



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

FORMANDO PROFESIONALES DE ÉLITE



FUNDAMENTOS DE REDES

CLASE 3

Ing. ANDRÉS PÉREZ





INTRODUCCIÓN A LA CLASE

1. Retroalimentación
2. Indicaciones generales
3. Objetivos de la clase



ITSQMET
INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

RETROALIMENTACIÓN

FORMANDO PROFESIONALES DE ÉLITE



Objetivos de la clase:

1. Realizar una conceptualización de los principales conceptos de seguridad de red y primeros comandos de configuración de dispositivos.



ÍNDICE

UNIDAD II: PROTOCOLOS Y MODELOS DE RED

- **Seguridad de la red** →
- **Configuración de switch en Packet Tracer.** →
- **Modos de usuario,** →
- **Modos de usuario, privilegiado en switch cisco.** →
- **Configuración de contraseña en las líneas de comandos** →



TENDENCIAS DE RED





TENDENCIAS RECIENTES



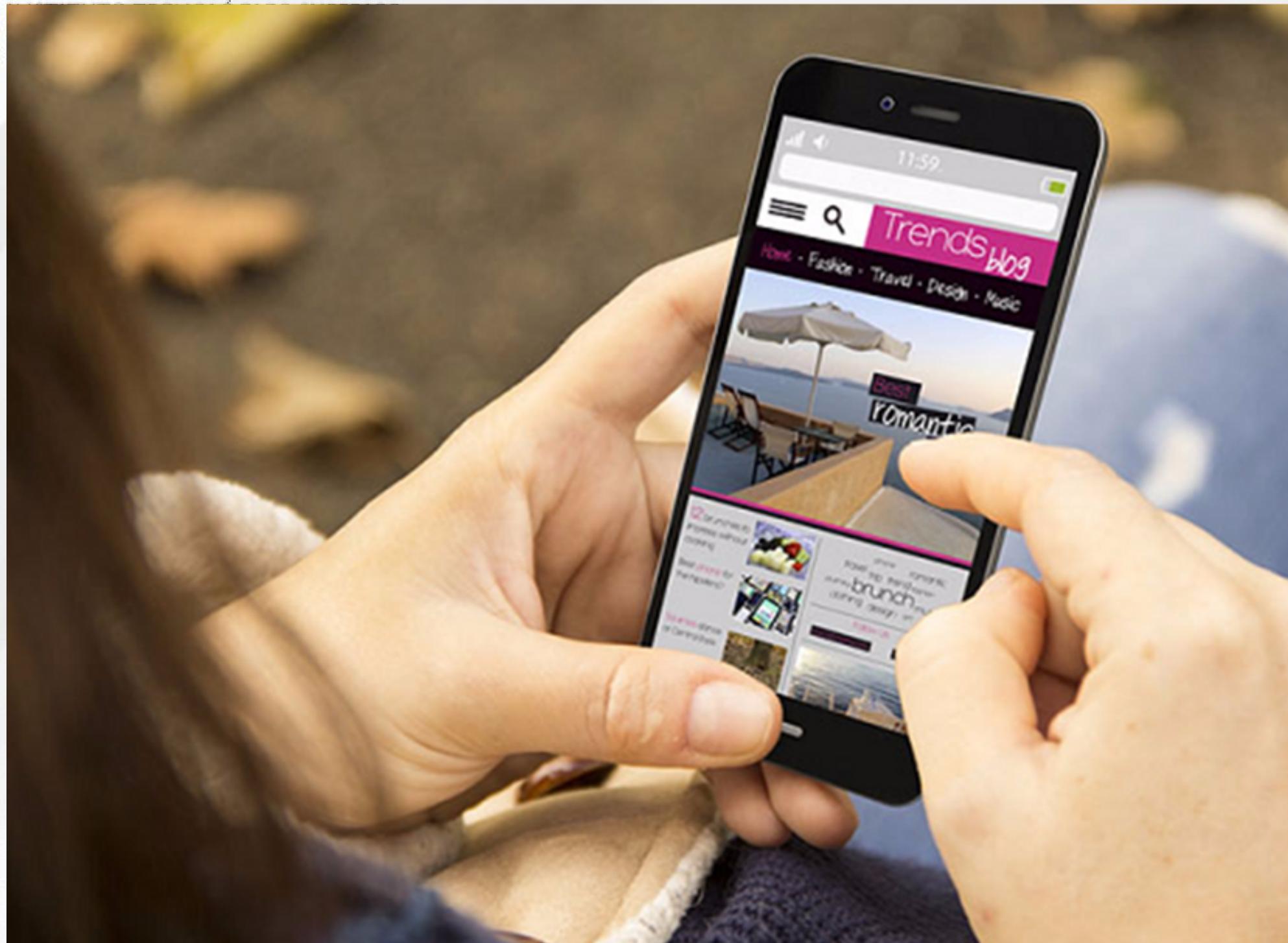
La función de la red se debe ajustar y transformar continuamente para poder mantenerse al día con las nuevas tecnologías y los nuevos dispositivos para usuarios finales, ya que se lanzan al mercado de manera constante.

Muchas nuevas tendencias de red que afectarán a organizaciones y consumidores:

- Traiga su propio dispositivo (BYOD)
- Colaboración en línea
- Comunicaciones de video
- Computación en la nube



TENDENCIAS RECIENTES

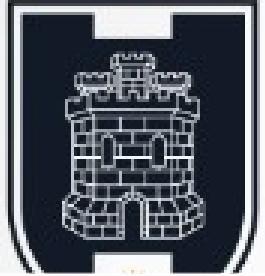


Trae tu propio dispositivo (BYOD) permite a los usuarios usar sus propios dispositivos, dándoles más oportunidades y una mayor flexibilidad.

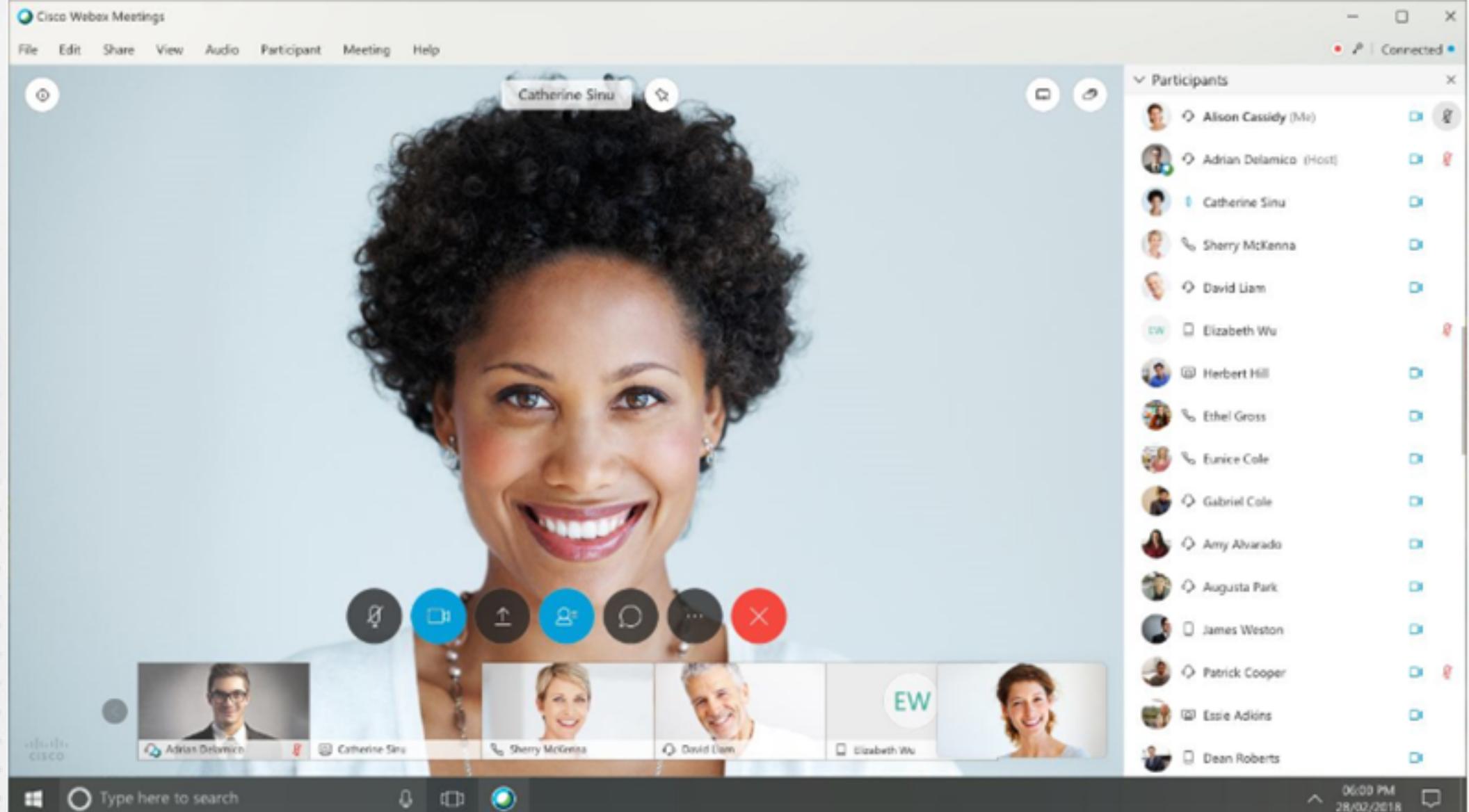
BYOD permite a los usuarios finales tener la libertad de utilizar herramientas personales para comunicarse y acceder a información mediante los siguientes dispositivos:

- Computadoras portátiles
- Netbooks
- Tablets
- Smartphones
- Lectores de libros electrónicos

BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar.



COLABORACIÓN EN LÍNEA



- Colaborar y trabajar con otros a través de la red en proyectos conjuntos.
- Las herramientas de colaboración, incluido Cisco WebEx (que se muestra en la figura), brindan a los usuarios una forma de conectarse e interactuar instantáneamente.
- La colaboración es una prioridad muy alta para las empresas y en la educación.
- Cisco Webex Teams es una herramienta de colaboración multifuncional.
 - Enviar mensajes instantáneos
 - Publicar imágenes
 - Publicar videos y enlaces



COMUNICACIÓN POR VIDEO

- Las videollamadas se realizan a cualquier persona, independientemente de dónde se encuentren.
- La videoconferencia es una herramienta poderosa para comunicarse con otros.
- El vídeo se está convirtiendo en un requisito crítico para una colaboración eficaz.
- Los poderes de Cisco TelePresence son una forma de trabajar donde todos, en todas partes.



COMPUTACIÓN EN LA NUBE

La computación en la nube nos permite almacenar archivos personales o respaldar nuestros datos en servidores a través de Internet.

- También se puede acceder a las aplicaciones mediante la nube.
- Permite a las empresas entregar a cualquier dispositivo en cualquier parte del mundo.

La computación en la nube es posible gracias a los centros de datos.

- Las empresas más pequeñas que no pueden costear sus propios centros de datos, arriendan servicios de servidores y almacenamiento de organizaciones con centro de datos más grandes en la nube.



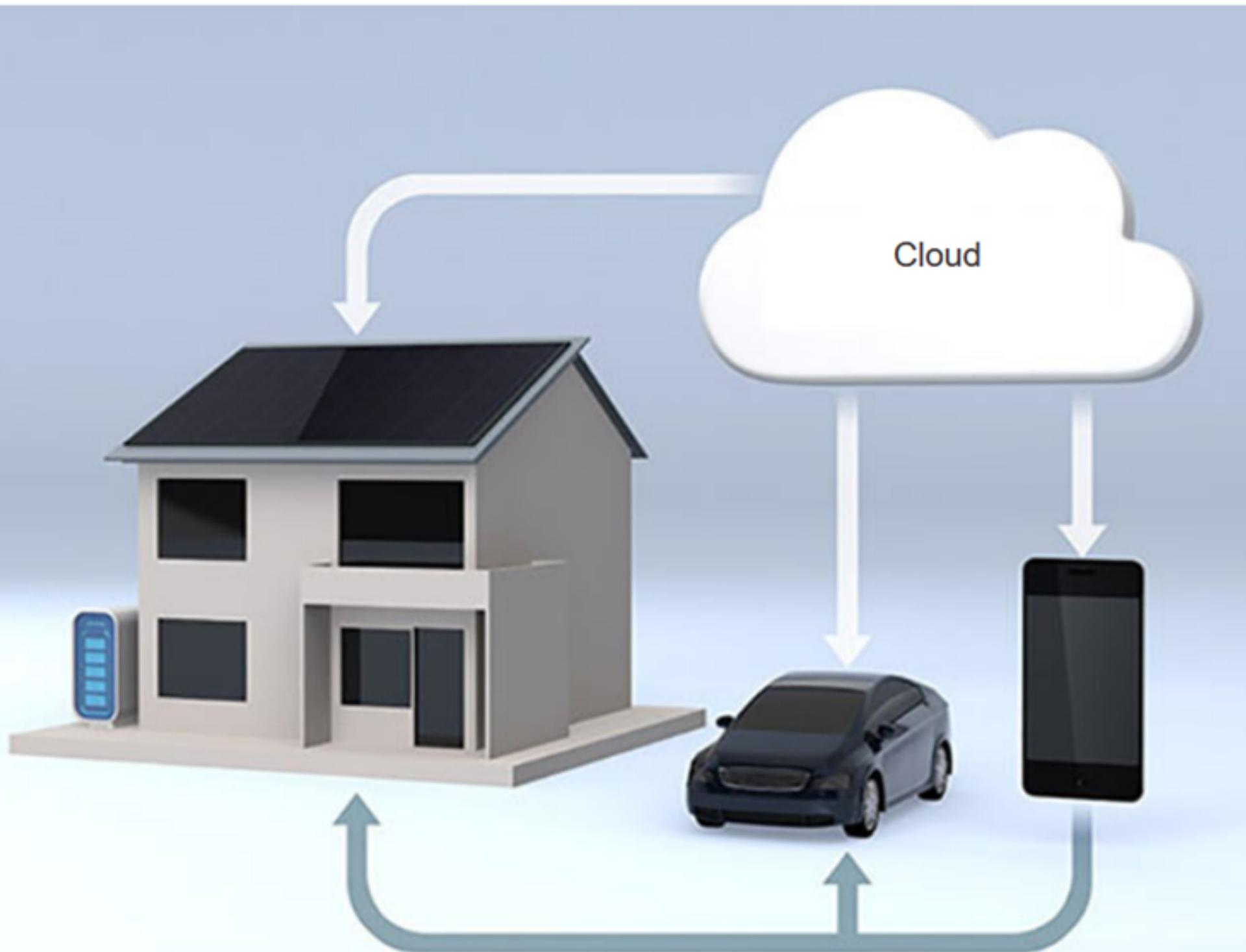
COMPUTACIÓN EN LA NUBE

Cuatro tipos de nubes:

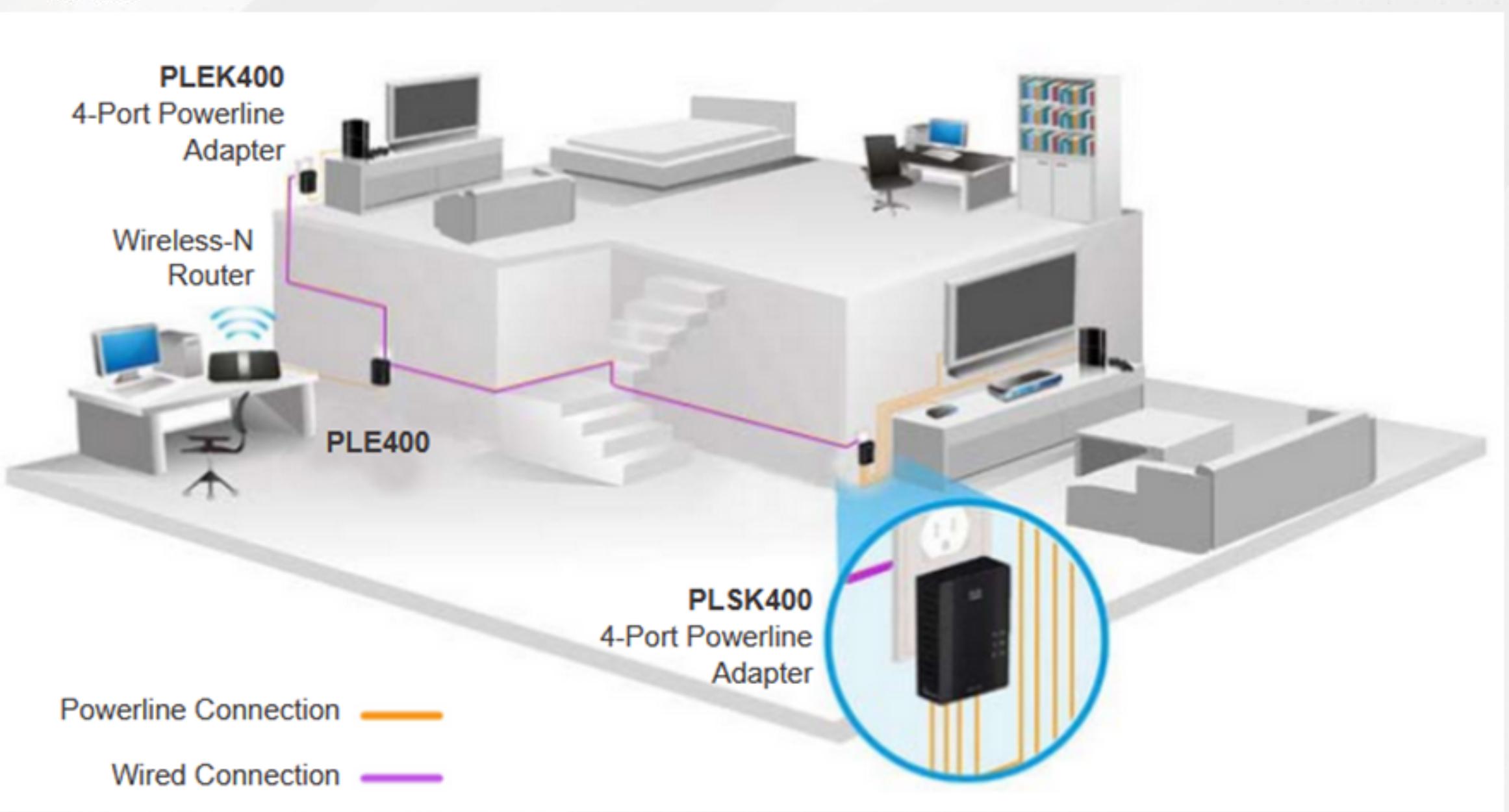
- Nubes públicas
 - Disponible para el público en general a través de un modelo de pago por uso o de forma gratuita.
- Nubes privadas
 - Destinado a una organización o entidad específica como el gobierno.
- Nubes híbridas
 - Están compuestas por dos o más tipos de nubes; por ejemplo, mitad personalizada y mitad pública.
 - Cada parte sigue siendo un objeto distinto, pero ambas están conectadas con la misma arquitectura.
- Nubes personalizadas
 - Creado para satisfacer las necesidades de una industria específica, como la atención médica o los medios de comunicación.
 - Puede ser privado o público.



COMPUTACIÓN EN LA NUBE



- La tecnología del hogar inteligente es una tendencia en alza que permite que la tecnología se integre a los dispositivos que se utilizan a diario, lo que permite que se interconecten con otros dispositivos.
- Los hornos podrían reconocer cuándo cocinar una comida para usted mediante la comunicación con su calendario para saber la hora en la que tiene programado regresar a casa.
- La tecnología de hogar inteligente se está desarrollando actualmente para todas las habitaciones dentro de una casa.



Las redes por línea eléctrica pueden permitir que los dispositivos se conecten a una red LAN donde los cables de la red de datos o las comunicaciones inalámbricas no son una opción viable.

- Con un adaptador estándar de línea eléctrica, los dispositivos pueden conectarse a la red LAN donde haya un tomacorriente mediante el envío de datos en determinadas frecuencias.
- La red Powerline es especialmente útil cuando los puntos de acceso inalámbrico no pueden llegar a todos los dispositivos en el hogar.



REDES DE LÍNEA ELÉCTRICA



Además de DSL y cable, la conexión inalámbrica es otra opción utilizada para conectar hogares y pequeñas empresas a Internet.

- El proveedor de servicios de Internet inalámbrico (WISP), que se encuentra con mayor frecuencia en entornos rurales, es un ISP que conecta a los suscriptores a zonas activas o puntos de acceso designados.
- La banda ancha inalámbrica es otra solución para el hogar y las pequeñas empresas.
 - Utiliza la misma tecnología de red celular que utiliza un Smartphone.
 - Se instala una antena fuera del hogar, que proporciona conectividad inalámbrica o por cable a los dispositivos en el hogar.



SEGURIDAD DE RED

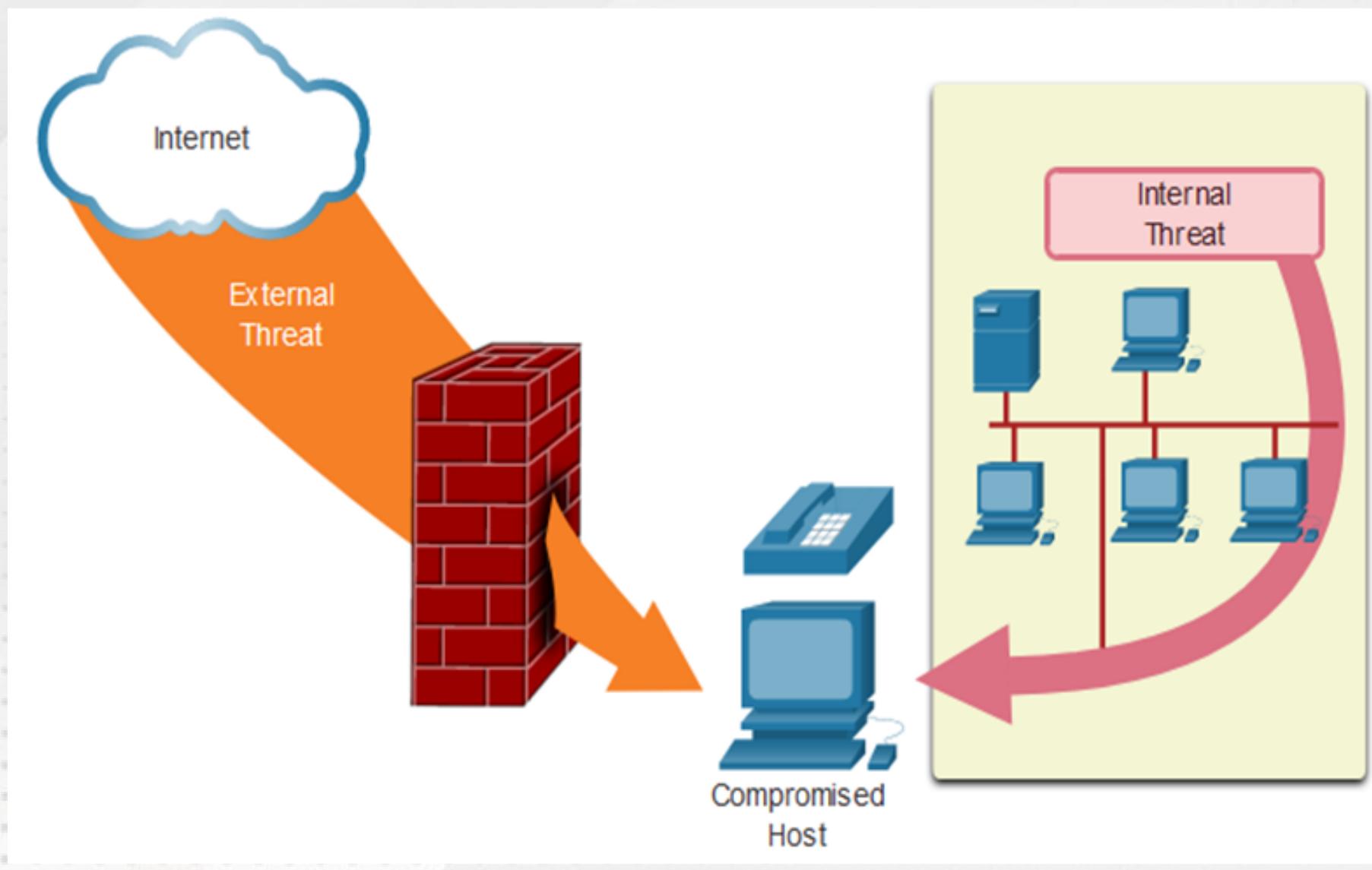




AMENAZAS DE SEGURIDAD

La seguridad de la red es una parte integral de la red informática, independientemente de si la red está en un hogar con una sola conexión a Internet o es una corporación con miles de usuarios.

Debe ser capaz de proteger los datos al tiempo que permite la calidad de servicio que los usuarios esperan de la red.

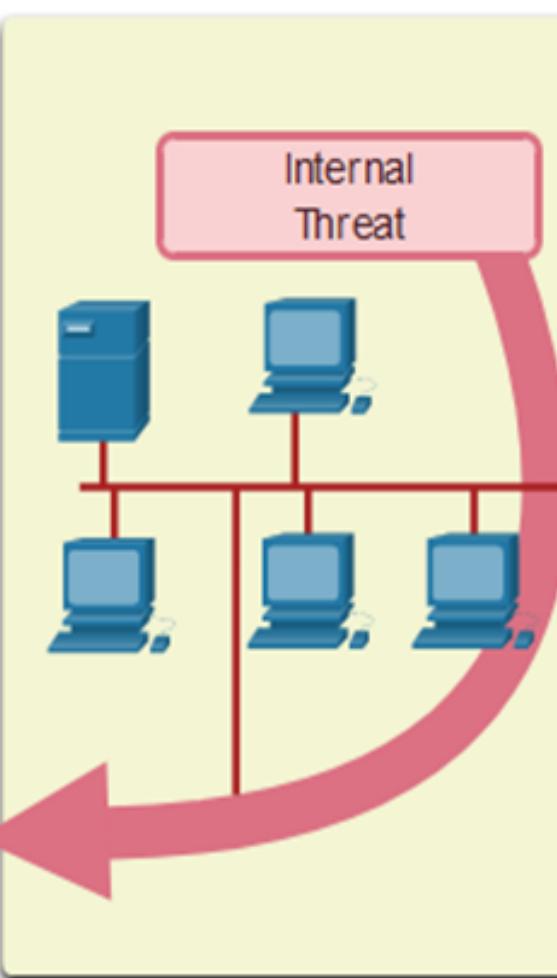


- La seguridad de la red es una parte fundamental de la red sin importar su tamaño.
- La seguridad de la red que se implementa debe tener en cuenta el entorno y proteger los datos, pero, a su vez, debe permitir la calidad de servicio que se espera de la red.
- La protección de la red incluye muchos protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar amenazas.
- Los vectores de amenazas pueden ser externos o internos.



Internet

External Threat



Amenazas externas:

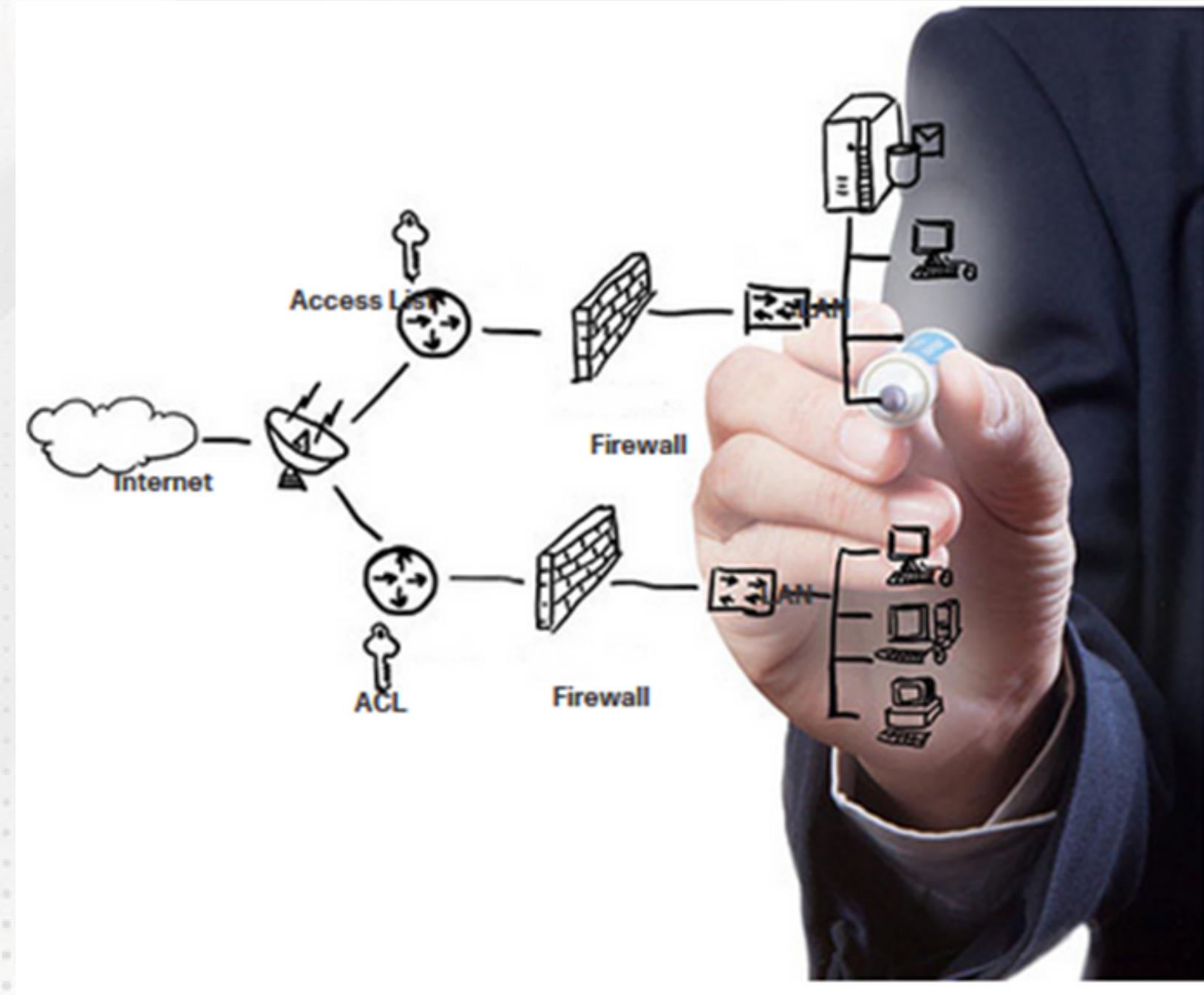
- Virus, gusanos y caballos de Troya
- Spyware y adware
- Ataques de día cero
- Ataques de actores de amenazas
- Ataques por denegación de servicio
- Intercepción y robo de datos
- Robo de identidad

Amenazas internas:

- dispositivos perdidos o robados
- uso indebido accidental por parte de los empleados
- empleados malintencionados



SOLUCIONES DE SEGURIDAD



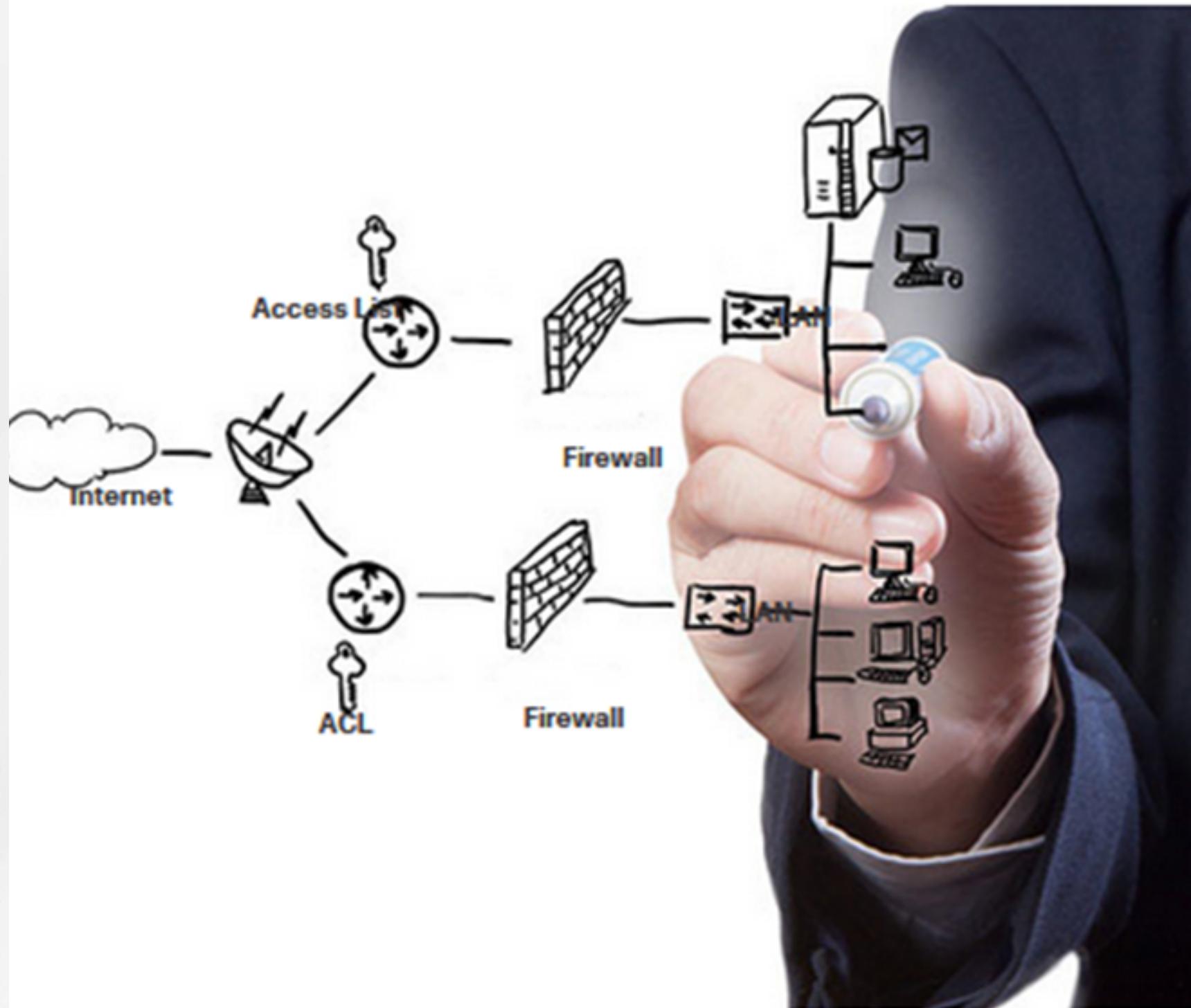
La seguridad debe implementarse en varias capas y debe utilizarse más de una solución de seguridad.

Componentes de seguridad de la red para la red de oficinas en el hogar o de pequeñas oficinas:

- Se debe instalar un software antivirus y antispyware en los terminales.
- El filtrado de firewall se utiliza para bloquear accesos no autorizados a la red.



SOLUCIONES DE SEGURIDAD



Las redes más grandes tienen requisitos de seguridad adicionales:

- Sistema de firewall dedicado
- Listas de control de acceso (ACL)
- Sistemas de prevención de intrusiones (IPS)
- Redes privadas virtuales (VPN)

El estudio de la seguridad de la red comienza con una comprensión clara de la infraestructura subyacente de conmutación y enrutamiento.



CONFIGURACIÓN BÁSICA DEL SWITCH EN PACKET TRACER





Modos de comando principales

Modo EXEC de usuario

- Permite el acceso solamente a una cantidad limitada de comandos básicos de monitoreo.

Router>

Modo EXEC Privilegiado:

- Permite el acceso a todos los comandos y funciones.

Router#



Modo de configuración global:

- Se utiliza para acceder a las opciones de configuración del dispositivo

```
Switch(config) #
```

Modo de configuración de línea:

- Se utiliza para configurar el acceso a la consola, SSH, Telnet o AUX

```
Switch(config-line) #
```

Modo de configuración de interfaz

- Se utiliza para configurar un puerto de switch o una interfaz de router.

```
Switch(config-if) #
```



▪ Modo EXEC privilegiado:

- Para pasar del modo EXEC del usuario al modo EXEC con privilegios, ingrese el comando **enable**.

```
Switch> enable  
Switch#
```

▪ Modo de configuración global:

- Para entrar y salir del modo de configuración global, use el comando **configure terminal** Para volver al modo EXEC privilegiado, use el comando **exit**

```
Switch(config)#  
Switch(config)#exit  
Switch#
```

▪ Modo de configuración de línea:

- Para entrar y salir del modo de configuración de línea, utilice el comando **line** seguido del tipo de línea de administración. Para volver al modo de configuración global, use el comando **exit**

```
Switch(config)#line console 0  
Switch(config-line)#exit  
Switch(config)#
```

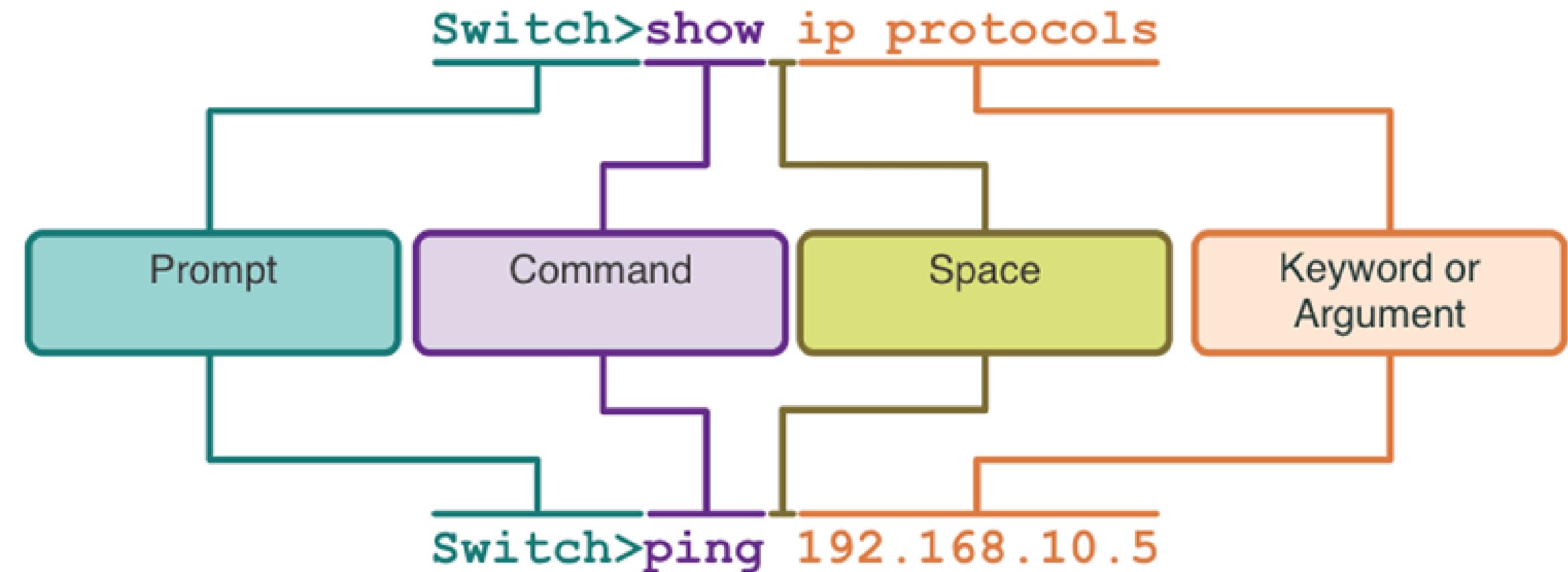


Modos de subconfiguración

- Para salir de un modo de subconfiguración y volver al modo de configuración global, utilice el comando **exit**. Para volver al modo EXEC de privilegios, utilice el comando **end** o la combinación de **teclas Ctrl +Z**.
- Para desplazarse directamente de un modo de subconfiguración a otro, escriba el comando de modo de subconfiguración deseado. En el ejemplo, el símbolo del sistema cambia de **(config-line)#** a **(config-if)#**.

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

```
Switch (config-line)#interface FastEthernet 0/1
Switch (config-if)#
```



- **Palabra clave**: un parámetro específico que se define en el sistema operativo.
- **Argumento**: no está predefinido; es un valor o variable definido por el usuario.



Convención	Descripción
negrita	El texto en negrita indica los comandos y las palabras clave que se introducen literalmente como se muestran.
<i>cursiva</i>	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento opcional (palabra clave o argumento).
{x}	Las llaves indican un elemento obligatorio (palabra clave o argumento).
[x {y z }]	Las llaves y las líneas verticales dentro de corchetes indican una opción obligatoria dentro de un elemento opcional. Los espacios se utilizan para delinear claramente partes del comando.



- La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.
- El comando es **ping** y el argumento definido por el usuario es la *dirección IP* del dispositivo de destino. Por ejemplo: **ping** 10.10.10.5.
- El comando es **traceroute** y el argumento definido por el usuario es la *dirección IP* del dispositivo de destino. Por ejemplo: **traceroute** 192.168.254.254.

```
ping ip-address
```

```
traceroute ip-address
```



El IOS tiene dos formas de ayuda disponibles: la ayuda contextual y el verificador de sintaxis de comandos.

- La ayuda contextual le permite encontrar rápidamente respuestas a estas preguntas:
 - ¿Qué comandos están disponibles en cada modo de comando?
 - ¿Qué comandos comienzan con caracteres específicos o grupo de caracteres?
 - ¿Qué argumentos y palabras clave están disponibles para comandos particulares?
- La verificación de la sintaxis del comando comprueba que el usuario haya introducido un comando válido.
 - Si el intérprete no puede comprender el comando que se ingresa, mostrará un comentario que describe el error del comando.

```
Router#ping ?  
WORD Ping destination address or hostname  
ip IP echo  
ipv6 IPv6 echo
```

```
Switch#interface fastEthernet 0/1  
^  
% Invalid input detected at '^' marker.
```



- La tabla siguiente es una breve lista de pulsaciones de teclas para mejorar la edición de la línea de comandos.

Pulsación de teclas	Descripción
Tab	Completa una entrada de nombre de comando parcial.
Retroceso	Borra el carácter a la izquierda del cursor.
Flecha izquierda o Ctrl+B	Desplaza el cursor un carácter hacia la izquierda.
Flecha derecha o Ctrl+F	Desplaza el cursor un carácter hacia la derecha.
Flecha arriba o Ctrl+P	Recupera los comandos en el búfer de historial, comenzando con los comandos más recientes.



- Cuando una salida de comando produce más texto del que se puede mostrar en una ventana de terminal, el IOS mostrará un mensaje «—More—» . En la siguiente tabla se describen las pulsaciones de teclas que se pueden utilizar cuando se muestra esta solicitud.
- En la siguiente tabla se enumeran los comandos que se pueden utilizar para salir de una operación.

Pulsación de teclas	Descripción
Tecla Enter	Muestra la siguiente línea.
Barra espaciadora	Muestra la siguiente pantalla.
Cualquier otra tecla	Termina la cadena que se muestra y vuelve al modo EXEC con privilegios.

Pulsación de teclas	Descripción
Ctrl-C	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC con privilegios.
Ctrl-Z	Cuando está en cualquier modo de configuración, termina el modo de configuración y regresa al modo EXEC con privilegios.
Ctrl-Shift-6	Secuencia de interrupción multiuso, utilizada para anular búsquedas DNS, traceroutes, pings, etc.



ITSQMET
INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

CONFIGURACIÓN BÁSICA DE DISPOSITIVOS

FORMANDO PROFESIONALES DE ÉLITE



- El primer comando de configuración en cualquier dispositivo debe ser darle un **nombre** de host único. **Nota:** Para devolver el cambio al indicador predeterminado, use el comando **no hostname** de configuración global.

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

Proteger el modo EXEC del usuario

- Primero ingrese al modo de configuración de la consola de línea usando el comando **line console 0** en el modo de configuración global.
- Luego, configure la contraseña de modo EXEC de usuario con el comando **password**.
- Finalmente, habilite el acceso EXEC de usuario con el comando **login**.

Asegurar el acceso al modo EXEC privilegiado

- Utilice el comando **enable secret password**.



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

Asegurar el acceso a la línea VTY:

- Primero ingrese el modo de configuración de línea VTY utilizando el comando **line vty 0 15** en el modo de configuración global.
- Los archivos startup-config y running-config muestran la mayoría de las contraseñas en texto simple.
- Para encriptar las contraseñas, utilice el comando de configuración global **service password-encryption**.
- Utilice el comando **show running-config** para verificar que las contraseñas se hayan encriptado.

```
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#
```

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

```
Sw-Floor-1# show running-config
!
!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

- Para crear un mensaje de aviso del día en un dispositivo de red, utilice el comando de configuración global **banner motd #el mensaje del día #**.



```
Sw-Floor-1# configure terminal  
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

Press RETURN to get started.

Authorized Access Only!

User Access Verification

Password:



- Existen dos archivos de sistema que almacenan la configuración de dispositivos.
 - **startup-config** - Este es el archivo de configuración guardado que se almacena en NVRAM. Contiene todos los comandos que usará el dispositivo al iniciar o reiniciar. Flash no pierde su contenido cuando el dispositivo está apagado.
 - **running-config** - Esto se almacena en la memoria de acceso aleatorio (RAM). Refleja la configuración actual.
NOTA: La memoria RAM es volátil. Pierde todo el contenido cuando el dispositivo se apaga o se reinicia.
- Para guardar los cambios realizados en la configuración en ejecución en el archivo de configuración de inicio utilice el comando **copy running-config startup-config** en el modo EXEC privilegiado.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetimestamp msec
no service timestamps debug datetimestamp msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetimestamp msec
no service timestamps debug datetimestamp msec
no service password-encryption
```



ITSQMET

INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI.

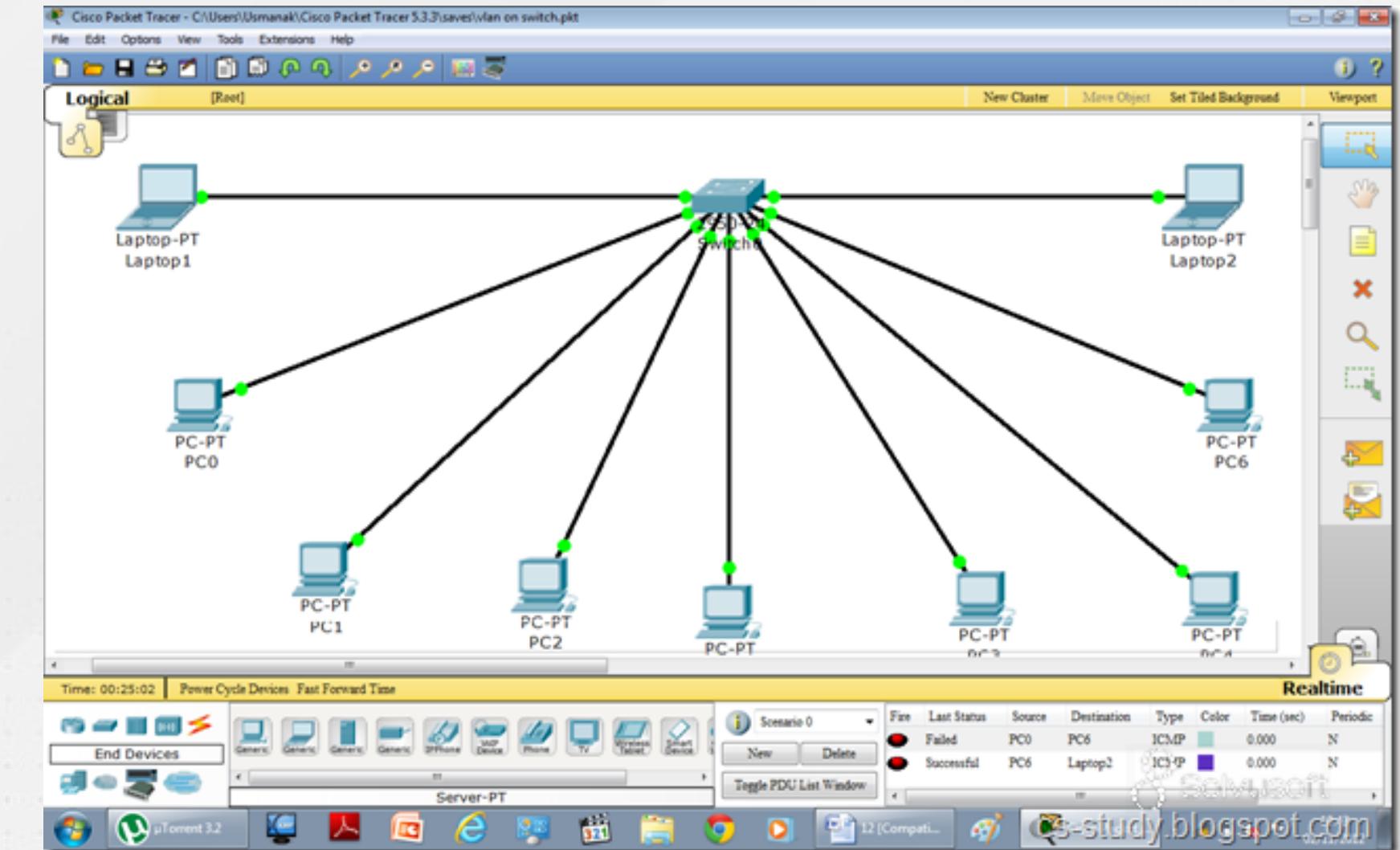
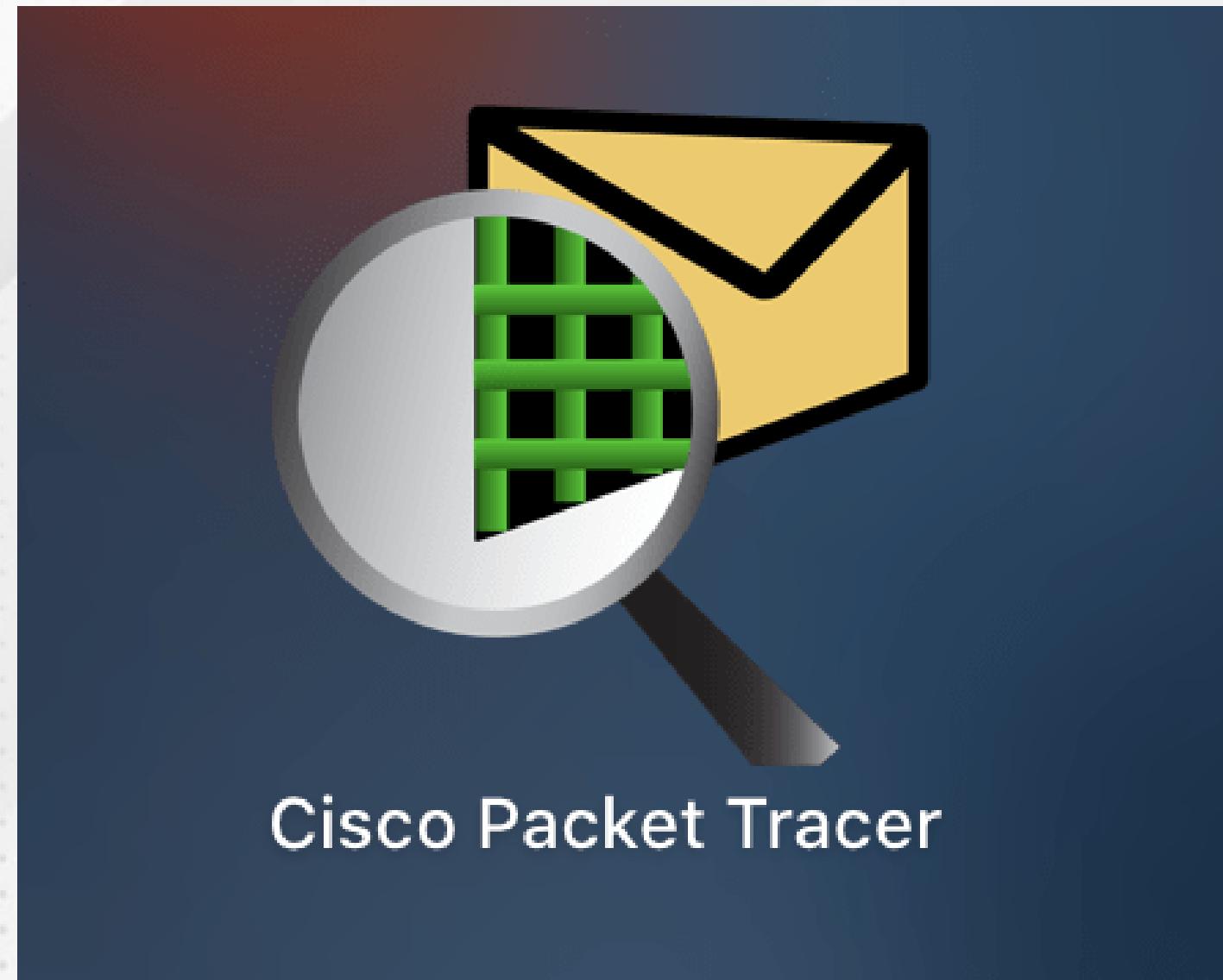
Para configurar un SVI en un switch:

- Ingrese el comando **interface vlan 1** en el modo de configuración global.
- A continuación, asigne una dirección IPv4 mediante el comando **ip address ip-address subnet-mask**
- Finalmente, habilite la interfaz virtual usando el comando **no shutdown**.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```



Cisco Packet Tracer





Seleccione un switch y debe constar con la siguiente configuración.

- Nombre: “**SU APELLIDO**”-SWITCH
- CONTRASEÑA PARA PASAR EL MODO EXEC PRIVILEGIADO: CISCO
- CONTRASEÑA PARA INGRESAR AL DISPOSITIVO: CLASS
- AVISO DE ADVERTENCIA: ‘DISPOSITIVO DE **SU NOMBRE**’
- COPIADA LA CONFIGURACIÓN QUE ESTA CORRIENDO AL ARCHIVO DE INICIO.



¿PREGUNTAS?



ITSQMET
INSTITUTO TECNOLÓGICO SUPERIOR
QUITO METROPOLITANO

GRACIAS

FORMANDO PROFESIONALES DE ÉLITE