

Comandos Packet tracer

1. Modo EXEC Usuario

Este es el nivel más básico de acceso. Los comandos aquí son limitados y se usan principalmente para verificar el estado del dispositivo.

- enable – Cambia al modo EXEC privilegiado.
- exit – Sale de la sesión actual.

2. Modo EXEC Privilegiado

Este modo permite ejecutar comandos de diagnóstico y configuración, así como acceder a configuraciones más avanzadas.

- configure terminal – Entra al modo de configuración global.
- show running-config – Muestra la configuración activa del dispositivo.
- show startup-config – Muestra la configuración almacenada en la NVRAM.
- show ip interface brief – Muestra un resumen de las interfaces IP y su estado.
- show version – Muestra información sobre el hardware y el software del dispositivo.
- ping [dirección IP] – Envía paquetes ICMP para verificar conectividad.
- traceroute [dirección IP] – Muestra la ruta que sigue el tráfico para llegar a la dirección de destino.
- copy running-config startup-config – Guarda la configuración activa en la configuración de inicio.

3. Modo de Configuración Global

Desde aquí, puedes configurar parámetros generales del dispositivo.

- hostname [nombre] – Cambia el nombre del dispositivo.
- enable secret [contraseña] – Configura una contraseña secreta encriptada para el modo privilegiado.
- no ip domain-lookup – Desactiva la resolución de nombres de dominio.
- banner motd # [mensaje] # – Configura un mensaje de advertencia (Message of the Day).
- ip default-gateway [dirección IP] – Configura la puerta de enlace predeterminada.
- service password-encryption – Encripta todas las contraseñas en el archivo de configuración.

4. Modo de Configuración de Interfaces

Este modo se usa para configurar las interfaces de red.

- interface [tipo][número] – Entra a la configuración de una interfaz específica (ej: interface fastethernet 0/0).
- ip address [dirección IP] [máscara de subred] – Configura una dirección IP y una máscara de subred en la interfaz.
- no shutdown – Habilita la interfaz (por defecto están deshabilitadas).
- description [texto] – Agrega una descripción a la interfaz.
- duplex [auto|full|half] – Configura el modo de dúplex de la interfaz.
- speed [auto|10|100|1000] – Configura la velocidad de la interfaz.
- ipv6 address [dirección IPv6] – Asigna una dirección IPv6 a la interfaz.
- shutdown – Desactiva la interfaz.

5. Modo de Configuración de Subinterfaces

Para crear y configurar subinterfaces en routers.

- interface [nombre].[número de subinterfaz] – Crea una subinterfaz (ej: interface gigabitethernet0/0.10).
- encapsulation dot1Q [vlan-id] – Configura la encapsulación VLAN en una subinterfaz.
- ip address [dirección IP] [máscara de subred] – Asigna una dirección IP a la subinterfaz.

6. Modo de Configuración de Rutas Estáticas

Para configurar rutas estáticas manualmente.

- ip route [red] [máscara] [next-hop] – Configura una ruta estática hacia una red específica.
- ipv6 route [red] [next-hop] – Configura una ruta estática para IPv6.

7. Modo de Configuración de VLAN

Comandos para configurar VLANs en switches.

- vlan [id] – Crea o accede a la configuración de una VLAN.
- name [nombre] – Asigna un nombre a la VLAN.
- interface [nombre de interfaz] – Selecciona una interfaz para configuración.
- switchport mode access – Configura la interfaz en modo de acceso.
- switchport access vlan [id] – Asigna la interfaz a una VLAN específica.
- switchport mode trunk – Configura la interfaz en modo trunk.
- switchport trunk allowed vlan [lista de VLANs] – Permite VLANs específicas en una interfaz trunk.

8. Modo de Configuración de RIP

Protocolo de enrutamiento dinámico RIP.

- router rip – Activa el protocolo RIP.
- version 2 – Configura la versión 2 de RIP.
- network [dirección de red] – Asigna redes para usar RIP.

9. Modo de Configuración OSPF

Protocolo de enrutamiento OSPF.

- router ospf [process-id] – Activa OSPF con un ID de proceso.
- network [dirección] [wildcard-mask] area [área] – Configura una red en un área OSPF.

10. Configuración de Contraseñas y Seguridad

Para gestionar la seguridad y autenticación.

- line console 0 – Configura la consola del dispositivo.
- password [contraseña] – Asigna una contraseña a la consola o VTY.
- login – Habilita el uso de la contraseña configurada.
- line vty 0 4 – Configura las líneas VTY (para acceso remoto).
- enable secret [contraseña] – Establece una contraseña encriptada para el modo privilegiado.

11. Configuración de NAT (Network Address Translation)

Para traducir direcciones IP privadas a públicas.

- ip nat inside source list [ACL] interface [interface] overload – Configura NAT sobrecargado.
- ip nat inside – Marca una interfaz como "inside" para NAT.
- ip nat outside – Marca una interfaz como "outside" para NAT.

12. DHCP (Dynamic Host Configuration Protocol)

Configurar un servidor DHCP en el router.

- ip dhcp pool [nombre] – Crea un pool de direcciones DHCP.
- network [dirección IP] [máscara] – Define la red que va a servir el pool.
- default-router [dirección IP] – Asigna una puerta de enlace predeterminada.
- dns-server [dirección IP] – Asigna un servidor DNS.

13. ACL (Access Control Lists)

Configurar listas de control de acceso.

- access-list [número] permit [protocolo] [origen] [wildcard] [destino] [wildcard] – Crea una ACL estándar o extendida.
- ip access-group [número] in|out – Asigna una ACL a una interfaz.

14. Configuración de EtherChannel

Para configurar la agregación de enlaces.

- interface port-channel [número] – Crea una interfaz de canal de puertos.
- channel-group [número] mode [on|auto|desirable] – Asigna interfaces físicas al EtherChannel.

15. Configuración de STP (Spanning Tree Protocol)

Comandos para gestionar STP.

- spanning-tree mode [pvst|rapid-pvst|mst] – Configura el modo de STP.
- spanning-tree vlan [id] root primary – Configura el switch como root para una VLAN.

16. Comandos SNMP (Simple Network Management Protocol)

Para la configuración y monitoreo de dispositivos de red usando SNMP.

- snmp-server community [nombre] [ro|rw] – Configura una comunidad SNMP con permisos de solo lectura (ro) o lectura/escritura (rw).
- snmp-server location [ubicación] – Especifica la ubicación del dispositivo.
- snmp-server contact [nombre] – Especifica el contacto responsable del dispositivo.
- snmp-server enable traps [opciones] – Habilita el envío de traps SNMP para eventos específicos (por ejemplo, snmp-server enable traps ospf).

17. Configuración de HSRP (Hot Standby Router Protocol)

HSRP permite la alta disponibilidad de routers.

- standby [grupo] ip [dirección IP] – Configura la dirección IP virtual de HSRP.
- standby [grupo] priority [valor] – Configura la prioridad del router (mayor valor, mayor prioridad).
- standby [grupo] preempt – Permite que el router tome el rol de activo si tiene mayor prioridad.
- standby [grupo] track [interfaz] [decremento] – Reduce la prioridad si una interfaz específica falla.

18. Configuración de VRRP (Virtual Router Redundancy Protocol)

Similar a HSRP, VRRP proporciona redundancia entre routers.

- vrrp [grupo] ip [dirección IP] – Configura la dirección IP virtual de VRRP.

- vrrp [grupo] priority [valor] – Configura la prioridad del router.
- vrrp [grupo] preempt – Habilita la preempción, permitiendo que un router con mayor prioridad se convierta en el router maestro.

19. Configuración de GLBP (Gateway Load Balancing Protocol)

Protocolo de balanceo de carga entre múltiples routers.

- glbp [grupo] ip [dirección IP] – Configura la dirección IP virtual de GLBP.
- glbp [grupo] priority [valor] – Configura la prioridad del router.
- glbp [grupo] preempt – Permite la preempción de un router.
- glbp [grupo] load-balancing [round-robin|weighted|host-dependent] – Configura el método de balanceo de carga.

20. Comandos EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP es un protocolo de enrutamiento avanzado.

- router eigrp [autonomous-system] – Habilita EIGRP en el sistema autónomo especificado.
- network [dirección IP] [wildcard-mask] – Especifica las redes que participarán en EIGRP.
- passive-interface [nombre de interfaz] – Evita que EIGRP envíe actualizaciones de enrutamiento a través de una interfaz específica.
- eigrp router-id [ID del router] – Configura manualmente el ID del router EIGRP.
- bandwidth [kbps] – Configura el ancho de banda en la interfaz para ajustar el cálculo métrico de EIGRP.
- variance [valor] – Permite el balanceo de carga de rutas no idénticas con EIGRP.

21. Comandos BGP (Border Gateway Protocol)

BGP es un protocolo de enrutamiento utilizado en redes grandes como Internet.

- router bgp [AS-number] – Inicia la configuración de BGP en un sistema autónomo.
- neighbor [dirección IP] remote-as [AS-number] – Define una relación de vecino BGP con un sistema autónomo remoto.
- network [dirección IP] mask [máscara] – Anuncia una red en BGP.
- neighbor [dirección IP] next-hop-self – Fuerza que este router use su propia IP como next-hop.
- neighbor [dirección IP] shutdown – Desactiva una conexión BGP.
- aggregate-address [dirección IP] [máscara] – Crea una ruta agregada.

22. Comandos PPP (Point-to-Point Protocol)

Para configurar la autenticación y el encapsulamiento en enlaces punto a punto.

- encapsulation ppp – Habilita el encapsulamiento PPP en la interfaz.
- ppp authentication chap – Habilita la autenticación CHAP en PPP.
- ppp authentication pap – Habilita la autenticación PAP en PPP.
- ppp chap hostname [nombre de usuario] – Especifica el nombre de usuario para CHAP.
- ppp chap password [contraseña] – Especifica la contraseña para CHAP.

23. Configuración de QoS (Quality of Service)

Para priorizar el tráfico en la red.

- policy-map [nombre] – Crea o entra en una política de QoS.
- class-map [nombre] – Crea o entra en una clase para definir el tráfico a priorizar.
- match ip address [ACL] – Especifica el tráfico a clasificar basado en una ACL.
- priority [kbps] – Asigna prioridad y especifica el ancho de banda garantizado.
- bandwidth [kbps] – Reserva ancho de banda para una clase específica.
- service-policy output [nombre de política] – Asigna una política de QoS a una interfaz de salida.

24. Configuración de Port Security en Switches

Controla qué dispositivos pueden conectarse a un puerto de switch.

- switchport port-security – Habilita la seguridad de puertos en una interfaz.
- switchport port-security maximum [número] – Establece el número máximo de direcciones MAC permitidas en el puerto.
- switchport port-security mac-address [dirección MAC] – Establece una dirección MAC estática en el puerto.
- switchport port-security violation [protect|restrict|shutdown] – Define la acción a tomar cuando se viola la seguridad del puerto.
- switchport port-security aging time [minutos] – Configura el tiempo de envejecimiento para las direcciones MAC.

25. Configuración de SPAN (Switched Port Analyzer)

SPAN permite monitorear tráfico en un puerto o VLAN.

- monitor session [número] source interface [nombre de interfaz] – Especifica el puerto de origen que será monitoreado.
- monitor session [número] destination interface [nombre de interfaz] – Especifica el puerto de destino donde se enviará el tráfico monitoreado.

- `monitor session [número] filter vlan [id]` – Filtra el tráfico por VLAN.

26. Comandos AAA (Authentication, Authorization, and Accounting)

Para gestionar la autenticación y autorización en los dispositivos.

- `aaa new-model` – Habilita el modelo de AAA en el dispositivo.
- `aaa authentication login default group [radius|tacacs+] local` – Configura la autenticación usando RADIUS o TACACS+ y luego el método local como respaldo.
- `aaa authorization exec default group [radius|tacacs+]` – Configura la autorización de comandos.
- `aaa accounting exec default start-stop group [radius|tacacs+]` – Habilita la contabilidad (accounting) de comandos ejecutados.

27. Comandos NTP (Network Time Protocol)

Sincroniza la hora de los dispositivos de red.

- `ntp server [dirección IP]` – Configura un servidor NTP.
- `ntp peer [dirección IP]` – Configura un dispositivo NTP como par.
- `ntp update-calendar` – Actualiza el calendario hardware con la hora NTP.
- `clock timezone [zona] [diferencia]` – Configura la zona horaria.
- `show ntp status` – Muestra el estado de sincronización NTP.

28. Configuración de VTP (VLAN Trunking Protocol)

Para gestionar las VLAN en un dominio de switches.

- `vtp mode [server|client|transparent]` – Establece el modo de operación de VTP.
- `vtp domain [nombre del dominio]` – Configura el nombre del dominio VTP.
- `vtp password [contraseña]` – Establece una contraseña para el dominio VTP.
- `vtp pruning` – Habilita el pruning de VLAN en el dominio VTP.

29. Configuración de MPLS (Multiprotocol Label Switching)

Comandos básicos para configurar MPLS.

- `mpls ip` – Habilita MPLS en el dispositivo.
- `mpls label protocol [ldp|tdp]` – Configura el protocolo de distribución de etiquetas MPLS.
- `mpls ldp router-id [interfaz] force` – Asigna manualmente un router ID para LDP.
- `mpls traffic-eng tunnels` – Habilita los túneles de ingeniería de tráfico MPLS.

30. Comandos de VRF (Virtual Routing and Forwarding)

VRF permite que un router mantenga varias tablas de enrutamiento.

- `ip vrf [nombre]` – Crea una VRF.
- `rd [ID del sistema autónomo]:[número]` – Asigna un identificador de ruta distinguido (Route Distinguisher) a la VRF.
- `interface [nombre] vrf forwarding [nombre de VRF]` – Asocia una interfaz con una VRF.

31. Comandos para IPSec (Internet Protocol Security)

IPSec se utiliza para asegurar la transmisión de datos a través de redes inseguras, como Internet.

- `crypto isakmp policy [número]` – Crea o configura una política ISAKMP.
- `authentication pre-share` – Configura la autenticación precompartida en la política ISAKMP.
- `encryption [aes|3des|des]` – Configura el tipo de cifrado para IPSec.
- `hash [sha|md5]` – Configura el algoritmo de hashing.
- `group [grupo]` – Configura el grupo de Diffie-Hellman para la negociación de claves.
- `crypto isakmp key [clave] address [dirección IP]` – Configura una clave precompartida con un dispositivo remoto.
- `crypto ipsec transform-set [nombre] [encryption] [hash]` – Crea un conjunto de transformaciones de IPSec.
- `crypto map [nombre] [secuencia] ipsec-isakmp` – Crea un mapa criptográfico que se vinculará a una interfaz.
- `set peer [dirección IP]` – Configura el dispositivo remoto en el mapa criptográfico.
- `set transform-set [nombre]` – Asocia un conjunto de transformaciones IPSec con el mapa criptográfico.
- `interface [nombre]` – Configura la interfaz para asociar el mapa criptográfico.
- `crypto map [nombre]` – Asocia el mapa criptográfico a la interfaz.

32. Configuración de DHCP Snooping

Protege la red contra ataques de DHCP.

- `ip dhcp snooping` – Habilita el DHCP Snooping globalmente.
- `ip dhcp snooping vlan [número]` – Habilita DHCP Snooping en una VLAN específica.
- `ip dhcp snooping trust` – Marca una interfaz como confiable para recibir mensajes DHCP.
- `ip dhcp snooping limit rate [paquetes por segundo]` – Limita la tasa de tráfico DHCP que puede pasar por una interfaz.
- `show ip dhcp snooping` – Muestra la configuración de DHCP Snooping en el dispositivo.

33. Comandos de Port Aggregation Protocol (PAgP)

PAgP se usa para configurar EtherChannel en switches.

- `channel-group [número] mode [auto|desirable]` – Configura el canal de puertos con PAgP.
 - `auto` – Configura el puerto para negociar la agregación solo si el otro extremo la solicita.
 - `desirable` – El puerto negocia activamente la agregación.

34. Configuración de LACP (Link Aggregation Control Protocol)

LACP es otra forma de configurar EtherChannel, estandarizada por IEEE.

- `channel-group [número] mode [active|passive]` – Configura la agregación de enlaces utilizando LACP.
 - `active` – Inicia la negociación activa de LACP.
 - `passive` – Espera recibir solicitudes LACP antes de negociar.

35. Comandos para NAT (Network Address Translation) Dinámico

Traducción de direcciones IP dinámicas.

- `ip nat inside` – Marca una interfaz como "inside" para NAT.
- `ip nat outside` – Marca una interfaz como "outside" para NAT.
- `ip nat pool [nombre] [inicio-IP] [fin-IP] netmask [máscara]` – Define un pool de direcciones IP para NAT dinámico.
- `ip nat inside source list [ACL] pool [nombre]` – Asocia una lista de control de acceso (ACL) con el pool de NAT.
- `ip nat inside source list [ACL] pool [nombre] overload` – Permite NAT con sobrecarga (PAT), donde múltiples direcciones privadas usan una única IP pública.

36. Comandos para NHRP (Next Hop Resolution Protocol)

NHRP se utiliza en redes DMVPN para resolver nexthops dinámicamente.

- `ip nhrp map [dirección IP pública] [dirección IP privada]` – Establece un mapeo entre una dirección IP pública y una privada.
- `ip nhrp network-id [número]` – Configura el identificador de red NHRP en la interfaz.
- `ip nhrp nhs [dirección IP]` – Establece el router de la sede central como el servidor de NHRP.
- `ip nhrp shortcut` – Habilita el uso de atajos en NHRP para rutas dinámicas.

37. Configuración de DMVPN (Dynamic Multipoint Virtual Private Network)

DMVPN permite la creación de conexiones VPN dinámicas.

- interface tunnel [número] – Crea una interfaz de túnel para DMVPN.
- tunnel source [interfaz] – Especifica la interfaz de origen para el túnel.
- tunnel mode gre multipoint – Configura el modo GRE multipunto para DMVPN.
- ip nhrp map multicast dynamic – Permite el mapeo de multidifusión en NHRP.
- ip nhrp network-id [número] – Asigna un identificador de red para NHRP.

38. Comandos de HSRP Avanzado

HSRP para redundancia de routers.

- standby [grupo] authentication md5 key-string [clave] – Configura la autenticación MD5 para HSRP.
- standby [grupo] timers [intervalo hello] [intervalo dead] – Ajusta los temporizadores de HSRP.

39. Configuración de LLDP (Link Layer Discovery Protocol)

LLDP es un protocolo de descubrimiento de dispositivos, similar a CDP pero estandarizado por IEEE.

- lldp run – Habilita LLDP globalmente en el dispositivo.
- lldp transmit – Habilita la transmisión de información LLDP en una interfaz.
- lldp receive – Habilita la recepción de información LLDP en una interfaz.
- show lldp neighbors – Muestra los dispositivos vecinos descubiertos mediante LLDP.

40. Configuración de IPv6

Comandos específicos para la configuración de IPv6 en routers y switches.

- ipv6 unicast-routing – Habilita el enrutamiento IPv6 en el dispositivo.
- interface [nombre] – Entra a la configuración de la interfaz.
- ipv6 address [dirección IPv6]/[longitud de prefijo] – Asigna una dirección IPv6 a la interfaz.
- ipv6 enable – Habilita IPv6 en la interfaz sin asignar una dirección estática.
- ipv6 route [red IPv6] [next-hop] – Configura una ruta estática en IPv6.
- ipv6 dhcp pool [nombre] – Crea un pool DHCPv6 para asignar direcciones IPv6 dinámicas.

41. Comandos para OSPFv3 (OSPF para IPv6)

OSPFv3 es la versión de OSPF que soporta IPv6.

- router ospfv3 [process-id] – Inicia el proceso OSPFv3.
- address-family ipv6 unicast – Habilita OSPFv3 para IPv6 unicast.
- interface [nombre] – Configura la interfaz para OSPFv3.

- `ipv6 ospf [process-id] area [número de área]` – Asocia la interfaz con un área OSPFv3.
- `show ipv6 ospf neighbor` – Muestra los vecinos de OSPFv3.

42. Comandos de VRF-Lite

VRF-Lite permite la creación de múltiples instancias de tablas de enrutamiento.

- `ip vrf [nombre]` – Crea una instancia VRF.
- `rd [AS]:[valor]` – Configura un identificador de Distinguido de Ruta (RD) para la VRF.
- `interface [nombre]` – Entra en la configuración de la interfaz.
- `ip vrf forwarding [nombre]` – Asocia la interfaz a una VRF.
- `ip route vrf [nombre VRF] [red] [máscara] [nexthop]` – Configura una ruta en una VRF específica.

43. Configuración de MPLS VPN

Multiprotocol Label Switching para redes VPN.

- `mpls ip` – Habilita MPLS en las interfaces.
- `ip vrf [nombre VRF]` – Crea una VRF.
- `rd [AS]:[valor]` – Define un identificador de ruta (RD) para la VRF.
- `route-target import [valor]` – Define el target de importación para la VRF.
- `route-target export [valor]` – Define el target de exportación para la VRF.

44. Comandos para VRRP Avanzado

VRRP (Virtual Router Redundancy Protocol) avanzado.

- `vrrp [grupo] priority [valor]` – Configura la prioridad del router.
- `vrrp [grupo] preempt` – Habilita la preempción de VRRP.
- `vrrp [grupo] authentication [palabra clave]` – Configura la autenticación para VRRP.

45. Configuración de IP SLA (Service-Level Agreement)

IP SLA permite monitorizar el rendimiento de la red y su tiempo de respuesta.

- `ip sla [número]` – Crea una operación de IP SLA.
- `icmp-echo [dirección IP]` – Configura una solicitud de eco ICMP (ping) para monitorización.
- `frequency [segundos]` – Establece la frecuencia con la que se ejecutará la operación.
- `ip sla schedule [número] start-time [ahora|hh:mm:ss] life [segundos]` – Programa el inicio y la duración de la operación de IP SLA.

- ip sla reaction-configuration [número] [tipo de condición] threshold-value [valor] – Configura una reacción basada en umbrales de rendimiento.
- show ip sla statistics – Muestra las estadísticas de las operaciones de IP SLA.

46. Configuración de Syslog

Syslog permite la gestión centralizada de logs de dispositivos de red.

- logging [dirección IP] – Configura el servidor Syslog remoto.
- logging trap [nivel] – Configura el nivel de severidad de los mensajes que se enviarán al servidor Syslog (de 0 a 7).
 - 0 – Emergencias
 - 1 – Alertas
 - 2 – Críticos
 - 3 – Errores
 - 4 – Advertencias
 - 5 – Notificaciones
 - 6 – Informativos
 - 7 – Depuración
- logging buffered [tamaño] – Configura el tamaño del buffer de logs locales.
- show logging – Muestra los mensajes del sistema almacenados en el dispositivo.

47. Configuración de Control Plane Policing (CoPP)

CoPP protege el plano de control del router contra ataques DoS o sobrecargas.

- access-list [número] permit [protocolo] [dirección IP] – Crea una lista de control de acceso para filtrar tráfico.
- class-map [nombre] – Crea una clase de tráfico para aplicar políticas.
- policy-map [nombre] – Crea una política de control de tráfico.
- service-policy input [nombre de política] – Aplica una política al tráfico entrante en el plano de control.
- control-plane – Entra en la configuración del plano de control.

48. Configuración de NetFlow

NetFlow permite la recolección de estadísticas sobre el tráfico de red.

- ip flow ingress – Habilita la captura de tráfico entrante.

- ip flow egress – Habilita la captura de tráfico saliente.
- ip flow-export destination [dirección IP] [puerto] – Configura el servidor donde se enviarán los datos de NetFlow.
- ip flow-export source [interfaz] – Configura la interfaz de origen para los datos de exportación de NetFlow.
- show ip flow statistics – Muestra las estadísticas de NetFlow.
- ip flow-export version [5 | 9] – Especifica la versión de NetFlow que se usará para la exportación.

49. Configuración de 802.1X (Autenticación basada en puertos)

802.1X se usa para la autenticación de dispositivos en redes LAN, permitiendo el acceso a usuarios autorizados.

- dot1x system-auth-control – Habilita 802.1X en todo el sistema.
- interface [nombre de interfaz] – Selecciona la interfaz donde se habilitará la autenticación.
- dot1x port-control [auto | force-authorized | force-unauthorized] – Configura el control de acceso del puerto.
 - auto – Autenticación basada en 802.1X.
 - force-authorized – El puerto se mantiene autorizado sin importar la autenticación.
 - force-unauthorized – El puerto permanece no autorizado, sin importar la autenticación.
- dot1x timeout [segundos] – Configura el tiempo de espera para la autenticación 802.1X.
- show dot1x – Muestra el estado de la autenticación 802.1X en el dispositivo.

50. Configuración de FHRP (First Hop Redundancy Protocol) con IPv6

Los protocolos como HSRP, VRRP, y GLBP tienen soporte para IPv6.

HSRP para IPv6:

- interface [nombre] – Entra en la configuración de la interfaz.
- standby version 2 – Habilita HSRPv2 (soporta IPv6).
- standby [grupo] ipv6 autoconfig – Configura una dirección IP virtual HSRP usando autoconfiguración.
- standby [grupo] priority [número] – Configura la prioridad del router en HSRP.
- standby [grupo] preempt – Habilita la preempción de HSRP.

VRRP para IPv6:

- vrrp [grupo] address-family ipv6 – Habilita VRRPv3 con soporte para IPv6.

- vrrp [grupo] ipv6 address [dirección IPv6] – Configura la dirección IPv6 virtual para VRRP.
- vrrp [grupo] priority [número] – Configura la prioridad del router en VRRP.

51. Configuración de EtherChannel con IPv6

EtherChannel con soporte para IPv6 permite la agregación de enlaces para aumentar el ancho de banda.

- interface range [interfaz1 - interfazN] – Selecciona el rango de interfaces para agregarlas al EtherChannel.
- channel-group [número] mode [active|passive|on] – Configura EtherChannel en las interfaces seleccionadas.
- interface port-channel [número] – Entra en la configuración del EtherChannel.
- ipv6 address [dirección IPv6]/[prefijo] – Asigna una dirección IPv6 al EtherChannel.

52. Comandos de Cisco TrustSec

TrustSec permite la segmentación basada en políticas y la autenticación de usuarios y dispositivos.

- cts role-based enforcement – Habilita el control de acceso basado en roles en la interfaz.
- cts credentials [nombre de usuario] password [contraseña] – Configura las credenciales CTS en el dispositivo.
- cts authorization list [nombre de lista] – Configura una lista de autorización CTS.
- show cts – Muestra la configuración de TrustSec en el dispositivo.

53. Configuración de GRE sobre IPv6

GRE (Generic Routing Encapsulation) es un protocolo de túnel que puede encapsular tráfico IPv6.

- interface tunnel [número] – Crea una interfaz de túnel.
- tunnel source [dirección IP|interfaz] – Especifica la fuente del túnel.
- tunnel destination [dirección IP] – Especifica el destino del túnel.
- tunnel mode gre ipv6 – Configura el túnel para operar con tráfico GRE sobre IPv6.
- ipv6 address [dirección IPv6]/[prefijo] – Asigna una dirección IPv6 a la interfaz de túnel.

54. Configuración de DMVPN (Dynamic Multipoint VPN) con IPv6

DMVPN permite establecer VPN dinámicas con IPv6.

- interface tunnel [número] – Crea la interfaz de túnel para DMVPN.
- tunnel source [interfaz] – Configura la interfaz fuente del túnel.
- tunnel mode gre multipoint – Configura GRE multipunto para el túnel DMVPN.

- `ipv6 nhrp map [dirección IPv6 pública] [dirección IPv6 privada]` – Mapea la dirección pública y privada para NHRP con IPv6.
- `ipv6 nhrp network-id [número]` – Configura el ID de la red NHRP para IPv6.

55. Configuración de MPLS con IPv6

MPLS (Multiprotocol Label Switching) también tiene soporte para IPv6 en redes avanzadas.

- `mpls ip` – Habilita MPLS en las interfaces (para IPv6 sobre MPLS).
- `ipv6 cef` – Habilita la tabla de reenvío de expresiones para IPv6 (CEF).
- `mpls label protocol ldp` – Configura el protocolo de distribución de etiquetas MPLS.
- `mpls ipv6 forwarding` – Habilita el reenvío de MPLS para tráfico IPv6.

56. Comandos para IS-IS (Intermediate System to Intermediate System) con IPv6

IS-IS es un protocolo de enrutamiento de estado de enlace que también admite IPv6.

- `router isis [nombre de proceso]` – Inicia la configuración de IS-IS.
- `address-family ipv6` – Configura IS-IS para IPv6.
- `interface [nombre]` – Entra en la configuración de la interfaz.
- `ipv6 router isis [nombre de proceso]` – Habilita IS-IS para IPv6 en la interfaz.
- `show isis neighbors` – Muestra los vecinos IS-IS en la red.