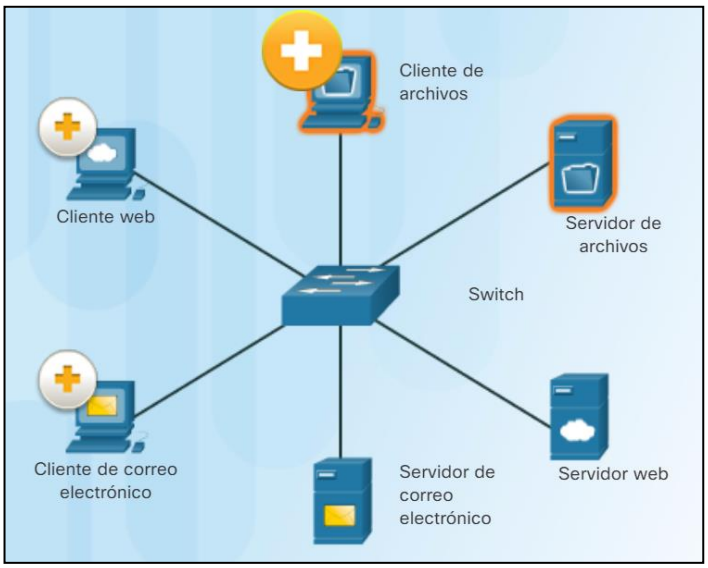
CAPÍTULO 1. EXPLORACIÓN DE LA RED

1.1.2.2 CLIENTES Y SERVIDORES

Todas las PC conectadas a una red que participan directamente en las comunicaciones de la red se clasifican como hosts o terminales. Cada servicio de la red requiere un software de servidor independiente.

En las conexiones entre cliente – servidor, el servidor ejecuta un software de servidor y el cliente un software de cliente para tener acceso a la información del servidor. Un PC con software de servidor puede proporcionar servicio a varios clientes.

Asimismo, una misma PC puede ejecutar varios software de servidor y varios software de cliente.



1.1.2.3 ENTRE PARES

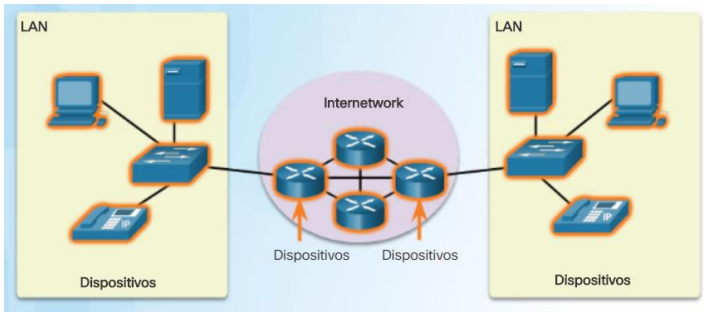
El software de servidor y de cliente normalmente se ejecutan en computadoras distintas, pero también es posible que una misma computadora cumpla las dos funciones a la vez.

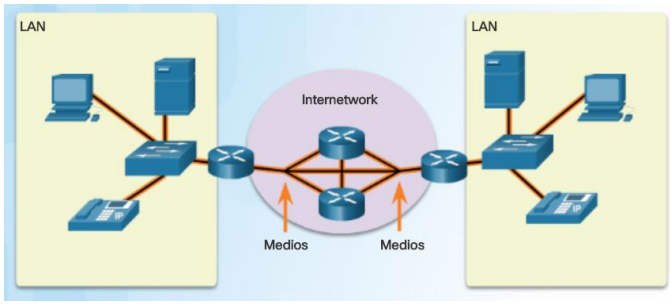
- Ventajas:
  - Configuración y uso más sencillos.
  - Menor costo.
- Desventajas:
  - Administración descentralizada.
  - Menos seguras y escalables.
  - Menor rendimiento por parte de la máquina.

1.2.1.1 DESCRIPCIÓN GENERAL DE LOS COMPONENTES DE LA RED

La infraestructura de red contiene tres categorías: dispositivos, medios y servicios. Los dispositivos y medios son los elementos físicos o hardware de la red y los servicios son las aplicaciones de red.

Dentro de esta infraestructura, los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red.





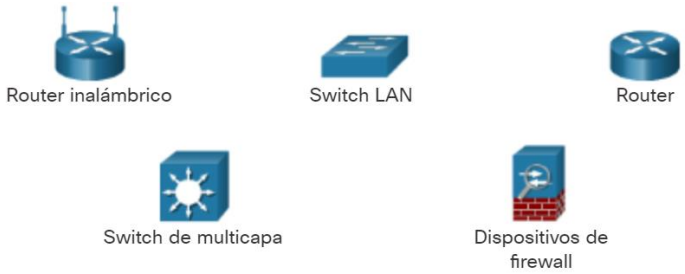
1.2.1.3 DISPOSITIVOS DE RED INTERMEDIARIOS

Los dispositivos intermediarios conectan los terminales individuales a la red o conectan redes con redes para formar una internetwork. De esta forma se consigue la conectividad y se garantiza un flujo de datos en toda la red.

Estos dispositivos se apoyan en la dirección del terminal de destina y en la información de interconexión de la red para determinar la ruta que deben tomar los mensajes a través de la red.

Un dispositivo intermediario puede admitir alguna de estas funciones o todas ellas:

- Volver a generar y transmitir las señales de datos.
- Conservar información de las rutas de la red y de internetwork.
- Notificar errores y fallas de comunicación a otros dispositivos.
- Redirigir los datos por rutas alternativas si hay una falla en un enlace.
- Permitir o denegar el flujo de datos de acuerdo a los parámetros de seguridad.



1.2.1.4 MEDIOS DE RED

El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino. Los medios usados actualmente son:

- **Hilos metálicos dentro de cables**: los datos se codifican en impulsos eléctricos.
- **Fibras de vidrio o plástico (cable de fibra óptica)**: los datos se codifican con pulsos de luz.
- **Transmisión inalámbrica**: los datos se codifican con longitudes de onda del espectro electromagnético.

Los criterios a tener en cuenta a la hora de elegir un medio son:

- Distancia máxima en la que el medio puede transportar una señal exitosamente.
- Tipo de entorno en el que se instalará el medio.
- Cantidad de datos y velocidad a la que se deben transmitir.
- Costo del medio y de la instalación.

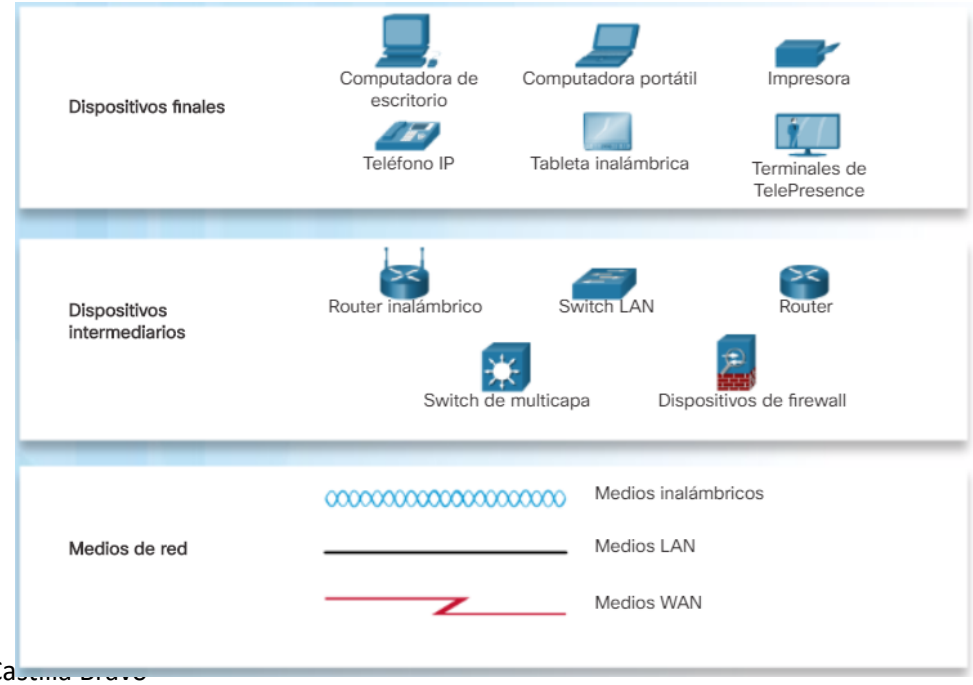
1.2.1.5 REPRESENTACIONES DE RED

Los diagramas de red o diagramas de topología utilizan símbolos para representar los diferentes dispositivos y conexiones que componen una red. Los diagramas van acompañados de una terminología especializada para hablar sobre cómo se conectan los dispositivos y los medios entre sí. Algunos términos son:

- **Tarjeta de interfaz de red (NIC o adaptador LAN):** permite realizar la conexión física entre la red y el PC u otro terminal.
- **Puerto físico**: conector en un dispositivo de red.
- **Interfaz:** puerto especializado en un dispositivo de red que se conecta a redes individuales.

Nota: con frecuencia, los términos puerto e interfaz se usan de forma indistinta.

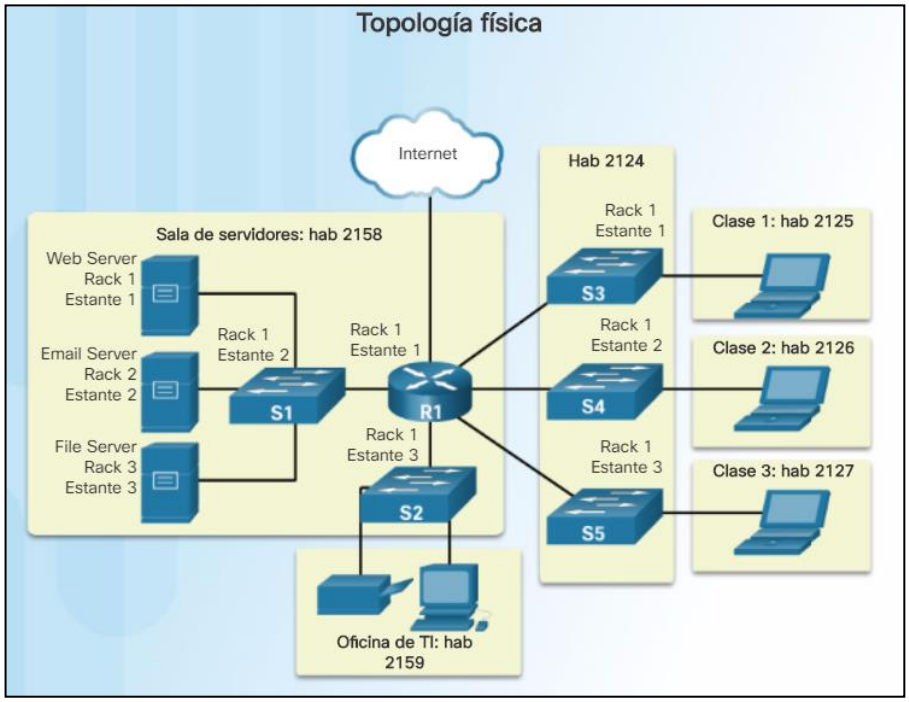
Símbolos para diagramas de topología

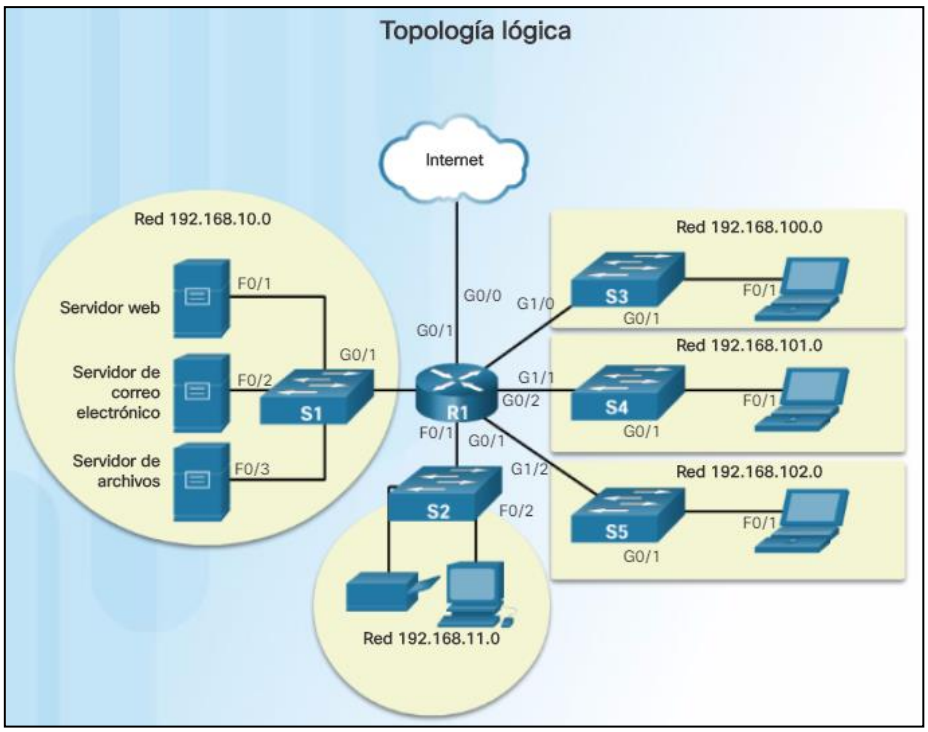


1.2.1.6 DIAGRAMAS DE TOPOLOGÍA

Existen dos tipos de diagramas de topología:

- **Diagramas de topología física**: identifican la ubicación física de los dispositivos intermediarios y la instalación de los cables.
- **Diagramas de topología lógica**: identifican dispositivos, puertos y el esquema de direccionamiento.





1.2.2.1 Tipos de redes

Las infraestructuras de red más comunes son:

- Red de área local (LAN). *Definida en los apuntes*.
- Red de área amplia (WAN). *Definida en los apuntes*
- Red de área metropolitana (MAN). *Definida en los apuntes.*
- LAN inalámbrica (WLAN): son similares a las LAN, solo que interconectan de forma inalámbrica a los usuarios y los extremos en un área geográfica pequeña.
- Red de área de almacenamiento (SAN): son infraestructuras de red diseñadas para admitir servidores de archivos y proporcionar almacenamiento, recuperación y replicación de datos.

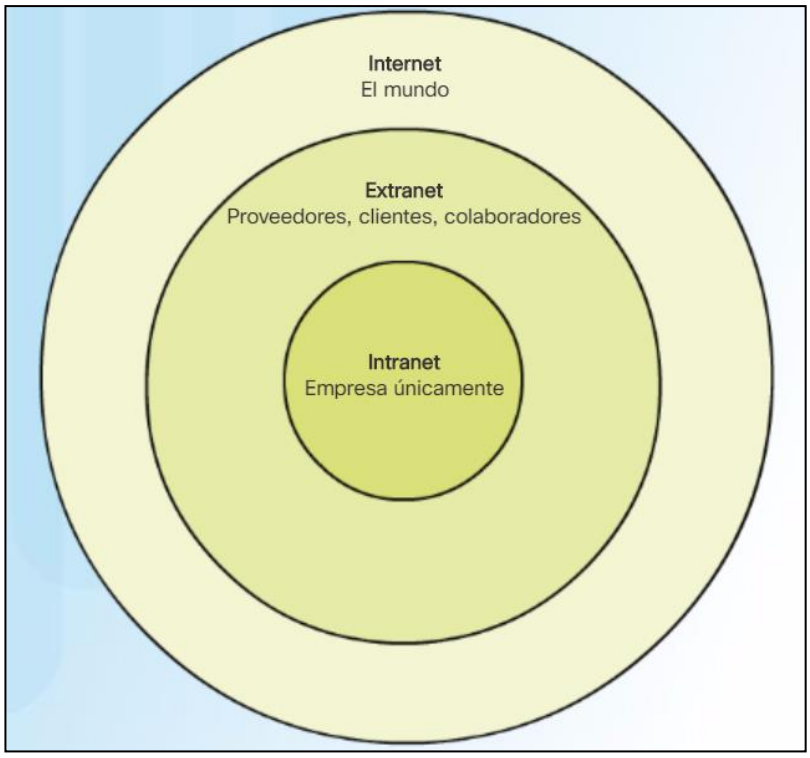
1.2.3.1 Internet

Internet se puede ver como una colección global de redes LAN y WAN interconectadas. Para continuar con el desarrollo de esta infraestructura y asegurar su mantenimiento, existen organizaciones como:

- El Grupo de trabajo de ingeniería de Internet (IETF).
- La Corporación de Internet para la Asignación de Nombres y Números (ICANN).
- El Consejo de Arquitectura de Internet (IAB).

1.2.3.2 Intranets y extranets

- Intranet: se utiliza para hacer referencia a una conexión privada de LAN y WAN que pertenece a una organización y está diseñada para que accedan a ella solo los miembros y los empleados de la organización u toras personas autorizadas.
- Extranet: permite proporcionar un acceso seguro a las personas que trabajan para otra organización pero requiere datos de la empresa.

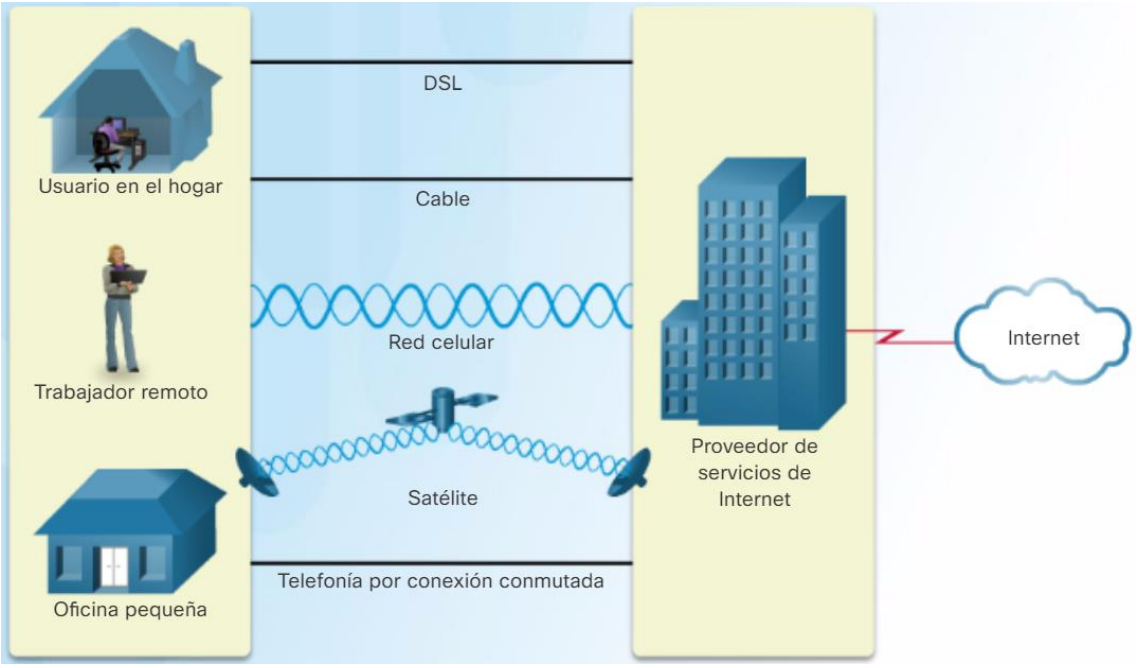


1.2.4.1 Tecnologías de acceso a Internet

- ISP: proveedor de servicios de internet.
- SP: proveedor de servicios.
- DSL: anda ancho por línea de suscriptor digital.
-

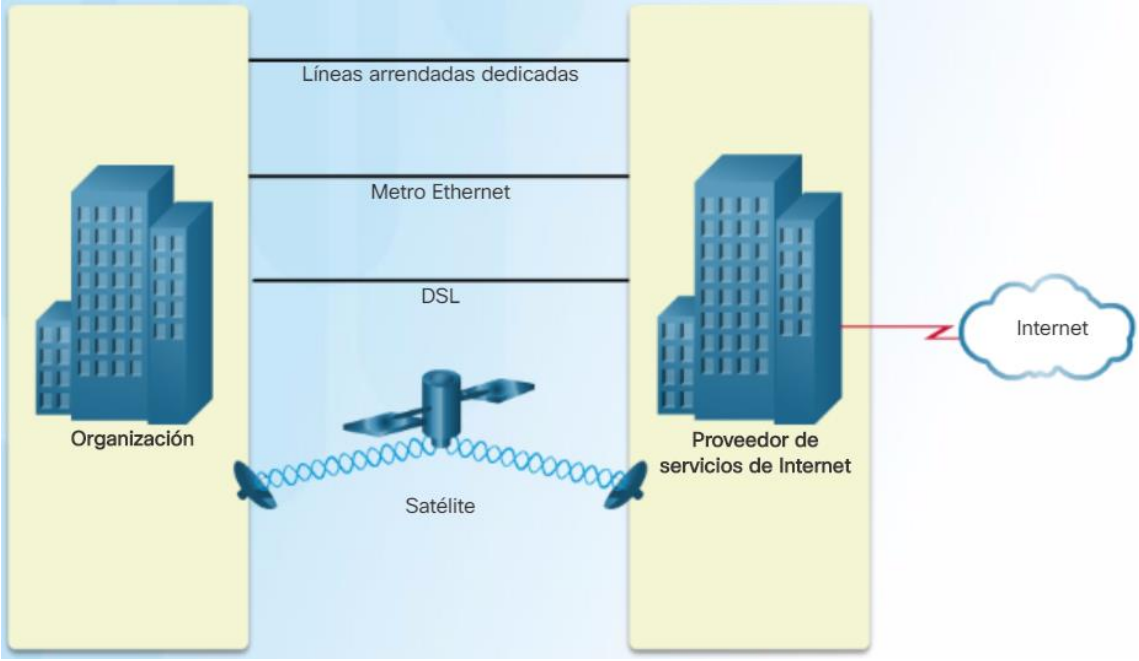
1.2.4.2 Conexiones a Internet domésticas y de oficinas pequeñas

- Cable: La señal se transporta por el cable de televisión. La línea siempre está activa y el ancho de banda es elevado.
- DSL (línea de suscriptor digital): La señal se transporta por el cable de teléfono. La línea siempre está activa y el ancho de banda es elevado.
- ADSL (línea de suscriptor digital asimétrica): la velocidad de descarga es mayor que la de carga.
- Red celular: Uso de datos móviles. El rendimiento depende del teléfono y de la torre de telefonía móvil a la que se conecte.
- Satelital: permite el acceso a internet en zonas donde no se tiene otro tipo de conectividad. Se necesitan antenas parabólicas que tengan una visión despejada del satélite.
- Telefonía por conexión conmutada: opción de bajo costo que funciona con cualquier línea telefónica y un módem. El ancho de banda es bajo.



1.2.4.3 Conexiones a Internet empresariales

- Líneas arrendadas dedicadas: circuitos reservados dentro de la red del proveedor para uso privado. Es una opción costosa.
- WAN Ethernet: amplía la tecnología de acceso LAN a una WAN.
- DSL: se ofrece en diversos formatos, entre ellos SDSL (línea de suscriptor digital simétrica).
- Satelital.



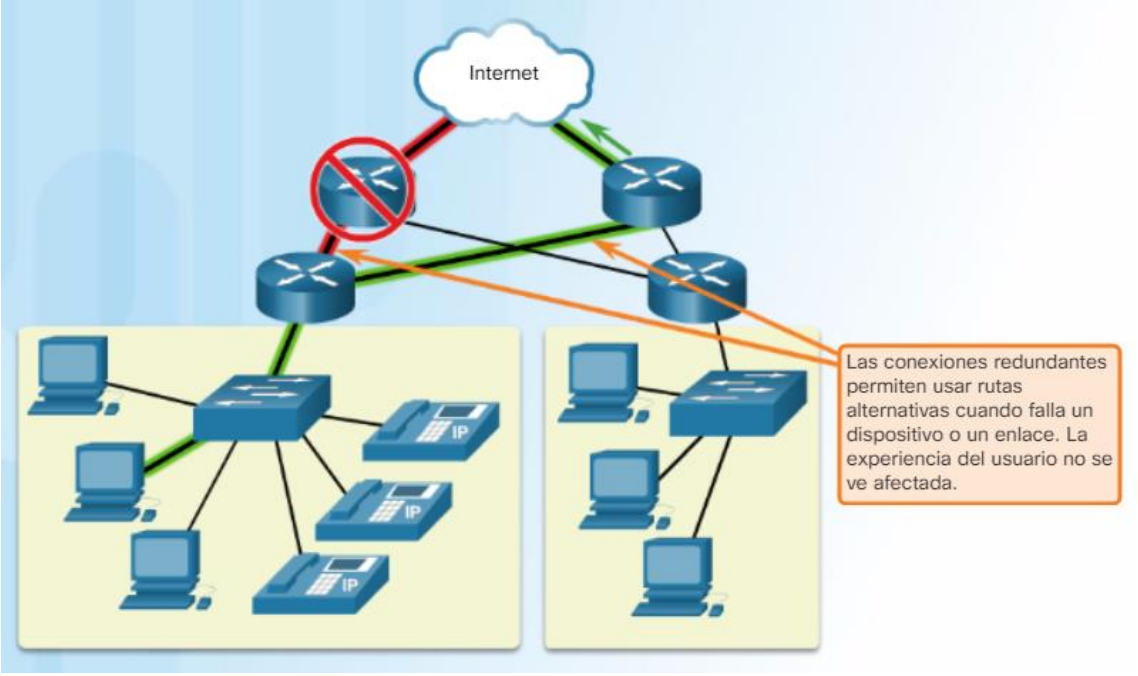
1.3.2.1 Arquitectura de red

La arquitectura de red se puede entender como las tecnologías que dan soporte a la infraestructura, servicios y protocolos que trasladan datos a través de la red. Existen cuatro características básicas que las arquitecturas deben cumplir:

- Tolerancia a fallas.
- Escalabilidad.
- Calidad de servicio (QoS).
- Seguridad.

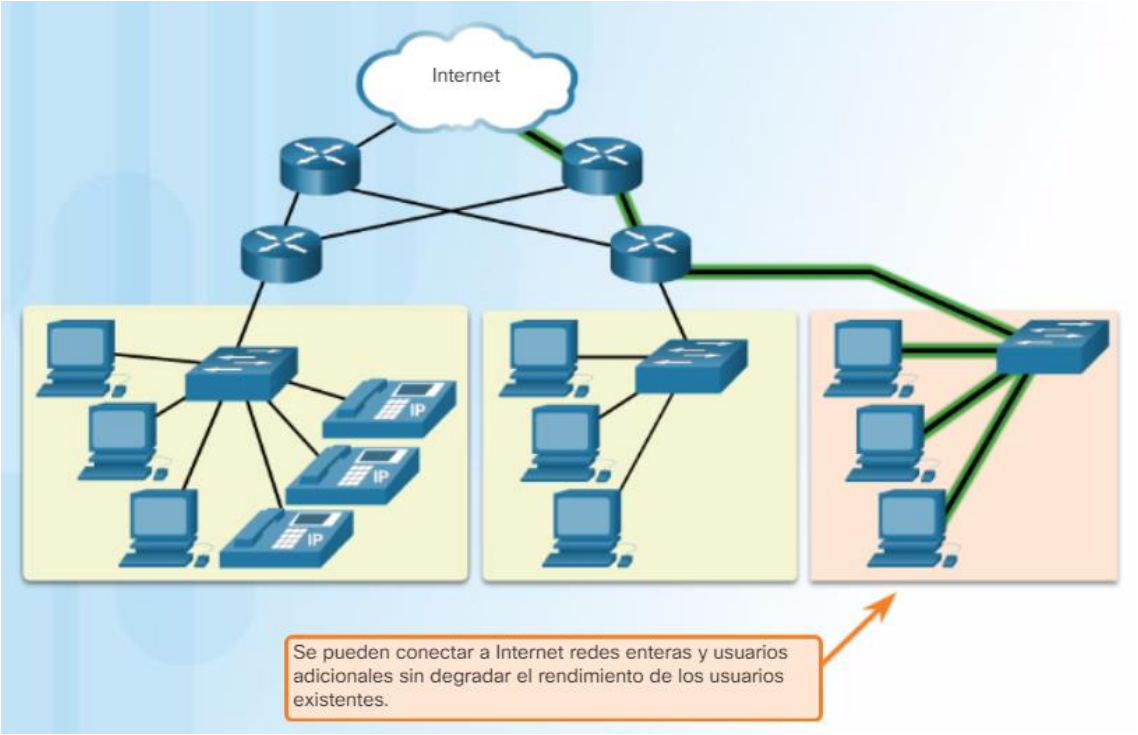
1.3.2.2 Tolerancia a fallas

Una red con tolerancia a fallas es aquella que limita el impacto de las fallas de manera que la cantidad de los dispositivos afectados sea la menor posible. Para ello, se usan rutas alternativas (redundancia). A través de la conmutación por paquetes, si se produce una falla, se pueden redirigir los paquetes por otro camino de forma transparente al usuario.



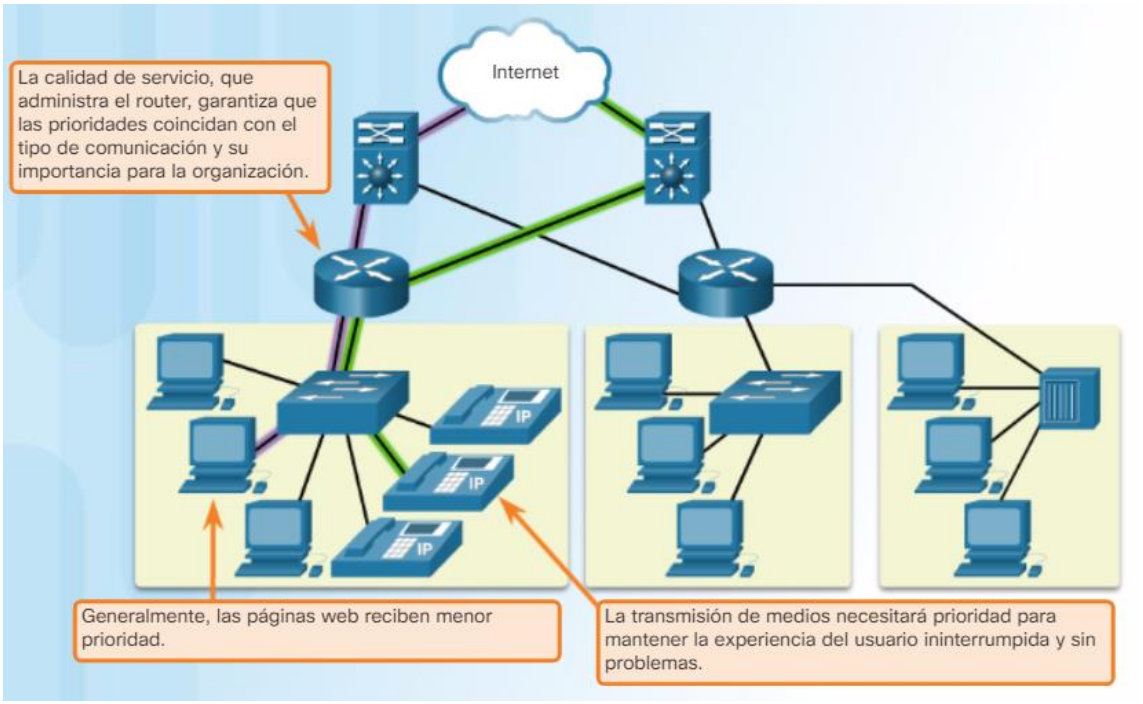
1.3.2.3 Escalabilidad

Se dice que una red es escalable cuando se pueden admitir nuevos usuarios y aplicaciones sin afectar al rendimiento del servicio enviado a los usuarios actuales.



1.3.2.4 Calidad de servicio (QoS)

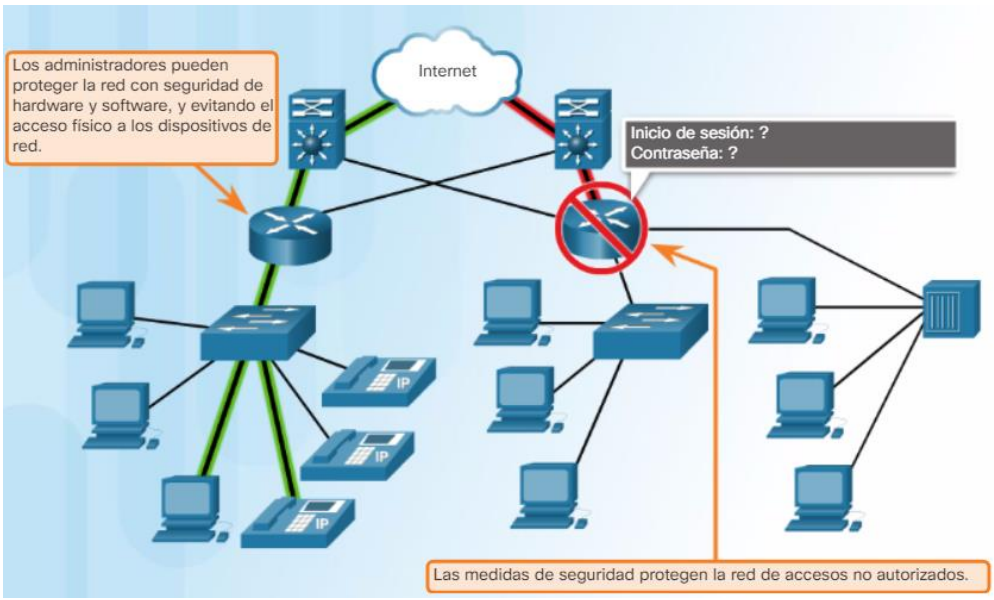
La calidad de servicio se mide en función de cómo se regula la congestión y de cómo se garantiza el envío confiable de contenido a todos los usuarios.



1.3.2.5 Seguridad

Los problemas de seguridad de red se pueden dividir en dos grupos:

- Seguridad de la infraestructura. Los dispositivos deben proporcionar conectividad y evitar el acceso no autorizado a su software administrativo.
- Seguridad de la información que se transmite por la red. Debe cumplir:
  - Confidencialidad.
  - Integridad: que los datos no se alteren durante la transmisión.
  - Disponibilidad.



1.4.1.1 Nuevas tendencias

Entre las principales tendencias encontramos:

- BYOD (Bring Your Own Device).
- Colaboración en línea.
- Comunicaciones de vídeo.
- Computación en la nube.

1.4.1.2 BYOD (Bring Your Own Device)

La tendencia BYOD les da a los usuarios finales la libertad de utilizar herramientas personales para acceder a información y comunicarse a través de una red. En definitiva, usar cualquier dispositivo, de cualquier persona, en cualquier lugar.

1.4.1.5 Computación en la nube

Diferenciamos cuatro tipos de nubes:

- Nubes públicas.
- Privadas.
- Híbridas.
- Personalizadas.

1.4.2.3 Banda ancha inalámbrica

Proveedor de servicios de Internet inalámbrico (WISP)

EL proveedor de servicios de internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado a una zona activa mediante tecnologías inalámbricas. Se coloca una antena en un punto elevado y otra en el techo del suscriptor. De esta forma se consigue la transmisión.

Servicio de banda ancha inalámbrico

Se instala una antena fuera del hogar que proporciona conectividad inalámbrica o por cale a los dispositivos del hogar.

1.4.3.1 Amenazas de seguridad

Las amenazas de seguridad pueden ser internas o externas. Las externas más comunes son:

- **Virus, gusanos y caballos de Troya:** software malicioso y códigos arbitrarios que se ejecutan en un dispositivo de usuario.
- **Spyware y adware:** software instalado que recopila información sobre un el usuario de forma secreta.
- **Ataques de día cero:** ataque que ocurre el mismo día que se hace pública una vulnerabilidad.
- **Ataques de hackers.**
- **Ataques por denegación de servicio:** ataques diseñados para reducir o bloquear aplicaciones y procesos en un dispositivo de red.
- **Interceptación y robo de datos:** un ataque para capturar información privada en la red de una organización.

1.4.3.2 Soluciones de seguridad

- **Antivirus o antispyware:** proteger de software malicioso.
- **Firewall:** bloquear accesos no autorizados exterior al interior y viceversa.
- **Listas de control de acceso (ACL):** filtran el acceso y el reenvío de tráfico.
- **Sistemas de prevención de intrusión (IPS):** identifican amenazas de rápida expansión.
- **Redes privadas virtuales (VPN):** proporcionan acceso seguro a trabajadores remotos.