CCNA Guia de Comandos

German Hernandez
CCIE #24492

CCNA GUIA DE COMANDOS

por

German Hernandez

CCIE #24492

German Hernandez

Heredia, Costa Rica

German@tecdemia.com

www.tecdemia.com

Tabla de contenidos

CAPITULO 1 — SWITCHING

1. CREACION DE VLANS

Una VLAN (red de área local virtual) es una agrupación lógica de dispositivos en un switch que están aislados de otros dispositivos en el mismo switch. Las VLAN se utilizan para segmentar el tráfico en una red, mejorar la seguridad y aumentar el rendimiento.

Para crear una VLAN en un equipo Cisco, necesitará:

1. Ingresar al modo de configuración global.
2. Utilice el comando `vlan` para crear la VLAN.
3. Asigne la VLAN a una interfaz.

Ejemplo

Para crear una VLAN con ID 10 y asignarla a la interfaz `GigaEthernet0/7`, debe usar los siguientes comandos:

Fragmento de código

```
configure terminal
vlan 10
name Ventas
interface GigaEthernet0/7
switchport access vlan 10
```

Una vez que haya creado una VLAN, puede verificar su configuración mediante el comando

```
show vlan
```

```
switch# show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
--
1    default                           active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                 Gi1/0/4, Gi1/0/5, Gi1/0/6
10   Ventas                            active    Gi1/0/7
```

En este ejemplo, se muestra la salida del comando "show vlan". Cada fila representa una VLAN y sus detalles asociados. Aquí hay una explicación de la información proporcionada:

VLAN: Número de identificación de la VLAN.

Name: Nombre descriptivo asignado a la VLAN.

Status: Estado de la VLAN, que en este caso es "active" (activa).

Ports: Puertos que pertenecen a la VLAN. En este ejemplo, se enumeran los puertos GigabitEthernet 1/0/1 a 1/0/6 para la VLAN 1 (default), el puerto 1/0/6 para la VLAN 10 (Ventas).

Este comando es útil para verificar la configuración actual de VLANs en el switch y asegurarse de que los puertos estén asignados correctamente a las VLANs correspondientes.

Beneficios de usar VLAN

1. Seguridad mejorada: las VLAN se pueden utilizar para segmentar el tráfico en una red, lo que puede ayudar a mejorar la seguridad. Por ejemplo, puede crear una VLAN para sus empleados y una VLAN separada para sus invitados. Esto ayudaría a evitar que sus empleados accedan a los datos de sus huéspedes.
2. Mayor rendimiento: las VLAN pueden ayudar a aumentar el rendimiento al reducir la cantidad de tráfico de difusión en una red. El tráfico de difusión se envía a todos los dispositivos de una red, lo que puede hacer mas lenta la red. Al crear VLAN, puede reducir la cantidad de tráfico de difusión en una red.
3. Capacidad de administración mejorada: las VLAN pueden ayudar a mejorar la capacidad de administración al facilitar la solución de problemas en una red. Por ejemplo, si tiene un problema con una VLAN, simplemente puede deshabilitar la VLAN para solucionar el problema. Esto puede ayudarle a identificar y solucionar rápidamente el problema.

2. PUERTOS TRUNK

Un puerto troncal en un switch Cisco es un puerto que puede transportar tráfico desde múltiples VLAN. Esto le permite conectar varios switches entre sí y hacer que se comuniquen entre sí aunque estén en VLAN diferentes.

Para configurar un puerto troncal en un switch Cisco, debe seguir los siguientes pasos:

1. Ingrese al modo de configuración global.
2. Introduzca el modo de configuración de la interfaz para el puerto que desea configurar como tronco.
3. Utilice el comando switchport mode trunk para establecer el modo port en trunk.
4. Utilice el comando switchport allowed vlans para especificar las VLAN que están permitidas en el puerto troncal.

Por ejemplo, para configurar un puerto troncal en la interfaz fa0/1 que permita el tráfico de VLAN 1, 2 y 3, debe usar los siguientes comandos:

Fragmento de código

```
switch(config)# interface fa0/1
switch(config-if)# switchport mode trunk
switch(config-if)# switchport allowed vlans 1,2,3
```

Una vez que haya configurado el puerto troncal, puede verificar la configuración mediante el comando show interfaces.

Aquí hay un ejemplo de la salida del comando show interfaces para un puerto troncal:

Fragmento de código

```
interface fa0/1
description Trunk haci el switch Core
switchport mode trunk
switchport allowed vlans 1,2,3
```

Como puede ver, la salida muestra que la interfaz está en modo troncal y que las VLAN 1, 2 y 3 están permitidas en el puerto.

3. SPEED Y DUPLEX

En los switches Cisco, el comando `"speed"` se utiliza para establecer manualmente la velocidad de una interfaz. Le permite especificar la velocidad de transferencia de datos deseada para una interfaz en particular. Las opciones disponibles suelen incluir velocidades automáticas, 10, 100, 1000 y, a veces, más altas, según el modelo y las capacidades del switch.

Aquí hay un ejemplo de cómo funciona el comando `"speed"` en los switches Cisco:

Digamos que tenemos un switch Cisco con una interfaz etiquetada como `"GigabitEthernet1/0/1"` y queremos configurar manualmente su velocidad a 1000 Mbps (1 Gbps). Estos son los pasos para configurarlo:

Ingrese al modo EXEC privilegiado en el switch escribiendo `"enable"` y proporcionando la contraseña adecuada si es necesario.

Cambie al modo de configuración global escribiendo "`configure terminal`" o simplemente "`conf t`".

Acceda al modo de configuración de la interfaz para la interfaz deseada mediante el comando interface. En nuestro ejemplo, sería:

```
interface GigabitEthernet1/0/1
```

Establezca la velocidad deseada mediante el comando de velocidad. En nuestro ejemplo, queremos establecerlo en 1000 Mbps, por lo que usaríamos:

```
speed 1000
```

Opcionalmente, también puede configurar el modo dúplex para la interfaz (por ejemplo, "`full duplex`" para dúplex completo o "`dúplex-auto`" para negociación automática).

Salga del modo de configuración de la interfaz escribiendo "exit".

Guarde los cambios de configuración escribiendo "`copy running-config startup-config`" para que la configuración sea persistente en los reinicios.

Al especificar la velocidad manualmente, anula el comportamiento predeterminado de negociación automática, este comportamiento permite que la interfaz negocie automáticamente y seleccione la mejor velocidad en función de las capacidades del dispositivo conectado. Sin embargo, tenga en cuenta que ambos extremos del enlace deben tener configuraciones de velocidad compatibles para una comunicación exitosa.

En el contexto de los switches Ethernet, dúplex se refiere a la capacidad de un dispositivo para enviar y recibir datos al mismo tiempo. Hay dos tipos de dúplex: semidúplex y dúplex completo.

1. **Half-duplex** es el modo de operación más antiguo y menos eficiente. En el modo half-duplex, un dispositivo solo puede enviar o recibir datos a la vez. Esto significa que si dos dispositivos están conectados al mismo segmento Ethernet y ambos intentan enviar datos, tendrán que turnarse. Esto puede provocar colisiones, lo que puede ralentizar la red.
2. **Full-duplex** es el modo de operación más nuevo y más eficiente. En el modo dúplex completo, un dispositivo puede enviar y recibir datos al mismo tiempo. Esto elimina la posibilidad de colisiones, lo que puede mejorar significativamente el rendimiento de la red.

La mayoría de los switches Ethernet modernos admiten el modo full duplex. Sin embargo, es posible que algunos dispositivos más antiguos solo admitan el modo dúplex medio. Si está conectando un nuevo dispositivo a una red Ethernet, es importante consultar la documentación para asegurarse de que admite el modo dúplex que utiliza la red.

En general, el modo dúplex completo es el modo de operación preferido para las redes Ethernet. Sin embargo, hay algunos casos en los que puede ser necesario el modo half-duplex, como cuando se conectan dispositivos más antiguos que no admiten dúplex completo (poco probable).

4. TABLA DE DIRECCIONES MAC

La administración adecuada de la tabla de direcciones MAC es esencial para garantizar un rendimiento óptimo y la seguridad de una red. Los switches Cisco ofrecen una amplia gama de comandos que permiten a los administradores configurar y supervisar eficientemente la tabla de direcciones MAC. En este artículo, exploraremos los comandos más importantes para administrar la tabla de direcciones MAC en switches Cisco.

Mostrar la tabla de direcciones MAC:

El primer paso para administrar la tabla de direcciones MAC es visualizar su contenido actual. Utilice el siguiente comando para ver la tabla de direcciones MAC en un switch Cisco:

```
show mac address-table
```

Este comando mostrará una lista de direcciones MAC aprendidas por el switch, junto con la interfaz de entrada correspondiente.

Borrar la tabla de direcciones MAC:

En algunos casos, es necesario borrar la tabla de direcciones MAC para eliminar entradas no deseadas o conflictivas. Puede hacerlo utilizando el siguiente comando:

```
clear mac address-table
```

Tenga en cuenta que este comando eliminará todas las entradas de la tabla de direcciones MAC.

Filtrar direcciones MAC específicas:

Si necesita filtrar direcciones MAC específicas para evitar que se aprendan o transmitan en el switch, puede utilizar el siguiente comando:

```
mac address-table static <mac_address> vlan <vlan_id> drop
```

Sustituya <MAC_address> por la dirección MAC que desea filtrar y <VLAN_ID> por el ID de VLAN correspondiente. Este comando evitará que el switch aprenda o transmita la dirección MAC especificada.

Configurar una dirección MAC estática:

En algunos casos, es útil configurar manualmente una dirección MAC en la tabla para garantizar su disponibilidad y evitar que sea eliminada. Utilice el siguiente comando para agregar una dirección MAC estática:

```
mac address-table static <mac_address> vlan <vlan_id> interface <interface>
```

Reemplace <MAC_address> por la dirección MAC que desea configurar, <VLAN_ID> por el ID de VLAN correspondiente y <interface> por la interfaz en la que se encuentra la dirección MAC.

Configurar el tiempo de envejecimiento de la tabla de direcciones MAC:

La tabla de direcciones MAC tiene un tiempo de envejecimiento que determina cuánto tiempo se mantienen las entradas antes de ser eliminadas automáticamente. Puede configurar este tiempo utilizando el siguiente comando:

```
mac address-table aging-time <time_in_seconds>
```

Sustituya <time_in_seconds> por el tiempo de envejecimiento deseado en segundos. Por ejemplo, si desea que las entradas se eliminen después de 300 segundos (5 minutos), utilice el valor "300" en este comando.

5. VLANS DE VOZ

Una VLAN de voz es una LAN virtual (VLAN) que se utiliza para transportar tráfico de voz desde teléfonos IP. Las VLAN de voz suelen configurarse en puertos de acceso que están conectados a teléfonos IP. Esto permite que el tráfico de voz se aísle del tráfico de datos, lo que puede mejorar la calidad y la seguridad de las llamadas.

Los teléfonos IP tienen dos puertos, uno para conectarse al switch y el otro para conectar la computadora. Esto permite tener solo una salida de cableado de red para estos dos dispositivos.

Acá un resumen de cada uno de los elementos que participan en esta configuración:

1. **VLAN de voz:** La VLAN de voz se utiliza para transportar tráfico de voz desde el teléfono IP.
2. **VLAN de datos:** La VLAN de datos se utiliza para transportar tráfico de datos desde computadoras y otros dispositivos.
3. **Teléfono IP:** El teléfono IP se conecta al switch mediante un puerto de acceso configurado para la VLAN de voz y para la VLAN de datos. El ip phose utiliza la VLAN de voz para su propio tráfico y permite el tráfico desde el ordenador para la VLAN de datos.
4. **Computadora:** La computadora está conectada al teléfono IP mediante un puerto de acceso configurado para la VLAN de datos.

Para configurar una VLAN de voz en un switch Cisco, necesitará:

1. Crear la VLAN de voz.
2. Asignar el teléfono IP a la VLAN de voz.

Creación de la VLAN de voz

Para crear una VLAN de voz, deberá usar el siguiente comando:

```
switchport voice vlan <vlan-id>
```

Donde `<vlan-id>` es el ID de la VLAN de voz.

Asignación del teléfono IP a la VLAN de voz

Para asignar el teléfono IP a la VLAN de voz, deberá usar el siguiente comando:

```
switchport access vlan <vlan-id>
```

Donde `<vlan-id>` es el ID de la VLAN de voz.

Beneficios de usar VLAN de voz

Calidad de llamada mejorada: las VLAN de voz pueden mejorar la calidad de las llamadas al aislar el tráfico de voz del tráfico de datos. Esto puede ayudar a reducir la latencia y el jitter, lo que puede mejorar la calidad de las llamadas de voz.

Mayor seguridad: las VLAN de voz pueden aumentar la seguridad al aislar el tráfico de voz del tráfico de datos. Esto puede ayudar a evitar el acceso no autorizado a los datos de voz.

Reducción de la congestión de la red: las VLAN de voz pueden ayudar a reducir la congestión de la red al aislar el tráfico de voz del tráfico de datos. Esto puede ayudar a mejorar el rendimiento de la red para todos los usuarios.

6. VTP

Cisco VLAN Trunking Protocol (VTP) es un protocolo utilizado en redes Cisco para facilitar la configuración y administración de VLANs (Virtual LANs). VTP permite a los administradores de red centralizar la administración de VLANs y simplificar la configuración al propagar automáticamente la información de VLAN a través de los switches de la red. En este artículo, exploraremos cómo configurar y verificar Cisco VTP en un entorno de red.

Configuración de Cisco VTP:

Configuración básica del modo VTP:
Para habilitar VTP en un switch Cisco, primero debemos ingresar al modo de configuración global mediante el siguiente comando:

```
switch# configure terminal
```

A continuación, habilitamos el modo VTP con el comando:

```
switch(config)# vtp mode {server | client | transparent}
```

Server: Un switch en modo servidor puede crear, modificar y eliminar VLANs y propagar esta información a otros switches en la red.

Client: Un switch en modo cliente solo recibe información de VLAN del servidor VTP y no puede realizar cambios en la configuración de VLAN.

Transparent: Un switch en modo transparente no participa en la propagación de información de VLAN a otros switches, pero permite la configuración local de VLAN.

Configuración del nombre de dominio VTP:

Es importante que todos los switches en una red VTP tengan el mismo nombre de dominio para que puedan intercambiar información correctamente. Para configurar el nombre de dominio VTP, utilizamos el siguiente comando:

```
switch(config)# vtp domain nombre_dominio
```

Configuración de revisiones de VTP:

Cada vez que se realiza un cambio en la configuración de VLAN en un switch en modo servidor, se incrementa el número de revisión de VTP. Para evitar problemas de propagación incorrecta de información, se recomienda establecer un número de revisión más alto en los switches que tienen la configuración VLAN más reciente. Utilizamos el siguiente comando para configurar el número de revisión de VTP:

```
switch(config)# vtp version numero_revision
```

Configuración de contraseñas de VTP (opcional):

Para agregar seguridad a la configuración de VTP, podemos configurar contraseñas de VTP. Esto garantiza que solo los switches con la contraseña correcta puedan participar en la propagación de información de VLAN. Utilizamos los siguientes comandos para configurar la contraseña de VTP:

```
switch(config)# vtp password contraseña
```

Además, podemos habilitar la encriptación de contraseñas VTP con el comando:

```
switch(config)# vtp password encryption
```

Verificación de Cisco VTP:

Después de configurar Cisco VTP en la red, podemos realizar algunas verificaciones para asegurarnos de que la configuración se haya realizado correctamente:

Verificar el modo de operación VTP:

Utilizamos el siguiente comando para verificar el modo de operación VTP en un switch:

```
switch# show vtp status
```

Verificar la información de VLAN:

Para verificar la información de VLAN recibida a través de VTP, usamos el comando:

```
switch# show vlan brief
```

Esto mostrará una lista de VLANs configuradas en el switch, junto con su estado y tipo.

Verificar la revisión VTP:

Podemos verificar la revisión VTP actual en un switch con el siguiente comando:

```
switch# show vtp status
```

Esto nos mostrará la revisión actual y la dirección MAC del switch VTP.

7. SPANNING TREE PROTOCOL

¿Qué es Cisco Spanning Tree?

Cisco Spanning Tree Protocol (STP) es un protocolo de capa 2 que se ejecuta en los switches. Originalmente fue desarrollado para los Bridges (puentes) antecesores a los enrutadores, para evitar bucles. Por esta razón se ve la palabra ¨bridge¨en algunos terminos y configuraciones de STP.

La especificación original para STP es IEEE 802.1D. El objetivo principal de STP es garantizar que no cree bucles cuando tenga rutas redundantes en la red.

Se produce un bucle cuando se envía una trama de un switch a otro switch y, a continuación, de vuelta al switch original. Esto puede suceder si hay dos o más rutas entre dos switches. Cuando

esto sucede, los switches continuarán enviando la trama hacia adelante y hacia atrás, lo que puede causar un atasco de tráfico.

STP evita los bucles deshabilitando los puertos no utilizados. Cuando STP está habilitado, cada switch calcula un Bridge ID. El Bridge ID es una combinación de la dirección MAC del switch y su prioridad. El switch con el Bridge ID más bajo se convierte en el puente raíz.

El root bridge envía BPDU (Bridge Protocol Data Unit) a todos los demás switches. Las BPDU contienen el Bridge ID y el puerto en el que se recibió la BPDU. Cada switch compara la BPDU que recibe con su propio Bridge ID. Si el Bridge ID de la BPDU es menor, el switch marcará el puerto que recibió la BPDU como puerto raíz (root port).

El puerto raíz es el puerto que utiliza el switch para comunicarse con el root Bridge. Todos los demás puertos se consideran puertos no root. Los puertos no root están bloqueados por STP. Esto evita que las tramas se envíen de un lado a otro entre los switches, lo que evita los bucles.

Tipos de STP

1. **802.1D** STP es el protocolo STP original. Es un protocolo de instancia única, lo que significa que solo puede haber una instancia de STP ejecutándose en una red.
2. **802.1w** Rapid STP es una versión más rápida de 802.1D STP. Esto se logra reduciendo el tiempo que lleva converger la red después de un cambio de topología.
3. **PVST+** es un protocolo STP de varias instancias. Esto significa que puede haber varias instancias de STP ejecutándose en una red, cada una con su propio puente raíz. PVST+ se utiliza en redes con enlaces redundantes entre switches.
4. **MSTP** Multiple Spanning Tree Protocol, definido en IEEE 802.1s, permite múltiples instancias de Spanning Tree en un solo switch. Proporciona una mayor flexibilidad al agrupar VLAN en varias instancias de STP, lo que reduce el número de instancias de STP necesarias para redes grandes.

Paso 1: Habilita el modo PVST+ en el switch.

```
switch(config)# spanning-tree mode pvst
```

Paso 2: Configura la prioridad para el switch. Los valores de prioridad más bajos indican una prioridad más alta. La prioridad predeterminada es 32768.

```
switch(config)# spanning-tree vlan vlan-id priority valor-prioridad
```

Ejemplo:

```
switch(config)# spanning-tree vlan 10 priority 4096
```

Paso 3: Configura el puente raíz (root bridge) para cada VLAN. El puente raíz es el puente con el ID de puente más bajo. Por defecto, el switch con la dirección MAC más baja se convierte en el puente raíz para todas las VLAN.

```
switch(config)# spanning-tree vlan vlan-id root primary
```

Ejemplo:

```
switch(config)# spanning-tree vlan 10 root primary
```

Paso 4: Configura el tipo de puerto para cada puerto del switch. Los puertos pueden ser designados como puertos de acceso (access) o puertos troncales (trunk). Los puertos de acceso se

utilizan para dispositivos finales, mientras que los puertos troncales transportan tráfico para múltiples VLAN.

```
Switch(config)# interface id-interfaz
Switch(config-if)# spanning-tree portfast
```

Ejemplo:

```
switch(config)# interface gigabitethernet0/1
switch(config-if)# spanning-tree portfast
```

Paso 5: (Opcional) Configura la prioridad del puerto para cada puerto. Los valores de prioridad más bajos indican una prioridad más alta. La prioridad predeterminada es 128.

```
switch(config)# interface id-interfaz
switch(config-if)# spanning-tree vlan vlan-id port-priority valor-prioridad
```

Ejemplo:

```
switch(config)# interface gigabitethernet0/1
switch(config-if)# spanning-tree vlan 10 port-priority 64
```

8. ETHERCHANNEL

¿Qué es EtherChannel?

EtherChannel es una tecnología de Cisco que le permite combinar múltiples interfaces Ethernet físicas en una sola interfaz lógica. Esto puede aumentar el ancho de banda entre dos dispositivos y proporcionar redundancia en caso de que uno de los enlaces falle.

¿Cómo funciona EtherChannel?

EtherChannel es una tecnología de Cisco que le permite combinar múltiples interfaces Ethernet físicas en una sola interfaz lógica. Esto puede aumentar el ancho de banda entre dos dispositivos y proporcionar redundancia en caso de que uno de los enlaces falle.

Conceptos básicos de EtherChannel:

Antes de profundizar en la configuración, es importante comprender los conceptos fundamentales de EtherChannel. EtherChannel combina varios enlaces físicos en un solo enlace lógico, conocido como "bundle" o "port-channel". Este enlace lógico se comporta como un solo enlace de mayor capacidad y proporciona mayor ancho de banda y redundancia.

Existen dos modos de EtherChannel:

Modo "on":

Todos los enlaces en el EtherChannel deben tener la misma configuración, incluidas las velocidades, los modos dúplex y los VLAN permitidos.
Si se detecta una diferencia en la configuración, el enlace se desactiva.

Modo "desirable":

Permite la formación de un EtherChannel cuando se detecta un dispositivo compatible en el otro extremo.

Se negocian automáticamente las configuraciones de velocidad, modo dúplex y VLAN permitidos.

Configuración de Etherchanel:

Paso 1: Verificar la compatibilidad del equipo y los enlaces:

Asegúrate de que los equipos Cisco involucrados sean compatibles con la tecnología EtherChannel y tengan los módulos o interfaces adecuados para la conexión de los enlaces.

Paso 2: Configurar las interfaces físicas:

Accede al modo de configuración del equipo Cisco a través de la línea de comandos o una interfaz de gestión.

Configura las interfaces físicas que deseas incluir en el EtherChannel. Por ejemplo, si los enlaces son Gigabit Ethernet 1/0/1 y Gigabit Ethernet 1/0/2, ejecuta los siguientes comandos:

```
interface GigabitEthernet1/0/1

channel-group 1 mode on

exit

interface GigabitEthernet1/0/2

channel-group 1 mode on

exit
```

Paso 3: Crear el EtherChannel:

Crea el enlace lógico EtherChannel utilizando el número de grupo especificado en los comandos anteriores. Por ejemplo:

```
interface Port-channel1

switchport mode trunk

switchport trunk allowed vlan 1-10

exit
```

Paso 4: Verificar la configuración y el estado del EtherChannel:

Utiliza el comando "show etherchannel summary" para ver una visión general de todos los EtherChannels configurados en el equipo Cisco.

Para verificar el estado y la configuración específica del EtherChannel creado, utiliza el comando "`show interfaces port-channel 1`".

9. CISCO DISCOVERY PROTOCOL (CDP)

¿Qué es Cisco Discovery Protocol (CDP)?

Cisco Discovery Protocol (CDP) es un protocolo de capa 2 que se ejecuta en dispositivos Cisco, como routers y switches, para descubrir y obtener información sobre otros dispositivos conectados directamente a la red. CDP permite que los dispositivos intercambien información, como el tipo de dispositivo, la dirección IP, el sistema operativo, los números de versión y otros detalles relevantes.

Beneficios de Cisco Discovery Protocol:

Descubrimiento automático: CDP permite que los dispositivos de red descubran automáticamente otros dispositivos vecinos y obtengan información sobre ellos sin necesidad de configuración manual.

Información detallada sobre dispositivos: CDP proporciona información detallada sobre los dispositivos vecinos, como el nombre del dispositivo, el modelo, la dirección IP y los números de versión del software. Esta información es valiosa para el monitoreo y la resolución de problemas en la red.

Administración simplificada: Al conocer la información de los dispositivos vecinos, los administradores de red pueden tomar decisiones informadas sobre la configuración y el mantenimiento de la red. CDP facilita la administración y el monitoreo de la red al proporcionar una visibilidad completa de los dispositivos conectados.

Configuración de Cisco Discovery Protocol:

La configuración de CDP en dispositivos Cisco es relativamente sencilla. A continuación, se muestra un ejemplo de configuración básica en un switch Cisco:

Ingresar al modo de configuración global:

```
switch> enable
```

```
switch# configure terminal
```

Habilitar CDP globalmente:

```
switch(config)# cdp run
```

Opcionalmente, configurar el intervalo de tiempo de actualización de CDP (por defecto es 60 segundos):

```
switch(config)# cdp timer <segundos>
```

Verificar la configuración de CDP:

```
switch(config)# end
```

```
switch# show cdp
```

Este comando mostrará una lista de dispositivos vecinos descubiertos y su información asociada.

Ejemplo de salida:

```
Device ID    Local Intrfce    Holdtme    Capability    Platform    Port ID
```

```
Switch2      Gig 0/1          167        S I           WS-C2960    Gig 0/1
```

10.LINK LAYER DISCOVERY PROTOCOL (LLDP)

Link Layer Discovery Protocol (LLDP) es un protocolo de capa 2 que permite a los dispositivos de red anunciar información sobre sí mismos a otros dispositivos de la red. Esta información puede incluir el nombre del dispositivo, la dirección MAC, la dirección IP y las capacidades. LLDP se puede utilizar para una variedad de propósitos, incluida la resolución de problemas, el inventario de red y la seguridad.

Cisco IOS es compatible con LLDP. Para configurar LLDP en un dispositivo Cisco, puede utilizar los siguientes pasos:

1. Ingrese al modo de configuración global.

2. Utilice el comando lldp run para habilitar LLDP.
3. (Opcional) Utilice el comando lldp timer seconds para especificar el intervalo en el que se envían las actualizaciones de LLDP.
4. (Opcional) Utilice el comando lldp tlv-select para especificar los TLV LLDP que se envían o reciben.
5. Guarde los cambios.

Aquí hay un ejemplo de cómo configurar LLDP en un dispositivo Cisco:

```
configure terminal
lldp run
lldp timer 30
lldp tlv-select system-name, chassis-id, port-id
end
```

Esta configuración habilitará LLDP en todas las interfaces y enviará actualizaciones de LLDP cada 30 segundos. Los TLV de nombre del sistema, ID de chasis e ID de puerto se enviarán con cada actualización.

Una vez habilitado LLDP, puede usar el comando show lldp neighbors para ver información sobre los dispositivos que están conectados a su dispositivo. Esta información se puede utilizar para la resolución de problemas, el inventario de red y la seguridad.

Este es un ejemplo de la salida del comando show lldp neighbors :

```
Device ID: cisco-switch-1
Chassis ID: MAC address: 00:11:22:33:44:55
Port ID: Interface: Gi0/1
Time to live: 120 seconds
```

```
Capabilities: Bridge, Router
Management IP address: 192.168.1.10
```

Esta salida muestra que el dispositivo está conectado a un switch Cisco con la dirección MAC 00:11:22:33:44:55. El switch está conectado a la interfaz Gi0/1 del dispositivo. El switch tiene una dirección IP de administración de 192.168.1.10.

LLDP es una herramienta valiosa para la resolución de problemas de red, inventario y seguridad. Al configurar LLDP en sus dispositivos Cisco, puede obtener información valiosa sobre los dispositivos que están conectados a su red.

11.INTERVLAN ROUTING CON SVIS

Los Switches Virtuales de Interfaz (SVIs, por sus siglas en inglés) son una función clave en los dispositivos de red Cisco que permite la conectividad de capa 3 en una red local. Al configurar un SVI, se crea una interfaz virtual que actúa como una puerta de enlace predeterminada para los dispositivos conectados a ese switch. En este artículo, exploraremos paso a paso cómo configurar SVIs en un switch Cisco.

Paso 1: Acceder al switch:

Lo primero que debemos hacer es acceder al switch Cisco mediante una conexión de red. Puedes utilizar una conexión de consola o acceder a través de una conexión de red remota utilizando Telnet, SSH o la interfaz web del switch.

Paso 2: Ingresar al modo de configuración:

Una vez que hayas iniciado sesión en el switch, debes ingresar al modo de configuración. Para ello, ejecuta el siguiente comando:

```
Switch> enable
Switch# configure terminal
```

Paso 3: Crear la interfaz SVI:

Para crear un SVI, debes asignar un número de VLAN y una dirección IP a la interfaz virtual. Utiliza el siguiente comando para crear la interfaz SVI y asignarle un número de VLAN:

```
switch(config)# interface vlan <numero_vlan>
```

Reemplaza <numero_vlan> por el número de VLAN que deseas asociar con el SVI.

Paso 4: Asignar una dirección IP al SVI:

Una vez creada la interfaz SVI, debemos asignarle una dirección IP. Puedes utilizar el siguiente comando:

```
switch(config-if)# ip address <direccion_ip> <mascara>
```

Reemplaza <direccion_ip> y <mascara> con la dirección IP y la máscara de red que deseas asignar al SVI.

Paso 5: Habilitar el SVI:

Después de asignar la dirección IP, debemos habilitar el SVI utilizando el siguiente comando:

```
switch(config-if)# no shutdown
```

CAPITULO 3 — ROUTING

1. RUTAS ESTATICAS

Las rutas estáticas son una parte esencial de la configuración de redes en equipos Cisco. Permiten a los administradores de red tener un control preciso sobre el flujo de tráfico en la red, dirigiendo paquetes a través de caminos específicos. En este artículo, aprenderemos cómo configurar rutas estáticas en equipos Cisco, y proporcionaremos ejemplos prácticos para ilustrar su implementación.

Paso 1: Acceder al modo de configuración

Para comenzar, debemos acceder al modo de configuración del equipo Cisco. Esto se puede hacer a través de una conexión de consola o a través de una conexión remota utilizando un protocolo como Telnet o SSH. Una vez que estemos conectados al equipo, ingresamos al modo privilegiado ejecutando el comando enable.

Paso 2: Configurar la ruta estática

Una vez en el modo privilegiado, podemos configurar la ruta estática utilizando el comando ip route. La sintaxis básica de este comando es la siguiente:

```
ip route <network> <netmask> <next-hop>
```

Donde:

<network>: especifica la red de destino a la que se enviará el tráfico.

<netmask>: especifica la máscara de red asociada a la red de destino.

<next-hop>: especifica la dirección IP del siguiente salto o destino al que se enviarán los paquetes.

Ejemplo 1: Configuración de una ruta estática predeterminada

Supongamos que queremos configurar una ruta estática predeterminada en un router Cisco con la siguiente información:

Dirección IP del siguiente salto (Next Hop): 192.168.1.1

Para configurar esta ruta estática, ejecutamos el siguiente comando:

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

Este comando envía todos los paquetes con una dirección de destino desconocida a la dirección IP 192.168.1.1.

Ejemplo 2: Configuración de una ruta estática para una red específica

Supongamos que tenemos dos redes: 192.168.1.0/24 y 10.0.0.0/8, y queremos configurar una ruta estática para enrutar el tráfico de la red 10.0.0.0/8 a través del siguiente salto 192.168.1.2.

La configuración de esta ruta estática se realiza con el siguiente comando:

```
ip route 10.0.0.0 255.0.0.0 192.168.1.2
```

Este comando envía todos los paquetes destinados a la red 10.0.0.0/8 al siguiente salto con la dirección IP 192.168.1.2.

Paso 3: Verificar la configuración

Después de configurar las rutas estáticas, es importante verificar que se hayan aplicado correctamente. Para hacer esto, utilizamos el comando `show ip route` que muestra la tabla de enrutamiento del equipo Cisco. Al ejecutar este comando, podremos ver las rutas estáticas configuradas y asegurarnos de que estén activas.

2. OSPF

Paso 1: Acceder al modo de configuración

El primer paso para configurar OSPF en un equipo Cisco es acceder al modo de configuración global. Para ello, conéctate a tu equipo Cisco a través de una sesión de consola o SSH, y luego inicia sesión con las credenciales adecuadas. Una vez que hayas iniciado sesión, ingresa al modo de configuración global escribiendo el siguiente comando:

```
enable
configure terminal
```

Paso 2: Habilitar OSPF en el router

Una vez en el modo de configuración global, debes habilitar OSPF en el router. Esto se logra utilizando el siguiente comando:

```
router ospf <proceso_ID>
```

El <proceso_ID> es un identificador numérico único que especifica el proceso OSPF en el router. Puedes elegir cualquier número que desees, pero asegúrate de usar el mismo proceso_ID en todos los routers dentro del área OSPF.

Paso 3: Configurar las interfaces de red

Después de habilitar OSPF, debes configurar las interfaces de red que participarán en el proceso OSPF. Para ello, ingresa al modo de configuración de interfaz utilizando el siguiente comando:

```
interface <tipo> <número>
```

Reemplaza <tipo> con el tipo de interfaz (por ejemplo, Ethernet, FastEthernet) y <número> con el número de interfaz correspondiente. Una vez en el modo de configuración de interfaz, utiliza el siguiente comando para activar OSPF en la interfaz:

```
ip ospf <proceso_ID> area <número_de_área>
```

El <proceso_ID> debe ser el mismo que especificaste en el paso anterior, y el <número_de_área> representa el número del área OSPF a la cual pertenece la interfaz.

Repite este paso para todas las interfaces de red que deseas agregar al proceso OSPF.

Paso 4: Configurar la red OSPF

Una vez que hayas configurado las interfaces de red, debes especificar las redes que estarán incluidas en el proceso OSPF. Para ello, utiliza el siguiente comando en el modo de configuración OSPF:

```
network <dirección_de_red> <máscara_de_red> area <número_de_área>
```

Reemplaza <dirección_de_red> con la dirección IP de la red y <máscara_de_red> con la máscara de subred correspondiente. El <número_de_área> debe coincidir con el número de área

OSPF que especificaste en el paso anterior. Puedes repetir este comando para cada red que desees agregar al proceso OSPF.

Paso 5: Verificar la configuración OSPF

Una vez completada la configuración OSPF, es importante verificar que todo esté funcionando correctamente. Utiliza los siguientes comandos para obtener información sobre el estado OSPF y verificar la conectividad de la red:

```
show ip protocols
show ip ospf neighbor
show ip ospf interface
show ip route ospf
```

Estos comandos te proporcionarán detalles sobre el estado de OSPF, los vecinos OSPF, las interfaces OSPF y las rutas aprendidas a través de OSPF.

3. HSRP

¿Qué es HSRP?

El Hot Standby Router Protocol (HSRP) es un protocolo de redundancia de primer salto que permite la creación de una puerta de enlace virtual (Virtual Gateway) a través de múltiples routers. HSRP proporciona una dirección IP virtual (Virtual IP) a un grupo de routers y garantiza la transferencia transparente del tráfico de red en caso de que uno de los routers falle. Esto

significa que si el router activo deja de funcionar, otro router de respaldo asume de forma automática su papel y mantiene la continuidad del flujo de datos sin interrupciones.

Configuración básica de HSRP:

A continuación, se presenta un ejemplo de configuración básica de HSRP en equipos Cisco:

Preparación:

Conecta los routers y asegúrate de que se pueda alcanzar la conectividad entre ellos.

Asegúrate de que las interfaces que se utilizarán para HSRP estén correctamente configuradas con las direcciones IP y las máscaras de subred correspondientes.

Configuración del grupo HSRP:

Accede a la interfaz de configuración del router activo (puedes utilizar el comando "configure terminal").

Crea el grupo HSRP con el comando `"standby grupo-numero ip dirección-ip-virtual"`.

Configura la prioridad del router activo con el comando `"standby grupo-numero priority prioridad"`.

Configura la dirección IP real del router activo con el comando `"standby grupo-numero preempt"`.

Configuración del router de respaldo:

Accede a la interfaz de configuración del router de respaldo.

Crea el mismo grupo HSRP con el comando "standby grupo-numero ip dirección-ip-virtual".

Configura la prioridad del router de respaldo con un valor menor al del router activo.

Configura la dirección IP real del router de respaldo con el comando "standby grupo-numero preempt".

Ejemplo práctico de configuración:

Supongamos que tenemos dos routers Cisco, R1 y R2, y deseamos configurar HSRP para garantizar la alta disponibilidad de la puerta de enlace predeterminada en nuestra red. A continuación, se muestra un ejemplo de configuración:

Router R1:

```
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
standby 1 ip 192.168.0.254
standby 1 priority 110
standby 1 preempt
```

Router R2:

```
interface FastEthernet0/0
ip address 192.168.0.2 255.255.255.0
standby 1 ip 192.168.0.254
standby 1 priority 100
standby 1 preempt
```

En este ejemplo, R1 se configura como el router activo con una prioridad de 110, mientras que R2 se configura como el router de respaldo con una prioridad de 100. Si R1 falla, R2 asume automáticamente el papel de router activo y continúa proporcionando conectividad a la red.

CAPITULO 4 — SERVICIOS IP

1. SSH

Para configurar SSH en equipos Cisco, sigue estos pasos:

Conéctate al equipo Cisco a través de una conexión de consola utilizando un cable de consola y un programa de emulación de terminal, como PuTTY o Tera Term.

Accede al modo de configuración global del dispositivo ingresando el siguiente comando:

```
enable
configure terminal
```

Genera una clave RSA para el cifrado SSH utilizando el siguiente comando:

```
crypto key generate rsa
```

Se te solicitará que ingreses el tamaño de la clave. Se recomienda utilizar al menos 1024 bits, aunque 2048 bits ofrecen una mayor seguridad.

Configura el acceso SSH permitiendo solo versiones de protocolo SSH seguras (SSHv2) y definiendo los algoritmos de cifrado que deseas utilizar. Utiliza los siguientes comandos:

```
ip ssh version 2
ip ssh encryption aes256-ctr
ip ssh dh min size 2048
```

Puedes ajustar los algoritmos de cifrado según tus necesidades.

Configura un nombre de usuario y una contraseña para acceder al equipo a través de SSH. Puedes crear un nuevo usuario o utilizar uno existente. Utiliza los siguientes comandos:

```
username <nombre_de_usuario> privilege 15 secret <contraseña>
```

Reemplaza <nombre_de_usuario> con el nombre de usuario que deseas utilizar y <contraseña> con la contraseña correspondiente.

Habilita el acceso SSH en la interfaz de administración a través del siguiente comando:

```
line vty 0 15
transport input ssh
login local
```

Esto permitirá que los usuarios se autentiquen localmente al acceder al equipo a través de SSH.

¡Listo! Ahora deberías poder acceder al equipo Cisco a través de SSH utilizando un cliente SSH, como PuTTY o OpenSSH.

Recuerda que estos pasos son solo una guía general y pueden variar dependiendo del modelo y la versión del sistema operativo del equipo Cisco que estés utilizando. Asegúrate de consultar la documentación oficial de Cisco o los manuales específicos del modelo para obtener instrucciones detalladas y actualizadas.

2. NTP

La sincronización precisa del tiempo es fundamental para el correcto funcionamiento de una red. En entornos de red, como los routers Cisco, el Protocolo de Tiempo de Red (NTP, por sus siglas en inglés) es ampliamente utilizado para garantizar la sincronización precisa de los relojes de los dispositivos. En este artículo, aprenderemos cómo configurar NTP en routers Cisco, paso a paso, y proporcionaremos ejemplos prácticos para una configuración exitosa.

Paso 1: Acceder al modo de configuración

Antes de comenzar con la configuración de NTP, es necesario acceder al modo de configuración del router. Puede hacerse a través de una conexión de consola o mediante una conexión SSH/Telnet. Una vez que haya iniciado sesión en el router, estará listo para comenzar.

Paso 2: Configurar la fuente de tiempo NTP

El siguiente paso es definir la fuente de tiempo NTP a la que el router se sincronizará. Puede elegir entre utilizar servidores NTP públicos o implementar su propio servidor NTP interno. A continuación se muestra un ejemplo de configuración para utilizar servidores NTP públicos:

```
Router(config)# ntp server 0.pool.ntp.org
Router(config)# ntp server 1.pool.ntp.org
Router(config)# ntp server 2.pool.ntp.org
Router(config)# ntp server 3.pool.ntp.org
```

En este ejemplo, hemos configurado cuatro servidores NTP públicos proporcionados por el proyecto "pool.ntp.org". Puede personalizar esta configuración según sus necesidades y preferencias.

Paso 3: Establecer la zona horaria

Es importante establecer la zona horaria correcta en el router para asegurar una sincronización precisa. Para ello, utilice el siguiente comando:

```
Router(config)# clock timezone <nombre de la zona horaria> <desplazamiento UTC>
```

Por ejemplo:

```
Router(config)# clock timezone EST -5
```

Este comando establece la zona horaria como "EST" (Hora estándar del este) con un desplazamiento de -5 horas con respecto al tiempo universal coordinado (UTC).

Paso 4: Habilitar la sincronización NTP

Una vez configuradas las fuentes de tiempo y la zona horaria, es necesario habilitar la sincronización NTP en el router. Utilice el siguiente comando:

```
Router(config)# ntp update-calendar
```

Este comando permite que el reloj del router se sincronice automáticamente con los servidores NTP definidos.

Paso 5: Verificar la configuración

Una vez finalizada la configuración, es importante verificar si la sincronización NTP se ha establecido correctamente. Puede utilizar el siguiente comando para verificar el estado de sincronización:

```
Router# show ntp status
```

Este comando mostrará información detallada sobre el estado de sincronización del reloj del router con los servidores NTP.

3. DHCP

Paso 1: Acceso al router

Antes de comenzar con la configuración del DHCP, debemos acceder al router Cisco a través de una conexión de consola o SSH. Asegúrese de tener los privilegios adecuados para realizar cambios de configuración.

Paso 2: Configuración de la interfaz

El primer paso consiste en configurar la interfaz desde la cual se asignarán las direcciones IP a los dispositivos cliente. Utilizaremos el siguiente ejemplo de configuración para una interfaz FastEthernet 0/1:

```
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

Paso 3: Creación del pool DHCP

Ahora crearemos un pool DHCP para especificar el rango de direcciones IP que se asignarán a los dispositivos cliente. En este ejemplo, crearemos un pool llamado "POOL_DHCP":

```
Router(config)# ip dhcp pool POOL_DHCP
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)# lease 7
```

En el ejemplo anterior, especificamos el rango de direcciones IP que abarca la red 192.168.1.0/24. "default-router" establece la dirección IP del router predeterminado que se enviará a los clientes DHCP. "dns-server" configura la dirección IP del servidor DNS que se

proporcionará a los clientes. "lease" establece la duración de tiempo en días para la asignación de la dirección IP.

Paso 4: Activar DHCP en la interfaz

Para habilitar DHCP en la interfaz configurada anteriormente, utilice el siguiente comando:

```
Router(config)# interface FastEthernet 0/1
Router(config-if)# ip helper-address 192.168.1.1
```

Asegúrese de reemplazar la dirección IP "192.168.1.1" con la dirección IP del router donde se encuentra configurado el pool DHCP.

Paso 5: Verificar la configuración de DHCP

Para verificar la configuración de DHCP en el router Cisco, puede utilizar los siguientes comandos:

```
Router# show ip dhcp binding
```

Este comando mostrará una lista de las direcciones IP asignadas actualmente a los dispositivos cliente y sus respectivas direcciones MAC.

4. SYSLOG

El sistema de registro de eventos, conocido como syslog, es una herramienta esencial para la administración y monitorización de redes. Permite la recolección y almacenamiento de información de eventos críticos, fallos y alertas, lo que resulta fundamental para la resolución de

problemas, la toma de decisiones informadas y el mantenimiento proactivo de la red. En este artículo, exploraremos cómo configurar syslog en routers Cisco, brindando ejemplos claros y prácticos para ayudarte a implementar esta función de vital importancia.

¿Qué es Syslog y por qué es importante en los routers Cisco?

Syslog es un protocolo estándar que permite la recopilación y gestión de registros de eventos en dispositivos de red. En el caso de los routers Cisco, la configuración de syslog es fundamental para el seguimiento de eventos importantes, como caídas del sistema, cambios de configuración, intentos de acceso no autorizados y otros problemas críticos. Al configurar correctamente syslog en un router Cisco, podrás recibir alertas en tiempo real, analizar los eventos registrados y tomar medidas para solucionar cualquier problema o amenaza.

Pasos para configurar Syslog en routers Cisco:

A continuación, te presentamos los pasos necesarios para configurar syslog en routers Cisco:

Paso 1: Acceder al modo de configuración

Para comenzar, inicia una sesión de administración en el router Cisco y accede al modo de configuración.

Paso 2: Configurar la dirección IP del servidor Syslog

Utiliza el siguiente comando para especificar la dirección IP del servidor Syslog al que deseas enviar los registros de eventos:

```
Router(config)# logging host <dirección_IP_servidor_syslog>
```

Paso 3: Establecer niveles de registro

Puedes configurar diferentes niveles de registro para determinar qué tipo de eventos se registrarán y enviarán al servidor Syslog. Utiliza el siguiente comando para establecer el nivel de registro deseado:

```
Router(config)# logging trap <nivel>
```

Paso 4: Configurar el origen de los registros

Elige qué tipos de eventos se registrarán. Puedes especificar diferentes fuentes para los registros utilizando el siguiente comando:

```
Router(config)# logging source-interface <interfaz>
```

Paso 5: Verificar y guardar la configuración

Para verificar la configuración actual de syslog, utiliza el siguiente comando:

```
Router# show logging
```

Si todo está configurado correctamente, guarda la configuración para que persista después de un reinicio utilizando el siguiente comando:

Ejemplos prácticos:

A continuación, te presentamos algunos ejemplos prácticos de configuración de syslog en routers Cisco:

Ejemplo 1: Configuración básica de Syslog:

```
Router(config)# logging host 192.168.1.100
```

```
Router(config)# logging trap notifications
Router(config)# logging source-interface GigabitEthernet0/0
Router(config)# end
```

Ejemplo 2: Configuración avanzada de Syslog:

```
Router(config)# logging host 10.0.0.1
Router(config)# logging trap informational
Router(config)# logging source-interface Loopback0
Router(config)# end
```

5. SNMP

SNMP es un protocolo de administración de red que le permite monitorear y administrar dispositivos de red. Utiliza un mecanismo simple de consulta-respuesta para recuperar información de los dispositivos y enviar notificaciones cuando ocurren ciertos eventos.
Antes de comenzar la configuración de SNMP en un router Cisco, es importante comprender los componentes básicos de SNMP, que incluyen:

Agentes SNMP: estos son los programas o módulos instalados en los dispositivos de red que recopilan y almacenan información de administración.
Administradores SNMP: son las aplicaciones o sistemas utilizados para controlar y monitorear los agentes SNMP.

MIB (Management Information Base): es una base de datos jerárquica que contiene información sobre los dispositivos administrados.

Comandos SNMP

Algunos de los comandos SNMP más comunes incluyen:

`snmp-server community`: Este comando configura la cadena de comunidad SNMP. La cadena de comunidad es una contraseña que se utiliza para autenticar solicitudes SNMP.

`snmp-server host`: Este comando configura la cadena de comunidad SNMP. La cadena de comunidad es una contraseña que se utiliza para autenticar solicitudes SNMP.

`snmp-server enable traps`: Este comando configura la cadena de comunidad SNMP. La cadena de comunidad es una contraseña que se utiliza para autenticar solicitudes SNMP

`show snmp`: Este comando muestra la configuración SNMP actual.

`show snmp traps`: Este comando muestra la configuración SNMP actual.

Este comando muestra la configuración SNMP actual.

```
snmp-server community public
```

Para configurar el host SNMP en 192.168.1.100:

```
snmp-server host 192.168.1.100
```

Para habilitar capturas SNMP para eventos de enlace arriba/abajo:

```
snmp-server enable traps linkup linkdown
```

Para mostrar la configuración SNMP actual:

```
show snmp
```

Para mostrar las capturas SNMP actuales:

```
show snmp traps
```

6. NAT

La traducción de direcciones de red, conocida como NAT (Network Address Translation), es una técnica que termite que las redes con direcciones IP privadas se conecten y comuniquen con la Internet pública utilizando direcciones IP públicas.

Modos de operación NAT:

Existen dos modos de operación principales en NAT: inside y outside. Estos modos se refieren a la relación entre las direcciones IP privadas y públicas en un entorno NAT.

Inside: Se refiere a las direcciones IP privadas utilizadas en una red local interna. Los dispositivos en modo inside son traducidos a direcciones IP públicas cuando se comunican con la red externa (outside).

Outside: Se refiere a las direcciones IP públicas utilizadas en la red externa, generalmente la Internet. Los dispositivos en modo outside son aquellos con direcciones IP públicas que se comunican con la red interna.

Variantes de NAT:

Existen diferentes variantes de NAT, cada una con sus características particulares:

NAT estático: En este tipo de NAT, se realiza una traducción uno a uno de direcciones IP internas a direcciones IP públicas estáticas. Esto es útil cuando se necesita asignar una dirección IP pública específica a un dispositivo interno, como un servidor web.

NAT dinámico: En NAT dinámico, las direcciones IP internas se traducen a direcciones IP públicas dinámicamente a medida que los paquetes salen de la red interna hacia la red externa. Esto permite compartir una cantidad limitada de direcciones IP públicas entre múltiples dispositivos internos.

NAT overload (PAT): También conocido como Port Address Translation, este tipo de NAT permite la traducción de múltiples direcciones IP internas a una única dirección IP pública utilizando diferentes puertos. El PAT es ampliamente utilizado para permitir que múltiples dispositivos compartan una única dirección IP pública.

Configuracion de NAT

Paso 1: Configuración de interfaces

Antes de comenzar con la configuración de NAT estático, es necesario configurar las interfaces de red correspondientes en el router Cisco. Esto implica asignar las direcciones IP internas y externas a las interfaces respectivas.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_interna> <máscara_de_red_interna>
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_externa> <máscara_de_red_externa>
Router(config-if)# exit
```

Paso 2: Creación de una lista de acceso

A continuación, es necesario crear una lista de acceso (ACL) para definir las direcciones IP que serán traducidas mediante NAT estático. La ACL permitirá el tráfico desde la dirección IP interna hacia la dirección IP externa.

```
Router(config)# access-list <nombre_de_ACL> permit <dirección_IP_interna>
```

Paso 3: Creación de una entrada NAT estática

Una vez que la ACL se ha configurado, se debe crear una entrada NAT estática para asociar la dirección IP interna con la dirección IP externa. Esto se realiza mediante el uso del comando `ip nat inside source static`.

```
Router(config)# ip nat inside source static <dirección_IP_interna>
<dirección_IP_externa>
```

Paso 4: Vinculación de la lista de acceso y la entrada NAT

Finalmente, es necesario vincular la lista de acceso y la entrada NAT estática al modo de interfaz correspondiente.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip nat outside
Router(config-if)# exit
```

¡

La configuración de NAT estático ha sido completada! Ahora, el router Cisco traducirá automáticamente la dirección IP interna especificada a la dirección IP externa asignada cada vez que el tráfico salga de la red interna hacia la red externa.

Es importante destacar que estos son solo pasos básicos para configurar NAT estático en equipos Cisco. Dependiendo de la topología de red y los requisitos específicos, pueden ser necesarias configuraciones adicionales, como rutas estáticas o ajustes de firewall. Siempre es recomendable consultar la documentación oficial de Cisco y seguir las mejores prácticas de configuración de seguridad.

Ejemplo de configuración de NAT estático:

Supongamos que tenemos un servidor web interno con la dirección IP 192.168.1.10 que deseamos traducir a una dirección IP pública estática 203.0.113.10. La configuración sería la siguiente:

```
Router(config)# interface <nombre_de_interfaz_interna>
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz_externa>
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# exit

Router(config)# access-list 1 permit 192.168.1.10

Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10

Router(config)# interface <nombre_de_interfaz_interna>
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz_externa>
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Configuración de NAT dinámico

El NAT dinámico, también conocido como NAT overload o NAT de sobrecarga, es ampliamente utilizado para permitir que múltiples dispositivos internos compartan una única dirección IP pública. A continuación, se describen los pasos para configurar NAT dinámico en equipos Cisco.

Paso 1: Configuración de interfaces

Antes de comenzar con la configuración de NAT dinámico, es necesario configurar las interfaces de red correspondientes en el router Cisco. Esto implica asignar las direcciones IP internas y externas a las interfaces respectivas.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_interna> <máscara_de_red_interna>
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_externa> <máscara_de_red_externa>
Router(config-if)# exit
```

Paso 2: Configuración del pool de direcciones IP

A continuación, se debe crear un pool de direcciones IP que serán asignadas dinámicamente a los dispositivos internos. Estas direcciones IP deben ser públicas y pueden ser proporcionadas por el proveedor de servicios de Internet (ISP).

```
Router(config)# ip nat pool <nombre_del_pool> <dirección_IP_inicial>
<dirección_IP_final> netmask <máscara_de_red_externa>
```

Paso 3: Creación de una lista de acceso

Se necesita una lista de acceso (ACL) para definir qué direcciones IP internas serán traducidas mediante NAT dinámico. La ACL permitirá el tráfico desde las direcciones IP internas hacia la dirección IP externa.

```
Router(config)# access-list <nombre_de_ACL> permit <dirección_IP_interna>
<máscara_de_red_interna>
```

Paso 4: Configuración de la sobrecarga NAT

A continuación, se debe configurar la sobrecarga NAT utilizando el comando ip nat inside source list junto con el pool de direcciones IP previamente creado.

```
Router(config)# ip nat inside source list <nombre_de_ACL> pool
<nombre_del_pool> overload
```

Paso 5: Vinculación de la lista de acceso y la interfaz

Finalmente, es necesario vincular la lista de acceso y la interfaz al modo correspondiente (inside o outside) en función de si son direcciones IP internas o externas.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
```

```
Router(config-if)# ip nat outside
Router(config-if)# exit
```

En este punto la configuración esta lista, ahora, el router Cisco asignará dinámicamente direcciones IP públicas del pool a medida que los dispositivos internos envíen tráfico hacia la red externa. Esto permite compartir una única dirección IP pública entre múltiples dispositivos internos.

Ejemplo de configuración de NAT dinámico:

Supongamos que tenemos una red interna con direcciones IP privadas en el rango 192.168.1.0/24 y queremos traducir estas direcciones a una dirección IP pública asignada por el ISP. La configuración sería la siguiente:

```
Router(config)# interface <nombre_de_interfaz_interna>
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz_externa>
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# exit

Router(config)# ip nat pool pool-publico 203.0.113.10 203.0.113.20 netmask
255.255.255.0

Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

```
Router(config)# ip nat inside source list 1 pool pool-publico overload


Router(config)# interface <nombre_de_interfaz_interna>
Router(config-if)# ip nat inside
Router(config-if)# exit


Router(config)# interface <nombre_de_interfaz_externa>
Router(config-if)# ip nat outside
Router(config-if)# exit
```

Estos son solo ejemplos básicos de configuración de NAT en equipos Cisco. Es importante adaptarlos a la topología de red y los requisitos específicos de cada entorno. Además, es recomendable implementar medidas de seguridad adicionales, como firewalls y listas de acceso, para proteger la red de posibles amenazas.

Recuerda consultar la documentación oficial de Cisco y seguir las mejores prácticas de configuración para obtener un entorno de red seguro y eficiente.

Configuración de NAT overload (PAT)

Paso 1: Configuración de interfaces

Antes de comenzar con la configuración de NAT dinámico, es necesario configurar las interfaces de red correspondientes en el router Cisco. Esto implica asignar las direcciones IP internas y externas a las interfaces respectivas.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_interna> <máscara_de_red_interna>
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip address <dirección_IP_externa> <máscara_de_red_externa>
Router(config-if)# exit
```

Paso 2: Configuración del pool de direcciones IP

A continuación, se debe crear un pool de direcciones IP que serán asignadas dinámicamente a los dispositivos internos. Estas direcciones IP deben ser públicas y pueden ser proporcionadas por el proveedor de servicios de Internet (ISP).

```
Router(config)# ip nat pool <nombre_del_pool> <dirección_IP_inicial>
<dirección_IP_final> netmask <máscara_de_red_externa>
```

Paso 3: Creación de una lista de acceso

Se necesita una lista de acceso (ACL) para definir qué direcciones IP internas serán traducidas mediante NAT dinámico. La ACL permitirá el tráfico desde las direcciones IP internas hacia la dirección IP externa.

```
Router(config)# access-list <nombre_de_ACL> permit <dirección_IP_interna>
<máscara_de_red_interna>
```

Paso 4: Configuración de la sobrecarga NAT

A continuación, se debe configurar la sobrecarga NAT utilizando el comando ip nat inside source list junto con el pool de direcciones IP previamente creado.

```
Router(config)# ip nat inside source list <nombre_de_ACL> pool
<nombre_del_pool> overload
```

Paso 5: Vinculación de la lista de acceso y la interfaz

Finalmente, es necesario vincular la lista de acceso y la interfaz al modo correspondiente (inside o outside) en función de si son direcciones IP internas o externas.

```
Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface <nombre_de_interfaz>
Router(config-if)# ip nat outside
Router(config-if)# exit
```

En este punto las configuración de NAT overload esta lista y el router Cisco asignará dinámicamente direcciones IP públicas del pool a medida que los dispositivos internos envíen tráfico hacia la red externa. Esto permite compartir una única dirección IP pública entre múltiples dispositivos internos.

7. CALIDAD DE SERVICIO (QOS)

La implementación de QoS en equipos Cisco implica la configuración de varios componentes clave, como clasificación, marcado, encolamiento y administración de ancho de banda. La clasificación permite identificar y diferenciar diferentes tipos de tráfico en función de sus características, como la prioridad, el protocolo o el origen y destino. El marcado implica agregar información específica (como etiquetas o valores DSCP) a los paquetes para indicar su prioridad. El encolamiento determina cómo se almacenan y priorizan los paquetes en la cola de salida. Y, finalmente, la administración de ancho de banda permite asignar y controlar la cantidad de ancho de banda disponible para cada tipo de tráfico.

Ejemplos de configuración de QoS en equipos Cisco:

1 Configuración de clasificación:

Para ilustrar la configuración de clasificación, supongamos que queremos priorizar el tráfico de voz en una red VoIP. Podemos utilizar el siguiente comando en un router Cisco para clasificar los paquetes de voz basados en su protocolo:

```
class-map voice
 match protocol rtp audio
```

Este comando crea una clase llamada "voice" que coincide con los paquetes de voz RTP (Real-time Transport Protocol) y audio.

2 Configuración de marcado:

Una vez que hemos clasificado el tráfico, necesitamos marcarlo para que pueda recibir un trato prioritario. A continuación, se muestra un ejemplo de marcado de tráfico de voz utilizando valores DSCP (Differentiated Services Code Point):

```
policy-map voice-qos
 class voice
  set dscp ef
```

Este comando crea una política llamada "voice-qos" que marca los paquetes clasificados como "voice" con el valor DSCP EF (Expedited Forwarding).

3 Configuración de encolamiento:

La configuración del encolamiento determina cómo se manejan los paquetes en la cola de salida. A continuación, se presenta un ejemplo de configuración para utilizar el encolamiento FIFO (First-In, First-Out) en una interfaz de salida:

```
interface GigabitEthernet0/1
 service-policy output voice-qos
```

Este comando aplica la política "voice-qos" a la interfaz GigabitEthernet0/1, lo que significa que los paquetes marcados como "voice" serán encolados y transmitidos utilizando el encolamiento FIFO.

4 Configuración de administración de ancho de banda:

La administración de ancho de banda es esencial para asignar recursos de manera adecuada a cada tipo de tráfico. A continuación, se muestra un ejemplo de cómo limitar el ancho de banda para el tráfico de datos a 1 Mbps en una interfaz:

```
policy-map data-qos
 class class-default
  shape average 1000000
```

Este comando crea una política llamada "data-qos" que limita el ancho de banda de la clase predeterminada a 1 Mbps.

CAPITULO 5 — SEGURIDAD

1. LISTAS DE ACCESO ESTANDAR Y EXTENDIDAS

¿Qué son las listas de acceso?

Las listas de acceso, también conocidas como ACL por sus siglas en inglés (Access Control Lists), son herramientas utilizadas para controlar el flujo de tráfico en una red. Permiten especificar qué tipo de tráfico se permite o se niega en función de criterios como direcciones IP, rangos de puertos y protocolos. Las listas de acceso se aplican a interfaces de red específicas y se

evalúan en orden, lo que significa que la primera regla que coincida con el tráfico determinará si se permite o se deniega el acceso.

Tipos de listas de acceso:

En los equipos Cisco, existen dos tipos principales de listas de acceso: las listas de acceso estándar y las listas de acceso extendido. Las listas de acceso estándar se utilizan principalmente para filtrar direcciones IP, mientras que las listas de acceso extendido ofrecen mayor flexibilidad al permitir filtrar por puertos y protocolos adicionales.

Configuración de listas de acceso estándar:

Para configurar una lista de acceso estándar en un equipo Cisco, se utiliza el siguiente comando:

```
access-list numero [deny | permit] source [source-wildcard]
```

Donde "numero" es el número de la lista de acceso, "deny" o "permit" indican si se debe denegar o permitir el tráfico, "source" es la dirección IP de origen y "source-wildcard" es la máscara de wildcard que define el rango de direcciones IP.

Por ejemplo, para permitir el tráfico de la dirección IP 192.168.1.0/24, se utilizaría el siguiente comando:

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

Configuración de listas de acceso extendido:

Las listas de acceso extendido permiten una mayor granularidad al filtrar el tráfico. Además de las direcciones IP, se pueden especificar puertos y protocolos específicos. El comando para configurar una lista de acceso extendido es el siguiente:

```
access-list numero [deny | permit] protocol source [source-wildcard]
destination [destination-wildcard] [eq port]
```

Donde "numero" es el número de la lista de acceso, "deny" o "permit" indica si se debe denegar o permitir el tráfico, "protocol" es el protocolo que se quiere filtrar (por ejemplo, TCP o UDP), "source" es la dirección IP de origen, "source-wildcard" es la máscara de wildcard para la dirección IP de origen, "destination" es la dirección IP de destino, "destination-wildcard" es la máscara de wildcard para la dirección IP de destino y "port" es el puerto que se quiere filtrar.

Por ejemplo, para permitir el tráfico TCP desde la dirección IP 192.168.1.0/24 al puerto 80 en la dirección IP de destino 10.0.0.1, se utilizaría el siguiente comando:

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 10.0.0.1 0.0.0.0 eq 80
```

Aplicación de listas de acceso:

Una vez que se han configurado las listas de acceso, se deben aplicar a las interfaces de red pertinentes utilizando el siguiente comando:

```
interface interface-name
ip access-group numero {in | out}
```

Donde "interface-name" es el nombre de la interfaz a la que se aplicará la lista de acceso, "numero" es el número de la lista de acceso y "in" o "out" indica si se aplicará a los paquetes entrantes o salientes.

2. LISTAS DE ACCESO NOMBRADAS

¿Qué son las Listas de Acceso con Nombre?

Las Listas de Acceso con Nombre, también conocidas como ACL con nombre, son una característica introducida por Cisco que permite asignar un nombre descriptivo a una lista de acceso. En lugar de utilizar números para identificar las listas de acceso, se les asigna un nombre significativo, lo que facilita su gestión y comprensión. Las Listas de Acceso con Nombre ofrecen la misma funcionalidad que las listas de acceso estándar y extendido, pero con una sintaxis más intuitiva.

Ventajas de las Listas de Acceso con Nombre:

Legibilidad mejorada: Los nombres descriptivos de las Listas de Acceso con Nombre facilitan la comprensión y el mantenimiento de la configuración de seguridad.
Flexibilidad: Las Listas de Acceso con Nombre admiten reglas adicionales y opciones de configuración más avanzadas que las listas de acceso estándar y extendido.
Reutilización: Puedes aplicar la misma lista de acceso con nombre a múltiples interfaces, lo que simplifica la administración y reduce la posibilidad de errores.

Configuración de Listas de Acceso con Nombre:

La configuración de una Lista de Acceso con Nombre en un equipo Cisco implica los siguientes pasos:

1 Crear la lista de acceso con nombre:

```
ip access-list standard nombre-lista
```

Donde "nombre-lista" es el nombre descriptivo que se asigna a la lista de acceso con nombre.

2 Configurar las reglas de la lista de acceso con nombre:

```
permit|deny source [source-wildcard]
```

Aquí, "permit" o "deny" indica si se permite o se deniega el tráfico, "source" es la dirección IP de origen y "source-wildcard" es la máscara de wildcard que define el rango de direcciones IP.

Por ejemplo, para permitir el tráfico de la dirección IP 192.168.1.0/24, se utilizaría el siguiente comando:

```
ip access-list standard nombre-lista
permit 192.168.1.0 0.0.0.255
```

Aplicación de Listas de Acceso con Nombre:

Una vez que se ha creado la lista de acceso con nombre, se puede aplicar a las interfaces de red correspondientes utilizando el siguiente comando:

```
interface interface-name
ip access-group nombre-lista {in | out}
```

Aquí, "interface-name" es el nombre de la interfaz a la que se aplicará la lista de acceso con nombre, y "in" o "out" indica si se aplicará a los paquetes entrantes o salientes.

Por ejemplo, para aplicar la lista de acceso con nombre "nombre-lista" a los paquetes entrantes en la interfaz GigabitEthernet0/1, se utilizaría el siguiente comando:

```
interface GigabitEthernet0/1
ip access-group nombre-lista in
```

3. PORT SECURITY

¿Qué es Port Security?

Port Security es una función de seguridad que se utiliza para restringir el acceso a los puertos de los switches Cisco. Permite limitar el número de direcciones MAC (Media Access Control) que pueden acceder a un puerto específico. Cuando se configura Port Security, los puertos solo aceptarán tráfico de los dispositivos con las direcciones MAC permitidas. Esto ayuda a prevenir

ataques de suplantación de identidad y asegura que solo los dispositivos autorizados tengan acceso a la red.

Configuración de Port Security:

La configuración de Port Security en equipos Cisco implica los siguientes pasos:

Habilitar Port Security en un puerto:

Para habilitar Port Security en un puerto específico, debemos ingresar al modo de configuración del switch y ejecutar el siguiente comando:

```
Switch(config)# interface <interface-id>
Switch(config-if)# switchport port-security
```

Este comando habilitará Port Security en el puerto especificado.

Configurar el número máximo de direcciones MAC permitidas:

Una vez habilitado Port Security, podemos establecer el número máximo de direcciones MAC permitidas en el puerto. Por ejemplo, si deseamos permitir solo una dirección MAC en el puerto, ejecutamos el siguiente comando:

```
Switch(config-if)# switchport port-security maximum 1
```

Esto asegurará que solo una dirección MAC sea permitida en el puerto.

Configurar la acción en caso de violación de seguridad:

Si una violación de seguridad ocurre, es importante establecer una acción específica que se llevará a cabo. Podemos elegir entre tres acciones principales: "shutdown", "protect" o "restrict".

"Shutdown": Esta acción deshabilitará el puerto en caso de violación de seguridad.

"Protect": Esta acción ignorará los paquetes que provienen de direcciones MAC no autorizadas.

"Restrict": Esta acción registra la violación en los registros, pero permite el tráfico.

Para configurar una acción, usamos el siguiente comando:

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

Ejemplos prácticos:

Configuración básica de Port Security:

Supongamos que queremos habilitar Port Security en el puerto FastEthernet 0/1 del switch Cisco y permitir solo una dirección MAC. Además, configuraremos la acción de violación como "shutdown".

```
Switch(config)# interface FastEthernet 0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation shutdown
```

Configuración de Port Security con restricciones adicionales:

En este ejemplo, habilitaremos Port Security en el puerto GigabitEthernet 0/1 y permitiremos dos direcciones MAC. Además, estableceremos la acción de violación como "protect".

```
Switch(config)# interface GigabitEthernet 0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation protect
```

4. DHCP SNOOPING

El Dynamic Host Configuration Protocol (DHCP) es una tecnología ampliamente utilizada para asignar direcciones IP de manera dinámica en redes IP. Sin embargo, en entornos de red no seguros, los ataques de Rogue DHCP pueden ser una amenaza importante. Los equipos Cisco ofrecen una solución eficaz para combatir estos ataques: DHCP Snooping. En este artículo, exploraremos cómo configurar DHCP Snooping en equipos Cisco y proporcionaremos ejemplos prácticos para proteger tu red contra los ataques de Rogue DHCP.

Fundamentos de DHCP Snooping

El DHCP Snooping es una función de seguridad que valida y registra los mensajes DHCP intercambiados entre los clientes DHCP y los servidores DHCP. Al habilitar DHCP Snooping, los switches Cisco pueden crear una base de datos confiable de direcciones IP asignadas a clientes legítimos. Además, DHCP Snooping puede bloquear o descartar paquetes DHCP no autorizados provenientes de fuentes no confiables, como servidores DHCP maliciosos.

Configuración de DHCP Snooping en equipos Cisco

Habilitar DHCP Snooping:

```
Switch(config)# ip dhcp snooping
```

```
Configurar las interfaces confiables:
```

```
Switch(config)# interface <interfaz>
Switch(config-if)# ip dhcp snooping trust
```

Opcional: configurar la detección de ataques DHCP:

```
Switch(config)# ip dhcp snooping information option
```

Opcional: configurar la vigilancia de DHCP binding:

```
Switch(config)# ip dhcp snooping database <nombre-de-base-de-datos>
```

Verificar la configuración:

```
Switch# show ip dhcp snooping
```

Ejemplos prácticos

Configuración básica de DHCP Snooping:

```
Switch(config)# ip dhcp snooping
Switch(config)# interface range gigabitEthernet 1/0/1-24
Switch(config-if-range)# ip dhcp snooping trust
```

Configuración con detección de ataques DHCP:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping information option
```

Configuración con vigilancia de DHCP binding:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping database dhcp_binding
```

5. AAA

La autenticación, autorización y contabilidad (AAA) son componentes esenciales en la seguridad de redes. Los equipos Cisco, reconocidos por su fiabilidad y funcionalidad, ofrecen un amplio conjunto de características para implementar AAA de manera efectiva. En este artículo, exploraremos la configuración de AAA en equipos Cisco, proporcionando una guía práctica acompañada de ejemplos concretos.

Autenticación:

La autenticación es el primer paso en un sistema AAA y garantiza que los usuarios sean quienes dicen ser antes de permitirles el acceso a la red. En equipos Cisco, existen diferentes métodos de autenticación, entre ellos:

a) Autenticación basada en contraseñas:

Uno de los métodos más comunes es la autenticación basada en contraseñas. A través del comando username, podemos crear cuentas de usuario con contraseñas asociadas. A continuación, se muestra un ejemplo de configuración:

```
username usuario1 privilege 15 password 0 contraseña123
```

b) Autenticación basada en servidores RADIUS:

Cisco también admite la autenticación a través de servidores RADIUS, que proporcionan una gestión centralizada de usuarios. Aquí hay un ejemplo de configuración para la autenticación RADIUS:

```
aaa new-model
aaa authentication login default group radius
aaa authentication enable default group radius
radius-server host 192.168.1.1
radius-server key clave_secreta
```

Autorización:

Una vez que los usuarios han sido autenticados, el siguiente paso es determinar qué recursos y servicios pueden utilizar en la red. La autorización permite aplicar políticas específicas basadas en roles o privilegios. Veamos algunos ejemplos de configuración:

a) Autorización basada en niveles de privilegio:

En equipos Cisco, los niveles de privilegio van del 0 al 15, donde 0 es el nivel más bajo y 15 el más alto. Podemos asignar niveles de privilegio a los usuarios utilizando el comando privilege. A continuación, se muestra un ejemplo:

```
username usuario1 privilege 15 password 0 contraseña123
```

b) Autorización basada en grupos:

Los grupos de autorización permiten agrupar usuarios con permisos similares. Podemos configurar grupos de autorización utilizando el comando aaa authorization. Aquí hay un ejemplo:

```
aaa authorization exec default group radius if-authenticated
aaa authorization commands 15 default group radius if-authenticated
```

Contabilidad:

La contabilidad registra el uso de los recursos de red por parte de los usuarios y es útil para el seguimiento y el cumplimiento de políticas. Cisco ofrece varias opciones para la contabilidad, incluyendo:

a) Contabilidad local:

La contabilidad local almacena los registros en el propio equipo Cisco. Aquí hay un ejemplo de configuración:

```
aaa accounting exec default start-stop group radius
aaa accounting commands 15 default start-stop group radius
```

b) Contabilidad basada en servidores RADIUS:

También podemos utilizar servidores RADIUS para el registro de contabilidad. Aquí hay un ejemplo de configuración:

```
radius-server accounting host 192.168.1.1
radius-server accounting key clave_secreta
```