

# Puertos y direcciones.

## Direcciones IP

El uso de direcciones IP es el principal medio para permitir que los dispositivos se ubiquen entre sí y para establecer la comunicación completa en Internet. Cada terminal en una red se debe configurar con direcciones IP.

- PC (estaciones de trabajo, PC portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Teléfonos inteligentes
- Dispositivos portátiles móviles (tal como los escáner inalámbricos para códigos de barras)

La estructura de una dirección IPv4 se denomina “notación decimal punteada” y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red.

**Nota:** en este curso, IP refiere a los protocolos IPv4 e IPv6. IPv6 es la versión más reciente de IP y el reemplazo para el protocolo IPv4 más común

Con la dirección IPv4, también se necesita una máscara de subred. Una máscara de subred IPv4 es un valor de 32 bits que separa la porción de red de la dirección de la porción de host. Combinada con la dirección IPv4, la máscara de subred determina la subred particular a la pertenece el dispositivo.

El ejemplo de la figura 1 muestra la dirección IPv4 (192.168.1.10), la máscara de subred (255.255.255.0) y el gateway predeterminado (192.168.1.1) asignados a un host. La dirección de gateway predeterminado es la dirección IP del router que el host utilizará para acceder a las redes remotas, incluso a Internet.

Las direcciones IP se pueden asignar tanto a los puertos físicos como a las interfaces virtuales de los dispositivos. Una interfaz virtual significa que no hay hardware físico en el dispositivo asociado a ella.

## Interfaces y puertos

Las comunicaciones de red dependen de las interfaces de los dispositivos para usuarios finales, las interfaces de los dispositivos de red y los cables que las conectan. Cada interfaz física tiene especificaciones o estándares que la definen. Los cables que se conectan a la interfaz deben estar diseñados para cumplir con los estándares físicos de la interfaz. Los tipos de medios de red incluyen los cables de cobre de par trenzado, los cables de fibra óptica, los cables coaxiales o la tecnología inalámbrica, como se muestra en la figura.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Algunas de las diferencias entre los distintos tipos de medios incluyen las siguientes:

- La distancia a través de la cual los medios pueden transportar una señal correctamente.
- El ambiente en el cual se instalará el medio.
- La cantidad de datos y la velocidad a la que se deben transmitir.
- El costo de los medios y de la instalación.

Cada enlace de Internet no solo requiere un tipo específico de medio de red, sino que también requiere una determinada tecnología de red. Por ejemplo, Ethernet es la tecnología de red de área local (LAN) de uso más frecuente en la actualidad. Hay puertos Ethernet en los dispositivos para usuarios finales, en los dispositivos de switch y en otros dispositivos de red que se pueden conectar físicamente a la red mediante un cable.

Los switches de la capa 2 de Cisco IOS cuentan con puertos físicos para conectar dispositivos. Estos puertos no son compatibles con las direcciones IP de la capa 3. En consecuencia, los switches tienen una o más interfaces virtuales de switch (SVI). Son interfaces virtuales porque no hay hardware físico en el dispositivo asociado a ellas. Una SVI se crea en el software.

La interfaz virtual proporciona un medio para administrar un switch de manera remota a través de una red usando IPv4. Cada switch viene con una SVI que aparece en la configuración predeterminada, fácil de instalar. La SVI predeterminada es interfaz VLAN1.

**Nota:** Un switch de capa 2 no necesita una dirección IP. La dirección IP asignada a la SVI se utiliza para acceder al switch de forma remota. No se necesita una dirección IP para que el switch realice estas operaciones.

## Configurar direccionamiento IP.

### Configuración manual de dirección IP para terminales

Para que un terminal se comuniquen a través de la red, se debe configurar con una dirección IPv4 y una máscara de subred únicas. La información de dirección IP se puede introducir en los terminales en forma manual o automáticamente mediante el Protocolo de configuración dinámica de host (DHCP).

Para configurar una dirección IPv4 de forma manual en un host de Windows, abra **Panel de Control > Centro de redes y recursos compartidos > Cambiar configuración del adaptador y seleccione el adaptador**. Luego, haga clic con el botón secundario y seleccione **Propiedades** para que aparezcan las **Propiedades de conexión de área local**, como se muestra en la figura 1.

Resalte el protocolo de Internet versión 4 (TCP/IPv4) y haga clic en **Propiedades** para abrir la ventana de **Propiedades del protocolo de Internet versión 4 (TCP/IPv4)**, como se muestra en la figura 2. Configure la información de la dirección IPv4 y la máscara de subred, y el gateway predeterminado.

**Nota:** La dirección del servidor DNS es la dirección IPv4 del servidor del sistema de nombres de dominio (DNS), que se utiliza para traducir direcciones IP a direcciones web, como [www.cisco.com](http://www.cisco.com).

## Configuración automática de direcciones IP para terminales

En general, las PC utilizan DHCP de forma predeterminada para la configuración automática de direcciones IPv4. DHCP es una tecnología que se utiliza en casi todas las redes. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo.

En una red, DHCP permite la configuración automática de direcciones IPv4 para cada terminal con DHCP habilitado. Imagine la cantidad de tiempo que le llevaría si cada vez que se conectara a la red tuviera que introducir manualmente la dirección IPv4, la máscara de subred, el gateway predeterminado y el servidor DNS. Multiplique eso por cada usuario y cada uno de los dispositivos en una organización y se dará cuenta del problema. La configuración manual también aumenta las posibilidades de configuraciones incorrectas provocadas por la duplicación de la dirección IPv4 de otro dispositivo.

Como se muestra en la figura 1, para configurar el protocolo DHCP en una PC con Windows, solo debe seleccionar “Obtener una dirección IP automáticamente” y “Obtener la dirección del servidor DNS automáticamente”. Su PC buscará un servidor DHCP y se le asignarán los ajustes de dirección necesarios para comunicarse en la red.

Es posible mostrar los ajustes de configuración IP en una PC con Windows usando el comando `ipconfig` cuando el sistema se lo solicite. El resultado muestra la información de dirección IPv4, máscara de subred y gateway que se recibió del servidor DHCP.

Verificador de sintaxis de la Figura 2 para practicar cómo mostrar la dirección IPv4 en una PC con Windows.

## Configuración de interfaz virtual de switch

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI. Para configurar una SVI en un switch, utilice el comando de configuración global **interface vlan 1**. La Vlan 1 no es una interfaz física real, sino una virtual. A continuación, asigne una dirección IPv4 mediante el comando **ip address ip-address subnet-mask** de la configuración de interfaz.

Finalmente, habilite la interfaz virtual con el comando de configuración de interfaz **no shutdown**.

Una vez que se configuran estos comandos, el switch tiene todos los elementos IPv4 listos para la comunicación a través de la red.

## **Verificador de sintaxis: Configuración de una interfaz virtual de switch**

### **Verificación de la conectividad. Verificación de la asignación de direcciones de interfaz**

Del mismo modo que se usan comandos y utilidades como ipconfig para verificar la configuración de red de un host de PC, se deben utilizar los comandos para verificar los ajustes de interfaces y dirección de los dispositivos intermediarios, como switches y routers.

## **Prueba de conectividad completa**

El comando ping puede utilizarse para probar la conectividad de otro dispositivo en la red o un sitio web en Internet.

## **Conclusión.**

### **Actividad de clase: Enséñeme**

Los estudiantes trabajarán de a dos. Para esta actividad, se requiere Packet Tracer.

Suponga que un colega nuevo le pidió que lo oriente sobre la CLI de Cisco IOS. Este colega nunca trabajó con dispositivos Cisco

Usted le explica los comandos y la estructura básicos de la CLI, porque desea que su colega comprenda que la CLI es un lenguaje de comandos simple pero eficaz que se puede comprender y navegar fácilmente.

Utilice Packet Tracer y una de las actividades disponibles en este capítulo como modelo de red simple (por ejemplo, la Práctica de laboratorio: Configuración de una dirección de administración del switch).

**Céntrese en estas áreas:**

- Si bien los comandos son técnicos, ¿se asemejan a enunciados del lenguaje corriente?

- ¿Cómo se organiza el conjunto de comandos en subgrupos o modos?  
¿Cómo sabe un administrador qué modo está utilizando?
- ¿Cuáles son los comandos individuales para configurar los parámetros básicos de un dispositivo Cisco? ¿Cómo explicaría este comando en términos sencillos? Establezca semejanzas con la vida real cuando sea adecuado.

Sugiera cómo agrupar distintos comandos según sus modos de manera que se necesite una cantidad mínima de desplazamientos entre modos.

Cisco IOS es un término que abarca diferentes sistemas operativos que se ejecutan en diversos dispositivos de redes. El técnico puede introducir comandos para configurar o programar el dispositivo a fin de que lleve a cabo diversas funciones de redes. Los routers y switches Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma esperada.

Se accede a los servicios que proporciona Cisco IOS mediante una interfaz de línea de comandos (CLI), a la que se accede a través del puerto de consola, el puerto auxiliar o mediante Telnet o SSH. Una vez que se conectan a la CLI, los técnicos de red pueden realizar cambios de configuración en los dispositivos Cisco IOS. Cisco IOS está diseñado como sistema operativo modal, esto significa que los técnicos de red deben navegar a través de diversos modos jerárquicos del IOS. Cada modo admite distintos comandos del IOS.

Los routers y switches Cisco IOS admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial durante su implementación en una red son idénticos para ambos dispositivos.

En este capítulo, se presentó Cisco IOS. Se explicaron los diversos modos de Cisco IOS en detalle y se analizó la estructura básica de comandos que se utiliza para configurarlo. También se exploró la configuración inicial de los dispositivos de switch Cisco IOS, que incluye la configuración de un nombre, la limitación del acceso a la configuración de dispositivos, la configuración de mensajes de aviso y el guardado de la configuración.

En el capítulo siguiente, se analiza cómo se desplazan los paquetes a través de la infraestructura de red y se presentan las reglas de comunicación de paquetes.

## **Configuración de los parámetros iniciales.**

### **Pasos básicos en la configuración de un switch.**

Los routers y switches Cisco tienen muchas similitudes. Admiten un sistema operativo similar, estructuras de comandos similares y muchos de los mismos

comandos. Asimismo, ambos dispositivos usan los mismos pasos de configuración inicial cuando se implementan en una red.

Antes de comenzar a configurar un router, revise las tareas iniciales de configuración de un switch que se indican en la figura 1. En la figura 2, se muestra una configuración de ejemplo.

## **Pasos básicos en la configuración de un router.**

De manera similar a cuando se configura un switch, cuando se configuran los parámetros iniciales en un router, se deben completar las tareas que se indican en la figura 1.

En las figuras 2 a 5, se proporciona un ejemplo de estas tareas que se configuran en un router. En la figura 2, se asigna un nombre de host al router. En la figura 3, se protegen las líneas de acceso EXEC privilegiado, EXEC del usuario y acceso remoto con una contraseña, y se cifran todas las contraseñas en el archivo de configuración. Las notificaciones legales se configuran en la figura 4. Por último, la configuración se guarda en la figura 5.

Utilice el verificador de sintaxis de la figura 6 para practicar estos pasos de configuración.

## **Configuración de interfaces.**

### **Configurar interfaces de routers.**

Para que se pueda llegar a los routers, se deben configurar las interfaces de router en banda. Existen muchos tipos diferentes de interfaces para los routers Cisco. En este ejemplo, el router Cisco de la serie 1941 tiene las siguientes características:

- Dos interfaces Gigabit Ethernet: GigabitEthernet 0/0 (G0/0) y GigabitEthernet 0/1 (G0/1)
- Una tarjeta de interfaz serial WAN (WIC) que consta de dos interfaces: serial 0/0/0 (S0/0/0) y serial 0/0/1 (S0/0/1)

Nota: Haga clic [aquí](#) para obtener más información sobre la abreviatura y la numeración de interfaces.

Las tareas para configurar una interfaz de router se indican en la figura 1. Observe cómo se asemeja a configurar una SVI de administración en un switch.

Si bien no es necesario, es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. El texto de la descripción tiene un límite de 240 caracteres. En las redes de producción, una descripción puede ser útil para la solución de problemas, dado que proporciona información con respecto al tipo de red a la que está conectada la interfaz y con respecto a otros routers que pueda haber en esa red. Si la interfaz se conecta a un ISP o a un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

Al usar el comando `no shutdown`, se activa la interfaz y es similar a darle energía. La interfaz también debe estar conectada a otro dispositivo, como un switch o un router, para que la capa física se active.

En la figura 2, se muestra la configuración de las interfaces de la red LAN conectadas al R1.

## Verificación de configuración de interfaz.

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. El más útil de ellos es **`show ip interface brief`**. El resultado generado muestra todas las interfaces, su dirección IPv4 y el estado actual. Las interfaces configuradas y conectadas deben mostrar un estado "up" y el protocolo "up". Cualquier otra cosa indica que existe un problema con la configuración o con los cables.

Puede verificar la conectividad de la interfaz con el comando **`ping`**. Los routers Cisco envían cinco pings consecutivos y miden los tiempos de ida y vuelta mínimo, máximo y promedio. Los signos de exclamación verifican la conectividad.

En la figura 1, se muestra el resultado del comando **`show ip interface brief`**, que muestra que las interfaces de la red LAN y el enlace WAN están activos y en funcionamiento. Observe que el comando **`ping`** genera cinco signos de exclamación que verifican la conectividad al R2.

Otros comandos de verificación de interfaz pueden ser los siguientes:

- **`show ip route`**: Muestra el contenido de la tabla de routing IPv4 que se almacena en la RAM.
- **`show interfaces`**: Muestra las estadísticas de todas las interfaces de un dispositivo.
- **`show ip interface`**: Muestra las estadísticas IPv4 de todas las interfaces de un router.

En la figura 2, se muestra el resultado del comando **`show ip route`**. Observe las tres redes conectadas directamente con las direcciones IPv4 de interfaz local.

Recuerde guardar la configuración con el comando `copy running-config`

`startup-config`. **Configuración del gateway predeterminado.**

## Gateway predeterminado para un host.

Para que un terminal se comuniquen a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de gateway predeterminado. El gateway predeterminado se usa solamente cuando el host desea enviar un paquete a un dispositivo de otra red. En general, la dirección de gateway predeterminado es la dirección de la interfaz de router conectada a la red



local del host. La dirección IP del dispositivo host y la dirección de interfaz de router deben estar en la misma red.

La topología de red en la Figura 1 y 2 consta de un router que interconecta las dos LAN separadas. G0/0 se conecta a la red 192.168.10.0, mientras que G0/1 se conecta a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de gateway predeterminado apropiada.

En la figura 1, la PC1 envía un paquete a la PC2. En este ejemplo, no se utiliza el gateway predeterminado. En cambio, PC1 dirige el paquete con la dirección IP de PC2 y lo reenvía directamente a PC2 a través del switch.

En la figura 2, la PC1 envía un paquete a la PC3. En este ejemplo, la PC1 dirige un paquete con la dirección IP de la PC3, pero luego envía el paquete al router. El router acepta el paquete, accede a su tabla de routing para determinar la interfaz de salida apropiada según la dirección de destino y, luego, envía el paquete por la interfaz apropiada para que llegue a la PC3.

## Gateway predeterminado para un switch.

Por lo general, un switch de grupo de trabajo que interconecta computadoras cliente es un dispositivo de capa 2. Como tal, un switch de capa 2 no necesita una dirección IP para funcionar adecuadamente. Sin embargo, si desea conectarse al switch y administrarlo en varias redes, debe configurar la SVI con una dirección IPv4, una máscara de subred y una dirección de gateway predeterminado.

Por lo general, la dirección del gateway predeterminado se configura en todos los dispositivos que desean comunicarse más allá de la red local. En otras palabras, para acceder de manera remota al switch desde otra red con SSH o Telnet, el switch debe tener una SVI configurado con una dirección IPv4, una máscara de subred y una dirección de gateway predeterminado. Si se accede al switch desde un host dentro de la red local, la dirección IPv4 de gateway predeterminado no es necesaria.

Para configurar un gateway predeterminado en un switch, use el comando de configuración global **ip default-gateway**. La dirección IP configurada es la de la interfaz de router del switch conectado.

En la Figura 1 se muestra un administrador que establece una conexión remota al switch S1 en otra red. El switch S1 se debe configurar con un gateway predeterminado, para que pueda responder y establecer una conexión SSH con el host administrativo.

Un concepto erróneo habitual es que el switch usa su dirección de gateway predeterminado configurada para determinar a dónde enviar los paquetes provenientes de los hosts conectados al switch y destinados a hosts de redes remotas. En realidad, la información de dirección IP y de gateway predeterminado se usa únicamente para los paquetes que se originan en el switch. Los paquetes que se originan en servidores conectados al switch ya deben crearse con la dirección de gateway predeterminado configurada en el sistema operativo de su servidor.



