Configuración básica en Router

Evitar que el enrutador intente resolver comandos ingresados incorrectamente como nombres de dominio	*Router(config)#no ip domain lookup*
Configurar el nombre de host de R1.	*Router(config)#hostname R1*
Configurar un banner MOTD apropiado.	*R1(config)#banner motd #Unauthorized Access is Prohibited#*
Configurar la contraseña de la consola y habilitar conexiones	*R1(config)#line console 0* *R1(config-line)#password ciscoconpass* *R1(config-line)#login* *R1(config-line)#exit*
Configurar una contraseña secreta de habilitación.	*R1(config)#enable secret ciscoenpass*
Encriptar todas las contraseñas en texto claro.	*R1(config)#service password-encryption*
Establecer la longitud mínima de las contraseñas recién creadas en 10 caracteres.	*R1(config)#security passwords min-length 10*

Configuración SSH

Crear un usuario administrativo en la base de datos de usuarios locales.	*R1(config)#username admin secret admin1pass*
Ingresar al Switch mediante telnet	*telnet <direccion_ip_del_S1>*
Cifrar contraseñas de texto no cifrado	*S1(config)# service password-encryption*
Verificar que las contraseñas estén cifradas	*S1# show running-config*
1. Establecer el nombre de dominio IP	*S1(config)# ip domain-name netacad.pka*
2. Generar claves RSA con una longitud de clave de 1024	*S1(config)# crypto key generate rsa general-keys modulus 1024*
3. Cree un usuario de SSH	*S1(config)# username admin password cisco*
4. Accede al modo de configuración de líneas VTY	*S1(config)# line vty 0 15*
5. Configura las líneas VTY para que solo permitan acceso mediante SSH:	*S1(config-line)# transport input ss*h
6. Elimina cualquier contraseña existente en las líneas VTY con el siguiente comando:	*S1(config-line)# no password* *S1(config-line)# login*
7. Verificar la implementación SSH	*PC : SSH -l username {target ip}*

Configuración de VLAN

Crear VLAN con número ID válido	*Switch(config)# vlan vlan-id*
Especificar nombre para identificar VLAN	*Switch(config-vlan)# name vlan-name*
Ingrese al modo de configuración de interfaz	*Switch(config)# interface interface-id*
Establezca el puerto en modo de acceso	*Switch(config-if)# switchport mode access*
Asigne el puerto a una VLAN	*Switch(config-if)# switchport access vlan vlan-id*
Encienda la interfaz	*Switch(config-if)# no shutdown*

Verificar información de la VLAN

Muestra nombre de la VLAN, el estado y sus puertos	*show vlan brief*
Muestra info sobre el número de ID de VLAN identificado.	*show vlan id vlan-id*
Muestra info sobre el número de ID de VLAN identificado	*show vlan name vlan-name*
Mostrar el resumen de información de la VLAN	*show vlan summary*

Comandos de Configuración troncal

Ingrese al modo de configuración de interfaz	*Switch(config)# interface interface-id*
Establezca el puerto en modo de enlace troncal permanente	*Switch(config-if)# switchport mode trunk*
Cambie la configuración de VLAN nativa a otra que no sea la VLAN1	*Switch(config-if)# switchport trunk native vlan vlan-id*
Especifique la lista de VLAN que se permitirán en el enlace troncal	*Switch(config-if)# switchport trunk allowed vlan vlan-list*
Mostrar configuración de la interfaz	*show interfaces fa0/1 switchport*
Eliminar las VLAN permitidas	*Switch(config-if)# no switchport trunk allowed vlan*
Restablecer la VLAN nativa del enlace troncal	*Switch(config-if)# no switchport trunk native vlan*
Verificar el modo DTP de la interface	*S1# show dtp interface fa0/1|*

Configuración Router-on-a-stick VLAN Routing

Crear y nombrar las VLANs	*S2(config)# vlan 10* *S2(config-vlan)# name LAN10*
Crear la interfaz de administración	*S2(config)# vlan 99* *S2(config-vlan)# name management* *S2(config)# interface vlan 99* *S2(config-if)# ip add 192.168.99.1 255.255.255.0* *S2(config-if)# no shutdown*
Configurar gateway	*S2(config)# ip default-gateway 192.168.99.1*
Configurar puertos de accesos	*S2(config-if)# switchport mode access*
Configurar puertos de enlace troncal	*S2(config-if)# switchport mode trunk*
Configurar sub-interfaces del Router	*R1(config)# interface G0/0/1.10* *R1(config-subif)# Description Default Gateway for VLAN 10* *R1(config-subif)# encapsulation dot1Q 10* *R1(config-subif)# Ip add 192.168.10.1 255.255.255.0*
Definir la interfaz física como trunk y encenderla	*R1(config)# interface G0/0/1* *R1(config-if)# no shutdown*
Mostrar todas las rutas que “ve” el router	*Show ip route*
Ver configuración troncal	*Show interfaces trunk*

Spanning-Tree Protocol

Pasar del modo de STP básico al Rapid STP o MSTP	*S1(config)# Spanning-tree mode rapid-psvt*
Elegir Root Bridge dándole prioridad	*S1(config)# spanning-tree VLAN 1 priority 4096*

Configuración VLAN Routing con Switch de capa 3

Crear y nombrar las VLANs	*D1(config)# vlan 10* *D1(config-vlan)# name LAN10*
Crear las interfaces VLAN SVI y asignar dirección de Gateway.	*D1(config)# interface vlan 10* *D1(config-if)# description Default Gateway SVI for 192.168.10.0/24* *D1(config-if)# ip add 192.168.10.1 255.255.255.0* *D1(config-if)# no shut*
Configurar puertos de acceso (esto podría hacerse en un switch de capa 2 si es que el mismo es quien está conectado a los host. Depende de la topología).	*D1(config)# interface G1/0/6* *D1(config-if)# Description access port to PC1* *D1(config-if)# switchport mode access* *D1(config-if)# switchport access vlan 10*
Habilitar IP Routing (obligatorio para inter vlan routing)	*D1(config)# ip routing*
Si hay un router conectado, Configurar dicho puerto como enrutado. Se puede agregar IP.	*D1(config)# interface G0/0/1* *D1(config-if)# no switchport* *D1(config-if)# ip add 10.10.10.1 255.255.255.0*

Configuración EtherChannel

Verificar que EtherChannel funciona en ambos switches	*S1# show etherchannel summary*
Ingresar al rango de interfaces	*S2(config)# interface range f0/23 - 24*
Apagar las interfaces	*S2(config-if-range)# shutdown*
Configurar el channel-group	*S2(config-if-range)# channel-group 1 mode passive, active o desirable (auto)*
Dar de alta las interfaces	*S2(config-if-range)# no shutdown*
Ingresar al channel-group	*S2(config-if-range)# interface port-channel 1*
Configurarlo como truncal	*S2(config-if)# switchport mode trunk*
Ver información de un port-channel particular	*S1# show etherchannel port-channel 1*
Se ve del punto de vista de la interfaz física, los datos del port-channel, modo, etc.	*S1# show interfaces etherchannel*
En el Router:	*R1(config)# interface port-channel 1* *R1(config)# interface range fa0/3-4* *R1(config-if-range)# channel-group 1* *R1(config)# interface port-channel 1.10* *R1(config-subif)# encapsulation dot1Q 10 native* *R1(config-subif)# ip add 10.10.10.1 255.255.255.0*

*Se debe configurar el channel-group en ambos switches.

Router como servidor DHCPv4

Excluir direcciones IP	R1(config)# ip dhcp excluded-address low-add high-add
Definir nombre de grupo DHCPv4	R1config)# ip dhcp pool pool-name
Configurar el grupo DHCPv4	R1(dhcp-config)# network network-number mask
	R1(dhcp-config)# default-router address (gateway)
	R1(dhcp-config)# dns-server add
	R1(dhcp-config)# domain-name example.com

Relay DHCPv4

Ir a la interfaz de salida (donde se encuentra la red de clientes)	R1(config)# interface G0/0/0
Configurar R1 como agente de retransmisión. (Acepta DHCP discover para enviarlo al servidor DHCP)	R1(config-if)# ip helper-address [DHCP server add]

Router como cliente DHCPv4

Ingresar a la interfaz de acceso	SOHO(config)# interface G0/0/1
Declarar como dhcp	SOHO(config-if)# ip address dhcp
Encender interfaz	SOHO(config-if)# no shutdown
Chequear	SOHO# show ip interface G0/0/1

Router como servidor DHCPv6 sin estado

Habilitar el enrutamiento IPV6 en el R1	*R1(config)# ipv6 unicast-routing (A=1)*
Defina un nombre de grupo DHCPv6	*R1(config)# ipv6 dhcp pool POOL-NAME*
Configure el grupo DHCPv6 con opciones	*R1(config)# dns-server X:X:X:X:X:X:X:X*
	R1(config)# domain-name example.com
Enlazar la interfaz al grupo (Ej: G0/0/0)	*R1(config-if)# ipv6 nd other-config-flag (O=1)*
	R1(config-if)# ipv6 dhcp server POOL-NAME

Router como cliente DHCPv6 sin estado

	R1(config)# ipv6 unicast-routing (A=1)
Entramos a la interfaz y configuramos el Router cliente para crear una LLA	*R1(config-if)# ipv6 enable*
Configuramos el Router cliente para utilizar SLAAC	*R1(config-if)# ipv6 address autoconfig*
Verificación	*R3# show ipv6 interface brief*

Router como servidor DHCPv6 con estado

Habilitar el enrutamiento IPV6 en el R1	*R1(config)# ipv6 unicast-routing (A=1)*
Defina un nombre de grupo DHCPv6	*R1(config)# ipv6 dhcp pool POOL-NAME*
Definir prefijo, dns server y dominio	*R1(config-dhcpv6)# address prefix 2001:DB8:0:1::/64*
	R1(config-dhcpv6)# dns-server 2001:DB8:0:1::1
	R1(config-dhcpv6)# domain-name example.com
Ingresamos a la interfaz EJ G0/0 y configuramos las FLAGs del RA	*R1(config-if)# ipv6 address fe80::1 link-local*
	R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
	R1(config-if)# ipv6 md managed-config-flag (M=1)
	R1(config-if)# ipv6 nd prefix default no-autoconfig (A=0)
	R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
	R1(config-if)# no shutdown

Router como cliente DHCPv6 con estado

	R1(config)# ipv6 unicast-routing (A=1)
Entramos a la interfaz y configuramos el Router cliente para crear una LLA	*R1(config-if)# ipv6 enable*
Configuramos el Router cliente	*R1(config-if)# ipv6 address dhcp*
Verificación	*R3# show ipv6 interface brief*

Verificación del servidor DHCPv6

R1(config)# show ipv6 dhcp pool
R1(config)# show ipv6 dhcp binding

Router como agente de retransmisión DHCPv6

Se accede a la interfaz del Router mas cercana a los host	*R1(config)# interface G0/0/1*
Especificación de la address del servidor DHCPv6 e interfaz de salida para llegar al servidor	*R1(config-if)# ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0*

Configuración de HSRP

Entrar a interfaz **física** y configurar grupo HSRP	*R1(config-if)# standby <group> ip <ip>*
Establecer prioridad HSRP	*R1(config-if)# standby <group> priority <priority>*
Configurar la direccion virtual de HSRP	*R1(config-if)# standby <group> ip <virtual-ip>*
Configurar el Router de respaldo	*R1(config-if)# standby <group> standby <backup-ip>*
Configurar el nombre del grupo HSRP	*R1(config-if)# standby <group> name <name>*

Configurar HSRP por interface vlan

```
D1(config)# interface VLAN 10
       Ip address 192.168.10.2 255.255.255.0
       Standby 10 ip 192.168.10.1 // IP virtual
       Standby 10 priority 150
       Standby 10 preempt
D2(config)# interface VLAN 10
       Ip address 192.168.10.3 255.255.255.0
       Standby 10 ip 192.168.10.1 // IP virtual
       Standby 10 priority 110
       Standby 10 preempt
```

Configurar HSRP con IPV6 en un Router:

```
Router(config)# interface <interface_type> <interface_number>
Router(config-if)# standby <group_number> ipv6 autoconfig
Router(config-if)# standby <group_number> ipv6 address <virtual_ipv6_address>
Router(config-if)# standby <group_number> priority <priority>
Router(config-if)# standby <group_number> preempt
```

Seguridad de puertos

Establecer interfaz con port-security (debe estar en modo acceso)	*S1(config-if)# switchport port-security*
Poner el signo de preg para ver las opciones que tiene port-security	*S1(config-if)# switchport port-security ?*

Mitigar ataques DHCP

Habilitar la inspeccion HDCP	*S1(config)# ip dhcp snooping*
Configurar los puertos que son de confianza	*S1(config-if)# ip dhcp snooping trust*
Limitar cantidad de mensajes de descubrimiento DHCP por puertos no confiables	*S1(config-if-range)# ip dhcp snooping limit rate 6*
Habilitar inspección DHCP por VLAN	*S1(config)# ip dhcp snooping vlan 5,10,50-52*

Mitigar ataques ARP (Implementacion de DAI)

Habilite la detección de DHCP.	S1(config)# ip dhcp snooping
Habilite la detección de DHCP en las VLAN seleccionadas.	S1(config)# ip dhcp snooping vlan 10
Habilite el DAI en las VLANs seleccionadas.	S1(config)# ip arp inspection vlan 10
Configure las interfaces de confianza para la detección de DHCP y la inspección de ARP ("no confiable" es la configuración predeterminada).	S1(config)# interface fa0/24 S1(config-if)# ip dhcp snooping trust S1(config-if)# ip arp inspection trust

Configurar PortFast y BPDU Guard

Habilitar portfast en una interfaz (debe estar en modo de acceso)	*S1(config-if)# spanning-tree portfast*
Habilitar portfast en todas las interfaces que esten en modo de acceso	*S1(config-if)# spanning-tree portfast default*
Habilitar BPDU Guard en un puerto	*S1(config-if)# spanning-tree bpduguard enable*
Habilitar BPDU Guard en todas las interfaces que esten en PortFast	*S1(config-if)# spanning-tree bpduguard default*
Verificar	*S1# show spanning-tree summary*

Note: Siempre active BPDU Guard en todos los puertos habilitados para PortFast.

Rutas IP estáticas

Configuración ruta IPv4 estática	*Router(config)# ip route network-address subnet-mask { ip-address | exit-intf [ip-address]} [distance]*
Network-address	*Red remota de destino*
Ip-adress	*IP de salida para reenviar paquetes*
Exit-intf	*Interfaz de salida para reenviar paquetes*
Distance	*Distancia administrativa*
Ej: Ruta predeterminada para enviar todo el tráfico sin ruta especificada por G0/0 al ISP	*R1(config)# ip route 0.0.0.0 0.0.0.0 G0/0*

Verificación de ruta estática

Mostrar solo rutas IPv4 estáticas	*R1# show ip route static | begin Gateway*
Mostrar una red IPv4 específica	*R1# show ip route 192.168.2.1*
Mostrar la configuración de la ruta estática IPv4	*R1# show running-config | section ip route*

Configuración OSPF

Habilitar OSPF (usar siempre el mismo id)	*R1(config)# router ospf <process-id>*
Configurar Router ID	*R1(config-router)# router-id <rid>*
Chequear router ID	*R1# show ip protocols | include router ID*
Especificar las interfaces que pertenecen a la red punto a punto	*R1(config-router)# network <network-address> <wildcard-mask> area <area-id>*
Configurar OSPF directo en la interfaz	*R1(config-if)# ip osfp <process-id> area <area-id>*
Evitar transmisión de mensajes de routing por una interfaz del Router	*R1(config-router)# passive-interface loopback 0*
Anunciar una ruta predeterminada (ruta por defecto) desde un router a otros routers en el área OSPF	*R1(config)# router ospf <process-ospf>* *R1(config-router)# default-information originate*

Comprobar funciones OSPFv2	*R1# show ip ospf interface G0/0/0*
Comprobar adyacencias OSPFv2	*R1# show ip ospf neighbor*
Establecer prioridad de la interfaz	*R1(config-if)# ip ospf priority <priority>*
Reestablecer proceso OSPF (hacer en todos los Router)	*R1# clear ip ospf process*
Ajustar ancho de banda de referencia (FastEthernet, GigE y 10 GigE tienen mismo costo)	*Auto-cost reference bandwith (Mbps)*
Establecer manualmente el valor del costo OSPF en las interfaces	*Ip cost ospf*
Establecer manualmente el valor de hello-interval	*R1(config-router)# hello-interval <segundos>*

Listas de Acceso Numeradas:

Crear la lista de acceso estándar:	*Router(config)# access-list <numero> permit|deny <source>*
Aplicar la lista de acceso en la interfaz	*Router(config)# interface <int_type> <int_number>* *Router(config-if)# ip access-group <numero> in|out*
Crear la lista de acceso extendida	*Router(config)# access-list <numero> permit|deny <protocol> <source> <source-wildcard> <destination> <destination-wildcard> [eq <port>]*
Aplicar la lista de acceso en la interfaz	*Router(config)# interface <int_type> <int_number>* *Router(config-if)# ip access-group <numero> in|out*

Listas de Acceso Nombradas

Crear la lista de acceso estándar	*Router(config)# ip access-list standard <nombre>* *Router(config-std-nacl)# permit|deny <source>*
Aplicar la lista de acceso en la interfaz de entrada o salida	*Router(config)# interface <int_type> <int_number>* *Router(config-if)# ip access-group <nombre> in|out*
Crear la lista de acceso extendida	*Router(config)# ip access-list extended <nombre>* *Router(config-ext-nacl)# permit|deny <protocol> <source> <source-wildcard> <destination> <destination-wildcard> [eq <port>]*
Aplicar la lista de acceso en la interfaz de entrada o salida	*Router(config)# interface <int_type> <int_number>* *Router(config-if)# ip access-group <nombre> in|out*

Otros comandos ACL

Elimina una ACL estándar específica.	*R1(config)# no access-list <número>*
Show access list	*Muestra cantidad de matcheos y la ACL*
En el modo de configuración de línea (como línea VTY), aplica una ACL a la/las línea/s.	*R1(config-line)# access-class <número> <in/out>*

Ejemplos de ACL

En el modo de configuración global, agrega una entrada para permitir respuestas ICMP (ping).	*R1(config)# access-list 1 permit icmp <origen> <máscara> <destino> <máscara> echo-reply*
En el modo de configuración global, agrega una entrada para permitir solicitudes ICMP (ping).	*R1(config)# access-list 1 permit icmp <origen> <máscara> <destino> <máscara> echo*
Ejemplo: una Access-list que permita ftp desde el host al servidor 172.22.34.62	*R1(config)#access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp*
Permitir tráfico desde una red específica	*Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255*
Permitir tráfico HTTP y HTTPS a un servidor específico	*Router(config)# access-list 3 permit tcp any host 10.0.0.1 eq 80* *Router(config)# access-list 3 permit tcp any host 10.0.0.1 eq 443*

Configurar NAT estática

Se establece la traducción estática entre una dirección local interna y una dirección global interna.	*Router(config)# ip nat inside source static local-ip global-ip*
Especificar la interfaz interna.	*Router(config)# interface number type*
Marque la interfaz como conectada al interior.	*Router(config-if)# ip nat inside*
Especificar la interfaz externa.	*Router(config)# interface number type*
Marque la interfaz como conectada al exterior.	*Router(config-if)# ip nat outside*

Configurar NAT dinámica

Definir el conjunto de direcciones globales que se debe usar para la traducción.	*Router(config)# ip nat pool {pool-name} start-ip end-ip {netmask netmask | prefix-length prefix-length}*
Configurar una lista de acceso estándar que permita las direcciones que se deben traducir.	*Router(config)# access-list access-list-number permit source [source-wildcard]*
Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen.	*Router(config)# ip nat inside source list access-list-number pool {pool-name}*
Identificar la interfaz interna.	*Router(config)# interface type number* *Router(config-if)# ip nat inside*
Identificar la interfaz externa.	*Router(config)# interface type number* *Router(config-if)# ip nat outside*

```
192-168.0.0 --- S0/0/0 --- S0/1/0 --- INT --- 209.165.200.252 (SERVER)
R2(config)# ip nat pool NAT-POOL-1 209.165.200.226 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL-1
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config-if)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Configurar NAT con sobrecarga (PAT) para conjunto de direcciones públicas

La diferencia principal entre esta configuración y la configuración para NAT dinámica uno a uno es que se utiliza la palabra clave overload. La palabra clave *overload* habilita PAT.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Configurar NAT con sobrecarga (PAT) para una única dirección IPV4 pública

Definir una lista de acceso estándar que permita las direcciones que se deben traducir.	*R1(config)# access-list número-lista-acceso permit source [source-wildcard]*
Especificar las opciones de ACL, interfaz de salida y sobrecarga para establecer la traducción dinámica de origen.	*R1(config)# ip nat inside source list access-list-number interface type number overload*
Identificar la interfaz interna.	*R1(config)# interface tipo número* *R1(config-if)# ip nat inside*
Identificar la interfaz externa.	*R1(config)# interface tipo número* *R1(config-if)# ip nat outside*

Configurar NAT con sobrecarga (PAT) para una pool address:

Router(config)# ip nat pool NAT-POOL-2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
Router(config)# Acces-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# Ip nat inside source list 1 pool NAT-POOL-1 overload
Router(config)# Int se0/1/0 Router(config-if)# Ip nat inside

Router(config)# Int se0/0/0
Router(config-if)# ip add 209.165.200.225 (IP que se utilizará como publica para el nateo)
Router(config-if)# Ip nat outside

Verificación de NAT.

Verificar NAT dinámica y/o estática	R2# show ip nat translations
Agregar la palabra clave **verbose** muestra información adicional sobre cada traducción, incluido cuánto tiempo hace que se creó y usó la entrada.	R2# show ip nat translation verbose
Muestra información sobre el número total de traducciones activas	R2# show ip nat statistics
Running-config	R2# show running-config | include NAT

Configurar CDP (Cisco Discovery Protocol)

Descripción	Comando Completo
Verificar el estado de CDP y mostrar información sobre CDP.	Router# show cdp
Habilitar CDP globalmente para todas las interfaces compatibles en el dispositivo.	Router(config)# cdp run
Deshabilitar CDP globalmente para todas las interfaces en el dispositivo.	Router(config)# no cdp run
Deshabilitar CDP en una interfaz específica.	Router(config-if)# no cdp enable
Habilitar nuevamente CDP en una interfaz específica.	Router(config-if)# cdp enable
Verificar el estado de CDP y mostrar una lista de vecinos.	Router# show cdp neighbors
Mostrar las interfaces habilitadas en CDP en el dispositivo.	Router# show cdp interface
Utilizar el comando `show cdp neighbors detail` para descubrir la dirección IP de S1.	Router# show cdp neighbors detail

Configurar LLDP (Link Layer Discovery Protocol)

Descripción	Comando Completo
Habilitar LLDP a nivel global en un dispositivo de red Cisco.	Router(config)# lldp run
Deshabilitar el LLDP a nivel global en un dispositivo de red Cisco.	Router(config)# no lldp run
Verificar si LLDP ya está habilitado en el dispositivo.	Router# show lldp
Configurar LLDP para transmitir anuncios en una interfaz específica.	Router(config-if)# lldp transmit
Configurar LLDP para recibir anuncios en una interfaz específica.	Router(config-if)# lldp receive
Detectar vecinos de dispositivo con LLDP habilitado.	Router# show lldp neighbors

Configurar NTP

Descripción	Comando Completo
Mostrar la hora actual en el reloj.	Router# show clock
Mostrar la hora actual en el reloj con detalles, indicando la fuente de tiempo.	Router# show clock detail
Configurar un servidor NTP en el modo de configuración global.	Router(config)# ntp server <ip-address>
Verificar la fuente de tiempo después de configurar un servidor NTP.	Router# show clock detail
Verificar las asociaciones NTP y el estado de sincronización.	Router# show ntp associations
Verificar el estado NTP, que incluye el estrato de sincronización.	Router# show ntp status

Comandos de SNMP

Descripción	Comando SNMP
Configura una cadena de comunidad SNMP con opciones de autorización y visualización.	snmp-server community <nombre> <autorización> <view>
Habilita la generación de trampas SNMP de un tipo específico.	snmp-server enable traps <tipo>
Configura un host de administración SNMP con una cadena de comunidad y, opcionalmente, una versión SNMP y puerto UDP.	snmp-server host <host> <comunidad> [version <versión>] [udp-port <puerto>]
Permite que los índices de interfaz SNMP persistan a través de reinicios.	snmp-server ifindex persist
Establece la ubicación física del dispositivo SNMP.	snmp-server location <ubicación>
Establece la información de contacto para el dispositivo SNMP.	snmp-server contact <contacto>
Muestra la configuración SNMP actual en el dispositivo.	show snmp
Muestra información sobre los grupos SNMP configurados en el dispositivo.	show snmp group
Muestra información sobre los usuarios SNMP configurados en el dispositivo.	show snmp user
Muestra información sobre los hosts SNMP configurados en el dispositivo.	show snmp host
Muestra información sobre las cadenas de comunidad SNMP configuradas en el dispositivo.	show snmp community

Syslog

Utiliza el comando `service timestamps log datetime` para forzar que los eventos registrados muestren la fecha y la hora.

Interfaces de Loopback

La interfaz de bucle invertido es una interfaz lógica interna del router. Se la considera una interfaz de software que se coloca automáticamente en estado "up" (activo), siempre que el router esté en funcionamiento. Es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, puede crear varias interfaces de bucle invertido en un router para simular más redes con fines de práctica de configuración y pruebas. En este plan de estudios, a menudo usamos una interfaz de bucle invertido para simular un enlace a Internet.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```