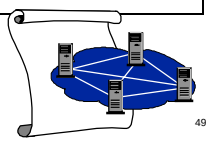
Contenido

- Redes Ethernet
- Protocolos TCP/IP
- Tecnología de ruteadores
- ATM en las redes LAN
- Nuevas aplicaciones
- Administración de redes
- Infraestructura física para redes LAN

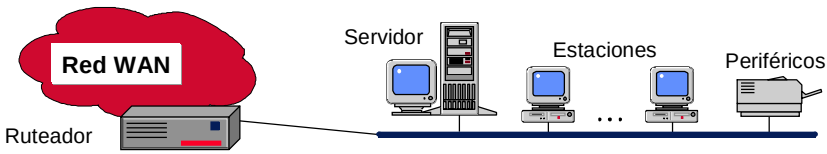
Un Poco de Historia de TCP/IP

- La red ARPANET nació como una propuesta de ARPA (*Advanced Research Projects Agency*) **en 1968**.
- ARPANET nació de **la necesidad de transferir archivos de una máquina a otra**, **inició** operando **con el protocolo NCP (*Network Control Program*).** Más adelante, con **FTP** se añadió el correo electrónico.
- **En 1973, ya no se podía manejar tanto tráfico con NCP y se propuso un nuevo protocolo estandarizado, con confirmación de extremo a extremo, descrito como independiente de la red, del hardware y con conectividad universal. El protocolo se llamó TCP/IP y fue desarrollado principalmente por Robert Kahn y Vinton Cerf.**
- **La versión de UNIX de la universidad de Berkeley y TCP/IP se convirtieron en el sistema operativo y el protocolo de comunicación más común en todas las universidades de EUA.**
- En 1981 se estandarizó **la versión 4 de TCP/IP** para ARPANET. Entre 1982 y 1983 TCP/IP sustituyó completamente a NCP cuando ARPA determinó que todas las computadoras que se conectarán a ARPANET debían usar TCP/IP.

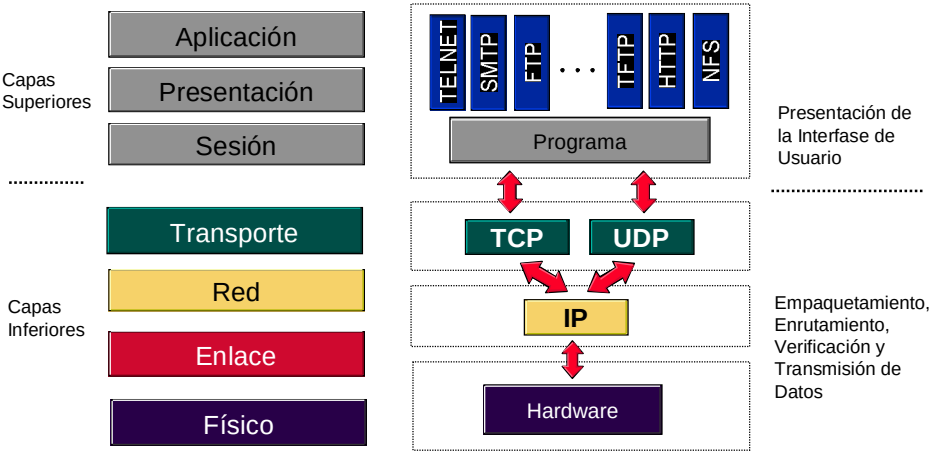


Algunas características de TCP/IP

- ✓ Los protocolos TCP/IP pueden ser usados en redes locales (LAN) como en redes de área amplia (WAN) y en ambos casos a diferentes velocidades.
- ✓ Los protocolos TCP/IP son muy flexibles por el hecho de que casi cualquier tecnología subyacente puede usarse para transferir tráfico de información TCP/IP.
- ✓ TCP/IP fue diseñado para proporcionar interconexión universal entre máquinas independientemente de la red a la que estén conectadas.

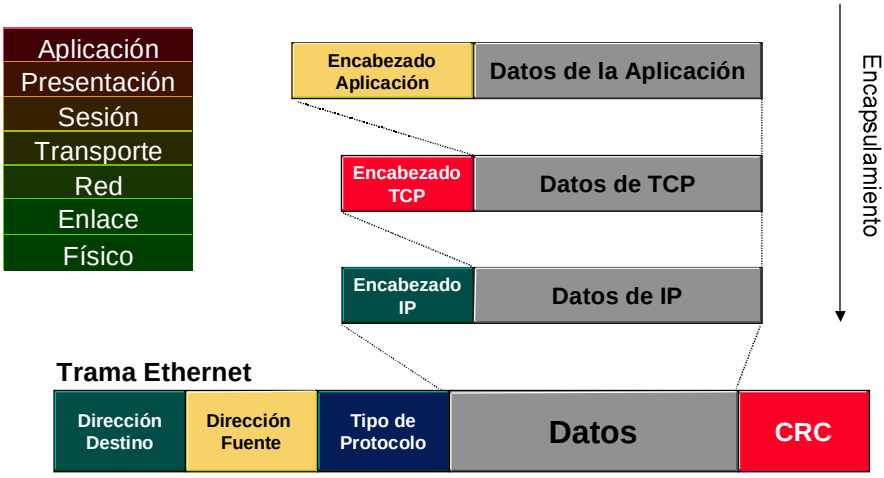


Familia de protocolos TCP/IP y el modelo OSI



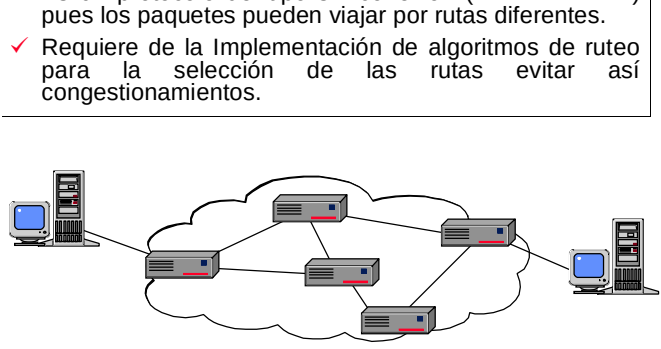
SMTP:	*Simple Mail Transfer Protocol*
FTP:	*File Transfer Protocol*
TFTP:	*Trivial File Transfer Protocol*
HTTP:	*Hypertext Transfer Protocol*
NFS:	*Network File System*

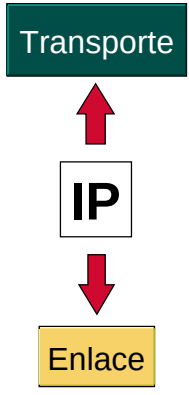
Encapsulamiento de Datos en TCP/IP



Protocolo IP (*Internet Protocol*)

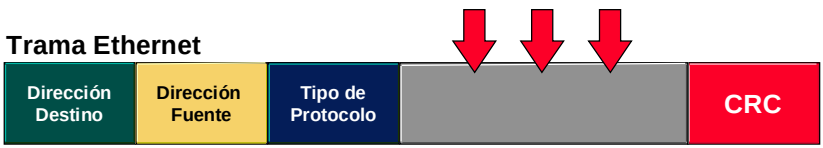
- ✓ Es el protocolo más conocido de la Internet y se encuentra definido en los RFC´s 791, 1122 y 1812.
- ✓ Su función principal es el direccionamiento que permite el llevar información de una máquina a otra través de la Internet.
- ✓ Es un protocolo del tipo sin conexión (*connectionless*) pues los paquetes pueden viajar por rutas diferentes.
- ✓ Requiere de la Implementación de algoritmos de ruteo para la selección de las rutas evitar así congestionamientos.



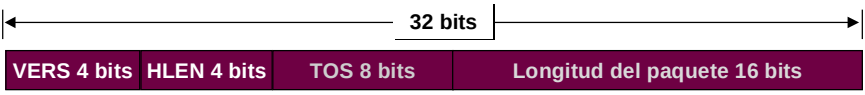


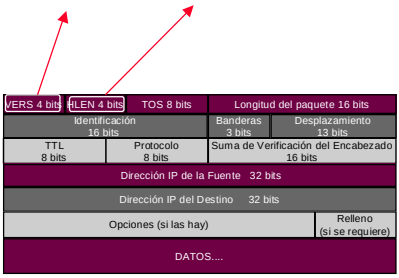
Estructura del paquete IP (Datagrama)

Trama Ethernet



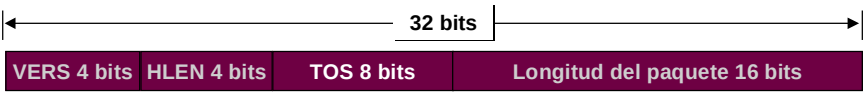
Campos: VERS y HLEN





- ✓ **VERS:** Versión, consta de 4 bits e indica la versión del protocolo. La versión más usada es 4 y ya existe también la versión 6 ó IPng.
- ✓ **HLEN:** Longitud de encabezado, consta de 4 bits e indica la longitud del encabezado en palabras de 32 bits. Se considera el encabezado hasta el inicio del campo de datos. Con esto se sabe si hay opciones adicionales en el encabezado o no. Si no hay opciones el valor es de 5 pues se tiene un total de 20 Bytes en el encabezado, lo que equivale a 5 palabras de 32 bits.

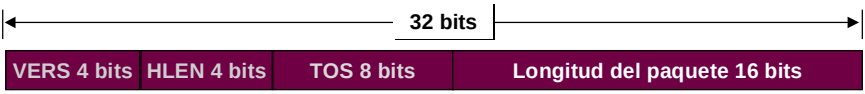
Campo: TOS (Type Of Service)



P: Estos 3 bits indican uno de los 8 niveles posibles de procedencia o prioridad.
D: Solicita una conexión de bajo retardo
T: Solicita alto troughput.
R: Solicita alta confiabilidad.
C: Solicita una ruta con el más bajo costo.
U: No se usa.

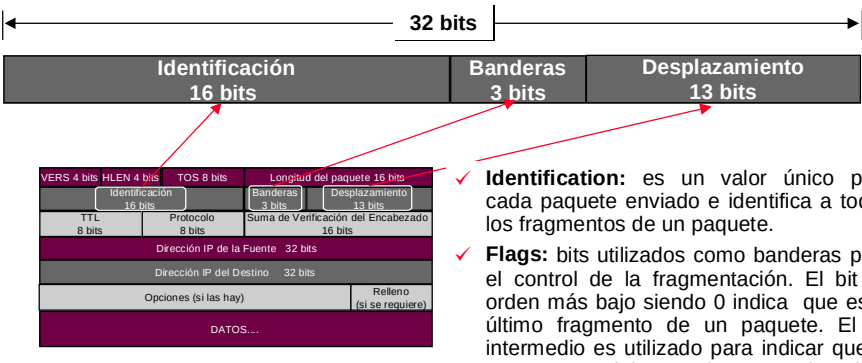
- ✓ **TOS:** Tipo de servicio, contiene las banderas utilizadas por TOS. Los primeros 3 bits son utilizados para indicar uno de los 8 niveles de precedencia. Este campo permite al software la solicitud de diferentes clases de desempeño para un datagrama.

Campo:Total Length



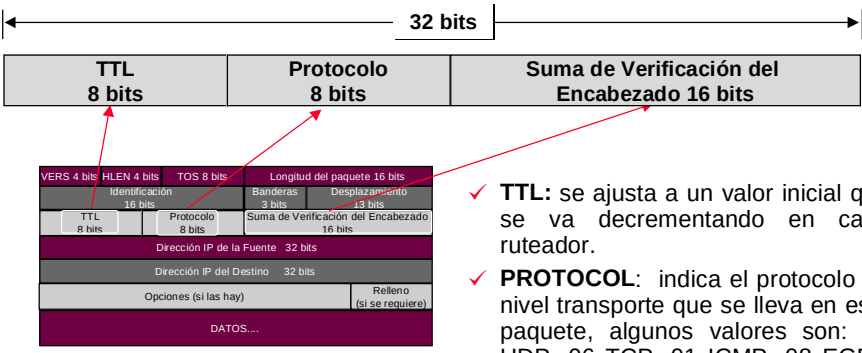
- ✓ **Total Length:** Longitud del paquete, consta de 16 bits e indica la longitud total del paquete de IP medido en Bytes incluyendo el encabezado y los datos. Los 16 bits de este campo implican que el tamaño máximo del paquete es de 65535 Bytes.

Campos: Identification, Flags y Offset



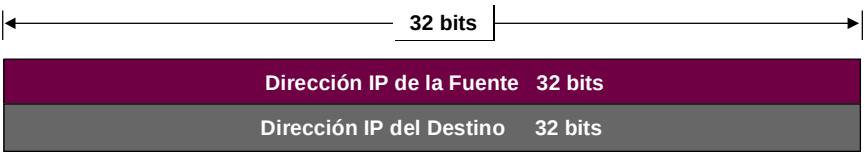
- ✓ **Identification:** es un valor único para cada paquete enviado e identifica a todos los fragmentos de un paquete.
- ✓ **Flags:** bits utilizados como banderas para el control de la fragmentación. El bit de orden más bajo siendo 0 indica que es el último fragmento de un paquete. El bit intermedio es utilizado para indicar que el paquete no debe ser fragmentado. El bit de orden superior no es utilizado.
- ✓ **Desplazamiento del fragmento**: consta de 13 bits y este campo es utilizado en los paquetes fragmentados para indicar la posición que los datos en este fragmento ocupan en el paquete original. El valor mostrado indica la posición en grupos de 8 Bytes.

Campos: TTL, Protocol y Checksum



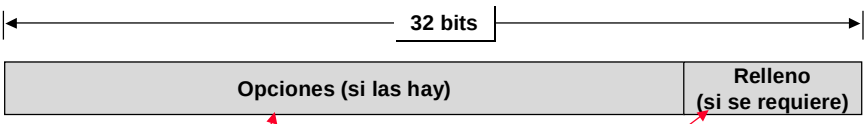
- ✓ **TTL:** se ajusta a un valor inicial que se va decrementando en cada ruteador.
- ✓ **PROTOCOL**: indica el protocolo de nivel transporte que se lleva en este paquete, algunos valores son: 17 UDP, 06 TCP, 01 ICMP, 08 EGP , 89 OSPF.
- ✓ **CHECKSUM:** Sirve para verificar la ocurrencia de errores pero sólo en el encabezado y no en los datos que están siendo transportados. Se debe recalcular cada vez que el paquete pasa por un ruteador.

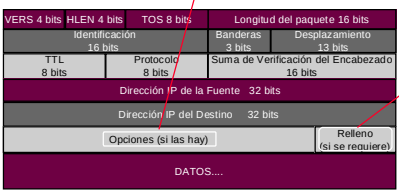
Campos: Source y Destination



- ✓ **SOURCE ADDRESS:** Dirección IP de la fuente, consta de 32 bits y es la dirección IP de la máquina que envía el paquete.
- ✓ **DESTINATION ADDRESS:** Dirección IP del destino, consta de 32 bits y es la dirección IP de la máquina que recibirá el paquete.

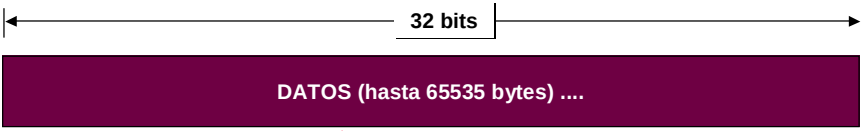
Campos: Options y Padding





- ✓ **OPTIONS**: soporta facilidades de operación y mantenimiento como solución de fallas, mediciones y seguridad. Un paquete puede contener varias opciones.
- ✓ **PADDING**: es de tamaño variable y representa a los 0´s utilizados de relleno para lograr que el encabezado sea un múltiplo entero de palabras de 32 bits.

Campo: DATOS

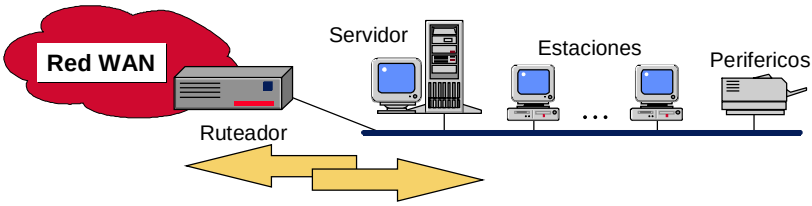


- ✓ **Datos**: es variable e incluye los encabezados de los protocolos de niveles superiores y los datos del usuario.
- ✓ Dado que el encabezado de longitud total es de 16 bits, el tamaño máximo del datagrama es de 65,535 octetos.
- ✓ Sin embargo, pueden ajustarse a los máximos de redes físicas, como 1500 para Ethernet.

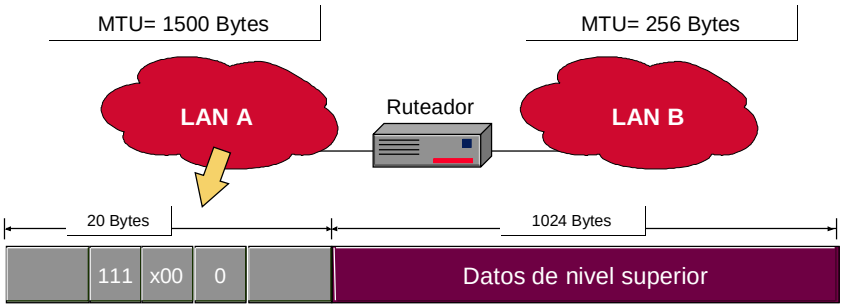
Nota : para más información sobre IP, referirse al RFC 791

Fragmentación y Reensamblaje (1)

- ✓ El tamaño de los paquetes está sujeto a la máxima capacidad de las tramas del nivel 2 e IP se encarga de reducir (fragmentar) los paquetes para que puedan ser transportados adecuadamente.
- ✓ En principio los niveles superiores pueden entregar a IP paquetes de información de cualquier tamaño e IP se debe encargar de fragmentar y reensamblar cuando se excede la capacidad de las tramas de nivel 2.
- ✓ Al límite del nivel 2 visto por IP se le conoce como **MTU (*Maximum Transfer Unit*).**
- ✓ Esto puede suceder en la frontera LAN-WAN y LAN-LAN.

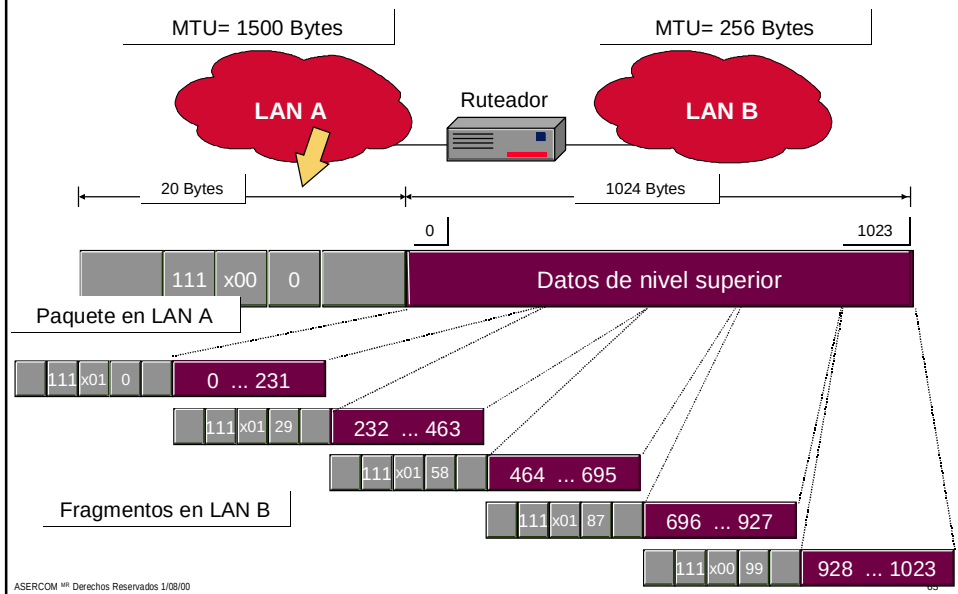


Fragmentación y Reensamblaje (2)



- ✓ Todos los fragmentos transportan los 32 bits que identifican al paquete original en el campo de identificación. Además, cada fragmento lleva información que indica su posición dentro del paquete original y si es o no el último fragmento.
- ✓ Con esta información es posible realizar el reensamblaje, el cual sólo se realiza en el destino final.

Fragmentación y Reensamblaje (3)



Características de TCP y UDP

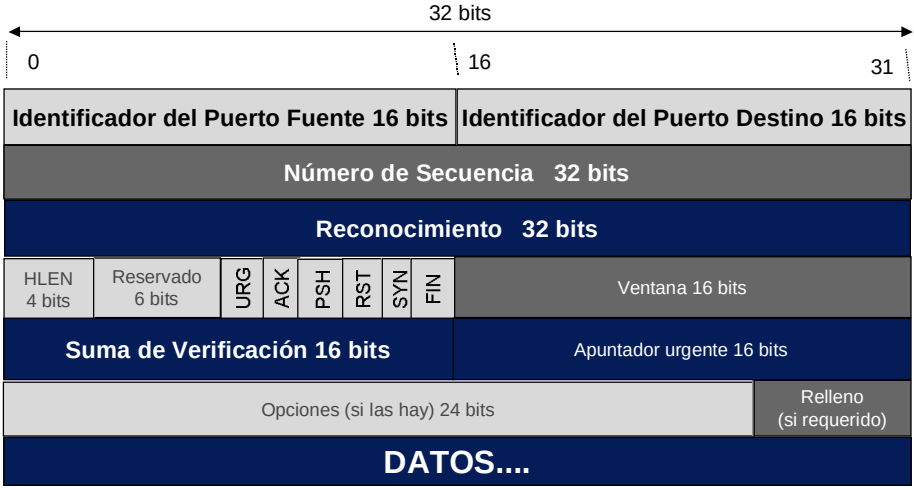
UDP

- ✓ Proporciona un servicio poco confiable y sin conexión.
- ✓ Permite transmitir datos a una o varias máquinas sin necesidad de establecer una conexión.
- ✓ Los paquetes se envían sin esperar confirmación de recepción.
- ✓ Aplicaciones como TFTP, NFS, RTP (VoIP) usan este modo de transporte.
- ✓ Para servicio de *broadcast*, UDP es la única opción.

TCP

- ✓ Proporciona un servicio orientado a conexión (una conexión es un enlace punto a punto, circuito virtual).
- ✓ TCP tiene la capacidad de proporcionar un servicio confiable entre 2 máquinas.
- ✓ Esta confiabilidad implica un aumento significativo en el encabezado (maneja ACK, control de flujo, timers).
- ✓ Aplicaciones como Telnet, FTP usan TCP.
- ✓ No hay posibilidad de *broadcast* o *multicast*.

Estructura de TCP

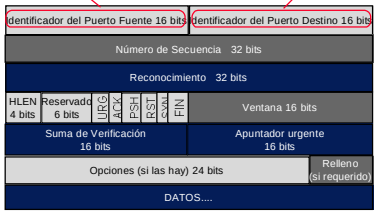


HLEN:	header length	URG:	urgent
ACK:	acknowledgement	PSH:	push request
RST:	reset the connection	SYN:	synchronize
FIN:	final flag, connection terminated		

Descripción de los campos TCP (1)

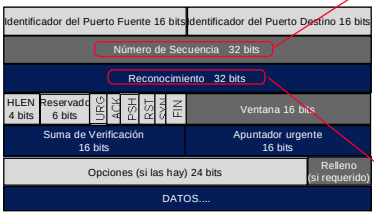
Puerto Fuente (**SOURCE PORT**): Campo de 16 bits que identifica el usuario de TCP local. Ejemplos: FTP 23, SMTP 25, 69 TFTP, 79 FINGER, 110 POP3, 161 SNMP, 179 BGP.

Puerto Destino (**DESTINATION PORT**): Campo de 16 bits que identifica el usuario de TCP de la máquina remota



Descripción de los campos TCP (2)

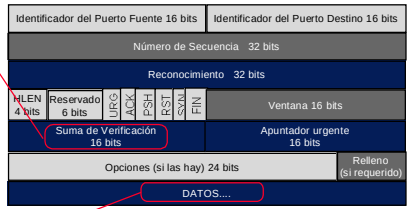
Número de Secuencia (**SEQUENCE NUMBER**): Posición del bloque actual en el mensaje total.



Número de Acuse de recibo (**ACKNOWLEDGEMENT NUMBER**): Número que indica el siguiente número de secuencia que se espera. (número de secuencia que se recibió más 1)

Descripción de los campos TCP (3)

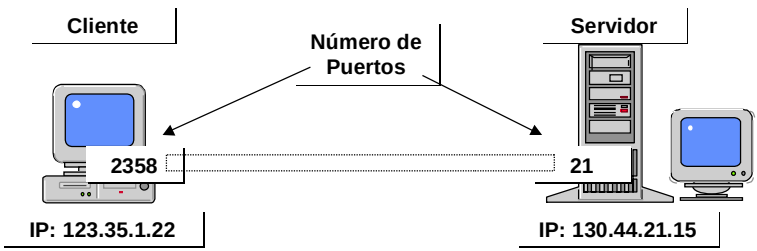
Suma de Verificación (**CHEKSUM**): Se calcula tomando el complemento a uno de 16 bits de la suma de complementos a uno de las palabras de 16 bits en el encabezado y el texto juntos.



DATOS: es variable e incluye los encabezados de los protocolos de niveles superiores y en algunas ocasiones los datos del usuario.

Nota: para más información sobre TCP, referirse al RFC 793

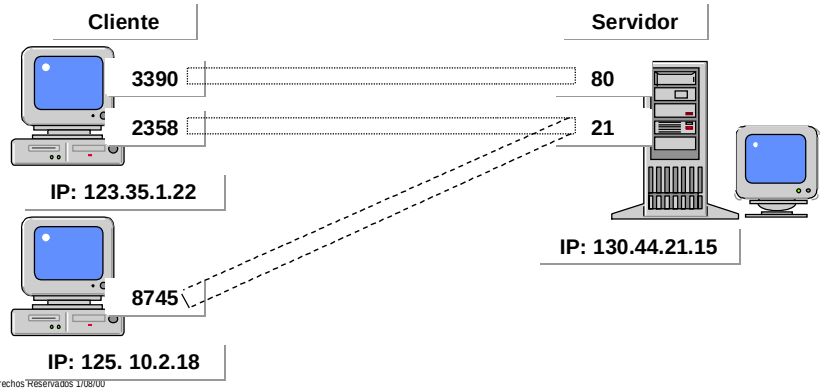
Puertos de TCP



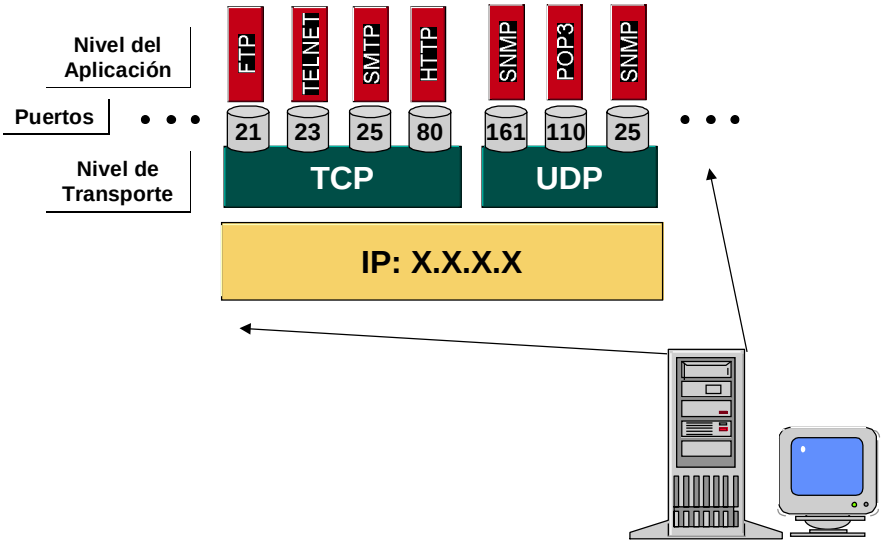
- ✓ Un cliente debe identificar cuál es el servicio que desea utilizar en un servidor **especificando la dirección IP del host que atenderá el servicio** junto con **su número de puerto TCP.**
- ✓ Un puerto es una dirección de 16 bits en cada máquina, Por lo que pueden existir **65535** puertos diferentes.
- ✓ Los Puertos se encuentran definidos en **RFC 1060**.
- ✓ Esta dirección o número de **puerto está relacionado a las aplicaciones** más comunes.
- ✓ Por otro lado el cliente utiliza en la mayoría de los casos un número de puerto no utilizado para atender las respuestas del servidor.
- ✓ Puertos más comúnes: **80(HTTP), 21(FTP), 23(TELNET), 25(SMTP), 161(SNMP).**

Sockets - I

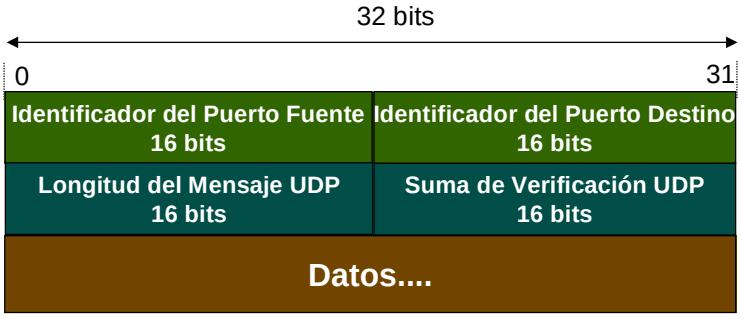
- ✓ La combinación lógica de una dirección IP más un puerto TCP se conoce como un Socket.
- ✓ Un servidor normalmente es capaz de manejar varios clientes al mismo tiempo.
- ✓ La dirección de Socket es única y será accesada simultáneamente por varios clientes.

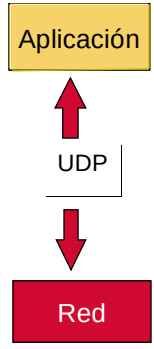


Sockets - II



Protocolo UDP (*User Datagram Protocol*)

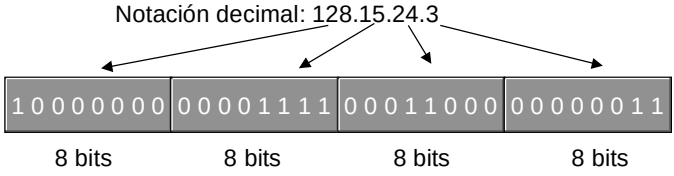




- ✓ Funciona de manera muy similar a TCP.
- ✓ A diferencia de TCP, UDP proporciona un servicio sin conexión, pues no se realizan confirmaciones.
- ✓ Tampoco se numeran los mensajes, por lo que pueden arribar en desorden.
- ✓ Sin embargo si se manejan los sockets de la misma manera que en TCP.
- ✓ Es utilizado por aplicaciones de audio sobre la Internet como Real Audio.

Direcciones IP

- ✓ La versión 4 de IP (IPv4) **asigna 32 bits** de longitud para el manejo de direcciones, con esto es posible manejar **4,294,967,296** direcciones diferentes.
- ✓ A cada interfaz física le es asignada **una única dirección.**
- ✓ Existen direcciones registradas y no registradas (**Homologadas**).
- ✓ Se pueden asignar de manera **estática** por el administrador o de manera **dinámica** (p.ej. Con DHCP).
- ✓ Cada paquete IP o datagrama contiene una **dirección fuente (source)** y una **dirección destino (destination**).
- ✓ Las direcciones se escriben en un **formato decimal "doted-decimal"** como se muestra en la figura siguiente:

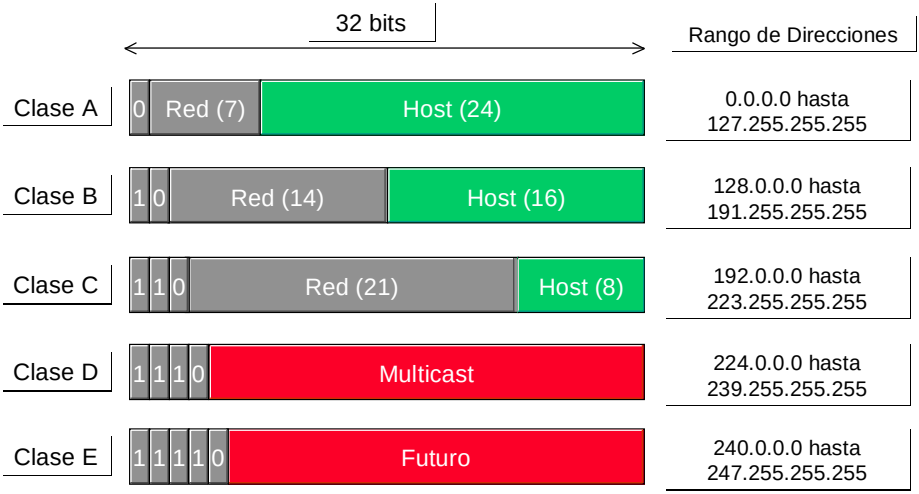


Direccionamiento con tipo de clase (Classfull)

- ✓ En 1981 se especificó que cualquier dispositivo basado en IP conectado a la Internet debía manejar una única dirección para cada interfaz de red.
- ✓ El modelo con tipo de clase divide a las direcciones IP en dos partes:

- ✓ Con esta división se crearon **5 clases** de direcciones:
  - **Clase A:** Para redes muy grandes, con **7** bits para el número de red.
  - **Clase B:** Para redes medianas, con **14** bits para el número de red.
  - **Clase C:** Para redes pequeñas, con **21** bits para el número de red.
  - **Clase D:** Esta clase está reservada para el servicio **IP Multicasting**.
  - **Clase E:** Esta clase se encuentra reservada para **uso futuro**.

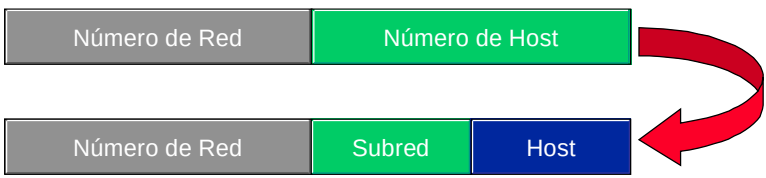
Clases de direcciones IP



- ✓ La dirección 0.0.0.0 se encuentra reservada para uso como identificador de red/host por omisión.
- ✓ La dirección 127.0.0.0 está reservada para la función de *loopback*.
- ✓ La dirección 255.255.255.255 se utiliza para *broadcast*.

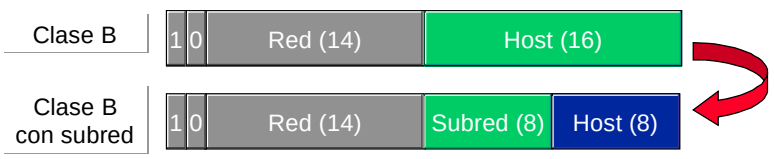
Subredes (Subnetting)

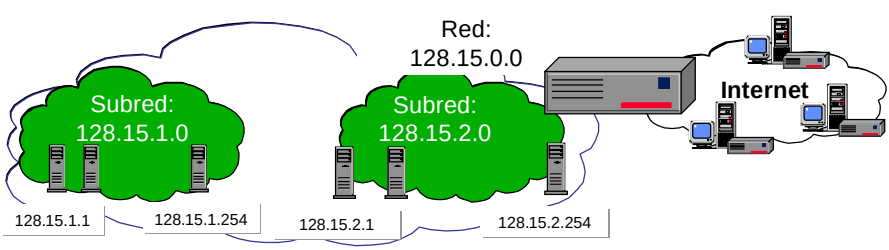
- ✓ En el diseño original del direccionamiento no se previeron ciertas limitantes que encontramos actualmente:
  - Inicialmente se **pensaba que se tenía una capacidad ilimitada** de direcciones y se hacía una asignación indiscriminada.
  - **Las clases** de direcciones eran bien entendidas e implementadas, sin embargo **no promovía una asignación eficiente** de un recurso que entonces se pensaba ilimitado.
  - **La división de clases no es muy adecuada**. Para una empresa mediana en realidad una dirección clase C (254 hosts) resultaba muy pequeña y una dirección clase B (65,534 hosts) muy grande.
- ✓ En respuesta a esto en **1985 se publicó el RFC 950**, el cual definía el procedimiento de **subredes (subnetting)** permitiendo un división de las clases A, B y C en unidades más pequeñas.



Ejemplo de Subredes

- ✓ El uso de subredes permite al administrador un manejo más eficiente de las direcciones y evita que las tablas de ruteo crezcan sin necesidad.
- ✓ A continuación un ejemplo en donde una dirección clase B es dividida en subredes tomando 8 bits de los 16 correspondientes al host.





Máscaras de Subred (Subnet Mask)

- ✓ Cada ruteador utiliza el número de red para determinar que tan lejos se encuentra de otras redes y el número de hosts para encontrar el destino físico.
- ✓ Cuando se introdujo el concepto de subredes fue necesario crear el concepto de Máscaras de Subred (Subnet Mask) para separar la porción de información de red de la porción de información de host.
- ✓ Este información le dice al ruteador el número de bits que corresponden al número de la red extendido (red + subred).

Ejemplo 1

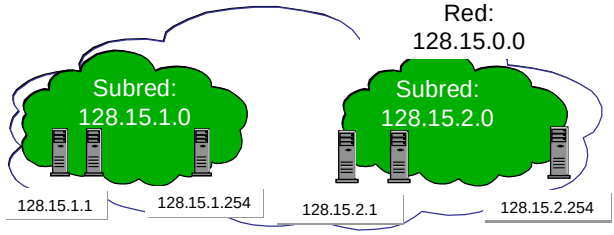
		Número de Red	Subred	Host
Dirección IP	130.5.5.25	10000010 . 00000101	. 00000101.	00011001
Máscara de Subred	255.255.255.0	11111111 . 11111111 .	11111111.	00000000

Ejemplo 2

		Número de Red	Subred	Host
Dirección IP	130.5.5.25	10000010 . 00000101	. 00000101.	00011001
Máscara de Subred	255.255.255.224	11111111 . 11111111 .	11111111.	11100000

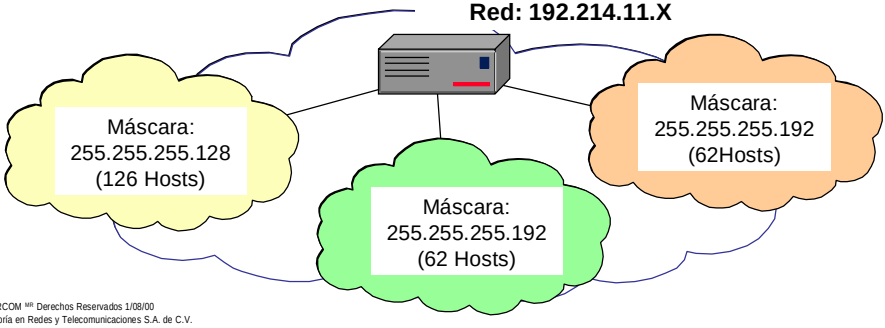
Consideraciones para la asignación de Subredes

- ✓ Determinar el número de subredes actual y futuro.
- ✓ Determinar el número de host actual y futuro en la subred más grande.
- ✓ Recordar que el número de subredes al igual que el número de hosts crece en potencia de dos (2^x), en donde x es el número de bits del número de subred o de host.
- ✓ Determinar si la dirección asignada actualmente satisface las necesidades definidas, en caso contrario se puede recurrir al direccionamiento privado o a la traslación de direcciones (NAT).



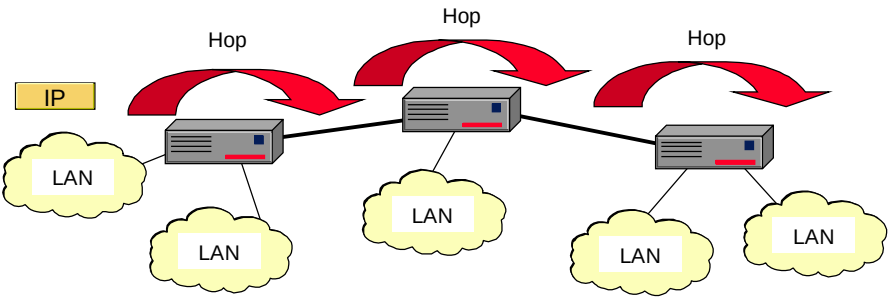
Longitud de Máscara de Subred Variable (VLSM)

- ✓ Longitud de Máscara de Subred Variable (VLSM: Variable Length Subnet Mask).
- ✓ En 1987, en el RFC 1009 se definió como un red podía utilizar más de una máscara de subred.
- ✓ Este concepto permite mayor flexibilidad en la divisón de una red en múltiples subredes. Permitiendo a cada subred manejar el número adecuado de hosts.
- ✓ Nota: Los protocolos de ruteo RIP V1.0 e IGRP no soportan VLSM.



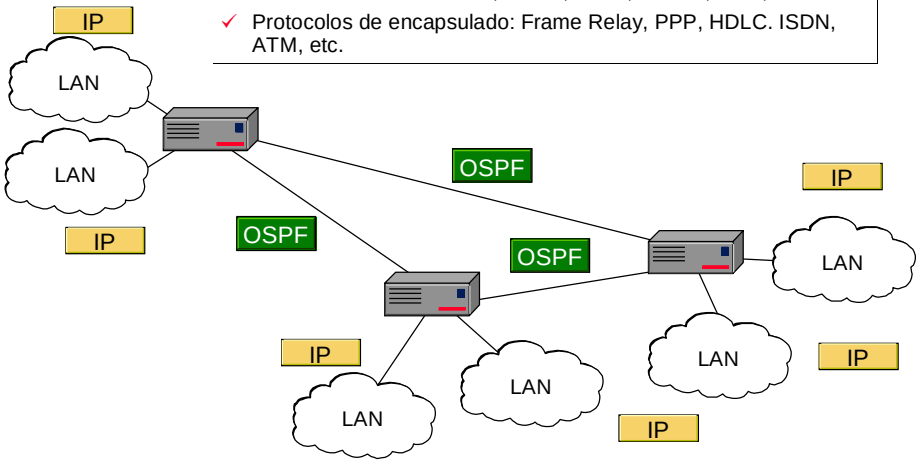
Funcionamiento básico de un ruteador

- ✓ Los ruteadores operan bajo un mecanismo conocido salto-a-salto **(hop-to-hop),** dando seguimiento a la información del "salto siguiente" o en inglés "next hop" que habilita a un paquete de datos llegar a su destino final.
- ✓ Cuando un ruteador no cuenta con una conexión física hacia un destino, verifica en su tabla de ruteo y transfiere el paquete a otro ruteador "salto siguiente".
- ✓ Este proceso se repite hasta que el paquete alcanza su destino final.



Protocolos en un ruteador

- ✓ Protocolos Ruteados: IP, IPX, DECnet, OSI, XNS, DDP, etc...
- ✓ Protocolos No ruteables: LAT, NETBEUI, etc...
- ✓ Protocolos de Ruteo: RIP, OSPF, IGRP, EIGRP, BGP, etc...
- ✓ Protocolos de encapsulado: Frame Relay, PPP, HDLC. ISDN, ATM, etc.



Tablas de Ruteo

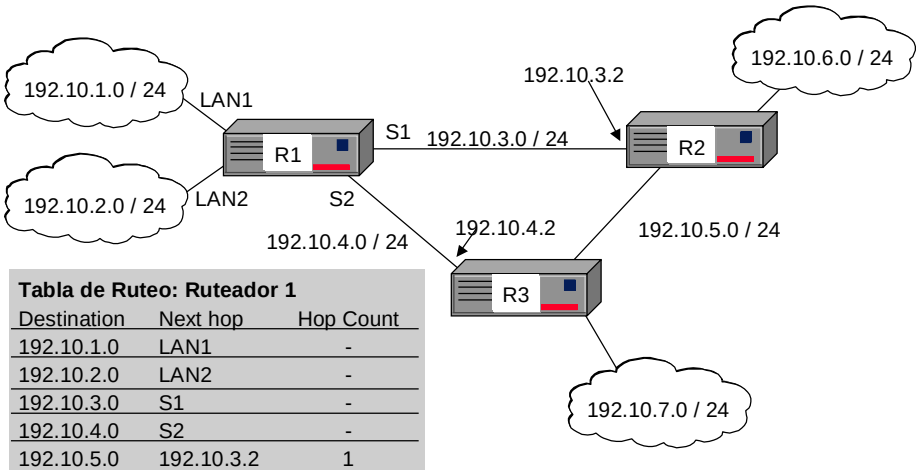


Tabla de Ruteo: Ruteador 1

Destination	Next hop	Hop Count
192.10.1.0	LAN1	-
192.10.2.0	LAN2	-
192.10.3.0	S1	-
192.10.4.0	S2	-
192.10.5.0	192.10.3.2	1
	192.10.4.2	1
192.10.6.0	192.10.3.2	1
192.10.7.0	192.10.4.2	1

Nota: La notación X.X.X.X / 24 nos dice la longitud en bits del número de red extendido (red + subred).

Classless Inter-Domain Routing (CIDR)

- ✓ En los últimos años **el crecimiento de las tablas de ruteo** dentro de la Internet comenzó a preocupar seriamente.
- ✓ El **agotamiento de las direcciones Clase B** no se veía muy lejano.
- ✓ Como respuesta a esto se **redefinieron las políticas de asignación** de direcciones y **adicionalmente en Septiembre de 1993 se publicaron los RFC 1517, 1518, 1519 y 1520,** en donde se definía el concepto de **Superredes (Supernetting) o Classless Inter-Domain Routing (CIDR).**
- ✓ Cuando se **anuncia una dirección con CIDR es necesario incluir una máscara** en donde se indica el número de bits de la porción de red de la dirección IP, sin hacer caso de los bits que definen las clases de direcciones.
- ✓ El uso de CIDR aporta dos características de gran beneficio para el sistema de ruteo de la Internet:
  - Con CIDR se **elimina el concepto** tradicional de manejo de clases de direcciones A, B y C **(Classless).** Esto permite una asignación más eficiente de las direcciones de IPv4 mientras IPv6 es implementado.
  - CIDR soporta la **agregación de rutas**, en donde una sola entrada a la tabla de ruteo puede representar cientos o miles de direcciones Classfull tradicionales

Notación para el uso de CIDR

- ✓ Los términos **agregada (aggregate**), **bloque CIDR (CIDR block) y superred (supernet)** regularmente son utilizados de manera **intercambiables** en la práctica. En forma general, con cualquiera de ellos se pretende indicar que **una lista de direcciones IP contiguas** han sido **resumidas en un solo mensaje**.
- ✓ Con la **notación se especifica la longitud en bits de la superred**. El prefijo de la superred es más pequeño que la máscara natural.
- ✓ Los dominios de **ruteo que soportan CIDR** se les llama sin clase (Classless).

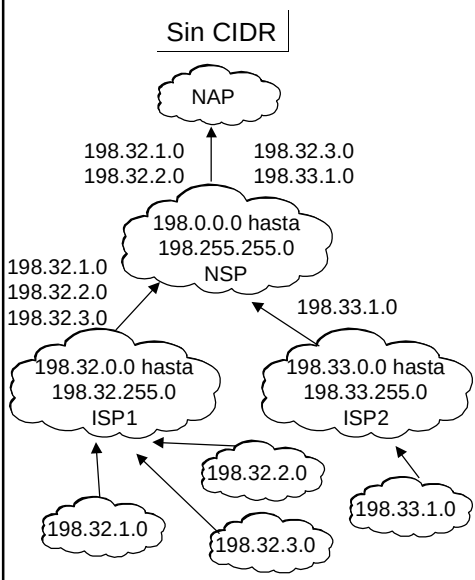
198.132.1.0 255.255.255.0 <==> 198.132.1.0 / 24
198.132.0.0 255.255.0.0 <==> 198.132.1.0 / 16

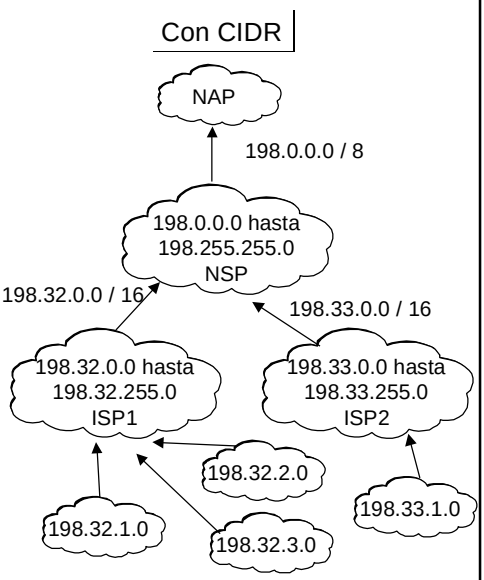
		Número de Red	Subred	Host
Dirección Clase C	198.132.1.0	11000110 . 00100000	. 00000001	. 00000000
Máscara	255.255.255.0	11111111 . 11111111	. 11111111	. 00000000
Máscara	255.255.0.0	11111111 . 11111111	. 00000000	. 00000000

Superred

Máscara Natural

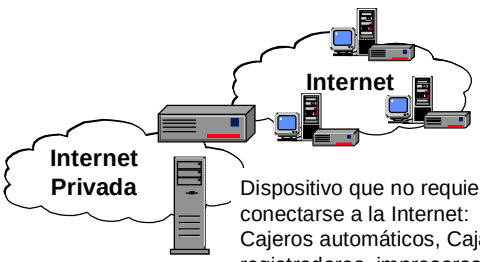
Ejemplo de uso de CIDR





Direcciones IP Privadas (*Private Addressing*)

- ✓ Prácticamente las necesidades de conectividad de la mayoría de las organizaciones cae en una de las siguientes categorías:
  - Conectividad global
  - Conectividad privada (total o parcial)
- ✓ En la segunda categoría encontramos algunos dispositivos dentro de la organización que no necesitan conectarse a la Internet.
- ✓ Para ellos el IANA ha reservado tres bloques de direcciones IP (Internets Privadas), RFC 1918.



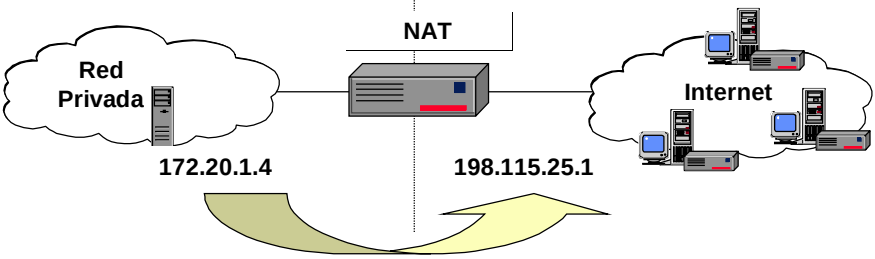
Dispositivo que no requiere conectarse a la Internet: Cajeros automáticos, Cajas registradoras, impresoras, etc.

Bloques reservados

- **10.0.0.0 a 10.255.255.255**
- **172.16.0.0 a 172.31.255.255**
- **192.168.0.0 a 192.168.255.255**

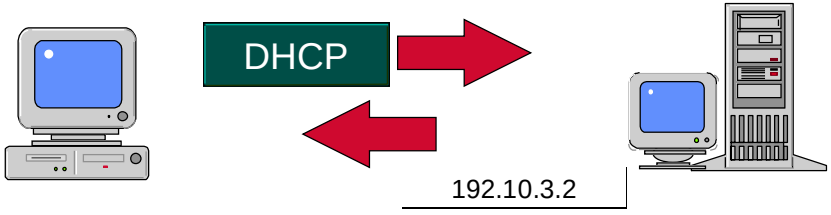
Network Address Translation (NAT)

- ✓ Las compañías que utilizan un esquema de direccionamiento privado por alguna razón, y desean conectividad con la Internet pueden resolver el problema de dos formas:
  - Reasignación de direcciones dentro de la organización
  - Utilización de la función de Traslación de direcciones de red (NAT).
- ✓ La utilización de NAT permite relacionar direcciones privadas con direcciones globales. Especificado en los **RFC 1631 y 2391**.
- ✓ Tiene como beneficios un uso más eficiente de las direcciones así como un esquema mejor de seguridad.
- ✓ Pero por otro lado se tiene un encabezado adicional y una tarea de administración adicional.



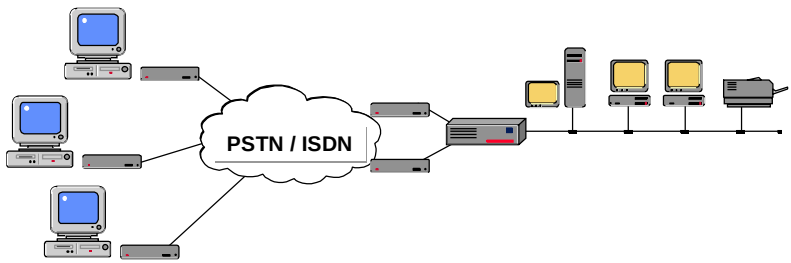
DHCP (*Dynamic Host Configuration Protocol*)

- ✓ Protocolo utilizado para la asignación automática de direcciones IP.
- ✓ Es utilizado por los proveedores de Internet para proporcionar las direcciones IP a los usuarios.
- ✓ También se utiliza en redes LAN.
- ✓ Especificado en los RFCs 2131, 2132, 1542 y 1534.
- ✓ Tiene como beneficios la simplicidad en la administración y la disponibilidad de direcciones IP.



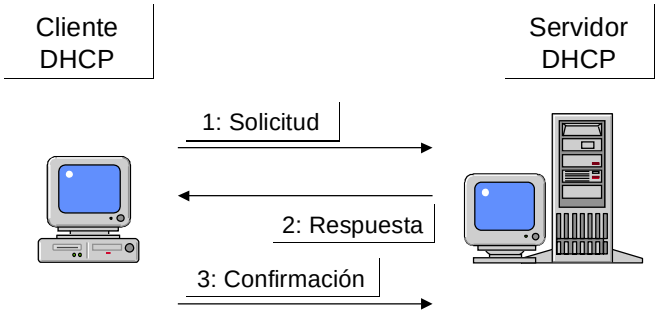
Modos de Operación de DHCP

- Modos de Operación (LAN o Acceso Remoto):
  - **Manual** : Al igual que en BOOTP el administrador puede configurar una dirección específica para una máquina específica al momento de solicitar su dirección.
  - **Automática**: El servidor DHCP asigna una dirección permanente a una máquina la primera vez que se conecta a la red.
  - **Dinámica**: El servidor DHCP asigna una dirección a la máquina por un tiempo limitado



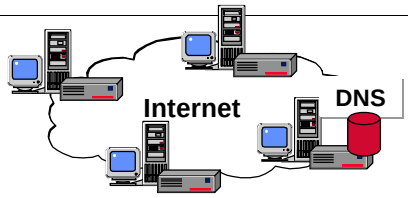
Operación Básica de DHCP

- Operación Básica:
  - 1: El cliente DHCP solicita una dirección.
  - 2: El servidor DHCP asigna la dirección.
  - 3: El cliente DHCP confirma



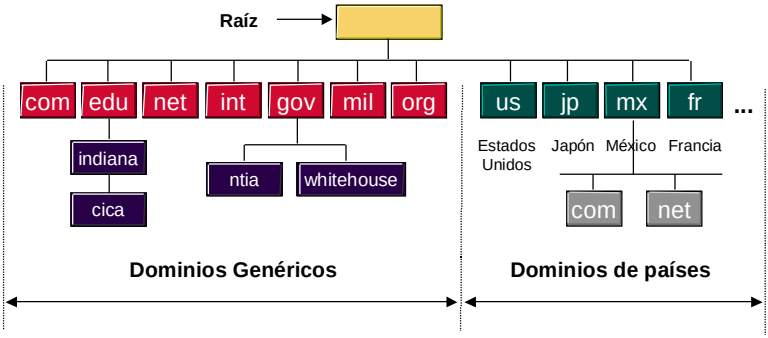
DNS (*Domain Name System*)

- ✓ El **DNS** (*Domain Name System*) fue uno de los desarrollos clave que permitió el gran crecimiento que tiene la Internet actualmente.
- ✓ Básicamente es una base de datos distribuida que contiene los nombres y las direcciones de cada sitio al cual se puede tener acceso vía Internet y evita el tener que manejar o memorizar complejas direcciones IP directamente.
- ✓ Características:
  - Los archivos DNS son administrados por miles de servidores en la red
  - Las bases de datos son actualizadas automáticamente.
  - Tiene mecanismos que permiten la identificación de los servidores de backup por si el servidor de nombres principal no se encuentra disponible.



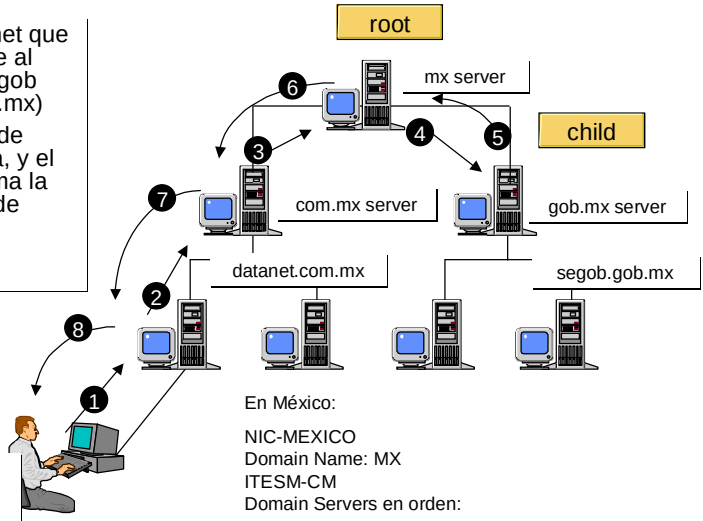
Estructura Jerárquica del DNS

- ✓ Todos los nombres de sitios terminan con un dominio de orden superior y van decreciendo en cobertura hasta llegar al dominio de una red en particular.
- ✓ En la realidad un servidor de nombres contiene grandes porciones del árbol de nombres. De está manera un servidor no tiene que enviar una consulta a través de muchos servidores de nombres para poder resolver el nombre que busca.
- ✓ Cada servidor de nombres es responsable por una o más zonas de la estructura del DNS y a su vez cada zona tiene un servidor de nombres primario y uno o varios secundarios como backup.



Ejemplo de consulta de dirección

- ✓ Usuario de Internet que desea conectarse al web site de la segob (www.segob.gob.mx)
- ✓ Este proceso es de manera recursiva, y el DNS primario toma la responsabilidad de encontrar la información.



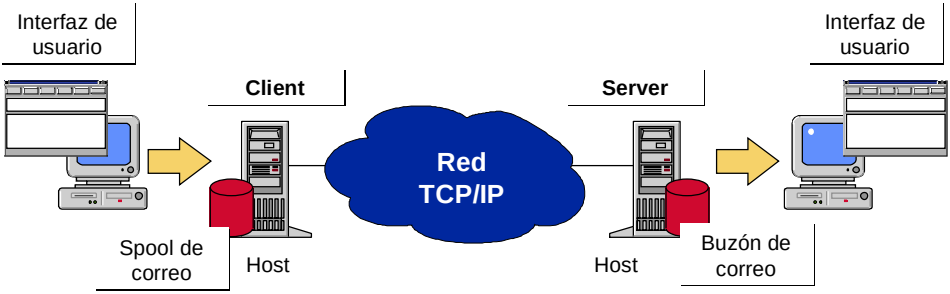
Usuario de datanet:
DNS Primario:
datanet.com.mx

En México:

NIC-MEXICO
Domain Name: MX
ITESM-CM
Domain Servers en orden:

NS.NIC.MX: 200.23.1.1
DNS.MTY.ITESM:MX: 131.178.38.39
SUNMEX.MEXNET.NET.MX 131.178.1.150

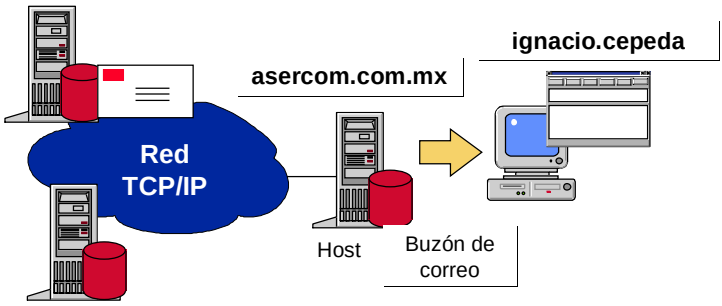
SMTP (*Simple Mail Transfer Protocol*)



- ✓ El protocolo SMTP permite enviar y recibir correo electrónico a través de una red IP pública o privada. Transmitiendo los correos de servidor a servidor hasta llegar al buzón del destinatario.
- ✓ Normalmente SMTP entrega el correo directamente desde el host origen a cada host receptor a través de una conexión TCP/IP confiable.
- ✓ Opera de una manera similar a FTP y se encuentra especificado en RFC 1869, RFC 1870 y RFC 1891.
- ✓ El transmisor envía comandos ASCII y el servidor responde con respuestas numéricas y de texto.

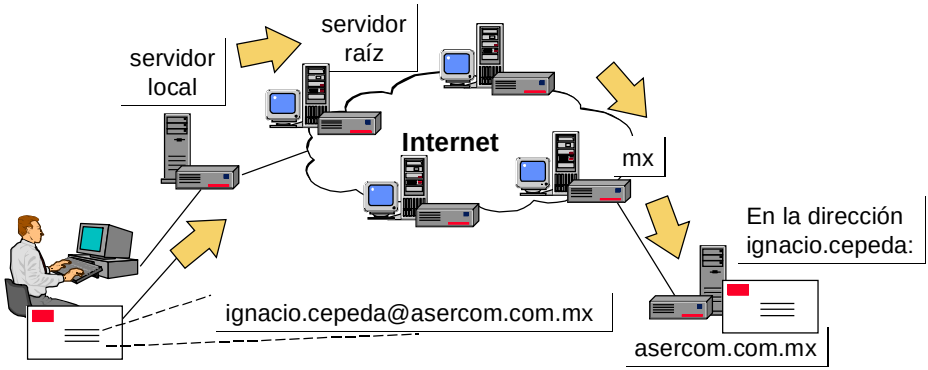
Direcciones e-mail

local-part@domain-name
ej: ignacio.cepeda@*asercom.com.mx*



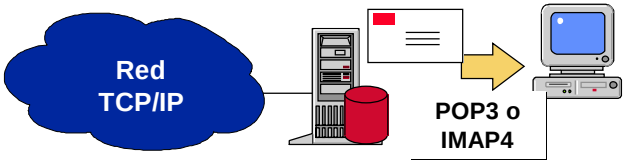
- ✓ **domain-name**: Es el servidor de dominio e identifica la dirección de red en donde se encuentra el host de correo.
- ✓ **local-part**: identifica al usuario o bien la entidad a la que efectivamente esta dirigido el correo.

DNS y el correo electrónico (e-mail)



Internet se sirve de los archivos DNS (*Domain Name Service*) presentes en los servidores, para buscar los nombres del destinatario. El servidor local inicia la operación conectándose al servidor raíz (computadora que conoce el dominio máximo), éste indica qué ruta tomar hasta llegar al "buzón" del usuario destino pasando por el dominio **mx**, después por **asercom.com** y finalmente al usuario **ignacio.cepeda (buzón)**.

Protocolos de Recuperación de Correo



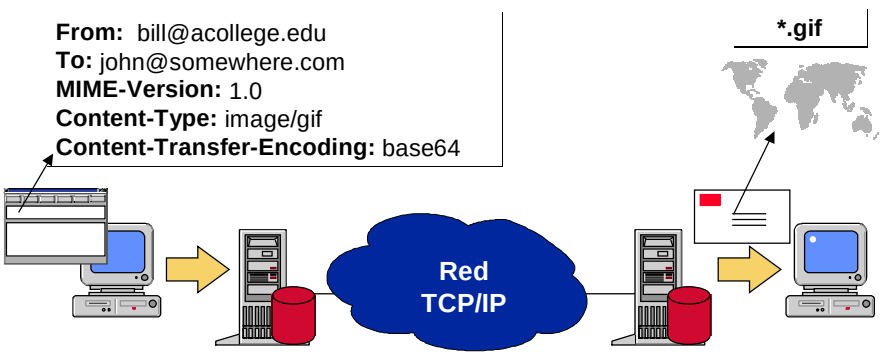
- ✓ **POP3 (Post Office Protocol version 3)**
  - Permite a un cliente recuperar su correo desde un servidor remoto
  - Este protocolo se usa en PC´s, que generalmente se desconectan varias veces, para recuperar su correo almacenado en un host permanente.
  - El host almacena los mensajes hasta que el cliente los solicite, de otra manera se generarían errores de entrega si el cliente estuviera desconectado
  - Especificado en RFC 1725
- ✓ **IMAP4 (Internet Message Access Protocol version 4)**
  - Protocolo similar a POP3
  - Además permite un movimiento bidireccional de mensajes y la administración de buzones remotos
  - Especificado en RFC 1730

MIME

- ✓ MIME (Multipurpose Internet Mail Extensions).
- ✓ Permite la transmisión de archivos binarios a través del e-mail.
- ✓ MIME permite que cualquier tipo de datos sean codificados en ASCII y después transmitidos con SMTP.

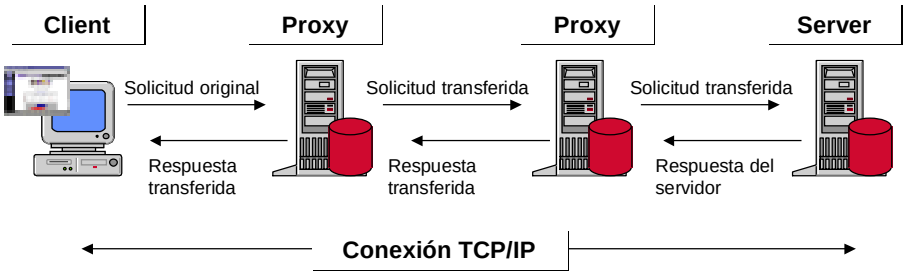
Encabezado de correo: identificador del tipo de datos

From: bill@acollege.edu
To: john@somewhere.com
MIME-Version: 1.0
Content-Type: image/gif
Content-Transfer-Encoding: base64



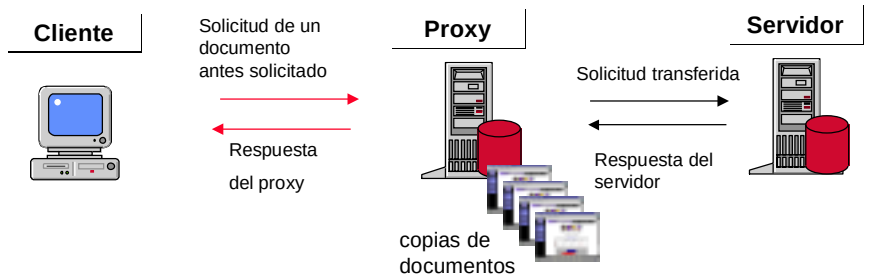
HTTP (*Hyper Text Transfer Protocol*)

- ✓ Este protocolo de nivel de aplicación es utilizado para acceder documentos hypermedia.
- ✓ El protocolo es genérico y puede ser utilizado para diversas tareas.
- ✓ Su uso principal ha sido como protocolo de transporte para el WWW.
- ✓ Se comunica mediante métodos de solicitud y respuestas para la transferencia de información.
- ✓ Utiliza TCP normalmente.



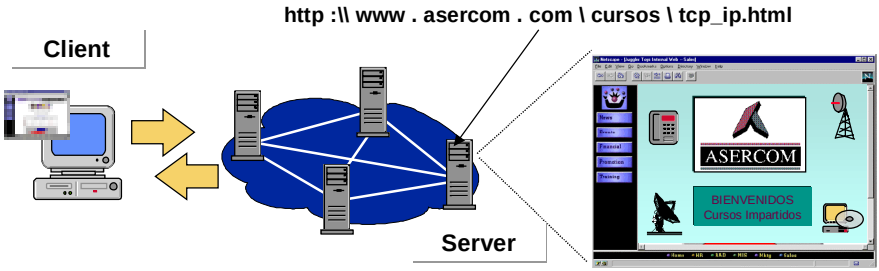
Proxy Server

- ✓ Un proxy es un servidor que direcciona las solicitudes de los clientes al servidor, o bien a otros servidores proxy.
- ✓ Cuando se forma una cadena de servidores proxy, un segundo ve al primero como cliente HTTP.
- ✓ Un proxy implementa copias de los documentos que recientemente se han accesado, si se vuelven a solicitar, ya no se piden al servidor y el proxy envía una de sus copias.



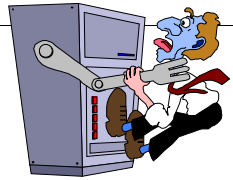
URL (*Universal Resource Locator*)

- ✓ El principal objetivo del Web es el proporcionar a los usuarios una forma sencilla de acceder a toda la información localizada en la Internet en forma de archivos.
- ✓ Para acceder esta información se debe especificar un URL, el cual es una secuencia de tres elementos:
  - Método (típicamente un protocolo: http, ftp, gopher, telnet, wais)
  - Localización en la Internet (dirección de host: www.asercom.com)
  - Nombre de archivo y subdirectorios (**** cursos \ tcp_ip.html)



El comando PING

- ✓ Es parte de un protocolo conocido como ICMP (*Internet Control Message Protocol*) que sirve para fines de diagnóstico.
- ✓ Los mensajes de Solicitud de eco (**Echo Request**) y Respuesta de eco (**Echo Reply**) pueden utilizarse para comprobar si un destino es alcanzable y si responde.
- ✓ El éxito de estos mensajes también implica un buen funcionamiento de los ruteadores intermedios de la red
- ✓ En muchos sistemas, el comando correspondiente se llama **PING (Packet Internet Groper).**
- ✓ Algunas versiones de PING envían una serie de mensajes, capturan las respuestas y proporcionan estadísticas sobre los paquetes (pérdidas, longitud, intervalos, etc.).



Ejemplo de comando PING