

# Redes - Primer documento

## **Introducción**

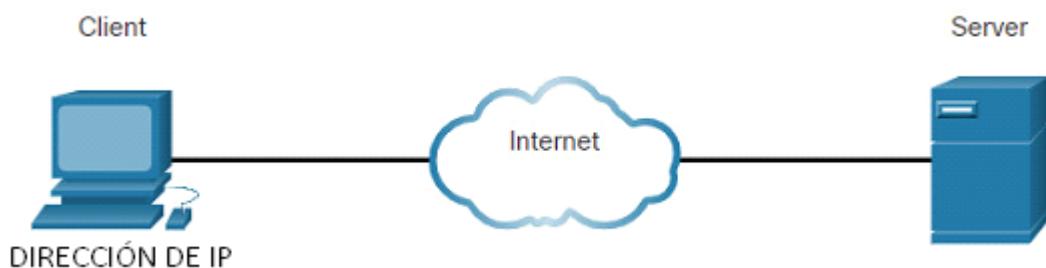
Los avances más significativos de redes son quizás los cambios más significativos en el mundo de hoy. Están ayudando a crear un mundo en el que las grandes distancias se vuelven menos significativas. El internet, las comunidades en línea y la creación de la nube nos permiten acceder a nuestros datos, debatir con gente y estar en línea en cualquier dispositivo.

## **Roles de Host**

Para estar en línea, primero hay que estar conectado a una red. Toda computadora conectada a una red participando directamente de la comunicación se llama **Host**.

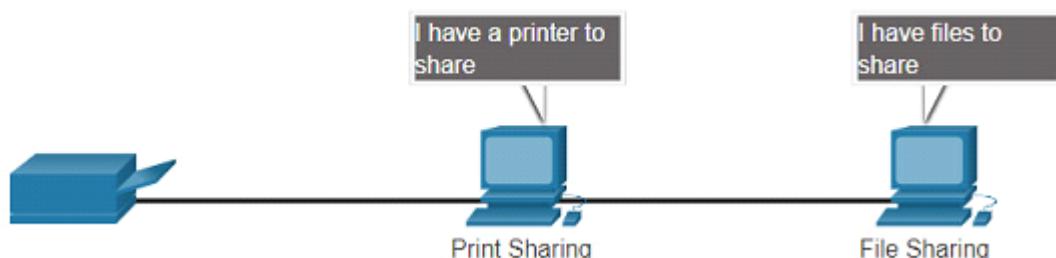
Los hosts también se llaman dispositivos finales o clientes. Sin embargo este término se refiere a dispositivos en la red que tienen un número asignado para fines de comunicación. Este número es su **IP** (Dirección de protocolo de Internet).

Los **servidores** permiten proporcionar información a otros dispositivos.



## **De igual a igual**

Se puede utilizar una computadora como **Cliente - Servidor** para pequeñas empresas u hogares. Este tipo de red se llama red de igual a igual.



### Ventajas:

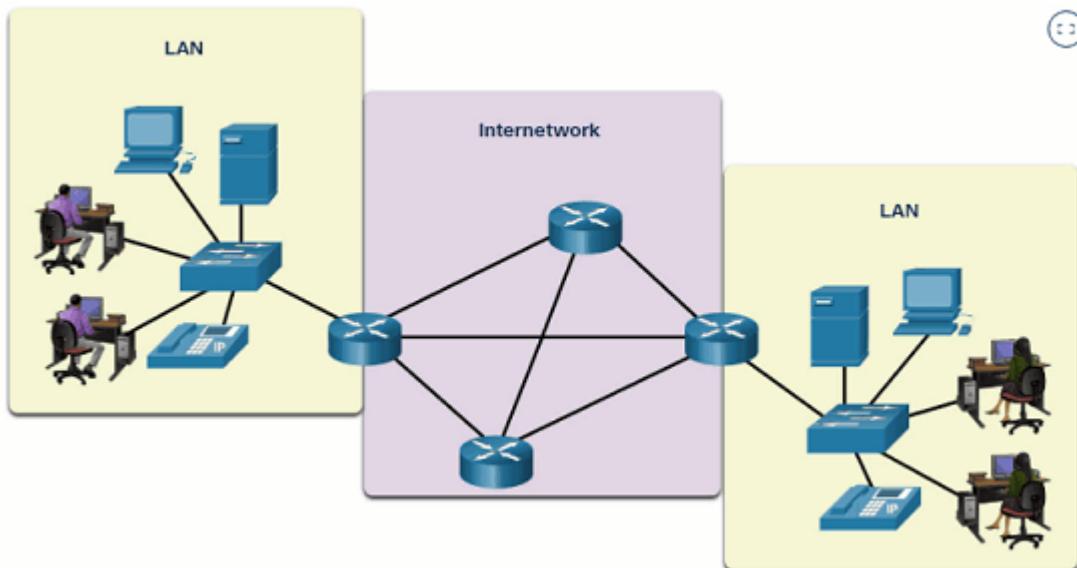
- Fácil de configurar
- Menos complejo
- Menor costo

### Desventajas:

- No tan seguro
- No escalable
- Bajo rendimiento

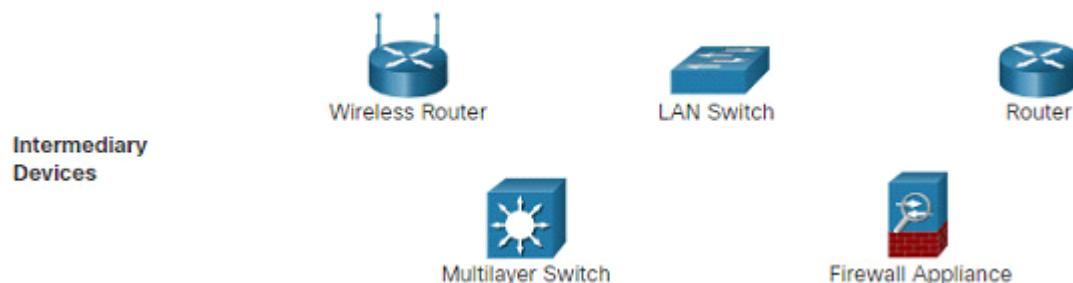
## Dispositivos Finales

Un dispositivo final es el origen o el destino de un mensaje transmitido a través de la red. Cada uno de estos tiene una dirección.



## Dispositivos Intermediarios

Los dispositivos intermediarios tienen el papel de conectar a los dispositivos finales a la red. También pueden conectar múltiples redes individuales para crear una red interna. Sirven de interconexiones para determinar rutas de mensajes.



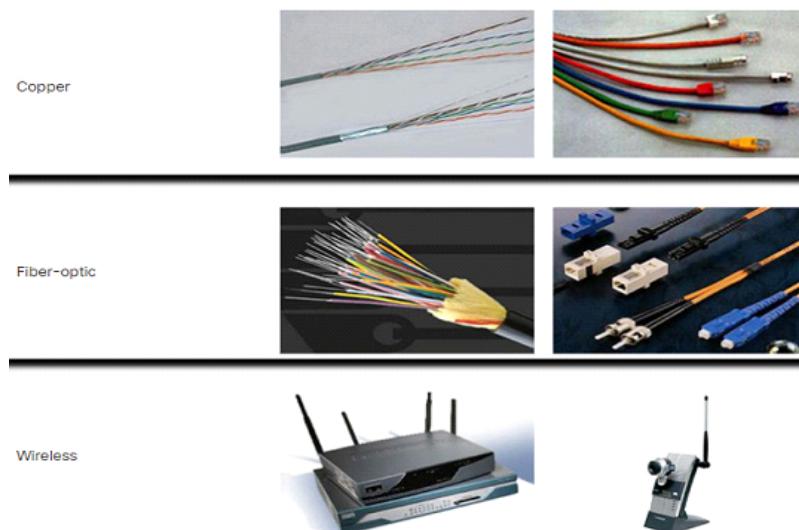
Estos realizan:

- Regenerar y retransmitir señales de comunicación.
- Mantener información de la red interna.
- Permitir o denegar flujo de datos.
- Notificar de fallas.

## Medios de Red (Canales)

Las redes modernas utilizan principalmente tres tipos de medios:

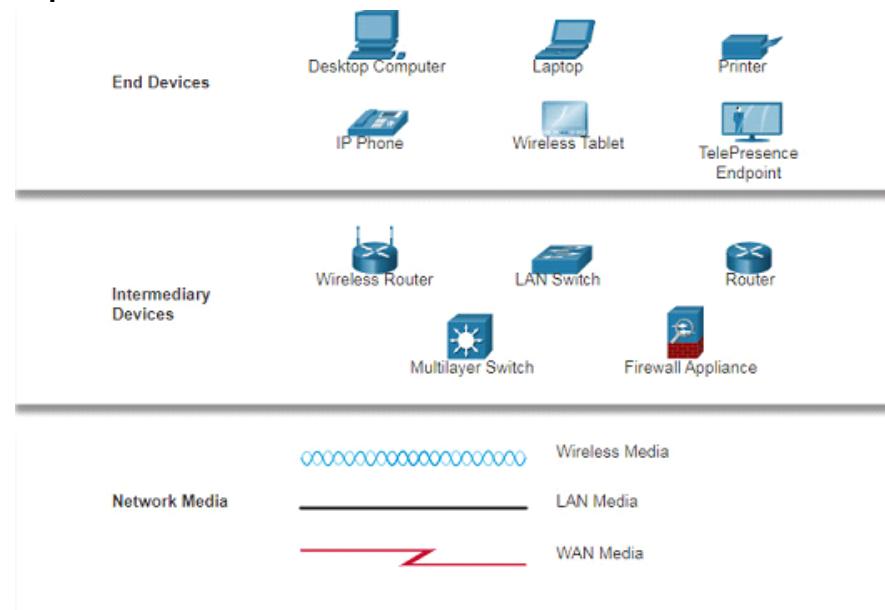
1. Cables de metal dentro de cables: Impulsos eléctricos para codificar datos.
2. Fibras de vidrio: Pulses de luz para codificar datos.
3. Transmisión inalámbrica: Modulación de frecuencias para codificar datos.



### Criterios para elegir medios de red:

- Distancia máxima.
- Entorno.
- Cantidad de datos.
- Velocidad de transferencia de datos.
- Costo de instalación.

## Representación de red



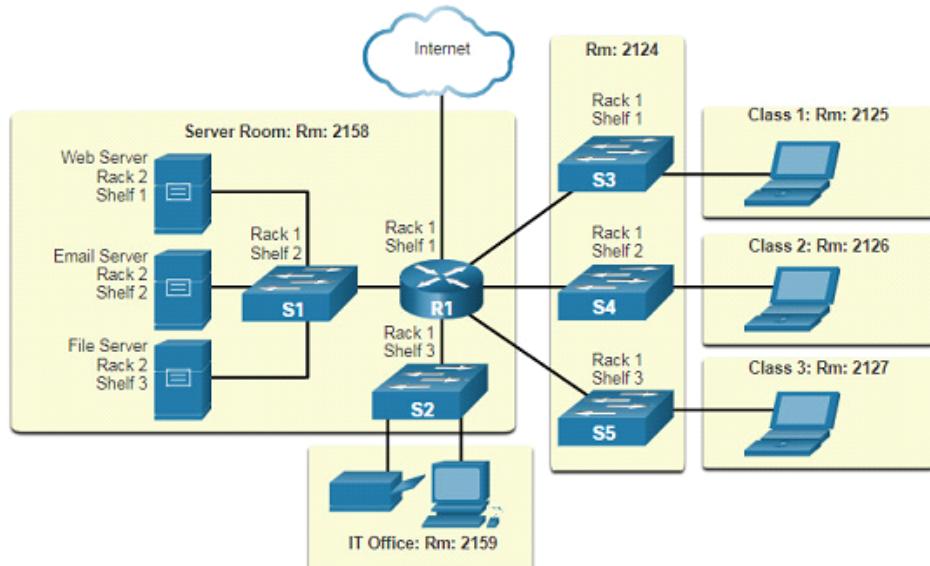
Además de estas representaciones, se utiliza una terminología especializada para describir cómo cada uno de estos dispositivos y medios trabajan entre sí:

- Tarjeta de Interfaz de red (NIC): Conecta físicamente el dispositivo final a una red.
- Puerto físico: Conector o salida en un dispositivo de red.
- Interfaz: Puertos especializados en un dispositivo de red.

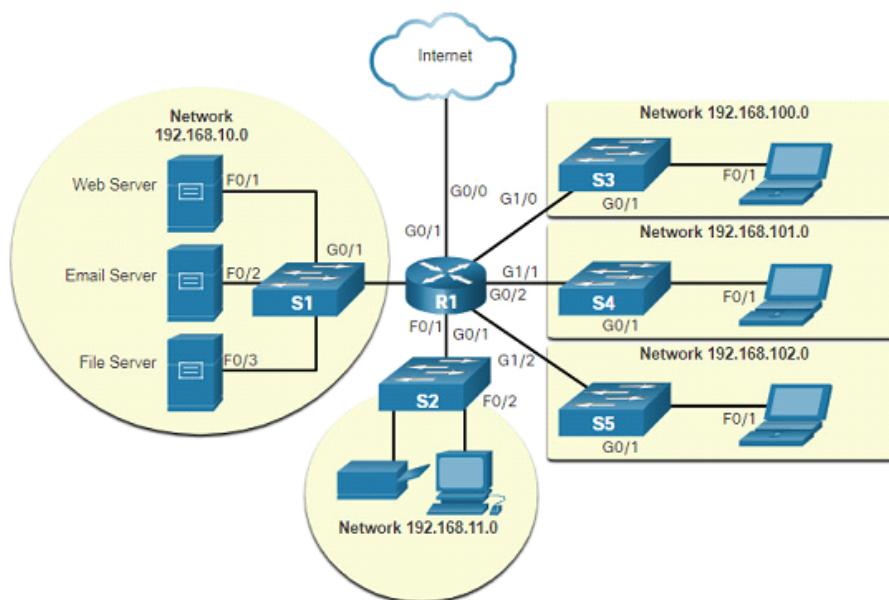
## Diagramas de topología

Proporcionan un mapa visual de cómo está conectada la red. Hay dos tipos de diagramas:

- Diagrama de topología física: Ilustran la ubicación física de los dispositivos intermedios y la instalación del cable.



- Diagrama de topología lógica: Ilustran dispositivos, puertos y el esquema de direccionamiento de la red.



## Redes de diversos tamaños

### Redes domésticas pequeñas

Conectan algunas computadoras entre sí y ellas a Internet.

### Redes de oficinas pequeñas y oficinas domésticas

La red SOHO (Small Office - Home Office) permite que las computadoras en una oficina hogareña o remota se conecten a una red corporativa o accedan a recursos compartidos centralizados.

### Redes medianas a grandes

Las redes medianas a grandes, como las utilizadas por corporaciones y escuelas, pueden tener muchas ubicaciones con cientos o miles de hosts interconectados.

### Redes mundiales

Internet es una red de redes que conecta a cientos de millones de computadoras en todo el mundo.

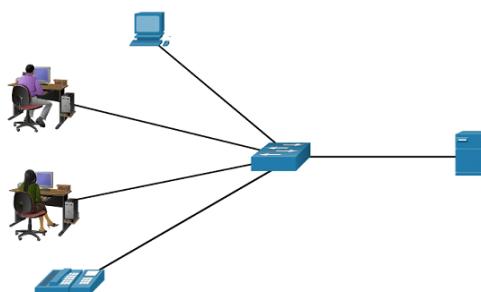
## LAN y WAN

Las infraestructuras de red varían mucho en términos de:

- Tamaño de área cubierta.
- Número de usuarios conectados.
- Número y tipos de servicios disponibles.
- Área de responsabilidad

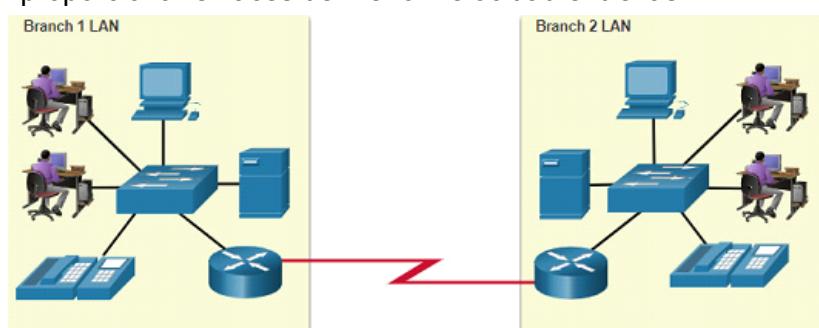
### LAN:

- Abarca una pequeña área geográfica.
- Interconectan dispositivos finales en hogares, escuelas u oficinas y campus.
- Administrada por un solo individuo o sola organización.
- Ancho de banda de alta velocidad a dispositivos finales.

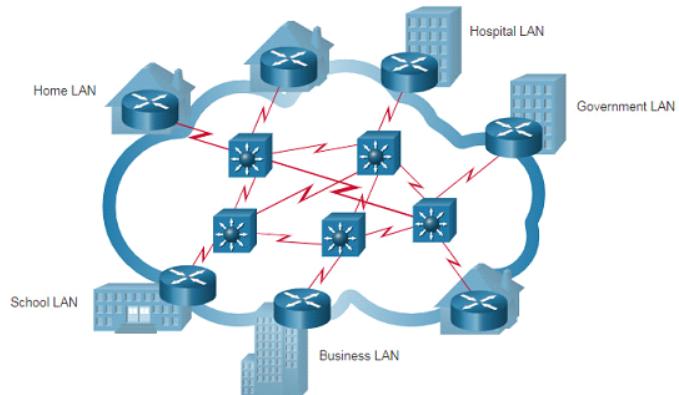


### WAN:

- Interconectan LAN en amplias áreas geográficas.
- Administradas por múltiples proveedores de servicios.
- Suelen proporcionar enlaces de menor velocidad entre las LAN.



## La internet



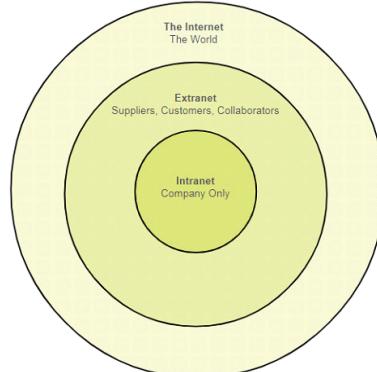
Internet es una colección de redes interconectadas. La figura muestra una forma de ver Internet como una colección de LAN y WAN interconectadas.

Internet no es propiedad de ningún individuo o grupo. Hay estándares que aseguran la comunicación efectiva como:

- IETF
- ICANN
- IAB

## Intranets y Extranets

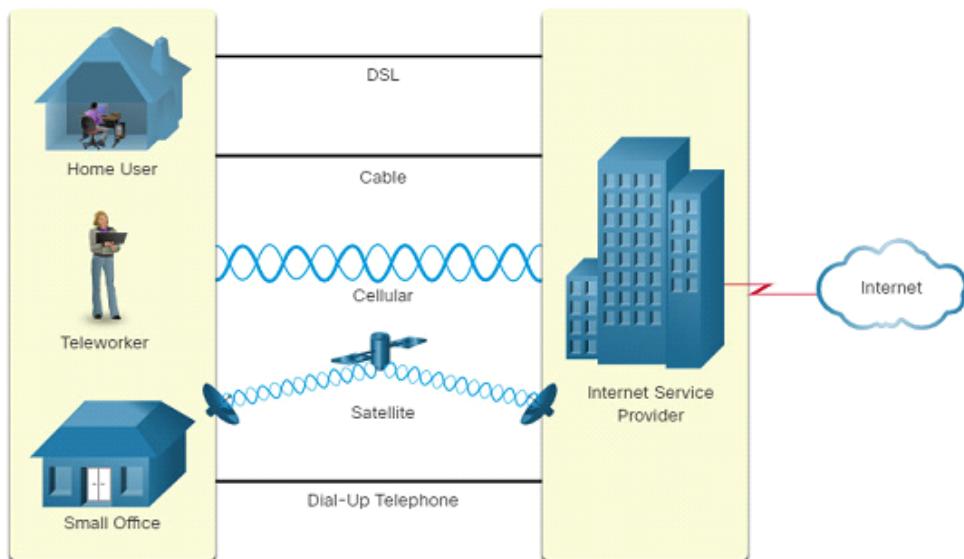
*Intranet* es un término utilizado a menudo para referirse a una conexión privada de LAN y WAN que pertenece a una organización. Una organización también puede usar una extranet para proporcionar acceso seguro a personas que trabajan para una organización (VPN)



## Tecnología de acceso a Internet

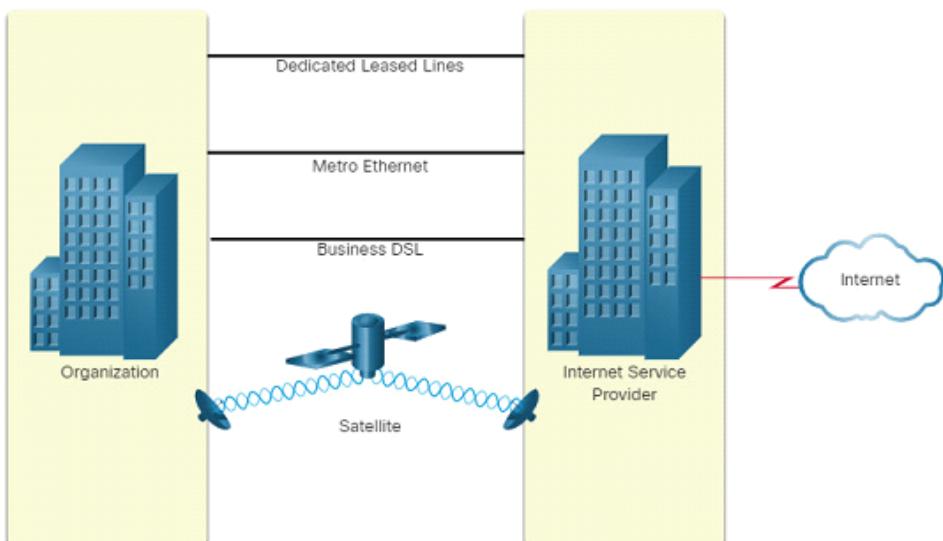
Los usuarios domésticos, trabajadores remotos y las oficinas pequeñas generalmente requieren una conexión ISP para acceder a Internet. Los SP ofrecen interconexiones de clase empresarial. Los servicios populares de clase empresarial incluyen DSL empresarial, líneas arrendadas y Metro Ethernet.

## Conexiones de Internet para el hogar y pequeñas oficinas



- **Cable:** Proporciona gran ancho de banda, alta disponibilidad y una conexión permanente a Internet.
- **DSL:** Línea de abonado digital proporciona un gran ancho de banda, alta disponibilidad y una conexión permanente a Internet
- **Celular:** El rendimiento será limitado por las capacidades del teléfono y la torre celular a la que está conectado.
- **Satélite:** Para áreas geográficas complicadas. Antenas parabólicas apuntan al satélite.
- **Teléfono de acceso público:** Bajo ancho de banda pero útil para el acceso móvil mientras se viaja.

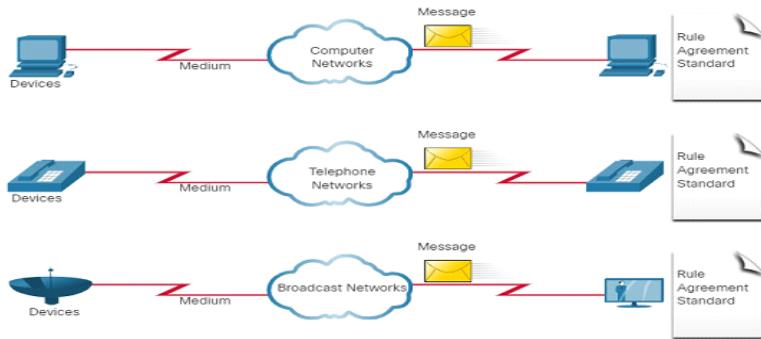
## Conexiones de Internet para Negocios



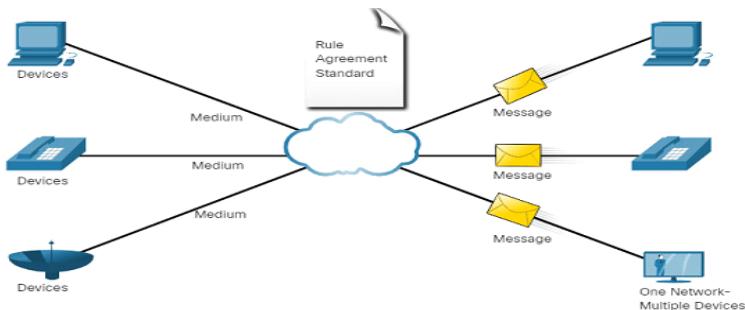
- **Línea arrendada dedicada:** Circuitos reservados para áreas geográficas separadas. Se alquilan a una tasa mensual/anual.
- **Metro Ethernet:** Extienden la tecnología LAN a WAN.
- **Business DSL:** Proporciona cargas y descargas a las mismas altas velocidades.
- **Satélite:** Para áreas geográficas complicadas. Antenas parabólicas apuntan al satélite.

## La red convergente

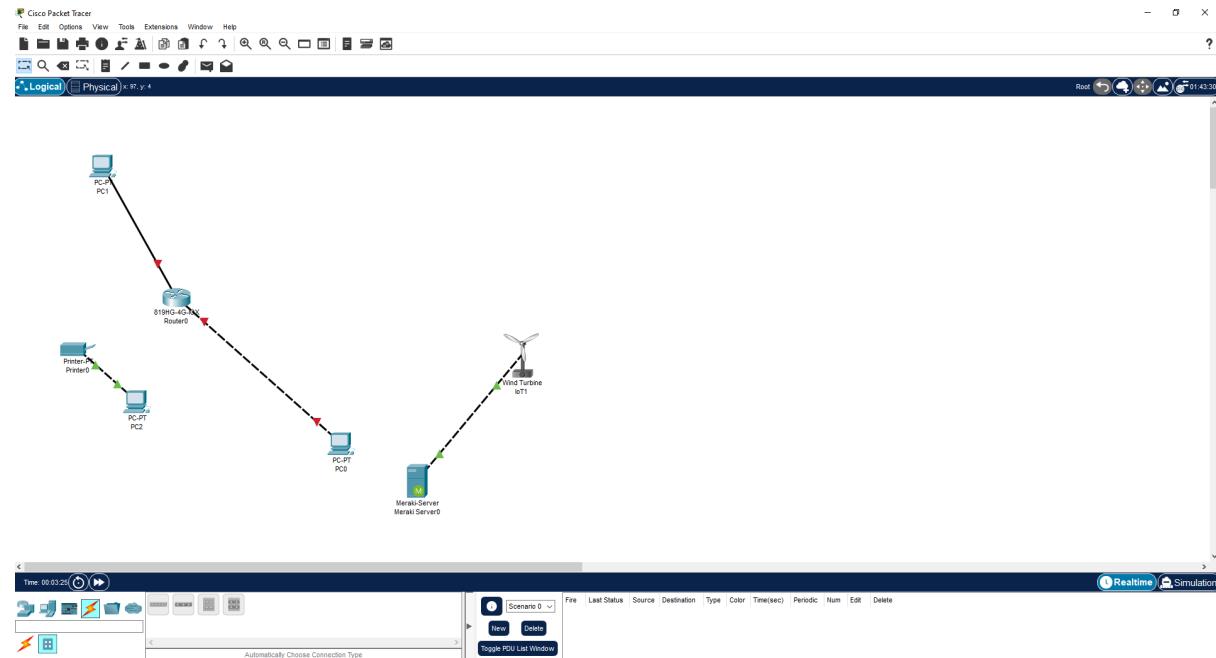
- Redes separadas tradicionales: Cada red tiene su propio conjunto de reglas y estándares. Tecnología vieja.



- Redes convergentes: A diferencia de las redes dedicadas, las redes convergentes son capaces de entregar datos, voz y video entre muchos tipos diferentes de dispositivos a través de la misma infraestructura de red.



## Descargar Cisco Packet Tracer y jugar un rato



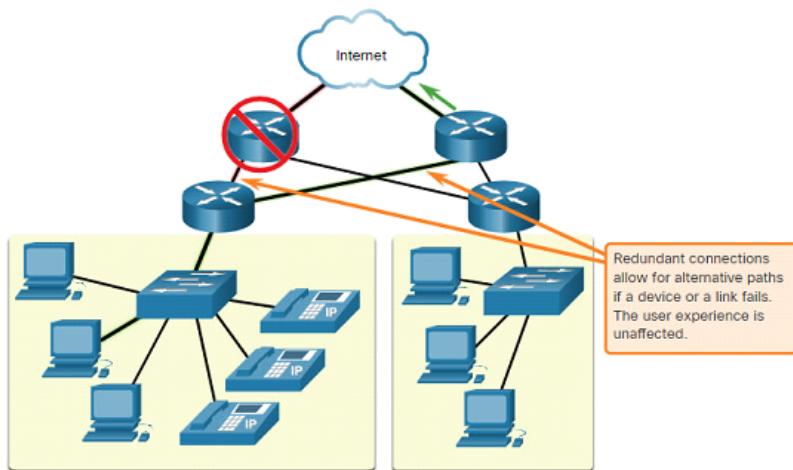
## Red de Arquitectura:

Las redes tienen el papel de ser un sistema que permite las conexiones de personas, dispositivos e información en un entorno de red convergente rico en medios.

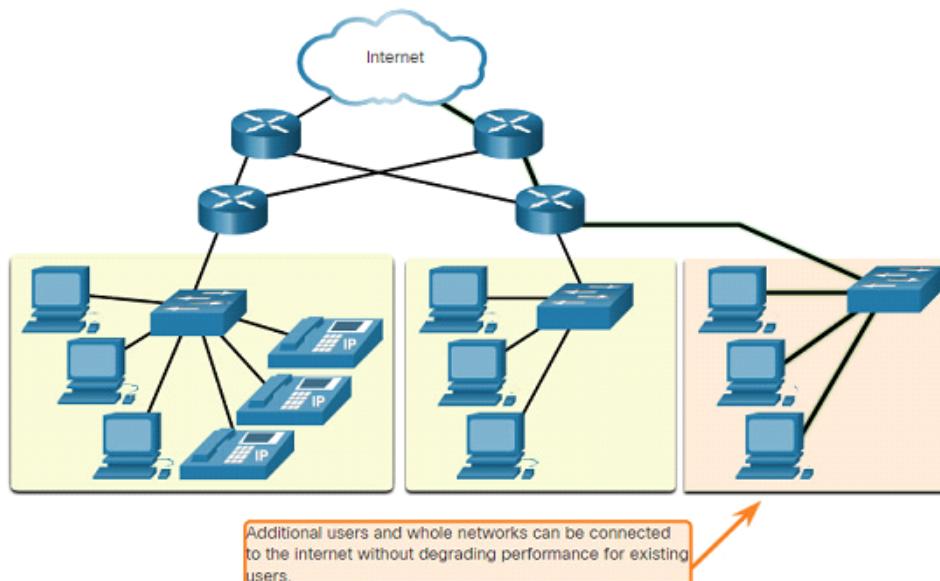
A medida que las redes evolucionan, hemos aprendido que hay cuatro características básicas que los arquitectos de redes deben abordar para cumplir con las expectativas del usuario.

- Tolerancia a fallos.
- Escalabilidad.
- Calidad de Servicio (QoS)
- Seguridad.

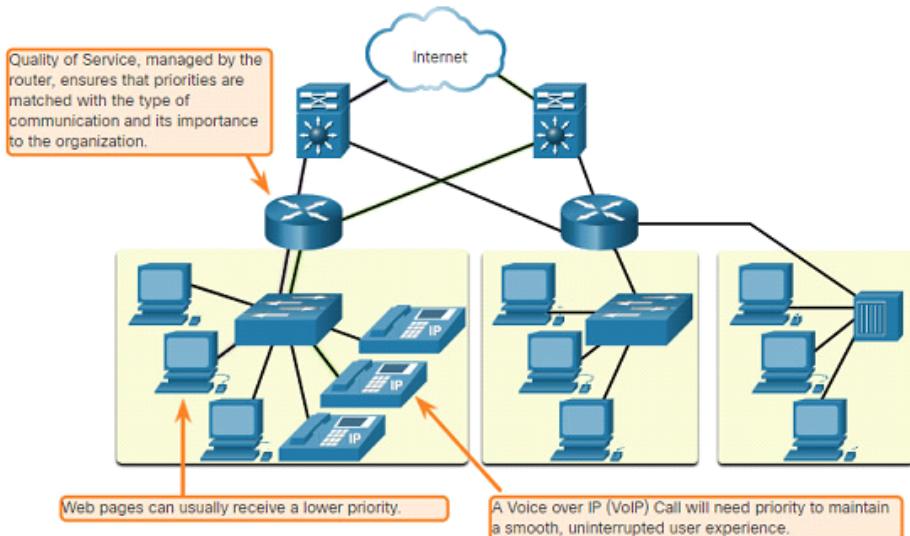
Una red tolerante a fallas es aquella que limite la cantidad de dispositivos afectados durante la falla. Si falla una ruta, los mensajes se envían a través de una ruta alterna. Tener múltiples rutas a un destino se conoce como redundancia.



Una red escalable, se expande rápidamente para admitir nuevos usuarios y aplicaciones sin denigrar el rendimiento de los usuarios existentes.

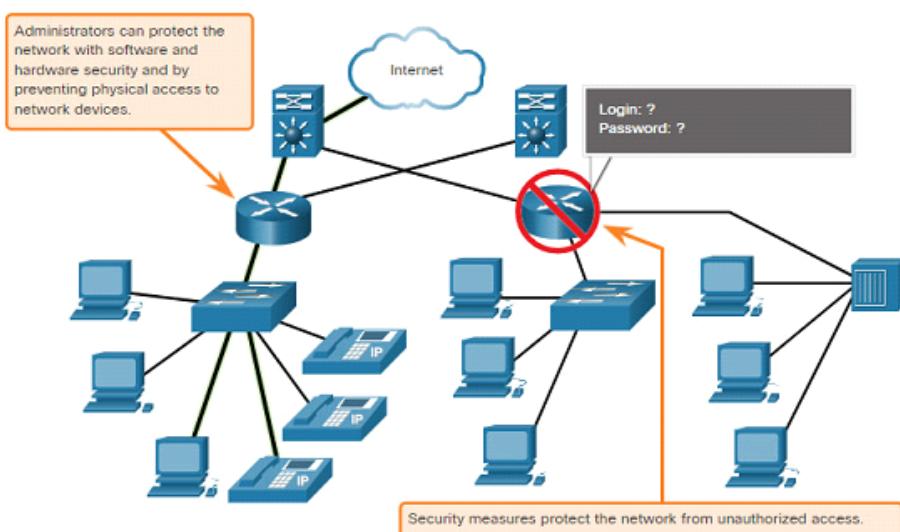


La calidad de servicio (QoS) es un requisito creciente de las redes. Se deben evitar las congestiones y la pérdida de datos para asegurar una conexión exitosa para lograr una buena experiencia de usuario.



Los administradores de red deben abordar dos tipos de problemas de seguridad de red cruciales:

- Seguridad de la infraestructura de red.
- Seguridad de la información que viaja en la red.



Para garantizar estos, hay tres requisitos principales:

- Confidencialidad: Acceso autorizado a los datos y la información.
- Integridad: Información no alterada en su transmisión.

- Disponibilidad: Acceso oportuno y confiable de la información.

### Tendencias de red

Las tendencias recientes de red indican que existen variedad de Inclinaciones de redes que afectan a las organizaciones y a los consumidores:

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

#### Traiga su propio dispositivo (BYOD)

BYOD permite a los usuarios finales la libertad de usar herramientas personales para acceder a la información y comunicarse a través de una red de negocios o campus.

BYOD significa cualquier dispositivo, con cualquier titularidad, utilizado en cualquier lugar.

#### Colaboración en línea

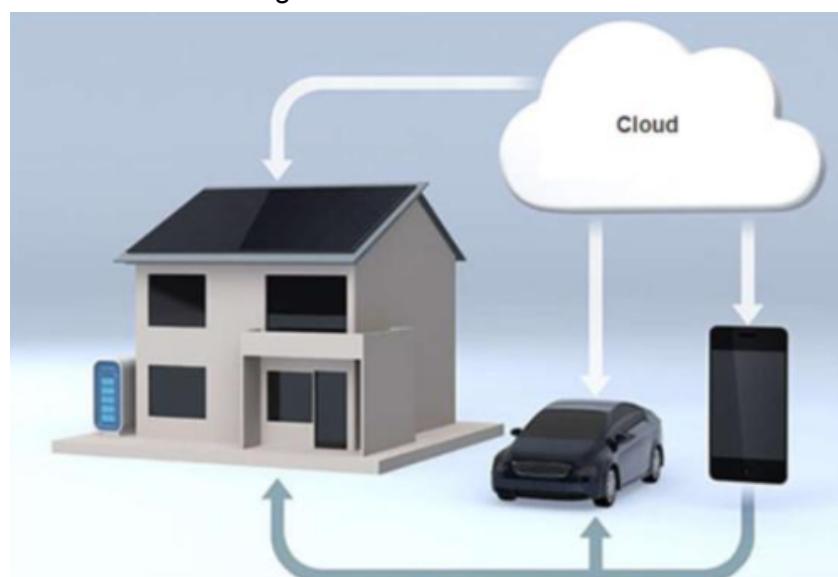
Hay diversas herramientas de colaboración como Cisco WebEx Team, para conectarse en línea y trabajar en un proyecto en conjunto. La colaboración es una prioridad crítica y estratégica que las organizaciones están utilizando para seguir siendo competitivas.

#### Computación en la nube

La computación en la nube marca tendencia, ya que es utilizada por usuarios normales o por empresas. Esto amplía la capacidad de TIs sin requerir inversión en nueva infraestructura. Estos servicios están disponibles a pedido y se entregan económicamente a cualquier dispositivo.

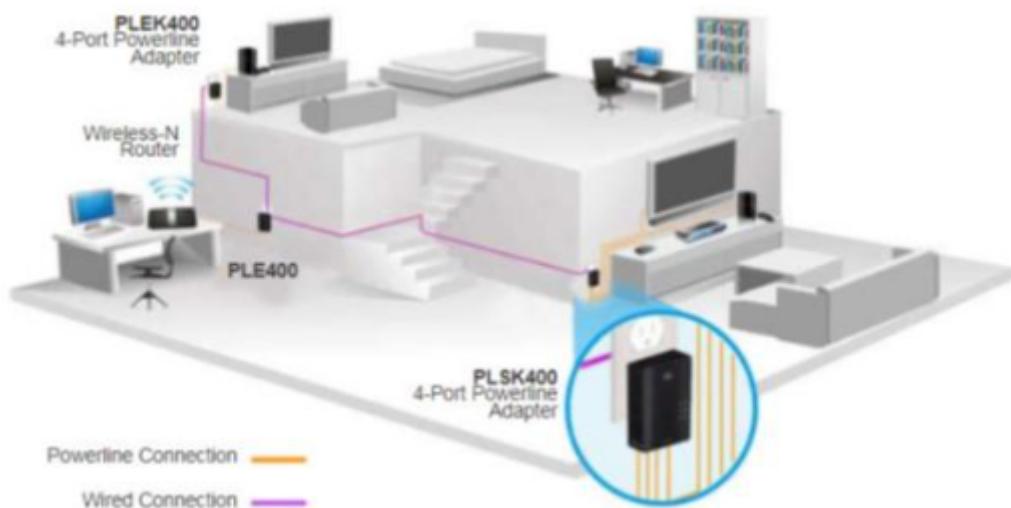
#### Tendencias tecnológicas en el hogar

La tecnología inteligente para el hogar se integra en los electrodomésticos de todos los días, que luego pueden conectarse con otros dispositivos para hacer que los electrodomésticos sean más “inteligentes”.



## Redes de línea eléctrica

La red Powerline para redes domésticas utiliza el cableado eléctrico existente para conectar dispositivos, como se muestra en la figura.



## Banda ancha inalámbrica

- Proveedor de servicios de Internet inalámbrico  
Un proveedor de servicios de Internet inalámbrico (WISP) es un ISP que conecta a los suscriptores a un punto de acceso designado o punto caliente utilizando tecnologías inalámbricas similares que se encuentran en las redes de área local inalámbricas (WLAN)
- Servicio de banda ancha inalámbrica  
Otra solución inalámbrica para el hogar y las pequeñas empresas es la banda ancha inalámbrica como se muestra en la figura:



## **Seguridad de la red**

### Amenazas de seguridad

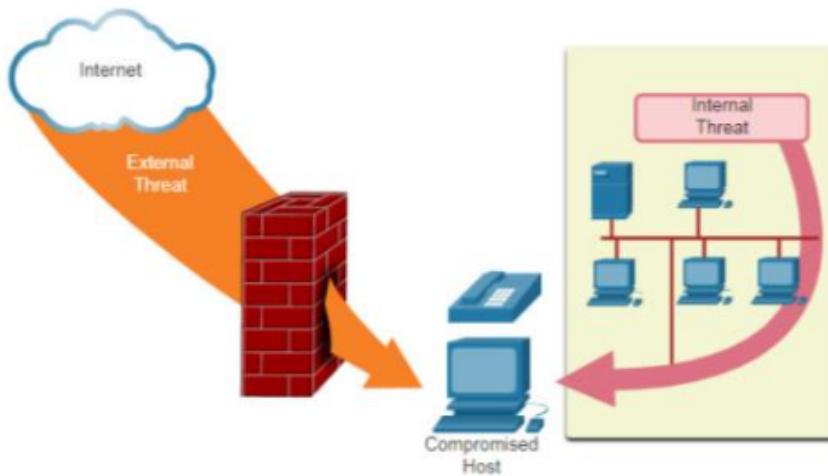
Existen varias amenazas externas comunes a las redes:

- Virus, Gusanos y caballos de Troya.

- Spyware y adware.
- Ataques de día cero.
- Amenaza de ataques de actores.
- Robo de identidad.
- Ataques de denegación de servicio.

También es importante aclarar que existen amenazas internas atribuidas a:

- Dispositivos perdidos o robados.
- Mal uso accidental por parte de los empleados.

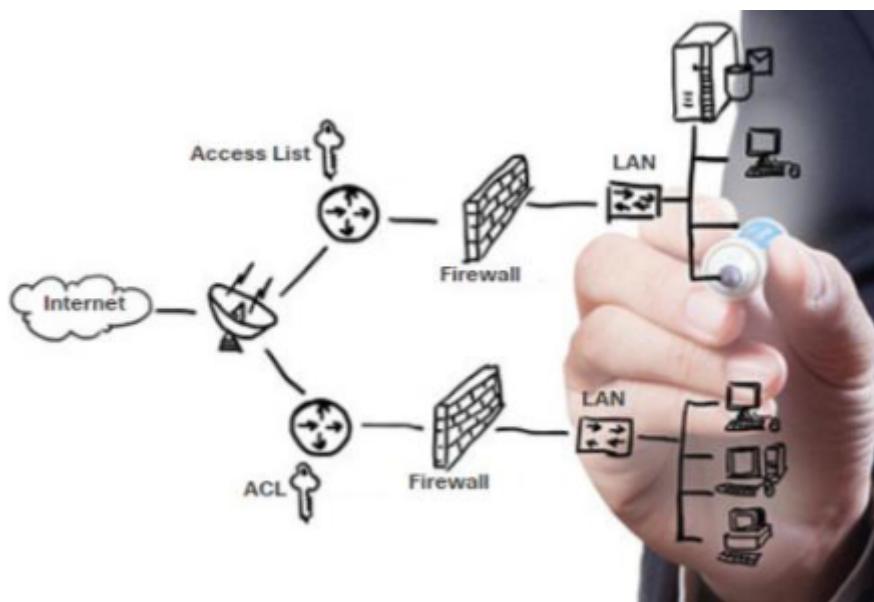


## Soluciones de seguridad

Estos son los componentes básicos de seguridad para una red doméstica o de oficina pequeña:

- Antivirus o antispyware.
- Filtrado de firewall (bloquea accesos no autorizados)
- Sistemas de firewall dedicados.
- Listas de control de acceso (ACL)
- Sistemas de prevención de instrucciones (IPS)
- Redes privadas virtuales (VPN)

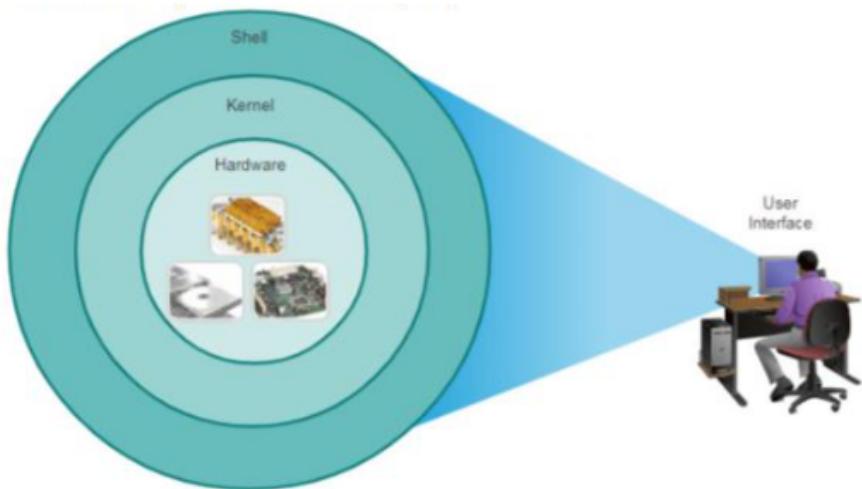
Los requisitos de seguridad de la red deben tener en cuenta el entorno, así como las diversas aplicaciones y los requisitos informáticos. Además, la solución de seguridad implementada debe ser adaptable a las tendencias crecientes y cambiantes de la red.



## Redes - Segundo documento

### **Sistemas operativos**

Todos los dispositivos finales y dispositivos de red requieren un sistema operativo (SO). El usuario va a interactuar con la shell a través de una interfaz gráfica de usuario (GUI) o una línea de comandos (CLI).



- Cáscara - Shell
- Núcleo - Kernel
- Hardware

La CLI requiere muy poca sobrecarga para funcionar. Para esto se necesita conocimiento del sistema.

```
analyst @ secOps
Descargas de escritorio lab.support.files second_drive
[ analyst @ secOps ~ ] $
```

### **Interfaz gráfica de usuario (GUI)**

Una GUI como Windows, macOS, Linux KDE o Android le permite al usuario interactuar con el sistema utilizando un entorno de iconos, gráficos y menús. Cisco utiliza Cisco Internetwork Operating System, que es un firmware.

Estos sistemas permiten:

- Usar un mouse para hacer selecciones.
- Ingresar un texto y comandos.
- Ver salida en un monitor.

### **Métodos de acceso**

Diversos métodos de acceso al SO:

- Consola: Este es un puerto de administración física que proporciona acceso fuera de banda a un dispositivo Cisco. (Acceso a través de un canal de administración dedicado)
- Shell seguro (SSH): Es un método recomendado y en banda para establecer de forma remota una conexión CLI, a través de una interfaz virtual.
- Telnet: Es un método inseguro en banda para establecer de forma remota una sesión CLI, a través de una interfaz virtual. No es una conexión encriptada.)

### **Programas de emulación terminal**

Estos programas permiten conectar un dispositivo a una red a través de una conexión de tipo SSH o una de puerto de consola.

Ejemplos:

- Putty.
- TeraTerm.
- SecureCRT.

## Navegación en Cisco IOS

Este tiene dos modos de comando para el acceso de administración:

- Exec de usuario: Este modo tiene capacidades limitadas pero es útil para operaciones básicas. Solo permite un número limitado de comandos de monitoreo básico.
- Exec privilegiado: Permite el acceso a todos los comandos y funciones. El usuario puede usar cualquier comando de monitoreo. Se identifica con #.

## Modos de configuración y subconfiguración

Para configurar un dispositivo se debe acceder con modo de configuración global. Este se debe realizar desde la navegación de Exec privilegiado.

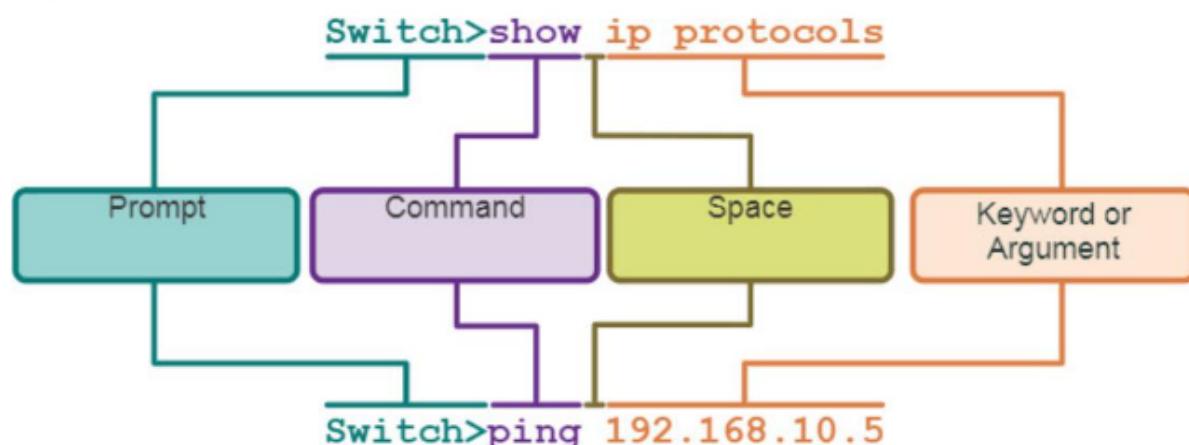
Dos tipos de modos comunes de subconfiguraciones son:

- Modo de configuración de línea: se utiliza para configurar el acceso a la consola, SSH, Telnet o AUX.
- Modo de configuración de interfaz: se utiliza para configurar un puerto de commutador o una interfaz de red de enrutador.

-Ver video de Modos de Comandos principales de la CLI de IOS-

## Estructura básica del comando IOS

Es un dispositivo que admite muchos comandos. Cada comando IOS tiene un formato específico, o sintaxis, y solo se puede ejecutar en el modo apropiado. La sintaxis general para un comando, es el comando seguido de cualquier palabra clave y argumentos apropiados.



Se da de la forma: PALABRA CLAVE - ARGUMENTO.

## **Funciones de Ayuda de IOS**

Se usa para la ayuda sensible el signo de interrogación. Esto nos dice los comandos disponibles en cada tipo de función.

Luego tenemos la verificación de comandos que nos ayudan para ver el argumento que debe llevar cada uno.

## **Direcciones IP**

El uso de direcciones IP es el medio principal para permitir que los dispositivos se ubiquen entre sí y establezcan una comunicación de extremo a extremo en Internet. Cada dispositivo final en una red debe configurarse con una dirección IP. El uso de las direcciones IP se refiere a los protocolos IPv4 e IPv6.

IPv4 → Necesita Máscara de Subred (valor de 32 bits que diferencia la porción de red de la dirección de la porción del host).

IPv6 → Tienen 128 bits de longitud escrita como hexadecimales.

## **Fundamentos de comunicaciones**

Origen del mensaje: Remitente

Destino del mensaje: Receptor

Canal: Medio por el que viaja el mensaje desde el origen al destino.

## **Protocolos de Comunicación**

Los envíos del mensaje se rigen por reglas llamadas protocolos.

Estos, comúnmente incluyen los siguientes requisitos:

- Codificación de mensajes: Los bits de información se codifican para que el host receptor los decodifique.
- Formato y encapsulación de mensajes: Según el tipo de red en el que se envíe (patrón de sonidos, ondas de luz o impulsos eléctricos)
- Tamaño del mensaje: Los mensajes de información no deben ser enormes.
- Tiempo de mensaje: Es el proceso de administrar la tasa de transmisión de datos.
- Opciones de entrega de mensajes: Unicast (1 dispositivo final) - Multicast (1 o más dispositivos finales) - Difusión (Todos los dispositivos finales)

## **Protocolos de comunicaciones de Red:**

Estos protocolos permiten que dos o más dispositivos se comuniquen a través de una o más redes.

TCP → Protocolo de control de transmisión

HTTP → Protocolo de transferencia de hipertexto

### **Protocolos de seguridad de red**

Estos protocolos se utilizan para cifrar los datos y proporcionar autenticación y seguridad.

SSL → Secure Sockets Layer

SSH → Secure Shell

TLS → Transport Layer Security

### **Protocolos de enrutamiento**

Estos protocolos permiten a los enrutadores intercambiar información de ruta, comparar información y luego seleccionar la mejor ruta a la red de destino.

OSPF → Open Shortest Path Fist

BGP → Border Gateway Protocol

### **Protocolos de descubrimiento de servicios**

Estos protocolos se utilizan para la detección automática de dispositivos o servicios.

DHCP → Configuración dinámica de host (Descubre direcciones de IP)

DNS → Sistema de nombres de dominio (Realiza traducciones de nombres a direc.IP)

**Direccionamiento:** Identifica al remitente y al destinatario previsto del mensaje utilizando un esquema de direccionamiento.

**Fiabilidad:** Esta función proporciona mecanismos de entrega garantizados en caso de que los mensajes se pierdan o se corrompan en tránsito.

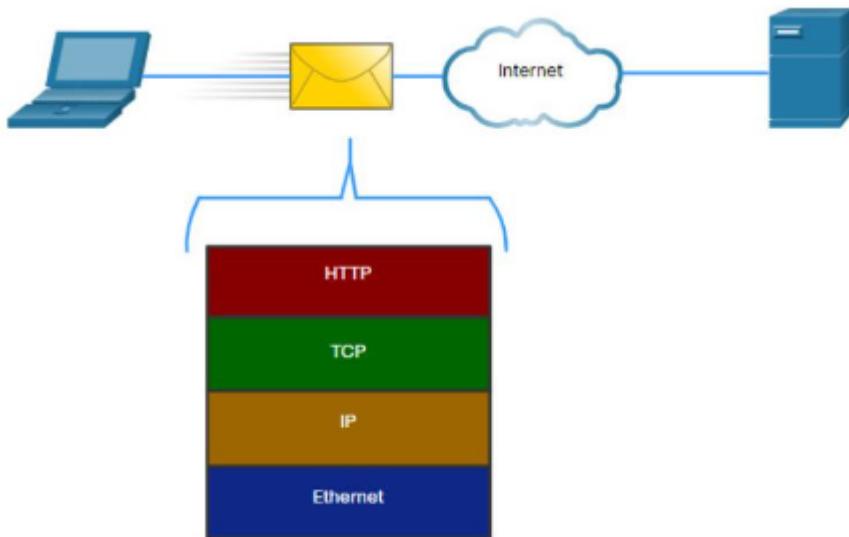
**Control de Flujo:** Esta función asegura que los datos fluyan a una velocidad eficiente entre dos dispositivos de comunicación.

**Secuenciación:** Esta función etiqueta de forma única cada segmento de datos transmitido.

**Detección de errores:** Esta función se utiliza para determinar si los datos se corrompieron durante la transmisión. Estos incluyen Ethernet, IPv4, IPv6 y TCP.

**Interfaz de Aplicación:** Los protocolos HTTP o HTTPS se utilizan para comunicarse entre los procesos web del cliente y del servidor.

## Interacción del Protocolo



Se pueden utilizar varios protocolos al mismo tiempo, en este caso se utilizan:

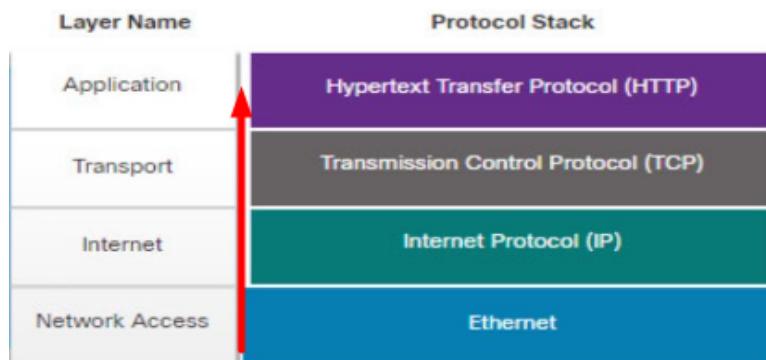
**HTTP:** Este protocolo rige la forma en que interactúan un servidor web y un cliente web. Define el contenido y el formato de las solicitudes.

**TCP:** Este protocolo gestiona las conversaciones individuales. TCP es responsable de garantizar la entrega confiable de la información.

**Protocolo de Internet IP:** Es responsable de entregar mensajes del remitente al receptor. Lo utilizan los enruteadores para reenviar los mensajes.

**Ethernet:** Este protocolo es responsable de la entrega de mensajes de una NIC a otra NIC en la misma red local (LAN) Ethernet.

Estos protocolos funcionan como pilas. Una pila de protocolos muestra cómo se implementan dentro de una SUITE. Estos se ven en términos de capas y cada servicio del nivel superior depende de los niveles inferiores. Las inferiores se ocupan de mover datos mientras que las superiores del contenido del mensaje que se envía.



- **Conjunto de protocolo estándar abierto:** Gratuito para el público.
- **Conjunto de protocolos basados en estándares:** Aprobado por los estándares de una organización.

### **Beneficios de usar un modelo en capas**

- Ayuda en el diseño de protocolos porque operan en una capa específica y tienen información definida sobre las otras capas.
- Proporcionan un lenguaje en común entre las capas.

Para describir las operaciones de red se utilizan dos modelos:

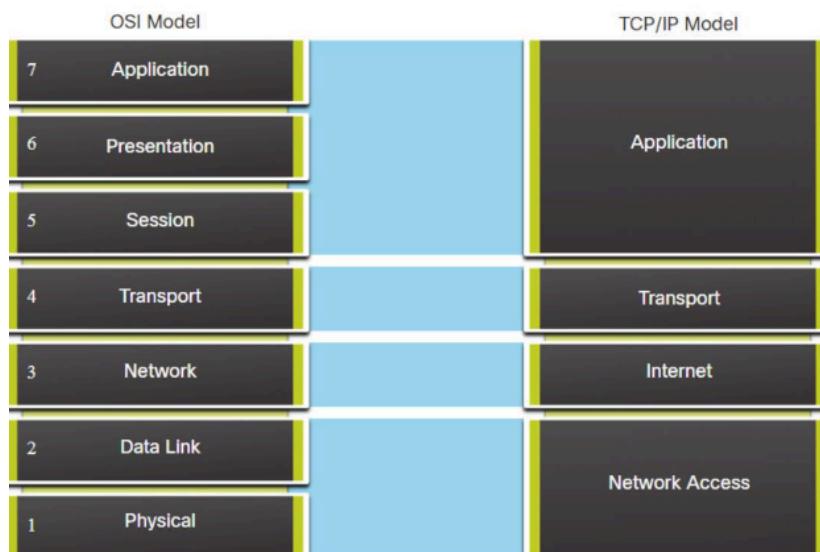
- OSI
- TCP/IP

### **Modelo de referencia OSI por capas**

1. Físico: Sirve para activar y desactivar conexiones físicas.
2. Enlace de datos: Intercambiar tramas de datos entre dispositivos.
3. Red: Intercambiar datos individuales entre dispositivos finales.
4. Transporte: Segmentar, transferir y reensamblar datos para las comunicaciones individuales.
5. Sesión: Organizar su diálogo y gestionar el intercambio de datos.
6. Presentación: Representación común de los datos.
7. Aplicación: Comunicaciones de proceso a proceso.

### **Modelo de Protocolo TCP / IP**

1. Acceso a la red: Controla hardware y los medios que componen la red.
2. Internet: Determina la mejor ruta a través de la red
3. Transporte: Admite la comunicación entre varios dispositivos a través de diversas redes.
4. Aplicación: Representa datos al usuario, además de codificación y control de diálogo.



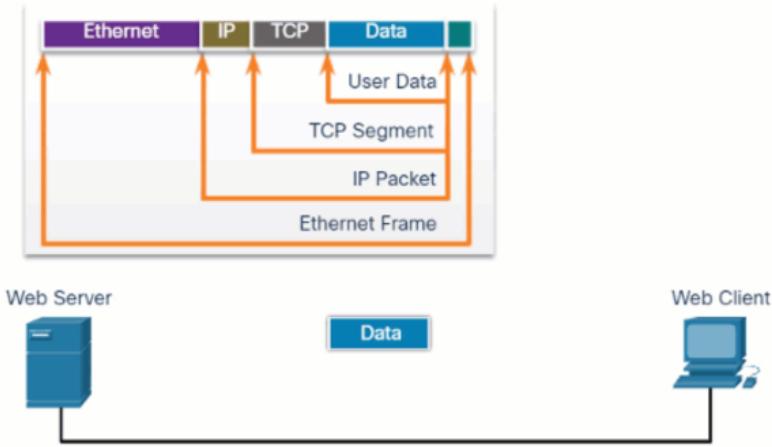
## Segmentar mensajes

Las ventajas de segmentar los mensajes son:

- Aumentar la velocidad: los grandes flujos de datos se segmentan en paquetes para intercalar muchas conversaciones diferentes en la red. **MULTIPLEXACIÓN**.
- Aumentar la eficiencia: si un paquete falla, solamente ese paquete no llega a destino, en lugar de retransmitir todo el flujo se retransmite ese solo.

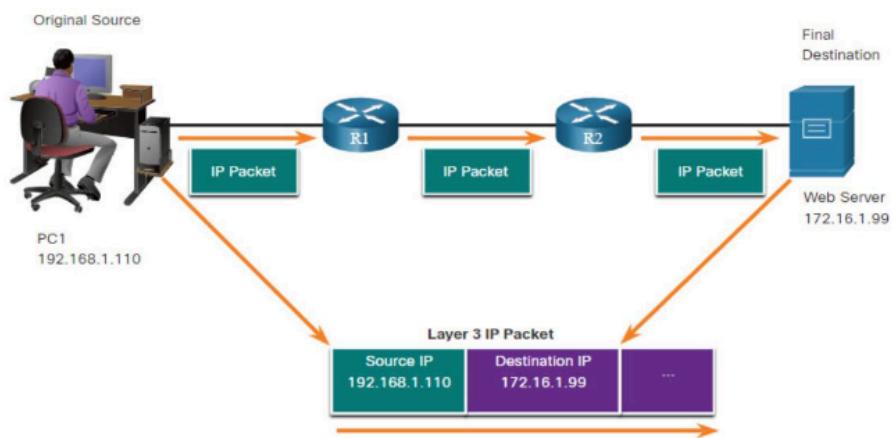
## Secuenciación

El protocolo TCP es responsable de secuenciar los segmentos individuales.

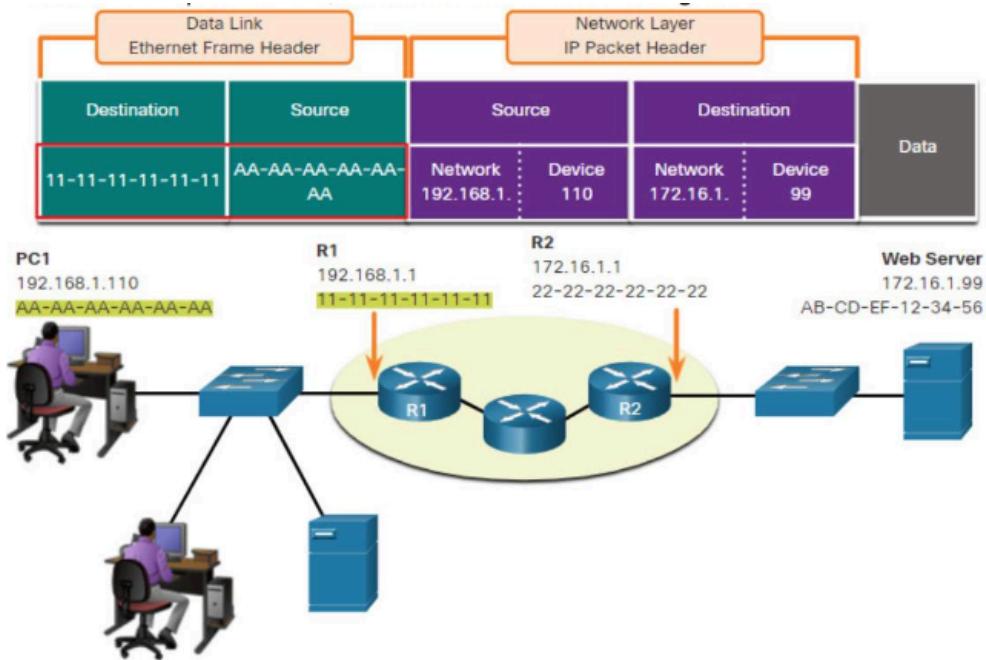


## Dirección lógica de capa 3

Es una dirección que se utiliza para entregar el paquete IP desde la fuente original hasta el destino.



## Papel de las direcciones de la capa de enlace de datos



## Capa física y la conexión física

Ya sea que se conecte a una impresora local en el hogar o un sitio web en otro país, antes de que se produzca cualquier comunicación de red, se debe establecer una conexión física a una red local.

Ejemplo:

Router inalámbrico: Presente en todos los hogares, permiten tanto conexión por cable como conexión inalámbrica.

## Capa física OSI

Proporciona los medios para transportar los bits que componen una trama de capa de enlace de datos a través de los medios de red. Lo hace a través de la codificación de fotogramas que crean señales eléctricas/ópticas/de radio que representan los bits.

Esto hace que abordemos tres áreas funcionales:

- Componentes físicos.
- Codificación: Proceso para convertir un flujo de bits de datos en un “código” (Grupo de bits).
- Señalización: Señales que representan “1” y “0” en los medios.

## Banda ancha

La transferencia de datos generalmente se analiza en términos de ancho de banda. Esta es la capacidad a la que un medio puede transportar datos.

- Latencia: Cantidad de tiempo para que los datos viajen.
- Rendimiento: medida de transferencia de bits a través de los medios.
- Goodput: datos transferidos en un periodo de tiempo determinado.

### **Cableado de cobre**

El cableado de cobre es el tipo de cableado más común utilizado en las redes en la actualidad. Los datos se transmiten como pulsos eléctricos.

Estos pulsos pueden ser alterados por:

- Interferencias electromagnéticas (EMI). (Corrompen señales)
- Diafonía. (Campos eléctricos)

Para contrarrestar estos efectos negativos, los cables están envueltos en blindajes metálicos y requieren conexiones a tierra.

### **Par trenzado sin blindaje**

El cableado de par trenzado sin blindaje (UTP) es el medio de red más común. Utiliza los conectores RJ-45.

Propiedades: Cancelación - Variación del número de giros por par de cables.

### **Par trenzado blindado**

El par trenzado blindado (STP) proporciona una mejor protección contra el ruido. Como el cable UTP, este utiliza también los conectores RJ-45.

### **Cable coaxial**

El cable coaxial se utiliza para transmitir señales electrónicas. Este tiene un aislamiento de plástico flexible. El material aislante está envuelto en una trenza de cobre tejida que utiliza como escudo.

### **Fibra Óptica**

Es un cableado costoso pero transmite datos a largas distancias, además es inmune a EMI y RFI. Se utiliza en la actualidad como cableado de punto a punto.

## **Resumen 4 falta terminar —**

### **Direcciones binarias e IPv4**

- El sistema de numeración binaria consta de 1s y 0s, llamados bits.
- Cada octeto contiene 8 bits (o 1 byte) separados por un punto.

### **Direcciones MAC e IPv6**

Direcciones MAC → Hexadecimales

Direcciones IPv6 → Hexadecimales (128bits)

Son las direcciones de capa 2 que representan una identidad (lo tienen todos los dispositivos de red).

### **Capa de enlace de datos**

Es la capa responsable de las comunicaciones entre las tarjetas de interfaz de red del dispositivo final.

- Permite que los protocolos de capa superior accedan a los medios de capa física.
- La capa de enlace de datos consta de dos subcapas
  - Control de enlaces lógicos (LLC): Se usa para comunicar entre capas. Conecta con la capa 3.

- Control de acceso a medios (MAC): Encapsula los datos. Conecta con la capa 1.

Los estándares IEEE 802 LAN/MAN son específicos para el tipo de red.

802.3 → Ethernet

802.11 → WLAN

802.15 → WPAN

### **El router realiza cuatro funciones básicas**

- Acepta una trama del medio de red.
- Desencapsula la trama para exponer el paquete encapsulado.
- Vuelve a encapsular el paquete en una nueva trama.
- Reenvía la nueva trama en el medio del siguiente segmento de red.

### **Topologías Físicas y Lógicas**

La topología de una red es la disposición y relación de los dispositivos de red, y las interconexiones entre ellos.

- Físicas: muestra las conexiones físicas y como están conectados los dispositivos.
- Lógica: identifica las conexiones virtual entre los dispositivos (Ejemplo: Dirección IP)

### **Topología WAN**

Existen tres tipos de topologías físicas comunes:

- Punto a punto: Enlace permanente entre dos puntos finales.
- Hub and spoke: similar a una topología en estrella donde un sitio central interconecta sitios de sucursal.
- Malla: proporciona alta disponibilidad pero requiere que cada sistema final esté conectado a cualquier otro sistema final.

### **Topologías LAN**

Se conectan mediante estrella o estrella extendida. (fáciles de usar e instalar)

- Bus: Todos los sistemas se encadenan entre sí. (Poco utilizado)
- Anillo: Se conecta con los dispositivos vecinos para formar un anillo.

### **Comunicación dúplex medio y completo**

semiduplex → redes inalámbricas (WLAN y topologías de bus heredadas)

duplex completo → los switches ethernet funcionan en este modo, reciben y transmiten simultáneamente.

### **Métodos de control de acceso**

#### Acceso basado en la contención CSMA/CD

Todos los nodos que operan en semiduplex, compiten por el uso del medio.

- Utilizan LAN Ethernet heredadas.
- Utiliza una detección de colisión para controlar cuándo pueden enviar un dispositivo y qué sucede si varios dispositivos envían al mismo tiempo.

Si hay colisión se espera un tiempo y se retransmite los datos.

## Acceso basado en la contención CSMA/CA

Funciona en modo semiduplex, donde se \*\*\*COMPLETAR\*\*\*

### **La trama de enlace de datos**

La trama se compone en tres partes:

- Encabezado: Campos de control e identificación de encapsulados (capa 3).
- Datos: Lleva la data.
- Tráiler: Detecciones de errores y final de la trama.

### **Direcciones de Capa 2 - Redes locales**

- También se conoce como la dirección física.
- Contenido en el encabezado de la trama
- Se utiliza para la entrega local de la trama.

### **Tramas LAN y WAN**

Tipos de protocolos de enlace

- Frame-Relay
- Point-to-Point
- Ethernet
- 802.11 inalámbrico

### **Subcapa MAC**

#### IEE 802.3

Trama de Ethernet: Esta es la estructura interna de la trama Ethernet.

Direccionamiento Ethernet: Incluye una dirección MAC de origen para entregar el mensaje en la misma LAN.

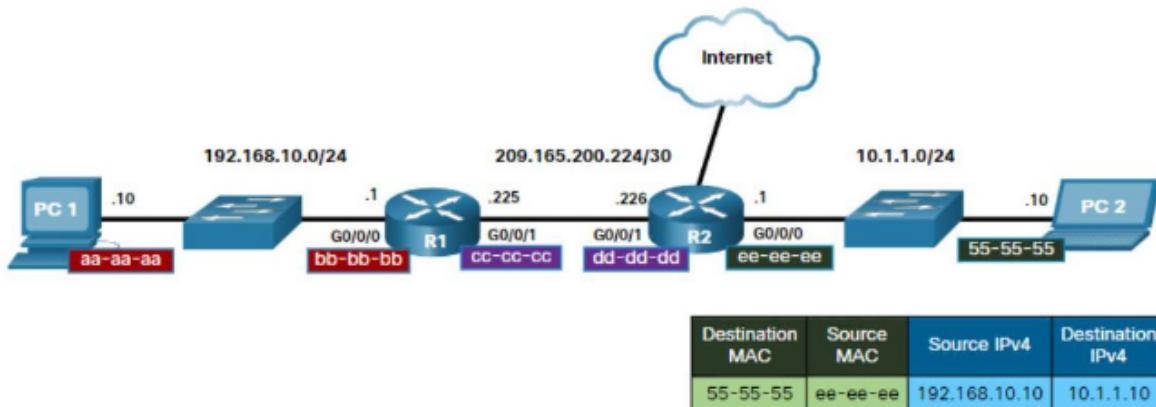
Detección de errores Ethernet: incluye remolques de secuencia.

#### Acceso a los medios:

La subcapa MAC se encarga de decodificar

**— Completar —**

## Destino en red remota



## ARP

Este protocolo sirve para asociar las direcciones IP de los paquetes IP en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta al destino.

Para los paquetes IPv4, esto se realiza mediante un proceso denominado Protocolo de resolución de direcciones (ARP).

Para enviar paquetes resuelve a través de una tabla buscando direcciones IPv4 y direcciones IPv4 correspondientes.

Para ver la tabla se utiliza arp -a en el CMD.

Los posibles problemas que puede tener la ARP son:

- ARP spoofing para realizar un ataque de envenenamiento. Agregar a la tabla ARP la dirección de un hacker.

## Mensajes de descubrimiento de vecinos IPv6

ARP → IPv4

ICMPv6 → IPv6

Realizan los siguientes servicios:

- Mensaje de solicitud
- Mensaje de anuncio
- Mensaje de solicitud de enrutador
- Mensaje de anuncio de enrutador
- Mensaje de redirección

## — Comandos para configurar routers con interfaces —

### Puerta de enlace predeterminada

Se usa cuando un host envía un paquete a otro dispositivo en OTRA red.

En general, la dirección de la puerta de enlace generalmente es la dirección de la interfaz del router.

Un comutador que interconecta las computadoras suele ser un dispositivo de Capa 2.

## Porciones de red y host

- ¿Cómo se compone una red IPv4? 32bits porción de red - porción de host
- ¿Qué determina la máscara de subred? porción de red - porción de host
- la longitud del prefijo es el número de bits establecido en 1
- unicast - transmisión de un dispositivo a otro dispositivo
- broadcast - transmisión a todos menos al origen
- multicast - transmisión a varios dispositivos pero no a todos - streaming
- anycast - comparte misma dirección y elige uno
- RFC 1918 → IPv4 públicas se enrutan globalmente entre routers
- ISP → proveedores de servicios de internet
- las ipv4 privadas NO se enrutan globalmente
- NAT → traduce direcciones ipv4 públicas a privadas y al revés
- NAT → traducción de direcciones de red
- loopback → se utiliza en un host para probar si TCP/IP está operativo
- 127.0.0.1 → localhost
- APIPA → direccionamiento IP privado automático → 169.254.x.x/16
- APIPA → direcciones autoasignadas
- APIPA → se usa cuando no estamos conectados a nada
- RFC 790 → direccionamiento por clases
- RFC 790 → desperdicia muchas direcciones IP
- RIR → asignan direcciones IP
- IANA → asigna direcciones IP por bloque de países
- DHCP → protocolo de detección
- cada subred es un dominio del broadcast
- router → corta dominios del broadcast
- crear más dominios → subneteo
- subneteo → menos tráfico de red (es bueno)
- broadcast → ocurre porque no se sabe el destino
- se limita el broadcast de capa 2
- broadcast trabaja en la red LAN
- subred por ubicación / función / tipo de dispositivo
- cada subred puede tener una directiva de seguridad
- subred → física
- subneteo → logica / virtual
- muchas tablas complicadas
- siempre la de mayor cantidad de host, es la primera subred
  
- direccionamiento ipv6
- el ipv4 se queda sin direcciones → se inventa ipv6
- las ipv6 tiene 128 bits de espacio de direcciones
- técnicas de migración: dual stack, tunneling y translation
- dual stack: se ejecutan las dos pilas de protocolos ipv4 e ipv6
- tunneling: el paquete ipv6 se encapsula en ipv4 y se transmite en red ipv4
- translation: traduce ipv4 a ipv6 (nat64)
- direcciones ipv6 → hexteto
- es x:x:x:x:x:x:x ( x → 4 valores hexadecimales)
- el 0 adelante no se escribe (00a → a)

- el **0000** → se puede escribir como **0**
- los **dos puntos dobles ::** pueden reemplazar cualquier cadena unica

- **Unicast** → 1 a 1
- **multicast** → varios destinos
- **anycast** → broadcast de ipv4
- **prefijo 64 bits — interface ID 64 bits**
- **SLAAC** → ID de interfaz de 64 bits

- **Direcciones publicas GUA (enrutables a través de internet)**
- **global routing prefix + subnet id -> primeros 64 bits**
- **Link-local Address (LLA) (no son enrutables, son de capa 3)**
- **comandos**

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
R1(config)# interface gigabitethernet 0/0/0
R1 (config-if) # ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

- **mensajes RS y RA**
- **EI RS → host a router**
- **EI RA →router a host**
- **metodos para configurar GUA IPv6: SLAAC, SLAAC Stateless, statefull**
- **Prefijo → viene en el FromRA Message**

- **módulo 14: capa de transporte**

- función de la capa de transporte:**

- la capa de transporte es la **responsable de comunicaciones lógicas** entre aplicaciones que se ejecutan en diferentes hosts

- Enlaza las capas de aplicación y las capas inferiores que se encargan de la transmisión a través de la red. **Gestiona las sesiones que se abren.**

**Tareas:**

- seguimiento de conversaciones

- segmentación de datos

- agregar información de encabezado

- utiliza segmentación y multiplexación

- multiplexación → agregar en un mismo canal varias conversaciones

**Protocolos:**

- TCP y UDP

- Especifican cómo transferir mensajes entre hosts

- TCP provee confiabilidad y control de flujo de operaciones básicas

- TCP fragmenta data y en el destino se reconstruye

- UDP → streaming de video

- UDP → es un protocolo sin conexión

- UDP → protocolo de mejor esfuerzo porque no hay reconocimiento en el destino

**Características de tcp:**

- establece una sesión entre dispositivos de origen y destino

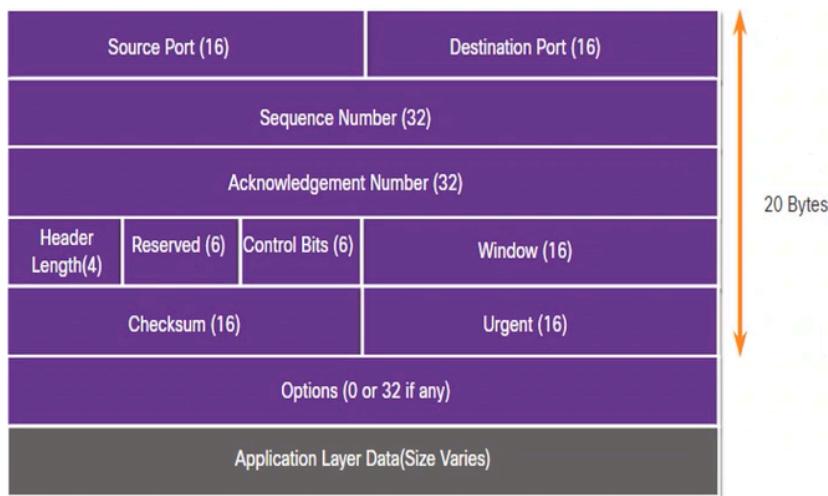
- garantiza una entrega confiable

- proporciona entrega en el mismo pedido

- admite control de flujo: puede solicitar que la aplicación reduzca la velocidad del flujo de datos

## encabezado de tcp

es un protocolo con estado, lo que significa que realiza un seguimiento del estado sesión de comunicación



## Aplicaciones que utilizan TCP

Maneja todas las tareas asociadas con la división del flujo de datos en segmentos, proporcionando confiabilidad, controlando el flujo de datos y reordenando segmentos.

TCP → HTTP, FTP, SMTP, SSH

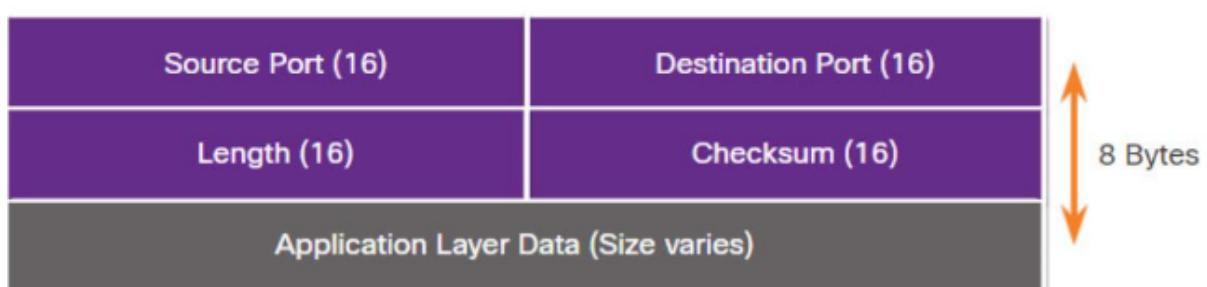
## Características UDP:

se reconstruyen los datos

UDP es un protocolo sin estado

No se rastrea el estado de la sesión de comunicación

La aplicación controla el protocolo de transporte.



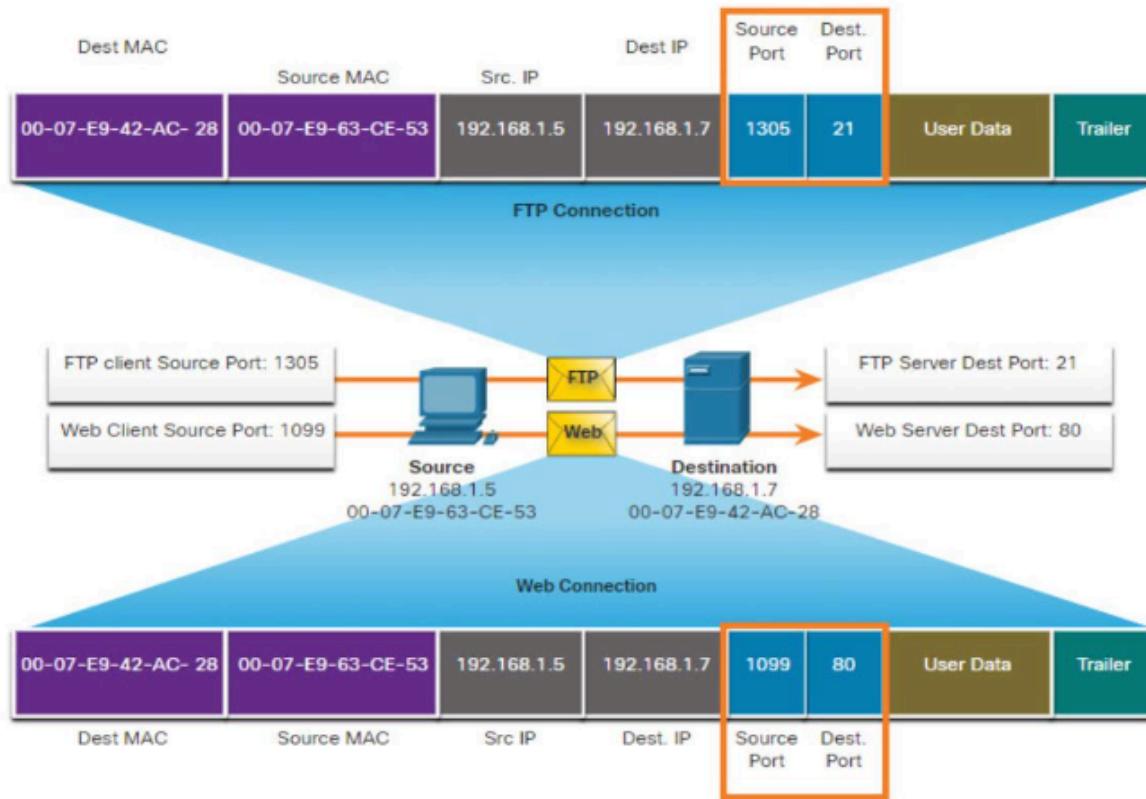
## Aplicaciones que utilizan UDP:

Aplicaciones de vídeo en directo y multimedia

Aplicaciones sencillas de solicitud y respuesta

Aplicaciones que control la confiabilidad en si misma

## Pares de Socket



Los sockets permiten que los diversos procesos que se ejecuten en un cliente se distingan entre sí.

**Se conoce como socket a la combinación de dirección de IP de origen y número de puerto de origen.**

**Grupos de números de puertos:**

**1 a 1023 PUERTOS BIEN CONOCIDOS**

**1024 A 49151 PUERTOS REGISTRADOS**

**49152 A 65535 PUERTOS PRIVADOS O DINÁMICOS**

**netstat** → comando para verificar conexiones.

**proceso de comunicación en TCP**

- Un servidor individual no puede tener dos servicios asignados al mismo número de puerto.
- Una aplicación de servidor activa asignada a un puerto específico se considera abierta.
- toda solicitud entrante de un cliente direccionada al socket es aceptada y los datos se envían a la aplicación del servidor.

**conexiones → saludos**

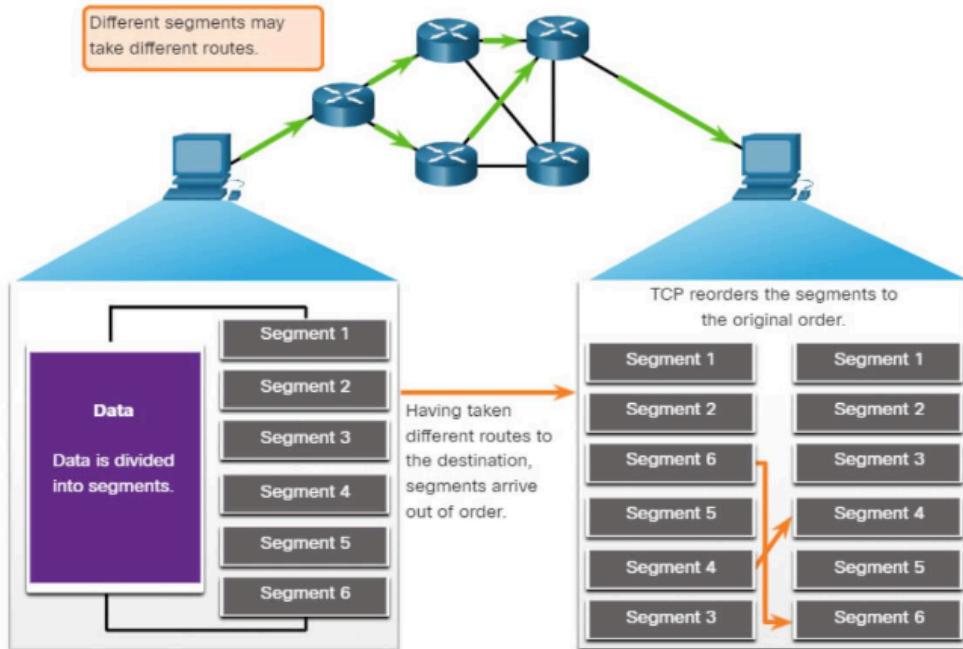
saludo de 3 vías:

- establece que el dispositivo esté presente en la red

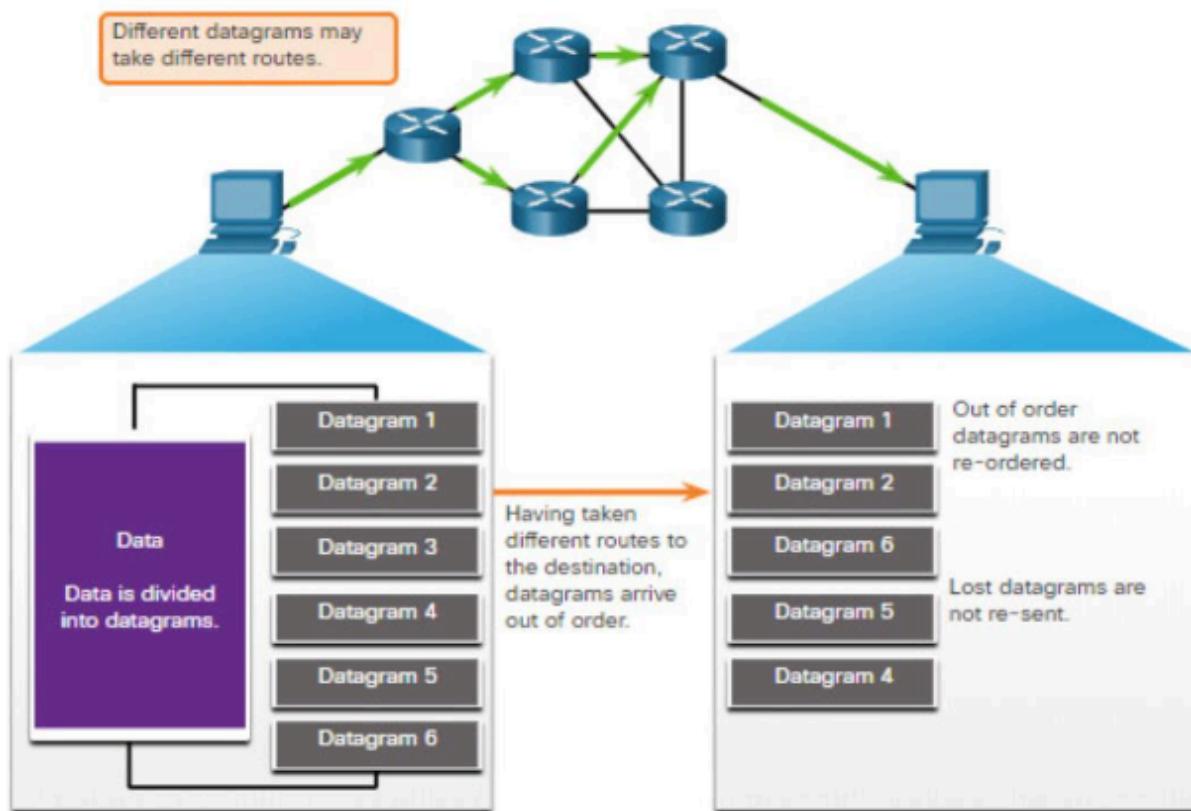
- verifica si tiene algún servicio activo
- informa que el dispositivo destino intenta establecer una comunicación en dicho puerto

## Comunicación TCP

**Los segmentos TCP se reordenan en el destino**



## Rearmado de datagramas UDP



## **NO SE ORDENAN EN EL DESTINO**

**El servidor del servicio de usuario de acceso telefónico de autenticación remota (RADIUS) proporciona la autenticación, la autorización y los servicios de contabilidad para manejar el acceso del usuario. La operación de RADIUS está fuera del alcance de este curso.**

**RADIUS es un componente esencial en la seguridad y gestión de acceso de muchas redes modernas, proporcionando un marco robusto para autenticar y autorizar usuarios y dispositivos, así como para monitorear y registrar su actividad.**

### **Capa de Aplicación y sesión**

Las tres capas superiores del modelo OSI (aplicación, presentación y sesión) .

La capa de presentación se encarga del formato de los datos (formatos de archivo).

La capa de sesión maneja intercambio de información para iniciar los diálogos y mantenerlos activos.

### **Protocolos de capa de Aplicación de TCP/IP**

#### **DNS: Sistema de nombres de dominio**

TCP, UDP

Traduce los nombres de dominio tales como “cisco.com” a direcciones IP

#### **Modelo cliente-servidor**

- Los procesos de cliente y servidor se consideran parte de la capa de **aplicación**.
- En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”
- Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores.

#### **Redes punto a punto**

Redes que utilizamos que comparten internet o impresora sin tener un servidor dedicado.

#### **Aplicaciones punto a punto**

Una aplicación P2P permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación.

Algunas aplicaciones P2P utilizan un sistema híbrido en el que cada par accede a un servidor de índice para obtener la ubicación de un recurso almacenado en otro par.

Las redes P2P comunes incluyen las siguientes:

- BitTorrent
- Conexión Directa
- eDonkey
- Freenet

### **Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto**

Cuando se escribe una dirección web o un localizador uniforme de recursos (URL) en un navegador web, el navegador establece una conexión con el servicio web. **HTTP**

- GET, POST y PUT
- se cifra el flujo de datos con Secure Socket Layer (SSL) antes de transportarse en la red (pasa a ser HTTPS)

### **Protocolos de correo electrónico**

#### **SMTP, POP e IMAP**

- **IMAP es un protocolo que describe un método para recuperar mensajes**

#### **DNS**

El protocolo DNS convierte un nombre de dominio ejemplo (cisco.com) en una dirección IP 198.133.219.25.

#### **DHCP**

El protocolo DHCP del servicio IPv4 automatiza la asignación de direcciones IPv4, máscaras de subred, puertas de enlace y otros parámetros de red IPv4.

**pool** → 192.168.1 (50 a 100) (rango CIDR)

### **Protocolo de transferencia de archivos**

El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una computadora cliente y se utiliza para insertar y extraer datos en un servidor FTP.

#### **SMB**

se utiliza para:

- iniciar o terminar sesiones
- controlar el acceso a los archivos y a las impresoras
- autorizar una aplicación para enviar o recibir mensajes.

#### **Seguridad**

- Robo de información.
- Pérdida y manipulación de datos
- Robo de identidad (Spoofing de MAC)
- Interrupción del servicio (DoS)

### **Seguridad física**

- Amenazas de hardware.
- Amenazas eléctricas.
- Amenazas de mantenimiento.

### **Tipos de cortafuegos**

- Filtrado de paquetes
- Filtrado de aplicaciones
- Filtrado URL
- Inspección de paquetes con estado (SPI)

### **Cisco AutoSecure**

- Habilitar SSH