

Comandos CCNA V5 R&S.

INTRODUCTION TO NETWORKS (CCNA1) :

Switch> show versión	Mostrar la versión de la imagen del IOS del switch
Switch# clock set 15:08:00 Oct 26 2012	Configurar el reloj
Switch# show clock	verificar los parámetros del reloj
Switch> enable	Ingresa al modo EXEC privilegiado
Switch# configure terminal	Entra al modo de configuración
Switch(config)# hostname S1	Paso 1: Asignar un nombre al switch
S1(config)# no ip domain-lookup	Evitar búsquedas de DNS no deseadas
S1(config)# enable secret class	Protección por consola. Configuración y login de acceso local.
S1(config)# line con 0	
S1(config-line)# password cisco	
S1(config-line)# login	
S1(config-line)# exit	
S1(config)# banner motd #SOLO ACCESO AUTORIZADO#	Introducir un mensaje MOTD (mensaje del día) de inicio de sesión
S1# copy running-config startup-config	guardar la configuración en ejecución en el archivo de inicio de la memoria de acceso aleatorio no volátil (NVRAM)
S1# show running-config	Mostrar la configuración actual
S1# show ip interface brief	Mostrar el estado de las interfaces conectadas en el switch y en un router
R1# show ip interface brief	
Switch# show flash	Ver los archivos almacenados en la memoria flash
Switch# delete vlan.dat	Borrar las VLANs de un switch
Switch# erase startup-config	Borrar el archivo de configuración de inicio
Switch# reload	Recargar el switch
Switch# enable secret class	Contraseña modo privilegiado protegida
S1#(config)# interface vlan 1	configurar la dirección IP de la SVI para permitir la administración remota de switch.
S1(config-if)# ip address 192.168.1.2 255.255.255.0	

S1(config-if)# no shut S1(config-if)# exit	No shutdown sirve para levantar las interfaces.
S1(config)# line vty 0 4 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# end	Configurar la línea de terminal virtual (VTY) para que el switch permita el acceso por Telnet
S2# show mac address-table	Visualizar la tabla de direcciones MAC del switch
S2# clear mac address-table dynamic	Borrar la tabla de direcciones MAC
R1(config)# service password-encryption	Encriptar las contraseñas de texto no cifrado
R1(config)# int g0/0 R1(config-if)# description Connection to PC-B. R1(config-if)# ip address 192.168.0.1 255.255.255.0 R1(config-if)# no shut	Configurar IPv4, describir y levantar una interfaz.
R1(config)# interface g0/0 R1(config-if)# ipv6 address 2001:db8:acad:a::1/64 R1(config-if)# no shutdown	Configurar IPv6 y levantar una interfaz.
R1# show ipv6 interface brief	verificar que se asignó la dirección IPv6 unicast correcta a cada interfaz
R1# show ipv6 interface g0/0	Ver información detallada de la interfaz
R1(config)# interface g0/0 R1(config-if)# ipv6 address fe80::1 link-local	Configurar una dirección IPv6 de enlace local.
R1(config)# ipv6 unicast-routing	Habilitar el enrutamiento IPv6
S1# traceroute 192.168.3.3	Verificar la ruta que siguen los paquetes
S1# ping 192.168.3.3	Probar conectividad hacia equipo remoto
Router(config)# hostname R1 R1(config)# ip domain-name ccna-lab.com R1(config)# crypto key generate rsa modulus 1024 R1(config)# username admin privilege 15 secret adminpass R1(config)# line vty 0 4 R1(config-line)# transport input telnet ssh R1(config-line)# login local R1(config-line)# end	Pasos para configurar y habilitar SSH. <ul style="list-style-type: none"> • Configurar hostname • Configurar dominio • Crear el par de claves rsa • Crear usuario con privilegios de enable y contraseña protegida • Ingresar a las líneas VTY • Habilitar sólo SSH en estas líneas • Habilitar el login a la base de datos local
S1# ssh -l admin 192.168.1.1	Ingresar por SSH al router

R1(config)# security passwords min-length 10	Habilita un mínimo de 10 caracteres para todas las contraseñas
R1(config)# line console 0 R1(config-line)# exec-timeout 5 0 R1(config-line)# line vty 0 4 R1(config-line)# exec-timeout 5 0 R1(config-line)# exit	Cierra la sesión de la línea después de cinco minutos de inactividad
R1(config)# login block-for 30 attempts 2 within 120	Si alguien falla en dos intentos en un período de 120 segundos, el router bloquea los intentos de inicio de sesión por 30 segundos
R1# show login	para ver el estado de inicio de sesión
R1(config)# interface loopback 0 R1(config-if)# ip address 209.165.200.225 255.255.255.224	Crear y configurar interfaz loopback
R1(config-if)# int g0/1 R1(config-if)# ip address 192.168.1.1 255.255.255.0 R1(config-if)# no shut R1(config-if)# description Connected to LAN	Configurar direccionamiento en la interfaz giga, levantarla y describirla
S1(config)# ip default-gateway 192.168.1.1	Configurar el gateway predeterminado en el switch
R1(config)# interface GigabitEthernet0/1 R1(config-if)# duplex auto R1(config-if)# speed auto	Configurar duplex y velocidad automática
R1(config)# interface GigabitEthernet0/1 R1(config-if)# duplex full R1(config-if)# speed 100	Configurar duplex y velocidad manual
S1# copy running-config tftp: Address or name of remote host []? 192.168.1.3 Destination filename [s1-config]?	Respaldo del archivo de ejecución en un servidor TFTP
S1# copy tftp: running-config Address or name of remote host []? 192.168.1.3 Source filename []? Switch1-config.txt Destination filename [running-config]?	Cargar el archivo desde un servidor TFTP al archivo de ejecución local (RAM)
R1# show file systems	Mostrar los sistemas de archivo del router
R1# copy running-config flash:	Respaldo el archivo de ejecución en la memoria flash
R1# more flash:R1-running-config-backup	Ver desde el router el archivo de ejecución
Router# copy flash:R1-running-config-backup running-config	Cargar desde la flash a la RAM el archivo de ejecución

<ol style="list-style-type: none"> 1. Establecer una conexión de terminal con el router utilizando Tera Term u otro emulador de terminal como SecureCRT (no Putty). 2. Arrancar en modo ROMMON, ya sea por medio de eliminar la memoria flash y reiniciar, o presionando Alt-b durante el reinicio. 3. Escribir confreg 0x2142 en la petición de entrada de ROMMON. 4. Escribir reset en la siguiente petición de entrada de ROMMON. 5. Escribir no en el cuadro de diálogo de configuración inicial. 6. Escribir enable en la petición de entrada del router. 7. Escribir copy startup-config running-config para cargar la configuración de inicio. 8. Escribir show running-config. 9. Registrar una contraseña de enable sin encriptar. Restablecer una contraseña de enable encriptada con enable secret cisco. 10. En el modo de configuración, escribir config-register 0x2102. 11. En el modo privilegiado, escribir copy running-config startup-config para guardar la configuración. 12. Utilizar el comando show version para verificar los parámetros del registro de configuración. 	Recuperación de contraseña y archivo de inicio de un router
R1#show arp	Ver caché arp
R1#show protocols	Verificar si el enrutamiento IP está habilitado
R1#show ip route	Ver la tabla de enrutamiento
S1#show vlan	Ver información de VLAN
R1#show interface	Ver estado y protocolo de interfaces incluyendo otra información
R1#show version	Ver información de IOS, interfaces, registro de configuración y otra.

ROUTING AND SWITCHING ESSENCIALS

(CCNA2) :

COMANDOS BÁSICOS DE SWITCH	
S1# configure terminal	Ingresa modo de configuración global al switch
S1(config)# vlan 99 S1(config-vlan)# exit S1(config)# interface vlan99 %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down S1(config-if)# ip address 192.168.1.2 255.255.255.0 S1(config-if)# no shutdown	Por defecto la VLAN asociada a la interfaz de administración es la VLAN 1. Por seguridad se recomienda cambiar esta a cualquier otra. Acá se crea la VLAN 99 y se configura con IP una SVI (Switching Virtual Interface) para administrar remotamente el switch.
S1(config)# interface range f0/1 - 24,g0/1 - 2 S1(config-if-range)# switchport access vlan 99 S1(config-if-range)# exit	Asignar un rango de puertos a una VLAN. En este caso se seleccionó de la F0/1 a la F0/24 y además la G0/1 a la G0/2 y se asignaron a la VLAN 99.
S1(config)# ip default-gateway 192.168.1.1	Para que el switch sea administrado desde una red remota se le debe agregar un gateway por defecto.
S1(config)# line con 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# logging synchronous S1(config-line)# exit	Configuramos contraseña en la consola. El logging synchronous sirve para que un mensaje (log) no nos corte el comando que estamos ingresando.
S1(config)# line vty 0 15 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# end	Configuramos contraseña en las líneas de terminal virtual (VTY). Los switch tienen 16 líneas (0-15)
S1# show mac address-table dynamic	Para visualizar la tabla de direcciones MAC. En este caso para ver las aprendidas de forma dinámica.
S1# clear mac address-table dynamic	Para limpiar la tabla de direcciones MAC.
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6	Para agregar una dirección de forma manual y estática a una interfaz
Switch# delete vlan.dat Switch# erase startup-config Switch# reload Proceed with reload? [confirm] System configuration has been modified. Save? [yes/no]: no	Para borrar las VLANs y el archivo de inicio de un switch. Si pregunta por guardar las modificaciones le decimos que no.
S1(config)# vlan 99	Crear y nombrar una VLAN.

S1(config-vlan)# name Management S1(config-vlan)# exit	
S1(config)# interface f0/5 S1(config-if)# switchport mode access S1(config-if)# switchport access vlan 99	Configurar una interfaz de acceso y asociarla a una VLAN.
S1(config)# ip domain-name CCNA-Lab.com S1(config)# username admin privilege 15 secret sshadmin S1(config)# line vty 0 15 S1(config-line)# transport input ssh S1(config-line)# login local S1(config-line)# exit S1(config)# crypto key generate rsa modulus 1024	Configuración y habilitación de SSH en las líneas VTY de un switch.
S1(config)# ip ssh time-out 75 S1(config)# ip ssh authentication-retries 2 S1(config)# ip ssh version 2	La sesión se cierra si el switch se deja desatendido por 75 segundos Permite sólo dos reintentos. Cambio a la versión segura de SSH (2)
S1(config)# interface range f0/1 - 4 S1(config-if-range)# shutdown	Bajar un rango de interfaces
S1(config)# interface f0/5 S1(config-if)# switchport port-security S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx S1(config-if)# switchport port-security mac-address sticky S1# show port-security S1# show port-security address	Habilitación de seguridad de puerto Agregar de forma estática y manual una MAC a una interfaz. Agregar una MAC a una interfaz de forma dinámica. Verificación de la configuración de port-security
COMANDOS DE VLAN Y TRONCAL (SWITCH)	
S1(config)# vlan 10 S1(config-vlan)# name Student S1(config-vlan)# vlan 20 S1(config-vlan)# end	Crear y nombrar una VLAN.
S1(config)# interface f0/6 S1(config-if)# switchport mode access S1(config-if)# switchport access vlan 10	Configuración y asociación a VLAN de un puerto de acceso.
S1# show vlan S1# show vlan brief	Verificación de VLANs
S1(config)# interface vlan 99 S1(config-if)# ip address 192.168.1.11 255.255.255.0 S1(config-if)# end	Configuración de la VLAN de administración.
S1# show ip interface brief	Verificación de estado e IP de interfaces

S1(config)# interface range f0/11-24 S1(config-if-range)# switchport mode access S1(config-if-range)# switchport access vlan 10 S1(config-if-range)# end	Configurar un rango de interfaces como acceso y asociarlas a una VLAN.
S1(config)# interface f0/24 S1(config-if)# no switchport access vlan S1(config-if)# end	Eliminar una asignación de VLAN.
S1(config)# no vlan 30	Eliminar una VLAN
S1(config)# interface f0/1 S1(config-if)# switchport mode dynamic desirable	Usar DTP (negociación) para iniciar un enlace troncal.
S1(config)# interface f0/1 S1(config-if)# switchport mode trunk	Configurar manualmente la interfaz como troncal
S2# show interfaces trunk	Verificar la configuración de los enlaces troncales
S1(config)# interface f0/1 S1(config-if)# switchport trunk native vlan 99	Modificar la VLAN nativa. Esto se debe hacer en los dos extremos del enlace.
S1(config)# interface f0/1 S1(config-if)# switchport nonegotiate	Deshabilitar la negociación DTP en la interfaz.
S1(config)# interface f0/1 S1(config-if)# switchport trunk allowed vlan 10,99	Restringir las VLAN permitidas en un enlace troncal.
COMANDOS DE CONFIGURACIÓN BASICA DE ROUTER	
Router# config terminal	Ingresar al modo de configuración global
Router(config)# hostname R1	Asignar nombre al router
R1(config)# no ip domain-lookup	Deshabilitar la búsqueda DNS
R1(config)# security passwords min-length 10	Establecer el requisito de largo de contraseñas
R1(config)# enable secret cisco12345	Asignar contraseña privilegiada protegida
R1(config)# line con 0 R1(config-line)# password ciscoconpass R1(config-line)# exec-timeout 5 0 R1(config-line)# login R1(config-line)# logging synchronous R1(config-line)# exit	Asignar la contraseña a la consola. Establecer un tiempo de espera por una sesión. Evita que los logs o alertas corten el comando que se está ingresando.
R1(config)# line vty 0 4 R1(config-line)# password ciscovtypass R1(config-line)# exec-timeout 5 0 R1(config-line)# login R1(config-line)# logging synchronous	Asignar contraseña a las líneas VTY (TELNET, SSH). Establecer un tiempo de espera por una sesión. Evita que los logs o alertas corten el comando que se está ingresando.

R1(config)# service password-encryption	Cifrar las contraseñas no protegidas
R1(config)# banner motd #INGRESO NO AUTORIZADO¡¡¡#	Crear aviso de advertencia al que accede.
R1(config)# int g0/0 R1(config-if)# description Connection to PC-B R1(config-if)# ip address 192.168.0.1 255.255.255.0 R1(config-if)# no shutdown	Describir y configurar una interfaz y luego activarla.
R1(config)# ip domain-name CCNA-lab.com R1(config)# username admin privilege 15 secret adminpass1 R1(config)# line vty 0 4 R1(config-line)# transport input ssh R1(config-line)# login local R1(config-line)# exit R1(config)# crypto key generate rsa modulus 1024 R1(config)# exit	Crear dominio. Crear usuario con privilegios de enable Habilitación de SSH en las líneas VTY Autenticación local Generar la clave RSA
COMANDOS DE DIRECCIONAMIENTO IPV6 ROUTER	
R1(config)# interface g0/0 R1(config-if)# ipv6 address 2001:db8:acad:a::1/64 R1(config-if)# ipv6 address fe80::1 link-local R1(config-if)# no shutdown R1(config-if)# exit R1(config)# ipv6 unicast-routing	Asignar IPv6 global a la interfaz Asignar IPv6 de link local Habilitar enrutamiento IPv6 unicast
R1# show ipv6 int brief	Verificar direccionamiento IPv6 y estado de las interfaces
COMANDOS PARA ACCESO HTTP, HTTPS, CCP Y SDM	
R1(config)# ip http server	Habilita servicio http (puerto 80 de TCP)
R1(config)# ip http secure-server	Habilita servicio https (puerto 443 de TCP)
R1(config)# username admin privilege 15 secret adminpass1	Crear usuario con privilegios de enable y contraseña protegida (MD5).
COMANDOS ENRUTAMIENTO ENTRE VLAN. ROUTE ON A STICK	
R1(config)# interface g0/1.1	Creación de las subinterfaces
R1(config-subif)# encapsulation dot1Q 1 R1(config-subif)# ip address 192.168.1.1 255.255.255.0	Encapsulamiento de la subinterfaz, se asocia a la VLAN correspondiente con el número de la VLAN. Asignación de IP a la subinterfaz
RUTAS ESTÁTICAS	
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2	Ruta estática con IP de router de siguiente salto

R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0	Ruta estática con interfaz de salida
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1	Ruta por defecto con interfaz de salida
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2	Ruta por defecto con IP de siguiente salto
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1	Ruta estática con interfaz de salida
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 FC00::2	Ruta estática con IP de router de siguiente salto
R1(config)# ipv6 route ::/0 serial 0/0/1	Ruta por defecto con interfaz de salida
R1(config)# ipv6 route ::/0 FC00::2	Ruta por defecto con IP de siguiente salto
ISP# show ipv6 route	Verificar tabla de enrutamiento
BRANCH# show ipv6 interface brief	Verificar interfaces por estado y configuración de IPv6
COMANDOS RIPV2 Y RIPNG	
R1(config)# router rip R1(config-router)# version 2 R1(config-router)# passive-interface g0/1 R1(config-router)# network 172.30.0.0 R1(config-router)# network 10.0.0.0 R1(config-router)# no auto-summary R2(config-router)# default-information originate	Ingresar a la configuración RIP. Cambiar a la versión 2. Evita que actualizaciones RIP se envíen por esa interfaz Declarar las redes directamente conectada. Desactiva a sumarización automática Redistribución de rutas por defecto
R1# show ip protocols	Confirma el protocolo configurado
R2# debug ip rip	Examinar actualizaciones RIP
R1(config)# ipv6 router rip Test1 R1(config)# interface g0/1 R1(config-if)# ipv6 rip Test1 enable R1(config)# interface s0/0/0 R1(config-if)# ipv6 rip Test1 enable	Configuración de RIPng
R1# show ipv6 protocols	Verificar el protocolo configurado.
R1# show ipv6 rip Test1	Verificar el proceso RIP configurado.
R2(config)# int s0/0/0 R2(config-if)# ipv6 rip Test2 default-information originate	Redistribución de una ruta por defecto dentro de la interfaz.
COMANDOS OSPF	
R1(config)# router ospf 1 R1(config-router)# network 192.168.1.0 0.0.0.255 area 0	Ingresar al modo de configuración de OSPF Declaración de las redes con sus correspondientes wildcard.

R1(config-router)# network 192.168.12.0 0.0.0.3 area 0 R1(config-router)# network 192.168.13.0 0.0.0.3 area 0	
R1# show ip ospf	Verificación del proceso OSPF
R1# show ip ospf interface brief R1# show ip ospf neighbor	Ver vecinos OSPF
R1# show ip ospf neighbor	
R1(config)# router ospf 1 R1(config-router)# router-id 11.11.11.11 Reload or use "clear ip ospf process" command, for this to take effect R1(config)# end	Configurar el ID de router OSPF. Si el router ya tiene un ID va a pedir reiniciar el proceso OSPF con el comando "clear ip ospf process"
R1# show ip ospf interface g0/0	Para ver detalles de OSPF dentro de la interfaz, por ejemplo los timers.
R1(config)# router ospf 1 R1(config-router)# passive-interface g0/0	Pone todas las interfaces como pasivas
R2(config)# router ospf 1 R2(config-router)# passive-interface default	Configurar como pasiva una interfaz.
R2# show ip route ospf	Ver la tabla de enrutamiento OSPF.
R1(config)# router ospf 1 R1(config-router)# auto-cost reference-bandwidth 10000	Modificar la fórmula de cálculo de los costos. Usar cuando se usen interfaces de mayor ancho de banda que 100Mbps.
R1(config)# interface s0/0/0 R1(config-if)# bandwidth 128	Esto, además de modificar el valor del ancho de banda, cambia el costo de la interfaz OSPF.
R1(config)# int s0/0/1 R1(config-if)# ip ospf cost 1565	Cambia el costo a un valor específico.
R1(config)# ipv6 router ospf 1 R1(config-rtr)# router-id 1.1.1.1	Configuración de OSPF V3 (IPv6) Se debe agregar un ID de router en formato IPv4
R1(config)# interface g0/0 R1(config-if)# ipv6 ospf 1 area 0	Habilitar las interfaces para OSPF IPv6
R2# show ipv6 ospf	Verificar el proceso OSPF V3
R1# show ipv6 ospf neighbor	Ver los vecinos OPSF IPv6
R1# show ipv6 protocols	Ver los protocolos de enrutamiento IPv6 configurados
R1# show ipv6 ospf interface R1# show ipv6 ospf interface brief	Ver las interfaces activas para OSPF V3
R2# show ipv6 route R2# show ipv6 route ospf	Ver la tabla de enrutamiento IPv6
R1# show ipv6 ospf interface g0/0	Ver información detallada de una interfaz OSPF
R1(config)# ipv6 router ospf 1	Poner pasiva una interfaz OSPF

R1(config-rtr)# passive-interface g0/0	
R2(config)# ipv6 router ospf 1 R2(config-rtr)# passive-interface default	Poner todas las interfaces pasivas por defecto
R2(config-rtr)# no passive-interface s0/0/1	Activar una interfaz que era pasiva para OSPF
LISTAS DE ACCESO	
R3(config)# access-list 1 remark Allow R1 LANs Access R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255 R3(config)# access-list 1 deny any	Describir la ACL numerada estándar (1-99). Permitir una red completa Denegar todo el resto
R3(config)# interface g0/1 R3(config-if)# ip access-group 1 out	Se aplica a una interfaz de entrada o de salida
R3# show access-lists 1 R3# show access-lists	Verificar la configuración de las ACL.
R3# show ip interface g0/1 R3# show ip interface	Para ver dónde se aplicó la ACL
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY R1(config-std-nacl)# permit host 192.168.30.3 R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255	Crea la ACL estándar nombrada Permite un único host. Permite una red completa
R1(config)# interface g0/1 R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out	Se aplica a una interfaz de salida o entrada.
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31 R1(config-std-nacl)# 40 deny any R1(config-std-nacl)# end	Las ACL nombradas se pueden editar indicando la posición de ella.
R1(config)# ip access-list standard ADMIN-MGT R1(config-std-nacl)# permit host 192.168.1.3 R1(config)# line vty 0 4 R1(config-line)# access-class ADMIN-MGT in R1(config-line)# exit	Crear una lista de acceso para ser aplicada para controlar los accesos a las líneas VTY. Especificar el o los hosts. Ingresar las líneas VTY. Aplicar la ACL de entrada a las líneas VTY.
R1(config)# access-list 100 remark Allow Web & SSH Access R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 R1(config)# access-list 100 permit tcp any any eq 80	Describir la ACL extendida (100-199) numerada. Permite a una IP origen a una IP destino y un puerto destino TCP 22 (SSH).

	Permite cualquier origen a cualquier destino al puerto destino TCP 80 (HTTP).
R1(config)# int s0/0/0 R1(config-if)# ip access-group 100 out	Se aplica de entrada o salida en una interfaz.
R3(config)# ip access-list extended WEB-POLICY R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80 R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80	Crear una ACL extendida nombrada. Permite a una red ir a un host al puerto destino TCP 80. Permite a una red ir a una subred al puerto destino TCP 80.
R3(config-ext-nacl)# int S0/0/1 R3(config-if)# ip access-group WEB-POLICY out	Se aplica de entrada o salida a una interfaz.
R1(config)# ipv6 access-list RESTRICT-VTY R1(config-ipv6-acl)# permit tcp 2001:db8:acad:a::/64 any R1(config-ipv6-acl)# permit tcp any any eq 22 R1(config-ipv6-acl)# line vty 0 4 R1(config-line)# ipv6 access-class RESTRICT-VTY in R1(config-line)# end	Crear una ACL nombrada IPv6. Permite tcp a una red a cualquier destino. Permite SSH de cualquier origen a cualquier destino. Se aplica la ACL de entrada en las líneas VTY.
R1(config)# ipv6 access-list RESTRICTED-LAN R1(config-ipv6-acl)# remark Block Telnet from outside R1(config-ipv6-acl)# deny tcp any 2001:db8:acad:a::/64 eq telnet R1(config-ipv6-acl)# permit ipv6 any any R1(config-ipv6-acl)# int g0/1 R1(config-if)# ipv6 traffic-filter RESTRICTED-LAN out R1(config-if)# end	Crear la ACL IPv6. Describirla. Denegar que desde una red se haga telnet. Se permite el resto. Se aplica de salida a una interfaz.
R1# show ipv6 access-lists RESTRICTED-LAN	Verificar la ACL
R1# clear ipv6 access-list RESTRICTED-LAN	Limpia los contadores de coincidencia.
DHCP	
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9	Excluye un rango de direcciones IP a asignar.
R2(config)# ip dhcp pool R1G1 R2(dhcp-config)# network 192.168.1.0 255.255.255.0 R2(dhcp-config)# default-router 192.168.1.1 R2(dhcp-config)# dns-server 209.165.200.225 R2(dhcp-config)# domain-name ccna-lab.com R2(dhcp-config)# lease 2	Crea el pool del DHCP. A la red a la cual le va asignar direccionamiento Define el gateway por defecto de la red. Define el DNS de la red. Algún servidor de dominio de la red. El tiempo de reserva de una IP
R1(config)# interface g0/0	Si el servidor DHCP está en otra red, se convierten los broadcast en

R1(config-if)# ip helper-address 192.168.2.254	direcciones unicast. La IP del servidor DHCP remoto.
CONFIGURACIÓN CON ESTADO (DHCP) Y SIN ESTADO (SLAAC) IPV6	
S1(config)# interface vlan 1 S1(config-if)# ipv6 address autoconfig	Para obtener una IPv6 a través de SLAAC
R1(config)# ipv6 dhcp pool IPV6POOL-A	Configurar un servidor DHCP IPv6. Se crea el pool DHCP.
R1(config-dhcpv6)# domain-name ccna-statelessDHCPv6.com	Se asigna un nombre al pool. Este DHCP es sin estado.
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd	Asigna una dirección del servidor DNS.
R1(config)# interface g0/1 R1(config-if)# ipv6 dhcp server IPV6POOL-A	Agrega un prefijo de red al pool. Se asigna el pool a una interfaz
R1(config-if)# ipv6 nd other-config-flag	Permite la detección de redes con paquetes de descubrimiento de vecinos (ND) en una interfaz
R1(config-dhcpv6)# address prefix 2001:db8:acad:a::/64 R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com	Para configurar un DHCP con estado. Para definir una dirección de asignación.
R1# show ipv6 dhcp binding R1# show ipv6 dhcp pool	Verificar asignación de IP e información del pool DHCP.
R1(config)# interface g0/1 R1(config-if)# shutdown R1(config-if)# ipv6 nd managed-config-flag R1(config-if)# no shutdown R1(config-if)# end	Para permitir que la interfaz envíe mensajes RA (Router Advertisement)
S1(config)# interface vlan 1 S1(config-if)# ipv6 address autoconfig	Permite a la interfaz VLAN obtener una dirección IPv6 a través de SLAAC.
NAT	
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225	Configura un NAT estático.
Gateway(config)# interface g0/1 Gateway(config-if)# ip nat inside Gateway(config-if)# interface s0/0/1 Gateway(config-if)# ip nat outside	Define la interfaz que va a la red interna Define la interfaz que va a la red externa
Gateway# show ip nat translations	Verifica la traducción
Gateway# show ip nat statistics	Verificar estadísticas de NAT
Gateway# clear ip nat translation * Gateway# clear ip nat statistics	Limpiar la tabla y estadísticas

NAT DINÁMICO	
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255	Permite que se traduzca la red especificada
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224	Define el conjunto de direcciones públicas utilizables a traducir.
Gateway(config)# ip nat inside source list 1 pool public_access	Define la lista origen interna que se va a traducir al conjunto externo.
NAT CON SOBRECARGA	
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255	Permitir que esas direcciones se traduzcan
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248	Define el conjunto de direcciones IP públicas utilizables.
Gateway(config)# ip nat inside source list 1 pool public_access overload	Define el NAT desde la lista origen al conjunto de IPs externas sobrecargado.
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload	NAT con sobrecarga sin definir el pool externo, sino que la interfaz de salida.
Gateway(config)# interface g0/1 Gateway(config-if)# ip nat inside Gateway(config-if)# interface s0/0/1 Gateway(config-if)# ip nat outside	Identifica las interfaces inside y outside.