Comándos CISCO CCNA Exploration

Daniel García Capel

13 de abril de 2011

Índice

1. General

! comentario Comentario.

 # hostname <nombre> Establece el nombre del equipo.

(config)# [no]ip domain-lookup Activa/Desactiva la búqueda DNS, evitando que el router se bloquee ante un comando mal introducido.

1.1. Información

 # show version Muestra información sobre la versión del software Cisco IOS que actualmente se está ejecutando en el router.

 # show ip route [ip] Muestra todas las rutas o una concreta.

 # show ip protocols Muestra información de los protocolos de enrutamiento.

1.2. Arranque

Información

 # show boot Muestra información de la variables de entorno del arranque.

Recuperación TFTP

IP_ADDRESS=<ip> IP de la primera interfaz del Router.

IP_SUBNET_MASK=<máscara> Máscara de la primera interfaz del Router.

DEFAULT_GATEWAY=<ip> Puerta de enlace.

TFTP_SERVER=<ip> IP del servidor TFTP que contiene la imagen a restaurar.

TFTP_FILE=<nombre ios> Nombre de la IOS en el servidor TFTP.

tftpdnld Ejecuta el modo de recuperación.

reset Reinicia el dispositivo para cargar la IOS.

Restauración XModem

xmodem [-cyr][nombre de archivo] Activa la recepción del fichero binario mediante el protocolo XModem mediante el enlace de consola. -c: CRC de 16 bits.
-y: Protocolo YModem.
-r: Copia la imagen a la memoria RAM.

1.3. Depuración

 # no debug all | undebug all Activa/Desactiva todos los modos de depuración.

(config)# service timestamps debug datetime msec Agrega una marca horario a los mensajes de Debug o de Registro.

 # show processes Muestra el uso de CPU de los procesos.

 # terminal monitor Muestra los resultados de debug en las conexiones VTY (telnet o ssh).

1.4. Respaldo y Restauración Configuración

reload Reinicia el dispositivo.

Local

copy running-config startup-config Copia la configuración de la DRAM a la NVRAM.

copy system:<running-config | startup-config>flash:<nombre archivo> Copia la configuración de la DRAM a un archivo de la NVRAM.

Remota

copy <system:running-config | nvram:startup-config>tftp:<ruta> Creación de la copia de seguridad.

copy tftp:<ruta><system:running-config | nvram:startup-config> Restauración de la copia de seguridad.

1.5. Ficheros

show file system Lista los sistemas de ficheros disponibles en el dispositivo.

dir Lista el contenido del directorio actual.

pwd Muestra el directorio actual. No disponible en Packet Tracer.

cd [tftp | flash | system | nvram:]<directorio> Cambia de directorio (change directory). No disponible en Packet Tracer.

copy <origen><destino> Copia un fichero.

delete <fichero> Borra un fichero.

rename <nombre inicial><nombre final> Renombra un fichero

archive tar /x Extrae el paquete TAR.

1.6. Historial

[no]terminal history habilita/deshabilita el historial del terminal.

terminal history size <tamaño> configura el tamaño del historial del terminal.

terminal no history size restablece el tamaño del terminal al valor predeterminado # 10 comandos #.

1.7. Servidor Web

Nota: no funciona en Packet Tracer 5.3.2.

(config)# ip http authentification <enable|local|tacacs> Activa la autentificación del servidor http.
enable: Utiliza la contraseña de enable.
local: Base de datos local del usuario
tacacs: Usa el servidor tacacs.

(config)# ip http server activa el servidor HTTP.

(config)# ip http secure-server Activa el servidor HTTPS.

1.8. Interfaces

Información

 # show ip interfaces <interfaz> Muestra información de toda las interfaces o de una concreta.

 # show ip interfaces brief Muestra información de todas las interfaces en formato resumido.

Configuración IPv4

(config)# interface <interfaz> Accede a la configuración de la interfaz.

(config-if)# ip address <ip><máscara> Establece la dirección IP y máscara de red a la interfaz.

(config-if)# [no]shutdown Activa/Desactiva la interfaz.

(config-if)# description # descripción # Establece una descripción a la interfaz.

Configuración IPv6

(config)# ipv6 unicast-routing Habilita el reenvío de tráfico IPv6.

(config-if)# ipv6 address <ip 128bits>/<máscara prefijo> Establece la dirección IP y máscara de red a la interfaz.

(config-if)# ipv6 address <ip 64bits>/<máscara prefijo>eui-64 Establece la dirección IP utilizazándo en los últimos 64 bits la dirección MAC y la máscara de red a la interfaz.

Configuración Ethernet

(config)# interface <faN/N | feN/N> Accede a la configuración de la interfaz FastEthernet.

Configuración Serial

(config)# interface <sN/N | sN/N/N | lookbackNN > Accede a la configuración de la interfaz Serial.

(config-if)# clock rate <bps> Establece la velocidad en bps de la interfaz Serial que hace de DCE.

Configuración LoopBack

(config)# interface <loN/N | loopbackN/N> Accede a la configuración de la interfaz de Loopback.

(config-if)# ip add <ip><máscara> Establece la (se permiten varias) dirección IP de la Interfaz.

2. Administración/Seguridad

2.1. General

(config)# banner [login | motd]# mensaje # Establece el mensaje de login o del día (Message of the Day).

(config)# line <vty | console>[nºinicial][nºfinal] Accede al modo de administración.

(config)# [no]service password-encryption Habilita/Deshabilita la codificación de las contraseñas de servicio.

2.2. Usuarios

(config)# username <usuario><password | secret><contraseña> Añade un usuario al equipo.
password: contraseña de tipo 7, propietaria de cisco y con seguridad baja.
secret: contraseña de tipo 5, md5 con seguridad alta, aunque algunas configuraciones pueden no funcionar, como por ejemplo PPP con autenticación PAP o CHAP.

(config)# enable <password | secret> Activa la contraseña para el modo privilegiado, en claro o codificada.

(config)# security passwords min-lenght <longitud> Establece la longitud mínima de todas las contraseña del sistema, no afectando a las ya establecidas.

2.3. Administración

General

(config)# login block-for <segundos>attempt <fallos>within <segundos> Bloquea durante un tiempo el intento de conexiones VTY si se produce un número de fallos en un tiempo determinado.

(config)# security authentication failute rate 5 log Activa el registro de eventos, como los fallos de autenticación.

2.3.1. Consola & VTY

(config-line)# [no]password <contraseña> Establece la contraseña o bloquea el inicio de sesión de la línea.

(config-line)# [no]login Habilita/Deshabilita la contraseña cuando se accede.

(config-line)# transport input <telnet | ssh | all> Establece el modo de acceso: telnet, ssh o cualquiera.

(config-line)# exec-timeout <minutos><segundos> Tiempo que mantiene una conexión inactiva abierta.

(config)# service tcp-keepalives-in Finaliza las conexiones que no responden como consecuencia de un periodo de inactividad en la conexión TCP.

2.3.2. SSH (Secure SHell)

Información

 # show ssh Muestra información del servidor SSH.

Configuración

(config)# hostname <nombre> Configura el nombre de Host.

(config)# ip domain-name <dominio> Establece el dominio de host.

(config)# crypto key generate rsa Genera las claves pública y privada para RSA.

(config)# ip ssh version <1 | 2> Activa la versión de SSH especificada.

(config)# line vty 0 15 Accede al modo de administración de las terminales virtuales (Virtual Terminal Lines).

(config-line)# transport input ssh Establece el modo de acceso a las vty por SSH.

Autenticación

(config-line)# password <contraseña> Se autentica mediante una contraseña.

(config-line)# login local Se autentica mediante un usuario y contraseña.

(config-line)# [no]login Habilita/Deshabilita la contraseña cuando se accede.

Conexión

(config)# ip ssh timeout <0-120 seg> Tiempo que permanece la conexión abierta sin actividad.

(config)# ip ssh authentication-retries <0-5> Número de conexiones simultaneas de un mismo usuario.

Otros

(config)# crypto key zeroize rsa Elimina las claves (pública y privada) de RSA.

2.4. Auditorías

(config)# service timestamps

SNMP (Simple Network Management Protocol) Nota: no funciona en Packet Tracer 5.3.2.

(config)# logging <ip> Define la IP donde enviar los mensajes de log.

(config)# logging trap <palabra clave> Establece el nivel de gravedad para el que se enviarán mensajes. Emergency: 0, Alert: 1, Critical: 2, Error: 3, Warning: 4, Notice: 5, Informational: 6, Debug: 7

(config)# logging console Establace el nivel de gravedad para el que se enviarán los mensajes a la consola.

2.5. Servicios

2.5.1. DNS (Domain Name Server)

(config)# ip name-server <dirección> Configura el Servidor de Nombres (DNS).

(config)# ip[v6]host <name>[puerto]<ip1>... <ip4> Asigna un nombre a una o varias direcciones de host.

2.5.2. DHCP (Dynamic Host Configuration Protocol)

Información

 # show ip dhcp binding Muestra una lista de todas las asignaciones de direcciones IP a direcciones MAC que proporcionó el servicio de DHCP.

 # show ip dhcp server [statistics] Muestra información numérica acerca de la cantidad de mensajes de DHCP que se envían y reciben.

 # show ip dhcp pool Resume la información del Pool de DHCP.

 # show ip dhcp conflict Muestra los conflictos en la asignación de direcciones.

Depuración (Básica)

 # show ip dhcp conflict

(config)# debug ip dhcp server packet

(config)# debug ip dhcp server events

Depuración (ACL)

(config)# access-list <nº lista>permit ip host 0.0.0.0 host 255.255.255.255 ACL que permite todo el tráfico.

(config)# debug ip packet detail <nº lista> Muestra los detalles de la ACL aplicada, de modo transparente para el dispositivo, es decir, sin interferir en el resto de las ACL.

Servidor (Básica)

(config)# [no]service dhcp Activa/Desactiva el servicio de DHCP. Si se dispone del servicio, por defecto está activado.

(config)# ip dhcp excluded-address <ip> Excluye de la asignación de DHCP una o varias direcciones IPs.

(config)# ip dhcp pool <nombre rango direcciones> Accede a configurar un rango (pool) de direcciones IP.

(dhcp-config)# network <ip><máscara> Agrega una red (obligatorio).

(dhcp-config)# default-route <ip> Establece la dirección por la que propaga la asignación de direcciones (obligatorio).

(dhcp-config)# domain-name <nombre> Establece el Nombre del Dominio (opcional).

(dhcp-config)# dns-server <ip> Establece el servidor de DNS (opcional).

(dhcp-config)# lease <dias | infinite>[horas][minutos] Define el tiempo de renovación de la dirección IP (opcional).

Servidor (Complementaria)

(config-if)# ip helper-address <ip servidor> Permite la propagación de servicios comunes (37 Tiempo, 49 TACACS, 53 DNS, 67 DHCP/BOOTP, 69 TFTP y 137&138 NetBIOS) a un servidor concreto.

(config-if)# ip fordward protocol udp <puerto>?? Permite la propagación de paquetes de servicio especificando especificando un puerto concreto.

Cliente

(config-if)# ip address dhcp Configura la interfaz para utilizar DHCP.

2.5.3. NAT (Network Address Translation)

Información/Depuración

 # show ip nat translation [verbose] Muestra la tabla de traducción NAT.

 # show ip nat statistics Muestra estadísticas de NAT.

 # [no]debug ip nat [detailed] Activa/Desactiva la depuración de NAT.

Tabla NAT

 # clear ip nat translation * Borra todas las traducciones NAT activas.

 # clear ip nat translation inside <ip global><ip local>[outside <local-ip><global-ip>] Elimina una simple entrada de traducción dinámica que contiene una traducción interna o ambas traducciones, interna y externa.

 # clear ip nat translation <protocol>inside <ip global>puerto global><ip local><puerto local>[outside <ip Elimina una entrada ampliada de traducción dinámica.

Configuración Estática 1:1

(config)# ip nat inside source static <ip interna><ip externa> Define como se traduce la dirección interna - externa.

(config-if)# ip nat <inside | outside> Aplica NAT en la interfaz correspondiente.

Configuración Dinámica con y sin Sobrecarga (N:M) Sin sobrecarga $N <= M$ y con sobrecarga (overload) $N >= M$.

(config)# access-list <nº ACL>permit <ip><máscara> ACL que define los host locales a traducirse.

(config)# ip nat pool <nombre pool = NAT-POOL2><ip pública inicio><ip pública fin> Define el rango de direcciones públicas a utilizar.

(config)# ip nat inside source list <nº ACL>pool <nombre pool = NAT-POOL2>[overload] Aplica NAT con el rango de direcciones privadas y públicas definidas anteriormente. El comando overload permite agregar el puerto a la traducción, es decir, que permita más de N equipos utilicen las M direcciones ip públicas.

(config-if)# ip nat <inside | outside> Aplica NAT en la interfaz privada o pública correspondiente.

Configuración Sobrecarga (N:1)

(config)# access-list <nº ACL><ip><máscara> ACL que permite el acceso a los host a locales a traducir.

(config)# ip nat inside source list 1 interface <interfaz>overload Aplica NAT con el rango de direcciones privadas y la pública, procedente de la interfaz. El comando overload permite agregar el número de puerto a la traducción, es decir, permite que varios equipos compartan la misma IP externa.

(config-if)# ip nat <inside | outside> Aplica NAT en la interfaz privada o pública correspondiente.

IP Fordwarding (Reenvío de Puertos)

(config)# ip nat inside source static [tcp | udp]<ip interna><puerto interno>interfaz <interfaz><puerto ext

Otros

(config)# ip nat translation timeout <segundos> Establece el tiempo que permanece una traducción sin volver a ser utilizada antes de ser borrada.

2.5.4. TFTP (Trivial File Transfer Protocol)

Nota: no funciona en Packet Tracer 5.3.1.

tftp-server nvram:[fichero]alias [alias fichero]

2.5.5. CDP (Cisco Discovery Protocol)

(config)# [no]cdp run Activa/Desactiva el protocolo de enlace CDP.

 # show cdp neighbors Muestra un resumen de los nodos vecinos.

 # show cdp neighbors detail Muestra en detalle los nodos vecinos.

2.5.6. SDM (Service Device Managent)

http://www.cisco.com/go/sdm

(config)# ip http server Activa el srrvidor HTTP.

(config)# ip http secure-server Activa el servidor HTTPS.

(config)# ip http autentication local Solo permite la autenticación de usuarios registrados.

(config)# username <usuario>privilege 15 secret <contraseña>

(config)# line vty 0 4

(config-line)# privilege level 15

(config-line)# login local

(config-line)# transport input telnet ssh

2.5.7. Prescindibles

Automático

(config)# auto secure [no interact]

Individuales Nota: todos los comandos excepto "no cdp run" y "no ip classless" no funcionan en Packet Tracer 5.3.1.

(config)# no service tcp-small-servers ó no service udp-small-servers Deshabilita los servicios pequeños tales como echo, discard y chargen.

(config)# no ip bootp server Deshabilita BOOTP (Bootstrap Protocol), protocolo para la obtención de direccionamiento IP de forma automática en las interfaces de red. Es el antecesor del DHCP.

(config)# no service finger Finger: use el comando

(config)# no ip http server Deshabilita el servidor HTTP.

(config)# no snmp-server Deshabilita el servidor SNMP (Simple Network Management Protocol).

(config)# no cdp run Deshabilita CDP (Cisco Discovery Protocol).

(config)# no service config Configuración remota.

(config)# no ip source-route Enrutamiento de origen.

(config)# no ip classless Deshabilita el enrutamiento sin clase, no permitiendo rutas "de último recurso".

(config)# no ip directed-broadcast Prevención de ataque de DOS denominado SMURF, que consiste en enviar un ping a cientos de máquinas con la dirección de destino del objetivo a atacar para que estas respondan.

(config)# no ip proxy-arp Enrutamiento ad hoc.

(config-if)# shutdown Deshabilita las interfaces no utilizadas.

(config-if)# no ip redirects

(config-if)# no ip proxy-arp

(config-if)# no ip unreachables

(config-if)# no ip directed-broadcast

(config-if)# no ip mask-reply

(config-if)# no mop enabled

3. Routing

3.1. Introducción

Ruta

(config)# [no]ip route <ip><máscara><ip salida | interfaz salida>

(config)# [no]ip route <ip><máscara><interfaz salida><ip salida>

(config)# [no]ip route <ip><máscara><interfaz salida>null0 Establece una ruta "nula" cuyo objetivo es el de filtrar tráfico a un rango IP.

Ruta por defecto

Estático

(config)# [no]ip route 0.0.0.0 0.0.0.0 <interfaz | ip> Establece la ruta de último recurso a la que se destinará el tráfico.

(config)# ip default-network <interfaz | ip> Establece la ruta candidata por defecto a la que destinará el tráfico, que puede condicionar o no la de último recurso.

Dinámico

(config-router)# [no]redistribute static Propaga la ruta por defecto en las actualizaciones del protocolo de enrutamiento dinámico utilizado.

(config-router)# default-information originate Propaga la ruta por defecto en las actualizaciones del protocolo de enrutamiento dinámico utilizado. (Cuidado: ni en el laboratorio ni en PacketTracer ha funcionado)

Sin Enrutamiento

(config)# ip default-gateway <ip> Establece la ruta a la que se destinará todo el tráfico, cuando el enrutamiento se encuentra desactivado (no ip routing).

Otros

(config)# [no]ip routing Activa/Desactiva el enrutamiento de paquetes en el router.

(config)# [no]ip classless Activa/Desactiva la utilización o no de clases para el comportamiento del enrutamiento.

(config)# [no]debug ip routing Activa/Desactiva el modo de depuración.

(config-router)# [no]auto-summary Activa/Desactiva la Sumarización de rutas del Protocolo dinámico de enrutamiento.

(config-router)# [no]passive-interface <interfaz | default> Activa/Desactiva la actualizaciones del protocolo dinámico de enrutamiento a una interfaz concreta o a todas.

3.2. Dinámico

3.2.1. RIP (Routing Information Protocol)

(config)# router rip Activa/Desactiva RIPv1 y entra su modo de configuración.

(config-router)# [no]debug ip rip Activa/Desactiva la depuración.

(config-router)# [no]network <ip> Publica una de sus redes (con clase) en las actualizaciones.

Versión 1

(config-router)# no version Envío de RIPv1 + Recepción RIPv1 & RIPv2.

(config-router)# version 1 Envío y recepción de RIPv1.

Versión 2

(config-router)# version 2 Envío y recepción de RIPv2.

Seguridad No funciona en Packet Tracer 5.3.2.

(config)# key chain <nombre clave = RIP_KEY> Gestión de "cadena de claves".

(config-keychain) key 1 Establece el número de contraseña.

(config-keychain) key-string <contraseña> Establece la contraseña.

(config)# interface <interfaz serial>

(config-if)# ip rip authentication mode md5 Establece el modo de autenticación a MD5.

(config-if)# ip rip authentication key-chain <nombre clave> Establece la contraseña anteriormente definida.

RIPng (RIP Next Generation) Nota: el enrutamiento de IPv6 tiene que ser habilitado antes de configurar RIPng.

(config)# ipv6 router rip <nombre> Crea e ingresa al modo de configuración de router RIPng.

(config-rtr)# exit Salir del modo de configuración.

(config-if)# ipv6 rip <nombre><enable | disable> A diferencia del comando "network" que se hace de manera grlobal, aquí se configura la interfaz para utilizar RIPng. Parámetro "nombre" debe coincidir con el del comando anterior.

3.2.2. EIGRP (Enhanced Interior Gateway Routing Protocol)

(config)# [no]router eigrp <instancia> Activa/Desactiva EIGRP y entra en su modo de configuración de la instancia. Debe ser identico para Router's que se comuniquen entre si.

(config)# debug eigrp fsm Activa/Desactiva la depuración (fsm=Final State Machine).

Información

 # show ip eigrp neighbor Vecinos adyacente que utilizan el protocolo.

 # show ip eigrp topology [all-links] Muestra [todos los enlaces] la tabla de topología.

Rutas

(config-router)# [no]network <ip red>[máscara wildcard] Publica la red [o subred] especificada en las actualizaciones.

(config-if)# ip summary-address eigrp <instancia><ip><máscara> Configura EIGRP para que propague en sus actualizaciones una superred.

Configuración - Métrica

(config-router)# metric weights <tos><k1><k2><k3><k4><k5> Modifica el peso del calcula de la métrica.

(config-if)# [no]bandwidth <kbps> Modifica/Restablece la métrica del ancho de banda.

Otros

(config-if)# [no]ip bandwidth-percent eigrp <instancia><porcentaje> Configura/Restablece el ancho de banda utilizado por el protocolo (en %).

(config-if)# [no]ip hello-interval eigrp <instancia><segundos> Configura/Restablece el intervalo de tiempo para el saludo (normalmente de 5 o 60 seg, según tipo de conexión).

(config-if)# [no]ip hold-time eigrp <instancia><segundos> Configura/Restablece el intervalo de tiempo máximo que espera para que el enlace responda al saludo antes de borrarlo. Debe ser menor o igual al del saludo.

Seguridad

(config)# key chain <nombre cad. clave = EIGRP_KEY> Crea una cadena de claves.

(config-keychain)# key <1> Primera clave.

(config-keychain-key)# key-string <contraseña> Contraseña de la clave.

(config)# interface <interfaz serial> Activa la verificación mediante MD5.

(config-if)# ip authentication mode eigrp <1><md5>

(config-if)# ip authentication key-chain eigrp <1><nombre cad. clave = EIGRP_KEY>

3.2.3. OSPF (Open Shortest Path First)

(config)# router ospf <id proceso> Activa/Descativa OSPF y entra en su modo de configuración del identificador de proceso local (puede ser distinto para routers que se comunican entre si).

Información

 # debug ip ospf adj Activa/Desactiva la depuración.

(config)# show ip ospf [interfaz] Muestra información del [las interfaces del] protocolo OSPF.

(config)# show ip ospf neighbor Muestra los vecinos adyacente que utilizan el protocolo.

Rutas

(config-router)# [no]network <ip red><máscara wildcard>area <area-id> Añade las redes (subredes) de las interfaces en las actualizaciones y las habilita a intervenir (enviar y recibir paquetes) en el protocolo para una área determinada.

(config-router)# router-id <dirección ip> Selecciona de forma manual (no automática) el identificador del protocolo, no teniendo que ser una la dirección de una interfaz existente (puede ser inventada).

Configuración

 # clear ip ospf process Reinicia el prceso de OSPF, consiguiendo renovar el identificador del Router.

(config-if)# [no]bandwidth <kbps> Modifica/Restablece la métrica del ancho de banda de la interfaz, utilizado para el protocolo de enrutamiento.

(config-if)# [no]ip ospf cost <costo> Modifica/Restablece el costo de la interfaz, utilizada para el protocolo de enrutamiento.
Costo = 10^8/bandwidth.
Ideal cuando se utilizan router no CISCO que no utilizan el ancho de banda para el cálculo de la métrica.

(config-if)# ip ospf priority <prioridad> Establece la prioridad para la asignación de DR (Router Designado) y BDR (Router Designado de Respaldo). 0 para que no sea elegible.

(config-router)# auto-cost reference-bandwidth <Mbps> Modifica/Establece el ancho de banda base, utilizado para el protocolo de enrutamiento (por defecto 100).
Costo = bandwidth base/bandwidth.
Es necesaria su configuración en todos los routers.

Configuración - Saludo

(config-if)# [no]ip ospf hello-interval <segundos> Modifica/Restablece el intervalo de tiempo entre saludos y el de enlace muerto a cuatro veces este. Por defecto 10 seg en enlaces multiacceso y Punto a Punto, 30 seg en multiacceso sin broadcast.

(config-if)# [no]ip ospf dead-interval <segundos> Modifica/Restablece el intervalo de tiempo para dar como muerto un enlace. Por defecto 4 veces el tiempo de saludo. Es necesaria su configuración en todos los routers, ya que si no puede que se pierda y recupere la adyacencia constantemente.

Seguridad - Autenticación en Claro)

(config)# inteface <interfaz serial>

(config-if)# ip ospf authentication-key <contraseña> Activa y establece la autenticación en claro.

(config)# router ospf <id proceso> Entra a configurar OSPF.

(config-route)# area <area>authentication Actica la autenticación de texto en claro.

Seguridad - Autenticación en MD5

(config)# inteface <interfaz serial>

(config-if)# ip ospf authentication message-digest Activa la autenticación MD5.

(config-if)# ip ospf message-digest-key 1 md5 <contraseña> Establece el tipo y la contraseña de la autenticación.

(config)# router ospf <id proceso> Entra a configurar OSPF.

(config-route)# area <area>authentication message-digest Activa la autenticación solo de MD5.

3.3. VLAN (Virtual LAN)

Nota: Para que las subinterfaces estén levantadas hay que levantar la interfaz principal.

(config)# interface fX/X.X Accede a la subinterfaz virtual concreta.

(config-subif)# encapsulation dot1q <vlan>[native] Configura la subinterfaz para que funcione en una VLAN específica, pudiendo declarar esta como nativa para interpretar correctamente el tráfico no etiquetado.

(config-subif)# ip address <ip><máscara> Asigna la dirección IP de la subinterfaz.

3.4. WAN (World Area Network)

 # show controllers Muestra entre otras cosas el tipo de cable conectado.

3.4.1. HDLC (High-Level Data Link Control)

(config-if)# encapsulation hdlc Establece la encapsulación.

3.4.2. PPP (Point to Point Protocol)

Depuración

 # debug ppp <packet | negotiation | error | authentication | compression | cbcp> Depuración de PPP.
packet: paquetes enviados y recibidos.
negotiation: paquetes enviados para la negociación inicial.
error: errores de los paquetes de los protocolos y los de la negociación inicial.
compression: paquetes erroneos con los números de secuencia cuando se utiliza compresión MPPC.
cbcp: paquetes erroneos de la negociación utilizando MSCB.

Básicos

(config-if)# encapsulation ppp Establece la encapsulación.

(config-if)# [no]ppp authentication <pap | pap chap | chap | chap pap> Establece/Elimina el método de autenticación.
pap: autenticación de contraseña, no seguro, se envía la contraseña en claro.
chap: autenticación de intercambio de señales, seguro, ya que codifica la contraseña mediante el reto y la recomprueba de forma periódica.

Autenticación PAP

(config)# username <usuario>password <contraseña> Autenticación del propio router.

(config-if)# ppp authentication <pap> Establece el método de autenticación.

(config-if)# ppp pap sent-username <usuario>password <contraseña> Configura la autenticación que utilizará para conectarse al otro enlace. Por lo tanto no es necesita configurar la contraseña secreta (enable secret).

Autenticación CHAP

(config)# username <usuario>password <contraseña> Establece la autenticación para el router remoto pueda conectarse

(config)# enable secret <contraseña> Contraseña que junto con su nombre de host (hostname) utilizará para autenticarse en el router remoto.

(config-if)# ppp authentication <chap> Establece el método de autenticación.

Opcionales

(config-if)# [no]compress <predictor | stac> Método de compresión utilizado.

(config-if)# ppp quality <1-100> Especifica el umbral de calidad del enlace.

(config-if)# ppp callback [accept | request] Configura la devolución de la llamada.

3.4.3. Frame Relay

Información

 # show frame-relay map Muestra la tabla de asignaciones de DLCI (Data Link Connection Identifier).

 # show frame-relay lmi Muestra el estado del control del enlace mediante la extesión del protocolo Frame Relay LMI (Local Management Interface).

 # show frame-relay pvc [pvc] Muestra el estado del enlace PVC (Permanent Virtual Circuit).

 # clear counters Borra los contadores de la estadísticas, entre ellos las del PVC (Permanent Virtual Circuit).

 # clear frame-relay inarp Borra la dirección del router remoto aprendida por ARP Inverso.

Depuración

 # debug frame-relay lmi Habilita/Deshabilita la depuración del control del enlace mediante la extensión LMI (Local Management Interface).

Configuración Básica & Dinámica Nota: las configuraciones en las subinterfaces pueden no tener efecto, por lo que se requiere guardar la configuración y reiniciar el router.

(config)# interface <interfaz> Accede a la configuración de la interfaz que hará de DTE.

(config-if)# no ip address Para que las subinterfaces funcionen, la interfaz física no puede tener una ip.

(config-if)# encapsulation frame-relay Establece la encapsulación del enlace serial a Frame Relay.

(config-if)# no shutdown Habilita la interfaz.

(config-if)# interface <interfaz>.<subinterfaz = DLCI><multipoint | point-to-point> Accede a la configuración de la subinterfaz que hará de DTE, permitiéndo tener varios PVC en un mismo enlace solucionando el problema del horizonte dividido de los protocolos de enrutamiento dinámico.

(config-subif)# ip address <ip><máscara> Establece la dirección IP su extremo del PVC (Permanent Virtual Circuit).

(config-subif)# frame-relay interface-dlci <dlci>

(config-subif)# bandwidth Modifica/Restablece la métrica del ancho de banda utilizada en los protocolos de enrutamiento dinámico como OSPF o IGRP.

Configuración Estática

(config-if)# no frame-relay inverse-arp Desactiva el ARP Inverso para configurar la dirección remota de forma estática.

(config-if)# frame-relay map ip <ip><dlci>[broadcast][cisco | ietf] Asigna de forma estática la dirección del enlace remoto. El parámetro broadcast permite la simulación de broadcast, y cisco o ietf especifica el tipo de encapsulación de Frame Relay, para utilizar dispositivos CISCO o de otras compañias.

Opcionales

(config-if) frame-relay lmi-type [cisco | ansi | q933a] Configura el tipo de extensión de LMI (Local Management Interface) de Frame Relay.

(config-if) keepalive Establece la temporización de los mensajes LMI. Por defecto 10 segundos.

Router como Switch Frame Relay

 # show frame-relay route Muestra las rutas Frame Relay existentes.

(config)# frame-relay switching Activa la conmutación Frame Relay en el Router.

(config)# interface <interfaz serial 1>

(config-if)# encapsulation frame-relay Establece la encapsulación del enlace serial a Frame Relay.

(config-if)# clock rate <bps> Velocidad en bps del enlace.

(config-if)# frame-relay intf-type dce Activa la interfaz como DCE.

(config-if)# frame-relay route <dlci origen>interface <interfaz destino><dlci destino> Crea una ruta de un DLCI entrante a una interfaz de salida con otro DLCI.

(config)# interface <interfaz serial 2>

(config-if)# encapsulation frame-relay Establece la encapsulación del enlace serial a Frame Relay.

(config-if)# clock rate <bps> Velocidad en bps del enlace.

(config-if)# frame-relay intf-type dce Activa la interfaz como DCE.

(config-if)# frame-relay route <dlci origen>interface <interfaz destino><dlci destino> Crea una ruta de un DLCI entrante a una interfaz de salida con otro DLCI.

3.5. ACL (Access Control List)

Información

 # show access-list [access-list-number | name] Muestra la Lista de Control de Acceso (ACL).

 # show running-config | include <texto=access-list> Utiliza la tubería para filtrar el running-config.

 # show running-config | begin <texto=access-list> Utiliza la tubería para filtrar desde el comienzo de el running-config.

Definición Identificadores ACL Estándar: 0-99 y 1300-1999. ACL Extendida: 100-199 y 2000-2699.
Notas: el parámetro LOG que muestra los eventos de bloque en consola, no funciona en Packet Tracer 5.3.2.

(config)# access-list <id>remark Establece un comentario.

(config)# access-list <id><permit | deny><ip origen | any>[wildcard origen]<ip destino | any>[wildcard des ACL Estándar.

(config)# access-list <id><permit | deny>host <ip> Permite/Deniega un host específico.

(config)# access-list <id><permit | deny><ip>255.255.255.255 Método alternativo al anterior del Host.

(config)# access-list <id><permit | deny>any Permite/Deniega todas las conexiones de origen.

(config)# access-list <id><permit | deny><ip cualquiera>0.0.0.0 Método alternativo al anterior.

(config)# access-list <id><permit | deny><ip | tcp | udp | icmp>

... <ip origen | any>[wildcard origen][eq | lt | gt <nº puerto | palabra clave>]

... <ip destino | any>[wildcard destino[eq | lt | gt <nº puerto | palabra clave>]

... [established] ACL Extendida.
established: evitar el tráfico desde fuera que no sea a consecuencia de una conexión TCP.

(config)# access-list <permit | deny>any Permite o deniega el resto de paquetes.

(config)# no access-list standard | extended><id | nombre> Elimina una ACL.

ACL Denominadas

(config)# ip access list [standard | extended]<name> Accede al modo de configuración de ACL Denominada para las estandar o extendidas.

(config-ext-nacl)# remark <comentario> Comentario de una ACL nombrada.

(config-ext-nacl)# <permit | deny><ACL Estándar o Extendida> ACL estándar o Extendida.

(config-ext-nacl)# <orden ACL><permit | deny><ACL Estándar o Extendida> Igual que la enterior pero estableciendo un order concreto para poder insertarlas entre otras ACL. Nota: no funciona en Packet Tracer 5.3.2.

Aplicación

(config-if)# ip access-group <id | nombre><in | out> Aplica a la interfaz una ACL de entrada (in) o salida (out).

VTY Aplica una ACL Estándar sobre VTY, aunque se podría hacer mediante una ACL Extendida. Además, solo funcionan las numeradas y no las renombradas.

(config-line)# access-class <id | nombre><in> Aplica una ACL sobre la "linea". Nota: no confundir con "ip access-class" que tiene un significado distinto.

3.5.1. ACLs Complejas

Dinámicas Los usuarios que deseen atraversar el router son bloqueados hasta que utilizan Telnet para conectarse al router y son autenticados. No entran en el temario.

(config)# username <usuario>password <contraseña>

(config)# access-list permit any host <ip>eq <puerto> Permite al host con la IP acceder al Router.

(config)# access-list <id>dynamic textlist timeout <minutos>permit ip <ip><wildcard><ip><wildcard>

(config)# interface <interfaz> Accede a la configuración de la Interfaz.

(config-if)# ip access-group <id>in Aplica la ACL como de entrada.

(config)# line vty 0 4 Accede a la configuración de las lineas VTY.

(config-line)# login local Permite el login de los usuarios definidos localmente.

(config-line)# autocommand access-enable host timeout <minutos>

Reflesivas Permiten el tráfico saliente y limitan el tráfico entrante como respuesta a sesiones que se originan dentro del router. No entran en el temario.

(config)# ip access-list extended <nombre=OUTBOUNDFILTERS> Crea una ACL (extendida) para el tráfico proveniente del interior del Router (enlace Ethernet).

(config-ext-nacl)# permit tcp <ip><wildcard>any reflect <TCPTRAFFIC> Crea una regla para permitir conexiones TCP de la red interna y "reflejarla" a la regla denominada TCPTRAFFIC.

(config-ext-nacl)# permit icmp <ip><wildcard>any reflect <ICMPTRAFFIC> Crea una regla para permitir conexiones ICMP de la red interna y "reflejarla" a la regla denominada ICMPTRAFFIC.

(config)# ip access-list extended <nombre=INBOUNDFILTERS> Crea una ACL (extendida) para el tráfico proveniente del exterior del Router (enlace Serial).

(config-ext-nacl)# evaluate TCPTRAFFIC Evalua que el tráfico del exterior del router (enlace Serial) se a consecuencia de la Regla "TCPTRAFFIC".

(config-ext-nacl)# evaluate ICMPTRAFFIC Idem para la regla "ICMPTRAFFIC".

(config)# interface <interfaz> Aplica a la interfaz las ACL anteriormente definidas.

(config-if)# ip access-group <INBOUNDFILTERS>in Aplica la ALC en el buffer de entrada para permitir el tráfico hacia fuera del router, desde la interfaz Ethernet a la Serial (normalmente).

(config-if)# ip access-group <OUTBOUNDFILTERS>out Aplica la ALC en el buffer de salida para permitir solo tráfico hacia dentro del router procedente de una conexión anterior hacia fuera, desde la interfaz Serial a la Ethernet (normalmente).

Basadas en Tiempo Permiten el control de acceso según la hora del día y la semana. No entran en el temario.

(config)# time-range <nombre> Crea un Rango de Tiempo.

(config-time-range)# periodic <Monday | ... | Sunday>[Monday | ... | Sunday][hora inicio]to [hora fin] Establece el Rango de Tiempo.

(config)# access-list <id>permit tcp <ip><wildcard>any eq telnet time-range <nombre> Aplica el rango de tiempo a la ACL.

(config)# interface <interfaz>

(config-if)# ip access-group <id>out Asigna la regla a la interfaz.

Recuperación

En una conexión de consola, mientras arranca el Router, presionar la tecla de pausa durante los 60 primeros segundos hasta que inicie el modo "ROMmon". En Packet Tracer utilizar Ctrl + C en vez de Pause.

rommon>confreg 0x2142 Establece el registro de configuración del Router para que no cargue la configuración la próxima vez que se inicie.

rommon>reset Reinicia el Router.

Restablecer las contraseñas.

(config)# config-register 0x2102 Restablece el resgistro de configuración a su valor predeterminado.

 # copy running-config startup-config

4. Switching

 # interface range <tipo interfaz><puerto inicio>-<puerto fin> Accede a la configuración de un rango de puertos de una interfaz.

4.1. Puertos

4.1.1. Enlace

(config)# mdix auto Establece a automático la gestión del cable (directo o cruzado) a utilizar.

(config-if)# duplex auto Modo duplex automático.

(config-if)# speed auto Velocidad automática.

4.1.2. Direcciones MAC

 # show mac-address-table Muestra la tabla de direcciones MAC's.

 # clear mac-address-table dynamic Borra la tabla de direcciones MAC dinámicas.

 # [no]mac-address-table static <MAC>vlan <1-4096, ALL>interface <id de la interfaz> Establece una dirección MAC como estática.

4.1.3. Seguridad

Información

 # show port-security interface [interfaz] Muestra los parámetros de configuración de la interfaz especificada.

 # show port-security address Muestra todas las direcciones MAC seguras configuradas.

Configuración

(config-if)# switchport port-security Activa la seguridad del puerto.

(config-if)# switchport port-security mac-address <dirección MAC | sticky> Especifica la dirección MAC a la que permite conectarse a la interfaz de forma estática (con la dirección) o dinámica (sticky).

(config-if)# switchport port-security mac-address sticky [MAC] Las direcciones MAC's que aprende dinámicamente las considera seguras. También se le puede especificar cual se preguardan, como si se hubiera conectado un PC.

(config-if)# switchport port-security maximum <número direcciones> Establece el número máximo de direcciones seguras.

(config-if)# switchport port-security violation <protect | restrict | shutdown> Configura el modo de actuación frente a una violación de seguridad, es decir, que se sobrepase el número máximo de direcciones.
protect: bloquea el tráfico.
restrict: bloquea el tráfico y aumenta el contador de violación.
shutdown: desactiva la interfaz.

Snooping DHCP Nota: no está disponible en Packet Tracer.

(config-if)# ip dhcp snooping Habilita el Snooping de DHCP.

(config-if)# ip dhcp snooping vlan number [vlan] Habilitar el snooping de DHCP para una VLAN específica.

(config-if)# ip dhcp snooping trust Define los puertos como confiables o no confiables.

(config-if)# ip dhcp snooping limit rate <velocidad> (Opcional) Limitar la tasa a la que un atacante puede enviar solicitudes de DHCP bogus de manera continua a través de puertos no confiables al servidor de DHCP.

4.2. VLAN (Virtual LAN)

Información

 # show vlan [brief | id <id vlan>| name <nombre vlan>summary] Muestra información de las VLANs.

 # show interface switchport Muestra información de los modos de conexión de todas las interfaces.

 # show interfaces <id interfaz | vlan <id vlan>>switchport Muestra información del modo de enlace de una interfaz.

 # show interface trunk Muestra información de las interfaces Troncales.

Conexión

(config)# ip default-gateway <ip> Configura el gateway predeterminado.

Creación

(config)# vlan <vlan> Crea la VLAN.

(config-vlan)# name <nombre> Asigna un nombre a la VLAN.

(config)# interface vlan <vlan> Ingresa en el modo configuración para la vlan determinada.

(config-if)# ip address <ip><máscara> Configura la dirección ip de la interfaz.

(config-if)# no shutdown Habilita la interfaz.

4.2.1. DTP (Dynamic Trunking Protocol)

Acceso

(config-if)# switchport mode access Define el enlace como de Acceso.

(config-if)# switchport access vlan <vlan> Asigna el puerto a una VLAN (¡y solo una!).

Troncal

(config-if)# switchport mode trunk Define el enlace como Troncal.

(config-if)# switchport trunk allowed vlan <vlan | add <vlan>| all | etc> Define mediante varias maneras las VLAN permitidas en el enlace Troncal.

(config-if)# switchport trunk native vlan <vlan> Determina la VLAN Nativa.

Negociación

(config-if)# switchport mode dynamic <auto | desirable> Enlace como Dinámico automático o deseado.
auto: modo automático, que si no hay intención clara por ninguna de las dos partes se configura en modo de Acceso.
desirable: modo automático deseado, que si no hay intención por ninguna de las dos partes se configura en modo Troncal.

(config-if)# switchport nonegotiate Desactiva el DTP.

4.2.2. VTP (VLAN Trunk Protocol)

Información

(config)# show vtp status Muestra el estado del protocolo VTP.

(config)# vtp pruning Habilita la depuración, que permite aun servidor VTP suprimir tráfico de broadcast IP para VLAN específicas aswitches que no tienen ningún puerto en esa VLAN.
Nota: no es soportado en Packet Tracer.

Configuración

(config)# vtp mode <client | server | trasparent> Selecciona el Modo, que por defecto es el Servidor.

(config)# vtp domain <nombre dominio> Configura el nombre de Dominio.

(config)# vtp password <contraseña> Configura la contraseña, que debe ser igual en el dominio.

(config)# vtp version <1, 2 o 3> Establece la versión de VTP, que deben ser iguales en el dominio.

4.2.3. STP (Spanning Tree Protocol)

Costos de las Interfaces según su velocidad: 10Gb/s = 2, 1Gbs = 4, 100Mb/s = 19, 10Mb/s = 100 Protocolo propietario de CISCO.

Información

 # show spanning-tree [detail | active | summary] Muestra información, en detalle, para las interfaces activas o resumida, del protocolo STP.

 # show spanning-tree vlan <vlan> Muestra información del protocolo STP de una VLAN determinada

 # debug spanning-tree events Activa el modo de depuración.
Nota: este comando no es soportado por Packet Tracer.

Configuración

(config)# spanning-tree vlan <vlan>priority <0-65536> Establece de forma manual la prioridad del puente, en el intervalo 0-65536 en incrementos de 4096.

(config)# spanning-tree vlan <vlan>root <primary | secondary> Establece de forma automática la prioridad del puente, en modo primario para que el enlace sea troncal o en secundario para que no lo sea. El primario establece un peso de 24576 y el secundario de 28672.

(config-if)# spanning-tree cost <1-200.000.000> Establece el costo de la interfaz, utilizado para determinar el puerto raíz mediante la ruta más corta.

(config-if)# spanning-tree port-priority <0-240> Establece la prioridad de la interfaz, utilizado para determinar el puerto raíz si las rutas de todos los puertos tienen igual costo. El valor está comprendido entre 0-240 en intervalos de 16.

(config-if)# [no]spanning-tree portfast Permite acelerar la conexión de dispositivos de la capa de acceso, evitando las etapas de esperar del protocolo STP. Tecnología propietaria de CISCO.

Configuración Avanzada

(config)# spanning-tree vlan <vlan>root primary diameter <valor> Configura el diámetro el diámetro de la red STP, por defecto 7. Únicamente debe configurarse en el Puente Raíz y modifica a su vez los valores internos de retardo de envío y antigüedad máxima.

Configuración PVST+ Fast

 # clear spanning-tree detected-protocols Borra todos los STP detectados.

(config)# spanning-tree mode rapid-pvst Configura STP con el protocolo PVST+ Rapid.

(config-if)# spanning-tre link-type point-to-point Especifica que el tipo de enlace para este puerto es punto a punto.

4.2.4. VoIP

(config-if)# mls qos trust cos Establece que el tráfico de voz sea prioritario. Nota: es necesario configurar toda la red y no solo el puerto concreto.

(config-if)# switchport voice vlan <vlan> Establece la VLAN de voz, por defecto la 150.

(config-if)# switchport mode access Establece que esté en modo acceso, es decir, solo empleará una VLAN.

(config-if)# switchport access vlan <vlan> Establece la VLAN de Voz.

4.3. Recuperación

Catalyst 2960 Apagar y volver a encender presionando el botón hasta que la luz de este se vuelva de color fijo, entonces aplicar los siguientes comandos.

switch:flash_init

switch:load_helper

switch:dir flash:

rename flash:config.text flash:config.old Renombra el fichero de configuración para que no sea cargado en el arranque.

boot Arranca IOS.

rename flash:config.old flash:config.text Deshace el renombrado del fichero de configuración para que la siguiente vez sea cargado correctamente.

copy flash:config.text system:running-config Carga la configuración inicial, pero encontrándonos en el modo Privilegiado para cambiar las contraseñas.