Guía de Referencia Profesional para la Configuración de Redes Cisco con Packet Tracer

1. Fundamentos de Cisco Packet Tracer y la CLI

1.1. ¿Qué es Cisco Packet Tracer?

Cisco Packet Tracer es una herramienta de simulación visual y multiplataforma que permite a los usuarios diseñar y simular topologías de red en un entorno virtual.1 Es un "laboratorio virtual" ideal para la enseñanza y el aprendizaje, especialmente para la preparación de certificaciones como CCNA y CCNP, ya que elimina la necesidad de hardware físico costoso.4 La herramienta permite visualizar cómo se transmite la información, practicar habilidades de cableado e integrar dispositivos IoT.4

A pesar de sus beneficios, es importante reconocer que Packet Tracer es una simulación y no un sustituto completo del hardware real. El conjunto de comandos es limitado y se centra en los conceptos fundamentales del currículo de certificación, no en la complejidad de los dispositivos de producción.2

1.2. Navegación en la Interfaz de Línea de Comandos (CLI)

La configuración de dispositivos Cisco se realiza a través de la CLI, que opera bajo una jerarquía de modos de acceso y configuración. Comprender esta estructura es fundamental, ya que cada comando solo es funcional en el modo correcto.8

- **Modo EXEC de Usuario:** Es el primer nivel de acceso (`Router>`). Permite tareas básicas de visualización, pero no cambios de configuración.9
- **Modo EXEC Privilegiado:** Es el nivel de gestión (`Router#`). Se accede con el comando `enable` .8 Permite ver la configuración completa y acceder a otros modos. Es un modo sensible que debe estar protegido con contraseña.9
- **Modo de Configuración Global:** Es el nivel principal (`Router(config)#`). Se accede desde el modo privilegiado con `configure terminal` o `conf t` .8 Los cambios aquí afectan al dispositivo en su totalidad.
- **Modos de Configuración Específicos:** A partir del modo global, se accede a modos para configurar componentes específicos, como interfaces (`Router(config-if)#`) o líneas de consola (`Router(config-line)#`).8

2. Guía de Comandos y Sintaxis

Esta sección presenta una referencia rápida y organizada de los comandos de configuración más comunes, ideal para la práctica en el laboratorio.

2.1. Comandos de Navegación y Gestión de Modos

- `enable` (`en`) - Permite el acceso al modo EXEC privilegiado.8
- `configure terminal` o `conf t` - Permite el acceso al modo de configuración global.8
- `exit` - Permite salir del modo de configuración actual y volver al modo anterior.9
- `end` - Permite volver directamente al modo EXEC privilegiado desde cualquier sub-modo de configuración.7
- `disable` - Permite salir del modo EXEC privilegiado y volver al modo de usuario.9
- `no <comando>` - Permite eliminar o negar un comando.10
- `copy running-config startup-config` o `copy r s` - Permite guardar la configuración actual (en la RAM) en la configuración de inicio (en la NVRAM) para que persista después de un reinicio.9
- `write` o `wr` - Es un comando para guardar la configuración, equivalente a `copy running-config startup-config`.9
- `reload` - Reinicia el dispositivo.10

2.2. Comandos de Configuración Global del Router

- `hostname <nombre>` - Cambia el nombre del dispositivo.8
- `enable secret <contraseña>` - Establece una contraseña encriptada para el acceso al modo EXEC privilegiado (método recomendado).8
- `enable password <contraseña>` - Establece una contraseña no encriptada para el acceso al modo EXEC privilegiado.10
- `service password-encryption` - Encripta todas las contraseñas de texto no cifrado.10
- `banner motd #<mensaje>#` - Configura un mensaje de bienvenida que se muestra al iniciar la sesión de consola.10
- `line console 0` - Entra en el modo de configuración de la consola.9
- `password <contraseña>` - Establece una contraseña para la línea de consola o Telnet.10
- `login` - Habilita la solicitud de contraseña en la línea de consola o Telnet.9
- `line vty <primera entrada> <última entrada>` - Entra en el modo de configuración para las líneas de acceso remoto (Telnet).9
- `ip route <red_destino> <máscara> <siguiente_salto>` - Crea una ruta estática para una red remota.10

2.3. Comandos de Configuración de Interfaces

- `interface <tipo/número>` - Selecciona una interfaz específica para configurarla.8

- `ip address <dirección_IP> <máscara_de_subred>` - Asigna una dirección IP y una máscara de subred a la interfaz.9
- `no shutdown` - Activa una interfaz y la pone en estado "up".9
- `shutdown` - Desactiva una interfaz.10
- `clock rate <frecuencia>` - Configura la tasa de sincronización en interfaces seriales que actúan como DCE (Equipo Terminal de Datos).10

2.4. Comandos de Configuración del Switch

- `vlan <id>` - Crea una VLAN.16
- `name <nombre>` - Asigna un nombre a la VLAN.16
- `interface Vlan<id>` - Entra en la interfaz lógica de la VLAN.8
- `ip default-gateway <dirección_IP>` - Configura la puerta de enlace predeterminada para el switch.3
- `interface range <tipo/número> - <número>` - Selecciona un rango de interfaces para su configuración.16
- `switchport mode access` - Configura un puerto del switch en modo de acceso.16
- `switchport access vlan <id>` - Asigna un puerto de acceso a una VLAN específica.16
- `switchport trunk encapsulation dot1q` - Configura el protocolo de encapsulación (IEEE 802.1Q) en un enlace troncal.16
- `switchport mode trunk` - Configura un puerto como enlace troncal para transportar tráfico de múltiples VLANs.16
- `switchport trunk allowed vlan <lista_de_vlan>` - Limita el tráfico del enlace troncal a las VLANs especificadas.16

2.5. Comandos de Verificación y Diagnóstico

- `show running-config` - Muestra la configuración actual del dispositivo en la memoria RAM.9
- `show startup-config` - Muestra la configuración guardada en la memoria no volátil (NVRAM).10
- `show ip route` - Muestra la tabla de enrutamiento del router.10
- `show ip interface brief` - Muestra un resumen conciso del estado de las interfaces.7
- `show int vlan 1` - Muestra el estado y la dirección IP de la interfaz VLAN 1 en un switch.3
- `ping <dirección_IP>` - Envía paquetes de eco para probar la conectividad de extremo a extremo.15
- `traceroute <dirección_IP>` - Traza la ruta que sigue un paquete para llegar a su destino, mostrando cada "salto" o router intermedio.17

3. Planificación y Configuración Práctica

Antes de la configuración en la CLI, la planificación es el paso más importante. El diseño de subredes permite dividir una red grande en segmentos eficientes.18 Un plan de direccionamiento detallado actúa como un mapa, especificando la dirección IP, máscara de subred y gateway para cada dispositivo, minimizando así los errores.18

Dispositivo / Subred	Interfaz	Dirección IP	Máscara de Subred	Gateway Predeterminado
Subred A (LAN)	R1 - Fa0/0	192.168.10.1	255.255.255.0	N/A
	PC1	192.168.10.10	255.255.255.0	192.168.10.1
Subred B (LAN)	R1 - Fa0/1	192.168.20.1	255.255.255.0	N/A
	PC2	192.168.20.10	255.255.255.0	192.168.20.1
Subred C (WAN)	R1 - S0/0/0	10.0.0.1	255.255.255.252	N/A
	R2 - S0/0/0	10.0.0.2	255.255.255.252	N/A

3.1. Pasos de Configuración del Router

1. **Conexión Inicial:** Utiliza un cable de consola (`RS-232` a `Console`) para acceder a la CLI a través de la aplicación "Terminal" en una PC.6
2. **Configuración Inicial:** Asigna un nombre al dispositivo con `hostname` y establece contraseñas con `enable secret` y `service password-encryption` .9
3. **Configuración de Interfaces:** Entra al modo de interfaz con `interface <tipo/número>` y asigna la dirección IP y la máscara de subred con `ip address` .9

   Crucial: Activa la interfaz con `no shutdown` .9

3.2. Verificación y Solución de Problemas

La verificación es una parte integral de cualquier proceso de configuración. Es esencial para asegurar que los cambios se hayan aplicado correctamente y para solucionar problemas.10

- `show ip route` : Utiliza este comando para verificar la tabla de enrutamiento y asegurarte de que el router conoce las redes remotas, especialmente después de configurar rutas estáticas.10

- `ping <dirección_IP>`: Se utiliza para verificar la conectividad de extremo a extremo.15 Para la solución de problemas, prueba la conectividad de forma incremental, comenzando por la puerta de enlace predeterminada.14
- `traceroute <dirección_IP>`: Este comando traza la ruta que toma un paquete hasta su destino, mostrando cada "salto" o router intermedio. Es invaluable para identificar exactamente en qué punto de la red se interrumpe la conectividad.17

Guía Completa de Cisco Packet Tracer: Arquitecturas y Configuraciones para Redes Residenciales y Empresariales

I. Introducción: El Entorno de Laboratorio Virtual

El diseño y la configuración de redes informáticas son disciplinas que requieren una comprensión profunda de los principios fundamentales y una práctica rigurosa. Cisco Packet Tracer se ha consolidado como una herramienta de simulación indispensable que ofrece un entorno virtual robusto para la práctica de habilidades en redes, Internet de las Cosas (IoT) y ciberseguridad.1 Este software va más allá de la simple emulación; proporciona una experiencia de aprendizaje activa y contextualizada que permite a los usuarios visualizar el flujo de datos y manipular equipos virtuales como si fueran reales, desde la organización de un rack de dispositivos hasta el tendido de cables en modo físico.1 Es un entorno de “sandbox” ideal tanto para principiantes que buscan entender los conceptos básicos como para profesionales que desean perfeccionar habilidades complejas de resolución de problemas.

El mero acto de conectar dispositivos no constituye una red funcional y resiliente. Un diseño de red bien planificado es la base para un sistema que puede crecer, adaptarse y funcionar de manera confiable con el tiempo. La planificación es fundamental para crear redes que cumplan con requisitos técnicos y objetivos empresariales, garantizando que el sistema sea escalable para soportar nuevos usuarios y aplicaciones, tenga alta disponibilidad para minimizar fallos, sea seguro para proteger datos sensibles y sea manejable para facilitar la administración.3 Este informe, estructurado en una progresión lógica, aborda estos principios, comenzando con las arquitecturas de red fundamentales, para luego aplicar estas teorías en la creación de escenarios prácticos, desde una red residencial simple hasta una red empresarial multicapa.

II. Paradigmas de Diseño de Red: El Plan para el Éxito

2.1. La Arquitectura SOHO (Small Office/Home Office)

La arquitectura de red de oficina pequeña/oficina en casa (SOHO) representa el modelo más sencillo y asequible de red. Su objetivo principal es proporcionar conectividad a Internet y servicios de red básicos para un número limitado de usuarios. Un diseño SOHO típicamente se

basa en un único dispositivo todo en uno, como un `Home Router`, que integra las funcionalidades de enrutador para la conexión a Internet, un conmutador (switch) para la conectividad por cable y un punto de acceso inalámbrico para la comunicación Wi-Fi.4 Este modelo es inherentemente simple y fácil de gestionar, lo que lo hace ideal para entornos donde la rentabilidad y la facilidad de uso son prioritarias sobre la complejidad y la escalabilidad.4

2.2. El Modelo Jerárquico Empresarial

Para organizaciones de mayor envergadura, el modelo SOHO resulta insuficiente. A medida que una red crece, un diseño "plano" (sin capas) se vuelve difícil de gestionar, solucionar problemas y escalar.3 Por ello, las grandes empresas adoptan un modelo jerárquico de tres capas: la capa de Acceso, la capa de Distribución y la capa de Núcleo (Core).4 La elección de esta arquitectura es una consecuencia directa del tamaño de la empresa, sus requisitos y sus proyecciones de crecimiento. Un diseño por capas asegura que el tráfico local permanezca local, que la red pueda crecer de manera organizada y que la complejidad se gestione por módulos, facilitando las tareas de diseño, implementación y mantenimiento.3

- **Capa de Acceso:** Esta es la capa más cercana a los usuarios finales, donde dispositivos como PCs, impresoras y teléfonos IP se conectan a la red. Los conmutadores de esta capa (switches) son responsables de proporcionar acceso a la red y de aplicar políticas de seguridad de Capa 2, como la seguridad de puertos para evitar conexiones no autorizadas.3
- **Capa de Distribución:** Actuando como un puente entre la capa de Acceso y la capa de Núcleo, esta capa de agregación interconecta los conmutadores de acceso de los diferentes departamentos. Es aquí donde se aplican políticas de enrutamiento, listas de control de acceso (ACLs) y se configura la redundancia para evitar puntos únicos de fallo. En esta capa se suelen utilizar conmutadores multicapa (multilayer switches) para realizar enrutamiento inter-VLAN.3
- **Capa de Núcleo (Core):** Conocida como la "columna vertebral" de la red, la capa de Núcleo se encarga del enrutamiento de alta velocidad y el transporte de paquetes entre las capas de Distribución. Para asegurar el máximo rendimiento, esta capa debe estar libre de políticas de filtrado o de seguridad complejas. Al igual que en la capa de Distribución, la redundancia es crucial para la estabilidad de la red.3

III. Escenario 1: Laboratorio de Red Residencial/SOHO

Este escenario se enfoca en la configuración de una red doméstica o de una pequeña oficina utilizando una topología simple con dispositivos básicos.

3.1. Topología y Selección de Dispositivos

La topología de este laboratorio consiste en una red estrella, donde todos los dispositivos finales se conectan a un punto central.

- **Dispositivos:** Se seleccionan los siguientes dispositivos para simular una red SOHO: un `Home Router`, un `PC` (escritorio), una `Laptop` y una `Printer`.5
- **Conexiones:** Se conecta el `PC` y la `Printer` al `Home Router` mediante cables `Copper Straight-Through`. Para la `Laptop`, se configura una conexión inalámbrica.

3.2. Guía de Configuración: Una Red Potenciada por DHCP

El uso del Protocolo de Configuración Dinámica de Host (DHCP) es una práctica estándar en redes SOHO para simplificar la gestión de direcciones IP. El DHCP permite que los dispositivos obtengan automáticamente su dirección IP, máscara de subred, puerta de enlace predeterminada y dirección de servidor DNS al conectarse a la red, eliminando la necesidad de configuración manual.7

- **Plan de Direccionamiento IP:** Para este laboratorio, se utilizará el espacio de direcciones privadas `192.168.0.0/24`.
- **Configuración del Home Router:**
  1. En Packet Tracer, se hace clic en el `Home Router` y se navega a la pestaña de configuración gráfica (GUI).
  2. Dentro de la configuración LAN, se establece la dirección IP del router como `192.168.0.1`.
  3. Se activa el servicio DHCP y se define el rango de direcciones IP disponibles (por ejemplo, desde `192.168.0.100` hasta `192.168.0.254`).
  4. Se configura la puerta de enlace predeterminada (`192.168.0.1`) y un servidor DNS público (como `8.8.8.8`).5
- **Configuración de Dispositivos Finales:**
  1. Para el `PC` y la `Laptop`, se accede a su configuración IP a través de la pestaña de escritorio.
  2. Se cambia la opción de configuración de `Static` a `DHCP`. Los dispositivos solicitarán automáticamente una dirección IP del servidor DHCP del `Home Router`.5

3.3. Verificación

Una vez que los dispositivos han obtenido sus direcciones IP, la conectividad se verifica con los siguientes pasos:

- **Verificación de IP:** Desde el `Command Prompt` del `PC` y la `Laptop`, se ejecuta el comando `ipconfig`. Esto confirmará que han recibido una dirección IP, máscara de subred, puerta de enlace y dirección DNS del pool de DHCP.5

- **Prueba de Conectividad:** Se utiliza el comando `ping` para probar la conectividad entre dispositivos (por ejemplo, `ping 192.168.0.101` desde el `PC` al `Laptop`) y con la puerta de enlace (`ping 192.168.0.1`).5

IV. Escenario 2: Laboratorio de Red de Campus Empresarial

Este escenario recrea una red empresarial a pequeña escala utilizando una arquitectura jerárquica para demostrar conceptos avanzados como VLANs, enrutamiento inter-VLAN, DHCP a gran escala y seguridad.

4.1. Diseño de Topología y Selección de Dispositivos

La topología se basa en el modelo jerárquico de tres capas:

- **Núcleo/Internet:** Un `Router PT-Router`.
- **Distribución:** Un `Multilayer Switch PT-MLS`.
- **Acceso:** Dos `Switch PT-2960`.
- **Dispositivos Finales:** `PCs`, `Laptops` y un `Server PT-Server` para servicios de DNS y web.3

4.2. Direccionamiento IP y Segmentación de Red con VLANs

La segmentación es un pilar de las redes empresariales. Las VLANs (Virtual LANs) permiten agrupar lógicamente dispositivos en redes separadas, sin importar su ubicación física, mejorando la seguridad, el rendimiento y la gestión.9 No obstante, la creación de VLANs aísla a los dispositivos en "islas de difusión" separadas. Para permitir la comunicación entre estas islas, es necesario un mecanismo de enrutamiento.10 Aquí reside la relación esencial entre VLANs y enrutamiento inter-VLAN: las VLANs segmentan la red para lograr un propósito (por ejemplo, organizar departamentos), mientras que el enrutamiento inter-VLAN proporciona la conectividad necesaria para que la red funcione como un todo cohesivo, superando el aislamiento inherente a la segmentación.

- **Creación de VLANs:** Se crean VLANs en los conmutadores de Acceso y Distribución con sus respectivos nombres y números (por ejemplo, `VLAN 10` para Ventas, `VLAN 20` para Recursos Humanos, `VLAN 30` para TI y `VLAN 99` para Gestión).6
- **Asignación de Puertos:** Los puertos de los conmutadores de Acceso se asignan a las VLANs correspondientes en modo `access`. Los enlaces entre los conmutadores de Acceso y el conmutador de Distribución se configuran en modo `trunk` para que puedan transportar el tráfico de múltiples VLANs simultáneamente.11

4.3. Enrutamiento Inter-VLAN: El Modelo "Router-on-a-Stick"

El modelo "Router-on-a-Stick" es una solución eficaz y económica para el enrutamiento inter-VLAN en redes pequeñas y medianas.10 Este método utiliza una única interfaz física en el enrutador de núcleo para enrutar el tráfico entre múltiples VLANs, al crear múltiples sub-interfaces lógicas, cada una asociada a una VLAN específica.10

- **Configuración:**
  1. Se conecta una única interfaz del `Core Router` al `Distribution Switch` (por ejemplo, `FastEthernet 0/0`).
  2. Se configura la interfaz física del enrutador sin dirección IP y se activa con el comando `no shutdown`.
  3. Para cada VLAN, se crea una sub-interfaz (por ejemplo, `interface FastEthernet0/0.10`).
  4. Dentro de cada sub-interfaz, se define el encapsulamiento (`encapsulation dot1Q <vlan-id>`) y se le asigna una dirección IP que servirá como puerta de enlace predeterminada para esa VLAN.10

4.4. Configuración de DHCP a Escala Empresarial

En un entorno profesional, la gestión manual de direcciones IP es inviable. El DHCP permite la asignación automática de direcciones, pero a diferencia de una red doméstica, es crucial reservar direcciones estáticas para dispositivos críticos como servidores y enrutadores para evitar conflictos y garantizar la estabilidad del servicio.8

- **IP Estática para Servidores:** Se asigna una dirección IP estática al `DNS/Web Server` para garantizar que su dirección no cambie, lo cual es fundamental para el acceso a servicios.15
- **Exclusión de Direcciones:** Se utiliza el comando `ip dhcp excluded-address` para excluir las direcciones de las puertas de enlace y de los servidores de los pools de DHCP, previniendo así conflictos de direcciones.8
- **Creación de Pools de DHCP:** Se crean pools de DHCP separados para cada VLAN (`ip dhcp pool VLAN10_SALES`, `ip dhcp pool VLAN20_HR`, etc.), especificando la red, la máscara de subred, la puerta de enlace predeterminada y el servidor DNS para cada departamento.8

4.5. Seguridad y Control de Acceso

La seguridad es un componente crítico en cualquier red empresarial.3

- **Listas de Control de Acceso (ACLs):** Las ACLs son utilizadas para filtrar el tráfico de red y aplicar políticas de seguridad. Se pueden configurar ACLs para restringir la comunicación entre departamentos, por ejemplo, impidiendo que el departamento de Ventas acceda a los recursos del departamento de TI.6

- **Seguridad de Puertos:** Se configura la seguridad de puertos en los conmutadores de Acceso para limitar el número de direcciones MAC permitidas en un puerto, lo cual impide la conexión de dispositivos no autorizados.6
- **Traducción de Direcciones de Red (NAT):** Para la conectividad a Internet, se implementa NAT con PAT (Traducción de Direcciones de Puerto) en el `Core Router`. Esto permite que múltiples dispositivos internos compartan una única dirección IP pública para la comunicación externa, conservando el limitado espacio de direcciones IP públicas.6

4.6. Enrutamiento hacia "Internet": Rutas Estáticas y Predeterminadas

Para que el tráfico de la red corporativa pueda llegar a destinos fuera de la red local, es necesario implementar un mecanismo de enrutamiento.18

- **Rutas Estáticas:** Las rutas estáticas son una forma de enrutamiento manual que funciona bien en redes pequeñas o en escenarios donde el control preciso de la ruta es necesario. Se configuran en el `Core Router` para dirigir el tráfico hacia una red simulada de "Internet".19
- **Ruta Predeterminada:** Para cualquier destino desconocido, se configura una ruta predeterminada, también conocida como la "puerta de enlace de último recurso". Este es un tipo de ruta estática que utiliza la dirección de red `0.0.0.0 0.0.0.0`, actuando como una "captura de tráfico" para todo lo que no tiene una ruta más específica y dirigiéndolo hacia la interfaz de salida a Internet.18

V. Análisis, Solución de Problemas y Mejores Prácticas

5.1. SOHO vs. Empresarial: Un Análisis Comparativo

La elección de una arquitectura de red depende fundamentalmente de los objetivos del negocio y de los requisitos técnicos, no de una preferencia arbitraria.3 Un análisis comparativo de las dos arquitecturas, tal como se implementaron en los laboratorios, ilustra claramente estas diferencias.

Característica	Red SOHO (Laboratorio 1)	Red Empresarial (Laboratorio 2)
Complejidad	Baja. Un solo dispositivo centralizado.	Alta. Múltiples capas y dispositivos con funciones especializadas.
Costo	Bajo. Se basa en un solo dispositivo integrado.	Alto. Requiere múltiples enrutadores, conmutadores multicapa y dispositivos de acceso.
Escalabilidad	Limitada. No se adapta a un aumento significativo de	Alta. El diseño modular permite añadir nuevas capas de acceso y

Característica	Red SOHO (Laboratorio 1)	Red Empresarial (Laboratorio 2)
	usuarios o servicios.	distribución fácilmente.
Seguridad	Básica. Firewall simple, seguridad inalámbrica.	Avanzada. Uso de ACLs, seguridad de puertos, NAT/PAT para control granular.
Disponibilidad	Vulnerable. Un punto único de fallo.	Alta. La redundancia en las capas de Distribución y Núcleo previene fallos.
Manejo	Simple. Configuración vía interfaz gráfica.	Complejo. Requiere personal especializado y conocimientos de CLI.

5.2. Solución de Problemas Comunes en Packet Tracer

La práctica en Packet Tracer incluye la resolución de problemas. Diagnosticar y corregir errores es una habilidad crucial.

- **Fallos de Ping:** Un ping fallido puede deberse a varias causas, como una interfaz del enrutador o conmutador que está administrativamente "caída". El comando `no shutdown` es esencial para activar las interfaces.22 Otros motivos incluyen máscaras de subred incorrectas o puertas de enlace predeterminadas mal configuradas, lo que impide que un dispositivo se comunique con redes externas.
- **Problemas de DHCP:** Si un dispositivo no recibe una dirección IP, el problema puede estar en el pool de DHCP del enrutador o conmutador, por ejemplo, un rango de direcciones mal definido o una exclusión incorrecta que impide la asignación.14 Es importante verificar que el pool de DHCP coincida con la subred de la red.
- **Problemas de Enrutamiento:** Cuando la comunicación falla entre redes diferentes, el problema suele estar en la tabla de enrutamiento. El comando `show ip route` permite verificar las rutas conocidas por el enrutador.18 Para trazar la ruta que toma un paquete, se utiliza el comando `traceroute`, lo que ayuda a identificar en qué punto de la ruta el tráfico se detiene.23

VI. Apéndices

Apéndice A: Plan Detallado de Direccionamiento IP

Laboratorio 1: Red SOHO

Dispositivo	Dirección IP	Máscara de Subred	Puerta de Enlace	Propósito
Home Router (LAN)	`192.168.0.1`	`255.255.255.0`	N/A	Puerta de enlace y DHCP

Dispositivo	Dirección IP	Máscara de Subred	Puerta de Enlace	Propósito
PC	DHCP (ej. `192.168.0.100`)	`255.255.255.0`	`192.168.0.1`	Dispositivo de usuario
Laptop	DHCP (ej. `192.168.0.101`)	`255.255.255.0`	`192.168.0.1`	Dispositivo de usuario
Printer	DHCP (ej. `192.168.0.102`)	`255.255.255.0`	`192.168.0.1`	Dispositivo de usuario

Laboratorio 2: Red Empresarial (Ejemplo de subredes)

Dispositivo	VLAN	Dirección IP	Máscara de Subred	Puerta de Enlace	Propósito
Core Router (sub-int)	10	`192.168.10.1`	`255.255.255.0`	N/A	Enrutamiento inter-VLAN
Core Router (sub-int)	20	`192.168.20.1`	`255.255.255.0`	N/A	Enrutamiento inter-VLAN
Core Router (sub-int)	30	`192.168.30.1`	`255.255.255.0`	N/A	Enrutamiento inter-VLAN
Servidor DNS/Web	30	`192.168.30.10`	`255.255.255.0`	`192.168.30.1`	Servidor estático
PCs de Ventas	10	DHCP	`255.255.255.0`	`192.168.10.1`	Dispositivos de usuario
PCs de RRHH	20	DHCP	`255.255.255.0`	`192.168.20.1`	Dispositivos de usuario
PCs de TI	30	DHCP	`255.255.255.0`	`192.168.30.1`	Dispositivos de usuario

Apéndice B: Fragmentos de Configuración de CLI Verificados

Configuración de DHCP en un Enrutador (Laboratorio 2)

```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)#ip dhcp excluded-address 192.168.20.1
Router(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.10
Router(config)#ip dhcp pool VLAN10_SALES
```

```
Router(config-dhcp)#network 192.168.10.0 255.255.255.0
Router(config-dhcp)#default-router 192.168.10.1
Router(config-dhcp)#dns-server 192.168.30.10
Router(config-dhcp)#exit
Router(config)#ip dhcp pool VLAN20_HR
Router(config-dhcp)#network 192.168.20.0 255.255.255.0
Router(config-dhcp)#default-router 192.168.20.1
Router(config-dhcp)#dns-server 192.168.30.10
Router(config-dhcp)#exit
Router(config)#ip dhcp pool VLAN30_IT
Router(config-dhcp)#network 192.168.30.0 255.255.255.0
Router(config-dhcp)#default-router 192.168.30.1
Router(config-dhcp)#dns-server 192.168.30.10
Router(config-dhcp)#exit
```

Configuración de "Router-on-a-Stick"

```
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface FastEthernet0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#interface FastEthernet0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit
```

Apéndice C: Lista de Dispositivos y Cables

Laboratorio 1

- **Dispositivos:** 1 x `Home Router`, 1 x `PC`, 1 x `Laptop`, 1 x `Printer`.
- **Cables:** `Copper Straight-Through` para conexiones por cable.

Laboratorio 2

- **Dispositivos:** 1 x `PT-Router`, 1 x `PT-MLS`, 2 x `PT-2960`, múltiples `PC`, `Laptop` y 1 x `PT-Server`.
- **Cables:** `Copper Straight-Through` para todas las conexiones Ethernet entre enrutadores, conmutadores y dispositivos finales.7

Laboratorio 1: Red Residencial/SOHO

Este laboratorio se centra en la configuración de un router como servidor DHCP para que los dispositivos finales obtengan su dirección IP automáticamente, tal como sucede en una red doméstica.

Paso 1: Configuración del Router (GUI)

En un entorno residencial, el `Home Router` se configura a menudo a través de su interfaz gráfica (GUI) en Packet Tracer. Los pasos son:

1. Haz clic en el `Home Router` en el espacio de trabajo de Packet Tracer.
2. Ve a la pestaña `GUI`.
3. En la sección `Network Setup` o `LAN Setup`, configura la dirección IP del router (por ejemplo, `192.168.0.1`) y la máscara de subred (`255.255.255.0`).
4. Activa el servicio DHCP (`DHCP Enabled`) y define el rango de direcciones que se asignarán (por ejemplo, un rango de inicio de `192.168.0.100` a `192.168.0.254`).
5. Guarda la configuración con el botón `Save Settings`.

Nota: La configuración de DHCP en un router estándar se hace a través de la CLI, como se muestra en el siguiente laboratorio.

Paso 2: Configuración de los Dispositivos Finales (PCs y Servidores)

Para que los dispositivos finales reciban una dirección IP del `Home Router`, debes configurarlos en modo DHCP.

1. Haz clic en un `PC` o una `Laptop`.
2. Ve a la pestaña `Desktop`.
3. Selecciona la aplicación `IP Configuration`.
4. Cambia la opción de `Static` a `DHCP`.

El dispositivo automáticamente solicitará y recibirá una dirección IP, una máscara de subred y la puerta de enlace predeterminada.

Paso 3: Verificación

Para confirmar que la red funciona, utiliza el `Command Prompt` de un PC.

- **Comprobar la dirección IP:**

  ```
  C:\> ipconfig
  ```

  Verifica que la dirección IPv4, la máscara y la puerta de enlace por defecto se hayan asignado correctamente.
- **Probar la conectividad:**

  ```
  C:\> ping 192.168.0.1
  ```

  Este comando envía paquetes de eco al router para verificar que hay conectividad con la puerta de enlace.

Laboratorio 2: Red de Campus Empresarial

Este laboratorio requiere una configuración más avanzada a través de la interfaz de línea de comandos (CLI) para cada dispositivo.

Paso 1: Configuración Inicial del Router (R-CORE)

Estos comandos establecen el nombre del dispositivo y configuran las interfaces para el enrutamiento inter-VLAN.

1. **Entrar al modo de configuración global:**

   ```
   Router> enable
   Router# configure terminal
   ```

   `enable` te da acceso al modo privilegiado.

`configure terminal` te permite hacer cambios en la configuración global del router.

- **Configurar la interfaz física para "Router-on-a-Stick":**

  ```
  Router(config)# interface FastEthernet0/0
  Router(config-if)# no ip address
  Router(config-if)# no shutdown
  Router(config-if)# exit
  ```

  `no ip address` elimina cualquier dirección IP preexistente en la interfaz física. `no shutdown` es un comando crucial que activa la interfaz, ya que por defecto están apagadas.

2. **Configurar sub-interfaces para cada VLAN:**

```
Router(config)# interface FastEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
Router(config)# interface FastEthernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

`encapsulation dot1Q` etiqueta el tráfico de la VLAN, y `ip address` asigna la puerta de enlace predeterminada para esa VLAN.

3. **Configurar el enrutamiento estático hacia Internet:**

```
Router(config)# ip route 0.0.0.0 0.0.0.0 <dirección-IP-del-siguiente-salto>
```

Este comando establece una ruta predeterminada (una "puerta de enlace de último recurso") para todo el tráfico que no tiene una ruta más específica, dirigiéndolo a una red simulada de Internet.

4. **Configurar el servicio DHCP:**

```
Router(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)# ip dhcp pool VENTAS
Router(config-dhcp)# network 192.168.10.0 255.255.255.0
Router(config-dhcp)# default-router 192.168.10.1
Router(config-dhcp)# dns-server 192.168.30.10
Router(config-dhcp)# exit
```

`ip dhcp excluded-address` se usa para evitar que el servidor asigne direcciones que ya están en uso (como las puertas de enlace o las de los servidores). El comando `ip dhcp pool` crea un pool de direcciones, definiendo la red, la puerta de enlace (`default-router`) y el servidor DNS.

Paso 2: Configuración del Switch (S1/S2 - Acceso)

Estos comandos segmentan la red con VLANs y configuran los puertos.

1. **Entrar al modo de configuración global:**

```
Switch> enable
Switch# configure terminal
```

2. **Crear VLANs y nombrarlas:**

```
Switch(config)# vlan 10
Switch(config-vlan)# name Ventas
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# name RRHH
Switch(config-vlan)# exit
```

`vlan <id>` crea la VLAN y `name` le asigna un nombre para una fácil identificación.

- **Configurar los puertos de acceso:**

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit
```

`switchport mode access` define el puerto para una sola VLAN, y `switchport access vlan` lo asigna a la VLAN correspondiente.

- **Configurar el puerto de enlace troncal (trunk):**

```
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# exit
```

`switchport mode trunk` permite que el puerto transporte el tráfico de varias VLANs.

`encapsulation dot1q` es necesario para etiquetar las tramas con su ID de VLAN.

Paso 3: Configuración del Dispositivo de Gestión (Servidor)

Para los servidores que deben tener una dirección IP fija, la configuración se realiza de forma estática a través de su interfaz gráfica.

1. Haz clic en el `Server`.
2. Ve a la pestaña `Desktop`.
3. Selecciona la aplicación `IP Configuration`.
4. Selecciona la opción `Static`.
5. Introduce la `dirección IPv4`, `Subnet Mask`, `Default Gateway` y `DNS Server` manualmente.

Paso 4: Verificación y Solución de Problemas

1. **Verificación de la tabla de enrutamiento (en el router):**

   ```
   Router# show ip route
   ```

   Este comando muestra la tabla de enrutamiento del router, lo que te permite verificar si ha aprendido las redes conectadas a través de las sub-interfaces y si la ruta estática está presente.

- **Verificación de la conectividad (en un PC):**

  ```
  C:\> ping <dirección-IP-del-destino>
  ```

  Se utiliza para comprobar la conectividad de extremo a extremo.
- **Trazar la ruta (en un PC):**

  ```
  C:\> traceroute <dirección-IP-del-destino>
  ```

  Este comando es útil para identificar en qué punto de la red se interrumpe la comunicación, ya que muestra cada salto (router) que un paquete atraviesa en su camino hacia el destino.