Unidad 1 – Modelos de Referencia OSI y TCP/IP

Juan Manuel Hurtado Angulo, MsC

Programa de Ingeniería de sistemas

Introducción

Debido al incremento de las redes la ISO Organización internacional de normalización, investigo la necesidad de crear un modelo de red para ayudar a los constructores a implementarlas y facilitar la comunicación y el trabajo entre ellas.

Protocolo

Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Los protocolos son implementados por dispositivos finales y dispositivos intermediarios en software, hardware o ambos. Cada protocolo de red tiene su propia función, formato y reglas para las comunicaciones.

Fuente: Introduction to Networks [Cisco NetAcad]

Tipos de Protocolos

Tipo de protocolo	Descripción
Protocolos de comunicaciones de red	Los protocolos permiten que dos o más dispositivos se comuniquen a través de uno o más compatibles. La familia de tecnologías Ethernet implica una variedad de protocolos como IP, Protocolo de control de transmisión (TCP), HyperText Protocolo de transferencia (HTTP) y muchos más.
Protocolos de seguridad de red	Los protocolos protegen los datos para proporcionar autenticación, integridad de los datos y Cifrado de datos Ejemplos de protocolos seguros incluyen Secure Shell (SSH), Secure Sockets Layer (SSL) y Capa de transporte Security (TLS).
Protocolos de routing	Los protocolos permiten a los routeres intercambiar información de ruta, comparar ruta y, a continuación, seleccionar la mejor ruta al destino e inalámbrica. Ejemplos de protocolos de enrutamiento incluyen Abrir ruta más corta primero OSPF y Protocolo de puerta de enlace de borde (BGP)
Protocolos de Detección de servicios	Los protocolos se utilizan para la detección automática de dispositivos o servicios. Entre los ejemplos de protocolos de descubrimiento de servicios se incluyen Dynamic Host Protocolo de configuración (DHCP) que descubre servicios para la dirección IP y Sistema de nombres de dominio (DNS) que se utiliza para realizar traducción de nombre a dirección IP.

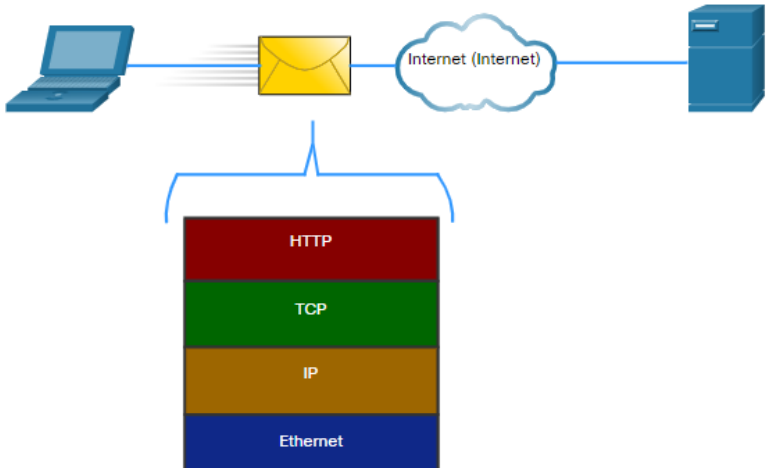
Fuente: Introduction to Networks [Cisco NetAcad]

Funciones del Protocolo de Red

Función	Descripción
Direccionamiento	Esto identifica al remitente y al destinatario previsto del mensaje utilizando un esquema de direccionamiento definido. Ejemplos de protocolos que proporcionan incluyen Ethernet, IPv4 e IPv6.
Confiabilidad	Esta función proporciona mecanismos de entrega garantizados en caso de mensajes se pierden o se corrompen en tránsito. TCP proporciona entrega garantizada.
Control de flujo	Esta función asegura que los datos fluyan a una velocidad eficiente entre dos dispositivos de comunicación. TCP proporciona servicios de control de flujo.
Secuenciación	Esta función etiqueta de forma única cada segmento de datos transmitido. La utiliza la información de secuenciación para volver a ensamblar el informationinformación correctamente correctly. Esto es útil si se pierdan los segmentos de dato, retrasado o recibido fuera de pedido. TCP proporciona servicios de secuenciación.
Detección de errores	Esta función se utiliza para determinar si los datos se dañaron durante de la voz. Varios protocolos que proporcionan detección de errores incluyen Ethernet, IPv4, IPv6 y TCP.
Interfaz de la aplicación	Esta función contiene información utilizada para proceso a proceso comunicaciones entre aplicaciones de red. Por ejemplo, al acceder a una página web, los protocolos HTTP o HTTPS se utilizan para comunicarse entre el cliente y servidor web.

Fuente: Introduction to Networks [Cisco NetAcad]

Interacción de Protocolos



Los protocolos de la figura se describen de la siguiente manera:

- **Protocolo de Transferencia de Hipertexto (HTTP)** - este protocolo de aplicación rige la manera en que interactúan un servidor web y un cliente web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor. Tanto el cliente como el software del servidor web implementan el HTTP como parte de la aplicación. HTTP se basa en otros protocolos para regular la forma en que se transportan los mensajes entre el cliente y el servidor.
- **Protocolo de control de transmisión (TCP)** - Este protocolo administra las conversaciones individuales. TCP se encarga de garantizar la entrega fiable de la información y de gestionar el control de flujo entre los dispositivos finales.
- **Protocolo de Internet (IP)** - Este protocolo es responsable de entregar los mensajes del remitente al receptor. IP es utilizado por los enrutadores para reenviar los mensajes a través de varias redes.
- **Ethernet** - Este protocolo es responsable de la entrega de mensajes de una NIC a otra NIC en la misma red de área local (LAN) Ethernet.

Fuente: Introduction to Networks [Cisco NetAcad]

Evolución de los Protocolos

Desde la década de 1970 ha habido varios conjuntos de protocolos diferentes, algunos desarrollados por una organización de estándares y otros desarrollados por varios proveedores.

Nombre de capa TCP / IP	TCP/IP	ISO	AppleTalk	Novell Netware
Aplicación	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transporte	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Acceso a la red	Ethernet ARP WLAN			

Fuente: Introduction to Networks [Cisco NetAcad]

Evolución de los Protocolos

- **Internet Protocol Suite o TCP/IP** - Este es el conjunto de protocolos más común y relevante que se utiliza hoy en día. El conjunto de protocolos TCP/IP es un conjunto de protocolos estándar abierto mantenido por Internet Engineering Task Force (IETF).
- **Protocolos de interconexión de sistemas abiertos (OSI)** - Esta es una familia de protocolos desarrollados conjuntamente en 1977 por la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT). El protocolo OSI también incluía un modelo de siete capas llamado modelo de referencia OSI. El modelo de referencia OSI categoriza las funciones de sus protocolos. Hoy OSI es conocido principalmente por su modelo en capas. Los protocolos OSI han sido reemplazados en gran medida por TCP/IP.
- **AppleTalk** - Un paquete de protocolos propietario de corta duración lanzado por Apple Inc. en 1985 para dispositivos Apple. En 1995, Apple adoptó TCP/IP para reemplazar AppleTalk.
- **Novell NetWare** - Un conjunto de protocolos propietarios de corta duración y sistema operativo de red desarrollado por Novell Inc. en 1983 utilizando el protocolo de red IPX. En 1995, Novell adoptó TCP/IP para reemplazar a IPX.

Fuente: Introduction to Networks [Cisco NetAcad]

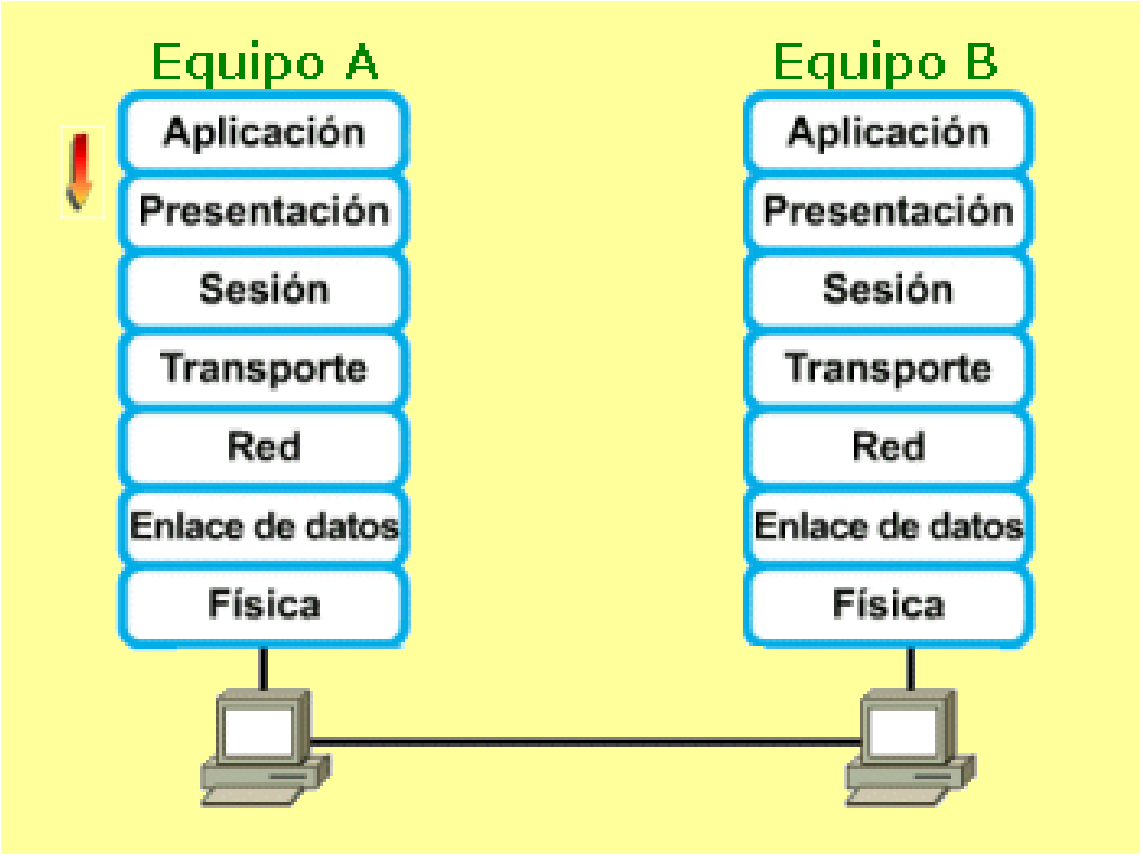
Modelo de referencia OSI

En 1984 fue lanzado el modelo OSI.

capa del modelo OSI	Descripción
7 - Aplicación	La capa de aplicación contiene protocolos utilizados para comunicaciones proceso a proceso. de comunicaciones.
6 - Presentación	la capa de presentación proporciona una representación común de los datos transferido entre los servicios de capa de aplicación.
5 - Sesión	La capa de sesión proporciona servicios a la capa de presentación para Organiza el diálogo y administra el intercambio de datos
4 - Transporte	La capa de transporte define servicios para segmentar, transferir y volver a montar los datos para las comunicaciones individuales entre el final .
3 - Red	La capa de red proporciona servicios para intercambiar las piezas individuales de a través de la red entre los dispositivos finales identificados.
2 - Enlace de datos	Los protocolos de la capa de enlace de datos describen métodos para intercambiar datos. tramas entre dispositivos a través de un medio común
1 - Fisica	Los protocolos de capa física describen los componentes mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para una transmisión de bits hacia y desde una red dispositivo.

Fuente: Introduction to Networks [Cisco NetAcad]

Modelo de referencia OSI



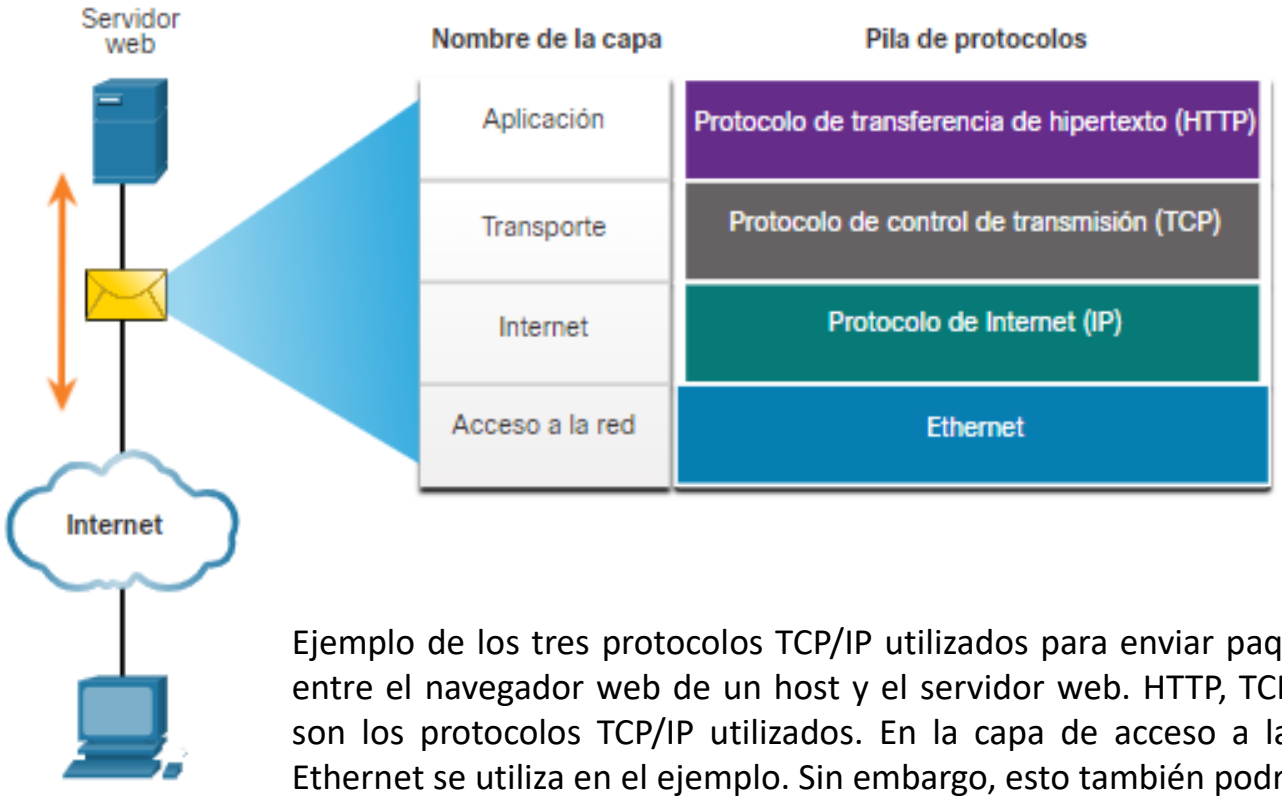
Modelo TCP/IP

El modelo de protocolo TCP/IP para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Este tipo de modelo coincide con precisión con la estructura de una suite de protocolos determinada. El modelo TCP/IP es un protocolo modelo porque describe las funciones que ocurren en cada capa de protocolos dentro de una suite de TCP/IP.

Capa del modelo TCP/IP	Descripción
4 - Aplicación	Representa datos para el usuario más el control de codificación y de diálogo.
3 - Transporte	Admite la comunicación entre distintos dispositivos a través de diversas redes.
2 - Internet	Determina el mejor camino a través de una red.
1 - Acceso a la red	Controla los dispositivos del hardware y los medios que forman la red.

Fuente: Introduction to Networks [Cisco NetAcad]

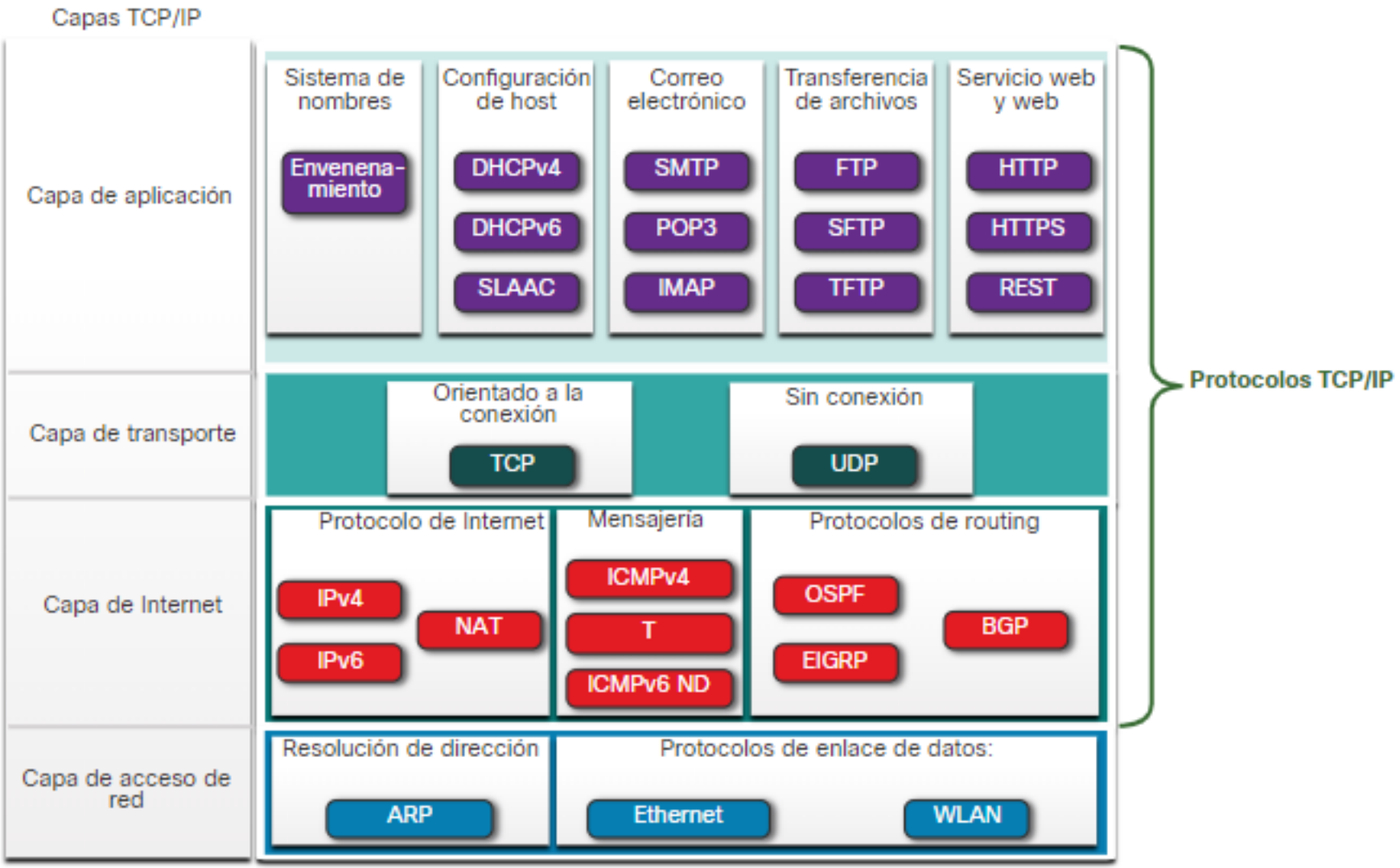
Modelo TCP/IP



Ejemplo de los tres protocolos TCP/IP utilizados para enviar paquetes entre el navegador web de un host y el servidor web. HTTP, TCP e IP son los protocolos TCP/IP utilizados. En la capa de acceso a la red, Ethernet se utiliza en el ejemplo. Sin embargo, esto también podría ser un estándar inalámbrico como WLAN o servicio celular.

Fuente: Introduction to Networks [Cisco NetAcad]

Conjunto de protocolos TCP/IP



Fuente: Introduction to Networks [Cisco NetAcad]

Capa 4: La capa de Aplicación

Sistema de nombres	• **DNS** - Domain Name System. Traduce los nombres de dominio tales como cisco.com a direcciones IP
Configuración de host	• **DHCPv4** - Protocolo de configuración dinámica de host para IPv4. Un servidor DHCPv4 asigna dinámicamente información de direccionamiento IPv4 a clientes DHCPv4 al inicio y permite que las direcciones se reutilicen cuando ya no sean necesarias. • **DHCPv6** - Protocolo de configuración dinámica de host para IPv6. DHCPv6 es similar a DHCPv4. Un servidor DHCPv6 asigna dinámicamente información de direccionamiento IPv6 a clientes DHCPv6 al inicio. • **SLAAC** - Autoconfiguración sin estado. Método que permite a un dispositivo obtener su información de direccionamiento IPv6 sin utilizar un servidor DHCPv6.
Correo electrónico	• **SMTP** - Protocolo para Transferencia Simple de Correo. Les permite a los clientes enviar correo electrónico a un servidor de correo y les permite a los servidores enviar correo electrónico a otros servidores. • **POP3** -Protocolo de Oficinca de Correo versión 3. Permite a los clientes recuperar el correo electrónico de un servidor de correo y descargarlo en la aplicación de correo local del cliente. • **IMAP** - Protocolo de Acceso a Mensajes de Internet Permite que los clientes accedan a correos electrónicos almacenados en un servidor de correo.

Fuente: Introduction to Networks [Cisco NetAcad]

Capa 4: La capa de Aplicación

Transferencia de Archivos

- **FTP** - Protocolo de Transferencia de Archivos. Establece las reglas que permiten a un usuario en un host acceder y transferir archivos hacia y desde otro host a través de una red. FTP Es un protocolo confiable de entrega de archivos, orientado a la conexión y con acuse de recibo.
- **SFTP** - SSH Protocolo de Transferencia de Archivos Como una extensión al protocolo Shell seguro (SSH), el SFTP se puede utilizar para establecer una sesión segura de transferencia de archivos, en el que el archivo transferido está cifrado. SSH es un método para el inicio de sesión remoto seguro que se utiliza normalmente para acceder a la línea de comandos de un dispositivo.
- **TFTP** - Protocolo de Transferencia de Archivos Trivial Un protocolo de transferencia de archivos simple y sin conexión con la entrega de archivos sin reconocimiento y el mejor esfuerzo posible. Utiliza menos sobrecarga que FTP.

Web y Servicio Web

- **HTTP** - Hypertext Transfer Protocol. Un Conjunto de reglas para intercambiar texto, imágenes gráficas, sonido, video y otros archivos multimedia en la World Wide Web.
- **HTTPS** - HTTP seguro. Una forma segura de HTTP que cifra los datos que se intercambian a través de la World Wide Web.
- **REST** - Transferencia de Estado Representacional. Servicio web que utiliza interfaces de programación de aplicaciones (API) y solicitudes HTTP para crear aplicaciones web.

Fuente: Introduction to Networks [Cisco NetAcad]

Capa 3: La capa de Transporte

Se le conoce como la capa host a host.

Orientado a la conexión

- **TCP** - Protocolo de Control de Transmisión. Permite la comunicación confiable entre procesos que se ejecutan en hosts independientes y tiene transmisiones fiables y con acuse de recibo que confirman la entrega exitosa.

Sin conexión

- **UDP** - Protocolo de Datagramas de Usuario Habilita un proceso que se ejecuta en un host para enviar paquetes a un proceso que se ejecuta en otro host Sin embargo, UDP No confirma la transmisión correcta de datagramas

Fuente: Introduction to Networks [Cisco NetAcad]

Capa 2: La capa de Internet

Protocolo de Internet

- **IPv4** - Protocolo de Internet versión 4. Recibe segmentos de mensajes de la capa de transporte, empaqueta mensajes en paquetes y dirige paquetes para entrega end-to-end a través de una red. IPv4 utiliza una dirección de 32 bits.
- **IPv6** - IP versión 6. Similar a IPv4 pero usa una dirección de 128 bits.
- **NAT** - Traducción de Direcciones de Red Traduce las direcciones IPv4 de una red privada en direcciones IPv4 públicas globalmente únicas.

Mensajería

- **ICMPv4** - Protocolo de Control de Mensajes de Internet Proporciona comentarios desde un host de destino a un host de origen con respecto a los errores en la entrega de paquetes
- **ICMPv6** - ICMP para IPv6. Funcionalidad similar a ICMPv4 pero se utiliza para paquetes IPv6.
- **ICMPv6 ND** - Protocolo de Descubrimiento de Vecinos versión 6 Incluye cuatro mensajes de protocolo que se utilizan para la resolución de direcciones y la detección de direcciones duplicadas.

Protocolos de Routing

- **OSPF** - Abrir el Camino más Corto Primero. Protocolo de enrutamiento de estado de vínculo que utiliza un diseño jerárquico basado en áreas. OSPF s un protocolo de routing interior de estándar abierto.
- **EIGRP** - EIGRP Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado. Es un protocolo de routing abierto desarrollado por Cisco, utiliza una métrica compuesta en función del ancho de banda, la demora, la carga y la confiabilidad.
- **BGP** - Protocolo de Puerta de Enlace de Frontera Un protocolo de enrutamiento de puerta de enlace exterior estándar abierto utilizado entre los proveedores de servicios de Internet (ISP). BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de enrutamiento.

Fuente: Introduction to Networks [Cisco NetAcad]

Capa 1: La capa de Acceso a la red

Se le conoce como capa de host a red.

Resolución de dirección

- **ARP** - Protocolo de Resolución de Direcciones Proporciona la asignación de direcciones dinámicas entre una dirección IP y una dirección de hardware.

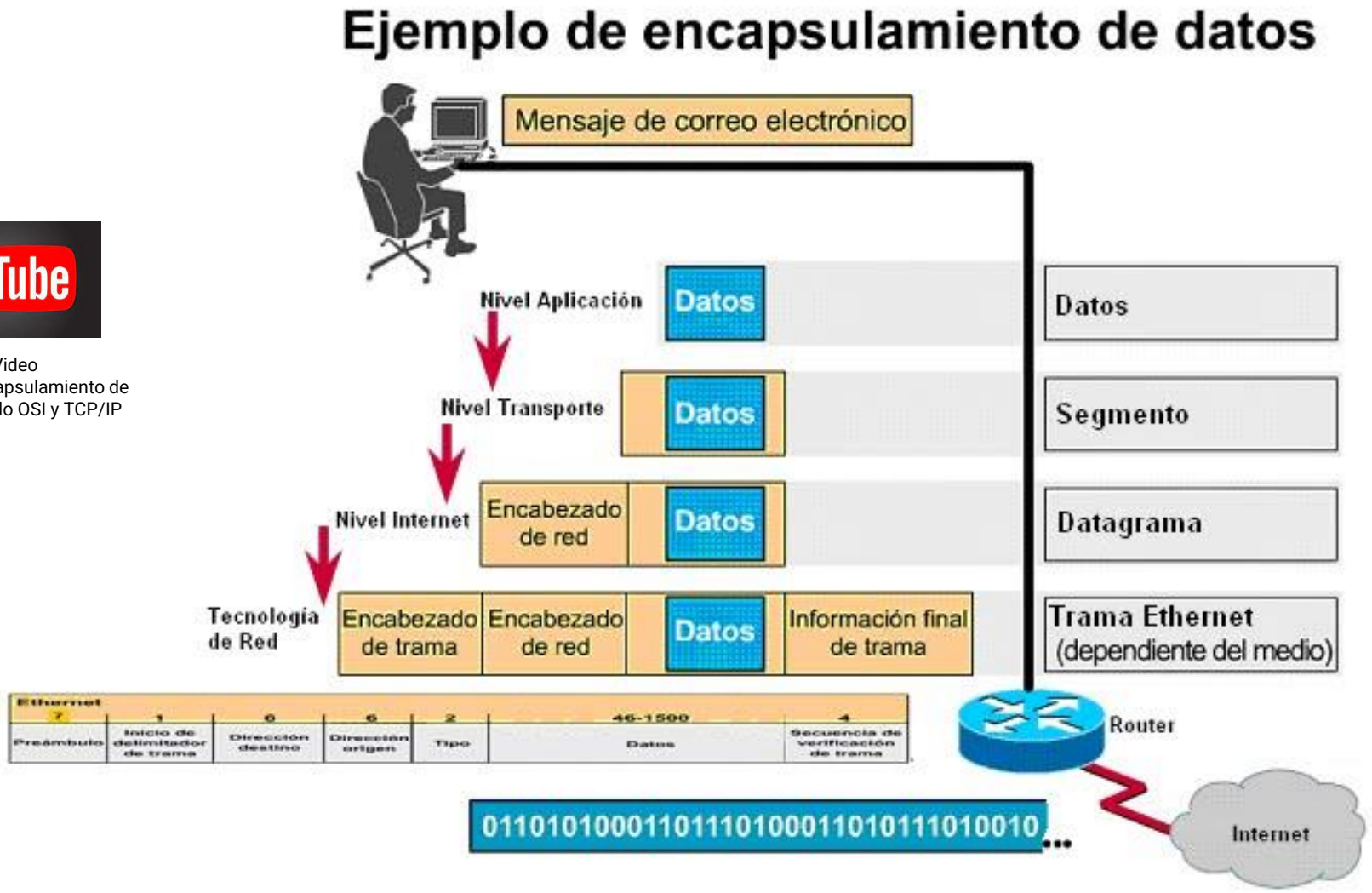
Protocolos de Enlace de Datos:

- **Ethernet** - define las reglas para conectar y señalizar estándares de la capa de acceso a la red.
- **WLAN** - Wireless Local Area Network. Define las reglas para la señalización inalámbrica a través de las frecuencias de radio de 2,4 GHz y 5 GHz.

Fuente: Introduction to Networks [Cisco NetAcad]

Proceso de Comunicación TCP/IP

Ver Video
Proceso de Encapsulamiento de Datos en Modelo OSI y TCP/IP



https://sites.google.com/site/redeslocalesyglobales/_/rsrc/1381508558301/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/4-proceso-de-encapsulacion-de-datos/tcpipencapsula.bmp

Proceso de Comunicación TCP/IP

Segmentación del mensaje

Es el proceso de dividir un flujo de datos en unidades más pequeñas para transmisiones a través de la red.

Aumenta la velocidad

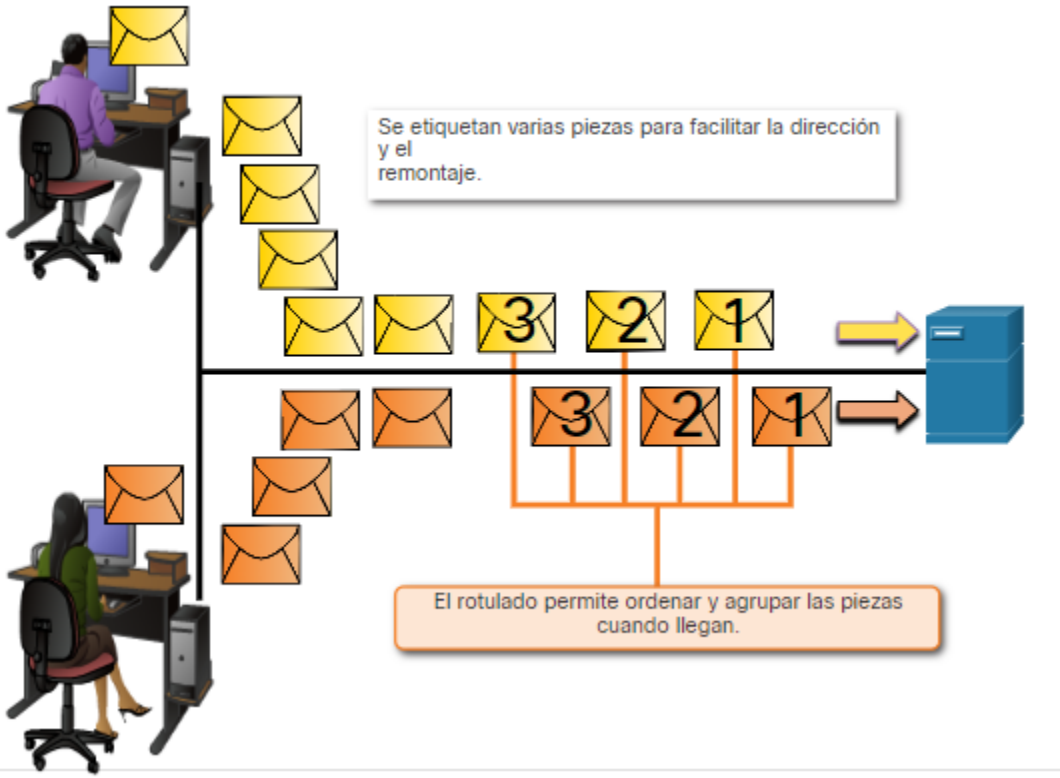
Se pueden enviar grandes cantidades de datos a través de la red sin atar un enlace de comunicaciones. Esto permite que muchas conversaciones diferentes se intercalen en la red llamada multiplexación.

Aumenta la eficiencia

Si un solo segmento no llega a su destino debido a una falla en la red o congestión de la red, solo ese segmento necesita ser retransmitido en lugar de volver a enviar toda la secuencia de datos.

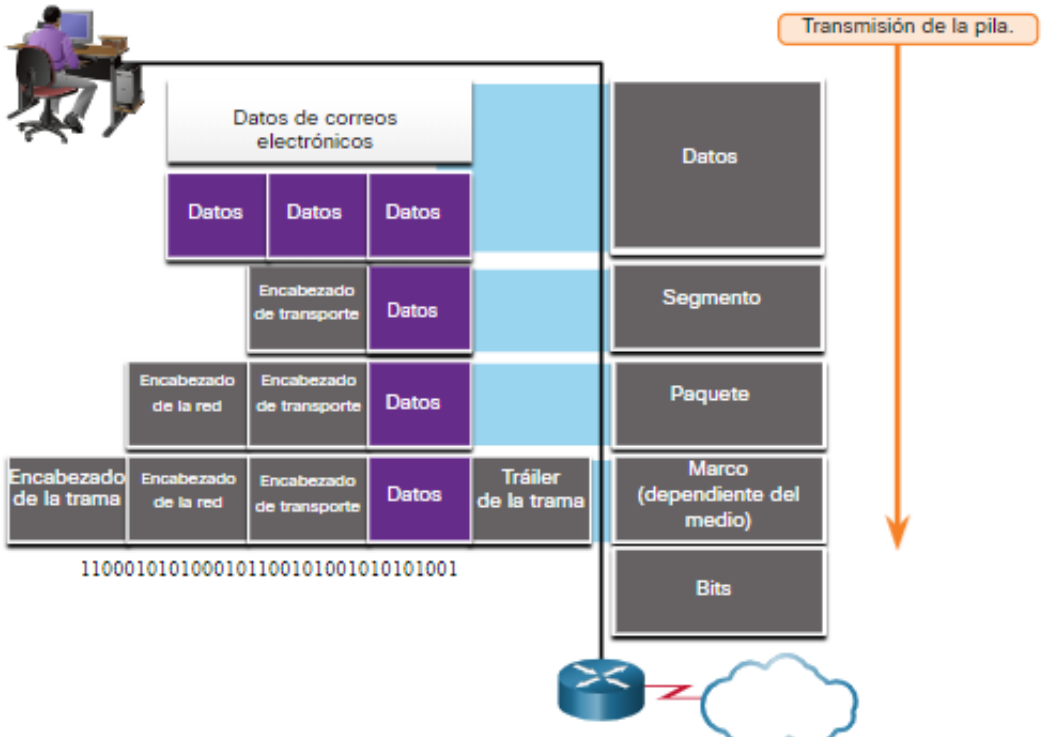
Proceso de Comunicación TCP/IP

Secuenciación



Proceso de Comunicación TCP/IP

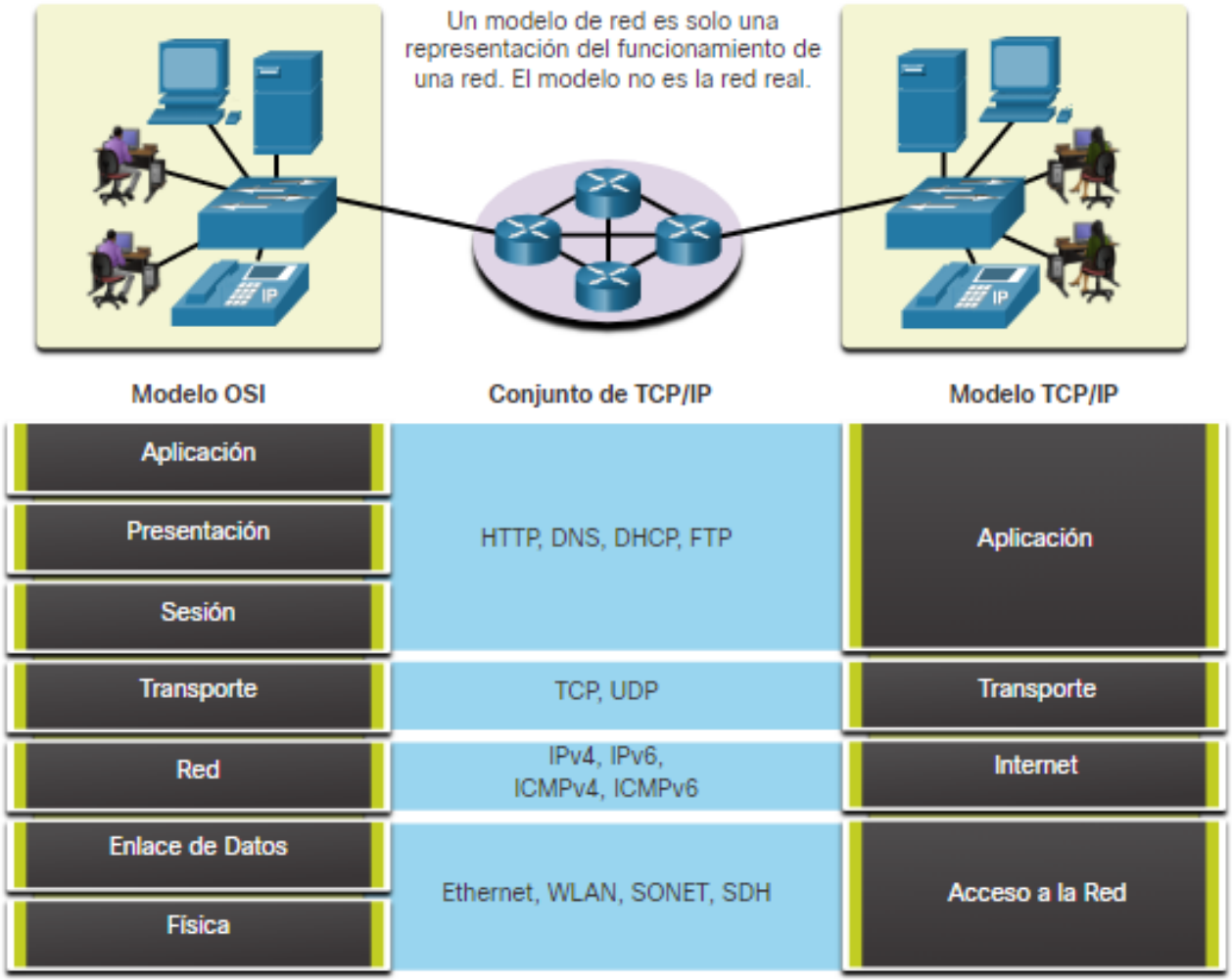
Unidades de datos de protocolo



- Datos: término general que se utiliza en la capa de aplicación para la PDU
- Segmento: PDU de la capa de transporte
- Paquete: PDU de la capa de red
- Trama: PDU de la capa de enlace de datos
- Bits: PDU de capa física que se utiliza cuando se transmiten datos físicamente por el medio

Nota: Si el encabezado de transporte es TCP, entonces es un segmento. Si el encabezado de transporte es UDP, entonces es un datagrama.

Correspondencia de capas Modelos TCP y OSI

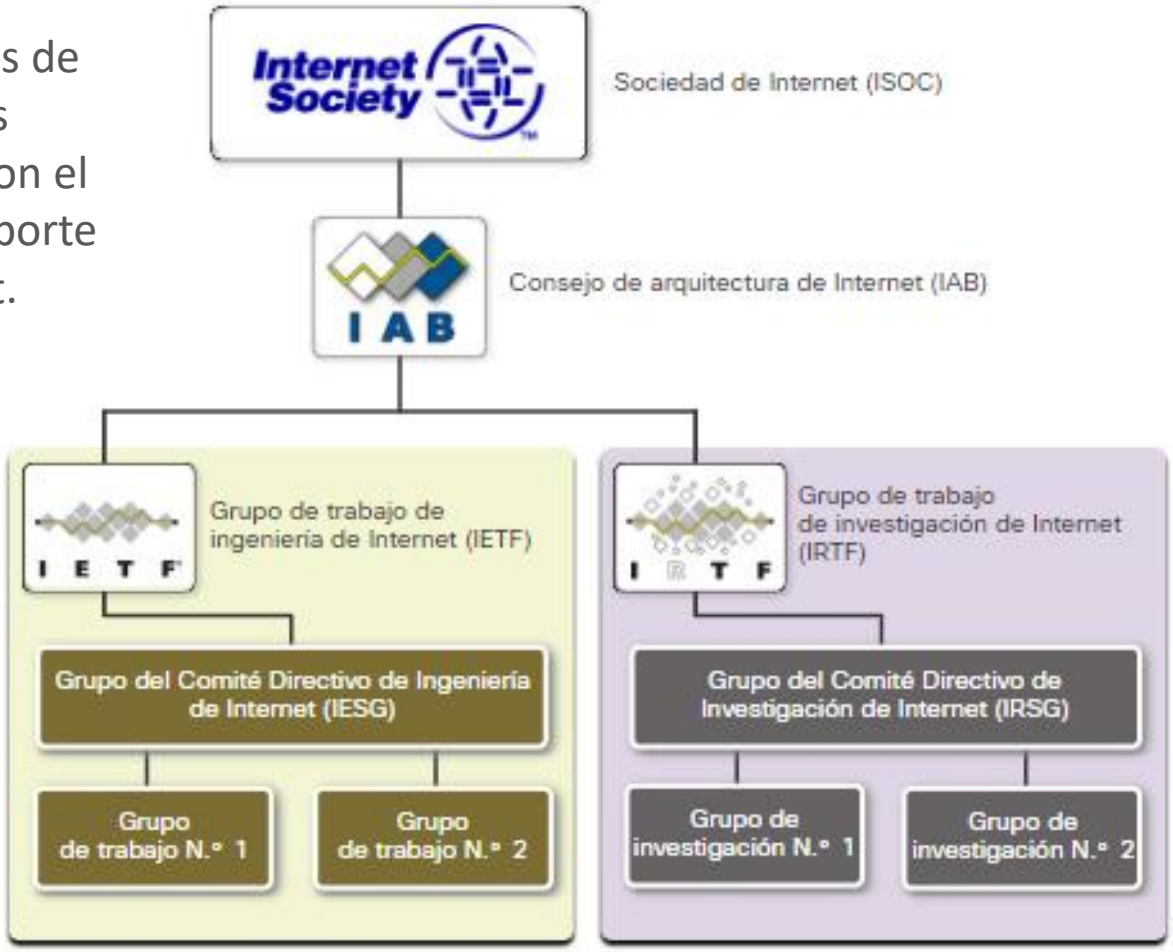


Fuente: Introduction to Networks [Cisco NetAcad]

Organizaciones estándares

Estándares de Internet

Organizaciones de estándares involucradas con el desarrollo y soporte de Internet.



Fuente: Introduction to Networks [Cisco NetAcad]

Organizaciones estándares

Estándares de Internet

- **Sociedad de Internet (ISOC)** - es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo.
- **Consejo de Arquitectura de Internet (IAB)** - es responsable de la administración y el desarrollo general de los estándares de Internet.
- **Grupo de trabajo de ingeniería de Internet (IEFT)** - desarrolla, actualiza y mantiene las tecnologías de Internet y de TCP/IP. Esto incluye el proceso y documentación para el desarrollo de nuevos protocolos y la actualización de los protocolos existentes, conocidos como documentos de petición de comentarios (RFC).
- **Grupo de trabajo de investigación de Internet (IRTF)** - está enfocado en la investigación a largo plazo en relación con los protocolos de Internet y TCO/IP, como los grupos Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG) y Peer-to-Peer Research Group (P2PRG).
- **Corporación de Internet para la Asignación de Nombres y Números (ICANN)** - con base en los Estados Unidos, coordina la asignación de direcciones IP, la administración de nombres de dominio y la asignación de otra información utilizada por los protocolos TCP/IP.
- **Autoridad de Números Asignados de Internet (IANA)** - responsable de supervisar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

Fuente: Introduction to Networks [Cisco NetAcad]

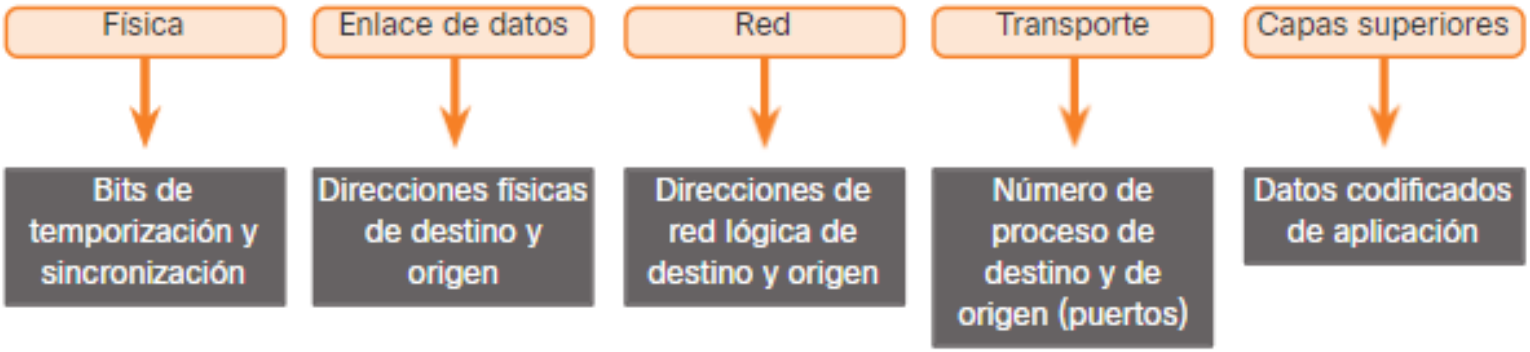
Organizaciones estándares

Organizaciones de estándares para comunicaciones y electrónica

- **Institute of Electrical and Electronics Engineers** (**IEEE**, pronounced "I-triple-E"): organización de electrónica e ingeniería eléctrica dedicada a avanzar en innovación tecnológica y a elaborar estándares en una amplia gama de sectores, que incluyen energía, servicios de salud, telecomunicaciones y redes. Los estándares importantes de red IEEE incluyen 802.3 Ethernet y 802.11 WLAN. Busque en Internet otros estándares de red IEEE.
- **Asociación de Industrias Electrónicas (EIA)**: es conocida principalmente por sus estándares relacionados con el cableado eléctrico, los conectores y los racks de 19 in que se utilizan para montar equipos de red.
- **Asociación de las Industrias de las Telecomunicaciones (TIA)**: es responsable de desarrollar estándares de comunicación en diversas áreas, entre las que se incluyen equipos de radio, torres de telefonía móvil, dispositivos de voz sobre IP (VoIP), comunicaciones satelitales y más. La figura muestra un ejemplo de un cable Ethernet certificado que fue desarrollado cooperativamente por la TIA y la EIA.
- **Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T)**: es uno de los organismos de estandarización de comunicación más grandes y más antiguos. El UIT-T define estándares para la compresión de videos, televisión de protocolo de Internet (IPTV) y comunicaciones de banda ancha, como la línea de suscriptor digital (DSL).

Fuente: Introduction to Networks [Cisco NetAcad]

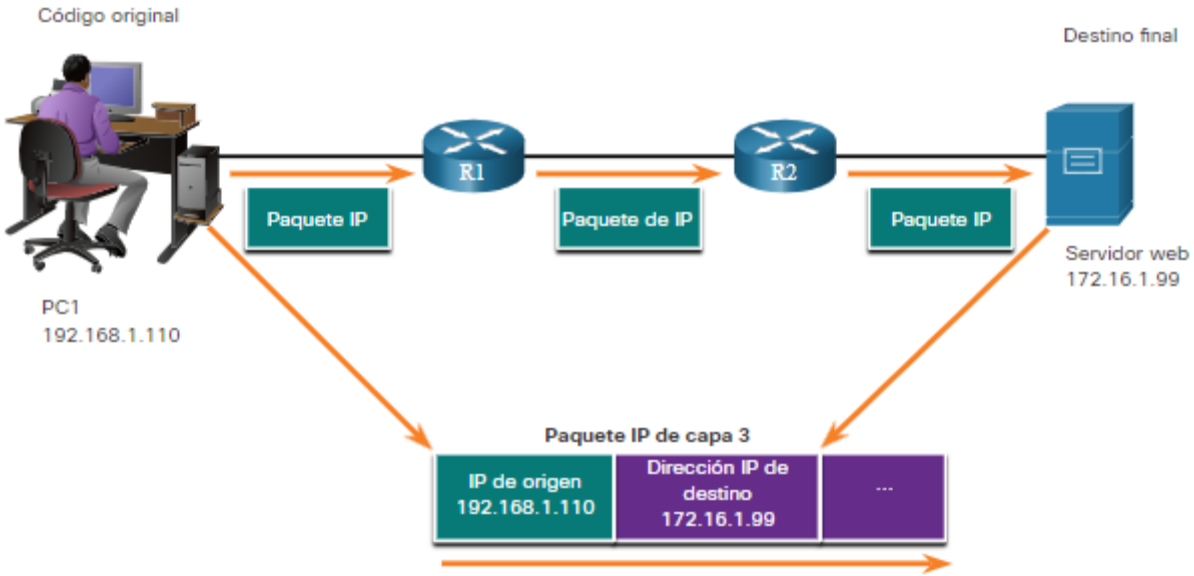
Direcciones



Direcciones de origen y de destino de la capa de red: son responsables de enviar el paquete IP desde el dispositivo de origen hasta el dispositivo final, ya sea en la misma red o a una red remota.

Direcciones de origen y de destino de la capa de enlace de datos: son responsables de enviar la trama de enlace de datos desde una tarjeta de interfaz de red (NIC) a otra en la misma red.

Dirección lógica de capa 3



Los paquetes IP contienen dos direcciones IP:
Dirección IP de origen: la dirección IP del dispositivo emisor, la fuente de origen del paquete..

Dirección IP de destino: la dirección IP del dispositivo receptor, es decir, el destino final del paquete..

Dirección lógica de capa 3

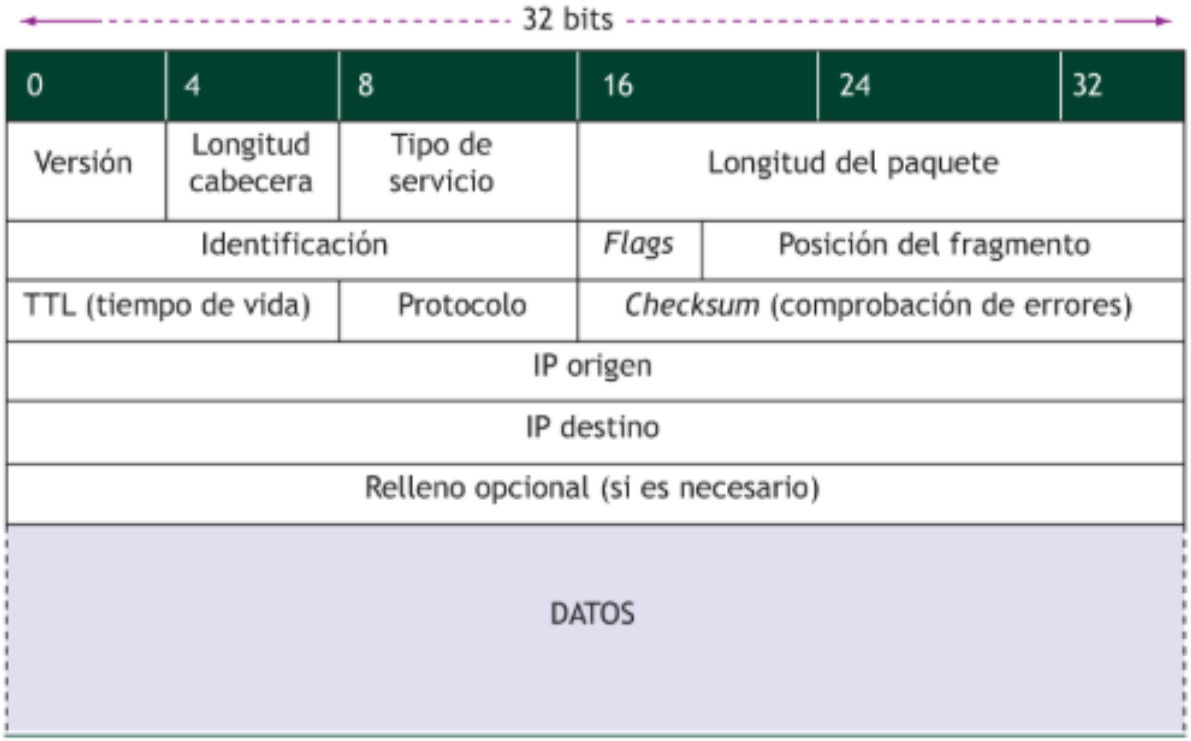
Las direcciones de la capa de red, o direcciones IP, indican el origen y el destino final. Esto es cierto si el origen y el destino están en la misma red IP o redes IP diferentes.

Un paquete IP contiene dos partes:

- **Porción de red (IPv4) o Prefijo (IPv6)**: la sección más a la izquierda de la dirección que indica la red de la que es miembro la dirección IP. Todos los dispositivos de la misma red tienen la misma porción de red de la dirección.
- **Porción de host (IPv4) o ID de interfaz (IPv6)**: la parte restante de la dirección que identifica un dispositivo específico de la red. La sección de host es única para cada dispositivo o interfaz en la red.

Nota: La máscara de subred (IPv4) o la longitud del prefijo (IPv6) se utiliza para identifica la porción de red de una dirección IP de la porción del host.

Protocolo IP v4



7.5. Formato de un paquete IPv4.

Fuente: Castaño Ribes, R. J. (2013). Redes locales. Macmillan Iberia, S.A. https://elibro-net.unipacifico.basesdedatosezproxy.com/es/ereader/unipacifico/43257?page=164

Formato de las Direcciones IP V4

Una dirección IP está formada por 32 números binarios agrupados en cuatro bytes. Para poder recordarlas más fácilmente, las direcciones IP se expresan en números decimales separados por puntos.

1 byte	1 byte	1 byte	1 byte
11000000	00000111	00100010	00001010
192	7	34	10

Se expresaría, por tanto, así: 192.7.34.10.

El valor máximo de cada uno de los bytes es 11111111, que da un valor decimal de 255. Por tanto, las direcciones que tienen un número mayor a 255 en alguno de sus octetos son consideradas inválidas.

Redes con clase

Existen cinco tipos que reciben los nombres de clase A, B, C, D y E. Las dos últimas son de tipo experimental y no se utilizan en la práctica

Red	Red	Host	Host
1 byte	1 byte	1 byte	1 byte
172	18	135	201

Redes con clase A

El primer octeto; si vale entre 0 y 126 será de esta clase (el 127 no se incluye porque se ha reservado como dirección especial).

Clase A

Las direcciones de clase A contienen 8 bits para direccionar la parte de red y 24 bits para direccionar la parte de host. Además, el primer bit de la dirección de red siempre ha de valer 0.

Rango
0.0.0.0
126.255.255.255

Se utilizan 7 bits; permite $2^7 = 128$ redes potenciales.

Se pueden conectar $2^{24} = 16.777.216$ equipos a cada una las redes.

Redes con clase B

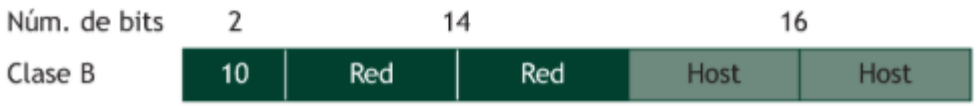
El primer octeto; si vale entre 128 y 191 la IP será de esta clase.

Rango:
128.0.0.1
191.255.255.255

Clase B

Las direcciones de clase B contienen 16 bits para la parte de red y 16 bits para la parte de host. Además, los dos primeros bits de la dirección de red siempre tienen que valer 10.

Actualmente, se asignan direcciones de clase B a universidades y grandes compañías que, por el agotamiento de direcciones IP, ya no tienen acceso a una dirección de clase A. Google, por ejemplo, tiene una dirección de clase B.



Se utilizan 14 bits, permite 2^{14} = 16.384 redes potenciales.

Se pueden conectar 2^{16} = 65.536 equipos a cada una las redes.

Redes con clase C

El primer octeto; si vale entre 192 y 223 la IP será de esta clase.

Rango:
192.0.0.0
223.255.255.255

Clase C

Las direcciones de clase C contienen 24 bits para la parte de red y 8 bits para la parte de host. Además, los tres primeros bits de la dirección de red siempre tienen que valer 110.

Se utilizan 21 bits; permite 2^{21} = 2.097.152 redes potenciales.

Se pueden conectar 2^{8} = 256 equipos a cada una las redes.

Redes con clase D

Clase D

Las direcciones de clase D contienen 8 bits para la parte de red y 24 bits para la parte de host. Además, los cuatro primeros bits de la dirección de red siempre valen 1110.

Para que una IP sea de esta clase, su primer octeto debe estar comprendido entre el rango de 224 a 239. Este tipo de direcciones se utiliza únicamente para experimentación *multicast*, que es una dirección exclusiva que dirige los paquetes a grupos de equipos.

Redes con clase E

Clase E

Las direcciones de clase E contienen 8 bits para la parte de red y 24 bits para la parte de host. Además, los cuatro primeros bits de la dirección de red siempre valen 1111.

En este tipo de direcciones solamente sería posible formar 16 tipos de redes, ya que $2^4 = 16$. Para que una IP sea de esta clase, el valor de su primer byte debe estar comprendido entre 240 a 255.

Este tipo de direcciones se reservan para que la IETF *(internet engineering task force)* realice investigaciones, por tanto no se emiten direcciones de clase E para ser utilizadas por Internet.

Mascara de subred

La máscara de subred tiene como función principal separar la parte de red de la de host de una dirección IP. Para ello, dispone de un formato de 32 bits con la parte de red colocada a 1 y la parte de host colocada a 0.

Un ejemplo de máscara de subred válida sería el siguiente:

11111111.11111111.11110000.00000000

O lo que es lo mismo: 255.255.240.0.

Podemos ver que, en este ejemplo, se utilizan 20 bits para la parte de red y 12 bits para la parte de host, lo que nos da los 2^12− 2 = 4.094 dispositivos a direccionar.

A: 11111111 000000000000000000000000
B: 1111111111111111 0000000000000000
C: 111111111111111111111111 00000000

Operación lógica AND

Por ejemplo, en la dirección 195.117.59.33/20 tendríamos:

11000011	01110101	00111011	00100001
195	117	59	33

Su máscara de subred sería la siguiente:

11111111	11111111	11110000	00000000
255	255	240	0

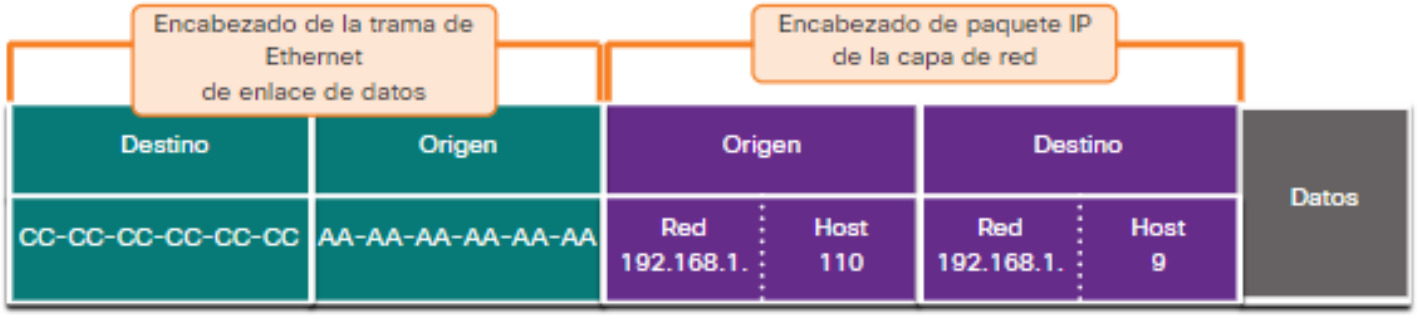
La operación AND sería la siguiente:

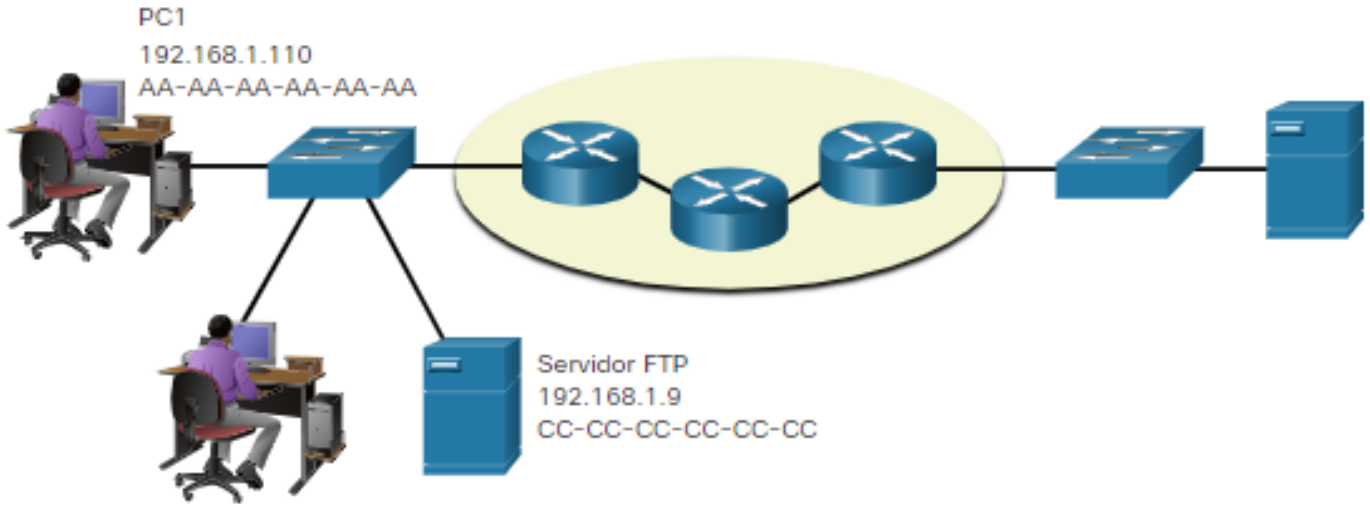
11000011	01110101	00111011	00100001
11111111	11111111	11110000	00000000
11000011	**01110101**	**00110000**	**00000000**
195	**117**	**48**	**0**

Por tanto, en la dirección IP del ejemplo, la parte de red y, a su vez, la dirección de red será 195.117.48.0.

Dispositivos en la misma red

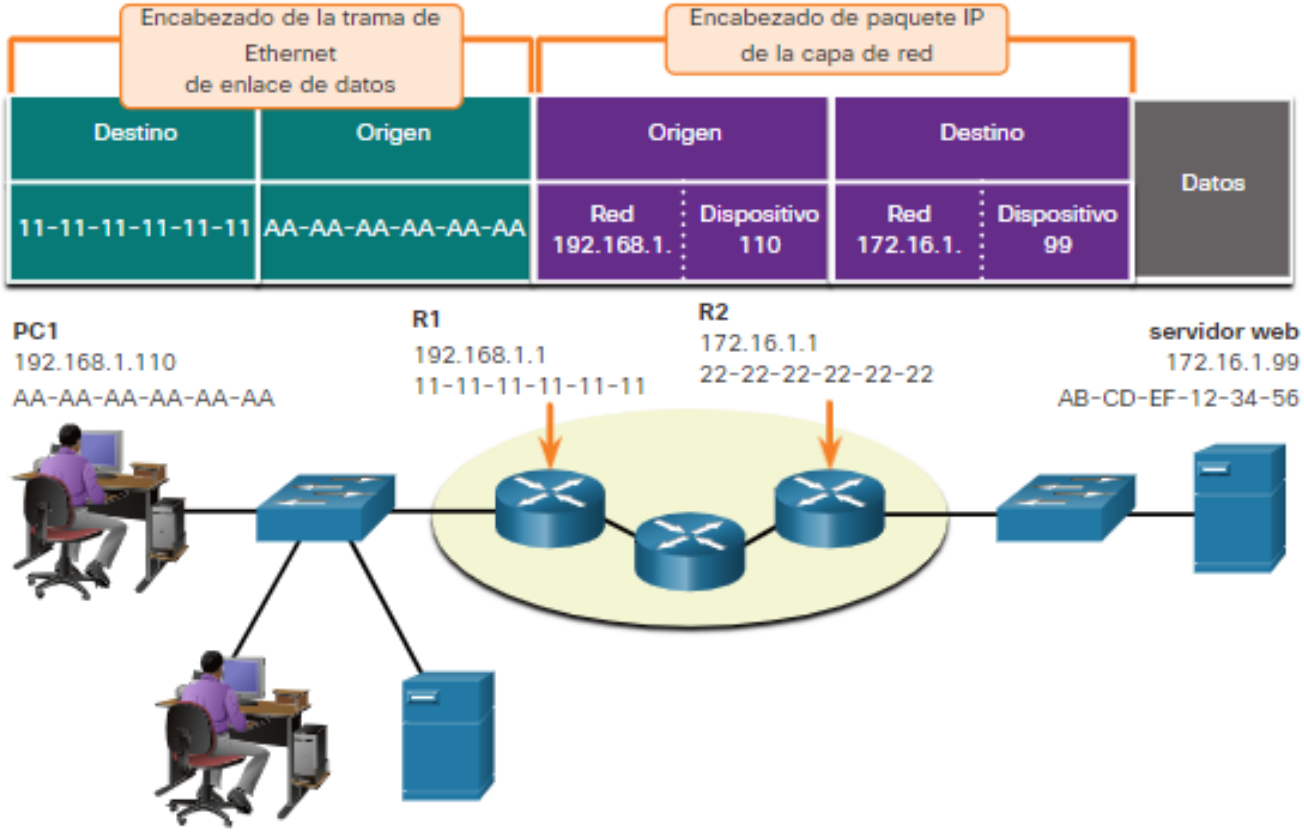
Dirección IPv4 de origen: - la dirección IPv4 del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
Dirección IPv4 de destino: - la dirección IPv4 del dispositivo receptor, el servidor FTP: 192.168.1.9.





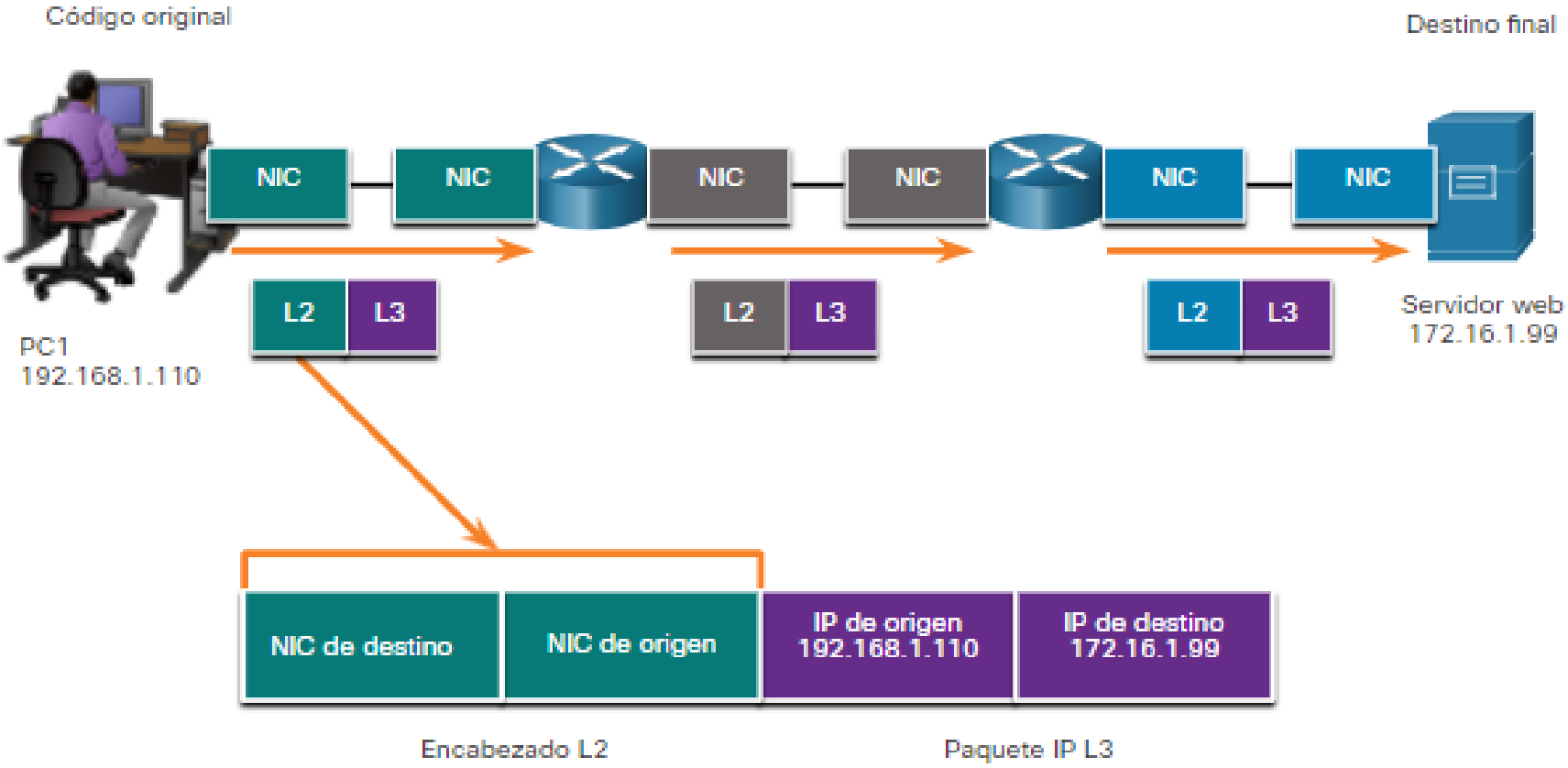
Dispositivos en una red remota

Dirección IPv4 de origen: - la dirección IPv4 del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
Dirección IPv4 de destino: - la dirección IPv4 del dispositivo receptor, es decir, el servidor web: 172.16.1.99.



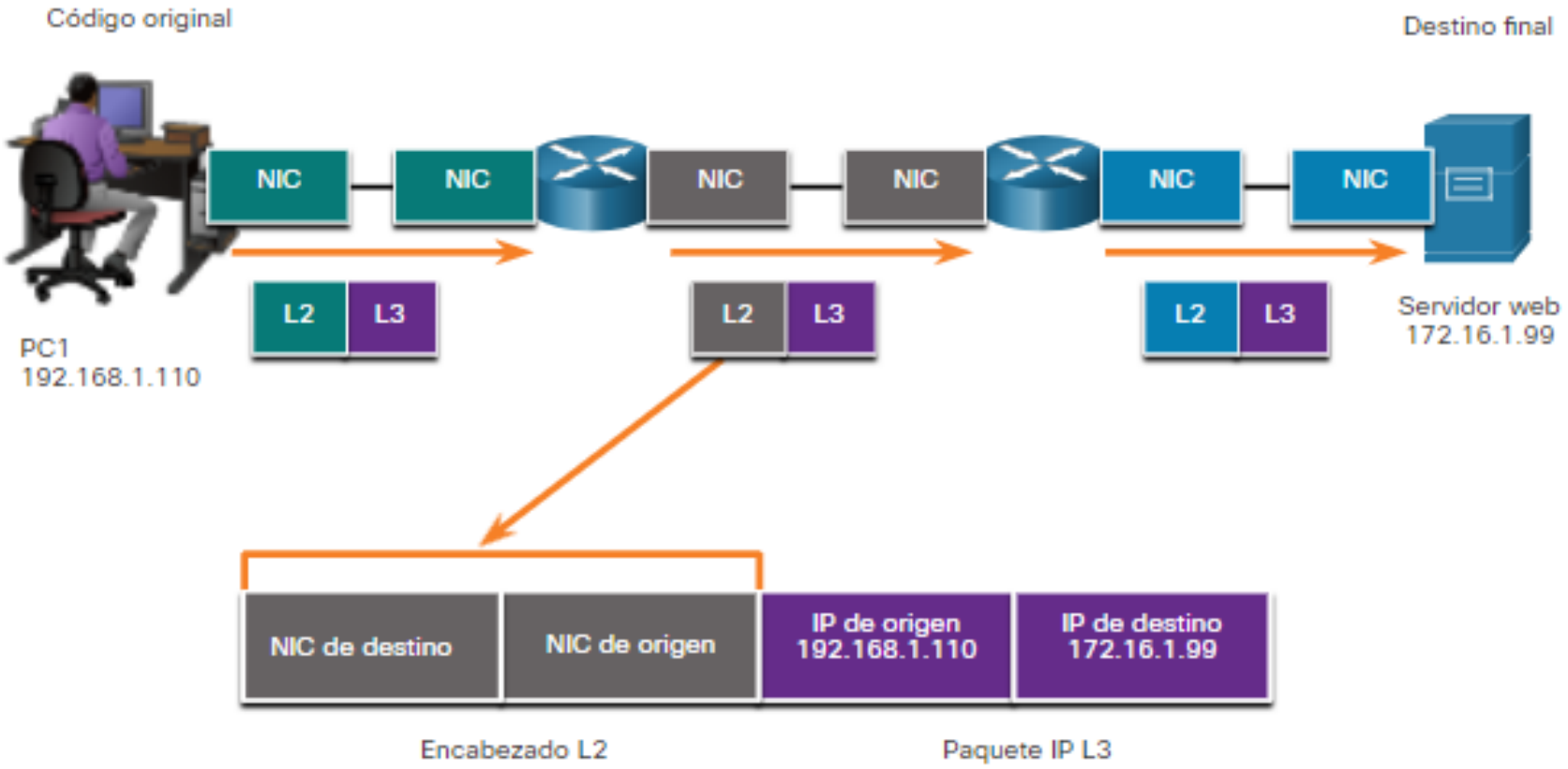
Direcciones de enlace de datos

Host a enrutador



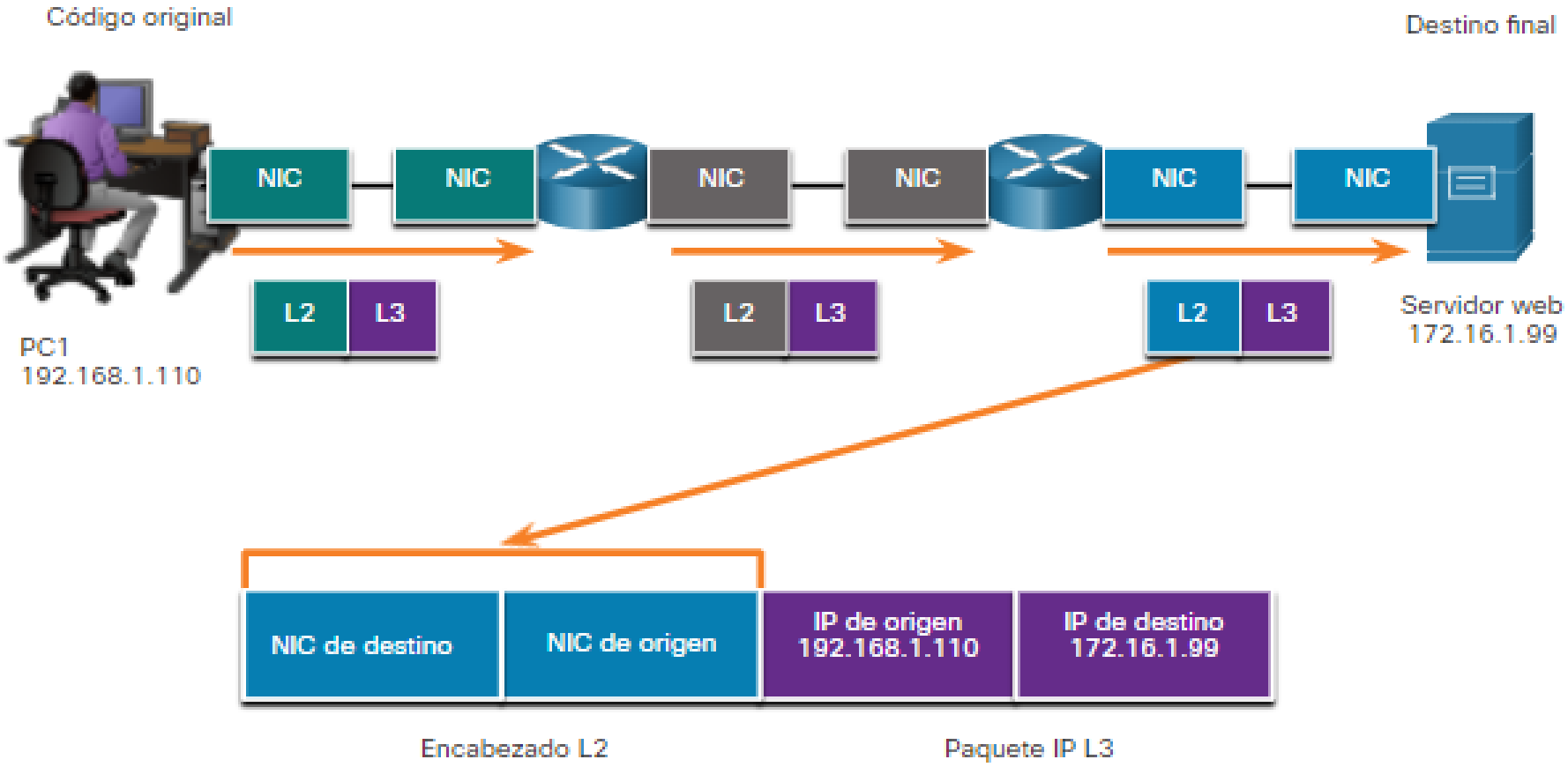
Direcciones de enlace de datos

Enrutador a enrutador



Direcciones de enlace de datos

Enrutador a servidor



Redes y direcciones IP especiales

La dirección de red o de cable hace referencia a toda la red y el router la utiliza cuando comunica una red a través de Internet (Toda la porción de Host es 0).
La dirección de difusión o broadcast es utilizada por los equipos cuando quieren que su datagrama sea visto por todos los dispositivos de la misma LAN (Toda la porción de Host es 1).

Ejemplo dirección de red o cable:

- 115.0.0.0 es una dirección de cable de clase A. Contiene, por ejemplo, al host 115.10.15.25
- 150.23.0.0 es una dirección de cable de clase B
- 193.15.28.0 es una dirección de cable de clase C

Ejemplo dirección de difusión:

- 115.255.255.255 es una dirección de difusión de clase A para la red 115.0.0.0.
- 150.23.255.255 es una dirección de difusión de clase B para la red 150.23.0.0.
- 193.15.28.255 es una dirección de difusión de clase C para la red 193.15.28.0.

Redes y direcciones IP especiales

El rango de direcciones desde 0.0.0.0 hasta 0.255.255.255 no puede utilizarse como dirección IP (indica el estado de un dispositivo que está a la espera de que se le asigne una dirección IP válida)

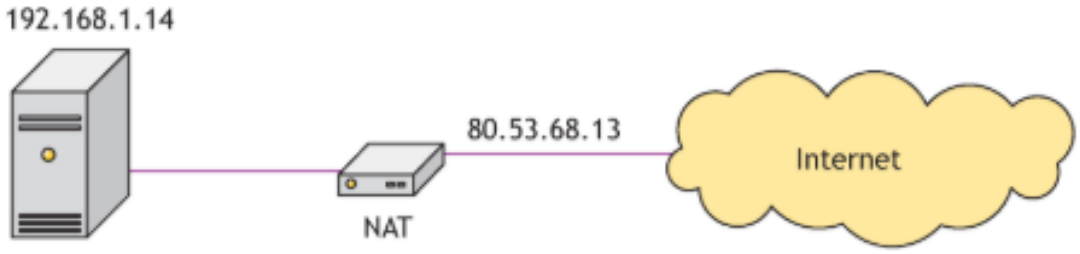
La dirección 127.0.0.1 se conoce como loopback address y define al dispositivo en el que uno se encuentra, su principal función es comprobar el correcto funcionamiento de la NIC que conecta el dispositivo a la red.

El rango de direcciones que va desde 14.0.0.0 hasta 14.255.255.255 está reservado para las redes públicas de datos.

Redes públicas y privadas

> Un número de dirección IP pública viene dado por uno de los cinco organismos encargados de proporcionar direcciones IP, los *regional internet registry*, mientras que los números de dirección IP privadas son números especiales que pueden utilizar los administradores de redes sin solicitar permiso a ninguna organización.

Las redes privadas necesitan que el Router posea un mecanismo llamado NAT (network address translation) para que sus dispositivos puedan acceder a Internet.



Redes públicas y privadas

Cuatro tipos de direcciones IP privadas, (RFC 1918):

Clase A: de 10.0.0.0 a 10.255.255.255 Permite conectar hasta 2^24− 2 = 16.777.214 dispositivos.

Clase B: de 169.254.0.0 a 169.254.255.255 Permite un máximo de 2^16 − 2 = 65.534 dispositivos. aparece cuando nuestro PC no tiene una dirección IP válida asignada por el router o el servidor.

Clase B: de 172.16.0.0 a 172.31.255.255 Permite 16 redes de clase B contiguas con un máximo de 2^16− 2 = 65.534 dispositivos cada una. Se usa en universidades y grandes compañías.

Clase C: de 192.168.0.0 a 192.168.255.255 Permite 256 redes de clase C contiguas con un máximo de 2^8− 2 = 254 dispositivos cada una. Se usa en compañías de mediano y pequeño tamaño.