



Protocolo TCP/IP

Msc. Ing. Soft. Carmen Tacuri Vintimilla
INSTITUTO SUPERIOR TECNOLOGICO DEL AZUAY.

Introducción Protocolo TCP/IP

- Es el protocolo de red más extendido y con mayor aceptación a nivel mundial.
- Este protocolo que comenzó a finales de los años 60 como un proyecto de investigación financiado por el gobierno de EE.UU., sobre la conmutación de paquetes, se convirtió en la década de los 90 en la estructura de red más ampliamente utilizada.
- Las siglas TCP/IP se refieren a un conjunto de protocolos para comunicaciones de datos. Este conjunto toma su nombre de dos de sus protocolos más importantes, el protocolo **TCP (Transmission Control Protocol)** y el protocolo **IP (Internet Protocol)**.

Introducción Protocolo TCP/IP

- La evolución del protocolo TCP/IP siempre ha estado muy ligada a la de Internet. En 1969 la agencia de proyectos de investigación avanzada, ARPA (Advanced Research Projects Agency) desarrolló un proyecto experimental de red conmutada de paquetes al que denominó ARPAnet.
- ARPAnet comenzó a ser operativa en 1975, pasando entonces a ser administrada por el ejército de los EEUU. En estas circunstancias se desarrolla el primer conjunto básico de protocolos TCP/IP.
- En la década de los ochenta, todos los equipos militares conectados a la red adoptan el protocolo TCP/IP y se comienza a implementar también en los sistemas Unix

Introducción Protocolo TCP/IP

- Poco a poco ARPAnet deja de tener un uso exclusivamente militar, y se permite que centros de investigación, universidades y empresas se conecten a esta red. Se habla cada vez con más fuerza de Internet y en 1990 ARPAnet deja de existir oficialmente.
- **En los años sucesivos y hasta nuestros días las redes troncales y los nodos de interconexión han aumentado de forma imparable. La red Internet parece expandirse sin límite, aunque manteniendo siempre una constante: el protocolo TCP/IP.** En efecto, el gran crecimiento de Internet ha logrado que el protocolo TCP/IP sea el estándar en todo tipo de aplicaciones telemáticas, incluidas las redes locales y corporativas. Y es precisamente en este ámbito, conocido como Intranet, donde TCP/IP adquiere cada día un mayor protagonismo

Introducción Protocolo TCP/IP

- La popularidad del protocolo TCP/IP se debe a una serie de características que responden a las necesidades de transmisión de datos en todo el mundo, entre ellas:
 - ❑ **Los estándares del protocolo TCP/IP son abiertos y ampliamente soportados por todo tipo de sistemas**, es decir, se puede disponer libremente de ellos y son desarrollados independientemente del hardware de los ordenadores o de los sistemas operativos.
 - ❑ **TCP/IP funciona prácticamente sobre cualquier tipo de medio**, no importa si es una red Ethernet, una conexión ADSL o una fibra óptica.
 - ❑ **TCP/IP emplea un esquema de direccionamiento que asigna a cada equipo conectado una dirección única en toda la red**, aunque la red sea tan extensa como Internet.

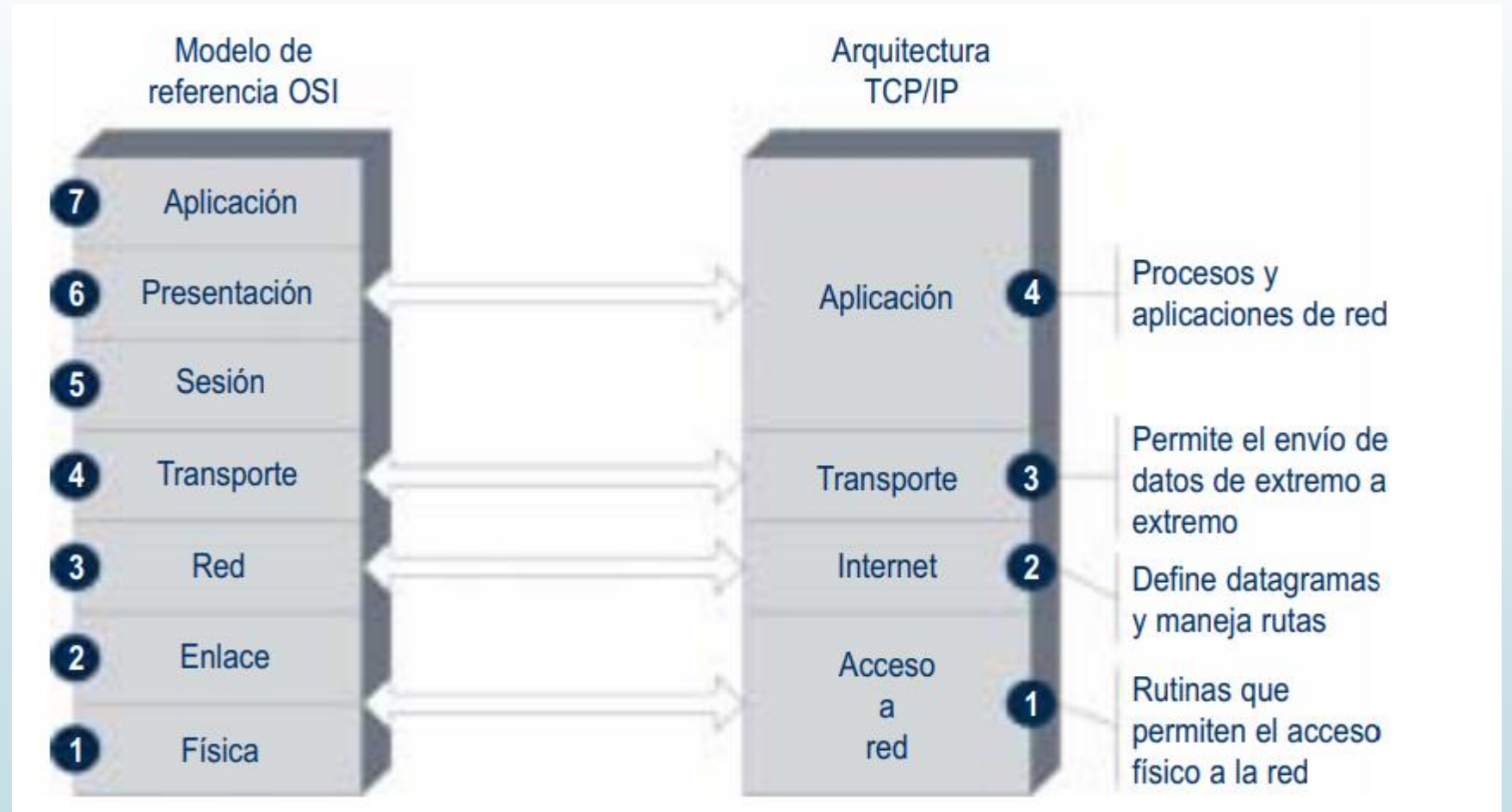
Introducción Protocolo TCP/IP

- La naturaleza abierta del conjunto de protocolos TCP/IP requiere de estándares de referencia disponibles en documentos de acceso público. Actualmente todos los estándares descritos para los protocolos TCP/IP son publicados como RFC (**Requests for Comments**) que detallan lo relacionado con la tecnología de la que se sirve Internet: protocolos, recomendaciones, comunicaciones, etcétera.

Arquitectura del protocolo TCP/IP

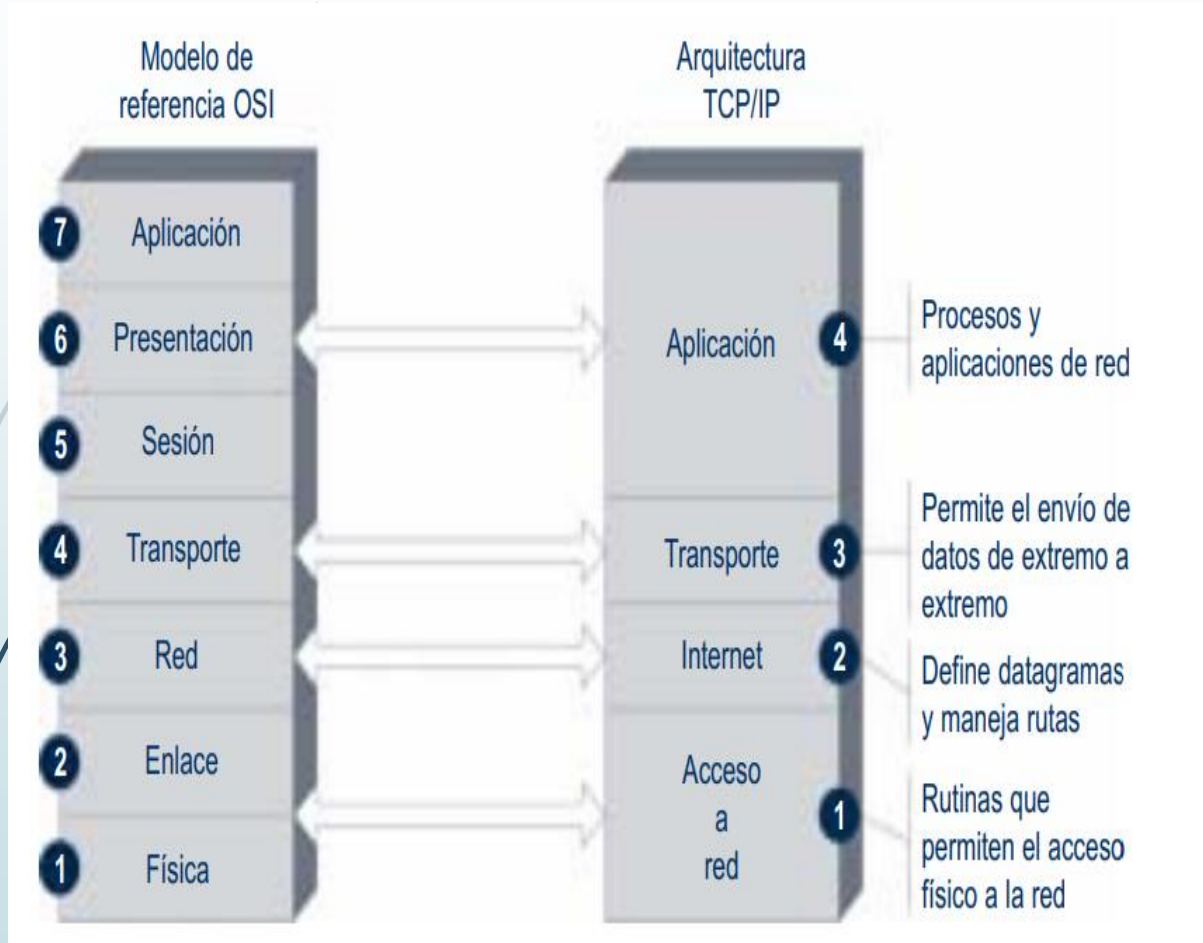
- El protocolo TCP/IP fue creado antes que el modelo de capas OSI, así que los niveles del protocolo TCP/IP no coinciden exactamente con los siete que establece el OSI.

Correspondencia del modelo OSI con TCP/IP



Arquitectura del protocolo TCP/IP

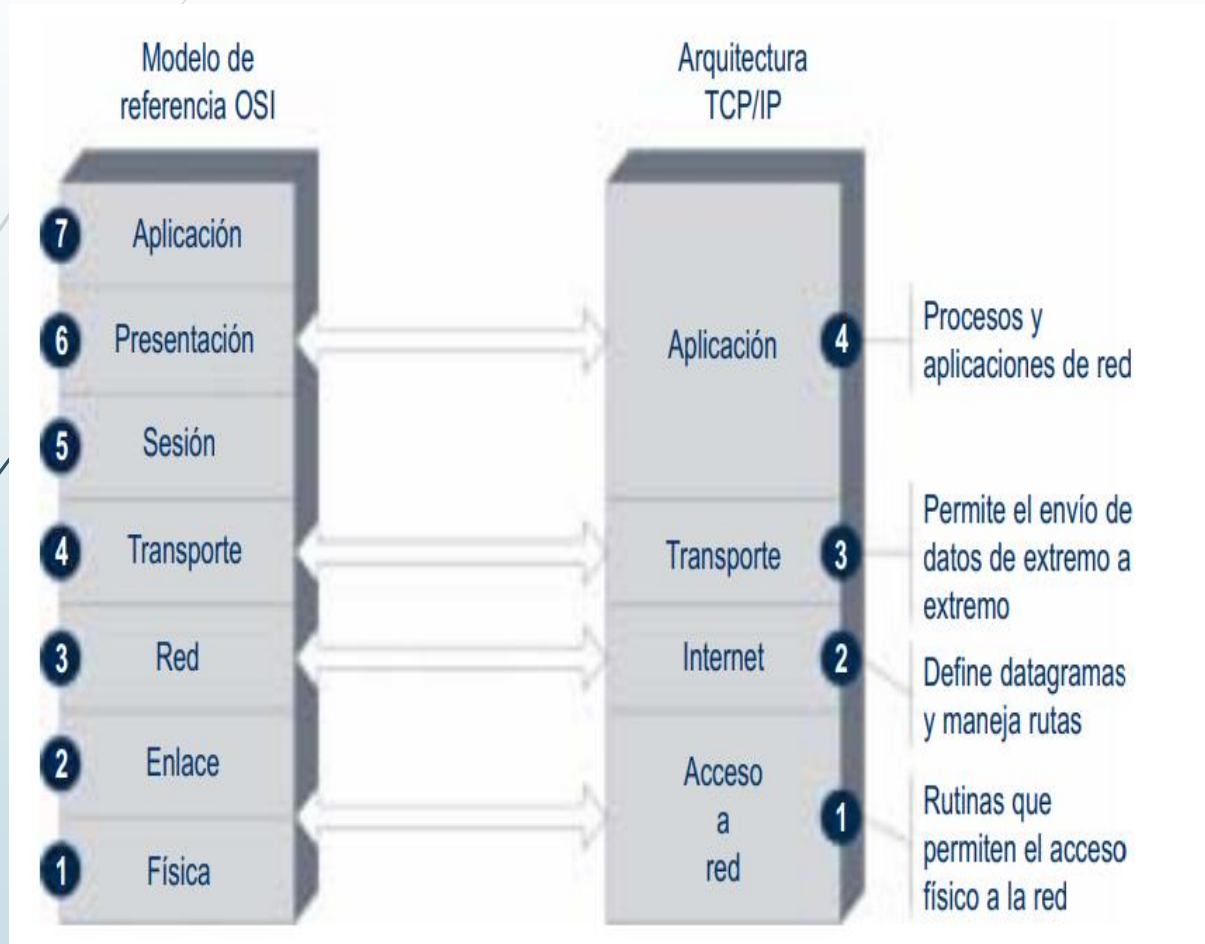
Correspondencia del modelo OSI con TCP/IP



- Existen descripciones del protocolo TCP/IP que definen de tres a cinco niveles. La Figura representa un modelo de cuatro capas TCP/IP y su correspondencia con el modelo de referencia OSI.
- Los datos que son enviados a la red recorren la pila del protocolo TCP/IP desde la capa más alta de aplicación hasta la más baja de acceso a red. Cuando son recibidos, recorren la pila de protocolo en el sentido contrario.

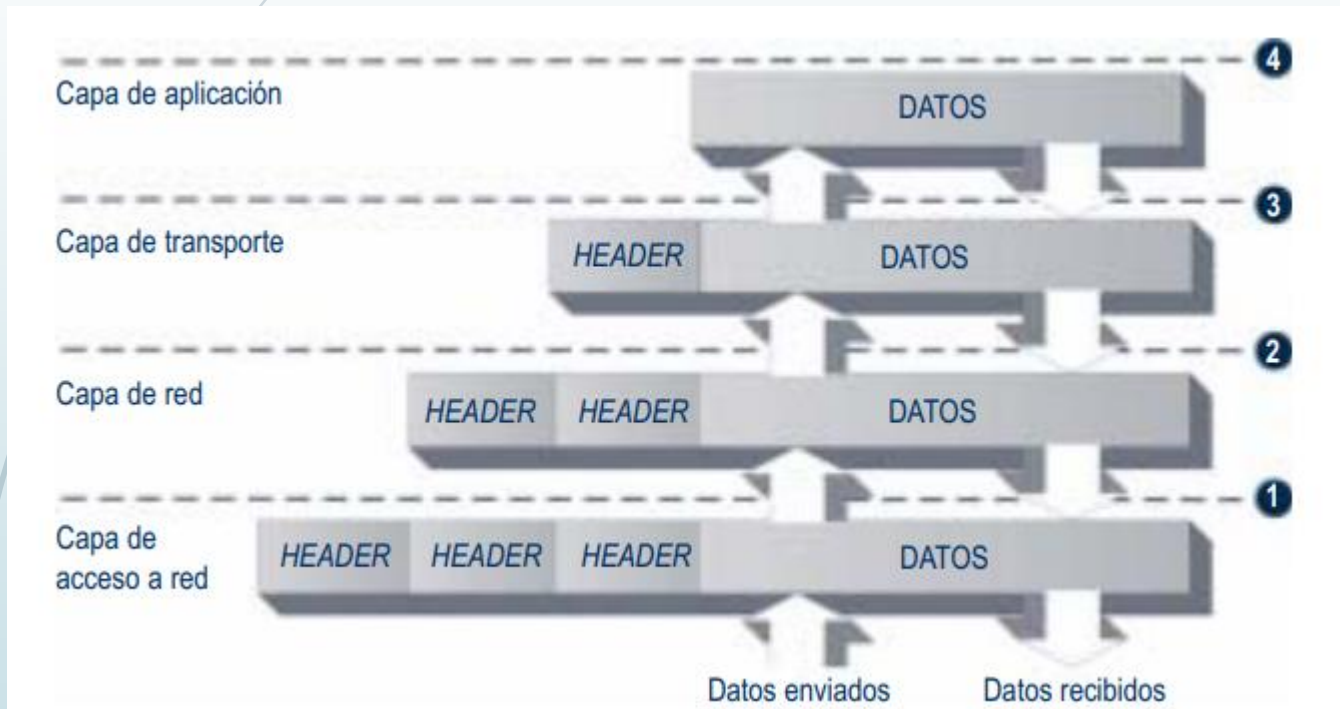
Arquitectura del protocolo TCP/IP

Correspondencia del modelo OSI con TCP/IP



- Durante estos recorridos, cada capa añade o sustrae cierta información de control a los datos para garantizar su correcta transmisión

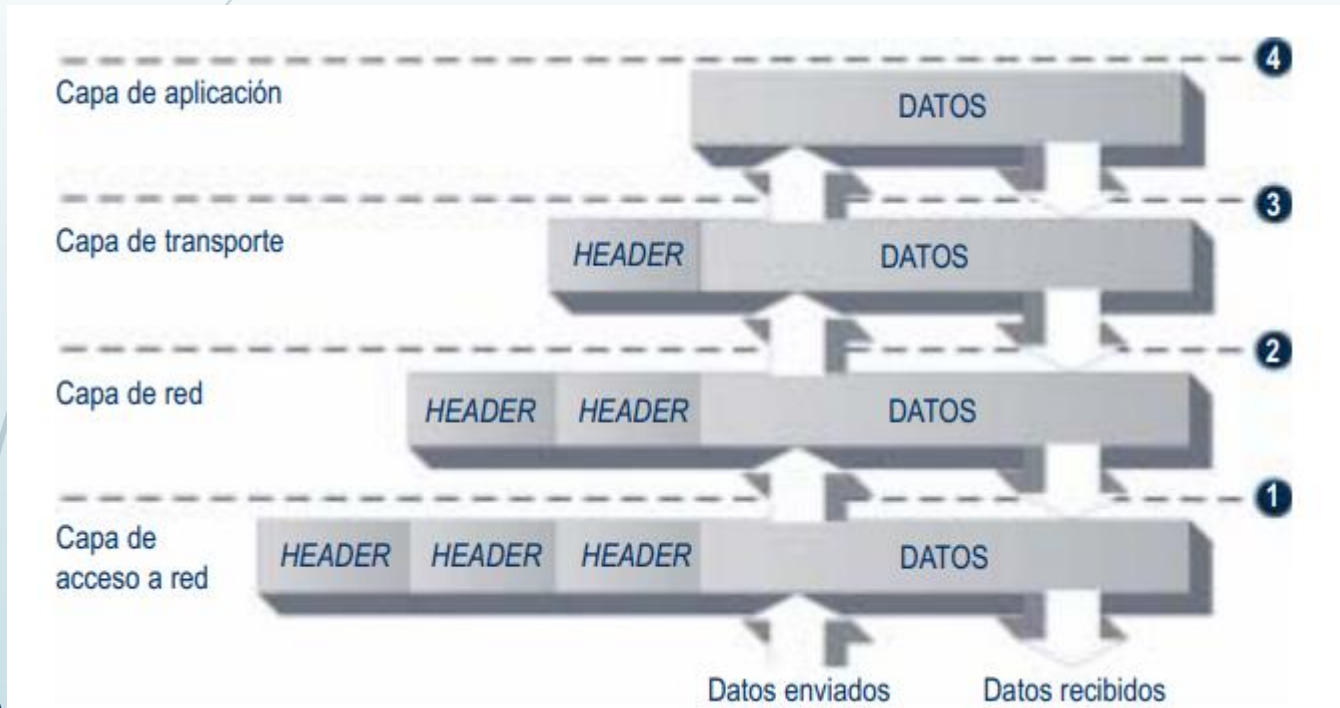
Encapsulado de datos por los niveles TCP/IP



Encapsulado de datos por los niveles TCP/IP.

- La información de control se sitúa antes de los datos que se transmiten, se llama cabecera (**header**).
- Se puede ver cómo **cada capa añade una cabecera a los datos que se envían a la red**. Este proceso se conoce como **encapsulado**.

Encapsulado de datos por los niveles TCP/IP



Encapsulado de datos por los niveles TCP/IP.

- Si en vez de transmitir datos se trata de recibirlos, el proceso sucede al revés. Cada capa elimina su cabecera correspondiente hasta que quedan sólo los datos.
- En teoría cada capa maneja una estructura de datos propia, independiente de las demás, aunque en la práctica estas estructuras de datos se diseñan para que sean compatibles con las de las capas adyacentes.

Capa de acceso a red

- Dentro de la jerarquía del protocolo TCP/IP la capa de acceso a red se encuentra en el nivel más bajo. Es en esta capa **donde se define cómo encapsular un datagrama IP en una trama que pueda ser transmitida por la red**, siendo en una inmensa mayoría de redes LAN una trama Ethernet.
- Otra función importante de esta capa **es la de asociar las direcciones lógicas IP a direcciones físicas de los dispositivos adaptadores de red (NIC)**.
- Por ejemplo: La dirección lógica IP 192.168.1.5 de un ordenador se asocia a la dirección física Ethernet 00-0C-6E-2B-49-65. **Así la dirección lógica es elegida por el usuario, mientras que la física no puede cambiarse e identifica inequívocamente al adaptador NIC dentro de la red Ethernet.**
- Dentro de la capa de acceso a red opera el protocolo ARP (Address Resolution Protocol), que se encarga precisamente de asociar direcciones IP con direcciones físicas Ethernet.

Capa de red: Internet

- **La capa Internet se encuentra justo encima de la capa de acceso a red. En este nivel el protocolo IP es el gran protagonista.** Existen varias versiones del protocolo IP: **IPv4** es en la actualidad la más empleada, aunque el crecimiento exponencial en el tamaño de las redes compromete cada vez más su operatividad. El número de equipos que IPv4 puede direccionar comienza a quedarse corto. Para poner remedio a esta situación se ha desarrollado la versión **IPv6**, con una capacidad de direccionamiento muy superior a IPv4, pero totalmente incompatible.



Capa de red: Internet

- **El protocolo IP se ha diseñado para redes de paquetes conmutados no orientadas a conexión**, lo cual quiere decir que cuando dos equipos quieren conectarse entre sí no intercambian información para establecer la sesión. **IP tampoco se encarga de comprobar si se han producido errores de transmisión**, confía esta función a las capas superiores. Todo ello se traduce en que **los paquetes de datos contienen información suficiente como para propagarse a través de la red sin que haga falta establecer conexiones permanentes**

Capa de red: Internet



Representación de la cabecera de una datagrama IP.

- Para el protocolo IP un datagrama es el formato que debe tener un paquete de datos en la capa de red.
- La figura muestra las seis primeras palabras de la cabecera y el punto desde el que se comienzan a transmitir los datos.
- Las cinco (o seis) primeras palabras de 32 bits contienen la información necesaria para que el datagrama se propague por la red, y a continuación se adjuntan los datos.

Capa de red: Internet



Representación de la cabecera de una datagrama IP.

► La lógica de funcionamiento del protocolo IP es :

para cada datagrama se **consulta la dirección origen (palabra 4) y la compara con la dirección destino (palabra 5)**. Si resulta que **origen y destino se corresponden** con equipos (hosts) de la misma red, **el datagrama se envía directamente de un equipo a otro**.

Si por el contrario, **los equipos pertenecen a redes distintas**, se hace necesaria **la intervención de una puerta de enlace o gateway que facilite el envío a redes diferentes**.

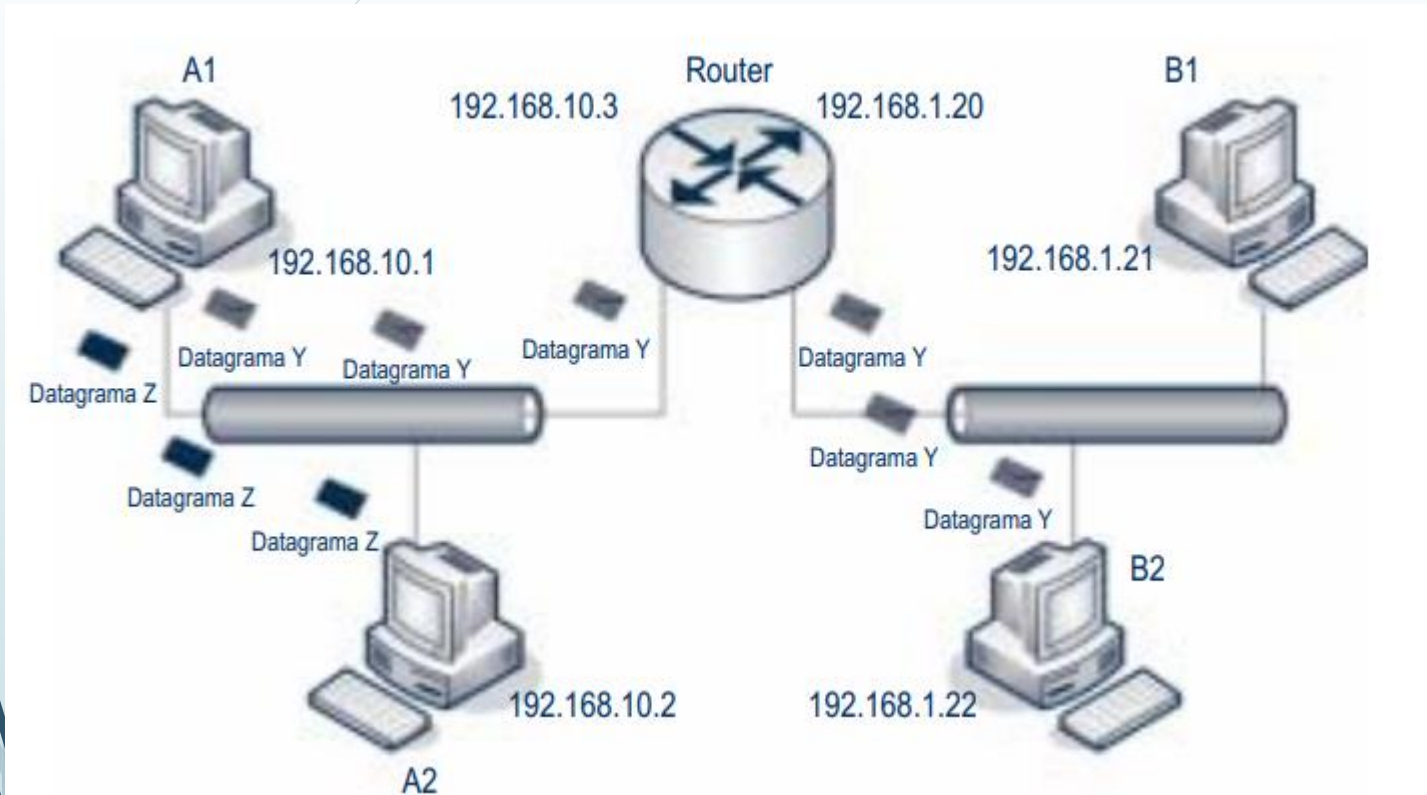
Capa de red: Internet



Representación de la cabecera de una datagrama IP.

- El paso de datos de una red a otra a través de una puerta de enlace es conocido como «salto» (hop).
- Un datagrama puede realizar varios saltos a través de diversas redes hasta alcanzar su destino. El camino que siguen los datos enviados por un equipo a otro no tiene por qué ser siempre el mismo.

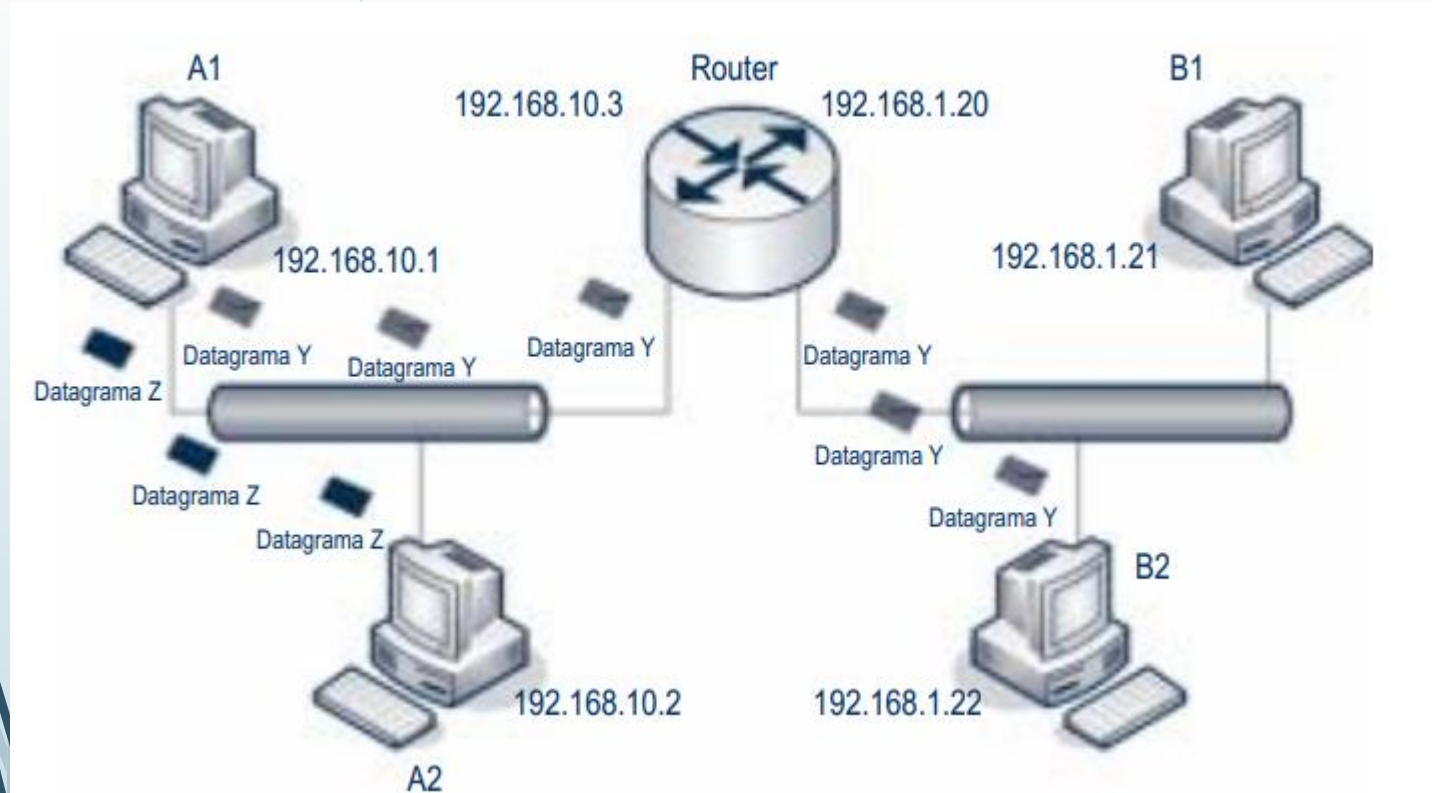
Capa de red: Internet



formas de enviar datagramas.

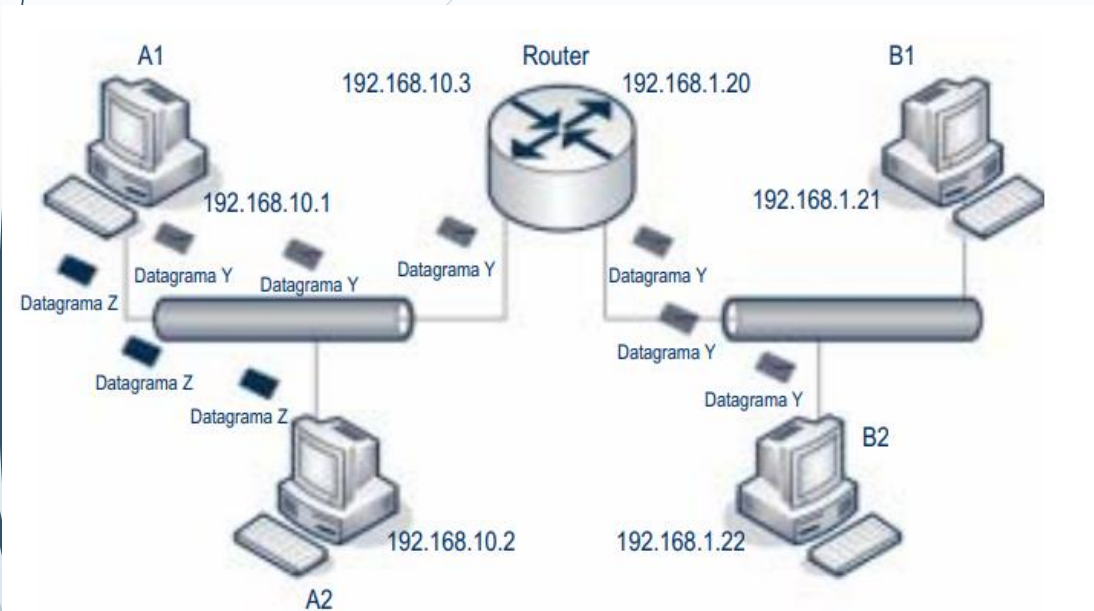
- La búsqueda del camino más adecuado a cada momento se denomina **enrutamiento**
- las puertas de enlace se les denomina enrutadores (routers). **enrutamiento.**

Capa de red: Internet



- En la Figura vemos un ejemplo de dos redes unidas por un router. En una el equipo A1 envía un datagrama Z al equipo A2. Como ambos pertenecen a la misma red 192.168.10.0, el datagrama Z es enviado directamente.

Capa de red: Internet



- Cuando el equipo A1 pretende enviar un datagrama al equipo B2 que se encuentra en otra red, resulta imprescindible la ayuda del router.
- Como la dirección destino del datagrama no se encuentra en la red de origen, se envía directamente a la dirección de la puerta de enlace 192.168.10.3, que es uno de los interfaces del router.
- Es ahora este dispositivo **router** quien decide qué camino debe seguir el datagrama. Para ello **consulta sus tablas internas, y comprueba que la dirección destino coincide con la red en la que tiene conectado su interfaz con dirección 192.168.1.20**. Una vez realizada esta consulta ya puede enviar el datagrama desde este puerto directamente al equipo B2 (192.168.1.22).
- El datagrama ha llegado a su destino realizando un salto entre redes

Protocolo ICMP

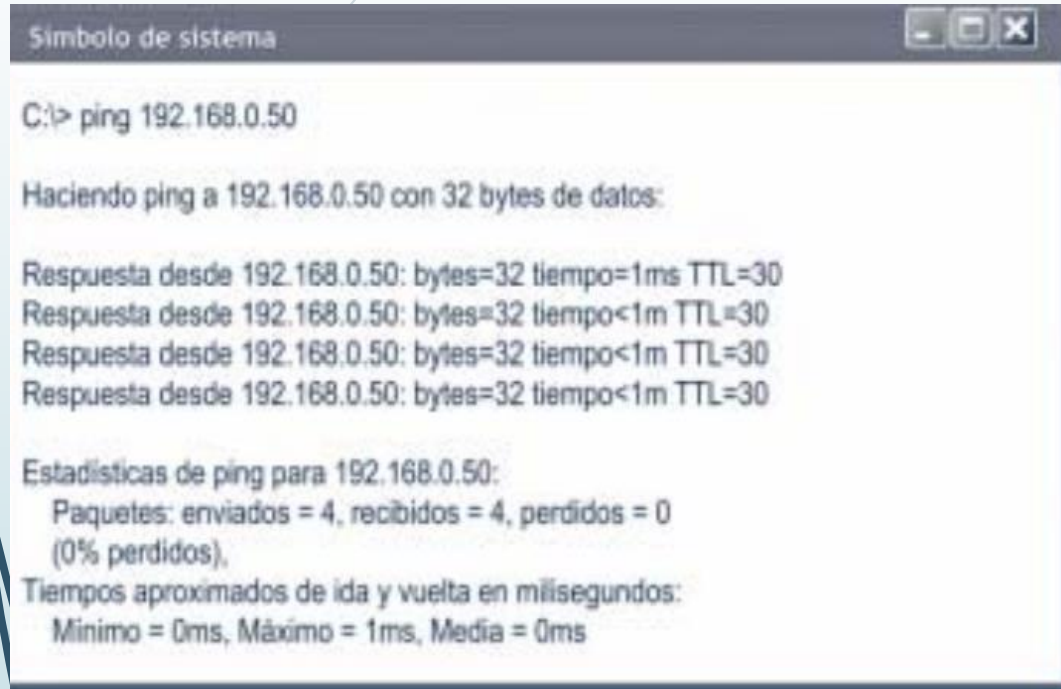
- En la misma capa de red en la que opera el protocolo IP tenemos también el importante protocolo ICMP (Internet Control Message Protocol), definido por la RFC 792.
- ICMP envía mensajes en forma de datagramas que permiten al conjunto del protocolo TCP/IP realizar entre otras las siguientes funciones:
 - **Control de flujo.** Si los datagramas llegan muy deprisa al host destino y éste se encuentra con dificultades para procesarlos, el host destino envía al host origen un mensaje ICMP solicitando que de forma temporal detenga su emisión.
 - **Detección de destinos inalcanzables.** Cuando la dirección destino de un datagrama no logra ser asociada a ningún equipo, el host que la ha enviado recibe un mensaje ICMP indicando que el destino indicado es inalcanzable.
 - **Redireccionamiento de rutas.** Una puerta de enlace puede enviar un mensaje ICMP a un host para hacerle saber que existe otra puerta de enlace dentro de la misma red, y que en ese momento resulta una mejor opción para encaminar sus datagramas hacia otras redes.
 - **Pruebas de conectividad.** Esta funcionalidad es la más conocida ya que es la que emplea el comando ping (Packet Internet Groper). Desde un equipo se puede enviar a otro un mensaje ICMP «con eco». **¿Qué significa «con eco»? Pues quiere decir que cuando el host destino recibe el mensaje lo devuelve inmediatamente al host origen.**



Protocolo ICMP

- ▶ Aunque el comando **ping** fue creado para sistemas Unix, casi cualquier sistema proporciona el software adecuado para su ejecución. **Ping se sirve normalmente de dos mensajes específicos: ECHO_REQUEST y ECHO_REPLY.**
- ▶ La conectividad IP entre equipos queda contrastada cuando se completa el camino de ida y vuelta de los mensajes ICMP. Además **el comando ping ofrece información acerca del tiempo que tardan el ir y volver los paquetes de datos.**

Pruebas de conectividad con ping



```
Símbolo de sistema

C:\> ping 192.168.0.50

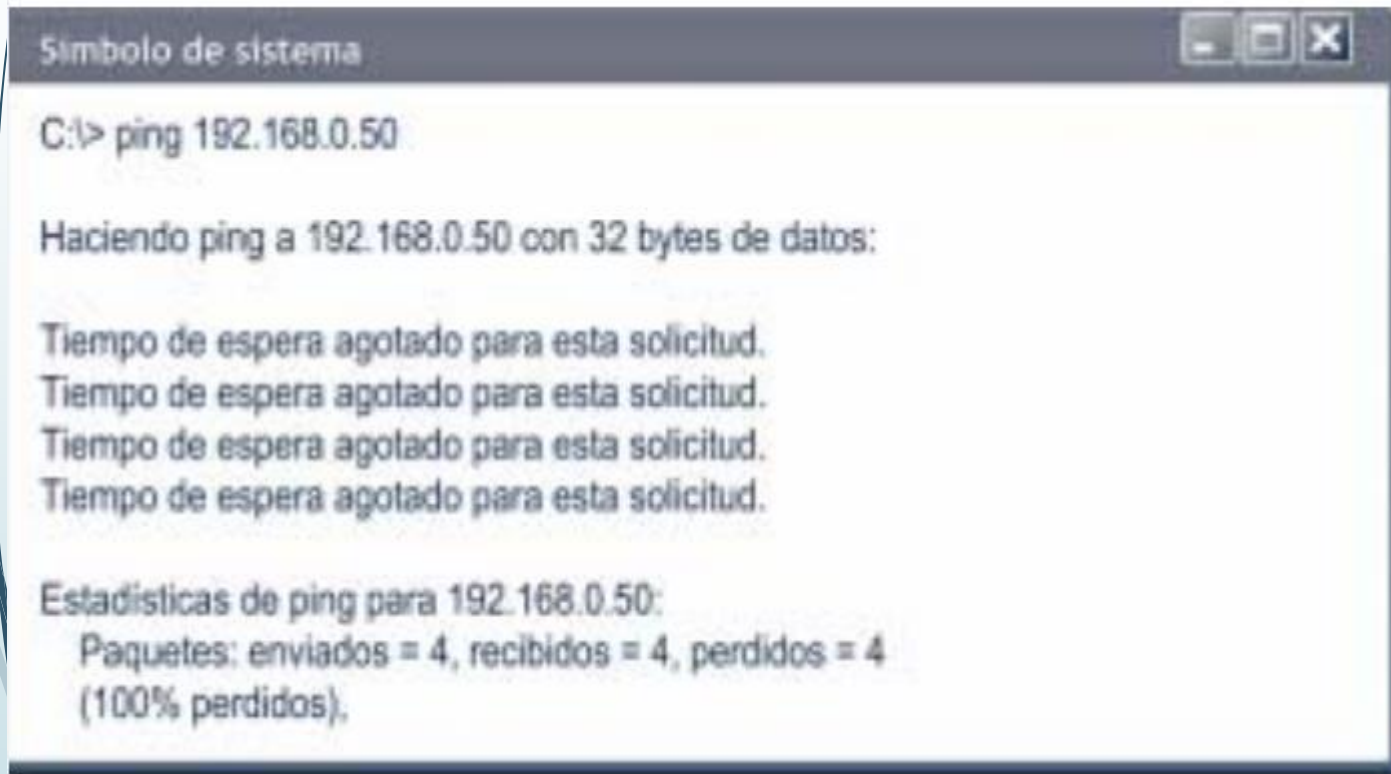
Haciendo ping a 192.168.0.50 con 32 bytes de datos:

Respuesta desde 192.168.0.50: bytes=32 tiempo=1ms TTL=30
Respuesta desde 192.168.0.50: bytes=32 tiempo<1m TTL=30
Respuesta desde 192.168.0.50: bytes=32 tiempo<1m TTL=30
Respuesta desde 192.168.0.50: bytes=32 tiempo<1m TTL=30

Estadísticas de ping para 192.168.0.50:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

- **El comando ping puede presentar ligeras diferencias y distintas opciones según el sistema o equipo desde el que se ejecute.** La versión de ping que viene con los sistemas operativos Windows envía por defecto cuatro paquetes ICMP de 32 bytes, y si el host de la dirección destino se encuentra activo y recibe los mensajes, responde a cada uno. La forma correcta de ejecutar el programa ping será desde la una ventana que permita teclear comandos.

Pruebas de conectividad con ping



```
Símbolo de sistema
C:\> ping 192.168.0.50

Haciendo ping a 192.168.0.50 con 32 bytes de datos:

Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.50:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
              (100% perdidos).
```

- Cuando el host destino no responde a los mensajes ICMP la pantalla muestra un mensaje como el de la Figura

Cada vez que se envía un paquete **ECHO_REQUEST** se guarda en el mismo paquete el instante exacto de su salida, y el host destino copia esta información en el paquete **ECHO_REPLY** que devuelve al host origen. Al recibir la respuesta se calcula el tiempo empleado, comparando la hora guardada en el paquete con la hora a la que ha sido recibido.

Pruebas de conectividad con ping

- A veces resulta interesante testear una conexión de forma continua. Al añadir -t a ping, se envían paquetes de datos hasta que se ordene lo contrario pulsando Control-C.
- **Por razones de seguridad, muchos administradores bloquean en los servidores la respuesta a mensajes ICMP en general o a ECHO_REQUEST en particular.** Se debe a que a veces el comando ping es utilizado por usuarios malintencionados para perpetrar sobre los servidores ataques DoS (Denial of Service) consistentes en envíos masivos de mensajes ICMP que **degradan el rendimiento de la red.**