TALLER DE NETWORKING

Unidad 2

Fundamentos de enrutamiento y de conmutación de LAN

ESCUELA CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Luis Jaque Zúñiga

Diseñadora instruccional: Evelyn Aguilera Bustos

Editora instruccional: Lorena Fernández Alfaro

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

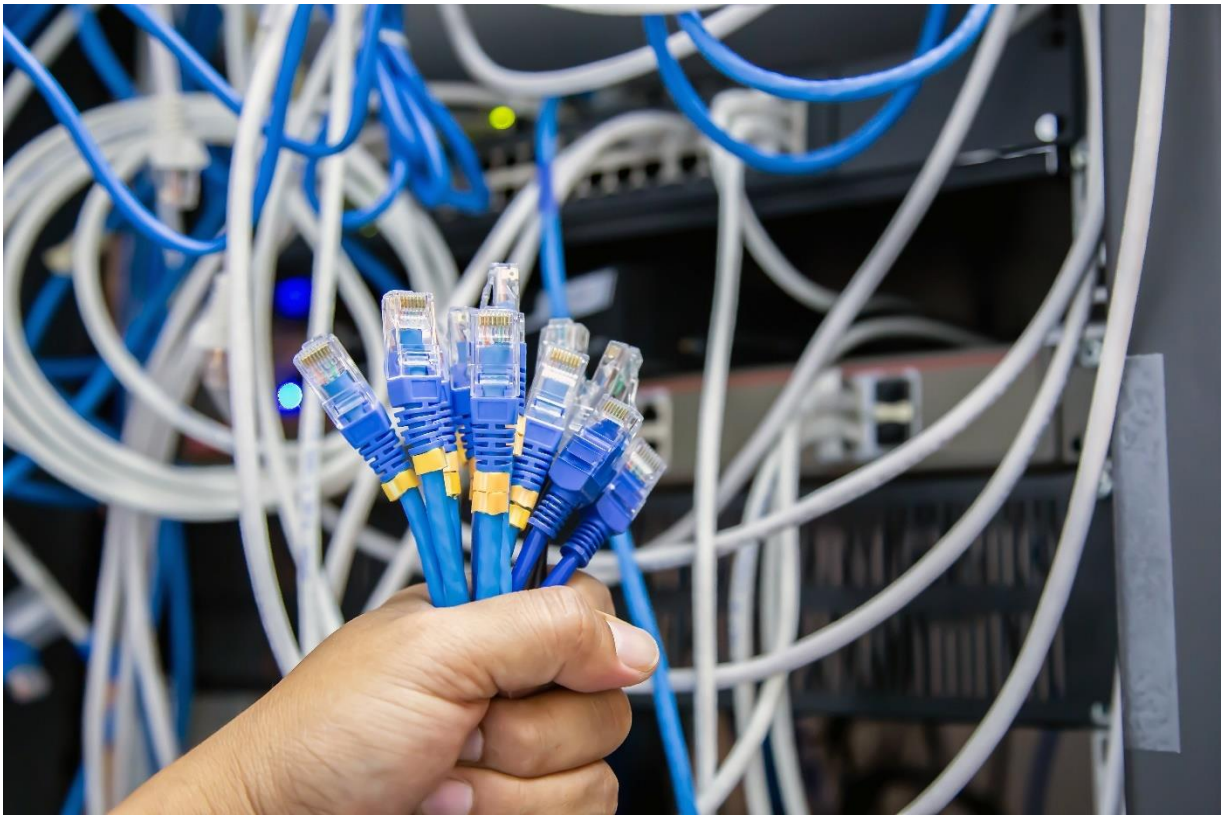
AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Implementan red LAN considerando configuración y sus servicios.



Fuente: Freepik. (s.f.-b)

Introducción

Estimados y estimadas estudiantes:

Durante esta semana profundizaremos los conceptos relacionados con la implementación de una red LAN considerando configuración y sus servicios.

Específicamente revisaremos:

- Uso de Telnet/SSH en conexión remota.
- Contraseñas y direccionamiento IP en dispositivos.
- Servicios DHCP, DNS, WEB e EMAIL.
- Dispositivos inalámbricos LAN.
- Asignación de direccionamiento.
- Cifrado de autenticación WPA2-WPA2-PERSONAL.
- Habilitación de DHCP.
- Filtrado por direcciones MAC.

Al finalizar la semana podremos responder preguntas, tales como:

- ¿Cómo se comprueban comandos básicos de switch y router basándose en Cisco IOS?
- ¿Cómo se configura una VLAN administrativa incorporando estándar vigente IEEE 802.1Q?
- ¿Cómo se configuran los servicios en el servidor, en función de los usuarios de la red local?
- ¿Cómo configurar un router inalámbrico aplicando estándares definidos por la Wi-Fi Alliance?

1. Acceso a Cisco IOS

1.1.- Sistemas operativos

Todos los dispositivos finales y dispositivos de red requieren un sistema operativo (OS). Como se muestra en la figura 1, la parte del Sistema Operativo que interactúa directamente con el hardware de la PC se conoce como kernel. La parte que interactúa con las aplicaciones y el usuario se conoce como shell. El usuario puede interactuar con el shell mediante la interfaz de línea de comandos (CLI) o la interfaz gráfica del usuario (GUI).

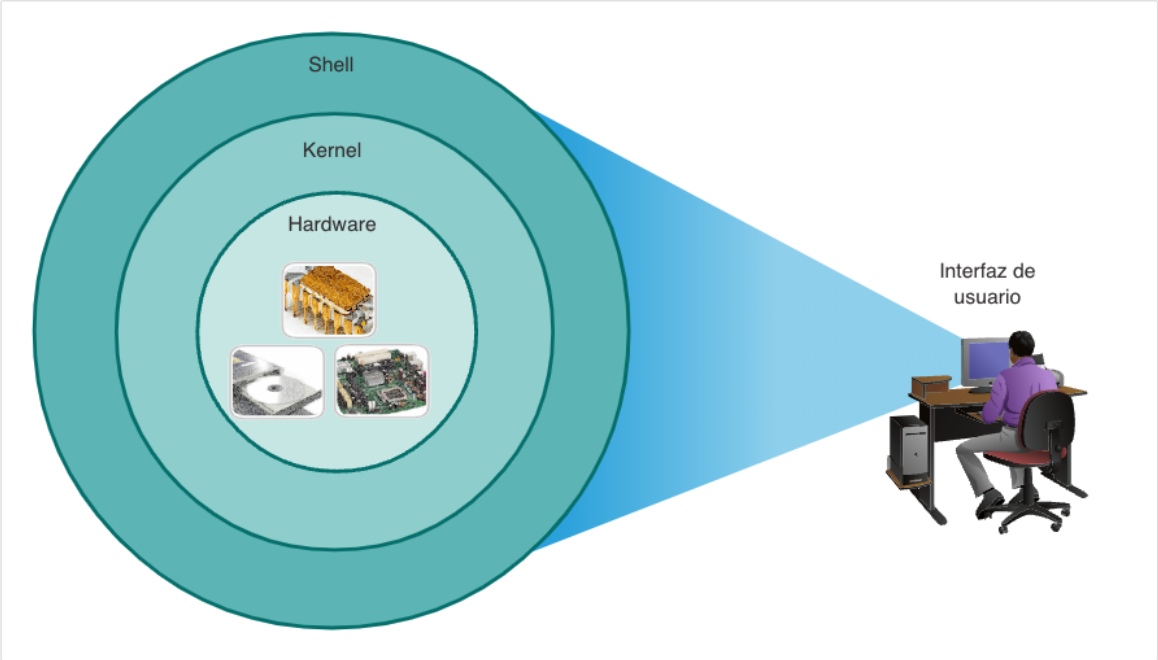


Figura 1. Partes de un Sistema Operativo.

Fuente: Cisco Networking Academy (2022)

Las definiciones de estas partes son:

Shell: la interfaz de usuario que permite a los usuarios solicitar tareas específicas del equipo. Estas solicitudes se pueden realizar a través de las interfaces CLI o GUI.

Kernel: establece la comunicación entre el hardware y el software de una computadora y administra el uso de los recursos de hardware para cumplir los requisitos del software.

Hardware: la parte física de una computadora, incluida la electrónica subyacente.

Cuando se usa una CLI, el usuario interactúa directamente con el sistema en un entorno basado en texto ingresando comandos en el teclado en un símbolo del sistema, como se muestra en el ejemplo (figura 2). El sistema ejecuta el comando y, por lo general, proporciona una respuesta en forma de texto. La CLI necesita muy poca sobrecarga para operar. Sin embargo, exige que el usuario tenga conocimientos de la estructura subyacente que controla el sistema.

Figura 2. Ejemplo de CLI.

Fuente: Cisco Networking Academy (2022)

1.2.- Propósito del OS

Los sistemas operativos de red son similares al sistema operativo de una PC. Mediante una GUI, un sistema operativo de PC permite que el usuario realice lo siguiente:

- Utilizar un mouse para hacer selecciones y ejecutar programas.
- Introducir texto y comandos de texto.
- Ver resultados en un monitor.

Un sistema operativo basado en CLI como el Cisco IOS en un switch o router, permite que un técnico de red realice lo siguiente:

- Utilizar un teclado para ejecutar programas de red basados en la CLI.
- Utilizar un teclado para introducir texto y comandos basados en texto.
- Ver resultados en un monitor.

Los dispositivos de red de Cisco ejecutan versiones especiales de Cisco IOS. La versión de IOS depende del tipo de dispositivo que se utilice y de las características necesarias. Si bien todos los dispositivos traen un IOS y un conjunto de características predeterminados, es posible actualizar el conjunto de características o la versión de IOS para obtener capacidades adicionales.

En la figura 3 se muestra una lista de las versiones del software IOS para un switch Cisco Catalyst 2960.

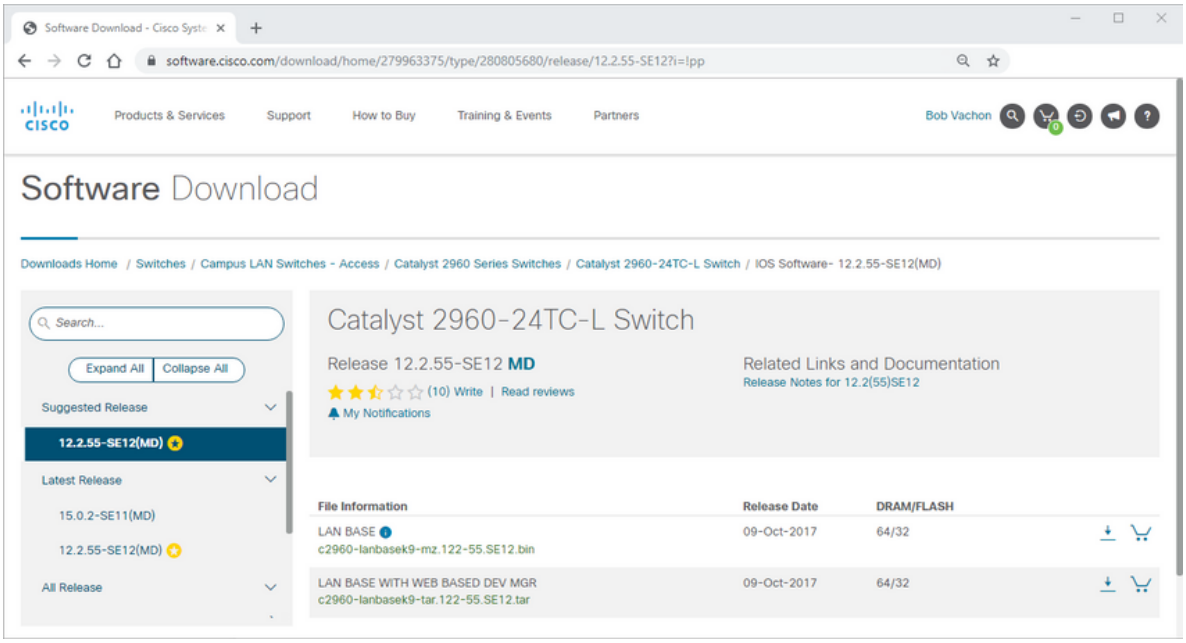


Figura 3. Ejemplo de descarga de software de Cisco.

Fuente: Cisco Networking Academy (2022)

1.3.- Métodos de acceso

Un switch reenviará el tráfico de forma predeterminada y no necesita configurarse explícitamente para funcionar. Por ejemplo, dos hosts configurados conectados al mismo switch nuevo podrían comunicarse.

Independientemente del comportamiento predeterminado de un switch nuevo, todos los switches deben estar configurados y protegidos.

Método	Descripción
Consola	Este es un puerto de administración físico que proporciona acceso fuera de banda a un dispositivo de Cisco. El acceso fuera de banda hace referencia al acceso por un canal de administración exclusivo que se usa únicamente con fines de mantenimiento del dispositivo. La ventaja de usar un puerto de consola es que el dispositivo es accesible incluso si no hay servicios de red configurados, como realizar la configuración inicial. Para una conexión de consola se requiere un equipo con software de emulación de terminal y un cable de consola especial para conectarse al dispositivo.
Secure Shell (SSH)	SSH, es un método para establecer de manera remota una conexión CLI segura a través de una interfaz virtual por medio de una red. A diferencia de las conexiones de consola, las conexiones SSH requieren servicios de red activos en el dispositivo, incluida una interfaz activa configurada con una dirección. La mayoría de las versiones de Cisco IOS incluyen un servidor SSH y un cliente SSH que pueden utilizarse para establecer sesiones SSH con otros dispositivos.
Telnet	Telnet es un método inseguro para establecer una sesión CLI de manera remota a través de una interfaz virtual por medio de una red. A diferencia de SSH, Telnet no proporciona una conexión segura y encriptada y solo debe usarse en un entorno de laboratorio. La autenticación de usuario, las contraseñas y los comandos se envían por la red en texto simple. La mejor práctica es usar SSH en lugar de Telnet. Cisco IOS incluye un servidor Telnet y un cliente Telnet.

Tabla 1. Métodos de acceso al IOS.

Fuente: Cisco Networking Academy (2022)

Nota: Algunos dispositivos, como los routers, también pueden admitir un puerto heredado auxiliar utilizado para establecer una sesión CLI de forma remota a través de una conexión telefónica utilizando un módem. Al igual que la conexión de consola, el puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red.

1.4.- Programación de emulación de terminal

Existen varios programas de emulación de terminal que puede usar para conectarse a un dispositivo de red, ya sea mediante una conexión en serie, a través de un puerto de consola o mediante una conexión SSH / Telnet. Estos programas permiten aumentar la productividad mediante ajustes del tamaño de la ventana, modificaciones de los tamaños de fuente y cambios en los esquemas de colores.

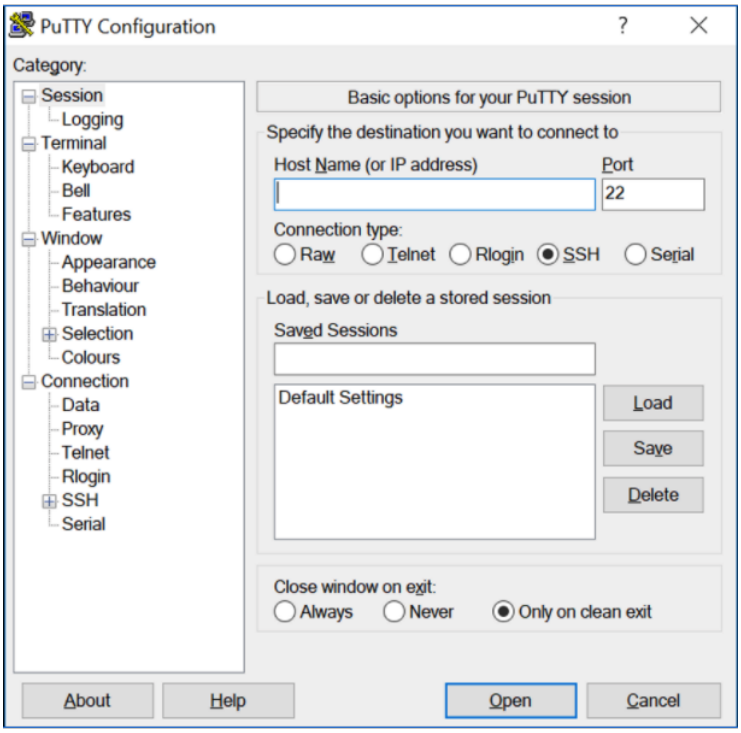


Figura 4. Ejemplo terminal PuTTY.

Fuente: Cisco Networking Academy (2022)

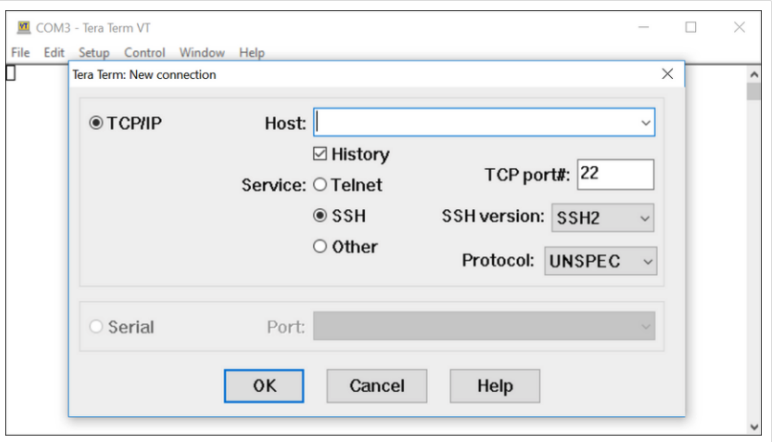


Figura 5. Ejemplo terminal Tera Term.

Fuente: Cisco Networking Academy (2022)

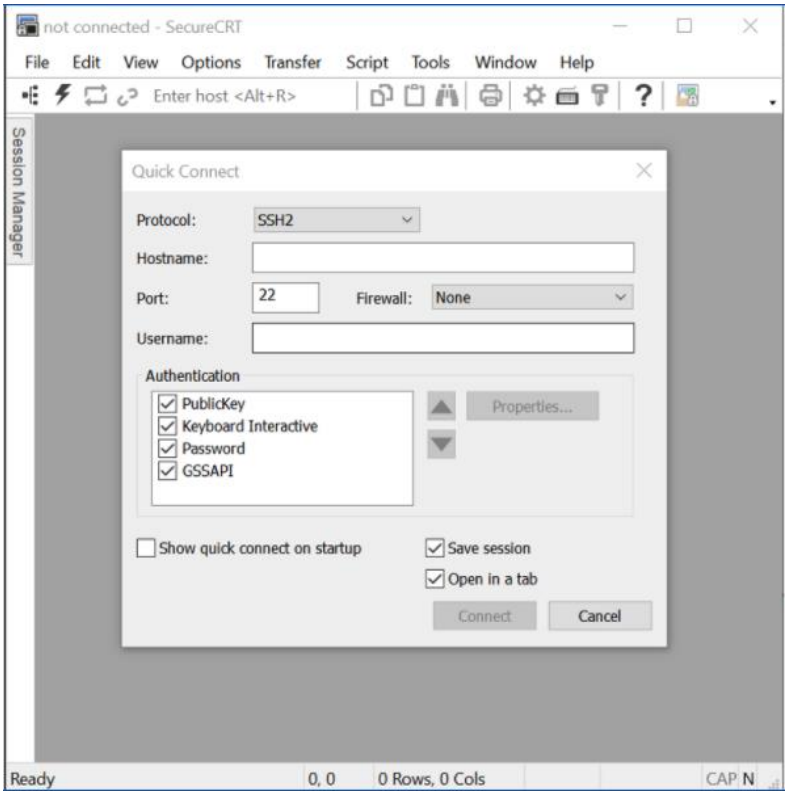


Figura 6. Ejemplo terminal Secure CRT.

Fuente: Cisco Networking Academy (2022)

1.5.- Modo de comando principales

En el tema anterior, revisamos que todos los dispositivos de red requieren un sistema operativo y que se pueden configurar mediante la CLI o una GUI. El uso de la CLI puede proporcionar al administrador de red un control y flexibilidad más precisos que el uso de la GUI. Aquí se describirá el uso de CLI para navegar por Cisco IOS.

Como característica de seguridad, el software IOS de Cisco divide el acceso de administración en los siguientes dos modos de comando:

- Modo de ejecución de usuario - Este modo tiene capacidades limitadas pero resulta útil en el caso de algunas operaciones básicas. Permite solo una cantidad limitada de comandos de monitoreo básicos, pero no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo. El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >.
- Modo de ejecución privilegiado - Para ejecutar comandos de configuración, un administrador de redes debe acceder al modo de ejecución privilegiado. Solo se puede ingresar al modo de configuración global y a los modos de configuración más altos por medio del modo EXEC con privilegios. El modo EXEC con privilegios se puede reconocer por la petición de entrada que termina con el # símbolo.

Modo de comando	Descripción	Indicador de dispositivo predeterminado
Modo EXEC del usuario	• El modo permite el acceso a solo un número limitado de monitoreo básico comandos. • A menudo se le conoce como un modo de "visualización solamente".	Switch> Router>
Modo EXEC privilegiado	• El modo permite el acceso a todos los comandos y funciones. • El usuario puede usar cualquier comando de monitoreo y ejecutar la configuración y comandos de administración.	Switch# Router#

Tabla 2. *Modos CLI predeterminados de un switch y router Cisco.*

Fuente: Cisco Networking Academy (2022)

1.6.- Modo de configuración y modos de subconfiguración

Para configurar el dispositivo, el usuario debe ingresar al modo de configuración global, que normalmente se denomina modo de config. global.

Desde el modo de configuración global, se realizan cambios en la configuración de la CLI que afectan la operación del dispositivo en su totalidad. El modo de configuración global se identifica mediante un mensaje que termina (config)# después del nombre del dispositivo, como Switch(config)#.

Antes de acceder a otros modos de configuración específicos, se accede al modo de configuración global. Desde el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. Dos modos de subconfiguración comunes incluyen:

- Modo de configuración de líneas - Se utiliza para configurar la consola, SSH, Telnet o el acceso auxiliar.
- Modo de configuración de interfaz - Se utiliza para configurar un puerto de switch o una interfaz de red de router.

Cuando se utiliza la CLI, el modo se identifica mediante la línea de comandos que es exclusiva de ese modo. De manera predeterminada, cada petición de entrada empieza con el nombre del dispositivo. Después del nombre, el resto de la petición de entrada indica el modo. Por ejemplo, el indicador predeterminado para el modo de configuración de línea es Switch(config-line)# and the default prompt for interface configuration mode is Switch(config-if)#.

2. Configuración básica de dispositivos

2.1.- Nombres de los dispositivos

El primer comando de configuración en cualquier dispositivo debe ser para darle un nombre de dispositivo único o nombre de host. De forma predeterminada, a todos los dispositivos se les asigna un nombre predeterminado de fábrica. Por ejemplo, un switch Cisco IOS es "Switch".

El problema es que si todos los switches de una red se quedaran con sus nombres predeterminados, sería difícil identificar un dispositivo específico. Por ejemplo, ¿cómo sabrías que estás conectado al dispositivo correcto al acceder remotamente a través de SSH?

El nombre de host proporciona la confirmación de que está conectado al dispositivo correcto.

El nombre predeterminado debe cambiarse a algo más descriptivo. Al elegir nombres atinadamente, resulta más fácil recordar, analizar e identificar los dispositivos de red. Estas son algunas pautas de nomenclatura importantes para los hosts:

- Comenzar con una letra.
- No contener espacios.
- Finalizar con una letra o dígito.
- Utilizar únicamente letras, dígitos y guiones.
- Tener menos de 64 caracteres de longitud.

Una organización debe elegir una convención de nomenclatura que haga que sea fácil e intuitivo identificar un dispositivo específico. Los nombres de host utilizados en el IOS del dispositivo conservan el uso de caracteres en mayúscula y minúscula. Por ejemplo, la figura 7 muestra que tres switches, que abarcan tres pisos diferentes, están interconectados en una red.

La convención de nomenclatura que se utilizó incorporó la ubicación y el propósito de cada dispositivo. La documentación de red debe explicar cómo se seleccionaron estos nombres para que se pueda seguir el mismo criterio en la denominación de los dispositivos adicionales.

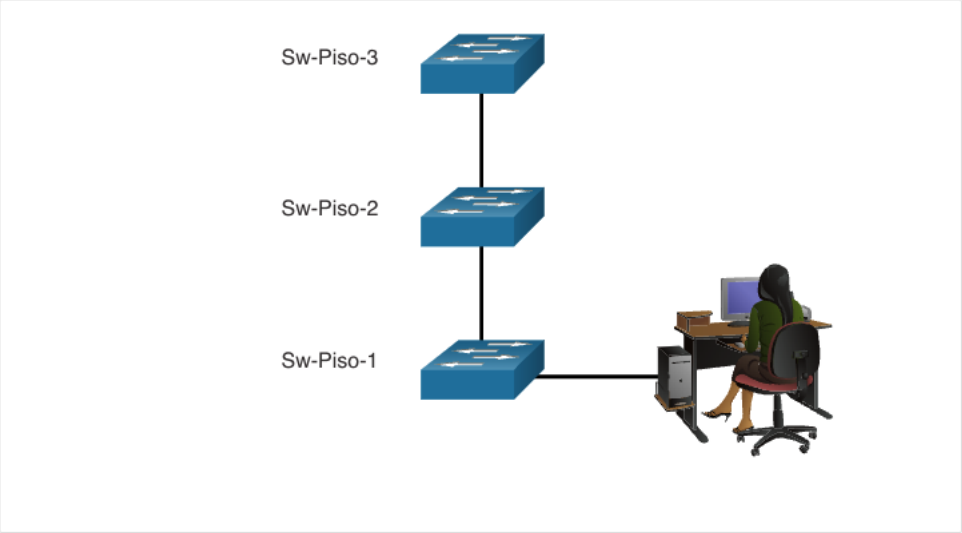


Figura 7. Asignación de nombres a switches.
Fuente: Cisco Networking Academy (2022)

Cuando se ha identificado la convención de nomenclatura, el siguiente paso es usar la CLI para aplicar los nombres a los dispositivos. Como se muestra en el ejemplo, desde el modo EXEC privilegiado, acceda al modo de configuración global ingresando el comando configurar terminal. Observa el cambio en el comando de petición de entrada:

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Figura 8. Comando petición de entrada.

Fuente: Cisco Networking Academy (2022)

Desde el modo de configuración global, ingrese el comando hostname seguido del nombre del equipo y presione. Enter. Observe el cambio en el comando de petición de entrada.

Nota: Para devolver el switch al indicador predeterminado, use el comando de configuración global no hostname.

Siempre hay que asegurarse que la documentación esté actualizada cada vez que se agrega o modifica un dispositivo. Es esencia identificar los dispositivos en la documentación por su ubicación, propósito y dirección.

2.2.- Configuración de contraseñas

Cuando se conecta inicialmente a un dispositivo, se encuentra en modo EXEC de usuario. Este modo está protegido usando la consola.

Para proteger el acceso al modo EXEC del usuario, se debe introducir el modo de configuración del CLI mediante el comando de configuración line console 0, como se muestra en el ejemplo, el cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola. Luego, se configura la contraseña de modo EXEC de usuario con el comando password y finalmente, se habilita el acceso EXEC de usuario con el comando login.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# end
Sw-Floor-1#
```

Figura 9. Comando password.

Fuente: Cisco Networking Academy (2022)

El acceso a la consola ahora requerirá una contraseña antes de permitir el acceso al modo EXEC del usuario.

Para tener acceso de administrador a todos los comandos del IOS, incluida la configuración de un dispositivo, se debe obtener acceso en modo EXEC privilegiado. Es el método de acceso más importante porque proporciona acceso completo al dispositivo.

Para asegurar el acceso privilegiado a EXEC, se debe usar el comando enable secret password , como se muestra en el ejemplo.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Figura 10. Comando enable secret password.
Fuente: Cisco Networking Academy (2022)

Las líneas de terminal virtual (VTY) permiten el acceso remoto mediante Telnet o SSH al dispositivo. Muchos switches de Cisco admiten hasta 16 líneas VTY que se numeran del 0 al 15.

Para proteger las líneas VTY, se debe introducir el modo VTY de línea mediante el comando line vty 0 15 global config. Luego, especificar la contraseña de VTY con el comando password. Por último, habilitar el acceso a VTY con el comando login.

Se muestra un ejemplo de seguridad de las líneas VTY en un switch.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
SW-Floor-1(config-line)# end
Sw-Floor-1#
```

Figura 11. Comando login.
Fuente: Cisco Networking Academy (2022)

2.3.- Encriptación de las contraseñas

Los archivos startup-config y running-config muestran la mayoría de las contraseñas en texto simple. Esta es una amenaza de seguridad porque cualquiera puede descubrir las contraseñas si tiene acceso a estos archivos.

Para encriptar todas las contraseñas de texto sin formato, se debe utilizar el comando service password-encryption global config como se muestra en el ejemplo:

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)#
```

Figura 12. Comando service password-encryption.
Fuente: Cisco Networking Academy (2022)

El comando aplica un cifrado débil a todas las contraseñas no encriptadas. Esta encriptación solo se aplica a las contraseñas del archivo de configuración; no a las contraseñas mientras se envían a través de los medios. El propósito de este comando es evitar que individuos no autorizados vean las contraseñas en el archivo de configuración.

show running-config se debe usar el comando para verificar que las contraseñas estén ahora encriptadas.

```
SW-Floor-1(config)# end
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
line vty 0 4
password 7 03095A0F034F38435B49150A1819
login
!
!
end
```

Figura 13. Comando show running-config.

Fuente: Cisco Networking Academy (2022)

3. Configurar direccionamiento IP

3.1.- Configuración manual de direcciones IP para dispositivos finales

Así como necesitas los números de teléfono de tus amigos para enviarles mensajes de texto o llamarlos, los dispositivos finales de tu red necesitan una dirección IP para que puedan comunicarse con otros dispositivos de tu red. En este tema, revisaremos la implementación de la conectividad básica configurando el direccionamiento IP en switches y PC.

La información de la dirección IPv4 se puede ingresar en los dispositivos finales de forma manual o automática mediante el Protocolo de configuración dinámica de host (DHCP).

Para configurar manualmente una dirección IPv4 en un host de Windows, se debe abrir Panel de Control > Network Sharing Center > Change adapter settings y elegir el adaptador. A continuación, hacer clic con el botón derecho y seleccionar Propiedades para mostrar el Local Area Connection Properties, como se muestra en la figura 14:

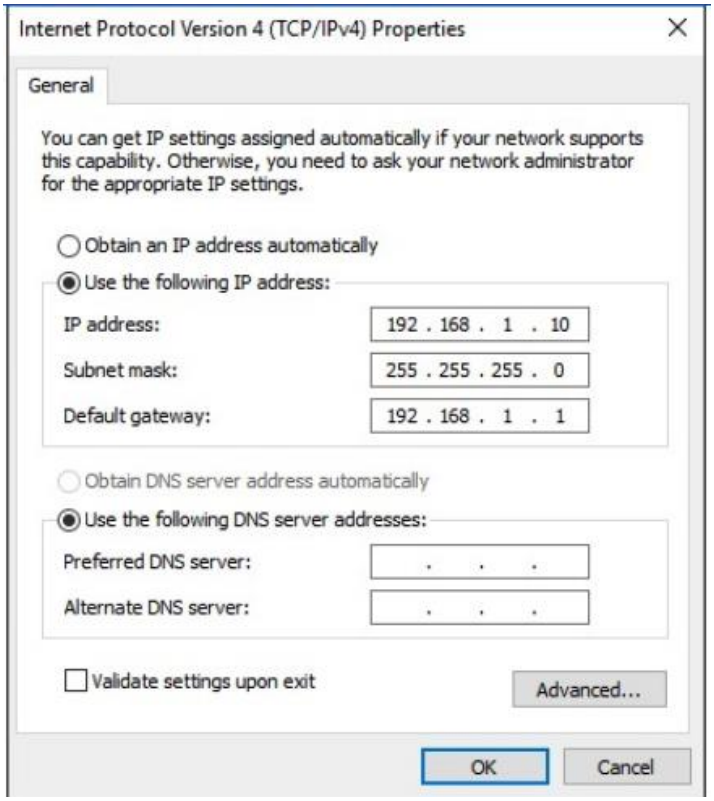


Figura 14. Configuración manual IP en un dispositivo final.

Fuente: Cisco Networking Academy (2022)

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

3.2.- Configuración automática de direcciones IP para dispositivos finales

Los dispositivos finales suelen usar DHCP de manera predeterminada para la configuración automática de la dirección IPv4. DHCP es una tecnología que se utiliza en casi todas las redes. Para comprender mejor por qué DHCP es tan popular, se debe considerar todo el trabajo adicional que habría que realizar sin este protocolo.

En una red, DHCP habilita la configuración automática de direcciones IPv4 para cada dispositivo final habilitado para DHCP. Imagina la cantidad de tiempo que llevaría si cada vez que te conectara a la red tuvieras que introducir manualmente la dirección IPv4, la máscara de subred, el gateway predeterminado y el servidor DNS. Multiplica eso por cada usuario y cada uno de los dispositivos en una organización y te darás 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 9, para configurar DHCP en una PC con Windows, solo necesitas seleccionar Obtain an IP address automatically y Obtain DNS server address automatically. Tu PC buscará un servidor DHCP y se le asignarán los ajustes de dirección necesarios para comunicarse en la red.

Nota: IPv6 utiliza DHCPv6 y SLAAC (configuración automática de direcciones sin estado) para la asignación dinámica de direcciones.

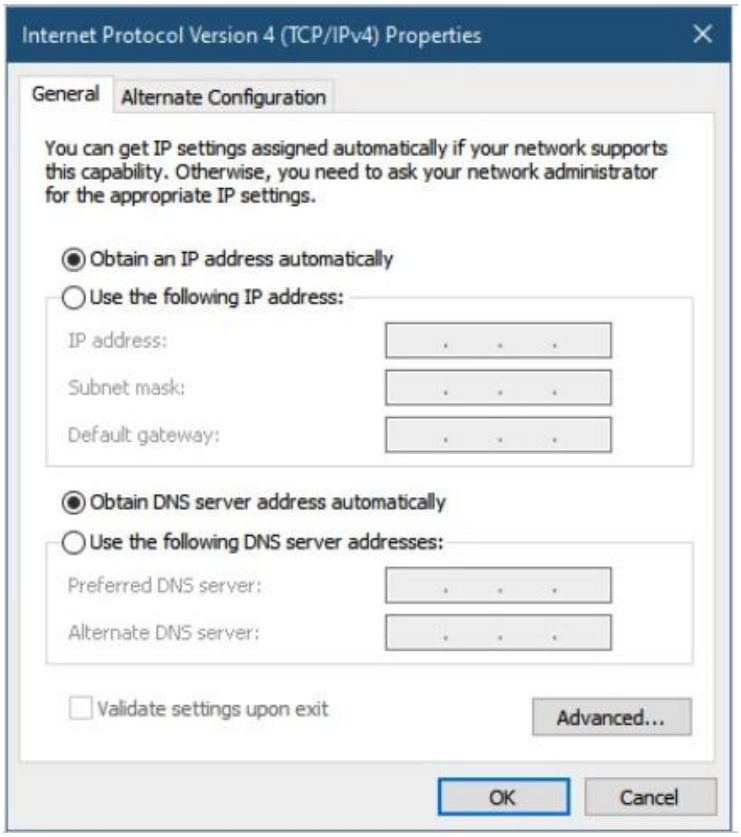


Figura 15. Configuración dinámica IP en un dispositivo final.

Fuente: Cisco Networking Academy (2022)

4. Definiciones de VLAN

Para organizar tu red en redes más pequeñas no es tan simple como separar tornillos y ponerlos en frascos. Pero hará que la red sea más fácil de administrar. Dentro de una red conmutada, las Redes de Área Local Virtuales (VLAN) proporcionan la segmentación y la flexibilidad organizativa. Un grupo de dispositivos dentro de una VLAN se comunica como si cada dispositivo estuviera conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Como se muestra en la figura 16, las VLAN en una red conmutada permiten a los usuarios de varios departamentos (por ejemplo, TI, recursos humanos y ventas) conectarse a la misma red, independientemente del switch físico que se esté utilizando o de la ubicación en una LAN del campus.

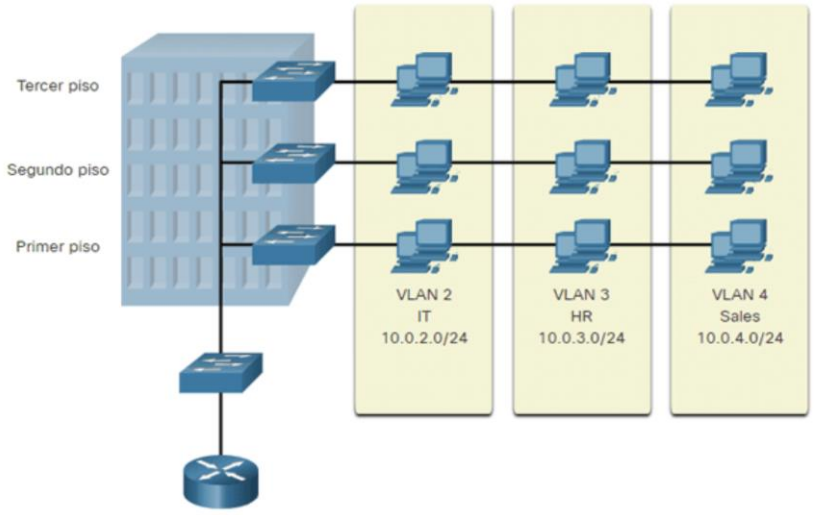


Figura 16. Ejemplo de VLAN en una empresa.
Fuente: Cisco Networking Academy (2022)

Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Cada VLAN se considera una red lógica diferente. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN. Cualquier puerto de switch puede pertenecer a una VLAN.

Los paquetes de unidifusión, difusión y multidifusión se reenvían solamente a terminales dentro de la VLAN donde los paquetes son de origen. Los paquetes destinados a dispositivos que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing.

Varias subredes IP pueden existir en una red conmutada, sin el uso de varias VLAN. Sin embargo, los dispositivos estarán en el mismo dominio de difusión de capa 2. Esto significa que todas las difusiones de capa 2, tales como una solicitud de ARP, serán recibidas por todos los dispositivos de la red conmutada, incluso por aquellos que no se quiere que reciban la difusión.

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben.

Mediante las VLAN, los administradores de red pueden implementar políticas de acceso y seguridad de acuerdo con a grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).

4.1.- 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 Interfaz Virtual de Switch (SVI). Para configurar una SVI en un switch, utiliza el comando de interface vlan 1 configuración global. La Vlan 1 no es una interfaz física real, sino una virtual. A continuación, asigna una dirección IPv4 mediante el comando ip address ip-address subnet-mask de la configuración de interfaz. Finalmente, habilita la interfaz virtual utilizando el comando de no shutdown configuración de la interfaz.

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

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# interface vlan 1
Sw-Floor-1(config-if)# ip address 192.168.1.20 255.255.255.0
Sw-Floor-1(config-if)# no shutdown
Sw-Floor-1(config-if)# exit
Sw-Floor-1(config)# ip default-gateway 192.168.1.1
```

Figura 17. no shutdown.

Fuente: Cisco Networking Academy (2022)

4.2.- Asignación de direcciones de dispositivo

Dentro de una red, hay diferentes tipos de dispositivos que requieren direcciones:

- **Clientes usuarios finales:** la mayoría de las redes asignan direcciones de manera dinámica con el protocolo de configuración dinámica de host (DHCP). Esto reduce la carga sobre el personal de soporte de red y elimina de manera virtual los errores de entrada. Con DHCP, las direcciones sólo se alquilan durante un período de tiempo y se pueden reutilizar cuando caduque la concesión. Esta es una característica importante para las redes que admiten usuarios transitorios y dispositivos inalámbricos. Cambiar el esquema de subredes significa que el servidor DHCP necesita ser reconfigurado y los clientes deben renovar sus direcciones IPv4. Los clientes IPv6 pueden obtener información de dirección mediante DHCPv6 o SLAAC.
- **Servidores y periféricos:** deben tener una dirección IP estática predecible. Se debe utilizar un sistema de numeración coherente para estos dispositivos.
- **Servidores a los que se puede acceder desde Internet:** los servidores que deben estar disponibles públicamente en Internet deben tener una dirección IPv4 pública, a la que se accede con mayor frecuencia mediante NAT. En algunas organizaciones, los servidores internos (no disponibles públicamente) deben ponerse a disposición de los usuarios remotos. En la mayoría de los casos, a estos servidores se les asignan direcciones privadas internamente y se requiere que el usuario cree una conexión de red privada virtual (VPN) para acceder al servidor. Esto tiene el mismo efecto que si el usuario accede al servidor desde un host dentro de la intranet.

- **Dispositivos intermediarios:** estos dispositivos tienen direcciones asignadas para la administración, monitoreo y seguridad de la red. Debido a que es necesario saber cómo comunicarse con dispositivos intermediarios, estos deben tener asignadas direcciones predecibles y estáticas.
- **Puerta de enlace:** los routeres y los dispositivos de firewall tienen una dirección IP asignada a cada interfaz que sirve como puerta de enlace para los hosts en esa red. Normalmente, la interfaz de router utiliza la dirección más baja o más alta de la red.

Al desarrollar un esquema de direccionamiento IP, generalmente se recomienda que tenga un patrón establecido de cómo se asignan las direcciones a cada tipo de dispositivo. Esto beneficia a los administradores a la hora de agregar y quitar dispositivos, ya que filtra el tráfico basado en IP, y también simplifica el registro.

5. ¿Cómo interactúan los clientes y los servidores?

Diariamente utilizamos los servicios disponibles en las redes y en Internet para comunicarnos con otras personas y realizar tareas de rutina. Pocas veces pensamos en los servidores, clientes y dispositivos de networking necesarios para poder recibir un correo electrónico, actualizar nuestro estado en los medios sociales o buscar las mejores ofertas en una tienda en línea. La mayoría de las aplicaciones de Internet más comunes se basa en interacciones complejas entre diversos servidores y clientes.

El término servidor, hace referencia a un host que ejecuta una aplicación de software que proporciona información o servicios a otros hosts conectados a la red. Un ejemplo conocido de dicha aplicación es un servidor Web. Hay millones de servidores conectados a Internet que proporcionan servicios como sitios web, correo electrónico, transacciones financieras, descargas de música, etc. Un factor fundamental para permitir el funcionamiento de estas interacciones complejas es que todos emplean estándares y protocolos acordados.

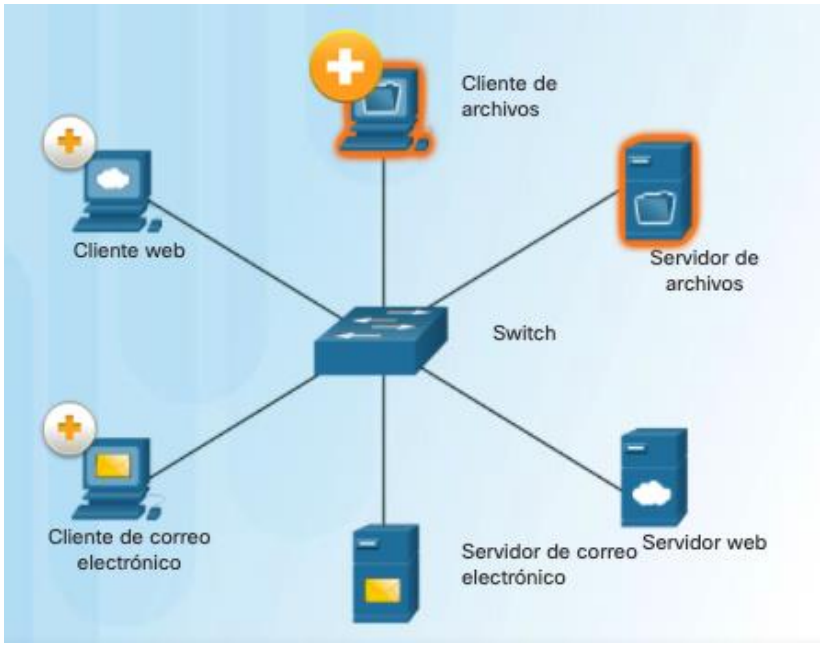


Figura 18. Servicios y clientes.

Fuente: Cisco Networking Academy (2022)

5.1.- Servicios de Internet comunes

¿Cuáles son los servicios de Internet más comunes que utiliza periódicamente?

Para la mayoría de las personas, la lista incluye servicios como búsquedas en Internet, sitios de medios sociales, transmisión de vídeo y audio, sitios de compras en línea, correo electrónico y mensajería. Cada uno de estos servicios depende de los protocolos de la suite de protocolos TCP/IP para poder transmitir de manera confiable la información entre los clientes y los servidores.

Algunos de los protocolos que se usan para los servicios de Internet son:

- **Sistema de nombres de dominio (DNS):** resuelve nombres de Internet en direcciones IP.

- **Secure Shell (SSH):** se utiliza para proporcionar acceso remoto a servidores y dispositivos de red.
- **Protocolo simple de transferencia de correo (SMTP):** envía mensajes de correo electrónico y archivos adjuntos de clientes a servidores y de los servidores a otros servidores de correo electrónico.
- **Protocolo de oficina de correos (POP):** lo utilizan los clientes de correo electrónico para recuperar el correo electrónico y los adjuntos de un servidor remoto.
- **Protocolo de acceso a mensajes de Internet (IMAP):** lo utilizan los clientes de correo electrónico para recuperar el correo electrónico y los adjuntos de un servidor remoto.
- **Protocolo de configuración dinámica de hosts (DHCP):** se utiliza para configurar dispositivos automáticamente con asignación de direcciones IP y otros datos necesarios para que puedan comunicarse por Internet.
- **Servidor web:** transfiere los archivos que conforman las páginas web de la Red informática mundial mediante el Protocolo de transferencia de hipertexto (HTTP).
- **Protocolo de transferencia de archivos (FTP):** se utiliza para la transferencia interactiva de archivos entre sistemas.

Si bien es necesario utilizar una dirección IP para enviar y recibir mensajes por Internet, DHCP no es la única forma en la que puede asignarse una dirección IP. Las direcciones IP pueden configurarse estáticamente en un dispositivo.

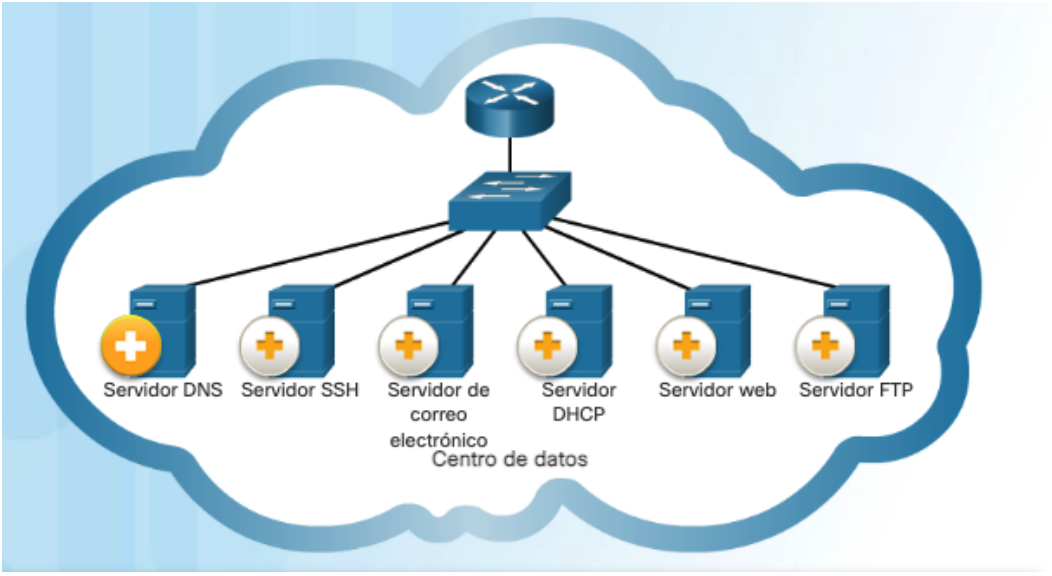


Figura 19. Centro de Datos de Servicios.

Fuente: Cisco Networking Academy (2022)

6. Tipos de redes inalámbricas

Las LAN inalámbricas (WLAN) se basan en los estándares IEEE y se pueden clasificar en cuatro tipos principales: WPAN, WLAN, WMAN y WWAN.

WPAN	Redes inalámbricas de área personal (WPAN) - Utiliza transmisores de baja potencia para una red de corto alcance, generalmente de 20 a 30 pies (6 a 9 metros). Los dispositivos basados en Bluetooth y ZigBee se usan comúnmente en WPANs. Los WPAN se basan en el estándar 802.15 y una frecuencia de radio de 2.4 GHz.
WLAN	Redes LAN Inalámbricas (WLAN) - Utiliza transmisores para cubrir una red de tamaño mediano, generalmente de hasta 300 pies. Las redes WLANs son adecuadas para uso en casas, oficinas, e inclusive campus. Las WLAN se basan en el estándar 802.11 y una frecuencia de radio de 2,4 GHz o 5 GHz.
WMAN	Redes MAN inalámbricos (WMAN) - Utiliza transmisores para proporcionar servicio inalámbrico en un área geográfica más grande. Las redes WMANs son adecuadas para proveer acceso inalámbrico a ciudades metropolitanas o distritos específicos. Las WMANs utilizan frecuencias específicas con licencia.
WWAN	Redes inalámbricas de área amplia (WWAN) - Utiliza transmisores para proporcionar cobertura en un área geográfica extensa. Las redes WWANs son adecuadas para comunicaciones nacionales y globales. Las WMANs utilizan frecuencias específicas con licencia.

Tabla 3. Tipos de redes inalámbricas.

Fuente: Cisco Networking Academy (2022)

6.1.- Componentes de la WLAN

6.1.1. NIC inalámbrica

Las implementaciones inalámbricas requieren un mínimo de dos dispositivos que tengan un transmisor de radio y un receptor de radio sintonizados a las mismas frecuencias de radio:

- Dispositivos finales con NIC inalámbricas.
- Un dispositivo de red, como un router inalámbrico o un AP inalámbrico.

Para comunicarse de forma inalámbrica, las computadoras portátiles, tabletas, teléfonos inteligentes e incluso los últimos automóviles incluyen NIC inalámbricas integradas que incorporan un transmisor / receptor de radio. Si un dispositivo no tiene una NIC inalámbrica integrada, se puede utilizar un adaptador inalámbrico USB, como se muestra en la figura.

Nota: muchos dispositivos inalámbricos con los que está familiarizado no tienen antenas visibles. Están integrados dentro de teléfonos inteligentes, computadoras portátiles y routers domésticos inalámbricos.

6.1.2. Adaptador inalámbrico USB

Figura 20. Adaptador inalámbrico.

Fuente: Cisco Networking Academy (2022)

6.1.3. Router de hogar inalámbrico

El tipo de dispositivo de infraestructura con el que se asocia y autentica un dispositivo final varía según el tamaño y los requisitos de la WLAN.

Un usuario doméstico generalmente interconecta dispositivos inalámbricos utilizando un pequeño router inalámbrico. El enrutador inalámbrico sirve como:

- **Punto de acceso -** Esto proporciona acceso inalámbrico 802.11a/b/g/n/ac
- **Switch -** Esto proporciona un switch Ethernet 10/100/1000 dúplex completo de cuatro puertos para interconectar dispositivos cableados.
- **Router -** Esto proporciona una puerta de enlace predeterminada para conectarse a otras infraestructuras de red, como Internet.

Figura 21. Router de hogar inalámbrico.
Fuente: Cisco Networking Academy (2022)

Un router inalámbrico se implementa comúnmente como una pequeña empresa o dispositivo de acceso inalámbrico residencial. El router inalámbrico anuncia sus servicios inalámbricos mediante el envío de beacons que contienen su identificador de conjunto de servicios compartidos (SSID). Los dispositivos descubren de forma inalámbrica el SSID e intentan asociarse y autenticarse con él para acceder a la red local y el Internet.

La mayoría de los routers inalámbricos también ofrecen funciones avanzadas, como acceso de alta velocidad, soporte para transmisión de video, direccionamiento IPv6, calidad de servicio (QoS), utilidades de configuración y puertos USB para conectar impresoras o unidades portátiles.

Además, los usuarios domésticos que desean ampliar sus servicios de red pueden implementar extensores de alcance Wi-Fi. Un dispositivo puede conectarse de forma inalámbrica al extensor, lo que aumenta sus comunicaciones para que se repitan al router inalámbrico.

6.1.4. Puntos de acceso inalámbrico

Si bien los extensores de alcance son fáciles de configurar, la mejor solución sería instalar otro punto de acceso inalámbrico para proporcionar acceso inalámbrico dedicado a los dispositivos del usuario. Los clientes inalámbricos usan su NIC inalámbrica para descubrir puntos de acceso cercanos compartiendo el SSID Los clientes luego intentan asociarse y autenticarse con un AP. Después de ser autenticados los usuarios inalámbricos tienen acceso a los recursos de la red.

Figura 22. Punto de acceso inalámbrico.

Fuente: Cisco Networking Academy (2022)

6.2.- Configuración de WLAN del sitio remoto

6.2.1. Router inalámbrico

Los trabajadores remotos, las oficinas pequeñas y las redes caseras, comúnmente usan routers de casa y oficina pequeña. A estos routers en ocasiones se les llama routers integrados porque típicamente incluyen un switch para dispositivos conectados por cable, un puerto para conectarse al Internet (a veces llamado "WAN"), y componentes inalámbricos para clientes de acceso inalámbrico, como se muestra en la figura del Cisco Meraki MX64W. En lo que resta de este módulo, a los routers de casas y oficinas pequeñas los llamaremos routers inalámbricos.

La figura muestra la parte de atrás de un router de casa o pequeña oficina. El router tiene dos antenas, una de cada lado. En el lado izquierdo, hay un botón de reset. Al lado del botón de reset hay cuatro puertos para conectar dispositivos LAN. Hay un puerto para la conexión WAN y finalmente el botón de encendido y el puerto para el cable de energía.

Figura 23. Cisco Meraki MX64W.
Fuente: Cisco Networking Academy (2022)

Estos routers inalámbricos comúnmente proveen seguridad WLAN, servicios de DHCP, Traducción de Direcciones de Red (NAT), Quality of Service (QoS), y una variedad de otras funciones. El conjunto de características varía de acuerdo al modelo del router.

Nota: La configuración del módem por cable o DSL generalmente se realiza, a través, del representante del proveedor de servicios, ya sea en el sitio o de manera remota, a través de un tutorial contigo en el teléfono. Si compras el módem, el mismo vendrá con la documentación sobre cómo conectarlo a tu proveedor de servicios, lo que muy probablemente incluirá el contacto con tu proveedor de servicios para obtener más información.

6.2.2. Conéctese al router inalámbrico

La mayoría de los routers inalámbricos están listos para utilizarse desde el primer momento. Están preconfigurados para conectarse a la red y proporcionar servicios. Por ejemplo, el router inalámbrico utiliza el DHCP para proporcionar automáticamente información de asignación de direcciones a los dispositivos conectados. Sin embargo, las direcciones IP predeterminadas del router inalámbrico, los nombres de usuario y las contraseñas se pueden encontrar fácilmente en Internet.

Simplemente ingresa la frase "dirección IP predeterminada del router inalámbrico" o "contraseñas predeterminada del router inalámbrico " para ver un listado de muchos sitios web que proporcionan esta información. Por ejemplo, el usuario y la contraseña para el router inalámbrico en la figura es "admin". En consecuencia, su prioridad principal debe ser cambiar estos valores predeterminados por razones de seguridad.

Para obtener acceso a la GUI de configuración del router inalámbrico, abra un navegador web. En el campo Dirección, ingresa la dirección IP privada predeterminada de su router inalámbrico. La dirección IP predeterminada se puede encontrar en la documentación que viene con el router inalámbrico o se puede buscar en Internet. La figura 24 muestra la dirección IPv4 192.168.0.1, que es un valor predeterminado común para muchos fabricantes.

Una ventana de seguridad solicita autorización para acceder a la GUI del router. La palabra admin se utiliza comúnmente como nombre de usuario y contraseña predeterminados. Nuevamente, consulta la documentación del router inalámbrico o busca en Internet.

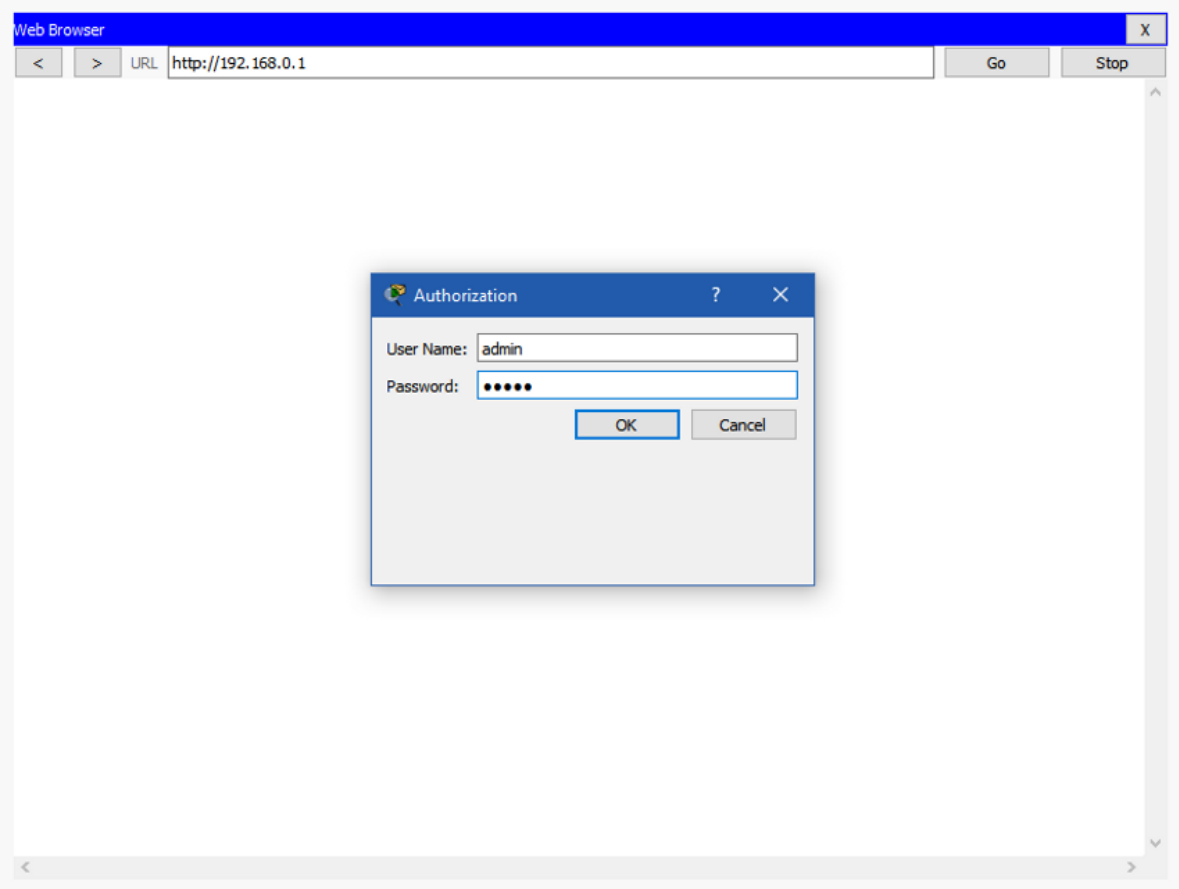


Figura 24. Acceso al router inalámbrico vía web.

Fuente: Cisco Networking Academy (2022)

6.2.3. Configuración básica de red

La configuración básica de la red incluye los siguientes pasos:

1. Iniciar sesión en el router desde un navegador web.
2. Cambiar la contraseña de administrador predeterminada.
3. Iniciar sesión con la nueva contraseña administrativa.
4. Cambiar las direcciones IPv4 predeterminadas del DHCP.
5. Renovar la dirección IP.
6. Iniciar sesión en el router con la nueva dirección IP.

6.2.3. Configuración inalámbrica

La configuración básica de la red inalámbrica incluye los siguientes pasos:

1. Ver los valores predeterminados de WLAN
2. Cambiar el modo de red.
3. Configurar el SSID
4. Configurar el canal
5. Configurar el modo de seguridad
6. Configurar la contraseña.

6.2.4. Configuración de una red de Malla inalámbrica

En una red de una oficina pequeña o doméstica, un router inalámbrico puede bastar para proporcionar acceso inalámbrico a todos los clientes. Sin embargo, si deseas extender el rango más allá de aproximadamente 45 metros en el interior y 90 metros en el exterior, puede agregar puntos de acceso inalámbricos. Como se muestra en la figura 25, en el red de malla Inalámbrica, dos puntos de acceso se configuran con las mismas configuraciones de WLAN de nuestro ejemplo anterior. Observa que los canales escogidos son 1 y 11, de

modo tal que los puntos de acceso no interfieren con el canal 6 configurado previamente en el router inalámbrico.

Las imágenes 25 y 26, muestran dos puntos de acceso inalámbricos en una red de oficina pequeña o casa. Los puntos de acceso inalámbrico se conectan de manera inalámbrica a un router. El router inalámbrico está conectado a un módem de banda ancha. El módem de banda ancha está conectado a una nube mostrando el Internet. Hay flechas apuntando desde el punto de acceso inalámbrico que muestra los ajustes de configuración. Un punto de acceso inalámbrico está en el canal 1 en 2.4GHz y el otro en el canal 11 en 2.4GHz.

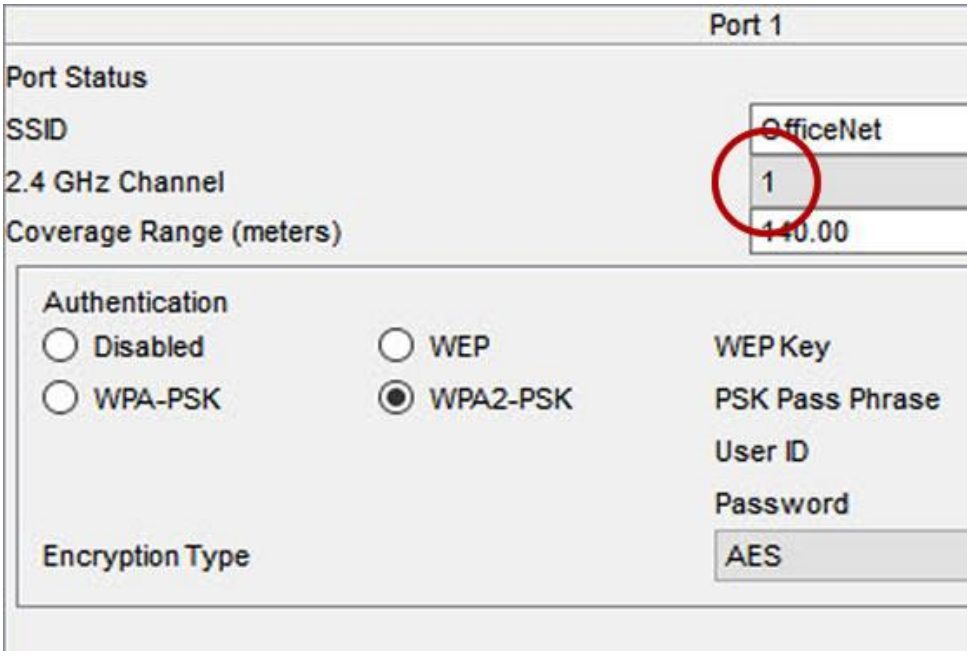


Figura 25. Canal 1 en un punto de acceso inalámbrico.

Fuente: Cisco Networking Academy (2022)

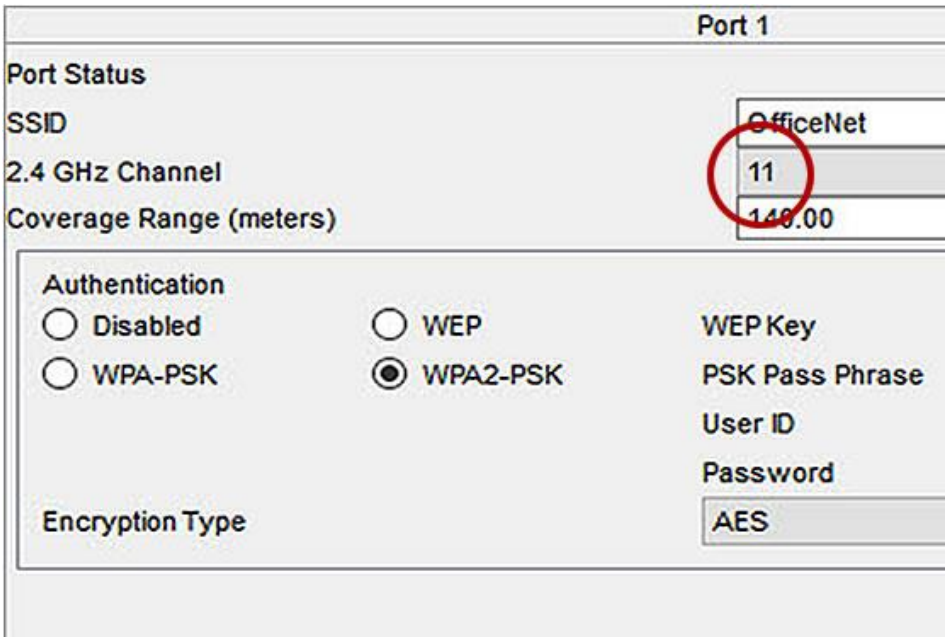


Figura 26. Canal 11 en un punto de acceso inalámbrico.

Fuente: Cisco Networking Academy (2022)

Protocolo

Extender una WLAN en una oficina pequeña o en el hogar se vuelve cada vez más fácil. Los fabricantes han creado una red de Malla Inalámbrica (WMN) a través de aplicaciones de teléfono inteligente. Al compra el sistema, dispersas los puntos de acceso, los conectas, descargas la aplicación y configuras su WMN en pocos pasos. Para encontrar las reseñas de las ofertas actuales, busca en Internet "el mejor sistema de red de Malla Inalámbrica"

6.3.- NAT para IPv4

En un router inalámbrico, si busca una página como la página de estado que se muestra en la figura 27, encontrarás la información de la asignación de direcciones IPv4 que el router utiliza para enviar datos a Internet. Observa que la dirección IPv4 es 209.165.201.11 es una red diferente a la dirección 10.10.10.1 asignada a la interfaz LAN del router. A todos los dispositivos en la LAN del router se les asignarán direcciones con el prefijo 10.10.10.

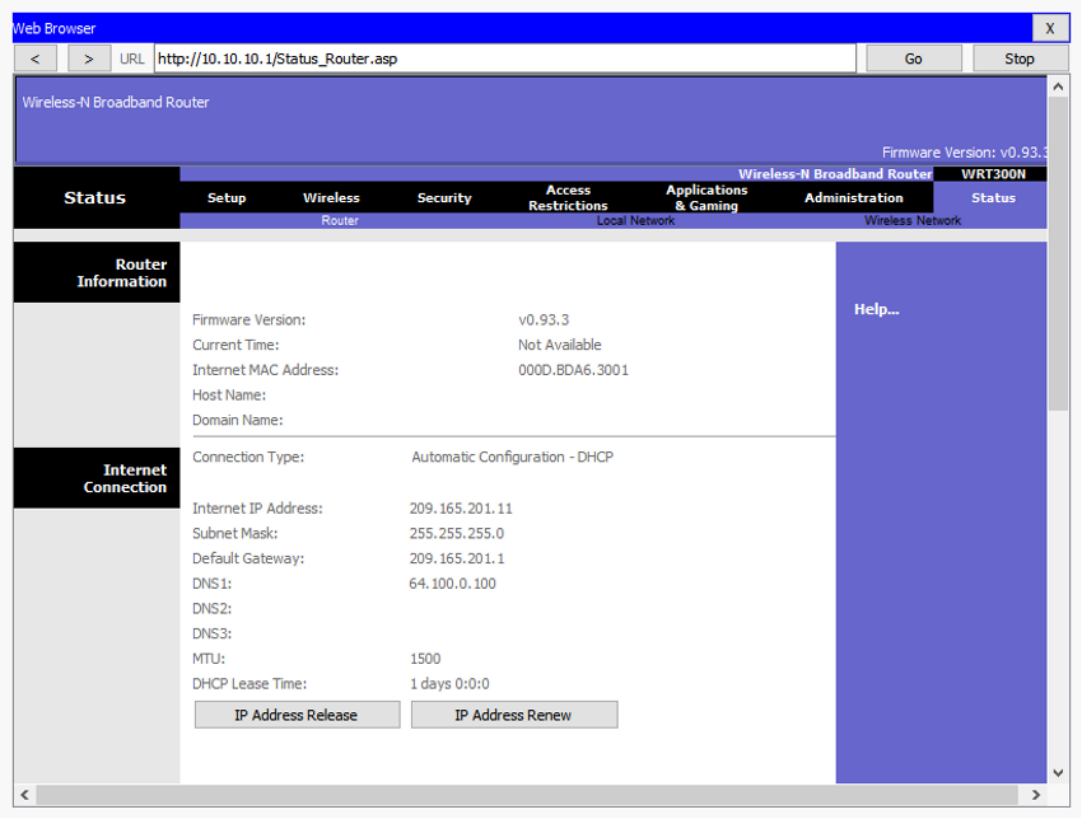


Figura 27. Asignación de direcciones IPv4.

Fuente: Cisco Networking Academy (2022)

La dirección IPv4 209.165.201.11 es públicamente enrutable en Internet. Cualquier dirección con el 10 en el primer octeto es una dirección IPv4 privada y no se puede enrutar en Internet. Por lo tanto, el router utilizará un proceso llamado Traducción de Direcciones de Red (NAT) para convertir las direcciones IPv4 privadas en direcciones IPv4 enrutables en Internet. Con NAT, una dirección IPv4 privada de origen (local) se traduce a una dirección pública (global). En el caso de los paquetes entrantes, el proceso es inverso. Por medio de NAT, el router puede traducir muchas direcciones IPv4 internas en direcciones públicas.

Algunos ISP utilizan la asignación de direcciones privadas para conectarse a los dispositivos del cliente. Sin embargo, al final, su tráfico abandonará la red del proveedor y se enrutará en Internet. Para ver las direcciones IP de sus dispositivos, busca "Cuál es mi dirección IP" en Internet. Haz esto para otros dispositivos en la misma red y verás que todos comparten la misma dirección IPv4 pública. NAT hace esto posible realizando un rastreo de los números de puerto de origen para cada sesión establecida por dispositivo. Si tu ISP tiene la IPv6 habilitada, verás una dirección IPv6 única para cada dispositivo.

Ideas Clave

Hoy en día, una red física está compuesta principalmente con uno o más switches. Estos dispositivos regulan el tráfico de datos entre los computadores, teléfonos, servidores y todo equipo que está conectado a una red. Todos los cables de red están conectados al switch y hacen posible la comunicación entre los diferentes dispositivos terminales. En la actualidad, los switches son capaces de conectar cientos de dispositivos que, a su vez, pueden comunicarse sin que se produzcan problemas. Sin embargo, a veces resulta útil poder segmentar o dividir estas redes tan grandes, sin tener que realizar cambios en la instalación física.

Una red de área local virtual (Virtual Local Area Network o VLAN) es un segmento lógico más pequeño, dentro de una gran red física cableada. Los diferentes terminales se combinan en una solución de red independiente de su ubicación: siempre que estén conectadas entre sí en la misma LAN, es posible asociarlas a través de una VLAN. Esto no genera problemas para que la LAN contenga varios switches. Lo más importante es que el switch también sea compatible con la VLAN. La única manera de crear VLAN es utilizando switches gestionables (Managed Switches).

Conclusiones

Las LANS virtuales (VLANs) es un grupo de dispositivos dentro de una VLAN que puede comunicarse con cada dispositivo como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. Los administradores utilizan VLAN para segmentar redes en función de factores como la función, el equipo o la aplicación. Cada VLAN se considera una red lógica diferente. Cualquier puerto de switch puede pertenecer a una VLAN. Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Cada VLAN de una red conmutada corresponde a una red IP; por lo tanto, el diseño de VLAN debe utilizar un esquema jerárquico de direccionamiento de red. Los tipos de VLAN incluyen la VLAN predeterminada, las VLAN de datos, la VLAN nativa, las VLAN de administración. y las VLAN de voz.

Los diferentes switches catalyst de Cisco soportan varias cantidades de VLAN, incluidas las VLAN de rango normal y las VLAN de rango extendido. Al configurar redes VLAN de rango normal, los detalles de configuración se almacenan en la memoria flash del switch en un archivo denominado vlan.dat. Aunque no es necesario, se recomienda guardar los cambios de configuración en ejecución en la configuración de inicio. Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Hay muchos comandos para definir un puerto como puerto de acceso y asignarlo a una VLAN. Las VLAN se configuran en el puerto del switch y no en el terminal. Un puerto de acceso puede pertenecer a sólo una VLAN por vez. Sin embargo un puerto puede también estar asociado a una VLAN de voz. Por ejemplo, un puerto conectado a un teléfono IP y un dispositivo final se asociaría con dos

VLAN: una para voz y otra para datos. Una vez que se configura una VLAN, se puede validar la configuración con los comandos **show** de IOS de Cisco, si el puerto de acceso del switch se ha asignado incorrectamente a una VLAN, simplemente vuelva a ingresar el comando **switchport access vlan** *vlan-id* interface configuration con el ID de VLAN correcto. El comando de modo de configuración gloabl **no vlan** *vlan-id* se usa para remover una VLAN desde el archivo del switch vl vlan.dat.

Para comunicarse de forma inalámbrica, la mayoría de los dispositivos incluyen NIC inalámbricas integradas que incorporan un transmisor / receptor de radio. El router inalámbrico sirve como un punto de acceso, un switch, y un router. Los clientes inalámbricos usan su NIC inalámbrica para descubrir puntos de acceso cercanos compartiendo el SSID Los clientes luego intentan asociarse y autenticarse con un AP. Después de ser autenticados los usuarios inalámbricos tienen acceso a los recursos de la red. Los AP se pueden clasificar como AP autónomos o AP basados en controladores.

El estándar 802.11 identifica dos modos principales de topología inalámbrica: modo Ad hoc y modo Infraestructura. El anclaje a red es usado para proveer un acceso inalámbrico rápido. El modo de infraestructura define dos bloques de construcción de topología: un conjunto de servicios básicos (BSS) y un conjunto de servicios extendidos (ESS). Todas las tramas 802.11 contienen los siguientes campos: control de frame, duración, dirección 1, dirección 2, dirección 3, control de secuencia y dirección 4. WLANs usan CSMA/CA como el método para determinar cómo y cuándo enviar datos en la red. Una parte importante del proceso 802.11 es descubrir una WLAN y conectarse a esta. Los dispositivos inalámbricos descubren un AP inalámbrico, se autentican con él y luego se asocian con él. Los clientes inalámbricos se conectan al AP mediante un proceso de exploración (sondeo) pasivo o activo.

Las redes inalámbricas son susceptibles a amenazas, que incluyen: interceptación de datos, intrusos inalámbricos, ataques DoS y puntos de acceso no autorizados. Los ataques DoS inalámbricos pueden ser el resultado de: dispositivos mal configurados, un usuario malintencionado que interfiere intencionalmente con la comunicación inalámbrica e interferencia accidental. Un AP falso es un AP o un router inalámbrico que se ha conectado a una red corporativa sin autorización explícita y en contra de la política corporativa. Una vez conectado, el atacante puede ser utilizado por un atacante para capturar direcciones MAC, capturar paquetes de datos, obtener acceso a recursos de red o lanzar un ataque de hombre en el medio. Ataque man-in-the-middle: el agente de amenaza se coloca entre dos entidades legítimas para leer, modificar o redirigir los datos que se transmiten entre las dos partes. Un ataque de "AP gemelo malvado" es un ataque MITM inalámbrico popular en el que un atacante introduce un AP falso y lo configura con el mismo SSID que un AP legítimo Para evitar la instalación de puntos de acceso no autorizados, las organizaciones deben configurar WLC con políticas de puntos de acceso no autorizados.

Referencias bibliográficas

CCNAv7 (2022) Introduction to Networks. Capítulo 2: Configuración básica de switches y terminals

CCNAv7 (2022) Networking Essentials. Capítulo 5 – Prestación de servicios de Red

CCNAv7(2022) Switching, Routing, and Wireless Essentials Capítulo 13. Configuraciones de redes inalámbricas WLAN

Freepik (s. f.-a) Empresario señalando su presentación en la pantalla digital futurista [imagen portada] Recuperado 18 de marzo de 2022, de https://www.freepik.com/free-photo/businessman-pointing-his-presentation-futuristic-digital-screen_15556741.htm

Home. (2017, December 22). Networking Academy. http://www.netacad.com

Premium Photo. (s. f.-b). Freepik. Recuperado 25 de marzo de 2022, de http://www.freepik.com/premium-photo/ cerrar mano elegir muchos cable de red lan_17944107.htm