

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 S1(config)# enable secret class S1(config)# line con 0 S1(config-line)# password cisco S1(config-line)# login S1(config-line)# exit	Evitar búsquedas de DNS no deseadas Protección por consola. Configuración y login de acceso local.
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 R1# show ip interface brief	Mostrar el estado de las interfaces conectadas en el switch y en un router
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 S1(config-if)# ip address 192.168.1.2 255.255.255.0	configurar la dirección IP de la SVI para permitir la administración remota de switch.

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)# <b>interface g0/0</b> R1(config-if)# <b>ipv6 address 2001:db8:acad:a::1/64</b> R1(config-if)# <b>no shutdown</b>	Configurar IPv6 y levantar una interfaz.
R1# <b>show ipv6 interface brief</b>	verificar que se asignó la dirección IPv6 unicast correcta a cada interfaz
R1# <b>show ipv6 interface g0/0</b>	Ver información detallada de la interfaz
R1(config)# <b>interface g0/0</b> R1(config-if)# <b>ipv6 address fe80::1 link-local</b>	Configurar una dirección IPv6 de enlace local.
R1(config)# <b>ipv6 unicast-routing</b>	Habilitar el enrutamiento IPv6
S1# <b>traceroute 192.168.3.3</b>	Verificar la ruta que siguen los paquetes
S1# <b>ping 192.168.3.3</b>	Probar conectividad hacia equipo remoto
Router(config)# <b>hostname R1</b> R1(config)# <b>ip domain-name ccna-lab.com</b> R1(config)# <b>crypto key generate rsa modulus 1024</b> R1(config)# <b>username admin privilege 15 secret adminpass</b> R1(config)# <b>line vty 0 4</b> R1(config-line)# <b>transport input telnet ssh</b> R1(config-line)# <b>login local</b> R1(config-line)# <b>end</b>	<b>Pasos para configurar y habilitar SSH.</b> <ul style="list-style-type: none"> <li>• Configurar hostname</li> <li>• Configurar dominio</li> <li>• Crear el par de claves rsa</li> <li>• Crear usuario con privilegios de enable y contraseña protegida</li> <li>• Ingresar a las líneas VTY</li> <li>• Habilitar sólo SSH en estas líneas</li> <li>• Habilitar el login a la base de datos local</li> </ul>
S1# <b>ssh -l admin 192.168.1.1</b>	<b>Ingresar por SSH al router</b>

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

<ol style="list-style-type: none"> <li>1. Establecer una conexión de terminal con el router utilizando Tera Term u otro emulador de terminal como SecureCRT (no Putty).</li> <li>2. Arrancar en modo <b>ROMMON</b>, ya sea por medio de eliminar la memoria flash y reiniciar, o presionando Alt-b durante el reinicio.</li> <li>3. Escribir <b>confreg 0x2142</b> en la petición de entrada de <b>ROMMON</b>.</li> <li>4. Escribir <b>reset</b> en la siguiente petición de entrada de <b>ROMMON</b>.</li> <li>5. Escribir <b>no</b> en el cuadro de diálogo de configuración inicial.</li> <li>6. Escribir <b>enable</b> en la petición de entrada del router.</li> <li>7. Escribir <b>copy startup-config running-config</b> para cargar la configuración de inicio.</li> <li>8. Escribir <b>show running-config</b>.</li> <li>9. Registrar una contraseña de enable sin encriptar. Restablecer una contraseña de enable encriptada con <b>enable secret cisco</b>.</li> <li>10. En el modo de configuración, escribir <b>config-register 0x2102</b>.</li> <li>11. En el modo privilegiado, escribir <b>copy running-config startup-config</b> para guardar la configuración.</li> <li>12. Utilizar el comando <b>show version</b> para verificar los parámetros del registro de configuración.</li> </ol>	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# <b>configure terminal</b>	Ingresa modo de configuración global al switch
S1(config)# <b>vlan 99</b> S1(config-vlan)# <b>exit</b> S1(config)# <b>interface vlan99</b> %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down S1(config-if)# <b>ip address 192.168.1.2 255.255.255.0</b> S1(config-if)# <b>no shutdown</b>	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)# <b>interface range f0/1 - 24,g0/1 - 2</b> S1(config-if-range)# <b>switchport access vlan 99</b> S1(config-if-range)# <b>exit</b>	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)# <b>ip default-gateway 192.168.1.1</b>	Para que el switch sea administrado desde una red remota se le debe agregar un gateway por defecto.
S1(config)# <b>line con 0</b> S1(config-line)# <b>password cisco</b> S1(config-line)# <b>login</b> S1(config-line)# <b>logging synchronous</b> S1(config-line)# <b>exit</b>	Configuramos contraseña en la consola. El logging synchronous sirve para que un mensaje (log) no nos corte el comando que estamos ingresando.
S1(config)# <b>line vty 0 15</b> S1(config-line)# <b>password cisco</b> S1(config-line)# <b>login</b> S1(config-line)# <b>end</b>	Configuramos contraseña en las líneas de terminal virtual (VTY). Los switch tienen 16 líneas (0-15)
S1# <b>show mac address-table dynamic</b>	Para visualizar la tabla de direcciones MAC. En este caso para ver las aprendidas de forma dinámica.
S1# <b>clear mac address-table dynamic</b>	Para limpiar la tabla de direcciones MAC.
S1(config)# <b>mac address-table static 0050.56BE.6C89 vlan 99 interface fastethernet 0/6</b>	Para agregar una dirección de forma manual y estática a una interfaz
Switch# <b>delete vlan.dat</b> Switch# <b>erase startup-config</b> Switch# <b>reload</b> Proceed with reload? [confirm] System configuration has been modified. Save? [yes/no]: <b>no</b>	Para borrar las VLANs y el archivo de inicio de un switch. Si pregunta por guardar las modificaciones le decimos que no.
S1(config)# <b>vlan 99</b>	Crear y nombrar una VLAN.

S1(config-vlan)# <b>name Management</b> S1(config-vlan)# <b>exit</b>	
S1(config)# <b>interface f0/5</b> S1(config-if)# <b>switchport mode access</b> S1(config-if)# <b>switchport access vlan 99</b>	Configurar una interfaz de acceso y asociarla a una VLAN.
S1(config)# <b>ip domain-name CCNA-Lab.com</b> S1(config)# <b>username admin privilege 15 secret sshadmin</b> S1(config)# <b>line vty 0 15</b> S1(config-line)# <b>transport input ssh</b> S1(config-line)# <b>login local</b> S1(config-line)# <b>exit</b> S1(config)# <b>crypto key generate rsa modulus 1024</b>	Configuración y habilitación de SSH en las líneas VTY de un switch.
S1(config)# <b>ip ssh time-out 75</b>  S1(config)# <b>ip ssh authentication-retries 2</b> S1(config)# <b>ip ssh version 2</b>	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)# <b>interface range f0/1 - 4</b> S1(config-if-range)# <b>shutdown</b>	Bajar un rango de interfaces
S1(config)# <b>interface f0/5</b> S1(config-if)# <b>switchport port-security</b> S1(config-if)# <b>switchport port-security mac-address xxxx.xxxx.xxxx</b> S1(config-if)# <b>switchport port-security mac-address sticky</b> S1# <b>show port-security</b> S1# <b>show port-security address</b>	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
<b>COMANDOS DE VLAN Y TRONCAL (SWITCH)</b>	
S1(config)# <b>vlan 10</b> S1(config-vlan)# <b>name Student</b> S1(config-vlan)# <b>vlan 20</b> S1(config-vlan)# <b>end</b>	Crear y nombrar una VLAN.
S1(config)# <b>interface f0/6</b> S1(config-if)# <b>switchport mode access</b> S1(config-if)# <b>switchport access vlan 10</b>	Configuración y asociación a VLAN de un puerto de acceso.
S1# <b>show vlan</b> S1# <b>show vlan brief</b>	Verificación de VLANs
S1(config)# <b>interface vlan 99</b> S1(config-if)# <b>ip address 192.168.1.11 255.255.255.0</b> S1(config-if)# <b>end</b>	Configuración de la VLAN de administración.
S1# <b>show ip interface brief</b>	Verificación de estado e IP de interfaces

S1(config)# <b>interface range f0/11-24</b> S1(config-if-range)# <b>switchport mode access</b> S1(config-if-range)# <b>switchport access vlan 10</b> S1(config-if-range)# <b>end</b>	Configurar un rango de interfaces como acceso y asociarlas a una VLAN.
S1(config)# <b>interface f0/24</b> S1(config-if)# <b>no switchport access vlan</b> S1(config-if)# <b>end</b>	Eliminar una asignación de VLAN.
S1(config)# <b>no vlan 30</b>	Eliminar una VLAN
S1(config)# <b>interface f0/1</b> S1(config-if)# <b>switchport mode dynamic desirable</b>	Usar DTP (negociación) para iniciar un enlace troncal.
S1(config)# <b>interface f0/1</b> S1(config-if)# <b>switchport mode trunk</b>	Configurar manualmente la interfaz como troncal
S2# <b>show interfaces trunk</b>	Verificar la configuración de los enlaces troncales
S1(config)# <b>interface f0/1</b> S1(config-if)# <b>switchport trunk native vlan 99</b>	Modificar la VLAN nativa. Esto se debe hacer en los dos extremos del enlace.
S1(config)# <b>interface f0/1</b> S1(config-if)# <b>switchport nonegotiate</b>	Deshabilitar la negociación DTP en la interfaz.
S1(config)# <b>interface f0/1</b> S1(config-if)# <b>switchport trunk allowed vlan 10,99</b>	Restringir las VLAN permitidas en un enlace troncal.
<b>COMANDOS DE CONFIGURACIÓN BASICA DE ROUTER</b>	
Router# <b>config terminal</b>	<b>Ingresar al modo de configuración global</b>
Router(config)# <b>hostname R1</b>	<b>Asignar nombre al router</b>
R1(config)# <b>no ip domain-lookup</b>	<b>Deshabilitar la búsqueda DNS</b>
R1(config)# <b>security passwords min-length 10</b>	Establecer el requisito de largo de contraseñas
R1(config)# <b>enable secret cisco12345</b>	Asignar contraseña privilegiada protegida
R1(config)# <b>line con 0</b> R1(config-line)# <b>password ciscoconpass</b> R1(config-line)# <b>exec-timeout 5 0</b> R1(config-line)# <b>login</b> R1(config-line)# <b>logging synchronous</b> R1(config-line)# <b>exit</b>	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)# <b>line vty 0 4</b> R1(config-line)# <b>password ciscovtypass</b> R1(config-line)# <b>exec-timeout 5 0</b> R1(config-line)# <b>login</b> R1(config-line)# <b>logging synchronous</b>	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)# <b>service password-encryption</b>	Cifrar las contraseñas no protegidas
R1(config)# <b>banner motd #INGRESO NO AUTORIZADO¡¡¡#</b>	Crear aviso de advertencia al que accede.
R1(config)# <b>int g0/0</b> R1(config-if)# <b>description Connection to PC-B</b> R1(config-if)# <b>ip address 192.168.0.1 255.255.255.0</b> R1(config-if)# <b>no shutdown</b>	Describir y configurar una interfaz y luego activarla.
R1(config)# <b>ip domain-name CCNA-lab.com</b> R1(config)# <b>username admin privilege 15 secret adminpass1</b> R1(config)# <b>line vty 0 4</b> R1(config-line)# <b>transport input ssh</b> R1(config-line)# <b>login local</b> R1(config-line)# <b>exit</b> R1(config)# <b>crypto key generate rsa modulus 1024</b> R1(config)# <b>exit</b>	Crear dominio. Crear usuario con privilegios de enable  Habilitación de SSH en las líneas VTY Autenticación local  Generar la clave RSA
<b>COMANDOS DE DIRECCIONAMIENTO IPV6 ROUTER</b>	
R1(config)# <b>interface g0/0</b> R1(config-if)# <b>ipv6 address 2001:db8:acad:a::1/64</b> R1(config-if)# <b>ipv6 address fe80::1 link-local</b> R1(config-if)# <b>no shutdown</b> R1(config-if)# <b>exit</b> R1(config)# <b>ipv6 unicast-routing</b>	Asignar IPv6 global a la interfaz Asignar IPv6 de link local  Habilitar enrutamiento IPv6 unicast
R1# <b>show ipv6 int brief</b>	Verificar direccionamiento IPv6 y estado de las interfaces
<b>COMANDOS PARA ACCESO HTTP, HTTPS, CCP Y SDM</b>	
R1(config)# <b>ip http server</b>	Habilita servicio http (puerto 80 de TCP)
R1(config)# <b>ip http secure-server</b>	Habilita servicio https (puerto 443 de TCP)
R1(config)# <b>username admin privilege 15 secret adminpass1</b>	Crear usuario con privilegios de enable y contraseña protegida (MD5).
<b>COMANDOS ENRUTAMIENTO ENTRE VLAN. ROUTE ON A STICK</b>	
R1(config)# <b>interface g0/1.1</b>	Creación de las subinterfaces
R1(config-subif)# <b>encapsulation dot1Q 1</b>  R1(config-subif)# <b>ip address 192.168.1.1 255.255.255.0</b>	Encapsulamiento de la subinterfaz, se asocia a la VLAN correspondiente con el número de la VLAN.  Asignación de IP a la subinterfaz
<b>RUTAS ESTÁTICAS</b>	
R1(config)# <b>ip route 192.168.1.0 255.255.255.0 10.1.1.2</b>	Ruta estática con IP de router de siguiente salto



## COMANDOS CCNA ROUTING & SWITCHING V5

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

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

R1(config-rtr)# <b>passive-interface g0/0</b>	
R2(config)# <b>ipv6 router ospf 1</b> R2(config-rtr)# <b>passive-interface default</b>	Poner todas las interfaces pasivas por defecto
R2(config-rtr)# <b>no passive-interface s0/0/1</b>	Activar una interfaz que era pasiva para OSPF
<b>LISTAS DE ACCESO</b>	
R3(config)# <b>access-list 1 remark Allow R1 LANs Access</b> R3(config)# <b>access-list 1 permit 192.168.10.0 0.0.0.255</b> R3(config)# <b>access-list 1 deny any</b>	Describir la ACL numerada estándar (1-99).  Permitir una red completa  Denegar todo el resto
R3(config)# <b>interface g0/1</b> R3(config-if)# <b>ip access-group 1 out</b>	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)# <b>ip access-list standard BRANCH-OFFICE-POLICY</b> R1(config-std-nacl)# <b>permit host 192.168.30.3</b> R1(config-std-nacl)# <b>permit 192.168.40.0 0.0.0.255</b>	Crea la ACL estándar nombrada  Permite un único host. Permite una red completa
R1(config)# <b>interface g0/1</b> R1(config-if)# <b>ip access-group BRANCH-OFFICE-POLICY out</b>	Se aplica a una interfaz de salida o entrada.
R1#(config)# <b>ip access-list standard BRANCH-OFFICE-POLICY</b> R1(config-std-nacl)# <b>30 permit 209.165.200.224 0.0.0.31</b> R1(config-std-nacl)# <b>40 deny any</b> R1(config-std-nacl)# <b>end</b>	Las ACL nombradas se pueden editar indicando la posición de ella.
R1(config)# <b>ip access-list standard ADMIN-MGT</b> R1(config-std-nacl)# <b>permit host 192.168.1.3</b> R1(config)# <b>line vty 0 4</b> R1(config-line)# <b>access-class ADMIN-MGT in</b> R1(config-line)# <b>exit</b>	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)# <b>access-list 100 remark Allow Web &amp; SSH Access</b> R1(config)# <b>access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22</b> R1(config)# <b>access-list 100 permit tcp any any eq 80</b>	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)# <b>int s0/0/0</b> R1(config-if)# <b>ip access-group 100 out</b>	Se aplica de entrada o salida en una interfaz.
R3(config)# <b>ip access-list extended WEB-POLICY</b> R3(config-ext-nacl)# <b>permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80</b> R3(config-ext-nacl)# <b>permit tcp 192.168.30.0 0.0.0.255 209.165.200.224 0.0.0.31 eq 80</b>	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)# <b>int S0/0/1</b> R3(config-if)# <b>ip access-group WEB-POLICY out</b>	Se aplica de entrada o salida a una interfaz.
R1(config)# <b>ipv6 access-list RESTRICT-VTY</b> R1(config-ipv6-acl)# <b>permit tcp 2001:db8:acad:a::/64 any</b> R1(config-ipv6-acl)# <b>permit tcp any any eq 22</b> R1(config-ipv6-acl)# <b>line vty 0 4</b> R1(config-line)# <b>ipv6 access-class RESTRICT-VTY in</b> R1(config-line)# <b>end</b>	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)# <b>ipv6 access-list RESTRICTED-LAN</b> R1(config-ipv6-acl)# <b>remark Block Telnet from outside</b> R1(config-ipv6-acl)# <b>deny tcp any 2001:db8:acad:a::/64 eq telnet</b> R1(config-ipv6-acl)# <b>permit ipv6 any any</b> R1(config-ipv6-acl)# <b>int g0/1</b> R1(config-if)# <b>ipv6 traffic-filter RESTRICTED-LAN out</b> R1(config-if)# <b>end</b>	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# <b>show ipv6 access-lists RESTRICTED-LAN</b>	Verificar la ACL
R1# <b>clear ipv6 access-list RESTRICTED-LAN</b>	Limpia los contadores de coincidencia.
<b>DHCP</b>	
R2(config)# <b>ip dhcp excluded-address 192.168.0.1 192.168.0.9</b>	Excluye un rango de direcciones IP a asignar.
R2(config)# <b>ip dhcp pool R1G1</b> R2(dhcp-config)# <b>network 192.168.1.0 255.255.255.0</b> R2(dhcp-config)# <b>default-router 192.168.1.1</b> R2(dhcp-config)# <b>dns-server 209.165.200.225</b> R2(dhcp-config)# <b>domain-name ccna-lab.com</b> R2(dhcp-config)# <b>lease 2</b>	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)# <b>interface g0/0</b>	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.
<b>CONFIGURACIÓN CON ESTADO (DHCP) Y SIN ESTADO (SLAAC) IPV6</b>	
S1(config)# <b>interface vlan 1</b> S1(config-if)# <b>ipv6 address autoconfig</b>	Para obtener una IPv6 a través de SLAAC
R1(config)# <b>ipv6 dhcp pool IPV6POOL-A</b>	Configurar un servidor DHCP IPv6. Se crea el pool DHCP.
R1(config-dhcpv6)# <b>domain-name ccna-statelessDHCPv6.com</b>	Se asigna un nombre al pool. Este DHCP es sin estado.
R1(config-dhcpv6)# <b>dns-server 2001:db8:acad:a::abcd</b>	Asigna una dirección del servidor DNS.
R1(config)# <b>interface g0/1</b> R1(config-if)# <b>ipv6 dhcp server IPV6POOL-A</b>	Agrega un prefijo de red al pool. Se asigna el pool a una interfaz
R1(config-if)# <b>ipv6 nd other-config-flag</b>	Permite la detección de redes con paquetes de descubrimiento de vecinos (ND) en una interfaz
R1(config-dhcpv6)# <b>address prefix 2001:db8:acad:a::/64</b> R1(config-dhcpv6)# <b>domain-name ccna-StatefulDHCPv6.com</b>	Para configurar un DHCP con estado. Para definir una dirección de asignación.
R1# <b>show ipv6 dhcp binding</b> R1# <b>show ipv6 dhcp pool</b>	Verificar asignación de IP e información del pool DHCP.
R1(config)# <b>interface g0/1</b> R1(config-if)# <b>shutdown</b> R1(config-if)# <b>ipv6 nd managed-config-flag</b> R1(config-if)# <b>no shutdown</b> R1(config-if)# <b>end</b>	Para permitir que la interfaz envíe mensajes RA (Router Advertisement)
S1(config)# <b>interface vlan 1</b> S1(config-if)# <b>ipv6 address autoconfig</b>	Permite a la interfaz VLAN obtener una dirección IPv6 a través de SLAAC.
<b>NAT</b>	
Gateway(config)# <b>ip nat inside source static 192.168.1.20 209.165.200.225</b>	Configura un NAT estático.
Gateway(config)# <b>interface g0/1</b> Gateway(config-if)# <b>ip nat inside</b> Gateway(config-if)# <b>interface s0/0/1</b> Gateway(config-if)# <b>ip nat outside</b>	Define la interfaz que va a la red interna  Define la interfaz que va a la red externa
Gateway# <b>show ip nat translations</b>	Verifica la traducción
Gateway# <b>show ip nat statistics</b>	Verificar estadísticas de NAT
Gateway# <b>clear ip nat translation *</b> Gateway# <b>clear ip nat statistics</b>	Limpiar la tabla y estadísticas

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