SERVICIOS TCP/IP

Módulo 9

Temas a tratar

1. Protocolo DHCP (Dynamic Host Configuration Protocol)
2. Servicio de Resolución de Nombres DNS (Domain Name System)
3. Protocolo de Correo Electrónico SMTP (Simple Mail Transfer Protocol)
4. Protocolo de Transferencia de Hipertexto HTTP (Hypertext Transfer Protocol)

Objetivos del módulo

Al finalizar el presente módulo el alumno debe ser capaz de:

- ✓ Conocer el alcance de las prestaciones de cuatros servicios claves en el desarrollo de internet: DHCP, DNS, Correo Electrónico y HTTP
- ✓ Comprender la arquitectura y el funcionamiento de los mismos
- ✓ Dimensionar la carga de tráfico que cada uno de ellos aporta a la red
- ✓ Entender aspectos principales relacionados con la implementación de estos servicios en el ámbito de una organización

Dynamic Host Configuration Protocol (DHCP)
Conceptos

- ✓ DHCP es un Servicio que se ejecuta desde la capa de Aplicación y que tiene como función principal configurar en forma automática los parámetros necesarios para que un dispositivo pueda ser parte activa de una red. RFC 1531, actual RFC 2131 y para IPv6 RFC 3315
- ✓ Cuando un sistema operativo arranca, inicia los protocolos y las aplicaciones. En el caso de la suite TCP/IP, necesita tener configurado al menos la dirección ip y la máscara de red. Esto se puede hacer en forma manual en cada dispositivo o automática, utilizando un protocolo como DHCP.
- ✓ Cumple dos funciones principales:
  - ✓ Asigna direcciones IP y otros parámetros TCP/IP (máscara de red, default gateway, servidor DNS, entre otros) en forma automática.
  - ✓ Negocia y transmite información específica del host.
- ✓ Extensión y mejora del protocolo Bootp (RFC 951)
- ✓ Usa UDP como puerto de transporte (67 y 68)

Dynamic Host Configuration Protocol (DHCP)
Fases del servicio

Cliente DHCP

Cliente solicita una dirección IP

Servidores DHCP ofrecen IP's

Cliente selecciona una dirección IP

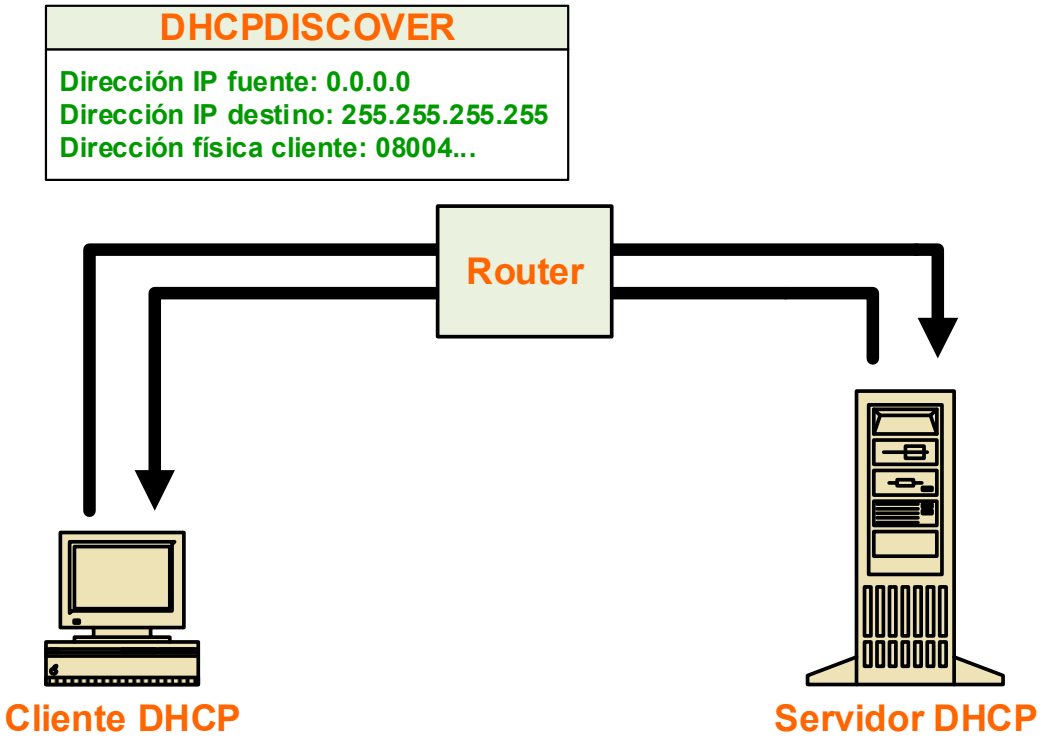
Servidor confirma alquiler de dirección IP

Servidor DHCP

Dynamic Host Configuration Protocol (DHCP)
¿ Por qué se solicita una dirección IP?

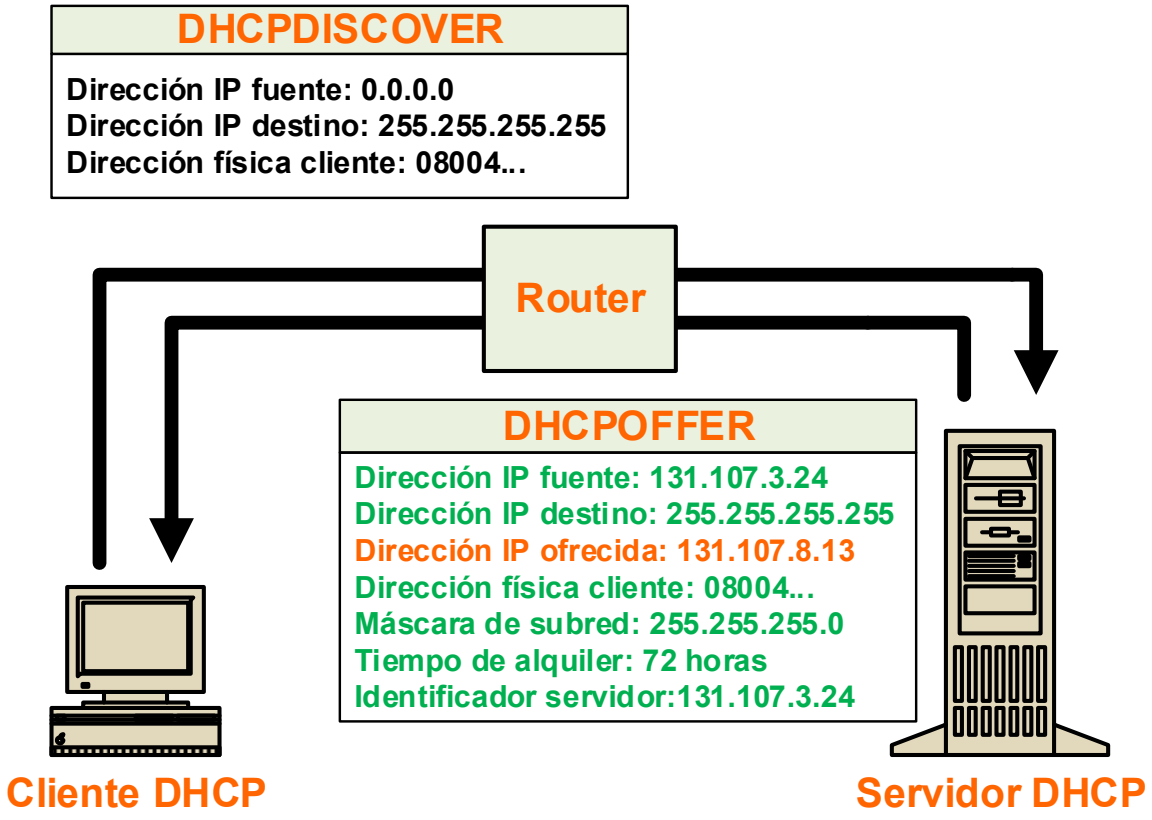
1. El cliente DHCP debe configurar su TCP/IP por primera vez
2. El cliente ha solicitado una dirección IP específica que le ha sido denegada. Esto puede suceder por los siguientes motivos:
   - ✓ El cliente estuvo mucho tiempo apagado y su dirección fue alquilada a otro cliente
   - ✓ La dirección IP denegada le fue alquilada anteriormente por otro servidor que en este momento está fuera de servicio
3. El cliente alquiló previamente una dirección pero la liberó. Entonces, la dirección fue alquilada a otro host y, por ese motivo, el cliente ahora solicita una nueva dirección para alquilar.

Dynamic Host Configuration Protocol (DHCP)
Fase 1: Solicitud de una dirección ip (DHCPDISCOVER)



Dynamic Host Configuration Protocol (DHCP)

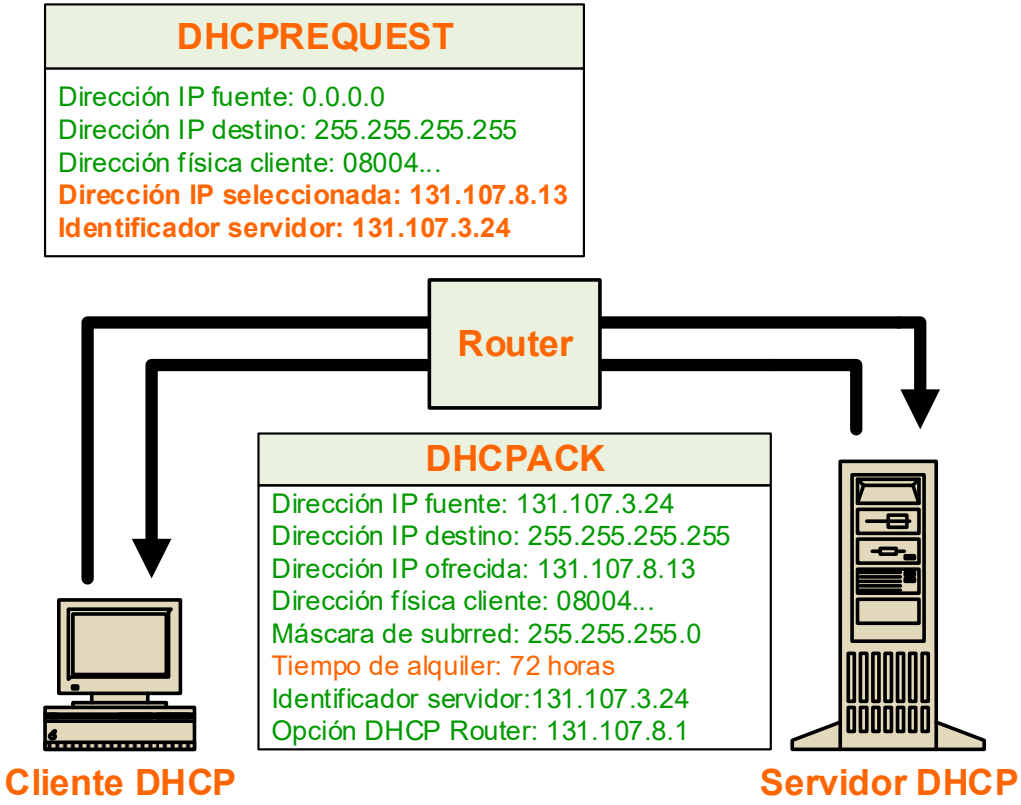
Fase 2: los servidores DHCP ofrecen una dirección IP (DHCPOFFER)



Dynamic Host Configuration Protocol (DHCP)
Fase 3: Selección de una dirección IP (DHCPREQUEST)

- ✓ Después que el cliente DHCP recibe y acepta una oferta, difunde un mensaje DHCPREQUEST que llega a todos los servidores DHCP indicando que ya ha seleccionado una dirección IP
- ✓ En este mensaje incluye la dirección IP del servidor cuya oferta fue aceptada
- ✓ Ante esta notificación del cliente DHCP, todos los demás servidores retiran sus ofertas

Dynamic Host Configuration Protocol (DHCP)
Fase 4: Confirmación del alquiler de la dirección IP (DHCPACK)



Dynamic Host Configuration Protocol (DHCP)
Denegación de una dirección IP (DHCPNACK)

- ✓ Puede ocurrir que el proceso de asignación de dirección IP no se haya completado satisfactoriamente.
- ✓ Cuando esto ocurre, el servidor DHCP difunde un mensaje **DHCPNACK (DHCP No ACK)** que significa "DHCP No Acknowledgment" o "DHCP No confirmado"
- ✓ Se trata de una operación fallida. Generalmente se debe a que el cliente ha intentado alquilar una dirección específica que:
- ✓ No está disponible. Ejemplo: la dirección fue alquilada a otro cliente
- ✓ Es inválida. Ejemplo: el cliente ha sido trasladado a otra subred y, por lo tanto, debe gestionar otra dirección IP (con otra Net ID)
- ✓ Cuando el cliente recibe una confirmación de asignación fallida, debe comenzar nuevamente el proceso de solicitar la asignación de una nueva dirección, es decir, debe comenzar con la 1ª Fase

Dynamic Host Configuration Protocol (DHCP)
Renovación del alquiler de una dirección IP

Primer intento de renovación del alquiler: ha expirado el **50%** del tiempo de alquiler de la dirección. El cliente intenta renovarlo enviando al servidor un DHCPREQUEST. Ante este envío, puede ocurrir que:

1. No hay problema. El servidor envía un DHCPACK confirmando la extensión del alquiler de la dirección y los demás parámetros
2. El cliente no puede establecer contacto con el servidor original. Puede deberse a:
   - ✓ La aplicación DHCP en el servidor no está activa
   - ✓ El servidor está apagado o fuera de servicio

Sucesivos arranques

Si al arrancar el cliente detecta que se ha superado el 50% del tiempo, lo primero que hace cuando levanta los servicios de red, es intentar la renovación del alquiler

En cualquier caso de imposibilidad de renovación, el cliente puede seguir usando la dirección porque todavía le queda el 50% restante, o menos.

Dynamic Host Configuration Protocol (DHCP)
Renovación del alquiler de una dirección IP

Nuevos intentos de renovación

Situación: se ha superado el 87,5% del tiempo de uso, pero aún no se ha completado el 100%.

Ante intentos infructuosos entre el 50 y 87,5% y una vez que se ha superado el 87,5%, el cliente intenta conectarse con cualquier servidor DHCP de la interred mediante una difusión enviando un DHCPREQUEST a todos los servidores

Ante este envío, el servidor puede responder de dos maneras:

- ✓ Renueva el alquiler
- ✓ No renueva el alquiler. Lo hace enviando un DHCPNACK. Este mensaje obliga al cliente a iniciar un nuevo proceso de asignación de dirección desde el comienzo (DHCPDISCOVER)

Dynamic Host Configuration Protocol (DHCP)
Renovación del alquiler de una dirección IP

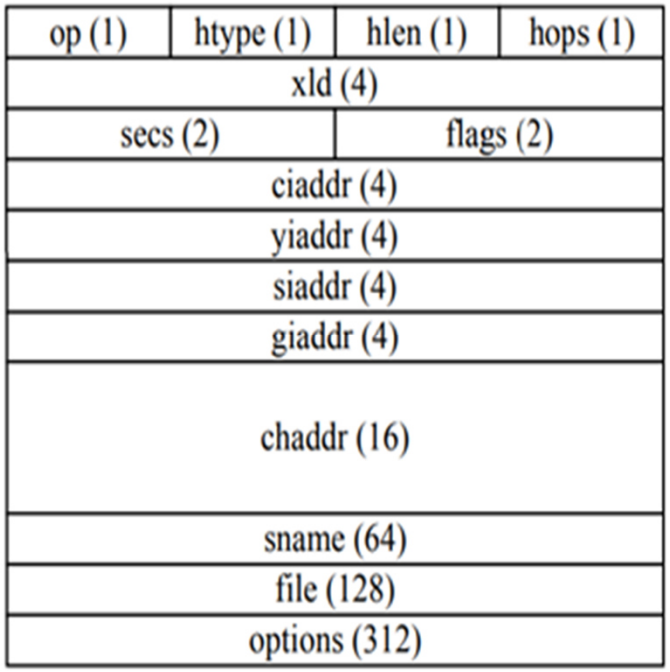
Situación: se ha superado el 100% del tiempo de alquiler, o el cliente ha recibido un DHCPNACK.

No hay renovación de alquiler

A partir de ese momento:

- Se suspende el uso de la dirección IP que ha venido usando el cliente. Se debe iniciar un nuevo proceso desde el principio (DHCPDISCOVER)
- Mientras dura la suspensión de la dirección IP, el cliente puede utilizar algún mecanismo de autoconfiguración de dirección IP, como por ejemplo APIPA (Automatic Private IP Addressing), hasta que pueda recibir una dirección de un servidor DHCP.

Dynamic Host Configuration Protocol (DHCP)
Formato del paquete



CAMPO	DESCRIPCIÓN
Op	Código de mensaje (tipo de mensaje). 1 = mensaje BOOTREQUEST 2 = mensaje BOOTREPLY.
Hype	Tipo de dirección hardware. Es el mismo usado por ARP. Por ejemplo un valor de 1 = 10 Mbps Ethernet.
Hlen	Longitud de dirección de hardware en octetos.
Hops	Puesto a cero por el cliente DCHP. Usado opcionalmente por los agentes repetidores en los routers cuando transmiten mensajes DCHP.
Xid	ID de transacción. Un número aleatorio usado por el DCHP cliente cuando genera un mensaje DCHP. Asocia mensajes del DCHP cliente con los del servidor.
Secs	Puesto por el DCHP Cliente. Son los segundos desde que el cliente empezó su inicialización (boot).
Flags	Usados para indicar si este es un mensaje broadcast. Ssi es así el bit mas al izquierda es 0 y los demás permanecen en 0
Ciaddr	Es la dirección IP del cliente DCHP. Puesto por el cliente en el mensaje BOOTREQUEST para verificar el uso de parámetros asignados
Yiaddr	Es la dirección IP del cliente DCHP retornada por el servidor DCHP
Siaddr	La dirección del servidor DCHP. Si el cliente DCHP desea contactar a un servidor DCHP específico inserta esta dirección en este campo
Giaddr	La dirección IP del router que corre el agente relay
Chaddr	La dirección hardware del cliente DCHP
Sname	El nombre de un servidor opcional si es conocido por el cliente DCHP
File	El nombre del archivo boot.
Options	Un campo para parámetros opcionales

Dynamic Host Configuration Protocol (DHCP)
Planificación para instalar servidor/es DHCP

- ✓ Identificar equipamiento que no puede recibir direcciones IP en forma automática
- ✓ Definir los equipos que deben recibir siempre una misma dirección IP
- ✓ Establecer el conjunto de direcciones que se van alquilar junto con el tiempo de vida de alquiler de cada una de ellas
- ✓ Determinar la cantidad de servidores DHCP que se van a desplegar y cuidar que los ámbitos de direcciones definidos en cada uno de ellos no se superpongan
- ✓ Calcular de la cantidad de "ámbito de direcciones" basados en las distintas subredes en las cuales se debe entregar direcciones IP en forma automática
- ✓ Configurar parámetros complementarios (opciones) a la dirección IP (default gateway, DNS, entre otros)
- ✓ Identificar el tipo de routers que forman parte de la red
- ✓ Determinar la necesidad de implementar agentes de reenvío de DHCP

Dynamic Host Configuration Protocol (DHCP)
Alcance de las Opciones en un servidor DHCP

- ✓ Dirección de Nivel Global. Son direcciones que están disponibles para todos los clientes DHCP para que puedan comunicarse con computadores específicos que prestan servicios comunes a toda la interred. Ejemplo: la dirección del servidor de DNS, de web, de impresión, entre otros.
- ✓ Dirección de Nivel de Grupo. Está dentro de un rango de direcciones disponibles sólo para un grupo dado de clientes Ejemplo: se define un entorno diferente de direcciones para cada subred, y en cada subred los computadores tendrán una dirección de router por defecto distinta (esta última es una dirección de nivel de grupo)
- ✓ Dirección de Nivel de Cliente. Es una dirección específica que se destinará a un cliente determinado. Las opciones que tendrá configurada este cliente, también están destinadas sólo a él.

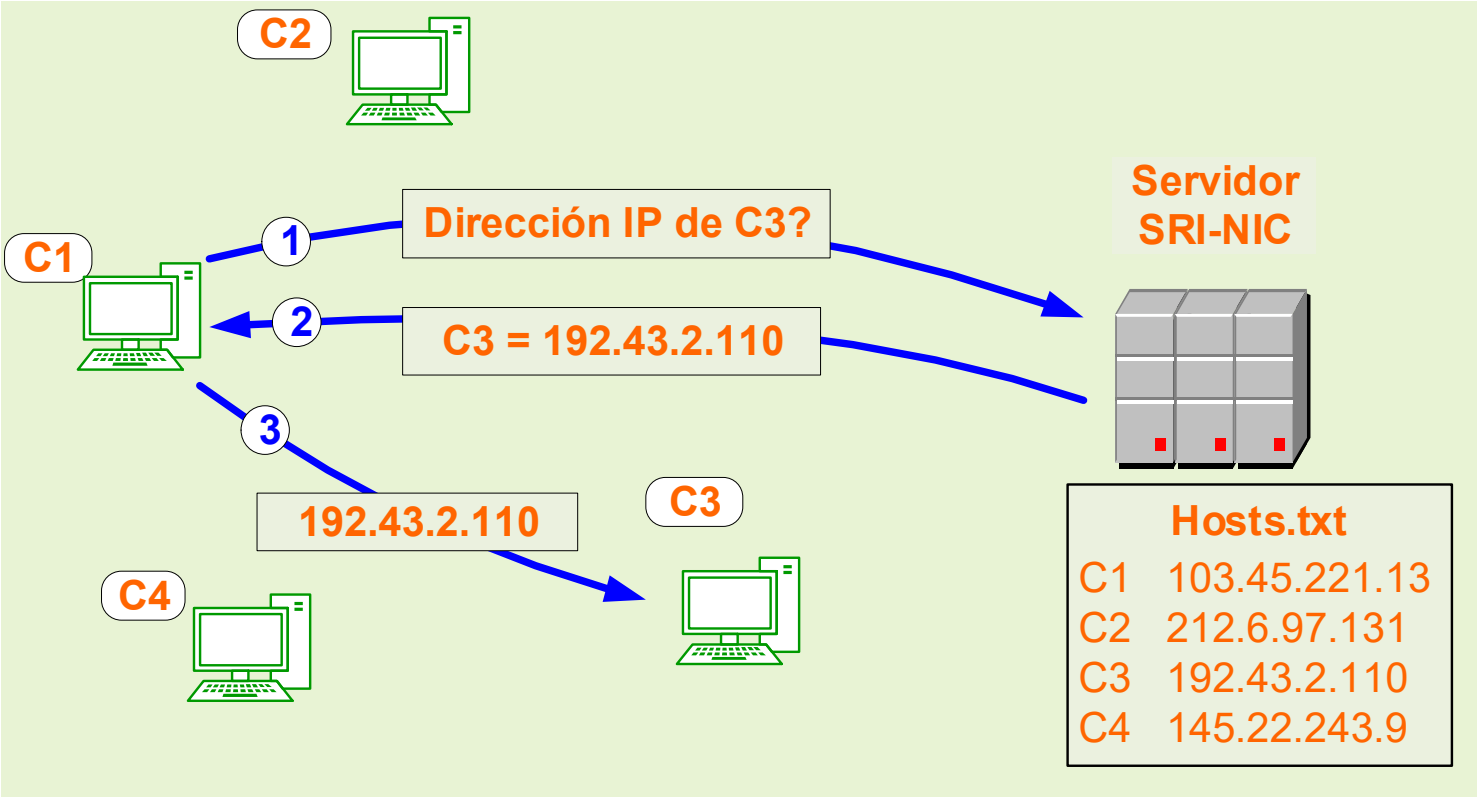
Domain Name System (DNS)
Conceptos

- ✓ Para establecer una comunicación desde un computador con otro, no se ingresa la dirección IP del computador destino sino un nombre formado por segmentos alfanuméricos separados por puntos. Ejemplo: www.google.com
- ✓ El ingreso de un nombre es muy práctico para los usuarios; sin embargo, los dispositivos en la red se identifican por su dirección IP
- ✓ El sistema que es capaz de traducir un nombre a una dirección ip se conoce como DNS. El primer RFC fue el 881. Actualmente está vigente los RFC 5890 y 5891
- ✓ Cuando un cliente consulta la dirección IP correspondiente a un nombre, está realizando una "Consulta Directa"

www.facet.unt.edu.ar es equivalente a la dirección IP 200.45.169.78

Domain Name System (DNS)

Conceptos: Antes de DNS una estructura plana en un archivo



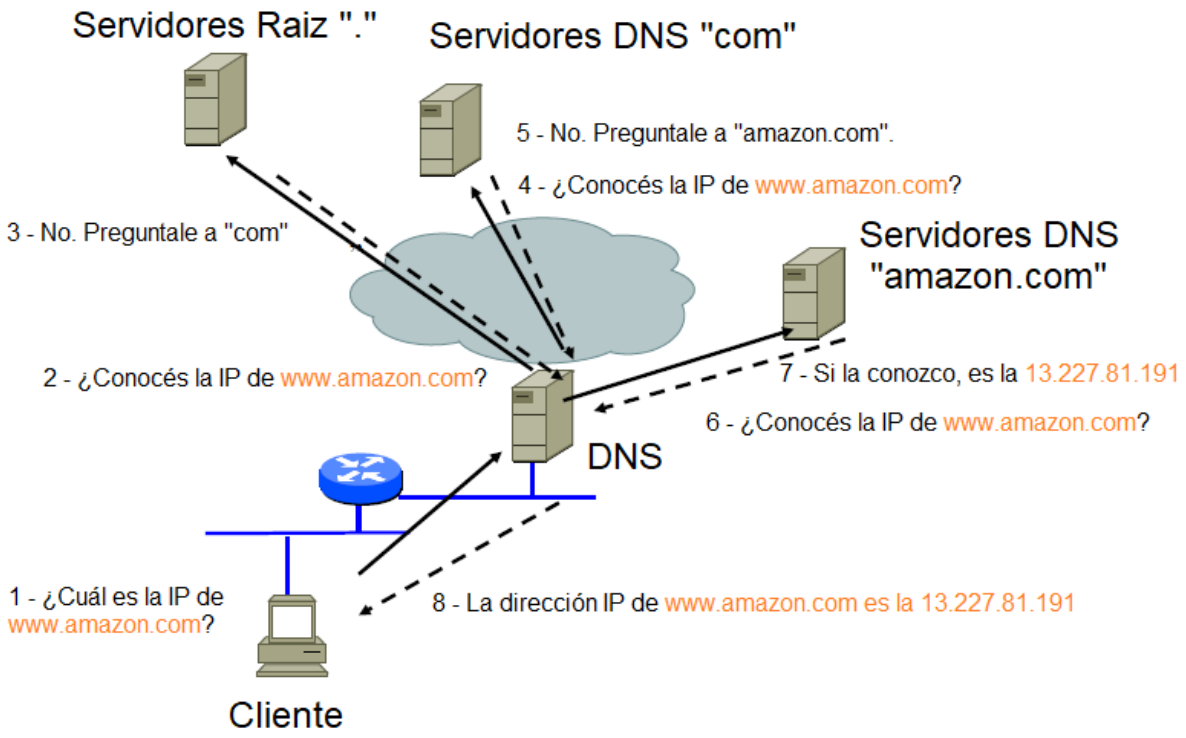
Domain Name System (DNS)
Conceptos

- ✓ El **sistema de nombres de dominio** se basa en un esquema jerárquico que permite asignar nombres, basándose en el concepto de dominio, utilizando para su gestión una base de datos (BD) distribuida.
- ✓ Las **consultas al DNS** son realizadas por los clientes a través de las rutinas de resolución ("resolver" o resolvedor o resolutor).
- ✓ Estas funciones son llamadas en cada host desde las aplicaciones de red (ping, telnet, ssh, http)
- ✓ Los servidores DNS contienen información de un segmento de la BD distribuida y la ponen a disposición de los clientes.
- ✓ Las peticiones de los clientes viajan en paquetes UDP al DNS local (puerto 53). Se usa TCP para transferencias de zona

Domain Name System (DNS)
Ventajas de usar DNS

- ✓ Desaparece la carga excesiva en la red y en los hosts: ahora la información esta distribuida por toda la red, al tratarse de una BD distribuida.
- ✓ No hay Duplicidad de Nombres: el problema se elimina debido a la existencia de dominios controlados por un único administrador. Puede haber nombres iguales pero en dominios diferentes.
- ✓ Consistencia de la Información: ahora la información que esta distribuida es actualizada automáticamente sin intervención de ningún administrador.

Domain Name System (DNS)
Funcionamiento: un modelo cliente/servidor



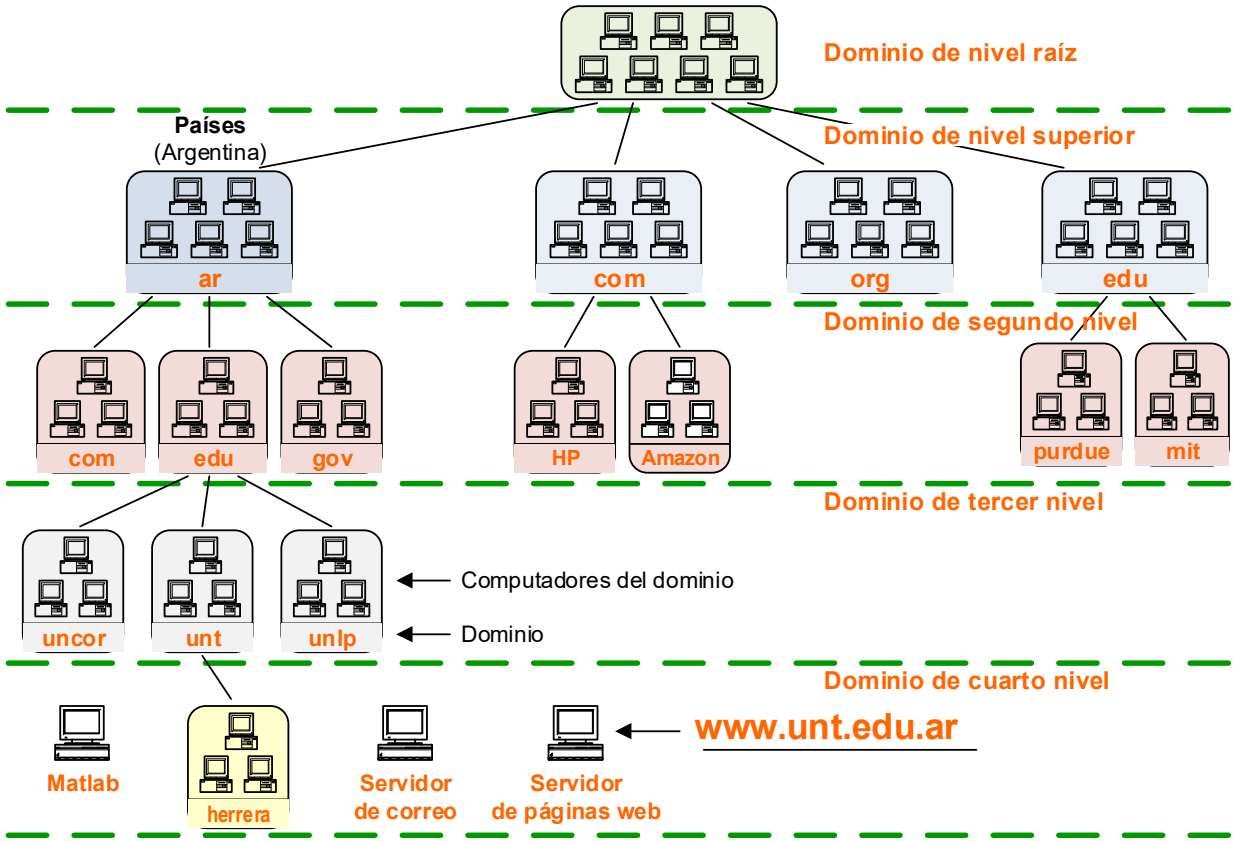
Domain Name System (DNS)
Funcionamiento: Servidores Raíz

Servidor	Operador	Instancias
A.ROOT-SERVERS.NET	Verisign, Inc	5
B.ROOT-SERVERS.NET	Information Sciences Institute	1
C.ROOT-SERVERS.NET	Cogent Communications	8
D.ROOT-SERVERS.NET	University of Maryland	109
E.ROOT-SERVERS.NET	NASA Ames Research Center	71
F.ROOT-SERVERS.NET	Internet Systems Consortium, Inc.	58
G.ROOT-SERVERS.NET	U.S. DOD Network Information Center	6
H.ROOT-SERVERS.NET	U.S. Army Research Lab	2
I.ROOT-SERVERS.NET	Netnod	50
J.ROOT-SERVERS.NET	Verisign, Inc	118
K.ROOT-SERVERS.NET	RIPE NCC	42
L.ROOT-SERVERS.NET	ICANN	158
M.ROOT-SERVERS.NET	WIDE Project	8
	Total	636

Domain Name System (DNS)
Sintaxis de un nombre de dominio

- ✓ Nombre de dominio es una cadena de hasta 255 caracteres, formada por etiquetas separadas por puntos (cada etiqueta inferior a 64 caracteres) de forma jerárquica o por niveles (comenzando el nivel superior por la derecha).
- ✓ Cada dominio es un índice en la BD del DNS.
- ✓ No se distinguen mayúsculas de minúsculas. Esto no se aplica a la parte izquierda de @ en las direcciones de correo.
- ✓ Ejemplo: www.amazon.com tiene 3 etiquetas, siendo el dominio de nivel superior "com", dominio de 2º nivel "amazon.com" y el dominio de nivel inferior "www.amazon.com."
- ✓ Un nombre de dominio puede representar el nombre de un host. Es el caso del ejemplo (www es el host donde hospeda las páginas Amazon).

Domain Name System (DNS)
Espacio de nombres de dominio: Estructura Jerárquica



Domain Name System (DNS)

Espacio de nombres de dominio: Dominio de nivel superior

Este nivel es compartido por varios dominios que responden a dos jerarquías de nombres conceptualmente diferentes:

1. Esquema organizacional: por tipo de actividad
2. Esquema geográfico: por país

Algunos de los dominios de nivel superior **(TLD, Top Level Domain)** más usados son:

com: orgs. comerciales	**mil**: orgs. militares
edu: instituciones educativas	**int**: orgs. internacionales
org: orgs. sin fines de lucro	**num**: números telefónicos
net: redes -backbone Internet-	**arpa**: opuesto a DNS
gov: orgs. gubernamentales	**xx**: código de país
tv: canales de televisión	

Domain Name System (DNS)

Espacio de nombres de dominio: Dominios de segundo nivel e inferior

Dominios de Segundo Nivel

- ✓ Esquema geográfico (países)

  Dominios por actividad de cada país (edu, com, org).

- ✓ Esquema organizacional (instituciones y empresas)

  Dominios de las organizaciones de EEUU, pero también pueden estar las organizaciones de otros países. (hay flexibilidad)

  Ejemplo: lagaceta.com

Dominios de Tercer Nivel

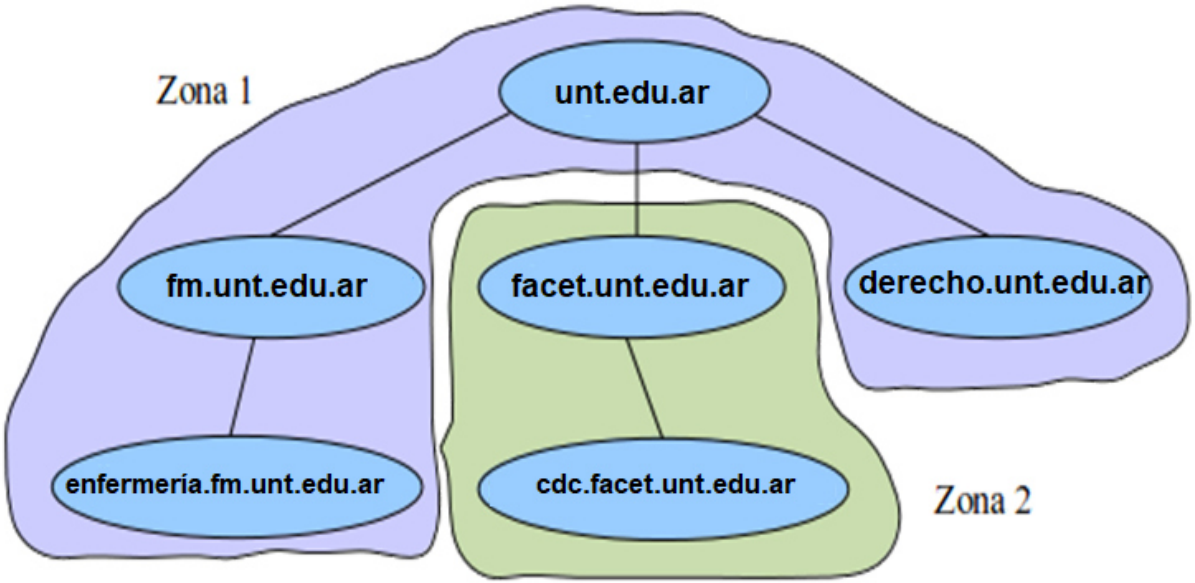
Dominios de las organizaciones de los países y los departamentos internos de las organizaciones de los países (ventas, educación, militar, etc.)

Ejemplo: mercadolibre.com.ar

Domain Name System (DNS)
Zona de Autoridad

- ✓ La administración del espacio de nombres de DNS se asigna a individuos u organizaciones
- ✓ Asumen la administración de por lo menos dos servidores de DNS
- ✓ La unidad de esa administración delegada es la **Zona**
- ✓ Es un subárbol del espacio de nombres que puede administrarse separadamente de otras **Zonas.**
- ✓ Una **Zona de Autoridad**, es la porción del Espacio de Nombres de Dominio, para la cual el servidor DNS tiene la autoridad de administrar y la responsabilidad de resolver una consulta.

Domain Name System (DNS)
Zona de Autoridad



Domain Name System (DNS)
Zona de Autoridad

- ✓ La solicitud de registro para comenzar a ser un Zona de Autoridad de un Dominio se realiza ante una autoridad competente, por ejemplo InterNIC (http://www.internic.net/) es una autoridad de registro.
- ✓ Cada país a su vez también dispone de autoridades de registro.
- ✓ Otra opción para solicitar un dominio, es contactar con los servicios ofrecidos por una empresa (ej. www.nombres.com.ar) y/o ISP.
- ✓ La autoridad del dominio TLD "ar." (Argentina) es la Subsecretaría Técnica de la Secretaría Legal y Técnica de la Presidencia de la Nación.
- ✓ El sitio para registrar dominios debajo de ".ar" es http://nic.ar

Domain Name System (DNS)
Zona de Autoridad: Base de Datos

- ✓ Los servidores DNS tienen información completa de una zona de autoridad, y la misma es implementada en una Base de Datos.
- ✓ La Zona de Autoridad abarca al menos un dominio, pudiendo incluir dominios de nivel inferior y tendrá normalmente un Servidor de Nombres "Primario". Existe al menos un administrador de la Zona
- ✓ Estos dominios de nivel inferior se pueden delegar en otros servidores locales, implementando nuevas Zonas de Autoridad que son administradas por administradores locales en los servidores locales.
- ✓ Según las características de la Zona y la forma de implementación de la base de datos, los servidores DNS se pueden clasificar en: Primarios, Secundarios, Maestros y Caché

Domain Name System (DNS)

Zona de Autoridad: Registros (RR, Resource Record)

- ✓ SOA: Inicio de autoridad, identificando el dominio o la zona. Fija una serie de parámetros para la zona (ejemplo TTL, Time to Live).
- ✓ NS (Name Server): Identifica al servidor de nombres (primario, secundario o máster)
- ✓ A (Address): permite resolver una nombre a una dirección IP
- ✓ MX (Mail Exchange): Servidor de correo, permite identificar un servidor de correo y resolver su dirección IP
- ✓ CNAME (canonical name): Permite resolver nombres alternativos a una dirección IP.
- ✓ TXT: Añade comentarios que puedan servir a quienes consultan sobre la Zona, por ejemplo, direcciones de correo alternativas del administrador
- ✓ HINFO: Información del host
- ✓ WKS: Servicios públicos (Well Known Services). Puede listar los servicios de las aplicaciones disponibles en el ordenador.

Domain Name System (DNS)
Zona de Autoridad: Registros

- ✓ Cada entrada en la tabla de un DNS contiene información, no sólo de las direcciones IP, si no de un registro de recursos, con 5 campos o tuplas

  [Nombre_dominio] [TTL] [Clase] Tipo Dato_Registro(Valor)

- ✓ Cuando un cliente (a través de un *resolver*) pregunta por un nombre de dominio al DNS, lo que recibe son los RR asociados a ese nombre y por tanto la función real del DNS es relacionar los dominios de nombres con los RR

Un ejemplo real (Consulta who is):

[Nombre_dominio]	[TTL]	[Clase]	Tipo	Dato_Registro(Valor)
facet.unt.edu.ar	1799	IN	A	200.45.169.78

Domain Name System (DNS)
Zona de Autoridad: Roles de Servidores DNS

Servidor Primario

- ✓ Contiene todos los registros de la o las zonas para lo cual el servidor es autoridad.
- ✓ Es el único servidor en el que deben realizarse los cambios que se producen en la zona, tal como agregar dominios o datos de computadores

Servidor Secundario

- ✓ Contiene una copia de todos los registros de la o las zonas para las cuales es autoridad.
- ✓ Diferencia con el Servidor Primario: el Servidor Secundario obtiene la información para su zona, a través de obtención de información de un Servidor Primario o Servidor Maestro que tiene autoridad en esa Zona.
- ✓ Cuando el Servidor Secundario obtiene información de la zona a través de la red se dice que hay una transferencia de zona

Domain Name System (DNS)
Roles de Servidores DNS

Servidor Maestro

- La función primordial de un Servidor Maestro es la de proveer respaldo de la información en la zona
- Usado para Transferir Información a los Servidores Secundarios, y descargar esa tarea al Servidor Primario. Cuando un Servidor Secundario se levanta, lo primero que hace es establecer conexión con el Servidor Maestro e iniciar una Transferencia de Zona con ése servidor

Servidor de Cache

- Ante una consulta DNS, busca la respuesta en el archivo caché del mismo. Si la tiene, le pasa al cliente y actualiza el tiempo de vida del registro en su memoria caché. Si no la tiene, consulta a su servidor DNS, y al recibir respuesta actualiza el archivo caché.
- El servidor de cache no es autoridad en una zona en particular

Domain Name System (DNS)

Tipos de Consultas

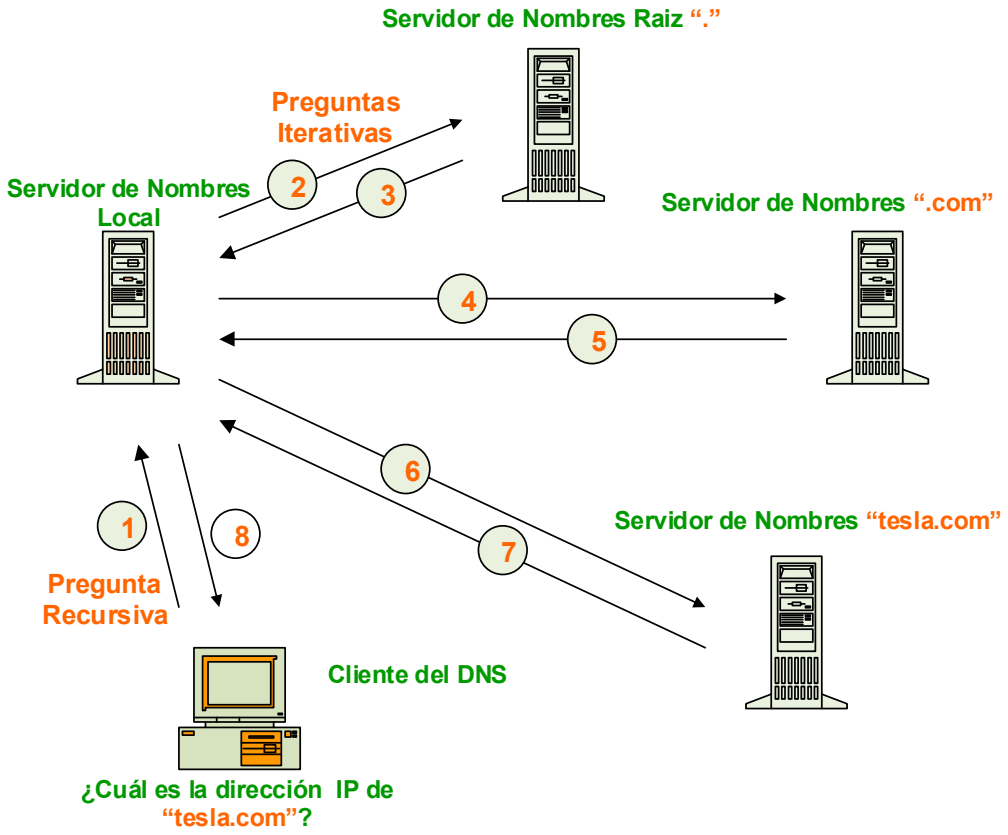
Consulta Recursiva o Recurrente:

- ✓ El servidor debe proveer la respuesta. Si no puede responderla, debe encargarse de conseguir la respuesta para entregársela al cliente. NO puede excusarse y derivarla para que otro servidor se haga cargo
- ✓ El único responsable de gestionar la respuesta es el servidor que recibió la pregunta recursiva.

Consulta Iterativa:

- ✓ El servidor que la recibe devuelve la mejor respuesta que puede y luego se libera de la responsabilidad
- ✓ La respuesta ante una pregunta iterativa puede ser:
  - ✓ La resolución del nombre o
  - ✓ La dirección de un servidor que eventualmente la pueda responder

Domain Name System (DNS)
Tipos de Consultas



Domain Name System (DNS)
Tipos de Consultas

Consulta Inversa

- ✓ Es aquella en que el resolutor (cliente) consulta el "nombre" correspondiente a una dirección IP
- ✓ Para ello se debe crear un dominio especial denominado in-addr.arpa
- ✓ Una dirección IP se interpreta de izquierda a derecha y el nombre de dominio de derecha a izquierda. el orden de los bytes de la dirección IP debe invertirse para que la interpretación de la pregunta pueda realizarse de derecha a izquierda
- ✓ En el dominio in-addr.arpa los nombres de los computadores están a continuación de las direcciones invertidas
- ✓ Una vez que se ha implementado el archivo con el dominio in-addr.arpa, deben agregarse los registros de punteros

78.169.45.200.in-addr.arpa domain name pointer facet.unt.edu.ar

Domain Name System (DNS)
Cómo procesan y almacenan las consultas

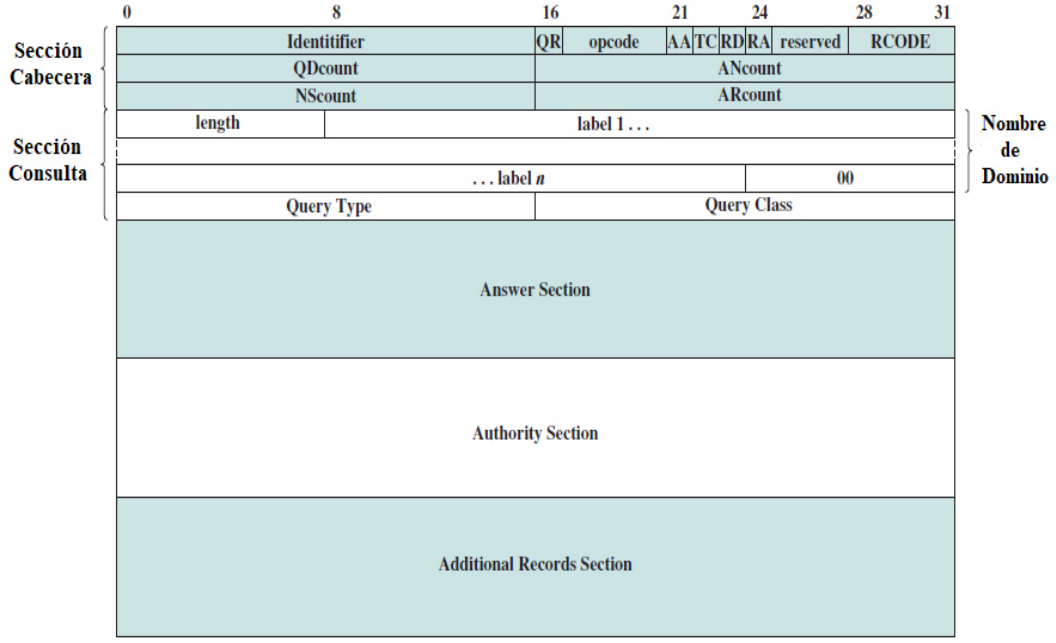
Almacenamiento de consultas

- ✓ Mientras el servidor está procesando una pregunta, pueden llegar otras preguntas
- ✓ Todas las consultas resueltas por el servidor se almacenan en una archivo caché. Para evitar el crecimiento indefinido de ese archivo, las respuestas resueltas por el servidor, son almacenadas sólo durante un tiempo.
- ✓ ¿Cuánto tiempo es almacenada una pregunta? Es por un tiempo determinado que se denomina tiempo de vida (TTL, Time To Live)

Tiempo de vida (TTL)

- ✓ Su valor es definido por el administrador del servidor DNS que es autoridad para la zona. Cada registro creado en la zona tiene asignado un TTL.
- ✓ Cuando un cliente resuelve una consulta, almacena en su archivo caché el registro resuelto e inicia una contador con el valor del campo TTL del mismo. A partir de ese momento, el TTL comienza a ser decrementado desde su valor original. En caso de llegar a 0, el registro es eliminado del caché.

Domain Name System (DNS)
Formato del paquete DNS



QR = query/response bit
AA = authoritative answer
TC = truncated
RD = recursion desired
RA = recursion available

RCODE = response code
QDcount = number of entries in question section
ANcount = number of resource records in answer section
NScount = number of name server resource records in authority section
ARcount = number of resource records in additional records section

Domain Name System (DNS)
DNS Dinámico

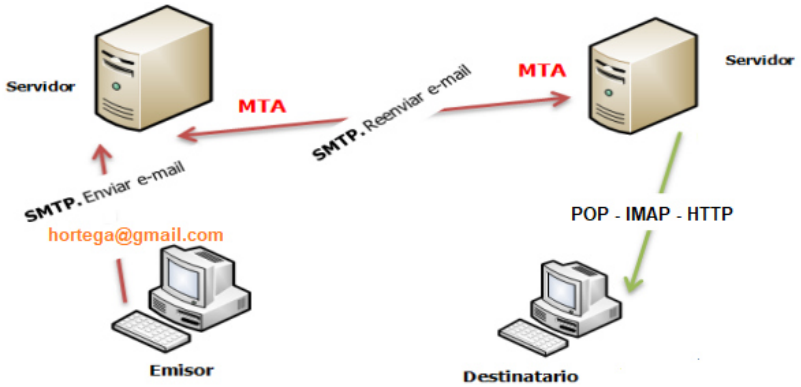
- ✓ Muchos ISP gestionan de forma dinámica las IP de los host conectados por DHCP de forma arbitraria, sin tener vinculación IP con la MAC.
- ✓ Si dentro del ISP, algún servidor ha de ser accedido desde el exterior, requerirá tener traducción a IP pública y además dicha IP estar ligada con un nombre, de forma consistente.
- ✓ **Ejemplo**: un usuario de un ISP, cuyo host se llama "miapellido" quiere ofrecer un servicio de HTTP. El nombre completo dentro del ISP del host es "miapellido.isp.com", pero dicho ISP utiliza DHCP sin vinculación a MAC, por lo cual nunca tiene la misma IP, sino puede tener cualquiera dentro del rango 181.94.89.0/24.
- ✓ Para que se pueda acceder desde el exterior, o bien conocen la IP asignada y se avisa al cliente que quiere conectarse, o bien el ISP configura un cliente DNS dinámico para actualizar los registros tipo A de miapellido.isp.com cada vez que alquile una nueva dirección IP por DHCP.

1. **DHCP entrega IP 189.94.89.19/24**
2. **Cliente DNS dinámico indica al DNS nuevo registro de "isp.com": miapellido A 181.94.89.0**

B R E A K

Correo Electrónico
Protocolos de Acceso al Correo

- ✓ SMTP: envío/almacenamiento a/en el servidor del destinatario.
- ✓ Protocolo de acceso al correo: recuperación desde el servidor.
  - ✓ POP: Protocolo de Oficina Postal [RFC 1939]
    - ✓ Autorización (agente <-->servidor) y descarga.
  - ✓ IMAP: Protocolo de Acceso al Correo Internet [RFC 1730]
    - ✓ Más características (más complejo).
    - ✓ Manipulación de los mensajes almacenados en el servidor.
  - ✓ HTTP: Gmail, Hotmail, etc.



Correo Electrónico
Arquitectura

- ✓ Conceptos de **envoltura** (destino, prioridad, seguridad, etc, un tipo de cabecera primitiva definida en RFC821) y **contenido o mensaje** (que a su vez se divide en cabecera del mensaje y cuerpo, separados por una línea en blanco y se define en RFC822).
- ✓ **Funciones** del sistema de correo:edición de mensajes, transferencia y generación de informes.
- ✓ **Subsistemas** que lo forman: agentes de transferencia (generalmente "demonios") y los agentes de usuario.
- ✓ Estos agentes se clasifican en:
  - ✓ Distribución: utilizando para ello el protocolo SMTP (Simple Mail Transfer Protocol) RFC 821 o SMTP extendido (ESMTP) RFC 1425
  - ✓ Entrega final: que permita al usuario gestionar su correo a través de una máquina remota, utilizando los protocolos POP3 (Post Office Protocol) RFC 1225 e IMAP (Interactive Mail Access Protocol) RFC 1064

Correo Electrónico
Terminología

- ✓ **DNS y registros MX**: son intercambiadores de correo, que reciben correo en nombre de otro servidor cuando el principal está fuera de servicio
- ✓ **Relay o reenvío:** indica si un servidor de correo, de transferencia y distribución, acepta correo de otro servidor para reenviar. Ejemplo, el servidor de correo de la facultad acepta reenviar correo de usuarios que no tienen cuenta de mail en el servidor (Peligroso)
- ✓ **SPAM:** envío masivo a un conjunto de direcciones gestionadas por un servidor. El servidor puede configurarse para marcarlas como SPAM. La obtención de usuarios de un servidor se puede realizar utilizando los comandos SMTP "VRFY" y "EXPN".

Correo Electrónico
Simple Mail Transfer Protocol – SMTP (RFC 2821)

- ✓ Utiliza TCP para transferir con seguridad el mensaje de correo electrónico del cliente al servidor, puerto 25.
- ✓ Transferencia directa: del servidor que envía al servidor que recibe.
- ✓ Las tres fases de la transferencia son:
  - ✓ "Acuerdo" (saludo).
  - ✓ Transferencia de mensajes.
  - ✓ Cierre.
- ✓ Interacción comando/respuesta:
  - ✓ Comandos: texto ASCII.
  - ✓ Respuesta: código de estatus y frase.
- ✓ Los mensajes deben tener siete bits en ASCII.

Correo Electrónico
SMTP: Funcionamiento

El servidor comienza por enviar una línea de texto que proporciona su identidad e indica si está preparado o no para recibir correo:

1. Si no lo está, el cliente libera la conexión y lo intenta después. Por defecto en Sendmail, cada 15 minutos durante 4 días.

2. Si está dispuesto a aceptar correo electrónico, el cliente anuncia de quién viene el mensaje, y a quién está dirigido. Si existe tal destinatario en el destino, el servidor da al cliente permiso para enviar el mensaje. Entonces el cliente envía el mensaje y el servidor acusa su recibo. Si existe más correo electrónico también se envía ahora. Una vez que todo el correo ha sido intercambiado en ambas direcciones, se libera la conexión.

Correo Electrónico
SMTP: Funcionamiento, comandos SMTP

Comando	Descripción
HELO (EHLO)	Identifica el remitente al destinatario.
MAIL FROM	Identifica una transacción de correo e identifica al emisor.
RCPT TO	Se utiliza para identificar un destinatario individual. Si se necesita identificar múltiples destinatarios es necesario repetir el comando.
DATA	Permite enviar una serie de líneas de texto. El tamaño máximo de una línea es de 1.000 caracteres. Cada línea va seguida de un retorno de carro y avance de línea <CR><LF>. La última línea debe llevar únicamente el carácter punto "." seguido de <CR><LF>.
RSET	Aborta la transacción de correo actual.
NOOP	No operación. Indica al extremo que envíe una respuesta positiva. Keepalives
QUIT	Pide al otro extremo que envíe una respuesta positiva y cierre la conexión.
VRFY	Pide al receptor que confirme que un nombre identifica a un destinatario valido.
EXPN	Pide al receptor la confirmación de una lista de correo y que devuelva los nombres de los usuarios de dicha lista.
HELP	Pide al otro extremo información sobre los comandos disponibles.
TURN	El emisor pide que se inviertan los papeles, para poder actuar como receptor. El receptor puede negarse a dicha petición.
SOML	Si el destinatario está conectado, entrega el mensaje directamente al terminal, en caso contrario lo entrega como correo convencional.
SAML	Entrega del mensaje en el buzón del destinatario. En caso de estar conectado también lo hace al terminal.
SEND	Si el destinatario está conectado, entrega el mensaje directamente al terminal.

Correo Electrónico
SMTP: Funcionamiento, códigos de respuesta del servidor

Código	Descripción
211	Estado del sistema.
214	Mensaje de ayuda.
220	Servicio preparado.
221	Servicio cerrando el canal de transmisión.
250	Solicitud completada con éxito.
251	Usuario no local, se enviará a <dirección de reenvío>
354	Introduzca el texto, finalice con <CR><LF>.<CR><LF>.
421	Servicio no disponible.
450	Solicitud de correo no ejecutada, servicio no disponible (buzón ocupado).
451	Acción no ejecutada, error local de procesamiento.
452	Acción no ejecutada, insuficiente espacio de almacenamiento en el sistema.
500	Error de sintaxis, comando no reconocido.
501	Error de sintaxis. P.ej contestación de SMTP a ESMTP
502	Comando no implementado.
503	Secuencia de comandos errónea.
504	Parámetro no implementado.
550	Solicitud no ejecutada, buzón no disponible.
551	Usuario no local, pruebe <dirección de reenvío>. Si no se tiene cuenta
552	Acción de correo solicitada abortada.
553	Solicitud no realizada (error de sintaxis).
554	Fallo en la transacción.

Correo Electrónico
SMTP: Funcionamiento, ejemplo

Ejecutar desde línea de commando: Telnet “nombreServidor” 25.

S: 220 Herrera.unt.edu.ar
C: HELO unlp.edu.ar
S: 250 Hello unlp.edu.ar, pleased to meet you
C: MAIL FROM: <jlopez@unlp.edu.ar>
S: 250 jlopez@unlp.edu.ar... Sender ok
C: RCPT TO: <hortega@Herrera.unt.edu.ar>
S: 250 hortega@Herrera.unt.edu.ar ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Te cuento que dictamos el curso de Java
C: Será los dias 17 y 18 de Agosto de 9 a 13 hs.
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 Herrera.unt.edu.ar closing connection

Correo Electrónico
RFC 822: campos principales

Cabecera	Descripción
To:	Direcciones de email de los destinatarios primarios.
Cc:	Direcciones de email de los destinatarios secundarios. En términos de entrega no existe diferencia con los destinatarios primarios.
Bcc:	Direcciones de email de las copias al carbón ciegas. Es como el campo anterior excepto que esta línea se borra de todas las copias enviadas a los destinatarios primarios y secundarios.
From:	Persona o personas que crearon el mensaje.
Sender:	Dirección de correo del remitente. *Puede omitirse si es igual al campo anterior.*
Received:	Línea agregada por cada agente de transferencia en la ruta. La línea contiene la identidad del agente, la fecha y hora de recepción del mensaje y otra información que puede servir para detectar fallos en el sistema de enrutamiento. Se añaden apiladas en la cabecera, a medida que se intercambia el email.
Return-Path:	Puede usarse para identificar una trayectoria de regreso al remitente.

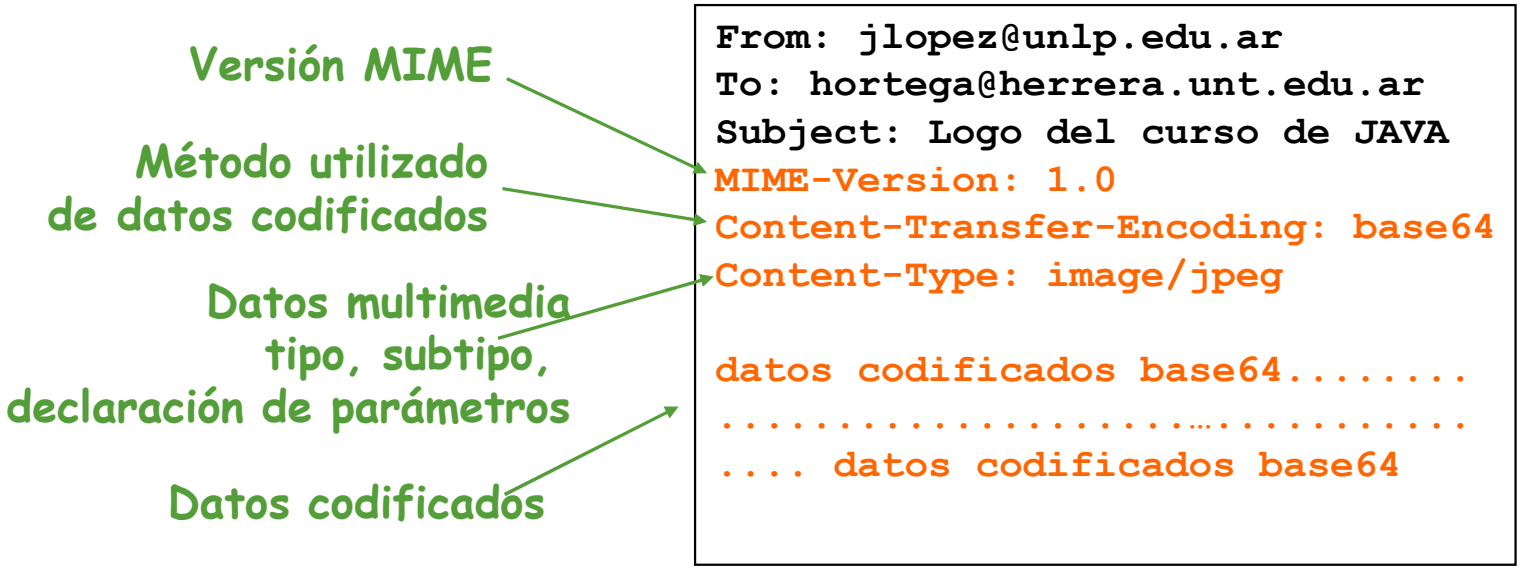
Correo Electrónico
RFC 822: Limitaciones

- ✓ SMTP no puede transmitir ficheros ejecutables u otros objetos binarios.
- ✓ SMTP no puede transmitir datos de texto que incluyan caracteres de lenguajes nacionales
- ✓ Los servidores SMTP pueden rechazar mensajes de correo que superen un cierto tamaño.
- ✓ Las pasarelas de SMTP que traducen caracteres ASCII a código EBCDIC no utilizan un conjunto consistente de correspondencias, lo que da lugar a problemas en la traducción.
- ✓ Las pasarelas de SMTP a redes de correo electrónico X.400 no pueden manejar los datos no textuales incluidos en mensajes X.400

Solución: Implementación de extensiones MIME (Multi purpose Internet Mail Extensions)

Correo Electrónico
Extensiones Multipropósito de correo electrónico (MIME)

- ✓ MIME: extensiones de correo multimedia, RFC 2045, 2056
- ✓ Las líneas adicionales en la cabecera del mensaje declaran el tipo de contenido MIME.



Correo Electrónico

Extensiones Multipropósito de correo electrónico (MIME)

Cabecera	Descripción
MIME-Version:	Identifica la version de MIME. Si no existe se considera que el mensaje es texto normal en inglés.
Content-Description:	Cadena de texto que describe el contenido. Esta cadena es necesaria para que el destinatario sepa si desea descodificar y leer el mensaje o no.
Content-Id:	Identificador único, usa el mismo formato que la cabecera estándar Message-Id.
Content-Transfer-Encoding:	Indica la manera en que está envuelto el cuerpo del mensaje.
Content-Type:	Especifica la naturaleza del cuerpo del mensaje.

Correo Electrónico

Extensiones Multipropósito de correo electrónico (MIME)

Tipo de Contenido (Content Type)

Tipo	Subtipo	Descripción
Texto	Nativo	Texto no formateado; puede ser ASCII o ISO 8859
Multipart («multiparte»)	*Mixed* («mixto»)	Las diferentes partes son independientes pero van a ser transmitidas juntas. Se deben presentar al receptor en el mismo orden en que aparecen en el mensaje de correo.
	Parallel («paralelo»)	Difiere del subtipo *mixed* solamente en que no se define orden para la entrega de las partes al receptor.
	Alternative («Alternativo»)	Las diferentes partes son versiones alternativas de la misma información. Están ordenadas en fidelidad creciente al original y el sistema de correo destino debe mostrar la mejor versión para el usuario.
	Digest («resumen»)	Similar al subtipo *mixed*, pero el tipo/subtipo por defecto para cada parte es message/rfc822.
Message («mensaje»)	rfc822	El propio cuerpo es un mensaje encapsulado que cumple con el RFC 822.
	Partial («parcial»)	Utilizado para permitir la fragmentación de elementos de correo grandes de forma que sea transparente al destino.
	External-body («cuerpo-externo»)	Contiene un puntero a un objeto que existe en otra parte.
Image («Imagen»)	jpeg	La imagen está en formato JPEG, codificación JFIF.
	gif	La imagen está en formato GIF.
Video («Vídeo»)	mpeg	Formato MPEG.
Audio	*Basic* («Básico»)	Codificación en ley-*mu* de RDSI, con un canal de 8 bits.
Application («aplicación»)	*Postscript*	Postscript de Adobe.
	octet-stream («flujo de octetos»)	Datos binarios generales compuestos por bytes de 8 bits.

Tipo de Codificación (Content Transfer Encoding)

7bit	Todos los datos se representan por líneas cortas de caracteres ASCII.
8bit	Las líneas son cortas, pero puede haber caracteres no ASCII (octetos con el bit de orden más alto establecido).
Binary («binario»)	Además de incluir caracteres no ASCII, las líneas pueden no ser lo suficientemente cortas para el transporte SMTP.
quoted-printable («imprimible textualmente»)	Codifica los datos de tal forma que si la mayoría de los datos que se codifican son texto ASCII, el texto codificado permanece en gran medida reconocible por los usuarios humanos.
base64	Codifica los datos convirtiendo bloques de 6 bits en bloques de 8 bits, todos ellos caracteres ASCII imprimibles.
x-token («esquema x»)	Una codificación no estándar.

Correo Electrónico

Protocolos de entrega final a usuario

POP3 (Post Office Protocol) RFC 1225. Tiene comandos para que un usuario establezca una sesión (USER y PASS), la termine (QUIT), obtenga mensajes (RETR) y los borre (DELE). El protocolo mismo consiste en texto ASCII y se asemeja a SMTP. El objetivo del POP3 es obtener correo electrónico del buzón remoto y almacenarlo en la máquina local del usuario para su lectura posterior. Existen versiones actualmente, que ya permiten no descargar el correo del buzón como IMAP.

IMAP (Interactive Mail Access Protocol) RFC 1064. La idea en que se basa IMAP es que el servidor de correo electrónico mantenga un depósito central al que puede accederse desde cualquier máquina. Por tanto, a diferencia del POP3, no copia el correo electrónico en la máquina personal del usuario dado que el usuario puede tener varias computadoras para consultar el correo, y observa si sus correos han sido leídos con anterioridad.

Correo Electrónico

Protocolos de entrega final a usuario

POP3 (Post Office Protocol) RFC 1225. Tiene comandos para que un usuario establezca una sesión (USER y PASS), la termine (QUIT), obtenga mensajes (RETR) y los borre (DELE). El protocolo mismo consiste en texto ASCII y se asemeja a SMTP. El objetivo del POP3 es obtener correo electrónico del buzón remoto y almacenarlo en la máquina local del usuario para su lectura posterior. Existen versiones actualmente, que ya permiten no descargar el correo del buzón como IMAP.

IMAP (Interactive Mail Access Protocol) RFC 1064. La idea en que se basa IMAP es que el servidor de correo electrónico mantenga un depósito central al que puede accederse desde cualquier máquina. Por tanto, a diferencia del POP3, no copia el correo electrónico en la máquina personal del usuario dado que el usuario puede tener varias computadoras para consultar el correo, y observa si sus correos han sido leídos con anterioridad.

Correo Electrónico
POP3

- ✓ Funciona sobre el puerto 110, (RFC 1225)
- ✓ Fases de operación
  - ✓ Establecer conexión TCP
  - ✓ Autorización
  - ✓ Transacción (entrega de mensajes, borrado, etc)
  - ✓ Actualización
  - ✓ Cierre de conexión
- ✓ Solo se consideran 2 posibles respuestas

  +OK, Aceptación

  -ERR, Indicación de Error
- ✓ Además contiene un texto descriptivo cuando se trata de un error

Correo Electrónico
POP3: Comandos

- ✓ USER Identificación del usuario
- ✓ PASS Contraseña del usuario
- ✓ STAT Indica cuantos mensajes y longitud
- ✓ RETR Retira mensaje del buzón
- ✓ DELE Marca mensaje para borrado
- ✓ LAST Entregar el último mensaje
- ✓ QUIT Cierre la conexión TCP

Correo Electrónico

IMAP

- ✓ RFC 1064 (IMAP2), puerto 143
- ✓ Modelo de manejo de correo que permite movilidad a usuarios.
- ✓ No se trae a la estación todo el buzón
- ✓ Manipulación remota de carpetas, extendida
  - ✓ Creación, Búsquedas sin traer todo el buzón...
- ✓ Alternativa para POP3
- ✓ Independiente de la forma de almacenamiento
- ✓ Comandos y Respuestas
  - ✓ Marcadas <CRLF>
- ✓ Proceso cliente/servidor:
  - ✓ Conexión / Respuesta de aceptación
  - ✓ Login /aceptación o rechazo
  - ✓ Selección de carpeta (inbox)
  - ✓ Acciones (leer, borrar, buscar...)
  - ✓ Despedida y cierre de conexión

Correo Electrónico
Comparación POP3 e IMAP

POP3

- ✓ Por defecto utiliza el modo "descargar y borrar".
- ✓ El usuarios no puede volver a leer el correo electrónico si cambia de cliente.
- ✓ "Descargar y guardar": copias de mensajes en diferentes clientes.
- ✓ POP3 es un protocolo sin estado entre sesiones.

IMAP

- ✓ Almacena todos los mensajes en un mismo lugar: el servidor.
- ✓ Permite al usuario organizar sus mensajes en carpetas.
- ✓ IMAP mantiene el estado de usuario entre sesiones:

  Los nombres de las carpetas y la correspondencia entre los números de identificación de los mensajes y el nombre de la carpeta.

Protocolo Hypertext Transfer Protocol (HTTP)

Introducción

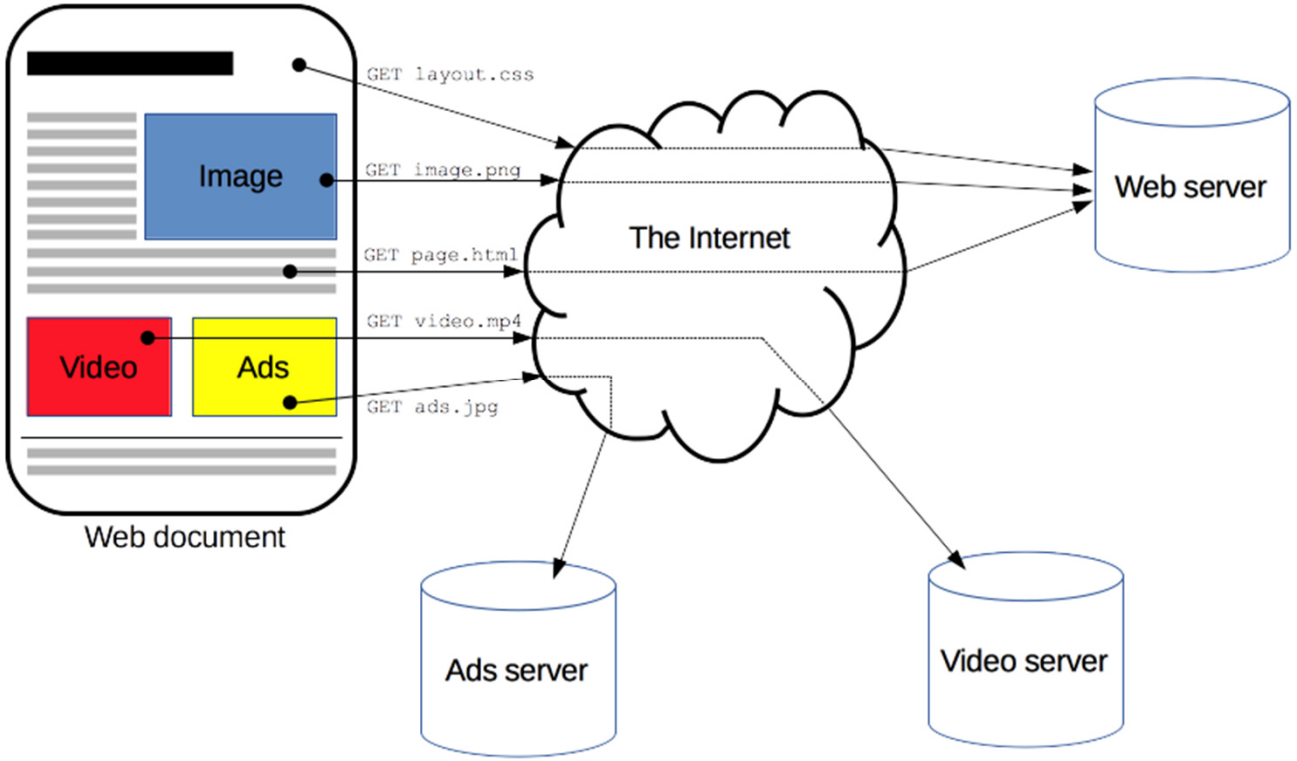
HTTP se basa en el envío de mensajes sobre el protocolo de transporte TCP:

- ✓ El cliente envía un mensaje de petición a un servidor, solicitando realizar una acción sobre un recurso determinado (habitualmente, obtener el recurso).
- ✓ El servidor envía un mensaje de respuesta a la petición del cliente (habitualmente, incluyendo el recurso solicitado).

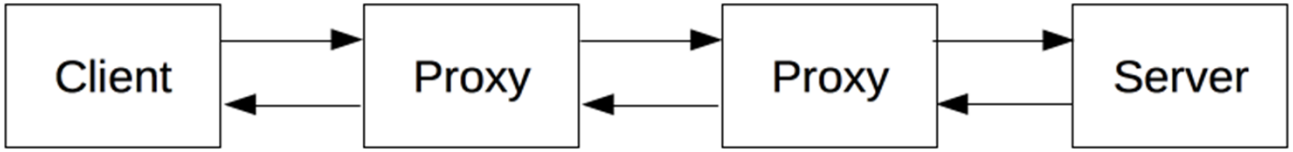
Las versiones más utilizadas actualmente son:

- ✓ HTTP/1.1: versión utilizada mayoritariamente desde finales de los 90.
- ✓ HTTP/2: versión desplegada en los últimos años. Mejora la eficiencia mediante codificación binaria de mensajes, compresión de cabeceras, multiplexación de múltiples peticiones/respuestas sobre una única conexión TCP, peticiones iniciadas por el servidor, etc.

Protocolo Hypertext Transfer Protocol (HTTP)
Arquitectura del Protocolo



Protocolo Hypertext Transfer Protocol (HTTP)
Arquitectura del Protocolo



- ✓ HTTP es un protocolo basado en el principio de cliente-servidor: las peticiones son enviadas por una entidad: el agente del usuario (o un proxy a petición de uno)
- ✓ La mayoría de las veces el agente del usuario (cliente) es un navegador Web
- ✓ Cada petición individual se envía a un servidor
- ✓ Los recursos se identifican a través de URI (Uniform Resource Identifier)
- ✓ Un proxy actúa en nombre de otros clientes y presenta las solicitudes de éstos a un servidor. Existen dos escenarios que requieren el uso de un representante:
  - ✓ Intermediario de seguridad
  - ✓ Intermediario Traductor: Diferentes versiones de HTTP

Protocolo Hypertext Transfer Protocol (HTTP)
Arquitectura del Protocolo: URI y URL

- ✓ Un URI es una secuencia de caracteres compacta que identifica a un recurso abstracto o físico, utilizado en múltiples protocolos y aplicaciones

  - Nombre de la computadora: `195.156.123.1` Directorios: `/backup/` (sin protocolo; sin archivo)
  - Protocolo: `http://` Nombre de la computadora: `yeahyeah.com` / (sin directorios; sin archivo)
  - Directorios: `/john/trabajo/` Archivo: `reporte.odt` (sin protocolo; sin nombre de la computadora)
  - Archivo: `index.html` (sin protocolo; sin nombre de computadora; sin directorios)
  - / (sin protocolo; sin nombre de computadora; sin directorios; sin archivo)

- ✓ Un URL es un tipo particular de URI que siempre incluye información acerca de cómo acceder al recurso identificado. Ejemplos

  - Protocolo: `ftp://` Nombre de la computadora: `algunservidor.com` Archivo: `/algun-recurso.php` (sin directorios)
  - Protocolo: `http://` Nombre de la computadora: `www.w3.org` Directorios: `/TR/CSS21/` (sin archivo)
  - Protocolo: `telnet://` Nombre de la computadora: `127.15.19.11` / (dirección IP)

Protocolo Hypertext Transfer Protocol (HTTP)

Partes de una URI

- ✓ Esquema: hace referencia al nombre de un esquema, que define como se asignan los identificadores en su ámbito. Los esquemas habituales en la Web serán http y https.
- ✓ Autoridad: elemento de una autoridad jerárquica de asignación de nombres, típicamente basado en un nombre de dominio de DNS o una dirección de red (IP, IPv6) y, opcionalmente, un numero de puerto.
- ✓ Ruta: elemento que idéntica un recurso en el ámbito del esquema y autoridad proporcionados, típicamente organizado jerárquicamente en fragmentos separados por \/".
- ✓ Consulta: datos no jerárquicos que permiten, en combinación en la ruta, identificar el recurso. Es habitual representarlo como uno o mas pares nombre/valor.
- ✓ Identificador de fragmento: identifica un recurso secundario en el contexto del recurso primario como, por ejemplo, un fragmento concreto de una pagina Web.

Protocolo Hypertext Transfer Protocol (HTTP)
Métodos HTTP

Los principales métodos utilizados por las aplicaciones Web son:

- ✓ GET: obtener el recurso.
- ✓ POST: realizar un procesado (de naturaleza específica para el recurso) basado en los datos que se envían con la petición.

Otros métodos definidos por el estándar son: HEAD, PUT, DELETE, CONNECT, OPTIONS y TRACE

Protocolo Hypertext Transfer Protocol (HTTP)
Método GET

Las peticiones GET:

- ✓ Se utilizan para obtener el contenido de recursos (paginas HTML, imágenes, etc.)
- ✓ Son generadas por los navegadores Web, entre otros, cuando se introduce un URL en la barra de direcciones, o se selecciona en un hipervínculo. También cuando se deben pedir recursos adicionales ligados a una pagina HTML recibida o se envían algunos formularios.
- ✓ Están sujetas al uso de caches para optimizar el uso de recursos.
- ✓ Se consideran seguras, esto es, no deben tener efectos no deseados en el servidor, estado de la aplicación, etc.

Protocolo Hypertext Transfer Protocol (HTTP)
Método POST

Las peticiones POST:

- ✓ Se utilizan para realizar acciones (autenticar a un usuario, añadir un producto al carro de la compra, con confirmar un pedido en una tienda, subir un nuevo mensaje a una red social, etc.).
- ✓ Son generadas por los navegadores Web cuando se envían algunos formularios.
- ✓ No están sujetas al uso de cachés.
- ✓ Pueden no ser seguras. Entre otros problemas potenciales, repetir la petición podría tener efectos no deseados (por ejemplo, realizar un mismo pedido dos veces).

Protocolo Hypertext Transfer Protocol (HTTP)
Componentes de una petición

- ✓ URL del recurso (sin esquema ni autoridad)
- ✓ Método
- ✓ Cabeceras de la petición: datos adicionales acerca de como debe ser procesada la petición
- ✓ Cuerpo de la petición (solo con algunos métodos): datos a ser procesados por el servidor
  - ✓ No puede ser incluido en peticiones GET.
  - ✓ Incluye, en un petición POST, los datos a utilizar en el servidor para procesarla.
  - ✓ Se suele acompañar de las cabeceras Content-Type y Content-Length de la petición.

Protocolo Hypertext Transfer Protocol (HTTP)
Componentes de una respuesta

- ✓ Un estado: código numérico indicando el resultado del procesado de la petición.
- ✓ Cabeceras de la respuesta: datos adicionales acerca de como debe ser procesada la respuesta.
- ✓ Cuerpo de la respuesta: representación de la respuesta a la petición, típicamente una pagina HTML, una imagen, etc.

Protocolo Hypertext Transfer Protocol (HTTP)
Principales cabeceras a peticiones y respuestas

- ✓ Connection: informa al otro extremo de si se debe cerrar o no la conexión TCP una vez completada la respuesta a la petición.
- ✓ Content-Encoding: tipo de codificación (típicamente compresión) aplicado al cuerpo de la petición o respuesta.
- ✓ Content-Length: longitud en bytes del cuerpo del mensaje.
- ✓ Content-Type: tipo MIME del cuerpo del mensaje (por ejemplo, text/html).
- ✓ Accept: preferencias del cliente acerca de los tipos de contenido a recibir.
- ✓ Accept-Encoding: preferencias del cliente acerca de los tipos de codificación del cuerpo de la respuesta a recibir (típicamente compresión).

Protocolo Hypertext Transfer Protocol (HTTP)
Principales cabeceras a peticiones y respuestas

- ✓ Cookie: envío de cookies de vuelta al servidor.
- ✓ Host: campo de autoridad del URL que se pide.
- ✓ If-Modified-Since: sello temporal de la ultima versión del recurso en cache del cliente.
- ✓ If-None-Match: valor ETag recibido con la ultima versión del recurso en cache del cliente.
- ✓ Referer: URL desde el cual se origino la petición actual.
- ✓ User-Agent: información (nombre, versión, etc.) acerca del software del cliente.

Protocolo Hypertext Transfer Protocol (HTTP)
Principales cabeceras a peticiones y respuestas

- ✓ Cache-Control: directivas acerca del almacenamiento de la respuesta en caché.
- ✓ ETag: código que identifica el contenido actual del recurso.
- ✓ Expires: indicación de hasta cuándo se puede guardar el recurso en caché.
- ✓ Vary: listado de cabeceras de la petición cuyos valores pueden afectar a que cambie el contenido de un recurso.
- ✓ Location: en respuestas de redirección, nuevo URL a pedir por el cliente.
- ✓ Server: información (nombre, versión, etc.) acerca del software del servidor.
- ✓ Set-Cookie: establece cookies que el cliente debe enviar en futuras peticiones.

Protocolo Hypertext Transfer Protocol (HTTP)
Campos cabeceras general

- ✓ Cache-Control (*"control de caché"*)
- ✓ Connection (*"conexión"*)
- ✓ Date (*"Fecha"*)
- ✓ Forwarded (*"reenviado"*)
- ✓ Keep-Alive (*"mantener activo"*)
- ✓ MIME-Version (*"versión de MIME"*)
- ✓ Pragma
- ✓ Upgrade (*"actualizar"*)

Protocolo Hypertext Transfer Protocol (HTTP)
Códigos de estado de las respuestas

Código	Razón	Significado
200	OK	Petición procesada con éxito.
301	Moved Permanently	Recurso movido a otro URL (cabecera `Location`), que el cliente debe usar siempre a partir de ahora.
302	Found	Recurso movido temporalmente a otro URL (cabecera `Location`).
303	See Other	Se debe cargar otro recurso (página de confirmación, progreso, etc.) con método `GET`.
304	Not Modified	El cliente puede usar su versión del recurso en caché.
400	Bad Request	El cliente envió una petición HTTP inválida (sintaxis, etc.).
403	Forbidden	El cliente no puede acceder al recurso.
404	Not Found	No existe un recurso con la ruta dada.
405	Method Not Allowed	El recurso no admite el método indicado en la petición.
500	Internal Server Error	Error en el servidor al procesar la petición.

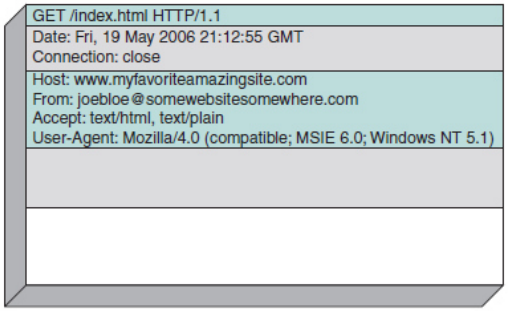
Protocolo Hypertext Transfer Protocol (HTTP)
Ejemplo de una petición en HTTP/1.1

```
GET /Inicio HTTP/1.1
Host: www.unt.edu.ar
Connection: keep-alive
Cache-Control: max-age=0
User-Agent: Chrome/62.0.32.02.89
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: es-ES,es;q=0.9,en;q=0.8,en-US;q=0.7
```

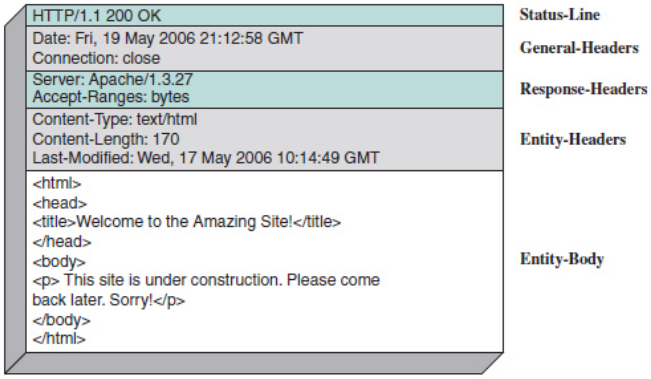
Protocolo Hypertext Transfer Protocol (HTTP)
Ejemplo de una respuesta HTTP/1.1

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E26E8...;
Domain=www.uc3m.es; HttpOnly
Cache-Control: no-store
Last-Modified: Fri, 10 Nov 2017 11:44:28 CET
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Fri, 10 Nov 2017 10:44:28 GMT
<!DOCTYPE html>
<html lang="es" class="no-js">
<head>
<title>Inicio | UC3M</title>
(...)
```

Protocolo Hypertext Transfer Protocol (HTTP)
Formato de los mensajes de petición y respuesta



(a) HTTP request (solicitud)



(b) HTTP response (respuesta)

Protocolo Hypertext Transfer Protocol (HTTP)
Cookies

- ✓ HTTP es un protocolo sin estado, esto es, cada petición es independiente de las demás.
- ✓ Las cookies permiten mantener estado: consisten en pequeñas cantidades de datos asociados a un nombre que el servidor genera y envía al cliente en mensajes de respuesta para que este las incluya en sucesivas peticiones.
- ✓ Algunos usos típicos de las cookies son los siguientes:
  - ✓ Gestión de sesiones
  - ✓ Almacenamiento de preferencias
  - ✓ Rastreo de usuarios

Protocolo Hypertext Transfer Protocol (HTTP)
Cookies

- ✓ Una cookie se representa como una pequeña cadena de texto que contiene:
  - ✓ Un nombre: un servidor puede establecer varias cookies con distintos nombres.
  - ✓ Un valor: los datos de la cookie en sí mismos.
  - ✓ Atributos:
    - ✓ Domain y Path: definen en qué peticiones, por autoridad y ruta, el cliente enviará la cookie al servidor.
    - ✓ Expires y Max-Age: definen cuando la cookie debe dejar de ser utilizada por el cliente. Si no se especifica ninguno, se elimina al cierre del navegador.
    - ✓ Secure: la cookie solo puede ser enviada por canales seguros (HTTPS típicamente).
    - ✓ HttpOnly: solo se debe enviar o permitir acceso a la cookie a través de HTTP o HTTPS. Por ejemplo, no debe ser accesible a código JavaScript.

Protocolo Hypertext Transfer Protocol (HTTP)
Cookies

- ✓ Creación de cookies (en respuestas HTTP):

```
Set-Cookie: sid=Aa119lVaY...;
Expires=Thu, 13 Feb 2020 21:47:38 GMT;
Path=/; Domain=.example.com; Secure; HttpOnly
```

- ✓ Envío de cookies (en peticiones HTTP):

```
Cookie: sid=Aa119lVaY...
```

Temas a tratados

1. Protocolo DHCP (Dynamic Host Configuration Protocol)
2. Servicio de Resolución de Nombres DNS (Domain Name System)
3. Protocolo de Correo Electrónico SMTP (Simple Mail Transfer Protocol)
4. Protocolo de Transferencia de Hipertexto HTTP (Hypertext Transfer Protocol)

FINAL DEL MÓDULO 9