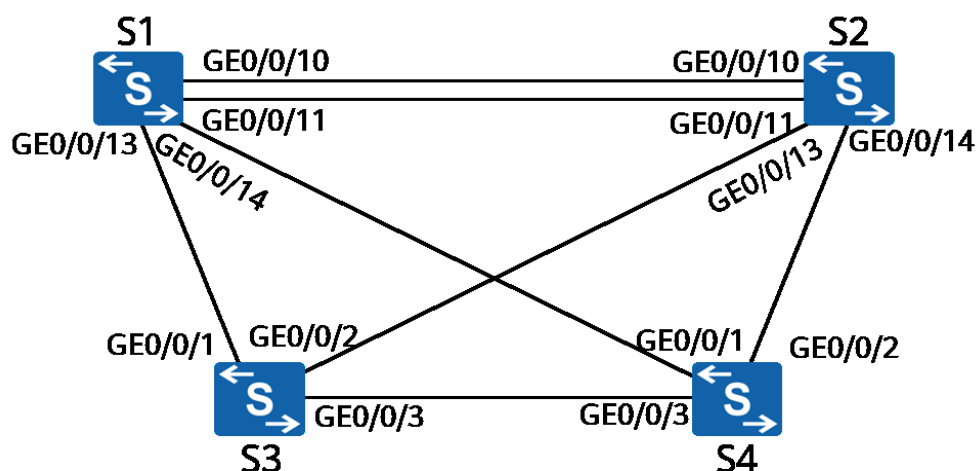
```
[S3-port-group]stp edged-port enable
```

El comando **stp edged-port enable** configura el puerto actual como un puerto de borde. Si un puerto de un dispositivo de conmutación recibe una BPDU después de haber sido configurado como puerto de borde, el dispositivo de conmutación configurará automáticamente el puerto como puerto de borde y recalculará el árbol de expansión.

----Fin

3.2.3 Verificación

1. Marque el puente raíz y el rol de cada puerto en el entorno de laboratorio según la convergencia de red real.





2. Deshabilitar cualquier puerto en cualquier switch y verificar que el tráfico llegue a todos los demás switches a través de los enlaces de respaldo.

3.2.4 Referencia de configuración

Configuración en S1

```
#
sysname S1
#
stp mode rstp
stp instance 0 root primary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

Configuración en S2

```
#
sysname S2
#
stp mode rstp
stp instance 0 root secondary
#
interface GigabitEthernet0/0/12
 shutdown
#
return
```

Configuración en S3

```
#
sysname S3
#
stp mode rstp
#
interface GigabitEthernet0/0/10
 stp edged-port enable
#
interface GigabitEthernet0/0/11
 stp edged-port enable
#
interface GigabitEthernet0/0/12
 stp edged-port enable
#
interface GigabitEthernet0/0/13
 stp edged-port enable
#
interface GigabitEthernet0/0/14
 stp edged-port enable
#
interface GigabitEthernet0/0/15
 stp edged-port enable
#
```



```
interface GigabitEthernet0/0/16
 stp edged-port enable
#
interface GigabitEthernet0/0/17
 stp edged-port enable
#
interface GigabitEthernet0/0/18
 stp edged-port enable
#
interface GigabitEthernet0/0/19
 stp edged-port enable
#
interface GigabitEthernet0/0/20
 stp edged-port enable
#
interface GigabitEthernet0/0/21
 stp edged-port enable
#
interface GigabitEthernet0/0/22
 stp edged-port enable
#
interface GigabitEthernet0/0/23
 stp edged-port enable
#
interface GigabitEthernet0/0/24
 stp edged-port enable
#
return
```

Configuración en S-4

```
#
sysname S4
#
stp mode rstp
#
interface GigabitEthernet0/0/1
 stp instance 0 cost 5000
#
return
```

3.2.5 Quiz

1. En el paso 3, si el costo de GigabitEthernet 0/0/14 en S1 se modifica a 50000, ¿se puede lograr el resultado deseado? - ¿Por qué?
2. En la topología actual, modifique la configuración para que GigabitEthernet0/0/11 de S2 sea el puerto raíz.
3. ¿Pueden los dos enlaces entre S1 y S2 estar en estado de reenvío al mismo tiempo? - ¿Por qué?



3.3 Laboratorio 3: Agregación de enlaces Ethernet

3.3.1 Introducción

3.3.1.1 Acerca de este laboratorio

A medida que las redes crecen a escala, los usuarios necesitan redes de red central Ethernet para proporcionar un mayor ancho de banda y disponibilidad. En el pasado, la única forma de aumentar el ancho de banda era actualizar la red con LPU de alta velocidad, lo cual es costoso e inflexible.

Por el contrario, la agregación de enlaces aumenta el ancho de banda al agrupar un grupo de puertos físicos en un solo puerto lógico, sin necesidad de actualizar el hardware. Además, la agregación de enlaces proporciona mecanismos de respaldo de enlaces, lo que mejora considerablemente la disponibilidad de enlaces. La agregación de enlaces tiene las siguientes ventajas:

- Mejora del ancho de banda: El ancho de banda máximo de un grupo de agregación de enlaces (LAG) es el ancho de banda combinado de todos los enlaces miembros.
- Mejora de la disponibilidad: Si un enlace es defectuoso, el tráfico se puede conmutar a otros enlaces de miembros disponibles.
- Balance de carga: La carga de tráfico puede equilibrarse entre los enlaces de los miembros activos de un GAL.

En esta actividad de laboratorio, aprenderá a configurar la agregación de enlaces Ethernet en modos manual y LACP.

3.3.1.2 Objetivos

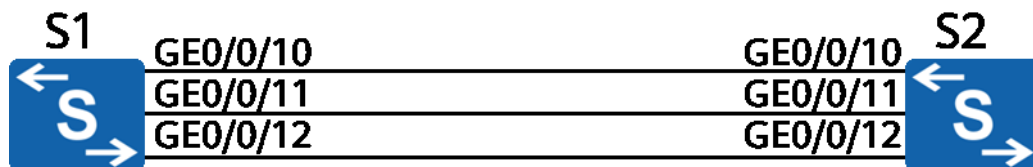
Una vez completada esta tarea, podrás:

- Aprender a configurar manualmente la agregación de enlaces
- Aprender a configurar la agregación de enlaces en modo LACP estático
- Aprender a determinar los enlaces activos en modo LACP estático
- Aprender a configurar algunas funciones LACP estáticas

3.3.1.3 Topología de redes

En la actividad de laboratorio de árboles de esparcimiento, los dos enlaces entre S1 y S2 no pueden estar en el estado de reenvío de datos al mismo tiempo. Para aprovechar al máximo el ancho de banda de los dos enlaces, es necesario configurar la agregación de enlaces Ethernet entre S1 y S2.

Figure 3-3 Topología de laboratorio para la configuración de la agregación de enlaces Ethernet



3.3.2 Configuración del laboratorio

3.3.2.1 Configuración Roadmap

1. Configurar la agregación de enlaces manualmente.
2. Configurar agregación de enlaces en modo LACP.
3. Modificar parámetros para determinar enlaces activos.
4. Cambiar el modo de balanceo de carga.

3.3.2.2 Procedimiento de configuración

Step 1 Configure la agregación de enlaces manualmente.

Cree un Eth-Trunk.

```
[S1]interface Eth-Trunk 1
```

El comando **interface eth-trunk** muestra la vista de un Eth-Trunk existente o crea un Eth-Trunk y muestra su vista. El número 1 de este ejemplo indica el número de puerto.

```
[S2]interface Eth-Trunk 1
```

Configure el modo de agregación de enlaces del Eth-Trunk.

```
[S1-Eth-Trunk1]modo de balanceo manual de carga
```

El comando **mode** configura el modo de operación de la troncal Ethernet, que puede ser LAP o balanceo de carga manual. Por defecto, se utiliza el modo de balanceo de carga manual. Por lo tanto, la operación anterior no es necesaria y se realiza únicamente con fines de demostración.

Agregue un puerto al Eth-Trunk.

```
[S1]interface GigabitEthernet 0/0/10
```

```
[S1-GigabitEthernet0/0/10]eth-trunk 1
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S1-GigabitEthernet0/0/10]quit
```

```
[S1]interface GigabitEthernet 0/0/11
```

```
[S1-GigabitEthernet0/0/11]eth-trunk 1
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S1-GigabitEthernet0/0/11]quit
```



```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]eth-trunk 1
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1-GigabitEthernet0/0/12]quit
```

Se puede ingresar a la vista de interfaces de un puerto individual y agregarlo a un Eth-Trunk. También puede ejecutar el comando **trunkport** en la vista de interfaces Eth-Trunk para agregar múltiples puertos al Eth-Trunk.

```
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Tenga en cuenta los siguientes puntos al agregar puertos físicos a un Eth-Trunk:

- Un Eth-Trunk contiene un máximo de 8 puertos miembros.
- No se puede agregar un Eth-Trunk a otro Eth-Trunk.
- Se puede agregar un puerto Ethernet a un solo Eth-Trunk. Para agregar un puerto Ethernet a otro Eth-Trunk, elimínelo primero del puerto original.
- Los puertos remotos conectados directamente a los puertos de miembro Eth-Trunk locales también se deben agregar a un Eth-Trunk; de lo contrario, los dos extremos no se pueden comunicar.
- Ambos extremos de un Eth-Trunk deben utilizar la misma cantidad de puertos físicos, velocidad de puerto y modo dúplex.

Muestra el estado de un Eth-Trunk.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL                Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1           Max Bandwidth-affected-linknumber: 32
Operate status: up                  Number Of Up Port In Trunk: 3
-----
PortName                Status    Weight
GigabitEthernet0/0/10   Up        1
GigabitEthernet0/0/11   Up        1
GigabitEthernet0/0/12   Up        1
```

Step 2 Configure la agregación de enlaces en modo LACP.

Elimine los puertos de miembro de un Eth-Trunk.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]undo trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]undo trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Antes de cambiar el modo de trabajo de un Eth-Trunk, asegúrese de que el Eth-Trunk no tiene puerto miembro.



Cambiar el modo de agregación.

```
[S1]interfaz Eth-Trunk 1
[S1-Eth-Trunk1]mode lacp
```

El comando **mode lacp** establece el modo de funcionamiento de un Eth-Trunk en LACP.

Nota: El comando es **mode lacp-static** en algunas versiones.

```
[S2]interfaz Eth-Trunk 1
[S2-Eth-Trunk1]mode lacp
```

Agregue un puerto al Eth-Trunk.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

```
[S2]interface Eth-Trunk 1
[S2-Eth-Trunk1]trunkport GigabitEthernet 0/0/10 to 0/0/12
Info: This operation may take a few seconds. Please wait for a moment...done.
```

Muestra el estado del Eth-Trunk.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay: Disabled        Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768          System ID: 4c1f-cc33-7359
Least Active-linknumber: 1      Max Active-linknumber: 8
Operate status: up             Number Of Up Port In Trunk: 3
-----
ActorPortName      Status  PortType  PortPri  PortNo  PortKey  PortState  Weight
GigabitEthernet0/0/10 Selected 1GE      32768    11      305     10111100   1
GigabitEthernet0/0/11 Selected 1GE      32768    12      305     10111100   1
GigabitEthernet0/0/12 Selected 1GE      32768    13      305     10111100   1

Partner:
-----
ActorPortName      SysPri   SystemID   PortPri  PortNo  PortKey  PortState
GigabitEthernet0/0/10 32768    4c1f-ccc1-4a02 32768    11      305     10111100
GigabitEthernet0/0/11 32768    4c1f-ccc1-4a02 32768    12      305     10111100
GigabitEthernet0/0/12 32768    4c1f-ccc1-4a02 32768    13      305     10111100
```

Step 3 En casos normales, solo GigabitEthernet0/0/11 y GigabitEthernet0/0/12 deben estar en estado de reenvío. y GigabitEthernet0/0/10 se utiliza como la copia de seguridad. Cuando la cantidad de puertos activos se reduce a continuación 2, la troncal Ethernet se apaga.

Establezca la prioridad ACP de S1 para hacer de S1 un dispositivo activo.

```
[S1]lacp priority 100
```



Configure las prioridades de los puertos de modo que GigabitEthernet0/0/11 y GigabitEthernet0/0/12 puedan tener una prioridad más alta.

```
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]lacp priority 40000
```

Las unidades de datos del Protocolo de Control de Agregación de Enlaces (LACPDU) son enviadas y recibidas por ambos extremos de un grupo de agregación de enlaces en modo ACP.

Primero, el actor es elegido.

1. Se compara el campo de prioridad del sistema. El valor de prioridad predeterminado es 32768, y un valor inferior indica una prioridad mayor. El criterio de valoración con mayor prioridad es elegido como actor del ACPL.
2. Si hay un empate en la prioridad, el punto terminal con una dirección Mac más pequeña se convierte en el actor.

Una vez elegido el actor, los dispositivos de ambos extremos seleccionan los puertos activos de acuerdo con la configuración de prioridad del puerto del actor.

Configure los umbrales superior e inferior de los puertos activos.

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]max active-linknumber 2
[S1-Eth-Trunk1]least active-linknumber 2
```

El ancho de banda y el estado de un Eth-Trunk dependen del número de puertos activos. El ancho de banda de un Eth-Trunk es el ancho de banda total de todos los puertos miembros en estado Up. Puede establecer los siguientes umbrales para estabilizar el estado y el ancho de banda de un Eth-Trunk, así como reducir el impacto generado por los frecuentes cambios en el estado del enlace de miembro.

- Umbral inferior: Cuando el número de puertos activos cae por debajo de este umbral, el Eth-Trunk baja. Este umbral determina el ancho de banda mínimo de un Eth-Trunk y se configura utilizando el comando **least active-linknumber**.
- Umbral superior: Cuando el número de puertos activos alcanza este umbral, el ancho de banda del Eth-Trunk no aumentará aunque más enlaces miembros vayan hacia arriba. El umbral superior garantiza la disponibilidad de la red y se configura utilizando el comando **max active-linknumber**.

Habilitar la función de preempción.

```
[S1]interfaz Eth-Trunk 1
[S1-Eth-Trunk1]lacp preempt enable
```

En el modo LACP, cuando un enlace activo falla, el sistema selecciona el enlace de respaldo con la prioridad más alta para reemplazar el fallido. Si el enlace defectuoso se recupera y tiene una prioridad mayor que el enlace de respaldo, el enlace recuperado puede restablecer el estado activo si se habilita la preempción. El comando **lacp preempt enable** habilita la preemption LACP. Por defecto, esta función está desactivada.



Muestra el estado del Eth-Trunk actual.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 30         Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100           System ID: 4c1f-cc33-7359
Least Active-linknumber: 2     Max Active-linknumber: 2
Operate status: up            Number Of Up Port In Trunk: 2
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10111100	1
GigabitEthernet0/0/12	Selected	1GE	32768	13	305	10111100	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	32768	4c1f-ccc1-4a02	32768	12	305	10111100
GigabitEthernet0/0/12	32768	4c1f-ccc1-4a02	32768	13	305	10111100

GigabitEthernet0/0/11 and GigabitEthernet0/0/12 are in active state.

Cierre GigabitEthernet0/0/12 para simular un fallo en el enlace.

```
[S1]interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 30         Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100           System ID: 4c1f-cc33-7359
Least Active-linknumber: 2     Max Active-linknumber: 2
Operate status: up            Number Of Up Port In Trunk: 2
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Selected	1GE	40000	11	305	10111100	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10111100	1
GigabitEthernet0/0/12	Unselect	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10111100
GigabitEthernet0/0/11	32768	4c1f-ccc1-4a02	32768	12	305	10111100
GigabitEthernet0/0/12	0	0000-0000-0000	0	0	0	10100011

GigabitEthernet 0/0/10 has become active.

Apague GigabitEthernet 0/0/11 para simular un error de enlace.

```
[S1]interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
```



```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 30         Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100           System ID: 4c1f-cc33-7359
Least Active-linknumber: 2     Max Active-linknumber: 2
Operate status: down          Number Of Up Port In Trunk: 0
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Unselect	1GE	32768	12	305	10100010	1
GigabitEthernet0/0/12	Unselect	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	0	0000-0000-0000	0	0	0	10100011
GigabitEthernet0/0/12	0	0000-0000-0000	0	0	0	10100011

El umbral inferior para la cantidad de enlaces activos se configura en 2. Por lo tanto, el Eth-Trunk se apaga. Aunque GigabitEthernet0/0/10 es Up, todavía está en estado Unselect.

Step 4 Cambiar el modo de balanceo de carga.

Habilite los puertos deshabilitados en el paso anterior.

```
[S1]inter GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]undo shutdown
[S1-GigabitEthernet0/0/11]quit
[S1]inter GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]undo shutdown
```

Espere aproximadamente 30 segundos y verifique el estado de Eth-Trunk 1.

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                      WorkingMode: STATIC
Preempt Delay Time: 30         Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100           System ID: 4c1f-cc33-7359
Least Active-linknumber: 2     Max Active-linknumber: 2
Operate status: down          Number Of Up Port In Trunk: 0
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
GigabitEthernet0/0/10	Unselect	1GE	40000	11	305	10100000	1
GigabitEthernet0/0/11	Selected	1GE	32768	12	305	10100010	1
GigabitEthernet0/0/12	Selected	1GE	32768	13	305	10100010	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
GigabitEthernet0/0/10	32768	4c1f-ccc1-4a02	32768	11	305	10110000
GigabitEthernet0/0/11	0	0000-0000-0000	0	0	0	10100011



GigabitEthernet0/0/12	0	0000-0000-0000	0	0	0	10100011
-----------------------	---	----------------	---	---	---	----------

La función de preferencia está habilitada en la troncal Ethernet. Por lo tanto, cuando GigabitEthernet0/0/11 y GigabitEthernet0/0/12 entra en el estado "UP"., GigabitEthernet0/0/11 y GigabitEthernet0/0/12 tiene una mayor prioridad que GigabitEthernet0/0/10. Como resultado, GigabitEthernet0/0/10 entra en el estado Unselect. Además, para garantizar la estabilidad del enlace, el tiempo de espera predeterminado para la preferencia es de 30 segundos. Por lo tanto, la preferencia se produce 30 segundos después de que se habiliten los puertos.

Cambie el modo de balanceo de carga del Eth-Trunk a balanceo de carga basado en direcciones IP de destino.

```
[S1]interface Eth-Trunk 1
[ S1-Eth-Trunk1]load-balance dst-ip
```

Para garantizar el balanceo de carga adecuado entre los enlaces físicos de un Eth-Trunk y evitar la congestión del enlace, utilice el comando **load-balance** para configurar el modo de balanceo de carga del Eth-Trunk. El balanceo de carga es válido sólo para tráfico saliente, por lo que los modos de balanceo de carga para los puertos de ambos extremos pueden ser diferentes.

----Fin

3.3.3 Verificación

Los detalles no se proporcionan aquí.

3.3.4 Referencia de configuración

Configuración en S1

```
#
sysname S1
#
lacp priority 100
#
interface Eth-Trunk1
 mode lacp
 least active-linknumber 2
 load-balance dst-ip
 lacp preempt enable
 max active-linknumber 2
#
interface GigabitEthernet0/0/10
 eth-trunk 1
 lacp priority 40000
#
interface GigabitEthernet0/0/11
 eth-trunk 1
#
interface GigabitEthernet0/0/12
```

```
eth-trunk 1
#
return
```

Configuración en S2

```
#
sysname S2
#
interface Eth-Trunk1
 mode lacp
#
interface GigabitEthernet0/0/10
 eth-trunk 1
#
interface GigabitEthernet0/0/11
 eth-trunk 1
#
interface GigabitEthernet0/0/12
 eth-trunk 1
#
return
```

3.3.5 Prueba

1. ¿Cuáles son los requisitos para los valores de **least active-linknumber** y **max active-linknumber**?



3.4 Laboratorio 4: Comunicación entre VLAN

3.4.1 Introducción

3.4.1.1 Acerca de este laboratorio

Las VLAN se separan en la capa 2 para minimizar los dominios de difusión. Para permitir la comunicación entre las VLAN, Huawei provee una variedad de tecnologías. Las dos tecnologías siguientes son de uso común:

- **Dot1q subinterfaz de terminación:** Estas subinterfaces son interfaces lógicas de capa 3. Similar a una interfaz VLANIF, luego de configurar una subinterfaz de terminación dot1q y su dirección ip, el dispositivo agrega la entrada correspondiente de direcciones MAC y configura el indicador de reenvío de Capa 3 para implementar la comunicación de Capa 3 entre las VLAN. Una subinterfaz de terminación Dot1q se aplica a escenarios en los que un puerto Ethernet de capa 3 se conecta a varias VLAN.
- **Interfaz VLANIF:** las interfaces VLANIF son interfaces lógicas de capa 3. Una vez configurada la interfaz VLANIF y su dirección Ip, el dispositivo agrega la dirección IP y la ID de la interfaz VLANIF a la tabla de direcciones IP y configura el indicador de reenvío de Capa 3 de la entrada de direcciones IP. Cuando la dirección física de destino de un paquete coincide con la entrada, el paquete se reenvía en la capa 3 para implementar la comunicación de capa 3 entre las VLAN.

En esta actividad de laboratorio, se utilizarán dos métodos para implementar la comunicación entre VLAN.

3.4.1.2 Objetivos.

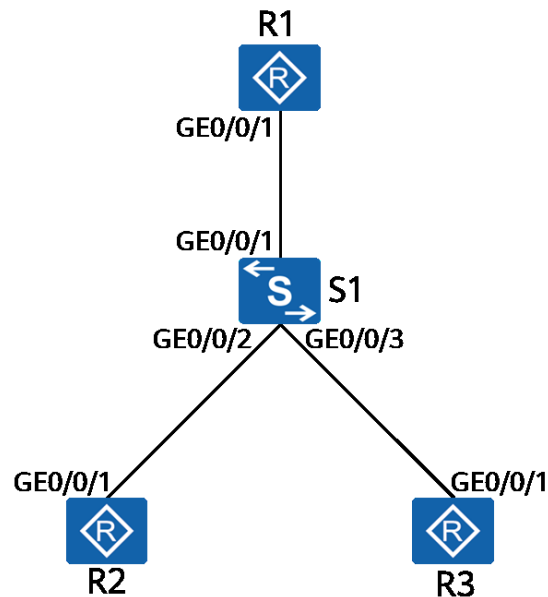
Una vez completada esta tarea, podrá:

- Aprenda a utilizar las subinterfaces de terminación Dot1q para implementar la comunicación entre VLAN.
- Aprenda a utilizar interfaces VLANIF para implementar la comunicación entre VLAN.
- Comprender el proceso de reenvío de la comunicación entre VLAN.

3.4.1.3 Topolog í a de networking

R2 y R3 pertenecen a diferentes VLAN y deben comunicarse entre sí a través de interfaces VLANIF y subinterfaces de terminación Dot1q.

Figure 3-4 Topología de laboratorio para la comunicación entre VLAN



1. Simule a los usuarios de terminales en R2 y R3 y asigne a las interfaces las direcciones IP 192.168.2.1/24 y 192.168.3.1/24.
2. Las direcciones de gateway de R2 y R3 son 192.168.2.254 y 192.168.3.254 respectivamente.
3. En S1, asigne GigabitEthernet0/0/2 y GigabitEthernet0/0/3 a VLAN 2 y VLAN 3, respectivamente.

3.4.2 Configuración de laboratorio

3.4.2.1 Configuración Roadmap

1. Configure las subinterfaces de terminación Dot1q para implementar la comunicación entre VLAN.
2. Configure las interfaces VLANIF para implementar la comunicación entre VLAN.

3.4.2.2 Procedimiento de configuración

Step 1 Completar la configuración básica del dispositivo.

Nombre R1, R2, R3 y S1.

Los detalles no se proporcionan aquí.

Configure direcciones IP y gateways para R2 y R3.

```
<R2> system-view
Enter system view, return user view with Ctrl+Z.
```



```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.2.1 24
[R2-GigabitEthernet0/0/1]quit
[R2]ip route-static 0.0.0.0 0 192.168.2.254
```

Configure una ruta predeterminada (equivalente a un gateway) para el dispositivo.

```
<R3>system-view
Enter system view, return user view with Ctrl+Z.
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.3.1 24
[R3-GigabitEthernet0/0/1]quit
[R3]ip route-static 0.0.0.0 0 192.168.3.254
```

En S1, asigne R2 y R3 a diferentes VLAN.

```
[S1]vlan batch 2 3
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 2
[S1-GigabitEthernet0/0/2]quit
[S1]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 3
```

Step 2 Configure las subinterfaces de terminación Dot1q para implementar la comunicación Inter-VLAN.

Configure un puerto troncal en S1.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
The link between S1 and R1 must allow packets from VLAN 2 and VLAN 3 to pass through because R1 needs to terminate the VLAN tags of packets exchanged between VLANs.
```

Configure una subinterfaz de terminación dot1q en R1.

```
[R1]interface GigabitEthernet 0/0/1.2
```

Se crea una subinterfaz y se muestra la vista de subinterfaz. En este ejemplo, 2 indica el número de subinterfaz. Se recomienda que el número de la subinterfaz sea el mismo que el de la id. de la VLAN.

```
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
```

El comando **dot1q termination vid** vlan-id configura el Id. de Vlan para la terminación Dot1q en una subinterfaz.

En este ejemplo, cuando GigabitEthernet0/0/ 1 recibe datos etiquetados con la VLAN 2, envía los datos a la subinterfaz 2 para la terminación de la VLAN y el procesamiento posterior. Los datos enviados desde la subinterfaz 2 también se etiquetan con la VLAN 2.

```
[R1-GigabitEthernet0/0/1.2]arp broadcast enable
```

Las subinterfaces para la terminación de etiquetas de VLAN no pueden reenviar paquetes de difusión y descartarlos automáticamente al recibir. Para permitir que dichas subinterfaces reenvíen paquetes de difusión, se debe habilitar la función de difusión ARP mediante el comando **arp broadcast enable**. Por defecto, esta función está habilitada en algunos dispositivos.

```
[R1-GigabitEthernet0/0/1.2]ip address 192.168.2.254 24
[R1-GigabitEthernet0/0/1.2]quit
[R1]interface GigabitEthernet 0/0/1.3
[R1-GigabitEthernet0/0/1.3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1.3]arp broadcast enable
[R1-GigabitEthernet0/0/1.3]ip address 192.168.3.254 24
[R1-GigabitEthernet0/0/1.3]quit
```

Pruebe la conectividad entre las VLAN.

```
<R2>ping 192.168.3.1
  PING 192.168.3.1: 56 data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=110 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=70 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=100 ms

  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/76/110 ms

<R2>tracert 192.168.3.1
  traceroute to 192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

  1 192.168.2.254 30 ms 50 ms 50 ms

  2 192.168.3.1 70 ms 60 ms 60 ms
VLAN 2 and VLAN 3 can communicate with each other.
```

Step 3 Configurar interfaces VLANIF para habilitar la comunicación entre VLAN.

Borrar la configuración en el paso anterior.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port trunk allow-pass vlan 2 3
[S1-GigabitEthernet0/0/1]undo port link-type
[R1]undo interface GigabitEthernet 0/0/1.2
[R1]undo interface GigabitEthernet 0/0/1.3
```

Crear una interfaz VLANIF en S1.

```
[S1]interface Vlanif 2
```

El comando **interface vlanif *vlan-id*** crea una interfaz VLANIF y muestra la vista de interfaces VLANIF. Se debe crear una VLAN antes de configurar una interfaz VLANIF.

```
[S1-Vlanif2]ip address 192.168.2.254 24
```



```
[S1-Vlanif2]quit
[S1]interface Vlanif 3
[S1-Vlanif3]ip address 192.168.3.254 24
[S1-Vlanif3]quit
```

Pruebe la conectividad entre las VLAN.

```
<R2>ping 192.168.3.1
PING 192.168.3.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=100 ms
  Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=50 ms
  Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=50 ms
  Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=60 ms
  Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=70 ms
--- 192.168.3.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 50/66/100 ms

<R2>tracert 192.168.3.1

tracert to 192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 192.168.2.254 40 ms 30 ms 20 ms

 2 192.168.3.1 40 ms 30 ms 40 ms
VLAN 2 and VLAN 3 can communicate with each other.
```

----Fin

3.4.3 Verificación

Los detalles no se proporcionan aquí.

3.4.4 Referencia de configuración

Configuración en S1

```
#
sysname S1
#
vlan batch 2 to 3
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
```



```
port link-type access
port default vlan 3
#
return
```

Configuración en R2

```
#
sysname R2
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
return
```

Configuración en R3

```
#
sysname R3
#
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
return
```

3.4.5 Prueba

1. Si R2 necesita acceder a la red conectada a R1, ¿qué configuración se debe realizar en S1?
2. Como interfaz de Capa 3, ¿cuándo se activará una interfaz VLANIF?



4

Conceptos básicos de seguridad de la red y acceso a la red

4.1 Laboratorio 1: Configuración de LCA

4.1.1 Introducción

4.1.1.1 Acerca de este laboratorio

Una lista de control de acceso (LCA) es una colección de una o más reglas. Una regla se refiere a una sentencia que describe una condición de coincidencia de paquetes, que puede ser una dirección de origen, una dirección de destino o un número de puerto.

Una lista de control de acceso es un filtro de paquetes basado en reglas. Los paquetes que coinciden con una lista de control de acceso se procesan según la política definida en la lista de control de acceso.

4.1.1.2 Objetivos.

Una vez completada esta tarea, podrá:

- Aprender a configurar las ACL
- Aprender a aplicar una lista de control de acceso en una interfaz
- Comprender los métodos básicos de filtrado de tráfico.

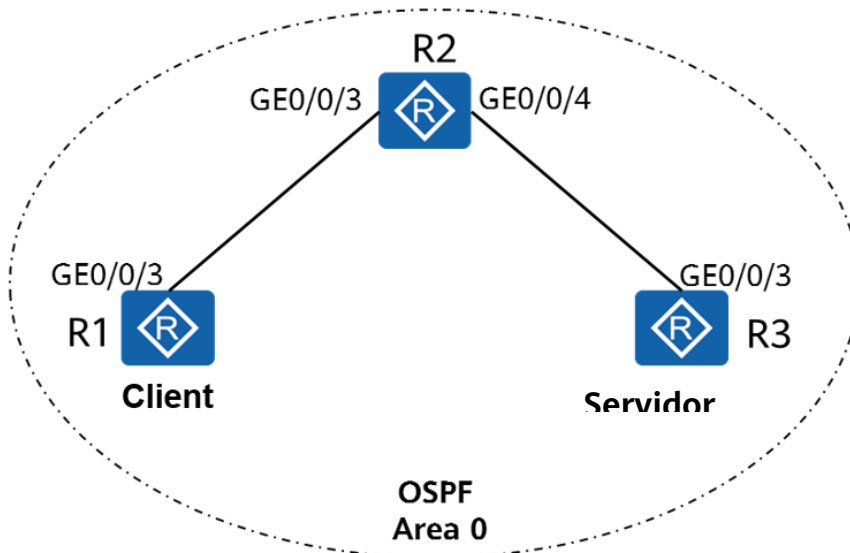
4.1.1.3 Topología de networking

Como se muestra en el diagrama de networking, R3 funciona como el servidor, R1 funciona como el cliente y se puede acceder a ellos para comunicarse con otros. Las direcciones IP de las interfaces físicas que conectan R1 y R2 son 10.1.2.1/24 y 10.1.2.2 /24 respectivamente, y las direcciones IP de las interfaces físicas que conectan R2 y R3 son 10.1.3.2 /24 y 10.1.3.1/24, respectivamente. Además, se crean dos interfaces lógicas LoopBack 0 y LoopBack 1 en la versión 1 para simular dos usuarios clientes. Las direcciones IP de las dos interfaces son 10.1.1.1 /24 y 10.1.4.1/24, respectivamente.

Un usuario (Loopback 1 de R1) necesita gestionar remotamente R3. Se puede configurar Telnet en el servidor, configurar la protección de contraseñas y

configurar una lista de control de acceso para garantizar que solo el usuario que cumpla con la política de seguridad pueda iniciar sesión en la lista de control de acceso.

Figure 4-1 Topología de laboratorio para la configuración de LCA



4.1.2 Configuración de laboratorio

4.1.2.1 Configuración Roadmap

1. Configurar IPs.
2. Configure OSPF para garantizar la conectividad de la red.
3. Cree una lista de control de acceso para que coincida con el tráfico deseado.
4. Configurar filtrado de tráfico.

4.1.2.2 Procedimiento de configuración

Step 1 Configurar IPs.

Configure las direcciones IP para R1, R2 y R3.

```

[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.1.1.1 24
[R1-LoopBack0]quit
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.1.4.1 24
[R1-LoopBack0]quit

```




```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.1.3.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.1.3.1 24
[R3-GigabitEthernet0/0/3]quit
```

Step 2 Configurar OSPF para garantizar la conectividad de la red.

Configurar OSPF en R1, R2 y R3 y asignarlos al área 0 para habilitar la conectividad.

```
[R1]ospf
[R1-ospf-1]zona 0
[R1-ospf-1-area-0.0.0.0]red 10.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]red 10.1.2.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]red 10.1.4.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]return
```

```
[R2]ospf
[R2-ospf-1]zona 0
[R2-ospf-1-area-0.0.0.0]red 10.1.2.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]return
```

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0
[R3-ospf-1-area-0.0.0.0]return
```

Ejecute el comando ping en R3 para probar la conectividad de la red.

```
<R3>ping 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms
Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms
Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms
Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms
Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 10.1.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 20/34/40 ms

<R3>ping 10.1.2.1
PING 10.1.2.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms
```

```
Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms
Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms
--- 10.1.2.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 30/34/50 ms

<R3>ping 10.1.4.1
PING 10.1.4.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms
Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms
Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms
Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms
Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms
--- 10.1.4.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 30/36/50 ms
```

Step 3 Configuración R3 como servidor.

Habilitar la función Telnet en R3, configurar el nivel de usuario en 3, y configurar la contraseña de inicio de sesión en Huawei@123.

```
[R3]telnet server enable
```

El comando **telnet server enable** activa el servicio Telnet.

```
[R3]user-interface vty 0 4
```

El comando **user-interface** muestra una o varias vistas de la interfaz de usuario.

La interfaz de usuario Virtual Type Terminal (VTY) gestiona y monitorea los usuarios que se inician sesión utilizando Telnet o SSH.

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa"
authentication mode.
Enter Password(<8-128>):Huawei@123
Confirm password:Huawei@123
[R3-ui-vty0-4] quit
```

Step 4 Configure una lista de control de acceso para que coincida con el tráfico deseado.

Método 1: Configure una LCA en la interfaz VTY de R3 para permitir que R1 inicie sesión en R3 a través de Telnet utilizando la dirección IP del bucle de retorno 1.

Configure una lista de control de acceso en R3.

```
[words
[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R3-acl-adv-3000 body-]rule 10 deny tcp source any
```



```
[R3-acl-adv-3000]quit
```

Filtrar tráfico en la interfaz VTY de R3.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

Muestra la configuración de la lista de control de acceso en la versión 3.

```
[R3]display acl 3000
```

El comando **display acl** muestra la configuración de LCA.

```
Advanced ACL 3000, 2 rules
```

Se crea una lista de control de acceso avanzada. Tiene el número 3000 y contiene dos reglas.

```
Acl's step is 5
```

El paso entre los números de reglas de LCA es 5.

```
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
```

La regla 5 permite que pase el tráfico correspondiente. Si no hay paquetes que coincidan con la regla, no se muestra el campo **matches**.

```
regla 10 denegar tcp
```

Método 2: Configurar un ACL en la interfaz física de R2 para permitir que R1 se conecte a R3 a través de Telnet desde la dirección IP de la interfaz física.

Configurar una ACL en R2.

```
[R2]acl 3001
[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001]rule 10 deny tcp source any
[R2-acl-adv-3001]quit
```

Filtrar tráfico en GE0/0/3 de R3.

```
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]traffic-filter inbound acl 3001
```

Muestra la configuración de ACL en R2.

```
[R2]display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)
```

La regla 5 permite pasar tráfico coincidente y 21 paquetes han coincidido con la regla.

```
rule 10 deny tcp (1 matches)
```

----Fin



4.1.3 Verificación

Probar el acceso a Telnet y verificar la configuración de ACL.

1. En R1, telnet al servidor con la dirección IP de origen 10.1.1.1 especificada.

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

El comando **telnet** permite al usuario utilizar el protocolo Telnet para iniciar sesión en otro dispositivo.

-a source-ip-address: especifica la dirección IP de origen. Los usuarios pueden comunicarse con el servidor desde la dirección IP especificada.

```
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Error: Can't connect to the remote host
```

2. En R1, telnet al servidor con la dirección IP de origen 10.1.4.1 especificada.

```
<R1>telnet -a 10.1.4.1 10.1.3.1
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Connected to 10.1.3.1 ...
```

```
Login authentication
```

```
Password:
```

```
<R3>quit
```

4.1.4 Referencia de configuración (método 1)

Configuración en R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
ip address 10.1.4.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.1.1.1 0.0.0.0
network 10.1.2.1 0.0.0.0
network 10.1.4.1 0.0.0.0
#
return
```

Configuración en R2

```
#
```



```
sysname R2
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Configuración en R3

```
#
sysname R3
#
acl number 3000
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
telnet server enable
#
user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password
 cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

4.1.5 Referencia de configuración (método 2)

Configuración en R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
```



```
ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
return
```

Configuración en R2

```
#
sysname R2
#
acl number 3001
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
 traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Configuración en R3

```
#
sysname R3
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
telnet server enable
#
user-interface vty 0 4
 authentication-mode password
 user privilege level 3
 set authentication password
 cipher %^%#Z5)H#8cE(YJ6YZ:=']c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```



4.1.6 Prueba

La dirección IP del bucle de retorno 0 en R1 debe utilizarse para acceder únicamente al servicio FTP, y la dirección IP del bucle de retorno 1 en R1 debe utilizarse para gestionar remotamente la R3 utilizando Telnet.

Configure una lista de control de acceso para cumplir con los requerimientos.



4.2 Laboratorio 2: Configuración local de AAA

4.2.1 Introducción

4.2.1.1 Acerca de este laboratorio

La autenticación, autorización y contabilidad (AAA) proporciona un mecanismo de gestión para la seguridad de la red.

El AAA ofrece las siguientes funciones:

- Autenticación: verifica si los usuarios pueden acceder a la red.
- Autorización: autoriza a los usuarios a utilizar determinados servicios.
- Contabilidad: registra los recursos de red utilizados por los usuarios.

Los usuarios pueden utilizar uno o más servicios de seguridad proporcionados por la AAA. Por ejemplo, si una empresa desea autenticar empleados que acceden a ciertos recursos de red, el administrador de red solo necesita configurar un servidor de autenticación. Si la empresa también desea registrar las operaciones realizadas por los empleados en la red, se necesita un servidor de contabilidad.

En resumen, el AAA autoriza a los usuarios a acceder a recursos específicos y registra las operaciones de los usuarios. El AAA se utiliza ampliamente porque ofrece una buena escalabilidad y facilita la gestión centralizada de la información de los usuarios. El AAA puede implementarse utilizando varios protocolos. Radius se utiliza con mayor frecuencia en escenarios reales.

En esta actividad de laboratorio, configurará el AAA local para gestionar y controlar los recursos para usuarios Telnet remotos.

4.2.1.2 Objetivos.

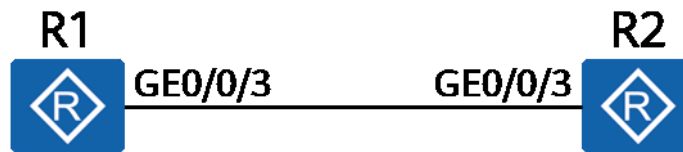
Una vez completada esta tarea, podrá:

- Aprenda a configurar el AAA local
- Aprenda cómo crear un dominio
- Aprenda cómo crear un usuario local
- Comprender la gestión de usuarios basada en dominios

4.2.1.3 Topología de networking

Funciona como cliente y funciona como dispositivo de red. Es necesario controlar el acceso a los recursos de la República 2. Por lo tanto, se debe configurar la autenticación de AAA local en la versión 1 y la versión 2 y gestionar usuarios basados en dominios, y configurar el nivel de privilegios para los usuarios autenticados.

Figure 4-2 Topología de laboratorio para la configuración local de AAA



4.2.2 Configuración de laboratorio

4.2.2.1 Configuración Roadmap

1. Configurar un esquema AAA.
2. Cree un dominio y aplique el esquema de AAA al dominio.
3. Configure usuarios locales.

4.2.2.2 Procedimiento de configuración

Step 1 Completar la configuración básica del dispositivo.

Nombre R1 y R2.

Los detalles no se proporcionan aquí.

Configure las direcciones IP para R1 y R2.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
```

Step 2 Configurar un esquema AAA.

Configure los esquemas de autenticación y autorización.

```
[R2-aaa]aaa
Acceda a la vista AAA.
[R2-aaa wordpom]indonscheme datacom
Información: Cree un nuevo esquema de autenticación.
Cree un esquema de autenticación denominado datacom.
[R2-aaa-authent-datacom] authentication-mode local
Configure el modo de autenticación como autenticación local.
[R2-aaa-authaut-datacom]quit
[R2-aaa]authorization-scheme datacom
Información: Cree un nuevo esquema de autorización.
Cree un esquema de autorización denominado datacom.
[R2-aaa-author-datacom]authorization-mode local
Configure el modo de autorización como autorización local.
[R2-aaa-aut-datacom]quit
```

Un dispositivo que funciona como un servidor AAA se denomina servidor AAA local, que puede realizar autenticación y autorización, pero no contabilidad.

El servidor de AAA local requiere una base de datos de usuarios local, que contiene el nombre de usuario, la contraseña y la información de autorización de los usuarios locales. Un servidor local es más rápido y más barato que un servidor remoto, pero tiene una capacidad de almacenamiento menor.

Step 3 Cree un dominio y aplique el esquema de AAA al dominio.

```
[R2]aaa
[R2-aaa]domain datacom
```

Los dispositivos gestionan a los usuarios según los dominios. Un dominio es un grupo de usuarios y cada usuario pertenece a un dominio. La configuración de AAA para un dominio se aplica a los usuarios del dominio. Cree un dominio llamado datacom.

```
[R2-aaa-domain-datacom]authentication-scheme datacom
El esquema de autenticación denominado datacom se utiliza para los usuarios del dominio.
[R2-aaa-domain-datacom]authorization-scheme datacom
El esquema de autorización denominado datacom se utiliza para los usuarios del dominio.
```

Step 4 Configure usuarios locales.

Cree un usuario local y una contraseña.

```
R2-aaa]local-user hcia@datacom password cipher HCIA-Datacom
Info: Add a new user.
```

Si el nombre de usuario contiene un delimitador de at sign (@), la cadena de caracteres antes del signo at es el nombre de usuario y la cadena de caracteres después del signo at es el nombre de dominio. Si el valor no contiene el signo at, la cadena de caracteres completa representa el nombre de usuario y el nombre de dominio es el predeterminado.

Configure los parámetros para el usuario local, como el tipo de acceso y el nivel de privilegios.

```
[R2-aaa]local-user hcia@datacom service-type telnet
```

El comando **local-user service-type** configura el tipo de acceso para un usuario local. Una vez especificado el tipo de acceso de un usuario, el usuario puede iniciar sesión correctamente solo cuando se utiliza el tipo de acceso configurado. Si el tipo de acceso se configura como telnet, el usuario no puede acceder al dispositivo a través de una página web. Se pueden configurar varios tipos de acceso para un usuario.

```
[R2-aaa]local-user hcia@datacom privilege level 3
```

Se especifica el nivel de privilegio del usuario local. Sólo los comandos dentro del nivel de privilegio especificado o de un nivel inferior están disponibles para un usuario.

Step 5 Habilite la función telnet en R2.

```
[R2ward]telnet server enable
```

Se habilita la función de servidor Telnet en el dispositivo. Esta función está habilitada por defecto en algunos dispositivos.



```
[R2]user-interface vty 0 4
[R2-ui-vty0-4]authentication-mode aaa
```

El comando **authentication-mode** configura un modo de autenticación para acceder a la interfaz de usuario. Por defecto, no se configura el modo de autenticación de usuario de la interfaz de usuario de VTY. Se debe configurar un modo de autenticación para la interfaz de inicio de sesión. De lo contrario, los usuarios no podrán iniciar sesión en el dispositivo.

Step 6 Verificar la configuración.

Telnet R2 desde R1.

```
<R1>telnet 10.0.12.2
Press CTRL_] to quit telnet mode
Trying 10.0.12.2 ...
Connected to 10.0.12.2 ...
```

Login authentication

Username:hcia@datacom

Password:

<R2>

R1 ha iniciado sesión en R2.

Muestra los usuarios en línea en la pantalla.

```
[R2]display users
```

User-Intf	Delay	Type	Network Address	AuthenStatus	AuthorcmdFlag
129 VTY 0	00:02:43	TEL	10.0.12.1	pass	

Username : hcia@datacom

----Fin

4.2.3 Verificación

Los detalles no se proporcionan aquí.

4.2.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
Interfaz GigabitEthernet0,/0,/3
ip address 10.0.12.1 255.255.255.0
#
return
```

Configuración en R2

```
#
sysname R2
```



```
#
aaa
 authentication-scheme datacom
 authorization-scheme datacom
 domain datacom
 authentication-scheme datacom
 authorization-scheme datacom
 local-user hcia@datacom password irreversible-
 cipher %^%#.}hB'1"=&=:FWx!Ust(3s^<.[Z]kEc/>==P56gUVU*cE^]5@|8/O5FC$9A%^%#
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

4.2.5 Quiz

Los detalles no se proporcionan aquí.

4.3 Laboratorio 3: Configuración de NAT

4.3.1 Introducción

4.3.1.1 Acerca de este laboratorio

Traducción de direcciones de red (NAT) traduce la dirección IP de un encabezado de paquete IP a otra dirección Ip. Como plan de transición, permite la reutilización de direcciones para aliviar la escasez de direcciones IPv4. Además de resolver el problema de la escasez de direcciones de P.I., el Plan Nacional de Acción ofrece las siguientes ventajas:

- Protege las redes privadas contra ataques externos.
- Permite y controla la comunicación entre redes privadas y públicas.

En esta actividad de laboratorio, configurará la navegación para comprender su principio.

4.3.1.2 Objetivos.

Una vez completada esta tarea, podrá:

- Aprenda a configurar la navegación dinámica



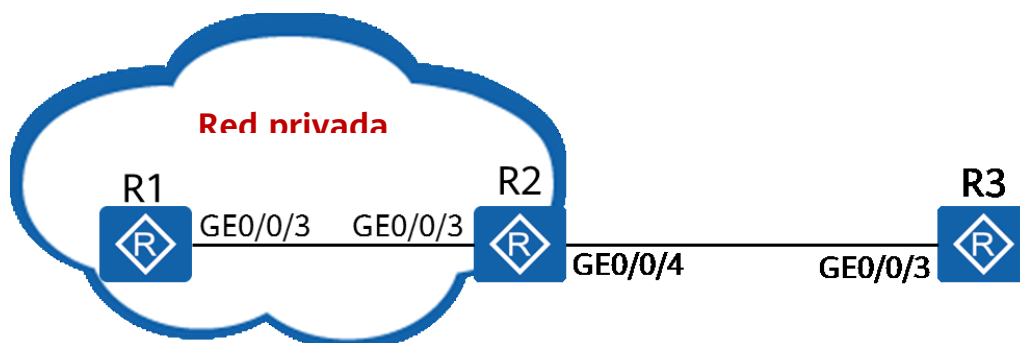
- Aprenda a configurar Easy IP
- Aprenda cómo configurar el servidor de red

4.3.1.3 Topología de networking

Debido a la escasez de direcciones IPv4, las empresas suelen utilizar direcciones IPv4 privadas. Sin embargo, los usuarios de la red empresarial a menudo necesitan acceder a la red pública y prestar servicios a usuarios externos. En este caso, se debe configurar el NAT para cumplir con estos requerimientos.

1. La red entre R1 y R2 es una intranet y utiliza direcciones IPv4 privadas.
2. Funciona como cliente y funciona como gateway de R1 y como router de egreso conectado a la red pública.
3. R3 simula la red pública.

Figure 4-3 Topología de laboratorio para la configuración de NATs



4.3.2 Configuración de laboratorio

4.3.2.1 Configuración Roadmap

1. Configure NAT dinámica.
2. Configure Easy Ip.
3. Configure el servidor NAT.

4.3.2.2 Procedimiento de configuración

Step 1 Configuraciones básicas completas.

Configure direcciones y rutas.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]IP address 192.168.1.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]IP route-static 0.0.0.0 0 192.168.1.254
```



```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 192.168.1.254 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 1.2.3.4 24
[R2-GigabitEthernet0/0/4]quit
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

Configure la función Telnet en R1 y R3 para la verificación posterior.

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]quit
[R1]aaa
[R1-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R1-aaa]local-user test service-type telnet
[R1-aaa]local-user test privilege level 15
```

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
[R3-ui-vty0-4]quit
[R3]aaa
[R3-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R3-aaa]local-user test service-type telnet
[R3-aaa]local-user test privilege level 15
[R3-aaa]quit
```

Probar conectividad.

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56 data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
  100.00% packet loss
```

```
[R2]ping 1.2.3.254
  PING 1.2.3.254: 56 data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=20 ms
```

```
Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms
```

```
--- 1.2.3.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 20/24/40 ms
```

No se puede comunicar con R3 porque no se ha configurado ninguna ruta a 192.168.1.0/24 en R3.

Además, las rutas a las redes privadas no se pueden configurar en la versión 3.

Step 2 La empresa obtiene las direcciones IPs públicas que van desde 1.2.3.10 hasta 1.2.3.20 y necesita la función de NAT dinámica.

Configure un grupo de direcciones de red.

```
[R2]nat address-group 1 1.2.3.10 1.2.3.20
```

El comando **nat address-group** configura un grupo de direcciones de red. En este ejemplo, 1 indica el número del pool de direcciones. El pool de direcciones debe ser un conjunto de direcciones IP consecutivas. Cuando los paquetes de datos internos llegan al borde de la red privada, las direcciones IPs de origen privado se traducen a direcciones IPs públicas.

Configure una lista de control de acceso.

```
[wordpressR2]acl 2000
[R2-acl-basic-2000 laved]rule 5 permit source any
```

Configure Dynamic NAT en GigabitEthernet0/0/4 de R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]nat outbound 2000 address-group 1
```

El comando **nat outbound** asocia una lista de control de acceso a un grupo de direcciones de red. Las direcciones IP de los paquetes que coincidan con la lista de control de acceso se traducirán a una dirección en el pool de direcciones. Si el grupo de direcciones tiene suficientes direcciones, puede agregar el argumento **no-pat** para habilitar la traducción de direcciones uno a uno. En este caso, solo se traducen las direcciones IP de los paquetes de datos y los puertos no se traducen.

Probar conectividad.

```
[R1]ping 1.2.3.254
PING 1.2.3.254: 56 data bytes, press CTRL_C to break
Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=60 ms
Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=20 ms
Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

--- 1.2.3.254 ping statistics ---
 5 packet(s) transmitted
```



```
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 20/32/60 ms

# Telnet R3 from R1 to simulate TCP traffic.
<R1>telnet 1.2.3.254
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.254 ...
  Connected to 1.2.3.254 ...

Login authentication

Username:test
Password:
<R3>
```

Muestra la tabla de sesiones NAT en R2.

```
[R2]display nat session all
NAT Session Table Information:
  Protocol      : TCP(6)
  SrcAddr  Port Vpn  : 192.168.1.1    62185    //Source IP address and source port before NAT
  DestAddr Port Vpn  : 1.2.3.254    23
  NAT-Info
  New SrcAddr   : 1.2.3.11          //Source IP address after NAT
  New SrcPort   : 49149             //Source port after NAT
  New DestAddr  : ----
  New DestPort  : ----

Total : 1
```

Aunque R3 no tiene una ruta a R1, R3 envía los datos a la dirección de origen traducida 1.2.3.11. Después de recibir los datos, R2 traduce la dirección de origen a la dirección de R1 en base a los datos de la tabla de sesiones NAT y reenvía los datos. Por lo tanto, R1 puede iniciar el acceso a R3.

Step 3 Si se asigna dinámicamente la dirección IP de GigabitEthernet0/0/4 en R2 (por ejemplo, a través de DHCP o dialup PPPoE), debe configurar Easy IP.

Eliminar la configuración en el paso anterior.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo nat outbound 2000 address-group 1
```

Configure Easy IP.

```
[R2-GigabitEthernet0/0/1]nat saliente 2000
```

Probar conectividad.

```
[R1]ping 1.2.3.254
PING 1.2.3.254: 56 data bytes, press CTRL_C to break
  Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
  Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
```



```
Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms
```

```
--- 1.2.3.254 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 30/30/30 ms
```

Telnet R3 desde R1 para simular tráfico de TPC.

```
[R2]display nat session all
NAT Session Table Information:
  Protocol      : TCP(6)
  SrcAddr  Port Vpn  : 192.168.1.1    58546           //Source IP address and source port before
NAT
  DestAddr Port Vpn  : 1.2.3.4    23
  NAT-Info
  New SrcAddr      : 1.2.3.4    //Source IP address after NAT, that is, the address of GigabitEthernet
0/0/4 on R2
  New SrcPort       : 49089           //Source port after NAT
  New DestAddr      : ----
  New DestPort      : ----

Total : 1
```

Step 4 R debe proporcionar servicios de red (telnet en este ejemplo) a los usuarios de la red pública. Como R3 no tiene una dirección IP pública, se debe configurar el servidor de NATs en la interfaz de salida de R2.

Configure el servidor en la versión 2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4] nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
```

El comando **nat server** define una tabla de mapeo de servidores internos para que los usuarios externos puedan acceder a los servidores internos a través de la traducción de direcciones y puertos. Se puede configurar un servidor interno para que los usuarios de una red externa puedan iniciar el acceso al servidor interno. Cuando un host de una red externa envía una solicitud de conexión a la dirección pública (dirección global) del servidor de red interno, el servidor de red traduce la dirección de destino de la solicitud en una dirección privada (dirección interna) y envía la solicitud al servidor de la red privada.

Telnet 1 desde R3.

```
< R3>telnet 1.2.3.4 2323
Press CTRL_] to quit telnet mode
Trying 1.2.3.4 ...
Connected to 1.2.3.4 ...

Login authentication

Username:test
Password:
<R1>
```



Muestra la tabla de sesiones de NAT2.

```
[R2]display nat session all
      Protocol           : TCP(6)
      SrcAddr  Port Vpn   : 1.2.3.254    61359
      DestAddr Port Vpn   : 1.2.3.4      2323           //Destination IP address and port before
NAT
      NAT-Info
      New SrcAddr         : ----
      New SrcPort         : ----
      New DestAddr        : 192.168.1.1      //Destination IP address after NAT, that is, the IP
address of R1
      New DestPort        : 23              //Destination port after NAT
Total : 1
```

-----Fin

4.3.3 Verificación

Los detalles no se proporcionan aquí.

4.3.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
aaa
local-user test password irreversible-
cipher %^%#y'BJ=em]VY(E%IH!+,f~[|n*L`HU#H=vlVzMJR'^+^U3qWRm%&:Kd't7oI$%^%#
local-user test privilege level 3
local-user test service-type telnet
#
interface GigabitEthernet0/0/3
ip address 192.168.1.1 255.255.255.0
#
telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
user-interface vty 0 4
authentication-mode aaa
#
return
```

Configuración en R2

```
#
sysname R2
#
acl number 2000
rule 5 permit
#
```



```
nat address-group 1 1.2.3.10 1.2.3.20
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 1.2.3.4 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
 nat outbound 2000
#
return
```

Configuración en R3

```
#
sysname R3
#
aaa
local-user test password irreversible-cipher %^%#s<LQ(8-
ZC6FNGG1#)n=.GgU|@)n`Z'n%$43+2>7,l>#XBkfcu()-3y+o:`UD%^%#
local-user test privilege level 15
local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 1.2.3.254 255.255.255.0
#
telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```

4.3.5 Prueba

1. Cuando se configura el servidor de NAT, ¿los puertos de destino antes de la traducción deben ser los mismos que después de la traducción?

5

Configuración básica de aplicaciones y servicios de red

5.1 Laboratorio 1: Configuración de FTPComment

5.1.1 Introducción

5.1.1.1 Acerca de este laboratorio

Se soportan múltiples modos de gestión de archivos.

como el Protocolo de transferencia de archivos, el Protocolo de transferencia trivial de archivos y el Protocolo de transferencia segura de archivos. Se puede seleccionar uno de acuerdo con los requerimientos de servicio y seguridad.

Un dispositivo puede funcionar como servidor o como cliente.

- Si el dispositivo funciona como servidor, se puede acceder al dispositivo desde un cliente para gestionar archivos en el dispositivo y transferir archivos entre el cliente y el dispositivo.
- Si el dispositivo funciona como cliente, se puede acceder a otro dispositivo (el servidor) desde el dispositivo para gestionar y transferir archivos.

5.1.1.2 Objetivos.

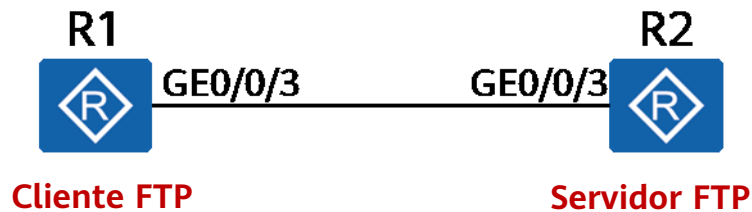
Una vez completada esta tarea, podrá:

- Comprender cómo se establece una conexión ftp
- Aprender a configurar los parámetros del servidor FTPComment
- Aprender cómo transferir archivos a un servidor FTP

5.1.1.3 Topología de redes

R1 necesita gestionar el archivo de configuración de R2.

R1 funciona como cliente FTP y R2 como servidor FTP.

Figure 5-1 Topología de laboratorio para configuración de FTP

5.1.2 Configuración del laboratorio

5.1.2.1 Configuración Roadmap

1. Configurar la función y los parámetros del servidor FTP.
2. Configurar usuarios FTP locales.
3. Inicie sesión en el servidor FTP desde el cliente FTP.
4. Realizar operaciones de archivos desde el cliente FTP.

5.1.2.2 Procedimiento de configuración

Step 1 Completa configuración básica del dispositivo.

Nombra los dispositivos.

Los detalles no se proporcionan aquí.

Configure las direcciones IP del dispositivo.

```
[R1]interfaz GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]dirección IP 10.0.12.1 24
```

```
[R2]interfaz GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]dirección IP 10.0.12.2 24
[R2-GigabitEthernet0/0/3]de forma
```

Guardar el archivo de configuración para su posterior verificación.

```
< R1>save test1.cfg
Are you sure to save the configuration to test1.cfg? (y/n)[n]:y
It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated
```

```
<R2>save test2.cfg
Are you sure to save the configuration to test2.cfg? (y/n)[n]:y
```



It will take several minutes to save configuration file, please wait.....
Configuration file had been saved successfully
Note: The configuration file will take effect after being activated

Muestra la lista de archivos actual.

```
<R1>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	23,963	Feb 21 2020	09:22:53	mon_file.txt
2	-rw-	721	Feb 21 2020	10:14:33	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	783	Jul 10 2018	14:46:16	default_local.cer
5	-rw-	0	Sep 11 2017	00:00:54	brdxpon_snmp_cfg.efs
6	drw-	-	Sep 11 2017	00:01:22	update
7	drw-	-	Sep 11 2017	00:01:48	shelldir
8	drw-	-	Feb 20 2020	21:33:16	localuser
9	drw-	-	Sep 15 2017	04:35:52	dhcp
10	-rw-	509	Feb 21 2020	10:18:31	private-data.txt
11	-rw-	2,686	Dec 19 2019	15:05:18	mon_lpu_file.txt
12	-rw-	3,072	Dec 18 2019	18:15:54	Boot_LogFile
13	-rw-	1,390	Feb 21 2020	10:18:30	test1.cfg

510,484 KB total available (386,448 KB free)

```
<R2>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	11,405	Feb 21 2020	09:21:53	mon_file.txt
2	-rw-	809	Feb 21 2020	10:14:10	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	782	Jul 10 2018	14:48:14	default_local.cer
5	-rw-	0	Oct 13 2017	15:36:32	brdxpon_snmp_cfg.efs
6	drw-	-	Oct 13 2017	15:37:00	update
7	drw-	-	Oct 13 2017	15:37:24	shelldir
8	drw-	-	Feb 20 2020	20:51:34	localuser
9	drw-	-	Oct 14 2017	11:27:04	dhcp
10	-rw-	1,586	Feb 21 2020	10:16:51	test2.cfg
11	-rw-	445	Feb 21 2020	10:16:52	private-data.txt
12	-rw-	4,096	Aug 06 2019	11:19:08	Boot_LogFile

510,484 KB total available (386,464 KB free)
The configuration files of the two devices are saved successfully.

Step 2 Configure la función y los parámetros del servidor FTP2.

```
[R2] ftp server enable
Info: Succeeded in starting the FTP server
```

El comando **ftp server enable** habilita la función de servidor ftp. Por defecto, la función FTP está deshabilitada.

Otros parámetros de configuración opcionales son el número de puerto del servidor FTP, la dirección IP de origen del servidor FTP y el tiempo máximo de inactividad de las conexiones FTP.

Step 3 Configure los usuarios FTP locales.

```
[R2]aaa
[R2-aaa]local-user ftp-client password irreversible-cipher Huawei@123
Info: Add a new user.
[R2-aaa]local-user ftp-client service-type ftp
[R2-aaa]local-user ftp-client privilege level 15
```

Se especifica el nivel de usuario. El nivel de usuario debe configurarse en 3 o superior para garantizar el establecimiento exitoso de la conexión.

```
[R2-aaa]local-user ftp-client ftp-directory flash:/
```

Se especifica el directorio autorizado del usuario ftp. Este directorio debe ser especificado. De lo contrario, el usuario FTP no puede iniciar sesión en el sistema.

Step 4 Inicie sesión en el servidor FTP desde el cliente FTP.

Inicie sesión en el cliente FTP.

```
< R1>ftp 10.0.12.2
Trying 10.0.12.2 ...

Press CTRL+K to abort
Connected to 10.0.12.2.
220 FTP service ready.
User(10.0.12.2:(none)):ftp-client
331 Password required for ftp-client.
Enter password:
230 User logged in.

[R1-ftp]
You have logged in to the file system of R2.
```

Step 5 Realice operaciones en los sistemas de archivos de la versión 2.

Configure el modo de transmisión.

```
[R1-ftp]ascii
200 Type set to A.
```

Los archivos se pueden transferir en modo ASCII o binario.

El modo ASCII se utiliza para transferir archivos de texto plano, y el modo binario se utiliza para transferir archivos de aplicación, como software del sistema, imágenes, archivos de vídeo, archivos comprimidos y archivos de base de datos. El archivo de configuración a descargar es un archivo de texto. Por lo tanto, se debe configurar el modo como ASCII. El modo de transferencia de archivos predeterminado es ASCII. Esta operación es sólo para fines de demostración.

Descargue el archivo de configuración.

```
[R1-ftp]get test2.cfg
```



```
200 Port command okay.
150 Opening ASCII mode data connection for test2.cfg.
226 Transfer complete.
FTP: 961 byte(s) received in 0.220 second(s) 4.36Kbyte(s)/sec.
```

Elimine el archivo de configuración.

```
[R1-ftp]delete test2.cfg
Warning: The contents of file test2.cfg cannot be recycled. Continue? (y/n)[n]:y
250 DELE command successful.
```

Cargue el archivo de configuración.

```
[R1-ftp]put test1.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test1.cfg.
226 Transfer complete.
FTP: 875 byte(s) sent in 0.240 second(s) 3.64Kbyte(s)/sec.
```

Cierre la conexión de ftp.

```
[R1-ftp ]bye
221 Server closing..

<R1>
```

----Fin

5.1.3 Verificación

Muestra los directorios de archivos de R1 y R2.

```
<R1>dir
Directory of flash:/
```

Idx	Attr	Size(Byte)	Date	Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016	17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	23,963	Feb 21 2020	09:22:53	mon_file.txt
2	-rw-	721	Feb 21 2020	10:14:33	vrpcfg.zip
3	drw-	-	Jul 04 2016	18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	783	Jul 10 2018	14:46:16	default_local.cer
5	-rw-	0	Sep 11 2017	00:00:54	brdxpon_snmp_cfg.efs
6	drw-	-	Sep 11 2017	00:01:22	update
7	drw-	-	Sep 11 2017	00:01:48	shelldir
8	drw-	-	Feb 20 2020	21:33:16	localuser
9	drw-	-	Sep 15 2017	04:35:52	dhcp
10	-rw-	1,586	Feb 21 2020	10:26:10	test2.cfg
11	-rw-	509	Feb 21 2020	10:18:31	private-data.txt
12	-rw-	2,686	Dec 19 2019	15:05:18	mon_lpu_file.txt
13	-rw-	3,072	Dec 18 2019	18:15:54	Boot_LogFile
14	-rw-	1,390	Feb 21 2020	10:18:30	test1.cfg

510.484 KB total disponible (386.444 KB gratis)

```
<R2>dir
```




Directory of flash:/

Idx	Attr	Size(Byte)	Date Time(LMT)	FileName
0	-rw-	126,538,240	Jul 04 2016 17:57:22	ar651c- v300r019c00Sspc100.cc
1	-rw-	11,405	Feb 21 2020 09:21:53	mon_file.txt
2	-rw-	809	Feb 21 2020 10:14:10	vrpcfg.zip
3	drw-	-	Jul 04 2016 18:51:04	CPM_ENCRYPTED_FOLDER
4	-rw-	782	Jul 10 2018 14:48:14	default_local.cer
5	-rw-	0	Oct 13 2017 15:36:32	brdxpon_snmp_cfg.efs
6	drw-	-	Oct 13 2017 15:37:00	update
7	drw-	-	Oct 13 2017 15:37:24	shelldir
8	drw-	-	Feb 20 2020 20:51:34	localuser
9	drw-	-	Oct 14 2017 11:27:04	dhcp
10	-rw-	1,390	Feb 21 2020 10:25:42	test1.cfg
11	-rw-	445	Feb 21 2020 10:16:52	private-data.txt
12	-rw-	4,096	Aug 06 2019 11:19:08	Boot_LogFile

510,484 KB total disponible (386,464 KB libre)

5.1.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
return
```

Configuración en R2

```
#
sysname R2
#
aaa
local-user ftp-client password irreversible-
cipher %^%#XqV;f=C;/1!\sQ6LA+Ow8GBO;W%0HBf0`>p(`[SpV]J%Amom!na3:4RvFv@%^%#
local-user ftp-client privilege level 15
local-user ftp-client ftp-directory flash:/
local-user ftp-client service-type ftp
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
ftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```



5.1.5 Quiz

1. ¿Funciona por defecto el ftp en modo activo o pasivo?



5.2 Laboratorio 2: Configuración de DHCP

5.2.1 Introducción

5.2.1.1 Acerca de este laboratorio

El Protocolo de Configuración Dinámica de Host (DHCP) configura y gestiona de manera uniforme las direcciones IPs de los hosts. Simplifica la implementación de la red y la capacidad de ampliación, incluso para redes pequeñas.

DCHP se define en la RFC2131 y utiliza el modo de comunicación cliente /server. Un cliente (cliente DHCP) solicita información de configuración a un servidor (servidor DHCP), y el servidor devuelve la información de configuración asignada al cliente.

Soporta la asignación dinámica y estática de direcciones IPs.

- Asignación dinámica: DHCP asigna una dirección IP con un período de validez limitado (conocido como arrendamiento) a un cliente. Este mecanismo se aplica a escenarios donde los hosts acceden temporalmente a la red y la cantidad de direcciones IPs inactivas es menor que la cantidad total de hosts.
- Asignación estática: DHCP asigna direcciones IP fijas a los clientes tal y como están configuradas. En comparación con la configuración manual de direcciones Ip, la asignación estática de DHCP evita errores de configuración manuales y permite el mantenimiento y la gestión unificados.

5.2.1.2 Objetivos.

Una vez completada esta tarea, podrá:

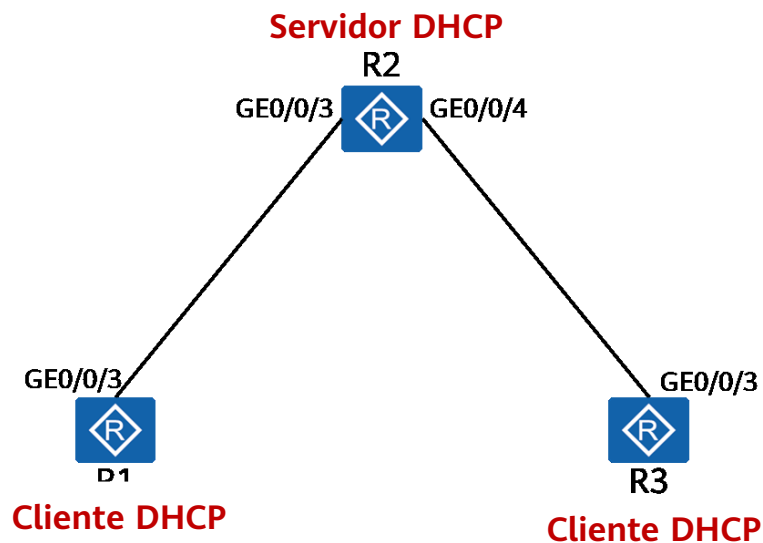
- Aprenda a configurar un pool de direcciones de interfaz en el servidor DHCP
- Aprenda a configurar un pool de direcciones globales en el servidor DHCP
- Aprenda cómo usar DHCP para asignar direcciones IP estáticas

5.2.1.3 Topolog í a de networking

A fin de reducir la carga de trabajo del mantenimiento de las direcciones de P.I. y mejorar la utilización de las direcciones de P.I., una empresa tiene previsto desplegar el DHCP en la red.

1. Configure R1 y R3 como clientes DHCP.
2. Configure R2 como el servidor DCHP para asignar direcciones IPs a R1 y R3.

Figure 5-2 Topología de laboratorio para la configuración de DHCP



5.2.2 Configuración de laboratorio

5.2.2.1 Configuración Roadmap

1. Configure el servidor DHCP.
2. Configure los clientes DHCP.

5.2.2.2 Procedimiento de configuración

Step 1 Configuraciones básicas completas.

Configure las direcciones de la interfaz en R2.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3] ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.0.23.2 24
[R2-GigabitEthernet0/0/4]quit
```

Step 2 Habilitar DHCP.

```
[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```

El comando **dhcp enable** debe ser ejecutado antes de ejecutar cualquier otro comando relacionado con DHCP, independientemente de los servidores o clientes de DHCP.

```
[R2]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
```



```
[R3]dhcp enable
```

Info: The operation may take a few seconds. Please wait for a moment.done.

Step 3 Configure un grupo de direcciones.

Configure un pool de direcciones IPs en G.E. 0/0/3 de R.2 para asignar una dirección IPs a R.1.

```
[R2]interface GigabitEthernet 0/0/3
```

```
[R2-GigabitEthernet0/0/3]dhcp select interface
```

El comando **dhcp select interface** habilita una interfaz para utilizar el pool de direcciones de la interfaz. Si no ejecuta este comando, no se pueden configurar los parámetros relacionados con el pool de direcciones de la interfaz.

```
[R2-GigabitEthernet0/0/wedd3 ]weddhcp server dns-list 10.0.12.2
```

El comando **dhcp server dns-list** configura las direcciones del servidor DNS para un grupo de direcciones de interfaz. Se pueden configurar hasta ocho direcciones de servidores de nombres. Estas IPs están separadas por espacios.

Configure un grupo de direcciones global.

```
[R2]ip pool GlobalPool
```

Info: It's successful to create an IP address pool.

Create an IP address pool named GlobalPool.

```
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
```

El comando **network** especifica una dirección de red para un pool de direcciones global.

```
[R2-ip-pool-GlobalPool]dns-list 10.0.23.2
```

```
[R2-ip-pool-GlobalPool]gateway-list 10.0.23.2
```

El comando **gateway-list** configura una dirección de puerta de enlace para un cliente DHCP. Una vez que obtiene una dirección Ip, genera una ruta predeterminada con la dirección de salto siguiente 10.0.23.2.

```
[ R2-ip-pool-GlobalPool-Edwards ]lease day 2 hour 2
```

El comando **lease** especifica el lease para direcciones IP en un pool de direcciones IP globales. Si el arrendamiento está puesto en **unlimited**, el arrendamiento es ilimitado. Por defecto, el arrendamiento de direcciones IPs es de un día.

```
[R2-ip-pool-GlobalPool words ]static-bind ip-address 10.0.23.mac-address 00e0-fc6f-6d1f
```

El comando **static-bind** asocia una dirección IP de un pool de direcciones globales a una dirección MAC de un cliente. 00e0-fc6f-6d1f es la dirección de MACs de GigabitEthernet0/0/3 en R3. Se puede ejecutar el comando **display interface GigabitEthernet0/0/3** en R3 para mostrar la dirección Mac de GigabitEthernet0/0/3. Una vez ejecutado el comando, R3 obtiene la dirección IP fija 10.0.23.3.

```
[R2-ip-pool-GlobalPool]quit
```

Step 4 Habilita la función de servidor DHCP en GigabitEthernet 0/0/4 de R2 para asignar una dirección IP a R3.



```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcp select global
```

El comando **dhcp select global** habilita una interfaz para utilizar el pool de direcciones global. Después de recibir una solicitud de un cliente DHCP, la interfaz busca en el pool de direcciones globales una dirección IP disponible y asigna la dirección IP al cliente DHCP.

Step 5 Configure un cliente DHCP.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address dhcp-alloc
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3] ip address dhcp-alloc
```

----Fin

5.2.3 Verificación

5.2.3.1 Muestra las direcciones IP y las rutas de R1 y R3.

```
[R1]display ip interface brief
```

Interface	IP Address/Mask	Physical	Protocol
GigabitEthernet0/0/3	10.0.12.254/24	up	up

Aquí sólo se proporciona información clave. El resultado del comando muestra que R1 ha obtenido una dirección ip.

```
[R1]display ip routing-table
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Unr	60	0	D	10.0.12.2	GigabitEthernet0/0/3

Aquí sólo se proporciona información clave. El resultado del comando muestra que R1 ha obtenido la dirección DNS-address.

```
[R1]display ip routing-table
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Unr	60	0	D	10.0.12.2	GigabitEthernet0/0/3

Aquí sólo se proporciona información clave. El resultado del comando muestra que R1 ha obtenido la ruta predeterminada.

```
[R3]display IP interface brief
```

Interface	IP Address/Mask	Physical	Protocol
GigabitEthernet0/0/3	10.0.23.3/24	up	up

Aquí sólo se proporciona información clave. El resultado del comando muestra que R3 ha obtenido una dirección IP fija.

```
[R3]display dns server
```

Type:

D:Dynamic S:Static

No.	Type	IP Address
-----	------	------------

1	D	2.23.0.10
---	---	-----------

Aquí sólo se proporciona información clave. El resultado del comando muestra que R3 ha obtenido la dirección DNS-address.

```
[R3]display ip routing-table
```



Route Flags: R - relay, D - download to fib

Routing Tables: Public

Destinations : 8 Routes : 8

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
0.0.0.0/0	Unr	60	0	D	10.0.23.2	GigabitEthernet0/0/3

Aquí sólo se proporciona información clave. El resultado del comando muestra que R3 ha obtenido la ruta predeterminada.

5.2.3.2 Muestra la asignación de direcciones en R2.

```
[R2]display ip pool name GlobalPool
```

Pool-name : GlobalPool
Pool-No : 1
Lease : 2 Days 2 Hours 0 Minutes
Domain-name : -
DNS-server0 : 10.0.23.2
NBNS-server0 : -
Netbios-type : -
Position : Local Status : Unlocked
Gateway-0 : **10.0.23.2**
Mask : **255.255.255.0**
VPN instance : --

Start	End	Total	Used	Idle(Expired)	Conflict	Disable
10.0.23.1	10.0.23.254	253	1	252(0)	0	0

El comando **display IP pool** muestra la información de configuración del pool de direcciones, que incluye el nombre, la concesión, el estado de bloqueo y el estado de la dirección IP.

```
[R2]display ip pool interface GigabitEthernet0/0/4
```

Pool-name : **GigabitEthernet0/0/4**
Pool-No : 0
Lease : 1 Days 0 Hours 0 Minutes
Domain-name : -
DNS-server0 : **10.0.12.2**
NBNS-server0 : -
Netbios-type : -
Position : Interface Status : Unlocked
Gateway-0 : **10.0.12.2**
Mask : 255.255.255.0
VPN instance : --

Start	End	Total	Used	Idle(Expired)	Conflict	Disable
10.0.12.1	10.0.12.254	253	1	252(0)	0	0

Cuando se configura un grupo de direcciones de interfaz, el nombre del grupo de direcciones es el nombre de la interfaz. La dirección del gateway asignado es la dirección IP de la interfaz y no se puede cambiar.



5.2.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
dhcp enable
#
interface GigabitEthernet0/0/3
ip address dhcp-alloc
#
return
```

Configuración en R2

```
#
sysname R2
#
dhcp enable
#
ip pool GlobalPool
gateway-list 10.0.23.2
network 10.0.23.0 mask 255.255.255.0
static-bind ip-address 10.0.23.3 mac-address a008-6fe1-0c47
lease day 2 hour 2 minute 0
dns-list 10.0.23.2
#
interface GigabitEthernet0/0/3
ip address 10.0.12.2 255.255.255.0
dhcp select interface
dhcp server dns-list 10.0.12.2
#
interface GigabitEthernet0/0/4
ip address 10.0.23.2 255.255.255.0
dhcp select global
#
return
```

Configuración en R3

```
#
sysname R3
#
dhcp enable
#
interface GigabitEthernet0/0/3
ip address dhcp-alloc
#
return
```

5.2.5 Quiz

1. ¿Cuáles son las diferencias entre los escenarios de aplicación de un pool de direcciones global y los de un pool de direcciones de interfaz?



2. Si hay varios grupos de direcciones globales, ¿cómo se determina el grupo de direcciones global para un cliente DHCP?



6 Creación de una red local inalámbrica

6.1 Introducción

6.1.1 Acerca de este laboratorio

Las LAN cableadas son caras y carecen de movilidad. La creciente demanda de portabilidad y movilidad exige tecnologías de redes inalámbricas inalámbricas. La red inalámbrica a internet es ahora el modo de acceso a la red más rentable y conveniente. WiFi permite a los usuarios moverse dentro del área cubierta.

En esta actividad de laboratorio, configurará una red local inalámbrica utilizando un CA y ajustará los AP.

6.1.2 Objetivos.

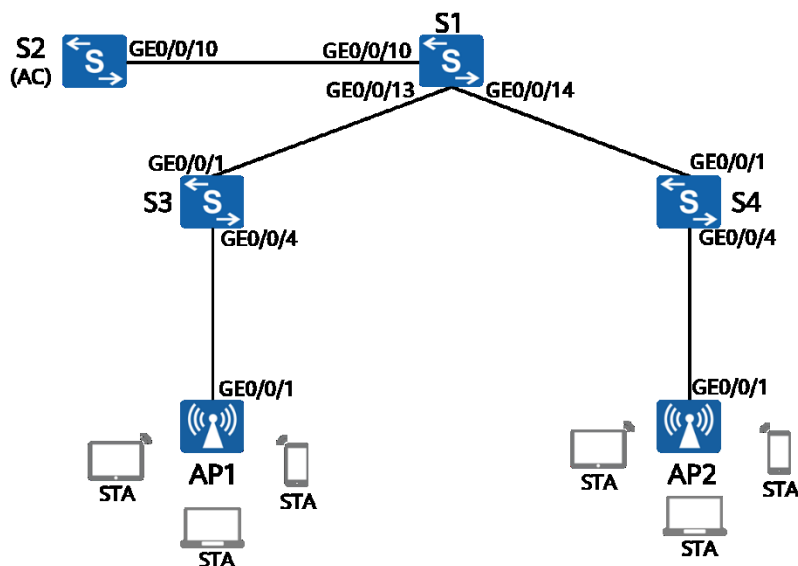
Una vez completada esta tarea, podrá:

- Aprender a autenticar AP
- Aprenda a configurar perfiles de red inalámbrica
- Comprender el proceso de configuración básica de la red WLAN.

6.1.3 Topología de networking

1. El switch S2soporta la función WLAN-AC. Si el switch no soporta la función WLAN-AC, utilice una CA común para reemplazar el switch. El CA del siguiente contenido es un switch S2.
2. El CA se implementa en modo fuera de ruta y se encuentra en la misma red de capa 2 que los AP.
3. El CA funciona como un servidor DHCP para asignar direcciones IPs a los AP, el S1 funciona como un servidor DHCP para asignar direcciones IPs a las estaciones (STA).
4. Los datos del servicio se reenvían directamente.

Figure 6-1 Topología de laboratorio para crear una red local inalámbrica



6.1.4 Planificación de datos

Una empresa necesita crear una red inalámbrica para facilitar la movilidad en el lugar de trabajo.

Table 6-1 Planificación de datos de CA

Elemento	Configuración
VLAN de gestión de PA	VLAN 100
VLANServicio	VLAN 101
Servidor DHCP	El CA funciona como un servidor DHCP para asignar direcciones IPs a los AP.
	Funciona como un servidor DHCP para asignar direcciones IPs a las STA. La dirección del gateway predeterminado de las STA es 192.168.101.254.
Pool de direcciones IPs para AP	192.168.100.1-192.168.100.253/24
Pool de direcciones IPs para STA	192.168.101.1-192.168.101.253/24
Dirección IP de la interfaz de origen del CI	VLANIF100:192.168.100.254 /24
Grupo de puntos de	Nombre: ap-group1



Elemento	Configuración
acceso	Perfiles de referencia: Perfil de VAP HCIA-wlan y perfil de dominio regulatorio default
Perfil de dominio regulatorio	Nombre: predeterminado
	Código del país: NC
Perfil de SSID	Nombre: HCIA-WLAN
	Nombre del SSID: HCIA-WLAN
Perfil de seguridad	Nombre: HCIA-WLAN
	Política de seguridad: WPA-WPA2+PSK+AES
	Contraseña: HCIA-Datacom
Perfil de PVA	Nombre: HCIA-WLAN
	modo de reenvío: reenvío directo
	Vlan de servicio: Vlan 101
	Perfiles de referencia: Perfil de SSID HICIA-WLAN y perfil de seguridad HICIA-WLAN

6.2 Configuración de laboratorio

6.2.1 Configuración Roadmap

1. Configure la conectividad de la red cableada.
2. Configure los AP y póngalos en línea.
 - (1) Cree grupos de puntos de acceso y agregue puntos de acceso de la misma configuración al mismo grupo para una configuración unificada.
 - (2) Configure los parámetros del sistema de CA, incluidos el código de país y la interfaz de origen utilizados por el CA para comunicarse con los AP.
 - (3) Configure el modo de autenticación de puntos de acceso e importe los puntos de acceso para ponerlos en línea.
3. Configure los parámetros del servicio WiFi y envíelos a los AP para que las STA accedan a la WiFi.

6.2.2 Procedimiento de configuración

Step 1 Configuraciones básicas completas de dispositivos.



Nombre los dispositivos (nombre S2 en el **CA** de topología)

Los detalles no se proporcionan aquí.

Cierre los puertos innecesarios entre S1 y CA. Este paso sólo se aplica al entorno descrito en HCIA-Datacom Lab Construction Guide V1.0.

```
[S1] interface GigabitEthernet 0/0/11
[S1-GigabitEthernet0/0/11]shutdown
[S1-GigabitEthernet0/0/11]quit
[S1] interface GigabitEthernet 0/0/12
[S1-GigabitEthernet0/0/12]shutdown
[S1-GigabitEthernet0/0/12]quit
```

Habilite la función PoE en los puertos S3 y S4 conectados a los AP.

```
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]poe enable
```

El comando **poe enable** habilita la función PoE en un puerto. Cuando un puerto detecta un dispositivo alimentado (DP) conectado a él, el puerto suministra energía a la DP. Por defecto, la función PoE está habilitada. Por lo tanto, este comando es innecesario y se proporciona únicamente con fines de demostración.

```
[S4- ]interface GigabitEthernet 0/0/4
[S4-GigabitEthernet0/0/4]poe enable
```

Step 2 Configure la red cableada.

Configure las VLAN.

```
[S1]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13]quit
[S1]interface GigabitEthernet 0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14]quit
[S1]interface GigabitEthernet 0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10]quit
```

```
[AC]vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC]interface GigabitEthernet 0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10]quit
```

```
[S3]vlan batch 100 101
```



Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S3]interface GigabitEthernet 0/0/1
[S3-GigabitEthernet0/0/1]port link-type trunk
[S3-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/1]quit
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]port link-type trunk
[S3-GigabitEthernet0/0/4]port trunk pvid vlan 100
[S3-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S3-GigabitEthernet0/0/4]quit
```

```
[S4]vlan batch 100 101
```

Info: This operation may take a few seconds. Please wait for a moment...done.

```
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1] port link-type trunk
[S4-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/1]quit
[S4]interface GigabitEthernet0/0/4
[S4-GigabitEthernet0/0/4] port link-type trunk
[S4-GigabitEthernet0/0/4] port trunk pvid vlan 100
[S4-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 to 101
[S4-GigabitEthernet0/0/4]quit
```

Configurar direcciones IP de la interfaz.

```
[S1]interface Vlanif 101
[S1-Vlanif101]ip address 192.168.101.254 24
Gateway for STAs
[S1-Vlanif101]quit
[S1]interface LoopBack 0
[S1-LoopBack0] ip address 10.0.1.1 32
This operation is for subsequent test only.
[S1-LoopBack0]quit
```

```
[AC]interface Vlanif 100
[AC-Vlanif100]ip address 192.168.100.254 24
```

Configurar el DHCP.

```
[S1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[S1]ip pool sta
Info:It's successful to create an IP address pool.
IP address pool for STAs
[S1-ip-pool-sta]network 192.168.101.0 mask 24
[S1-ip-pool-sta]gateway-list 192.168.101.254
[S1-ip-pool-sta]quit
[S1]interface Vlanif 101
[S1-Vlanif101]dhcp select global
[S1-Vlanif101]quit
```

```
[AC]dhcp enable
```



```
Info: The operation may take a few seconds. Please wait for a moment.done.
```

```
[AC]ip pool ap
```

```
Info: It is successful to create an IP address pool.
```

```
IP address pool for APs
```

```
[AC-ip-pool-ap]network 192.168.100.254 mask 24
```

```
[AC-ip-pool-ap]gateway-list 192.168.100.254
```

```
[AC-ip-pool-ap]quit
```

```
[AC]interface Vlanif 100
```

```
[AC-Vlanif100]dhcp select global
```

```
[AC-Vlanif100]quit
```

S1 es el servidor DHCP para las STA y el CA es el servidor DHCP para los APs.

Step 3 Configure los AP para ponerlos en línea.

Cree un grupo de puntos de acceso y nómbrelo ap-group1.

```
[AC]wlan
```

```
[AC-wlan-view]ap-group name ap-group1
```

```
Info: This operation may take a few seconds. Please wait for a moment.done.
```

```
[AC-wlan-ap-group-ap-group1]quit
```

Cree un perfil de dominio regulatorio y configure el código de país de CA en el perfil.

```
[AC]wlan
```

```
[AC-wlan-view]regulatory-domain-profile name default
```

Un perfil de dominio regulador proporciona configuraciones de código de país, canal de calibración y ancho de banda de calibración para un punto de acceso.

El perfil de dominio regulatorio predeterminado se denomina **default**. Por lo tanto, se muestra el perfil predeterminado.

```
AC-wlan-regulate-domain-default]country-code cn
```

```
Info: The current country code is same with the input country code.
```

Un código de país identifica el país en el que se despliegan los AP. Diferentes países requieren diferentes atributos de radio de punto de acceso, entre ellos la potencia de transmisión y los canales soportados. La configuración correcta del código de país garantiza que los atributos de radio de los AP cumplan con las leyes y reglamentaciones locales. Por defecto, se configura el código de país NC.

```
[AC-wlan-regulate-domain-default]quit
```

Vincule el perfil de dominio regulatorio a un grupo de puntos de acceso.

```
[AC]wlan
```

```
[AC-wlan-view]ap-group name ap-group1
```

```
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
```

```
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
```

El comando **regulatory-domain-profile** de la vista de grupo de puntos de acceso vincula un perfil de dominio regulador a un punto de acceso o grupo de puntos de acceso. De forma predeterminada, el perfil de dominio regulatorio **default** está vinculado a un grupo de puntos de acceso, pero ningún perfil de dominio



regulatorio está vinculado a un punto de acceso. En el perfil de dominio regulador por defecto, el código de país es NC. Por lo tanto, los canales de calibración de 2,4GHz incluyen los canales 1, 6 y 11, y los canales de calibración de 5 GHz incluyen los canales 149, 153, 157, 161 y 165. Por lo tanto, este paso y el paso anterior se pueden omitir.

```
[AC-wlan-ap-group-ap-group1]quit
```

Especifique una interfaz de origen en el CA para establecer túneles Capwap.

```
[AC]capwap source interface Vlanif 100
```

El comando **capwap source interface** configura la interfaz utilizada por el CA para configurar túneles Capwap con AP.

Importe AP al CA y agregue AP al grupo de AP **ap-group1**.

Los AP se pueden agregar a un CA de las siguientes maneras:

- Configuración manual: Especifique las direcciones MACs y los números de serie (NS) de los AP en el CA con antelación. Cuando los AP se conectan con el CA, el CA detecta que sus direcciones MAC y los SN coinciden con los preconfigurados y establece conexiones con ellos.
- Detección automática: cuando el modo de autenticación de punto de acceso está configurado como sin autenticación, o el modo de autenticación de punto de acceso está configurado como autenticación de punto de acceso o de punto de acceso y las direcciones de punto de acceso o los SN están en la lista blanca, el controlador de acceso detecta automáticamente los puntos de acceso conectados y establece conexiones con ellos.
- Confirmación manual: Si el modo de autenticación de punto de acceso se configura como autenticación de MACs o NS y la dirección MACs o NS de un punto de acceso conectado no se incluye en la lista blanca del CA, el CA agrega el punto de acceso a la lista de puntos de acceso no autorizados. Puede confirmar manualmente la identidad de dicho punto de acceso para ponerlo en línea.

```
[AC]wlan
```

```
[AC-wlan-view]ap auth-mode mac-auth
```

El comando **ap auth-mode** configura el modo de autenticación de punto de acceso. Solo los AP autenticados pueden conectarse. Los modos de autenticación incluyen la autenticación de direcciones MAC, la autenticación de NS y la no autenticación. El modo de autenticación de punto de acceso predeterminado es la autenticación de direcciones de MACs.

Nota: Para obtener información sobre la dirección física y el NS de un punto de acceso, compruebe la etiqueta de dirección física y la etiqueta de NS del paquete.

```
[AC-wlan-view]ap-id 0 ap-mac 60F1-8A9C-2B40
```

El comando **ap-id** agrega un punto de acceso o muestra la vista de punto de acceso.



El argumento **ap-mac** especifica la autenticación de direcciones MACs, y el argumento **ap-sn** especifica la autenticación de NS.

En la vista de puntos de acceso, puede introducir ap-id para introducir la vista de puntos de acceso correspondiente.

```
[AC-wlan-ap-0]ap-name ap1
```

El comando **ap-name** configura el nombre de un punto de acceso. Los nombres de los puntos de acceso deben ser únicos. Si el nombre del punto de acceso no está configurado, el nombre predeterminado es la dirección física del punto de acceso.

```
[ AC-wlan-ap-0]ap-group ap-group1
```

El comando **ap-group** configura el grupo para un punto de acceso. El CA entrega la configuración a los AP. Por ejemplo, si se agrega AP1 a ap-group1, el perfil de dominio regulatorio, el perfil de radio y el perfil de AP1 asociado a ap-group1 se entregan a AP1. Por defecto, no se agrega un punto de acceso a ningún grupo. Cuando se agrega un punto de acceso a un grupo o el grupo de un punto de acceso cambia, la configuración del grupo será enviada automáticamente por el punto de acceso y el punto de acceso se reiniciará automáticamente para unirse al grupo.

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y //Enter y to confirm.

Info: This operation may take a few seconds. Please wait for a moment.. done.

```
[AC-wlan-ap-0]quit
```

```
[AC-wlan-view]ap-id 1 ap-mac B4FB-F9B7-DE40
```

```
[AC-wlan-ap-1]ap-name ap2
```

```
[AC-wlan-ap-1]ap-group ap-group1
```

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, Whether to continue? [Y/N]:y //Enter y to confirm.

Info: This operation may take a few seconds. Please wait for a moment.. done.

```
[AC-wlan-ap-1]quit
```

Muestra la información del punto de acceso actual.

```
[AC]wlan
```

```
[AC-wlan-view]display ap all
```

Info: This operation may take a few seconds. Please wait for a moment..done.

Total AP information:

nor : normal [2]

ID	MAC	Name	Group	IP	Type	State	STA	Uptime
0	00e0-fc25-0ed0 ap1	ap-group1		192.168.100.206	AirEngine5760	nor	0	30M:4S
1	00e0-fc0f-07a0 ap2	ap-group1		192.168.100.170	AirEngine5760	nor	0	31M:31S
Total: 2								

El comando **display ap** muestra la información de los puntos de acceso, incluida la dirección Ip, el modelo (AirEngine5760), el estado (normal) y la duración en línea del punto de acceso.

Además, puede agregar el *estado* **by-state** o un *ssid* **by-ssid** para filtrar los AP en un estado especificado o utilizando un identificador de sistema especificado.

El resultado del comando muestra que los dos AP funcionan correctamente. (Para obtener más información sobre el estado, consulte el apéndice de este laboratorio.)

Step 4 Configure los parámetros del servicio WLAN.

Cree el perfil de seguridad **HCIA-WLAN** y configure una política de seguridad.

```
[ AC-wlan-view ]security-profile name HCIA-WLAN
[ AC-wlan-sec-prof-HCIA-WLAN ~ ]security wpa-wpa2 psk pass-phrase HCIA-Datacom aes
```

El comando **security psk** configura la autenticación y el cifrado de clave precompartida WPA2.

En la actualidad, se utilizan tanto WP2 como WP2. Los terminales de usuario se pueden autenticar mediante WPA o WPA2. La clave de acceso del proveedor se configura como **HCIA-Datacom**. Los datos de usuario se cifran mediante el algoritmo de cifrado de la tarjeta de acceso.

```
[ AC-wlan-sec-prof-HCIA-WLAN]quit
```

Cree el perfil de SSID **HCIA-WLAN** y establezca el nombre de SSID en **HCIA-WLAN**.

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
SSID profile HCIA-WLAN is created.
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
The SSID name is set to HCIA-WLAN.
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-HCIA-WLAN]quit
```

Cree el perfil de VAP **HCIA-WLAN**, configure el modo de reenvío de datos y la VLAN de servicio, y aplique el perfil de seguridad y el perfil de SSID al perfil de VAP.

```
[AC]wlan
[AC-wlan-view]vap-profile name HCIA-WLAN
```

El comando **vap-profile** crea un perfil de punto de acceso virtual.

Se puede configurar el modo de reenvío de datos en un perfil de punto de acceso virtual y asociar el perfil de punto de acceso, el perfil de seguridad y el perfil de tráfico al perfil de punto de acceso virtual.

```
[ AC-wlan-vap-prof-HCIA-WLAN ] forward-mode direct-forward
```

El comando **forward-mode** configura el modo de reenvío de datos en un perfil de punto de acceso virtual. Por defecto, el modo de reenvío de datos es el reenvío directo.

```
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
```

El comando **service-vlan** configura la Vlan de servicio de un Vap. Una vez que la AT accede a una red local, los datos de usuario enviados por el punto de acceso transportan la etiqueta de **service-VLAN**.

```
Info: This operation may take a few seconds, please wait.done.
```

```
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
```

```
Security profile HCIA-WLAN is bound.
```

```
Info: This operation may take a few seconds, please wait.done.
```

```
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
```

```
SSID profile HCIA-WLAN is bound.
```

```
Info: This operation may take a few seconds, please wait.done.
```

```
[AC-wlan-vap-prof-HCIA-WLAN]quit
```

Vincule el perfil de punto de acceso al grupo de punto de acceso y aplique las configuraciones del perfil de punto de acceso **HCIA-WLAN** a la radio 0 y a la radio 1 de los puntos de acceso del grupo de punto de acceso.

```
[AC]wlan
```

```
[AC-wlan-view]ap-group name ap-group1
```

```
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

El comando **vap-profile** enlaza un perfil de punto de acceso virtual a una radio. Una vez ejecutado este comando, todas las configuraciones del punto de acceso virtual, incluidas las configuraciones de los perfiles asociados al punto de acceso virtual, se entregan a los radios de los puntos de acceso.

```
Info: This operation may take a few seconds, please wait...done.
```

```
[AC-wlan-ap-group-ap-group1]quit
```

----Fin

6.3 Verificación

1. Use una AT para acceder a la WiFi con el identificador de red SSID de **HCIA-WLAN**. Verifique la dirección IP obtenida por la EST y haga ping a la dirección IP (10.0.1.1) del LoopBack0 en S1.
2. Cuando se conecta la estación de prueba al aire acondicionado, ejecute el comando **display station all** en el aire acondicionado para verificar la información de la estación de prueba.

6.4 Referencia de configuración

Configuración en S1



```
#
sysname S1
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool sta
 gateway-list 192.168.101.254
 network 192.168.101.0 mask 255.255.255.0
#
interface Vlanif101
 ip address 192.168.101.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/14
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
interface LoopBack0
 ip address 10.0.1.1 255.255.255.255
#
return
```

Configuración en el AC

```
#
sysname AC
#
vlan batch 100 to 101
#
dhcp enable
#
ip pool ap
 gateway-list 192.168.100.254
 network 192.168.100.0 mask 255.255.255.0
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/10
 port link-type trunk
 port trunk allow-pass vlan 100 to 101
#
wlan
```



```
security-profile name HCIA-WLAN
  security wpa-wpa2 psk pass-phrase %^%#V-rr;CTW$X%,nJ/0jcmO!tRQ(pt;^8IN,z1||UU)%^%# aes
ssid-profile name HCIA-WLAN
  ssid HCIA-WLAN
vap-profile name HCIA-WLAN
  service-vlan vlan-id 101
  ssid-profile HCIA-WLAN
  security-profile HCIA-WLAN
ap-group name ap-group1
  radio 0
    vap-profile HCIA-WLAN wlan 1
  radio 1
    vap-profile HCIA-WLAN wlan 1
  radio 2
    vap-profile HCIA-WLAN wlan 1
ap-id 0 type-id 75 ap-mac 60f1-8a9c-2b40 ap-sn 21500831023GJ9022622
  ap-name ap1
  ap-group ap-group1
ap-id 1 type-id 75 ap-mac b4fb-f9b7-de40 ap-sn 21500831023GJ2001889
  ap-name ap2
  ap-group ap-group1
provision-ap
#
return
```

Configuración en S3

```
#
sysname S3
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
  port link-type trunk
  port trunk pvid vlan 100
  port trunk allow-pass vlan 100 to 101
#
return
```

Configuración en S4

```
#
sysname S4
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
  port link-type trunk
  port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet0/0/4
  port link-type trunk
```



```
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 101
#
return
```

6.5 Quiz

1. En el networking actual, si GigabitEthernet0/0 /10 del AC no permite que pasen los paquetes de la VLAN 101, ¿cuál es el impacto en el acceso de las STA a la S1? - ¿Por qué? ¿Qué pasa si se utiliza el reenvío de túneles?
2. Si se deben asignar STA conectadas a AP1 y AP2 a diferentes VLAN, ¿qué operaciones se deben realizar en el CA?

6.6 Apéndice

Estado PA	Descripción
commit-failed	Las configuraciones del servicio de WiFi no se pueden entregar al punto de acceso una vez que el punto de acceso se conecta en un punto de acceso.
committing	Las configuraciones del servicio de red inalámbrica se entregan al punto de acceso una vez que el punto de acceso se conecta en un punto de acceso.
config	Las configuraciones de los servicios de red inalámbrica se envían al punto de acceso cuando el punto de acceso se conecta en un punto de acceso.
config-failed	Las configuraciones del servicio de red inalámbrica no se pueden enviar al punto de acceso cuando el punto de acceso se está conectando en un CA.
download	El punto de acceso se encuentra en estado upgrade.
fault	El punto de acceso no se conecta.
idle	Es el estado de inicialización del punto de acceso antes de establecer un enlace con el punto de acceso por primera vez.
name-conflicted	El nombre del punto de acceso entra en conflicto con el de un punto de acceso existente.
normal	El punto de acceso funciona correctamente.
standby	El PA se encuentra en estado normal en el CA standby.
unauth	El punto de acceso no se ha autenticado.



7

Creación de una red IPv6

7.1 Introducción

7.1.1 Acerca de este laboratorio

La versión 6 del protocolo de Internet también se denomina Next Generation (IPng). Diseñado por el Grupo de Trabajo de Ingeniería de Internet, el IPv6 es una versión actualizada del IPv4.

Ipv6 tiene las siguientes ventajas sobre Ipv4:

- Espacio de direcciones infinito
- Estructura jerárquica de direcciones
- Plug-and-play
- Encabezado de paquete simplificado
- Seguridad.
- Movilidad
- Funciones de calidad del servicio mejoradas

Este capítulo describe cómo configurar una red IPv6 para ayudarle a entender los principios básicos y la configuración de direcciones de IPv6.

7.1.2 Objetivos.

Una vez completada esta tarea, podrá:

- Aprenda a configurar direcciones IP v6 estáticas
- Aprenda a configurar un servidor DHCPv6
- Aprenda a configurar direcciones sin estado
- Aprenda a configurar rutas estáticas de IPv6
- Obtenga información sobre cómo ver la información de IPv6

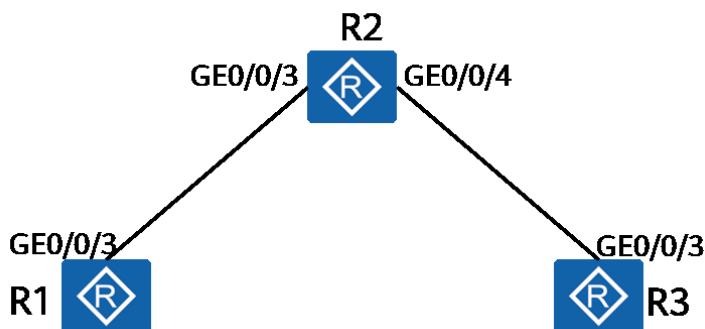
7.1.3 Topología de networking

Una empresa debe implementar IPv6 en su red.



1. Configure direcciones IP v6 estáticas para las dos interfaces de R2.
2. Configure la configuración automática de direcciones sin estado en GigabitEthernet0/0/3 de R1.
3. Configure una dirección IPv6 para GigabitEthernet0/0/3 de R3 mediante DHCPv6.

Figure 7-1 Topología de laboratorio para crear una red IPv6



7.2 Configuración de laboratorio

7.2.1 Configuración Roadmap

1. Configure direcciones IP v6 estáticas.
2. Configure DHCPv6.
3. Configure la asignación de direcciones sin estado de IPv6.
4. Mostrar direcciones IPv6.

7.2.2 Procedimiento de configuración

Step 1 Completar la configuración básica del dispositivo.

Nombra los dispositivos.

Los detalles no se proporcionan aquí.

Step 2 Configure las funciones IPv6 en los dispositivos y las interfaces.

Habilite IPv6 globalmente.

```
[R1 ]ipv6
```

El comando **ipv6** permite al dispositivo reenviar paquetes unicast IPv6, lo que incluye enviar y recibir paquetes IPv6 locales.

```
[R2]ipv6
```



```
[R3]ipv6
```

Habilite IPv6 en la interfaz.

```
[R1]interface GigabitEthernet 0/0/3
```

El comando **ipv6 enable** habilita la función ipv6 en una interfaz.

```
[R1-GigabitEthernet0/0/3]ipv6 enable  
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3  
[R2-GigabitEthernet0/0/3]ipv6 enable  
[R2-GigabitEthernet0/0/3]quit  
[R2]interface GigabitEthernet 0/0/4  
[R2-GigabitEthernet0/0/4]ipv6 enable  
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet 0/0/3  
[R3-GigabitEthernet0/0/3]ipv6 enable  
[R3-GigabitEthernet0/0/3]quit
```

Step 3 Configure una dirección local del vínculo para la interfaz y pruebe la configuración.

Configure una interfaz para generar automáticamente una dirección local del vínculo.

```
[R1]interface GigabitEthernet 0/0/3
```

El comando **ipv6 address auto link-local** permite la generación de una dirección local de vínculo para una interfaz.

Solo se puede configurar una dirección local de vínculo para cada interfaz. Para evitar conflictos de direcciones locales del vínculo, se recomiendan las direcciones locales del vínculo generadas automáticamente. Una vez configurada una dirección global unicast IPv6 para una interfaz, se generará automáticamente una dirección local de vínculo.

```
[R1-GigabitEthernet0/0/3]ipv6 address auto link-local  
[R1-GigabitEthernet0/0/3]quit
```

```
[R2]interface GigabitEthernet 0/0/3  
[R2-GigabitEthernet0/0/3]ipv6 address auto link-local  
[R2-GigabitEthernet0/0/3]quit  
[R2]interface GigabitEthernet 0/0/4  
[R2-GigabitEthernet0/0/4]ipv6 address auto link-local  
[R2-GigabitEthernet0/0/4]quit
```



```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ipv6 address auto link-local
[R3-GigabitEthernet0/0/3]quit
```

Muestra el estado IPv6 de la interfaz y prueba la conectividad.

```
< R1>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP //The physical and protocol status is Up.
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE4D:355 //The link-local address for the interface
has been generated.
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF4D:355
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/3
GigabitEthernet0/0/3 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6486
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF12:6486
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R2>display ipv6 interface GigabitEthernet 0/0/4
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE12:6487
  No global unicast address configured
  Joined group address(es):
    FF02::1:FF12:6487
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

```
<R3>display ipv6 interface GigabitEthernet 0/0/3
```

```
GigabitEthernet0/0/4 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE3C:5133
No global unicast address configured
Joined group address(es):
  FF02::1:FF3C:5133
  FF02::2
  FF02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

Pruebe la conectividad de red entre R1 y R2.

```
<R1>ping ipv6 FE80::2E0:FCFF:FE12:6486 -i GigabitEthernet 0/0/3
PING FE80::2E0:FCFF:FE12:6486 : 56 data bytes, press CTRL_C to break
  Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=1 hop limit=64 time = 90 ms
  Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=2 hop limit=64 time = 10 ms
  Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=3 hop limit=64 time = 20 ms
  Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=4 hop limit=64 time = 10 ms
  Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=5 hop limit=64 time = 30 ms

--- FE80::2E0:FCFF:FE12:6486 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
round-trip min/avg/max = 10/32/90 ms
```

Al hacer ping a una dirección local del vínculo, debe especificar la interfaz de origen o la dirección IPv6 de origen.

Step 4 Configure las direcciones IP v6 estáticas en R2.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ipv6 address 2000:0012::2 64
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ipv6 address 2000:0023::2 64
[R2-GigabitEthernet0/0/4]quit
```

Step 5 Configure la función de servidor DHCPv6 en R2 y configure R3 para obtener direcciones IPv6 a través de DHCPv6.

Configure la función de servidor DHCPv6.

```
[R2]dhcp enable
[R2]dhcpv6 pool pool1
An IPv6 address pool named pool1 is created.
[R2-dhcpv6-pool-pool1]address prefix 2000:0023::/64
The IPv6 address prefix is configured.
```



```
[R2-dhcpv6-pool-pool1]dns-server 2000:0023::2
The IP address of the DNS server is specified.
[R2-dhcpv6-pool-pool1]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]dhcpv6 server pool1
[R2-GigabitEthernet0/0/4]quit
```

Configure la función de cliente DHCPv6.

```
[R3]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ipv6 address auto dhcp
[R3-GigabitEthernet0/0/3]quit
```

Muestra la dirección del cliente y la información del servidor DNS-Server.

```
[R3]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                Physical      Protocol
GigabitEthernet0/0/3      up           up
[IPv6 Address] 2000:23::1

[R3]display dns server
Type:
D:Dynamic    S:Static
No configured ip dns servers.
No.  Type  IPv6 Address                Interface Name
1    D     2000:23::2                  -
```

GigabitEthernet0/0/3 en R3 ha obtenido una dirección global unicast de IPv6.

¿Cómo se configura el servidor DHCPv6 para asignar información de gateway a los clientes?

El servidor DHCPv6 no asigna una dirección de gateway IPv6 a un cliente.

Cuando se configura el modo con estado DHCPv6, los clientes DHCPv6 aprenden la ruta predeterminada del gateway IPv6 mediante el comando **ipv6 address auto global default**. Cuando se configura el modo sin estado DHCPv6, los clientes DHCPv6 aprenden la dirección global unicast IPv6 y la ruta predeterminada al gateway IPv6 a través de este comando. Asegúrese de que la interfaz del dispositivo equivalente conectado al dispositivo local ha sido habilitada para enviar paquetes de AR utilizando el comando **undo ipv6 nd ra halt**.

Configure el servidor DHCPv6 para asignar la dirección del gateway a los clientes.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo ipv6 nd ra halt
```

El comando **undo ipv6 nd ra halt** permite al sistema enviar paquetes de AR. Por defecto, las interfaces del router no envían paquetes de AR.

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig managed-address-flag
```

El comando **ipv6 nd autoconfig managed-address-flag** configura el flag "administrated address configuration " (M flag) en los mensajes de AR, indicando si los hosts deben usar autoconfiguration stateful para obtener direcciones. Por defecto, el indicador no se configura.

- Si se configura el indicador M, un host obtiene una dirección IPv6 a través de la configuración automática de estado.
- Si no se configura el indicador M, un host utiliza una configuración automática sin estado para obtener una dirección IPv6, es decir, el host genera una dirección IPv6 basada en la información de prefijo del paquete AR.

```
[R2-GigabitEthernet0/0/4]ipv6 nd autoconfig other-flag
```

El comando **ipv6 nd autoconfig other-flag** configura el flag "Other Configuration" (Flag O) en los mensajes RA. Por defecto, el indicador no se configura.

- Si se configura el indicador de O, un host utiliza la configuración automática con estado para obtener otros parámetros de configuración (excluida la dirección IPv6), como la vida útil del Router, el tiempo de proximidad alcanzable, el intervalo de retransmisión y la UPMT.
- Si se elimina este indicador, un host puede obtener configuraciones (excluyendo la dirección IPv6), como la vida útil del router, el tiempo de proximidad alcanzable, el intervalo de retransmisión y la PMTU en configuración automática sin estado. Esto significa que un dispositivo de enrutamiento anuncia estas configuraciones usando mensajes de AR a los hosts conectados.

```
[R2-GigabitEthernet0/0/4]quit
```

Configure el cliente para aprender la ruta predeterminada a través de mensajes de AR.

```
[R3]interface GigabitEthernet 0/0/3
```

```
[R3-GigabitEthernet0/0/3] ipv6 address auto global default
```

Muestra las rutas de R3.

```
[R3]display ipv6 routing-table
```

Routing Table : Public

Destinations : 4

Routes : 4

Destination	: ::	PrefixLength	: 0
NextHop	: FE80::A2F4:79FF:FE5A:CDAE	Preference	: 64
Cost	: 0	Protocol	: Unr
RelayNextHop	: ::	TunnelID	: 0x0
Interface	: GigabitEthernet0/0/3	Flags	: D
Destination	: ::1	PrefixLength	: 128
NextHop	: ::1	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	: ::	TunnelID	: 0x0
Interface	: InLoopBack0	Flags	: D



Destination	: 2000:23::1	PrefixLength	: 128
NextHop	: ::1	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	: ::	TunnelID	: 0x0
Interface	: GigabitEthernet0/0/3	Flags	: D
Destination	: FE80::	PrefixLength	: 10
NextHop	: ::	Preference	: 0
Cost	: 0	Protocol	: Direct
RelayNextHop	: ::	TunnelID	: 0x0
Interface	: NULL0	Flags	: D

Step 6 Configure R1 para obtener una dirección IPv6 en modo sin estado.

Habilite la AR en GigabitEthernet0/0/3 de R2.

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]undo ipv6 nd ra halt
```

Enable stateless address autoconfiguration on GigabitEthernet0/0/3 of R1.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3] ipv6 address auto global
```

Muestra la configuración de la dirección IP de R1.

```
[R1]display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
```

Interface	Physical	Protocol
GigabitEthernet0/0/3	up	up

```
[IPv6 Address] 2000:12::2E0:FCFF:FE4D:355
```

GigabitEthernet0/0/3 genera una dirección global unicast de Ipv6 basada en el prefijo de dirección Ipv6 obtenido del mensaje de AR enviado por Ipv2 y el identificador de interfaz generado localmente.

Step 7 Configure una ruta estática IPv6.

Configure una ruta estática en la R1 para habilitar la conectividad entre GigabitEthernet0/0/3 en la R1 y GigabitEthernet0/0/3 en la R3.

```
[R1]ipv6 route-static 2000:23:: 64 2000:12::2
```

Info: The destination address and mask of the configured static route mismatched, and the static route 2000:23::/64 was generated.

Probar conectividad.

```
[R1]ping ipv6 2000:23::1
PING 2000:23::1 : 56 data bytes, press CTRL_C to break
Reply from 2000:23::1
bytes=56 Sequence=1 hop limit=63 time = 20 ms
Reply from 2000:23::1
bytes=56 Sequence=2 hop limit=63 time = 20 ms
Reply from 2000:23::1
bytes=56 Sequence=3 hop limit=63 time = 30 ms
Reply from 2000:23::1
```



```
bytes=56 Sequence=4 hop limit=63  time = 20 ms
Reply from 2000:23::1
bytes=56 Sequence=5 hop limit=63  time = 30 ms

--- 2000:23::1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 20/24/30 ms
```

R1 tiene una ruta estática a la red de 2000 : 23 : : /64. Obtiene la ruta predeterminada a través de DHCPv6. Por lo tanto, GigabitEthernet0/0/3 en R1 y GigabitEthernet0/0/3 en R3 pueden comunicarse entre sí.

Muestra la información de vecinos IPv6.

```
[R1]display ipv6 neighbors
-----
IPv6 Address   : 2000:12::2
Link-layer     : 00e0-fc12-6486          State      : STALE
Interface      : GE0/0/3                  Age        : 8
VLAN           : -                       CEVLAN     : -
VPN name       :                         Is Router   : TRUE
Secure FLAG    : UN-SECURE

IPv6 Address   : FE80::2E0:FCFF:FE12:6486
Link-layer     : 00e0-fc12-6486          State      : STALE
Interface      : GE0/0/3                  Age        : 8
VLAN           : -                       CEVLAN     : -
VPN name       :                         Is Router   : TRUE
Secure FLAG    : UN-SECURE
-----
Total: 2        Dynamic: 2        Static: 0
```

----Fin

7.3 Verificación

Los detalles no se proporcionan aquí.

7.4 Referencia de configuración

Configuración en R1

```
#
sysname R1
#
ipv6
#
interface GigabitEthernet0/0/3
```




```
ipv6 enable
ipv6 address auto link-local
ipv6 address auto global
#
ipv6 route-static 2000:23:: 64 2000:12::2
#
return
```

Configuración en R2

```
#
sysname R2
#
ipv6
#
dhcp enable
#
dhcpv6 pool pool1
address prefix 2000:23::/64
dns-server 2000:23::2
#
interface GigabitEthernet0/0/3
ipv6 enable
ipv6 address 2000:12::2/64
ipv6 address auto link-local
undo ipv6 nd ra halt
interface GigabitEthernet0/0/4
#
ipv6 enable
ipv6 address 2000:23::2/64
ipv6 address auto link-local
undo ipv6 nd ra halt
ipv6 nd autoconfig managed-address-flag
dhcpv6 server pool1
#
return
```

Configuración en R3

```
#
sysname R3
#
ipv6
#
dhcp enable
#
interface GigabitEthernet0/0/3
ipv6 enable
ipv6 address auto link-local
ipv6 address auto global default
ipv6 address auto dhcp
#
return
```



7.5 Quiz

1. ¿Por qué se debe especificar la interfaz de origen en el Paso 3 (probar la conectividad entre las direcciones locales del vínculo) pero no en el Paso 7 (probar la conectividad entre las direcciones GUA)?
2. Describa la diferencia entre la configuración de direcciones con estado y la configuración de direcciones sin estado y explique por qué.



8

Conceptos básicos de programación y automatización de redes

8.1 Introducción

8.1.1 Acerca de este laboratorio

Después de completar esta actividad de laboratorio, podrá aprender a usar el telnetlib de Python.

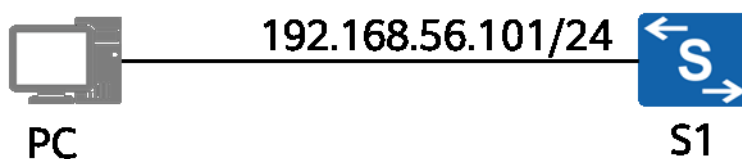
8.1.2 Objetivos.

- Aprenda la sintaxis básica de Python
- Aprenda a usar telnetlib

8.1.3 Topología de networking

Una empresa tiene un switch cuya dirección IP de gestión es 192.168.56.101/24. Es necesario escribir un script de automatización para ver el archivo de configuración actual del dispositivo.

Figure 8-1 Topología de laboratorio para la programación y automatización de redes





8.2 Configuración de laboratorio

8.2.1 Configuración Roadmap

1. Configure Telnet: configure la contraseña Telnet, habilite Telnet y permita el acceso Telnet.
2. Compilar un script Python: Invocar telnetlib para iniciar sesión en el dispositivo y comprobar la configuración.

8.2.2 Procedimiento de configuración

Step 1 Configure Telnet en el switch.

Cree una contraseña de inicio de sesión Telnet.

```
[Huawei]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode password
[Huawei -ui-vty0-4]set authentication password simply Huawei wed@123
[Huawei-ui-vty0-4]protocol inbound telnet
[Huawei-ui-vty0-4]user privilege level 15
```

Antes de utilizar un script en Python para iniciar sesión en un dispositivo a través de Telnet, se debe crear una contraseña Telnet y habilitar la función Telnet en el dispositivo. Configure la contraseña de inicio de sesión Telnet como **Huawei@123**.

Habilite el servicio Telnet para permitir el acceso Telnet.

```
[Huawei]telnet server enable
Info: The Telnet server has been enabled.
```

Telnet al switch desde el ordenador usando la interfaz de comandos.

```
C:\Users\XXX>telnet 192.168.56.101
Login authentication

Password:
Info: The max number of VTY users is 5, and the number of current VTY users on line is 1.
The current login time is 2020-01-15 21:12:57.
<Huawei>
```

La configuración de Telnet se realizó con éxito.

Step 2 Escribe el código de Python.

```
import telnetlib
import time

host = '192.168.56.101'
password = 'Huawei@123'

tn = telnetlib.Telnet(host)

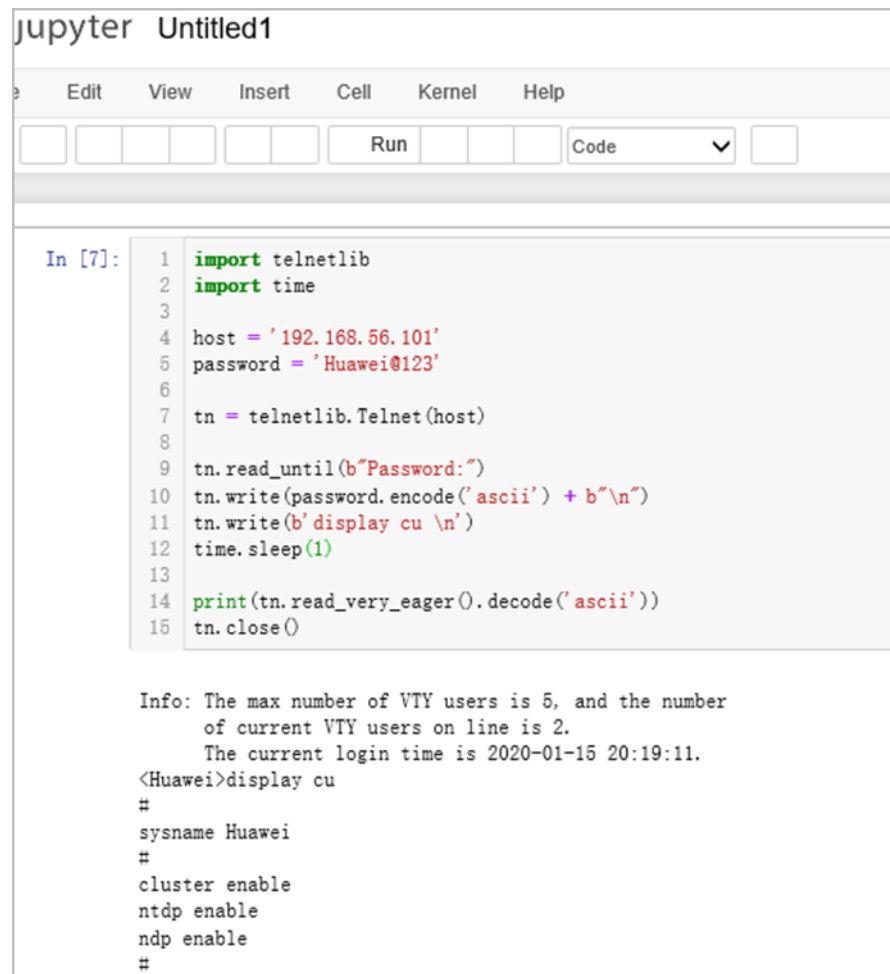
tn.read_until(b"Password:")
tn.write(password.encode('ascii') + b"\n")
tn.write(b'display cu \n')
```

```
time.sleep(1)

print(tn.read_very_eager().decode('ascii'))
tn.close()
```

El script Python invoca al módulo telnetlib para iniciar sesión en S1, ejecuta el comando **display current-configuration** y muestra la salida del comando.

Step 3 Ejecutar el compilador:



The screenshot shows a Jupyter Notebook interface with a menu bar (Edit, View, Insert, Cell, Kernel, Help) and a toolbar with buttons for running and saving cells. The code cell contains a Python script that uses telnetlib to connect to a device at 192.168.56.101 with the password Huawei@123. After a one-second delay, it prints the output of the 'display current-configuration' command. The output shows the device name 'Huawei' and the configuration for the cluster, including 'cluster enable', 'ntdp enable', and 'ndp enable'.

```
In [7]: 1 import telnetlib
        2 import time
        3
        4 host = '192.168.56.101'
        5 password = 'Huawei@123'
        6
        7 tn = telnetlib.Telnet(host)
        8
        9 tn.read_until(b"Password:")
       10 tn.write(password.encode('ascii') + b"\n")
       11 tn.write(b'display cu \n')
       12 time.sleep(1)
       13
       14 print(tn.read_very_eager().decode('ascii'))
       15 tn.close()

Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 2.
      The current login time is 2020-01-15 20:19:11.
<Huawei>display cu
#
sysname Huawei
#
cluster enable
ntdp enable
ndp enable
#
```

El compilador usado en este ambiente de laboratorio es el Cuaderno de Jupyter. También puede utilizar otros compiladores.

Step 4 La salida es la siguiente:

```
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 2.
      The current login time is 2020-01-15 20:19:11.
<Huawei>display cu
#
sysname Huawei
#
cluster enable
```

```
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
 ip address 192.168.56.101 255.255.255.0
 ---- More ----
```

----Fin

8.2.3 Interpretación del código

Step 1 Importe el módulo.

```
import telnetlib
import time
```

Importar los módulos telnetlib y time. Los dos módulos son proporcionados por Python y no necesitan ser instalados.

Esta sección describe las clases y métodos comunes del Telnetlib como cliente, por ejemplo, los métodos read _ until, read _ very_eager(), y write() en la clase Telnet. Para obtener más métodos Telnet, consulte el documento oficial de telnetlib en <https://docs.python.org/3/library/telnetlib.html#telnet-example>.

De forma predeterminada, Python ejecuta todo el código en secuencia sin intervalos. Cuando se utiliza Telnet para enviar comandos de configuración a un switch, es posible que el switch no responda a tiempo o que la salida del comando esté incompleta. En este caso, puede utilizar el método sleep en el módulo time para pausar manualmente el programa.

Step 2 Inicie sesión en el dispositivo.

Invocar múltiples métodos de la clase Telnet en telnetlib para iniciar sesión en S1.

```
Host = '192.168.56.101'
password ='Huawei @ 123'
tn = telnetlib.Telnet (host)
```

Cree dos variables. host y password son la dirección de inicio de sesión y la contraseña del dispositivo respectivamente, que son las mismas que las configuradas en el dispositivo. En este ejemplo, solo se configura la contraseña Telnet para iniciar sesión. Por lo tanto, no se requiere un nombre de usuario.

telnetlib.Telnet () indica que se invoca el método Telnet () de la clase telnetlib. Este método contiene los parámetros de inicio de sesión, incluyendo la dirección IP y el número de puerto. Si no se introduce información sobre el puerto, se utiliza el puerto 23 por defecto.

En este ejemplo, tn = telnetlib.Telnet (host) indica que se debe iniciar sesión en el dispositivo cuyo host es 192.168.56.101 y asignar el valor de telnetlib.Telnet (host) a tn.

```
tn.read_until(b"password:")
```

Cuando se inicia sesión en el dispositivo en 192.168.56.101 a través de Telnet, aparece la siguiente información:

```
<TelnetClient>telnet 192.168.56.101
Trying 192.168.56.101 ...
Press CTRL+K to abort
Connected to 192.168.56.101 ...
```

```
Login authentication
```

```
Password:
```

Tenga en cuenta que el programa no sabe qué información necesita ser leída. Por lo tanto, read_until() es usado para indicar que la información entre paréntesis debe ser leída.

En este ejemplo, tn.read _ until (b"Password:") indica que los datos se leen hasta que aparezca "Password:". La letra "b" antes de "Password:" indica que el código Unicode por defecto en Python3 se cambia a bytes. Este es el requerimiento de la función en los datos de entrada. Para obtener más detalles, consulte el documento oficial de telnetlib. Si este parámetro no se transporta, el programa informa de un error.

```
tn.write(password.encode('ascii') + b"\n")
```

Después de que aparezca Password: en el código, el programa introduce la contraseña. Este parámetro ha sido definido y se utiliza como contraseña de inicio de sesión Telnet. Use write () para escribir la contraseña.

En este ejemplo, tn.write (password.encode ('ascii ') + b "\n ") consta de dos partes: password.encode ("ascii") y b "\n ". password.encode ('ascii ') indica que el tipo de codificación de la cadena de caracteres Huawei@123 representada por contraseña es ASCII. "+" indica que las cadenas de caracteres antes y después del símbolo se concatenarán. \n es un carácter de nueva línea, que equivale a pulsar

Intro. Por lo tanto, el código en esta línea es equivalente a ingresar la contraseña de Huawei@123 y presionar Enter.

Step 3 Emitir comandos de configuración.

Después de iniciar sesión en el dispositivo a través de Telnet, utilice el script Python para emitir comandos en el dispositivo.

```
tn.write(b 'display cu\n')
```

`write ()` se utiliza para introducir comandos en el dispositivo. El comando `display cu` es la forma abreviada del comando `display current-configuration`, que muestra la configuración actual del dispositivo.

```
time.sleep(1)
```

`time.sleep (1)` se utiliza para pausar el programa durante un segundo para esperar la salida del switch antes de ejecutar el código siguiente. Si no se especifica el tiempo de espera, el programa ejecuta directamente la siguiente línea de código. Como resultado, no se pueden leer datos.

```
print(tn.read_very_eager().decode('ascii'))
```

`print ()` indica que el contenido de los corchetes se muestra en la consola.

`tn.read_very_eager()` indica leer tantos datos como sea posible.

`. decode('ascii'))` indica que los datos leídos se decodifican a ASCII.

En este ejemplo, el código se utiliza para mostrar la salida de S1 en un segundo en la consola después de ejecutar el comando **display cu**.

Step 4 Cierre la sesión.

```
tn.close ()
```

La sesión se cierra invocando `close ()`. La cantidad de conexiones VTY en el dispositivo es limitada. Por lo tanto, se debe cerrar la sesión Telnet después de ejecutar el script.

----Fin

8.3 Verificación

Los detalles no se proporcionan aquí.

8.4 Referencia de configuración

Los detalles no se proporcionan aquí.



8.5 Quiz

1. ¿Cómo se usa telnetlib para configurar un dispositivo, por ejemplo, la dirección IP de la interfaz de gestión del dispositivo?
2. ¿Cómo se guarda el archivo de configuración en un directorio local?



9 Configuración de una red de campus

9.1 Información de referencia

Los comandos y las referencias que se muestran en este documento son sólo de referencia. Los comandos y referencias correctos están sujetos a su modelo y versión del producto.

Referencias:

1. Documentación de productos AR600 y AR6000
2. Documentación de productos de switches Ethernet de la serie S2720, S5700 y S6700
3. Documentación del producto Controlador de acceso inalámbrico (CA y Fit AP)
4. Arquitecturas y prácticas típicas de redes de campus

Enlaces de referencia:

1. <http://support.huawei.com/>
2. <http://e.huawei.com/>

9.2 Introducción

9.2.1 Acerca de este laboratorio

Las redes de comunicación son ubicuas en la sociedad de la información, y las redes de campus son siempre una parte fundamental. Los campus están en todas partes, incluyendo fábricas, edificios e instalaciones gubernamentales, centros comerciales, edificios de oficinas, campus escolares y parques. Según las estadísticas, el 90 % de los residentes urbanos trabaja y vive en campus, el 80 % del producto interno bruto (PIB) se crea en campus, y cada persona permanece en campus durante 18 horas al día. Las redes de campus, como infraestructura para que los campus se conecten al mundo digital, son una parte indispensable de la construcción de campus y desempeñan un papel cada vez más importante en el trabajo diario, R&D, la producción y la gestión de operaciones.

En esta actividad de laboratorio, creará una red de campus para entender las tecnologías comunes y sus aplicaciones en las redes de campus.



9.2.2 Objetivos.

Una vez completada esta tarea, podrá:

- Comprender los conceptos y la arquitectura comunes de la red de campus.
- Comprender las tecnologías de red comunes
- Comprender el ciclo de vida de las redes de campus
- Estar familiarizado con la planificación y el diseño de redes de campus, la implementación y la implementación, la operación y el mantenimiento de redes y la optimización de redes.
- Conocer el proceso de implementación de un proyecto de red de campus

9.2.3 Topología de networking

Es necesario construir una red en un edificio de oficinas. El edificio de oficinas tiene seis pisos. En la actualidad, se han puesto en funcionamiento tres plantas: la sala de recepción de la primera planta, el departamento administrativo y la oficina del director general de la segunda planta, el departamento de R&D marketing de la tercera planta. La sala de equipos principal se implementa en el primer piso y una pequeña sala se implementa en cada una de las otras plantas para alojar los dispositivos de red.

Establecer un equipo de proyecto para completar la construcción de la red.

9.3 Tareas de laboratorio

9.3.1 Recolección y análisis de requerimientos

¿Qué información debe obtenerse de la empresa? Enumere al menos cinco elementos.

Ejemplo: Número de terminales que se conectarán a la red empresarial.

1. _____
2. _____
3. _____
4. _____
5. _____



Analizar los requerimientos recolectados.

1. Presupuesto del Proyecto

El presupuesto es ajustado. Los requisitos deben aplicarse a un coste mínimo.

2. Tipos de terminales a conectar

Se instalarán terminales alámbricos e inalámbricos.

3. Cantidad de terminales

Primer piso: 10 terminales alámbricas y 100 terminales inalámbricas Segundo y tercer piso: 200 terminales alámbricas y 50 terminales inalámbricas

4. Modo de gestión de red

SNMP se utiliza para la gestión unificada de redes.

5. Volumen y tendencia del tráfico de red

La mayor parte del tráfico es interno. Se requiere acceso por cable de / de 100 Mbit. No hay otros requisitos especiales.

6. Requerimientos de Disponibilidad

La red de Capa 3 necesita algunas capacidades de redundancia y failover.

7. Requerimientos de Seguridad

Se debe controlar el tráfico de la red.

8. Modo de acceso a Internet

Los dispositivos de salida de la red del campus utilizan direcciones IP estáticas para conectarse a Internet.

9. Requerimientos de Expansión de Red

Cuando se pongan en uso otros pisos, no debería ser necesario reemplazar los dispositivos existentes.



9.3.2 Planificación y diseño

Task 1. Selección de dispositivos y diseño de topología física (opcional)

Antecedentes:

La siguiente tabla enumera la cantidad total de terminales de la red.

Piso	Primer Piso	Segundo Piso	Tercer piso	Otros pisos (Reservado)
Terminales cableados	10.	200.	200.	500.
Terminales inalámbricos	100.	50.	50.	200.
Observaciones:	Terminales inalámbricos de invitado + servidores	Ordenadores + teléfonos móviles		

El tráfico de los terminales inalámbricos es el tráfico de acceso a Internet. Cada cliente tiene una velocidad de 2 Mbit/s.

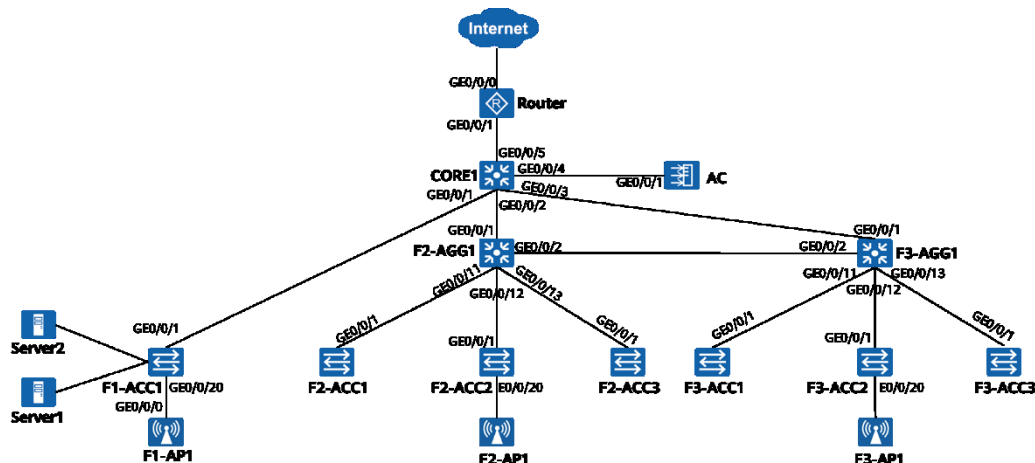
Asegúrese de que los equipos tienen una velocidad de 100 Mbit/s y los servidores tienen una velocidad de 1000 Mbit/s.

Para mejorar la calidad del acceso inalámbrico, se requieren al menos tres AP de doble banda en cada piso.

Tarea:

Diseñe la topología física de la red en la secuencia de la capa de acceso, la capa de agregación, la capa de core y el área de egreso y seleccione los dispositivos en consecuencia.

Respuesta de referencia:



Los números de interfaz del dispositivo son los siguientes:

Dispositivo	Interfaces
F2-ACC1, F2-ACC2, F2-ACC3, F3-ACC1, F3-ACC2 y F3-ACC3	E0/0/1~E0/0/222 GE0/0/1~GE0/0/2
F1-ACC1, F2-AG1, F3-AGG1 y CORE1	GE0/0/1~GE0/0/24
CA	GE0/0/1~GE0/0/8
F1-AP1, F2-AP1 y F3-AP1	GE0/0/0~GE0/0/1
Router	GE0/0/0~GE0/0/2

Las *Prácticas en proyectos de red de campus* en el manual de certificación de HCIA-Datacom detalla el diseño de la red y el proceso de diseño de topología basado en los requisitos anteriores. Esta parte se omite en este documento. En la red real, hay un gran número de switches de acceso y APs. Con el fin de simplificar el networking y facilitar las pruebas posteriores, en este documento se utiliza una topología de red simplificada.

Task 2. Diseño de red de capa 2

Antecedentes:

- Creación de VLAN en la red cableada:
 - Los puertos de conmutador de acceso GE0/0/1 a GE0/0/10 en la sala de equipos core se conectan a los servidores y se asignan a la misma VLAN.
 - En el segundo piso, F2-ACC2 está conectado a la oficina del gerente general y otros interruptores están conectados al departamento administrativo. Los dos departamentos pertenecen a diferentes VLAN.



- En la tercera planta, E0/0/1 a E0/0/10 de F3-ACC1 y F3-ACC3 pertenecen al departamento de marketing, y E0/0/11 a E0/0/20 pertenecen al departamento de R&D.
- E0/0/1 a E0/0/19 de F3-ACC2 pertenecen al departamento de marketing.
- Creación de VLAN en la red inalámbrica:
 - Los terminales inalámbricos en diferentes pisos deben ser asignados a diferentes VLAN.
 - La VLAN de gestión de red inalámbrica de cada piso es diferente.



Se deben reservar las VLAN de interconexión de dispositivos y las VLAN de gestión de dispositivos.

Tapa:

Rellenar la tabla de planificación de la red de capa 2 de acuerdo a la información y requerimientos existentes.

ID de VLAN	Descripción
Ejemplo: 1	VLAN de gestión de dispositivos de capa 2



ID de VLAN	Descripción

Respuesta de referencia:

ID de VLAN	Descripción
1	VLAN de gestión de dispositivos de capa 2 en la primera planta
2	VLAN de gestión de dispositivos de capa 2 en la segunda planta
3	VLAN de gestión de dispositivos de capa 2 en la tercera planta
100	VLAN para servidores
101	VLAN para la Oficina del Gerente General
102	VLAN para el Departamento Administrativo
103	VLAN para el Departamento de Marketing
104	VLAN para el Departamento de I+D
105	VLAN para terminales inalámbricas en la primera planta
106	VLAN para terminales inalámbricas en la segunda planta
107	VLAN para terminales inalámbricas en la tercera planta
213	Vlan para la interconexión entre F2-AG1 y CORE1
202.	Vlan para la interconexión entre F3-AG1 y CORE1
203.	Vlan para la interconexión entre F2-AG1 y F3-AG1
204	VLANS para la interconexión entre el CORE1 y el router
205.	VLANS de gestión de red inalámbrica en la primera planta
206.	Vlan de gestión de red inalámbrica en el segundo piso
207.	Vlan de gestión de red inalámbrica en el tercer piso

Task 3. Diseño de red de capa 3

Antecedentes:

- El rango de direcciones es la red 192.168.0.0/16. Las necesidades son las siguientes:

- Primer piso:
 - Los servidores utilizan IPs estáticas. Las direcciones IP de las estaciones inalámbricas y los AP son asignadas por el CORE1 a través del DHCP. El portal está en CORE1.
 - Las IPs de gestión de los switches de acceso son IPs estáticas y el gateway está en CORE1.
- Segundo y tercer piso:
 - Las direcciones IP de todos los terminales alámbricos, los terminales inalámbricos y los AP inalámbricos son asignados por el switch de agregación del piso o pisos correspondientes a través de DHCP. El gateway se implementa en los switches de agregación.
 - Las direcciones IP de gestión de los switches de acceso son direcciones IP estáticas, y el gateway se encuentra en el switch de agregación de la planta correspondiente(s).
- Se utiliza en toda la red para permitir la conectividad entre las redes de servicio. Todos los terminales acceden a Internet a través del router.

Tarea:

Rellene la tabla de planificación de red de Capa 3 según la información y los requerimientos existentes.

Red IP	Método de asignación de direcciones y gateway	Modo de enrutamiento	Descripción de la Red
192.168.1.0/24	DHCP; 192.168.1.254	OSPF	Red de gestión de dispositivos de capa 2



Red IP	Método de asignación de direcciones y gateway	Modo de enrutamiento	Descripción de la Red

Respuesta de referencia:

Red Ip	Método de asignación de direcciones y gateway	Configuración de enrutamiento	Descripción de la Red
192.168.1 .0/ 24	Direcciones estáticas; CORE1	Ruta predeterminada que apunta al CORE1	Red de gestión de dispositivos de capa 2 en la primera planta
192.168.2 .0/ 24	Direcciones estáticas; F2-AG1	Ruta predeterminada que apunta a F2-AGG1	Red de gestión de dispositivos de capa 2 en la segunda planta
192.168.3 .0/ 24	Direcciones estáticas; F3-AGG	Ruta predeterminada que apunta a F3-AGG	Red de gestión de dispositivos de capa 2 en el tercer piso
192.168.1 00.0/ 24	Direcciones estáticas; CORE1	Anunciado en OSPF a través de dispositivos gateway	Red de servidores
192.168.1 01.0/ 24	Asignado por F2-AG1 a través de DHCP; F2-AG1		Red de la Gerencia General
192.168.1 02.0 /24			Red del Departamento Administrativo
192.168.1 03.0/ 24	Asignado por F3-AGG1 a través de DHCP; F3-AGG1		Red del Departamento de Marketing
192.168.1 04.0/ 24			Red del departamento de I&D



Red Ip	Método de asignación de direcciones y gateway	Configuración de enrutamiento	Descripción de la Red
192.168.1 05.0/ 24	Asignado por el CORE1 a través del DHCP; CORE1		Red de terminales inalámbricos en la primera planta
192.168.1 06.0/ 24	Asignado por F2-AG1 a través de DHCP; F2-AG1		Red de terminales inalámbricos en la segunda planta
192.168.1 07.0/ 24	Asignado por F3-AGG1 a través de DHCP; F3-AGG1		Red de terminales inalámbricos en el tercer piso
192.168.2 01.0/ 30	Direcciones estáticas; no se necesita gateway	OSPF está habilitado, se establece la relación con los vecinos, y la ruta predeterminada es anunciada por el router	Red para la interconexión entre F2-AGG1 y CORE1
192.168.2 02.0/30			Red para la interconexión entre F3-AGG1 y CORE1
192.168.2 03.0/30			Red para la interconexión entre F2-AGG1 y F3-AGG1
192.168.2 04.0/30			Red para la interconexión entre el CORE1 y el router
192.168.2 05.0/24	Asignado por CORE1 a través de DHCP; CORE1	Advertida en OSPF a través de dispositivos de gateway	Red de gestión de red inalámbrica en la primera planta
192.168.2 06.0/24	Asignado por F2-AGG1 a través de DHCP; F2-AGG1		Red de gestión de red inalámbrica en la segunda planta
192.168.2 07.0/24	Asignado por F3-AGG1 a través de DHCP; F3-AGG1		Red de gestión de red inalámbrica en la tercera planta

Task 4. Diseño de WLAN

Antecedentes:

- Todos los AP son gestionados por el AC de manera unificada, y el AC tiene un rendimiento de reenvío limitado.

- Los AP en la primera planta se registran en la capa 2.
- Todos los AP en la segunda y tercera planta se registran con el AC en la capa 3. La gateway del AC es CORE1.
- Crear un SSID para cada piso.
 - Se utiliza la política de seguridad WPA-WPA2+PSK+AES.
 - Cada piso tiene un SSID y una contraseña diferentes.

Tarea:

Rellenar la tabla de planificación de la red WLAN basándose en la información y los requerimientos existentes.

Elemento	WLAN en la primera planta	WLAN en la segunda planta	WLAN en la tercera planta
VLAN de gestión de AP			
VLAN de servicio			
Servidor DHCP			
Dirección IP de la interfaz de origen del AC			
Grupo de puntos de acceso			
Perfil de dominio regulatorio			
Perfil SSID			
Perfil de seguridad			
VAP perfil			
Otras configuraciones			

Respuesta de referencia:

Elemento	WLAN en la primera planta	WLAN en la segunda planta	WLAN en la tercera planta
VLAN de gestión de AP	VLAN 205	VLAN 206	VLAN 207
VLAN Servicio	VLAN105	VLAN106	VLAN107
Servidor DHCP	El CORE1 asigna direcciones IP a los AP y las STA.	F2-AG1 asigna IPs a AP y STA.	F3-AG1 asigna IPs a AP y STA.



Dirección IP de la interfaz de la Fuente de la CA	VLANIF205:192.168.205.253/24		
Grupo de puntos de acceso	Nombre: perfil WLAN-F1VAP: WLAN-F1 Perfil de dominio regulatorio: predeterminado	Nombre: perfil WLAN-F2VAP: WLAN-F2 Perfil de dominio regulatorio: predeterminado	Nombre: perfil WLAN-F3VAP: WLAN-F3 Perfil de dominio regulatorio: predeterminado
Perfil de dominio regulatorio	Nombre: default Código de país: CN		
Perfil de SSID	Nombre: WLAN-F1 SSID Nombre: WLAN-F1	Nombre del perfil: WLAN-F2 Nombre del SSID: WLAN-F2	Nombre del perfil: WLAN-F3 Nombre del SSID: WLAN-F3
Perfil de seguridad	Nombre: WLAN-F1 Política de seguridad: WPA-WPA2+PSK+AES Password: WLAN@Guest123	Nombre: WLAN-F2 Política de seguridad: WPA-WPA2+PSK+AES Paspota: WLAN@Employee2	Nombre: WLAN-F3 Política de seguridad: WPA-WPA2+PSK+AES sword: WLAN@Employee3
VAP perfil	Nombre:WLAN-F1 Modo de reenvío: reenvío directo Servicio VLAN: VLAN: 105 Perfiles: Perfil SSID: WLAN-F1; Perfil de seguridad: WLAN-F1	Nombre: WLAN-F2 Modo de reenvío Reenvío directo Servicio VLAN: 106 Perfiles: Perfil SSID: WLAN-F2 Perfil de seguridad: WLAN-F2	Nombre: WLAN-F3 Modo de reenvío: Reenvío directo Servicio VLAN: VLAN: 107 Perfiles: Perfil SSID: WLAN-F3 Perfil de seguridad: WLAN-F3

Task 5. Diseño de seguridad y salida

Antecedentes:

- El SSID invitado no puede acceder a la intranet de la empresa.

- Solo los terminales inalámbricos pueden acceder a Internet.
- El router utiliza una dirección IP estática para acceder a Internet. El operador asigna direcciones IP 1.1.1.1.1.10 (con una máscara de 24 bits) al router. La dirección IP del siguiente salto para el router para acceder a Internet es 1.1.1.254.
- Un servidor web en la empresa debe proporcionar servicios a usuarios externos. La dirección IP privada del servidor web es 192.168.100.1 y el número de puerto es 80. Con el fin de garantizar la seguridad de los servidores, el mapeo NAT se proporciona únicamente para los servicios web.

Tareas:

Rellene la tabla de planificación de seguridad y egreso según la información y los requisitos existentes.

Requerimiento	Aplicación

Respuesta de referencia:

Requerimiento	Aplicación
Control de acceso a intranet aplicable a invitados	Configure un filtro de tráfico o una política de tráfico en el CORE1.
Control de acceso a Internet	Configure NAT en el router y deshabilite la traducción de direcciones para las redes especificadas.
Mapeo de servidores Web	Configure el servidor NAT en la interfaz del router.

Task 6. Diseño de gestión de red**Antecedentes:**

- El SNMPv3 se utiliza para comunicarse con el sistema de gestión de red y la autenticación y el cifrado se configuran para mejorar la seguridad.
- Todos los dispositivos, excepto el router y el CA, se comunican con el sistema de gestión de red en 192.168.100.2 /24 a través de la VLAN de gestión.

- Los routers se comunican con el sistema de gestión de red a través de la interfaz de usuario 0/0/1.
- El CA se comunica con el sistema de gestión de red a través de la VLANIF 205.
- Todos los dispositivos deben poder reportar alarmas SNMP al NMS.

Tarea:

De acuerdo con los requerimientos anteriores, se deben optimizar las configuraciones de los dispositivos en la fase de despliegue e implementación.

9.3.3 Aplicación

Task 1. Esquema de configuración

Rellenar el esquema de configuración para cada equipo de acuerdo al esquema de planificación y diseño.

Router:

Elemento	Configuración
Configuración básica	
Configuración de direcciones Ip	
OSPF	
Configuración de salida	
configuración SNMP	
Otras configuraciones	

Nucleo 1

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de interfaz VLANIF	
Configuración OSPF	
configuración DHCP	
Control de acceso	
configuración SNMP	



Otras configuraciones	
-----------------------	--

F2-AGG1:

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de VLANs en interfaces	
Configuración de la interfaz VLANIF	
Configuración de OSPF	
Configuración DHCP	
Configuración SNMP	
Otras configuraciones	

F3-AGG1:

Elemento	Configuración
Configuración básica	
Configuración de VLAN	
Configuración de VLAN en interfaces	
Configuración de la interfaz VLANIF	
Configuración de OSPF	
Configuración DHCP	
Configuración SNMP	
Otras configuraciones	

AC:

Elemento	Configuración
Configuración básica	
Configuración de la red cableada	



Elemento	Configuración
Configuración de la red inalámbrica	
Configuración SNMP	
Otras configuraciones	

F1-ACC1:

Elemento	Configuración
Configuración básica	
Configuración de VLAN	
Configuración de la interfaz VLANIF	
Configuración de enrutamiento	
Configuración SNMP	
Otras configuraciones	

F2-ACC1:

Elemento	Configuración
Configuración básica	
Configuración de VLAN	
Configuración de la interfaz VLANIF	
Configuración de enrutamiento	
Configuración SNMP	
Otras configuraciones	

F2-ACC2:

Elemento	Configuración
Configuración básica	
Configuración de VLAN	
Configuración de la interfaz VLANIF	



Elemento	Configuración
Configuración de enrutamiento	
Configuración SNMP	
Otras configuraciones	

F2-ACC3:

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de interfaz VLANIF	
Configuración de enrutamiento	
configuración SNMP	
Otras configuraciones	

F3-ACC1:

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de interfaz VLANIF	
Configuración de enrutamiento	
configuración SNMP	
Otras configuraciones	

F3-ACC2:

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de interfaz VLANIF	



Elemento	Configuración
Configuración de enrutamiento	
configuración SNMP	
Otras configuraciones	

F3-ACC3:

Elemento	Configuración
Configuración básica	
Configuración de VLANs	
Configuración de interfaz VLANIF	
Configuración de enrutamiento	
configuración SNMP	
Otras configuraciones	

Configuración

Configure el entorno del laboratorio y las configuraciones correspondientes de acuerdo con los esquemas de configuración anteriores en un plazo de 40 minutos.

Task 2. Aceptación del proyecto

Una vez finalizada la configuración del dispositivo, ¿qué elementos se deben verificar para la aceptación? ¿Cómo se verifican? Enumere al menos cinco elementos.

1. _____
2. _____
3. _____
4. _____
5. _____

Respuesta de referencia:

1. Verificar que los clientes inalámbricos puedan detectar señales inalámbricas y acceder a la red en forma exitosa.
2. Verifique si la relación de vecinos OSPF es normal.

3. Verificar la conectividad dentro de las redes.
4. Verificar la conectividad entre redes.
5. Verificar el control de acceso para los invitados inalámbricos.
6. Verificar el control de acceso a Internet.
7. Verificar si el NMS puede gestionar dispositivos de red.

9.3.4 Operación y mantenimiento de la red

Task 1. Transferencia de O&M

Una vez entregado el proyecto, ¿cómo se organiza el trabajo de mantenimiento en el futuro? Discutir con su equipo y enumerar al menos cinco elementos de mantenimiento.

1. _____
2. _____
3. _____
4. _____

Respuesta de referencia:

Intervalo de mantenimiento recomendado	Verificar el elemento	Método de verificación	Criterios de evaluación
Diariamente	Conexiones de energía	Observaciones	El cable de alimentación se conecta correctamente y de forma segura a la posición especificada del dispositivo. El indicador de alimentación del dispositivo debe estar constante en (verde).
	Temperatura del dispositivo	Temperatura de pantalla <HUAWEI>	La temperatura de cada módulo se sitúa entre el límite superior y el límite inferior.
	Información de alarmas	<HUAWEI> alarma de pantalla urgente	Se registran las alarmas y se analizan y procesan inmediatamente las alarmas mayores o más graves.



Intervalo de mantenimiento recomendado	Verificar el elemento	Método de verificación	Criterios de evaluación
	Uso de la CPU	<HUAWEI> display cpu-use	El uso de la CPU de cada módulo es normal. Si el uso de la CPU supera el 80% con frecuencia o persistentemente, se requiere una atención adecuada.
	Uso de la memoria	<HUAWEI> uso de la memoria de pantalla	El uso de la memoria es normal. Si el valor de Porcentaje de uso de la memoria supera el 60%, se requiere una atención adecuada.
Semanal	Temperatura ambiente en la sala de equipos	Medición de instrumentos	La temperatura de funcionamiento a largo plazo de la sala de equipos oscila entre 0°C y 50°C, y la temperatura de funcionamiento a corto plazo oscila entre -5°C y 55°C.
	Humedad ambiente en la sala de equipos	Medición de instrumentos	La humedad ambiente en la sala de equipos debe variar entre 10% y 90% RH.
Mensual	Posición del dispositivo	Observación y medición de instrumentos	El dispositivo se coloca de forma estable en una posición plana en un entorno bien ventilado, seco y limpio.
	Tabla de enrutamiento	<HUAWEI> display IP routing-table	En todos los dispositivos que ejecutan el mismo protocolo de enrutamiento en la misma capa de una red, el número de rutas no debe variar ampliamente.



Intervalo de mantenimiento recomendado	Verificar el elemento	Método de verificación	Criterios de evaluación
	Backup de configuración	NA	La información de configuración de los dispositivos debe ser respaldada cada mes.
	Cambio de contraseña	NA	Las contraseñas de inicio de sesión del dispositivo deben ser cambiadas cada mes.

9.3.5 Optimización de la red

Task 1. Optimización de rendimiento

Con el desarrollo de la empresa, el tráfico interno, especialmente el tráfico entre el segundo y el tercer piso, aumenta considerablemente. La capacidad del enlace entre switches de agregación es insuficiente para una cantidad tan grande de tráfico. ¿Cómo se puede optimizar el enlace?

Respuesta de referencia:

1. Puede agregar enlaces físicos entre F2-AGG1 y F3-AGG1 y configurar la agregación de enlaces Ethernet.
2. Cambiar los costos de OSPF para implementar balanceo de carga para que algún tráfico pueda ser reenviado a través de CORE1.

9.4 Verificación

Los detalles no se proporcionan aquí.

9.5 Referencia de configuración

Configuración en el router

```
#
sysname Router
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 tra
```



```
p-paramsname datacom
snmp-agent target-host trap-paramsname datacom v3 securityname test privacy
snmp-agent usm-user v3 test datacom authentication-mode md5 4DE14BB77015FFE895A
65FDE05B8F6E9 privacy-mode aes128 4DE14BB77015FFE895A65FDE05B8F6E9
snmp-agent trap source GigabitEthernet0/0/1
snmp-agent trap enable
snmp-agent
#
acl number 2000
rule 5 permit source 192.168.105.0 0.0.0.255
rule 10 permit source 192.168.106.0 0.0.0.255
rule 15 permit source 192.168.107.0 0.0.0.255
#
nat address-group 1 1.1.1.2 1.1.1.10
#
interface GigabitEthernet0/0/0
ip address 1.1.1.1 255.255.255.0
nat server protocol tcp global current-interface 8080 inside 192.168.100.1 www
nat outbound 2000 address-group 1
#
interface GigabitEthernet0/0/1
ip address 192.168.204.1 255.255.255.252
#
ospf 1
default-route-advertise always
area 0.0.0.0
network 192.168.204.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
#
return
```

Configuración en CORE1

```
#
sysname CORE1
#
vlan batch 100 105 201 to 202 204 to 205
#
dhcp enable
#
acl number 3000
rule 5 deny ip source 192.168.105.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
rule 10 permit ip
#
ip pool ap-f1
gateway-list 192.168.205.254
network 192.168.205.0 mask 255.255.255.0
excluded-ip-address 192.168.205.253
#
ip pool sta-f1
gateway-list 192.168.105.254
network 192.168.105.0 mask 255.255.255.0
#
interface Vlanif1
ip address 192.168.1.254 255.255.255.0
```



```
#
interface Vlanif100
 ip address 192.168.100.254 255.255.255.0
#
interface Vlanif105
 ip address 192.168.105.254 255.255.255.0
 dhcp select global
#
interface Vlanif201
 ip address 192.168.201.1 255.255.255.252
#
interface Vlanif202
 ip address 192.168.202.1 255.255.255.252
#
interface Vlanif204
 ip address 192.168.204.2 255.255.255.252
#
interface Vlanif205
 ip address 192.168.205.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 201
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 202
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 205
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 204
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.100.0 0.0.0.255
  network 192.168.105.0 0.0.0.255
  network 192.168.205.0 0.0.0.255
  network 192.168.201.0 0.0.0.3
  network 192.168.202.0 0.0.0.3
  network 192.168.204.0 0.0.0.3
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC635139
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
```




```
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 %_#_3UJ'3!M;9]$R@P:G
H1!! privacy-mode des56 %_#_3UJ'3!M;9]$R@P:GH1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
return
```

Configuración en F2-AGG1

```
#
sysname F2-AGG1
#
vlan batch 2 101 to 102 106 201 203 206
#
dhcp enable
#
ip pool admin
gateway-list 192.168.102.254
network 192.168.102.0 mask 255.255.255.0
#
ip pool ap-f2
gateway-list 192.168.206.254
network 192.168.206.0 mask 255.255.255.0
option 43 sub-option 3 ascii 192.168.205.253
#
ip pool manager
gateway-list 192.168.101.254
network 192.168.101.0 mask 255.255.255.0
#
ip pool sta-f2
gateway-list 192.168.106.254
network 192.168.106.0 mask 255.255.255.0
#
interface Vlanif2
ip address 192.168.2.254 255.255.255.0
#
interface Vlanif101
ip address 192.168.101.254 255.255.255.0
dhcp select global
#
interface Vlanif102
ip address 192.168.102.254 255.255.255.0
dhcp select global
#
interface Vlanif106
ip address 192.168.106.254 255.255.255.0
dhcp select global
#
interface Vlanif201
ip address 192.168.201.2 255.255.255.252
#
interface Vlanif203
ip address 192.168.203.1 255.255.255.252
#
```



```
interface Vlanif206
 ip address 192.168.206.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 201
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 203
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 101 106 206
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.101.0 0.0.0.255
  network 192.168.102.0 0.0.0.255
  network 192.168.106.0 0.0.0.255
  network 192.168.201.0 0.0.0.3
  network 192.168.203.0 0.0.0.3
  network 192.168.206.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC070327
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 +3V3OM/)GC'7M+H\V-;;
(!!! privacy-mode des56 +3V3OM/)GC'7M+H\V-;;(!!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Configuración en F3-AGG1

```
#
sysname F3-AGG1
#
vlan batch 3 103 to 104 107 202 to 203 207
```



```
#
ip pool ap-f3
 gateway-list 192.168.207.254
 network 192.168.207.0 mask 255.255.255.0
 option 43 sub-option 3 ascii 192.168.205.253
#
ip pool marketing
 gateway-list 192.168.103.254
 network 192.168.103.0 mask 255.255.255.0
#
ip pool rd
 gateway-list 192.168.104.254
 network 192.168.104.0 mask 255.255.255.0
#
ip pool sta-f3
 gateway-list 192.168.107.254
 network 192.168.107.0 mask 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface Vlanif103
 ip address 192.168.103.254 255.255.255.0
 dhcp select global
#
interface Vlanif104
 ip address 192.168.104.254 255.255.255.0
 dhcp select global
#
interface Vlanif107
 ip address 192.168.107.254 255.255.255.0
 dhcp select global
#
interface Vlanif202
 ip address 192.168.202.2 255.255.255.252
#
interface Vlanif203
 ip address 192.168.203.2 255.255.255.252
#
interface Vlanif207
 ip address 192.168.207.254 255.255.255.0
 dhcp select global
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 202
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 203
#
interface GigabitEthernet0/0/11
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
```



```
#
interface GigabitEthernet0/0/12
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 107 207
#
interface GigabitEthernet0/0/13
 port link-type trunk
 port trunk pvid vlan 3
 port trunk allow-pass vlan 3 103 to 104
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.103.0 0.0.0.255
  network 192.168.104.0 0.0.0.255
  network 192.168.107.0 0.0.0.255
  network 192.168.202.0 0.0.0.3
  network 192.168.203.0 0.0.0.3
  network 192.168.207.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCFB0564
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 5>5W!8N^H,L8E-@(C*:@
AQ!! privacy-mode des56 5>5W!8N^H,L8E-@(C*:@AQ!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Configuración en the AC

```
#
sysname AC
#
vlan batch 205
#
interface Vlanif205
 ip address 192.168.205.253 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 205
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent group v3 datacom privacy
snmp-agent target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datacom
snmp-agent target-host trap-paramsname datacom v3 securityname %^%#TvvWF~zi>Sgp
XL=P81^I^^(P&`UR97&h,l`eK8%^%# privacy
snmp-agent trap source Vlanif205
snmp-agent trap enable
snmp-agent
```



```
#
ip route-static 0.0.0.0 0.0.0.0 192.168.205.254
#
capwap source interface vlanif205
#
wlan
security-profile name WLAN-F1
    security wpa-wpa2 psk pass-phrase %^%#53mQ@x*]z+u72&YdCR7A=11u&USV+9^Qw""O43X>%^%# aes
security-profile name WLAN-F2
    security wpa-wpa2 psk pass-phrase %^%#YKB4ZI%zFQxmOS76yL08],Z41lhJV"S[db(kar0X%^%# aes
security-profile name WLAN-F3
    security wpa-wpa2 psk pass-phrase %^%#|8)z/PyjU1ssX8Cr(3M=%x\{CP*t,BCahW84sqvK%^%# aes
ssid-profile name WLAN-F1
    ssid WLAN-F1
ssid-profile name WLAN-F2
    ssid WLAN-F2
ssid-profile name WLAN-F3
    ssid WLAN-F3
vap-profile name WLAN-F1
    service-vlan vlan-id 105
    ssid-profile WLAN-F1
    security-profile WLAN-F1
vap-profile name WLAN-F2
    service-vlan vlan-id 106
    ssid-profile WLAN-F2
    security-profile WLAN-F2
vap-profile name WLAN-F3
    service-vlan vlan-id 107
    ssid-profile WLAN-F3
    security-profile WLAN-F3
ap-group name WLAN-F1
    radio 0
        vap-profile WLAN-F1 wlan 1
    radio 1
        vap-profile WLAN-F1 wlan 1
    radio 2
        vap-profile WLAN-F1 wlan 1
ap-group name WLAN-F2
    radio 0
        vap-profile WLAN-F2 wlan 2
    radio 1
        vap-profile WLAN-F2 wlan 2
    radio 2
        vap-profile WLAN-F2 wlan 2
ap-group name WLAN-F3
    radio 0
        vap-profile WLAN-F3 wlan 2
    radio 1
        vap-profile WLAN-F3 wlan 2
    radio 2
        vap-profile WLAN-F3 wlan 2
ap-id 0 type-id 60 ap-mac 00e0-fcca-2e20 ap-sn 2102354483108B3A413A
    ap-name F1-AP1
    ap-group WLAN-F1
ap-id 1 type-id 60 ap-mac 00e0-fcf0-7bc0 ap-sn 210235448310D45A674C
```



```
ap-name F2-AP1
ap-group WLAN-F2
ap-id 2 type-id 60 ap-mac 00e0-fcb2-72f0 ap-sn 210235448310C73E4033
ap-name F3-AP1
ap-group WLAN-F3
#
return
```

Configuración en F1-ACC1

```
#
sysname F1-ACC1
#
vlan batch 100 105 205
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 105 205
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/4
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/5
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/6
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/7
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/8
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/9
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/10
 port link-type access
```



```
port default vlan 100
#
interface GigabitEthernet0/0/20
port link-type trunk
port trunk pvid vlan 205
port trunk allow-pass vlan 105 205
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC03178D
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datcom v3
snmp-agent usm-user v3 test datcom authentication-mode md5 3@^>FD5!85E`A!>CAH"1
U1!! privacy-mode des56 3@^>FD5!85E`A!>CAH"1U1!!
snmp-agent trap source Vlanif1
snmp-agent trap enable
#
return
```

Configuración en F2-ACC1

```
#
sysname F2-ACC1
#
vlan batch 2 102
#
interface Vlanif2
ip address 192.168.2.1 255.255.255.0
#
interface Ethernet0/0/1
port link-type access
port default vlan 102
#
interface Ethernet0/0/2
port link-type access
port default vlan 102
#
interface Ethernet0/0/3
port link-type access
port default vlan 102
#
interface Ethernet0/0/4
port link-type access
port default vlan 102
#
interface Ethernet0/0/5
port link-type access
port default vlan 102
#
interface Ethernet0/0/6
port link-type access
port default vlan 102
#
interface Ethernet0/0/7
```



```
port link-type access
port default vlan 102
#
interface Ethernet0/0/8
port link-type access
port default vlan 102
#
interface Ethernet0/0/9
port link-type access
port default vlan 102
#
interface Ethernet0/0/10
port link-type access
port default vlan 102
#
interface Ethernet0/0/11
port link-type access
port default vlan 102
#
interface Ethernet0/0/12
port link-type access
port default vlan 102
#
interface Ethernet0/0/13
port link-type access
port default vlan 102
#
interface Ethernet0/0/14
port link-type access
port default vlan 102
#
interface Ethernet0/0/15
port link-type access
port default vlan 102
#
interface Ethernet0/0/16
port link-type access
port default vlan 102
#
interface Ethernet0/0/17
port link-type access
port default vlan 102
#
interface Ethernet0/0/18
port link-type access
port default vlan 102
#
interface Ethernet0/0/19
port link-type access
port default vlan 102
#
interface Ethernet0/0/20
port link-type access
port default vlan 102
#
```




```
interface Ethernet0/0/21
 port link-type access
 port default vlan 102
#
interface Ethernet0/0/22
 port link-type access
 port default vlan 102
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 2
 port trunk allow-pass vlan 2 102
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC456509
snmp-agent sys-info version v3
snmp-agent group v3 datcom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
 datcom v3
snmp-agent usm-user v3 test datcom authentication-mode md5 (H\O$K,P78:9;\H&H"Ma
+A!! privacy-mode des56 (H\O$K,P78:9;\H&H"Ma+A!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Configuración en F2-ACC2

```
#
sysname F2-ACC2
#
vlan batch 2 101 106 206
#
interface Vlanif1
#
interface Vlanif2
 ip address 192.168.2.2 255.255.255.0
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 101
#
interface Ethernet0/0/5
 port link-type access
```



```
port default vlan 101
#
interface Ethernet0/0/6
port link-type access
port default vlan 101
#
interface Ethernet0/0/7
port link-type access
port default vlan 101
#
interface Ethernet0/0/8
port link-type access
port default vlan 101
#
interface Ethernet0/0/9
port link-type access
port default vlan 101
#
interface Ethernet0/0/10
port link-type access
port default vlan 101
#
interface Ethernet0/0/11
port link-type access
port default vlan 101
#
interface Ethernet0/0/12
port link-type access
port default vlan 101
#
interface Ethernet0/0/13
port link-type access
port default vlan 101
#
interface Ethernet0/0/14
port link-type access
port default vlan 101
#
interface Ethernet0/0/15
port link-type access
port default vlan 101
#
interface Ethernet0/0/16
port link-type access
port default vlan 101
#
interface Ethernet0/0/17
port link-type access
port default vlan 101
#
interface Ethernet0/0/18
port link-type access
port default vlan 101
#
interface Ethernet0/0/19
```



```
port link-type access
port default vlan 101
#
interface Ethernet0/0/20
port link-type trunk
port trunk pvid vlan 206
port trunk allow-pass vlan 106 206
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 101 106 206
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCA5263C
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
    datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 RN,<E0K"S8Z3K7.NSN8+
L1!! privacy-mode des56 RN,<E0K"S8Z3K7.NSN8+L1!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Configuración en F2-ACC3

```
#
sysname F2-ACC3
#
vlan batch 2 102
#
interface Vlanif2
ip address 192.168.2.3 255.255.255.0
#
interface Ethernet0/0/1
port link-type access
port default vlan 102
#
interface Ethernet0/0/2
port link-type access
port default vlan 102
#
interface Ethernet0/0/3
port link-type access
port default vlan 102
#
interface Ethernet0/0/4
port link-type access
port default vlan 102
#
interface Ethernet0/0/5
port link-type access
```



```
port default vlan 102
#
interface Ethernet0/0/6
port link-type access
port default vlan 102
#
interface Ethernet0/0/7
port link-type access
port default vlan 102
#
interface Ethernet0/0/8
port link-type access
port default vlan 102
#
interface Ethernet0/0/9
port link-type access
port default vlan 102
#
interface Ethernet0/0/10
port link-type access
port default vlan 102
#
interface Ethernet0/0/11
port link-type access
port default vlan 102
#
interface Ethernet0/0/12
port link-type access
port default vlan 102
#
interface Ethernet0/0/13
port link-type access
port default vlan 102
#
interface Ethernet0/0/14
port link-type access
port default vlan 102
#
interface Ethernet0/0/15
port link-type access
port default vlan 102
#
interface Ethernet0/0/16
port link-type access
port default vlan 102
#
interface Ethernet0/0/17
port link-type access
port default vlan 102
#
interface Ethernet0/0/18
port link-type access
port default vlan 102
#
interface Ethernet0/0/19
```



```
port link-type access
port default vlan 102
#
interface Ethernet0/0/20
port link-type access
port default vlan 102
#
interface Ethernet0/0/21
port link-type access
port default vlan 102
#
interface Ethernet0/0/22
port link-type access
port default vlan 102
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 2
port trunk allow-pass vlan 2 102
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC6E2774
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 :S@4*#]%O_-M9=:>$BB:
7!!! privacy-mode des56 :S@4*#]%O_-M9=:>$BB:7!!!
snmp-agent trap source Vlanif2
snmp-agent trap enable
#
return
```

Configuración en F3-ACC1

```
#
sysname F3-ACC1
#
vlan batch 3 103 to 104
#
interface Vlanif3
ip address 192.168.3.1 255.255.255.0
#
interface Ethernet0/0/1
port link-type access
port default vlan 103
#
interface Ethernet0/0/2
port link-type access
port default vlan 103
#
interface Ethernet0/0/3
port link-type access
port default vlan 103
```



```
#
interface Ethernet0/0/4
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/5
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/6
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/7
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/8
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/9
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/10
 port link-type access
 port default vlan 103
#
interface Ethernet0/0/11
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/12
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/13
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/14
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/15
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/16
 port link-type access
 port default vlan 104
#
interface Ethernet0/0/17
 port link-type access
```



```
port default vlan 104
#
interface Ethernet0/0/18
port link-type access
port default vlan 104
#
interface Ethernet0/0/19
port link-type access
port default vlan 104
#
interface Ethernet0/0/20
port link-type access
port default vlan 104
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCC75F9A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 FD5[3#*%a/!W$IOS;(RD
3Q!! privacy-mode des56 FD5[3#*%a/!W$IOS;(RD3Q!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Configuración en F3-ACC2

```
#
sysname F3-ACC2
#
vlan batch 3 103 107 207
#
interface Vlanif3
ip address 192.168.3.2 255.255.255.0
#
interface MEth0/0/1
#
interface Ethernet0/0/1
port link-type access
port default vlan 103
#
interface Ethernet0/0/2
port link-type access
port default vlan 103
#
interface Ethernet0/0/3
port link-type access
```



```
port default vlan 103
#
interface Ethernet0/0/4
port link-type access
port default vlan 103
#
interface Ethernet0/0/5
port link-type access
port default vlan 103
#
interface Ethernet0/0/6
port link-type access
port default vlan 103
#
interface Ethernet0/0/7
port link-type access
port default vlan 103
#
interface Ethernet0/0/8
port link-type access
port default vlan 103
#
interface Ethernet0/0/9
port link-type access
port default vlan 103
#
interface Ethernet0/0/10
port link-type access
port default vlan 103
#
interface Ethernet0/0/11
port link-type access
port default vlan 103
#
interface Ethernet0/0/12
port link-type access
port default vlan 103
#
interface Ethernet0/0/13
port link-type access
port default vlan 103
#
interface Ethernet0/0/14
port link-type access
port default vlan 103
#
interface Ethernet0/0/15
port link-type access
port default vlan 103
#
interface Ethernet0/0/16
port link-type access
port default vlan 103
#
interface Ethernet0/0/17
```




```
port link-type access
port default vlan 103
#
interface Ethernet0/0/18
port link-type access
port default vlan 103
#
interface Ethernet0/0/19
port link-type access
port default vlan 103
#
interface Ethernet0/0/20
port link-type trunk
port trunk pvid vlan 207
port trunk allow-pass vlan 107 207
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 107 207
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCCF3804A
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 0=.SBW74%B[6NT)>.>:]
aA!! privacy-mode des56 0=.SBW74%B[6NT)>.>:]aA!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

Configuración en F3-ACC3

```
#
sysname F3-ACC3
#
vlan batch 3 103 to 104
#
interface Vlanif3
ip address 192.168.3.3 255.255.255.0
#
interface Ethernet0/0/1
port link-type access
port default vlan 103
#
interface Ethernet0/0/2
port link-type access
port default vlan 103
#
interface Ethernet0/0/3
port link-type access
```



```
port default vlan 103
#
interface Ethernet0/0/4
port link-type access
port default vlan 103
#
interface Ethernet0/0/5
port link-type access
port default vlan 103
#
interface Ethernet0/0/6
port link-type access
port default vlan 103
#
interface Ethernet0/0/7
port link-type access
port default vlan 103
#
interface Ethernet0/0/8
port link-type access
port default vlan 103
#
interface Ethernet0/0/9
port link-type access
port default vlan 103
#
interface Ethernet0/0/10
port link-type access
port default vlan 103
#
interface Ethernet0/0/11
port link-type access
port default vlan 104
#
interface Ethernet0/0/12
port link-type access
port default vlan 104
#
interface Ethernet0/0/13
port link-type access
port default vlan 104
#
interface Ethernet0/0/14
port link-type access
port default vlan 104
#
interface Ethernet0/0/15
port link-type access
port default vlan 104
#
interface Ethernet0/0/16
port link-type access
port default vlan 104
#
interface Ethernet0/0/17
```

```
port link-type access
port default vlan 104
#
interface Ethernet0/0/18
port link-type access
port default vlan 104
#
interface Ethernet0/0/19
port link-type access
port default vlan 104
#
interface Ethernet0/0/20
port link-type access
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3
port trunk allow-pass vlan 3 103 to 104
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
snmp-agent
snmp-agent local-engineid 800007DB034C1FCC224BC2
snmp-agent sys-info version v3
snmp-agent group v3 datacom privacy
snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname
datacom v3
snmp-agent usm-user v3 test datacom authentication-mode md5 P'5R[2VCVEX8"$Y!=87`
1A!! privacy-mode des56 P'5R[2VCVEX8"$Y!=87`1A!!
snmp-agent trap source Vlanif3
snmp-agent trap enable
#
return
```

9.6 Quiz

1. En este proyecto, CORE1, F2-AG1 y F3-AGG1 forman un anillo físico. Sin embargo, en la fase de planificación y diseño de la red, los enlaces de interconexión entre los tres dispositivos se asignan a diferentes VLAN. Por lo tanto, no hay bucle. Sin embargo, durante el laboratorio, puede encontrar que la relación de vecindad entre dos dispositivos no se puede establecer correctamente. Por favor, encuentre la causa raíz y la solución.
2. ¿Qué has aprendido en este laboratorio? ¿Cómo puede ayudarte el conocimiento en tu futuro estudio o trabajo?



Respuestas de referencia

Fundamentos de configuración y VRPs de Huawei

1. Omitido.
2. El comando **reset saved-configuration** borra el archivo de configuración de inicio y cancela la configuración anterior del archivo de configuración de inicio. El archivo de configuración de inicio actual es test.cfg. Por lo tanto, después de ejecutar este comando, el contenido de test.cfg se borra y el archivo de configuración predeterminado vrpcfg.zip se utiliza como archivo de configuración de inicio. En el paso 4, se guarda la configuración en ejecución. Por lo tanto, la configuración no se modifica una vez reiniciado el dispositivo.

Enrutamiento y direccionamiento IPv4

1. Se agrega una ruta estática a la tabla de enrutamiento cuando se cumplen las siguientes condiciones:
 - a El siguiente salto de la ruta es accesible.
 - b Esta ruta es la ruta óptima hacia la red o host de destino.Por lo tanto, cuando el siguiente salto no se puede alcanzar, la ruta no se agrega a la tabla de enrutamiento de IPs.
2. Cuando se realiza una operación de ping en un dispositivo Huawei, el dispositivo busca en la tabla de enrutamiento para determinar la interfaz de salida. La dirección IP de la interfaz de salida se utiliza como la dirección IP de origen de los paquetes ICMP.

Enrutamiento OSPF

1. R2 responde a R1 a lo largo de la ruta de R2-> R1. Después de que el costo de GigabitEthernet0/0/3 en R1 se cambia a 10, el costo de la ruta de R1->R2 es 10. Por lo tanto, la ruta de Bucle de Back0 en R1 a Bucle de Back0 en R2 es R1->R3-> R2. En este caso, R2 no sabe que el costo de GigabitEthernet0/0/3 en R1 se ha cambiado a 10 y todavía utiliza el costo de GigabitEthernet0/0/3 en R1 para calcular el costo de la ruta. Por lo tanto, se utiliza la ruta R2-> R1 como ruta de respuesta.

Configuración de Ethernet Básica y VLANs

Configuración Roadmap:

- Crear una vlan para PC con necesidades especiales.
- Asociar las mac-address de los PC con las VLAN.
- Asigne interfaces a las VLAN para implementar el reenvío de Capa 2.

Procedimiento de configuración:

Cree VLAN.

```
[S1]vlan 10
```

Asocie la dirección MAC de la computadora con la VLAN 10.

```
[S1]vlan 10
[S1-vlan10]mac-vlan mac-address 00e0-fc1c-47a7
[S1-vlan10]quit
```

En este ejemplo, la dirección Mac del ordenador es 00e0-fc1c-47a7.

Habilite la asignación de VLANs basada en MACs.

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]mac-vlan enable
[S1-GigabitEthernet0/0/1]quit
```

Configure GE0/0/1 connected to S2 como a hybrid port to allow data frames of the corresponding VLAN to pass through in untagged mode.

```
[S1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 10
[S1-GigabitEthernet0/0/1]quit
```

Configure GE0/0/2 conectado a la red de la empresa para transmitir paquetes de forma transparente desde las VLAN asociadas con las direcciones MACs.

```
[S1]interface gigabitethernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 10
[S1-GigabitEthernet0/0/2]quit
```

Árbol de esparcimiento

1. No. Después de recibir las BPDUs STP, todos los puentes agregan el costo del puerto local al RPC en las BPDUs para calcular el costo de la ruta raíz del puerto. Por lo tanto, cuando el costo de GigabitEthernet 0/0/14 sobre S1 cambia, el costo de la ruta raíz de S4 no se ve afectado.
2. Cambiar la prioridad de GigabitEthernet0/0/11 en S1.
3. No. El enlace entre S1 y S2 formará un bucle. Por lo tanto, se debe bloquear un enlace.

Agregación de enlaces Ethernet

1. El número de enlace activo mínimo debe ser inferior o igual al número de enlace activo máximo.

Comunicación Inter-VLAN

1. Crear una interfaz de capa 3 en S1 para conectarse a GigabitEthernet0/0/1 de R1 y configurar una ruta a la red correspondiente.
2. Si alguna interfaz física que permita el paso de la VLAN va hacia arriba, la interfaz VLANIF correspondiente va hacia arriba.

Configuración de ACL

Configuración Roadmap:

- Configurar OSPF para habilitar la conectividad.
- Activar Telnet y FTP en R3.
- Configure un ACL avanzado para coincidir con el tráfico deseado.

Procedimiento de configuración:

Configurar conectividad de red, Telnet y FTP.

Configure un ACL en R2.

```
[R2] acl 3001
[R2-acl-adv-3001] rule 5 permit tcp source 10.1.2.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001] rule 10 permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port range 20 21
[R2-acl-adv-3001] rule 15 deny tcp source any
[R2-acl-adv-3001] quit
```

Aplicar la ACL en GE0/0/3 de R2.

```
[R2] interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3] traffic-filter inbound acl 3001
```

Configuración AAA local

Los detalles no se proporcionan aquí.

Configuración de NAT

1. No es necesario.

Configuración de FTP

1. Modo activo

Configuración DHCP

1. Un pool de direcciones de interfaz sólo contiene direcciones IP en la misma subred que la interfaz.
Un pool de direcciones globales puede contener direcciones IP en la misma subred que la interfaz o direcciones IP de diferentes subredes (como en la red de retransmisión DHCP).
2. En la hipótesis sin agente de retransmisión, un pool de direcciones IP en la misma subred que la interfaz se selecciona entre los pools de direcciones globales, y las direcciones IP se asignan a los clientes de acuerdo a los parámetros del pool de direcciones. En el escenario con un agente de retransmisión: Basándose en la subred solicitada por el agente de retransmisión, se selecciona un pool de direcciones IP en la subred solicitada entre los pools de direcciones globales, y las direcciones IP se asignan a los clientes de acuerdo a los parámetros del pool de direcciones.

Creación de una WLAN



1. No hay impacto. Se realiza el reenvío directo y los datos no pasan por GigabitEthernet0/0/10 del AC. Si se utiliza el reenvío de túneles, configure GigabitEthernet0/0/10 para permitir el paso de paquetes desde VLAN 101. De lo contrario, las STA no pueden acceder a S1.
2. AP1 y AP2 utilizan diferentes perfiles VAP y diferentes parámetros de servicio-VLAN se configuran en los perfiles VAP.

Creación de una red IPv6

1. El router tiene múltiples interfaces en la red FE80::/10. Cuando la dirección IPv6 de destino es una dirección local de enlace, la interfaz saliente no se puede determinar consultando la tabla de enrutamiento. Por lo tanto, se debe especificar la interfaz de origen.
2. En el modo de estado, todos los 128 bits de una dirección de interfaz IPv6 son especificados por el servidor DHCPv6. En modo sin estado, se genera un ID de interfaz de 64 bits basado en la especificación EUI-64.

Configuración de una red de campus

1. A pesar de que se ha implementado la prevención de bucles en la capa VLAN, todavía existen bucles físicos. Las BPDUs STP no llevan etiquetas VLAN. Por lo tanto, uno de los enlaces entre los tres switches debe ser bloqueado. Como resultado, la relación vecina no se puede establecer entre dos de los switches. En el despliegue real, se ha implementado la prevención de bucles a nivel de VLAN. Por lo tanto, puede deshabilitar STP en las interfaces entre los dispositivos.
2. Omitido.

Básicos de programación y automatización de red

1. Utilice la función write() de telnetlib para escribir el script para configurar línea por línea las interfaces del dispositivo.
2. Para obtener más detalles, consulte la biblioteca estándar de E/S de Python.