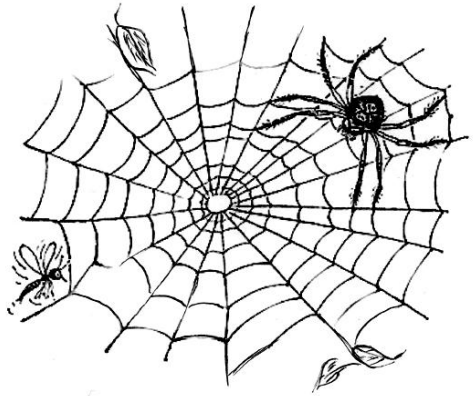
# Introducción a TCP/IP

Inter
Net
Working

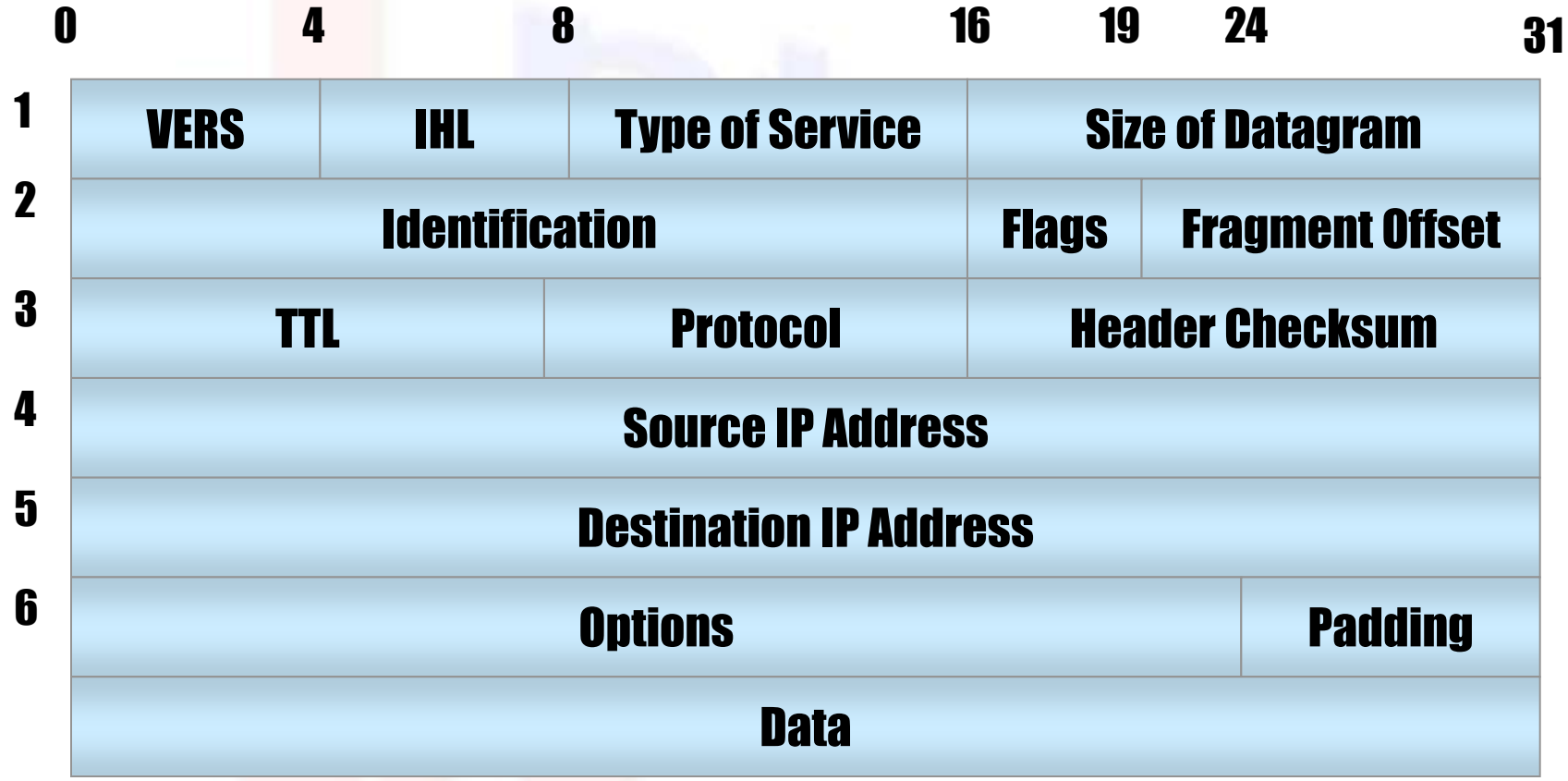


# Formato de Paquetes IP

# IP - Internet Protocol

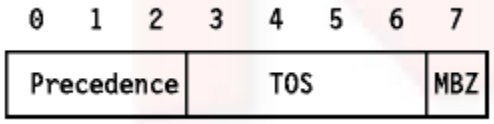
- Protocolo no orientado a la conexión.
- No transmite información de control.
- No establece una conexión end-to-end. antes de transmitir los datos.
- No es confiable.

# Header del Datagrama IP



# Descripción de Campos 1

- Vers. Version de IP.
- IHL. IP Header Length. Número de palabras de 32 bits que forman el header. Usualmente 5.
- Type of Service. Ahora conocido como Differentiated Services Code Point (DSCP) (usualmente 0, pero puede indicar una Calidad de Servicios solicitada a la red, DSCP define uno de los tipos de Clase de Servicio)




- Precedencia : Es una medida de la naturaleza y prioridad de este datagrama.
  - 000 Rutina
  - 001 Prioridad
  - 010 Imediato
  - 011 "Flash"
  - 100 "Flash override"
  - 101 Crítico
  - 110 Control de red("Internetwork control")
  - 111 Control de red("Network control")

- TOS "*type of service*":
  - 1000 Minimizar retardo
  - 0100 Maximizar la densidad de flujo
  - 0010 Maximizar la fiabilidad
  - 0001 Minimizar el coste monetario
  - 0000 Servicio normal
- MBZ
  - Reservado para uso futuro(debe ser cero, a menos que participe en un experimento con IP que haga uso de este bit)
  - Una descripción detallada del TOS se puede encontrar en el RFC 1349.

# Descripción de Campos 2

- Identification. Número de 16 bit number que junto con la dirección fuente identifica en forma única al paquete. Se utiliza especialmente para reensamblar datagamas fragmentados.
- Flags. Secuencia de tres flags usados para control si los routers tienen permitido fragmentar paquetes e indicar las partes de un paquete que reciben.


- **0** Reservado, debe ser cero
- **DF** No fragmentar("Don't Fragment")
  - 0 permite la fragmentación
  - 1 no.
- **MF** Más fragmentos("More fragments")
  - 0 significa que se trata del último fragmento del datagrama.
  - 1 que no es el último.

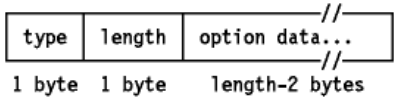
# Descripción de Campos 3

- Fragmentation Offset. Contador de bytes desde el comienzo del paquete original enviado enviando por un router que realizó una fragmentación.
- TTL. Time To Live. Número de saltos o links que los paquetes puedes ser ruteados, el valor es decrementado al pasar por los routers. Es usado para prevenir loops de ruteo accidentales.
- Size of Datagram. Largo del datagrama IP incluye largo del header + data.
- Protocol. Indica el tipo de transporte empaquetado
  - 1 = ICMP
  - 2 = IGMP
  - 4 = IP encapsulation
  - 6 = TCP
  - 17 = UDP
  - 89 = OSPF
- Header Checksum. Chequeo de Errores del encabezado utilizado para detectar errores de procesamiento en los routers.
- Source/Destination IP Address. Dirección IP de la fuente original o del destino final del paquete.

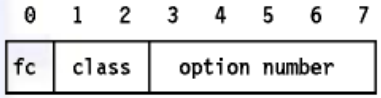
# Descripción de Campos 4

- Options. Este campo tiene longitud variable. Puede haber cero o más opciones. Hay dos formatos para estas. El formato usado depende del valor del número de opción hallado en el primer byte.


  - Un byte de de tipo (“type byte”).
  - Un byte de tipo, un byte de longitud y uno o más bytes de opciones




- Estructura del “type byte”
  - fc "Flag copy", que indica si el campo se ha de copiar(1) o no(0) cuando el datagrama está fragmentado.
  - class Un entero sin signo de 2 bits:
    - 0 control
    - 1 reservado
    - 2 depurado y mediciones
    - 3 reservado




- option number Entero sin signo de 5 bits.
  - 0 Fin de la lista de opciones, con "class" a cero, fc a cero, y sin byte de longitud o de datos. Es decir, la lista termina con el byte X'00'. Sólo se requiere si la longitud de la cabecera IP(que es un múltiplo de 4 bytes) no se corresponde con la longitud real de las opciones.
  - 1 No operación. Tiene "class" a cero, fc a cero y no hay byte de longitud ni de datagramas. Es decir, un byte X'01' es NOP("no operation"). Se puede usar para alinear campos en el datagrama.
  - 2 Securidad. Tiene "class" a cero, fc a uno y el byte de longitud a 11 y el de datos a 8. Se usa para la info de seguridad que necesitan las especificaciones del depto de defensa de US.
  - 3 LSR("Loose Source Routing"). Tiene "class" a cero, fc a uno y hay un campo de datos de longitud variable.
  - 4 IT("Internet Timestamp"). Tiene "class" a 2, fc a cero y hay un campo de datos de longitud variable.
  - 7 RR("Record Route"). Tiene "class" a 0, fc a cero y hay un campo de datos de longitud variable.
  - 8 SID("Stream ID", o identificador de flujo). Tiene "class" a 0, fc a uno y hay un byte de longitud a 4 y un byte de datos. Se usa con el sistema SATNET.
  - 9 SSS("Strict Source Routing"). Tiene "class" a 0, fc a uno y hay un campo de datos de longitud variable.

# Fragmentación 1

- Un datagrama puede pasar de una red física a otra y estas imponen un tamaño máximo de las tramas llamado MTU (Maximum Transmission Unit). Por lo tanto es necesario disponer de un mecanismo para fragmentar datagramas IP grandes en otros más pequeños y luego reensamblarlos en el host destino.
  - Un datagrama sin fragmentar tiene a cero toda la información de fragmentación. Es decir, el flag fc y el fo(fragment offset) están a cero.
  - Cuando se ha de realizar la fragmentación, se ejecutan los siguientes pasos:
    - Se chequea el bit de flag DF para ver si se permite fragmentación. Si está a uno, el datagrama se desecha y se devuelve un error al emisor usando ICMP.
    - Basándose en el valor MTU, el campo de datos se divide en dos o más partes. Todas las nuevas porciones de datos, excepto la última, se alinean a 8 bytes.
    - Todas las porciones de datos se colocan en datagramas IP. Las cabeceras se copian de la cabecera original, con algunas modificaciones:
      - El bit de flag mf(more fragments) se pone a uno en todos los fragmentos, excepto en el último.
      - El campo fo se pone al valor de la localización de la porción de datos correspondiente en el at original, con respecto al comienzo del mismo. Su valor se mide en unidades de 8 bytes.
      - Si se incluyeron opciones en el datagrama original, el bit de orden superior del byte "type option" determina si se copiaran o no en todos los fragmentos o sólo en el primero. Por ejemplo, las opciones e encaminamiento de la fuente se tendrán que copiar en todos los fragmentos y por tanto tendrán a uno este bit.
      - Se inicializa el campo de longitud(length) del nuevo datagrama.
      - Se inicializa el campo de longitud(length) total del nuevo datagrama.
      - Se recalcula el checksum de la cabecera.
    - Cada uno de estos datagramas se envía como un datagrama IP normal. IP maneja cada fragmento dde forma independiente, es decir, los fragmento pueden atravesar diversas rutas hacia su destino, y pueden estar sujetos a nuevas fragmentaciones si pasan por redes con MTUs inferiores.

# Fragmentación 2

- En el host de destino, los datos se tienen que reensamblar. El host emisor inicializó el campo ID a un número único(dentro de los límites impuestos por el uso de un número de 16 bits). Como la fragmentación no altera este campo, los fragmentos que le van llegando al destino se pueden identificar, si este ID se usa junto con las direcciones IP fuente y destino(source, destination) del datagrama. También se chequea el campo de protocolo
- Con el fin de reensamblar los fragmentos, el receptor destina un buffer de almacenamiento en cuanto llega el primer fragmento. Se inicia una rutina para un contador. Cuando el contador a un timeout y no se han recibido todos los datagramas, se desecha el datagrama. El valor inicial el contador es el TTL(time-to-live). Depende de la implementación, y algunas permiten configurarlo.
- Cuando llegan los fragmentos siguientes, antes de que expire el tiempo, los datagramas se copian al buffer en la localización indicada por el fo(fragment offset). Cuando han llegado todos los datagramas, se restaura el datagrama original y continúa su procesamiento.
- Nota: IP no proporciona el contador de reensamblado. Tratará cada datagrama, fragmentado o no, de la misma forma. Depende de una capa superior el implementar un timeout y reconocer la pérdida de fragmentos. Esta capa podría ser TCP para el transporte en un red orientada a conexión o UDP, para el caso contrario.

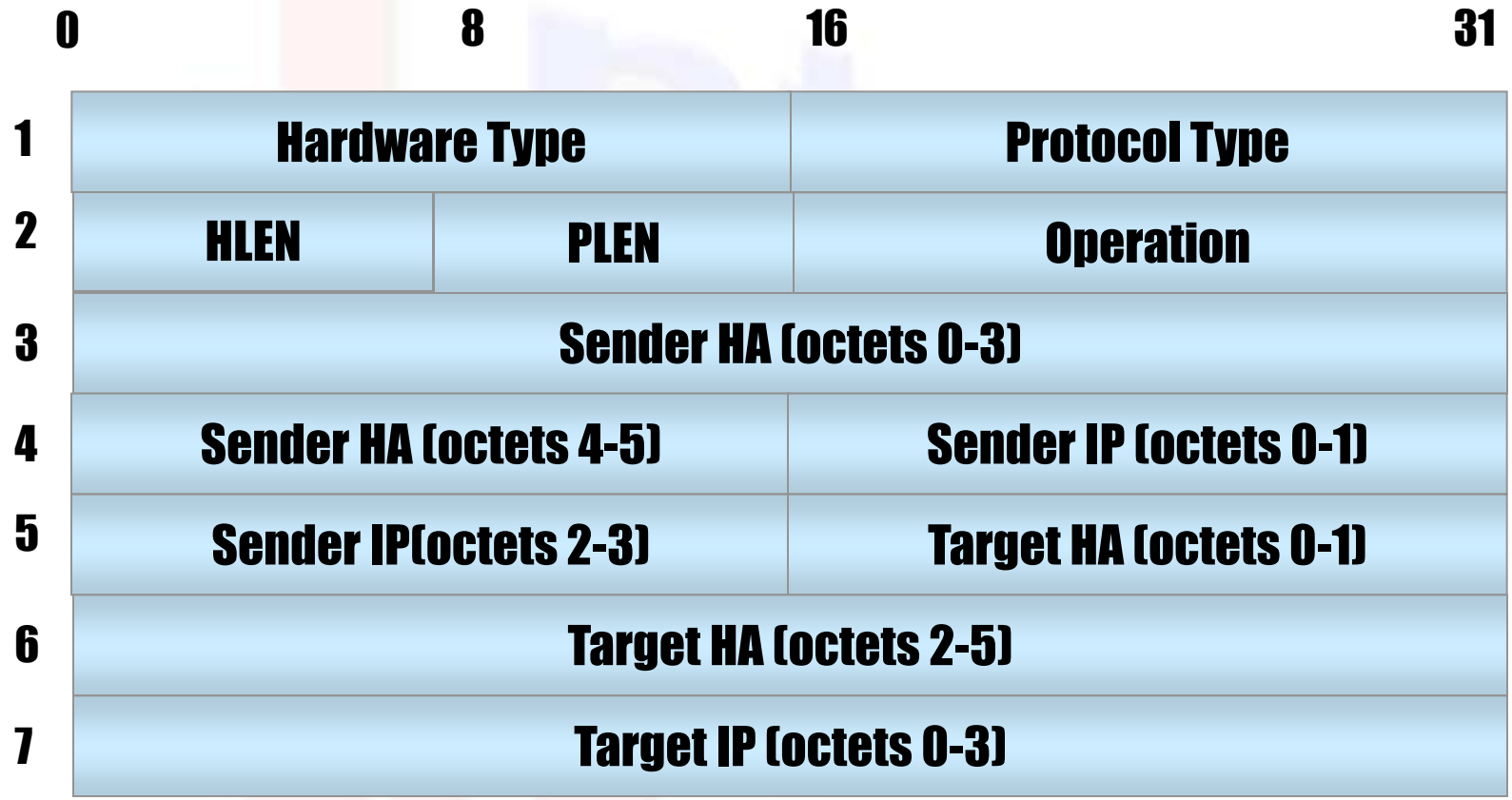
- http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html

# ARP

# ARP Address Resolution Protocol

- Es un protocolo utilizado por IP para asociar una dirección IP a una dirección física y de este modo establecer una comunicación.
- El protocolo envía un broadcast preguntando por una dirección IP determinada y la estación que la posee responde indicando de este modo su dirección física.
- Para optimizar la consulta continua los equipos poseen una tabla cache con las últimas interrogaciones solicitadas.
- RARP. Corresponde a la consulta inversa es decir cuando se requiere saber la dirección IP de un dispositivo con dirección MAC conocida.

# Formato del Mensaje ARP



# Tipos de Mensajes

- ARP request
- ARP reply
- RARP request
- RARP reply

# Tablas ARP

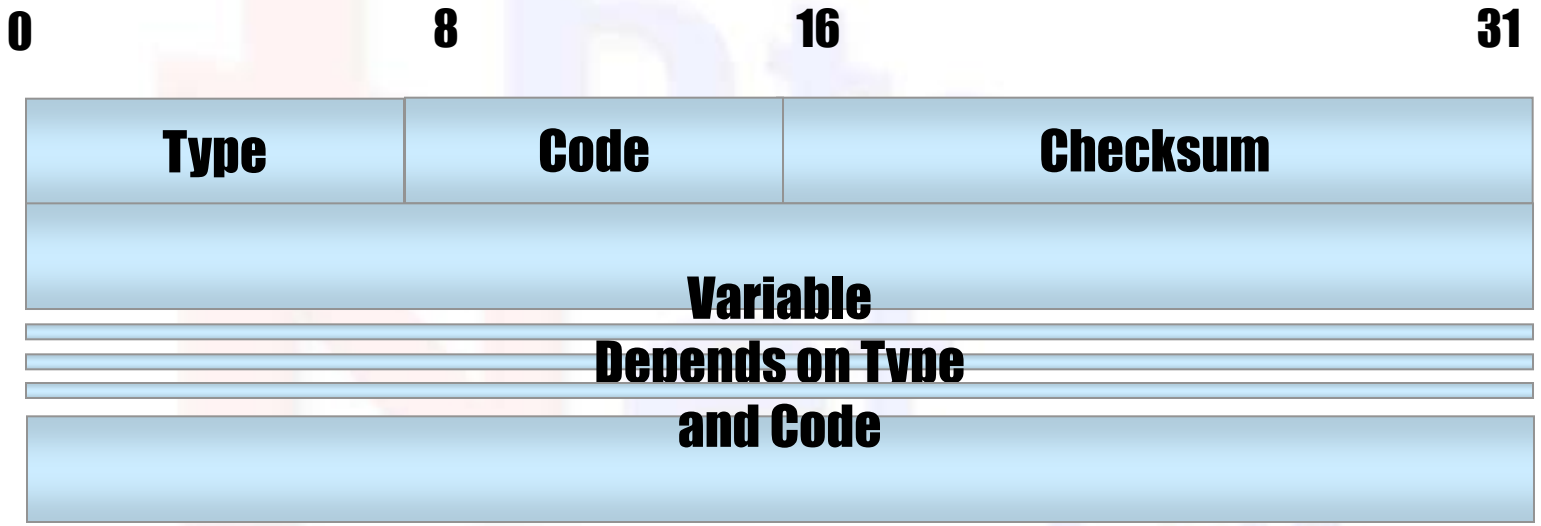
```
matrix% arp
Usage: arp hostname
       arp -a
       arp -d hostname
       arp -s hostname ether_addr [temp] [pub] [trail]
       arp -f filename
matrix% arp -a

Net to Media Table: IPv4
Device   IP Address               Mask      Flags   Phys Addr
------ -------------------- -------------- ----- ---------------
hme0   172.16.231.90        255.255.255.255      00:05:5d:5f:af:c2
hme0   172.16.231.83        255.255.255.255      00:02:3f:22:af:24
hme0   172.16.231.77        255.255.255.255      00:10:b5:f5:ce:8e
hme0   jsandova.tmovil.cl   255.255.255.255      00:02:3f:22:a3:0b
hme0   172.16.231.121       255.255.255.255      00:08:02:8f:c8:2f
```

# ICMP

# ICMP- Internet Control Mensaje Protocol

- RFC 792
- Control de flujo.
  - ICMP source quench message.
- Detecta destino inaccequible.
  - Destination unreacheable message
- Redirecciona rutas.
  - ICMP redirect message.
- Chequea host remotos (PING)
  - ICMP echo message.

# Formato del Mensaje ICMP



# Tipos de Mensajes

- Type Especifica el tipo del mensaje:
  - 0 Echo reply
  - 3 Destination unreachable
  - 4 Source quench
  - 5 Redirect
  - 8 Echo
  - 9 Router Advertisement
  - 10 Router Solicitation
  - 11 Time exceeded
  - 12 Parameter Problem
  - 13 Timestamp request
  - 14 Timestamp reply
  - 15 Information request(obsolete)
  - 16 Information reply(obsolete)
  - 17 Adress mask request
  - 18 Adress mask reply

# Tipos de Mensajes 1

- Destination Unreachable Message.
  - Indica que de acuerdo a la tabla de ruteo la red es inalcanzable por el host origen.
- Time Exceeded Message
  - Indica que el TTL ha llegado a Cero y que el paquete ha sido descartado.
- Parameter Problem Message
  - Indica que se ha detectado un problema con los parámetros del header y no puede seguir procesándose el datagrama por lo que se descartará.
- Source Quench Message
  - Indica que no tiene espacio en el buffer para enviarlo a la próxima red.

# Tipos de Mensajes 2

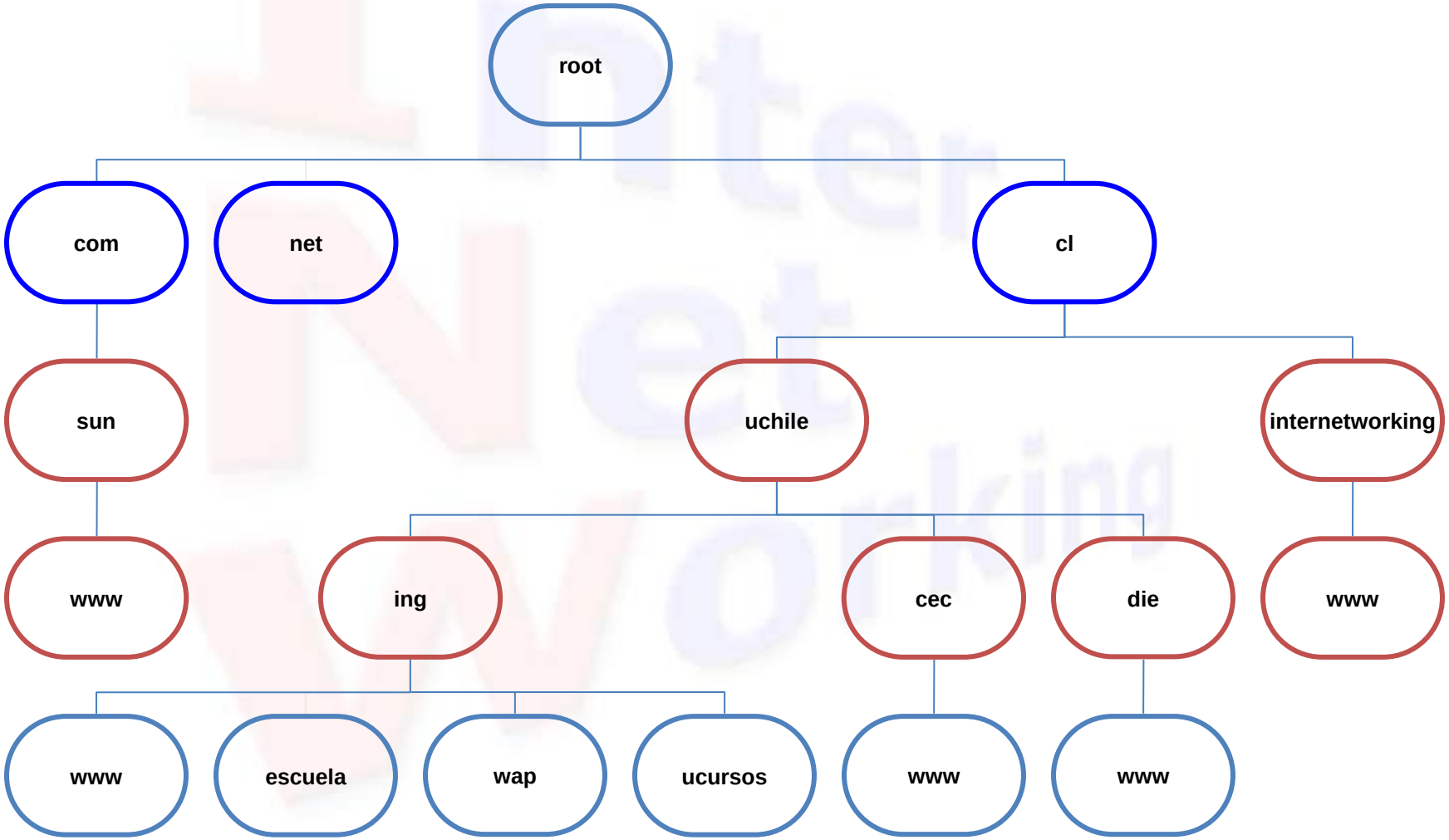
- Redirect Message
  - El router detecta que el próximo salto es un router dentro de la misma red del equipo que recibio el datagrama por lo que le informa que es mejor que se lo envie al otro router.
- Echo or Echo Reply Message.
  - La información recibida en un mensaje echo debe ser devuelta en un mensaje echo reply. Usualmente utilizado para medir Round Trip y perdida de paquetes
- Timestamp or Timestamp Reply Message
  - Usado pora identificar tiempos de vieje y de procesamiento del mensaje contine: Originate Timestamp, Receive Timestamp y Transmit Timestamp.
- Information Request or Information Reply Message
  - Utilizado para determinar las redes a las que se encuentra conectado un host.

# DNS

# DNS

- Aplicación distribuida que permite asociar un nombre a una dirección IP.
- Posee una estructura jerárquica.
- Delegación de autoridad
- BIND. Berkeley Internet Name Domain
- Conceptos:
  - Servidor Primario. Actualiza
  - Servidor Secundario. Informa
  - Servidor Cache. Informa sin autoridad

# Estructura jerárquica



# Delegación de Autoridad

- Se delegan a subdominios definiendo un record NS.
- Las preguntas sobre hosts de un subdominio son derivadas al DNS del subdominio

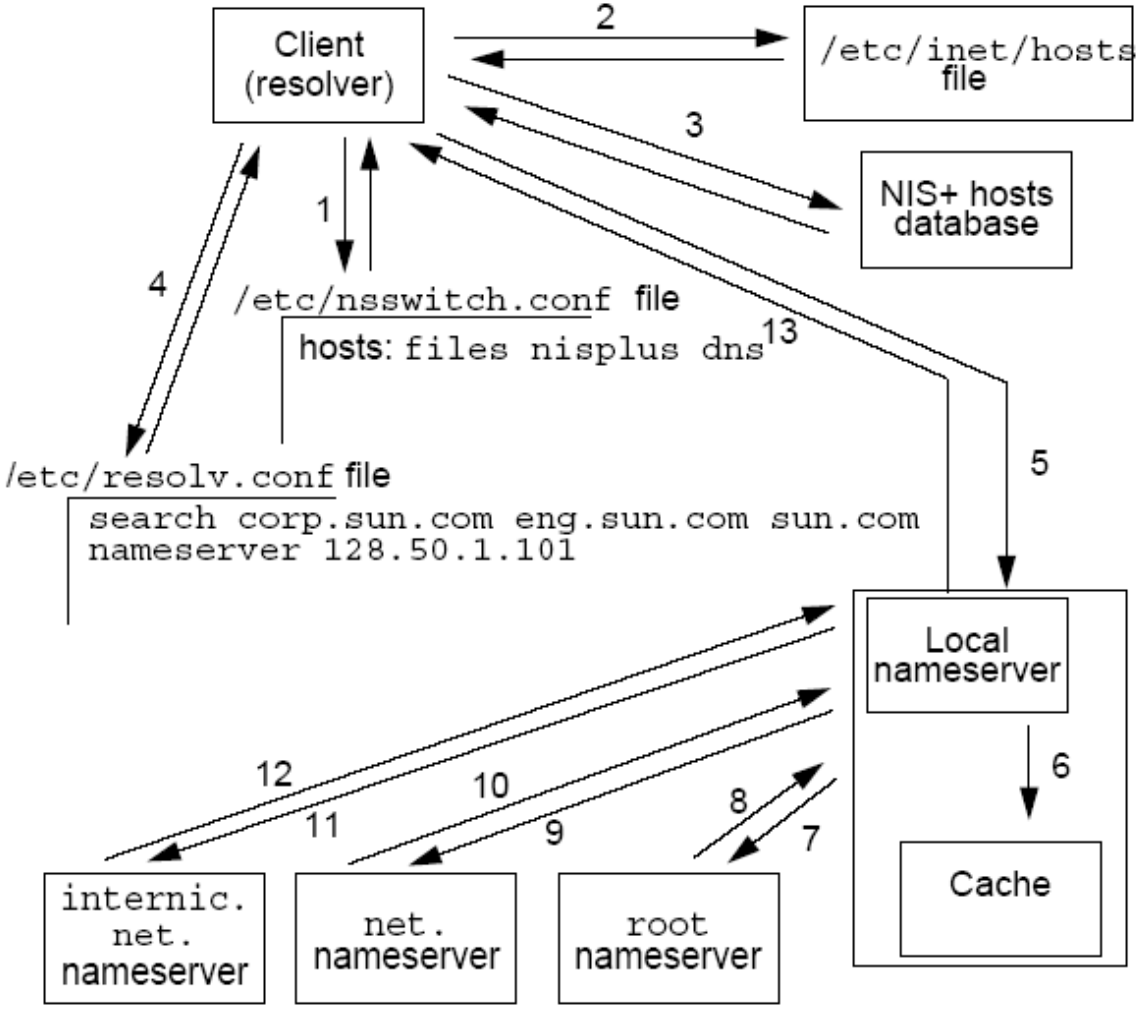
# Tipos de Registros

- **A** Address Record. Para definir un host
- **CNAME** Canonical Name. Usado para definir una alias de un host.
- **NS** Name Service. Para definir un DNS
- **MX** Mail Exchange. Para definir un servidor SMTP
- **PTR** para definir un dominio inverso
- **SOA** Start of Authority

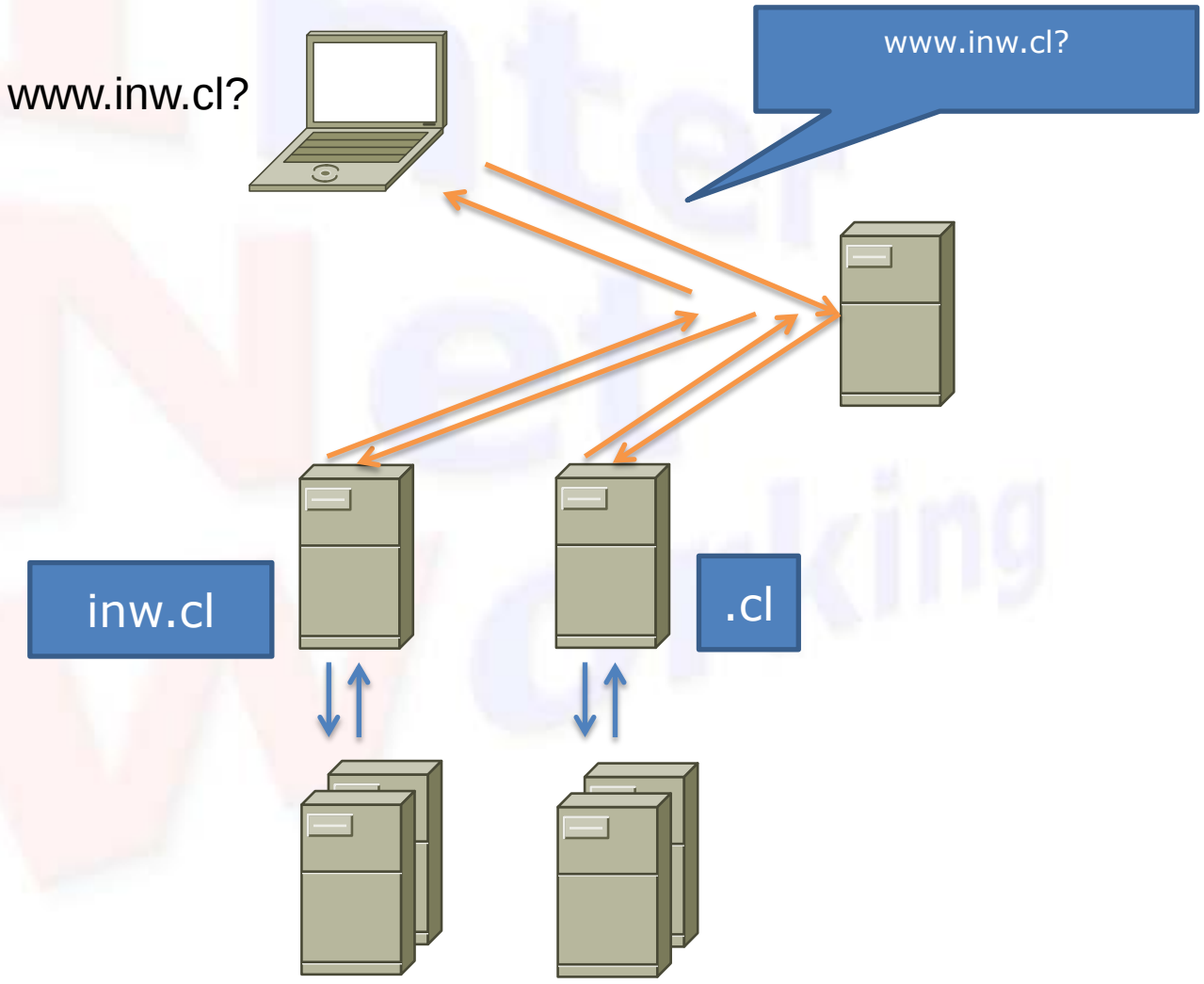
# SOA Start of Authority

- **Serial Number**. Habitualmente en formato yyyymmddhh para indicar modificación. Se asume una nueva versión si este número se incrementa.
- **Refresh**. Cada cuanto tiempo el secundario refresca.
- **Retry**. Cada cuanto tiempo reintenta si la actualización del secundario fracaza.
- **Expire**. Indica cuanto tiempo puede estar la copia en el secundario sin refrescar.
- **TTL**. Tiempo que permanecerán los registros en los caches de los DNSs.

# Ejemplo de resolución de nombres



# Tipos de Servidores de Nombres



# named.conf

- Servidor Maestro

```
zone "example.com" IN {
 type master;
 file "example.com.zone";
 allow-update { none; };
 };
```

- Servidor Esclavo

```
zone "example.com" {
 type slave;
 file "example.com.zone";
 masters { 192.168.0.1; };
 };
```

# Archivo de Zona

```
$ORIGIN example.com.
$TTL 86400
@ IN SOA dns1.example.com. hostmaster.example.com. (
                              2001062501 ; serial
                              21600 ; refresh after 6 hours
                              3600 ; retry after 1 hour
                              604800 ; expire after 1 week
                              86400 ) ; minimum TTL of 1 day
          IN       NS       dns1.example.com.
          IN       NS       dns2.example.com.
          IN       MX       10 mail.example.com.
          IN       MX       20 mail2.example.com.
          IN       A        10.0.1.5
server1   IN       A        10.0.1.5
server2   IN       A        10.0.1.7
dns1      IN       A        10.0.1.2
dns2      IN       A        10.0.1.3
ftp       IN       CNAME    server1
mail      IN       CNAME    server1
mail2     IN       CNAME    server2
www       IN       CNAME    server2
```

# Resolución Inversa

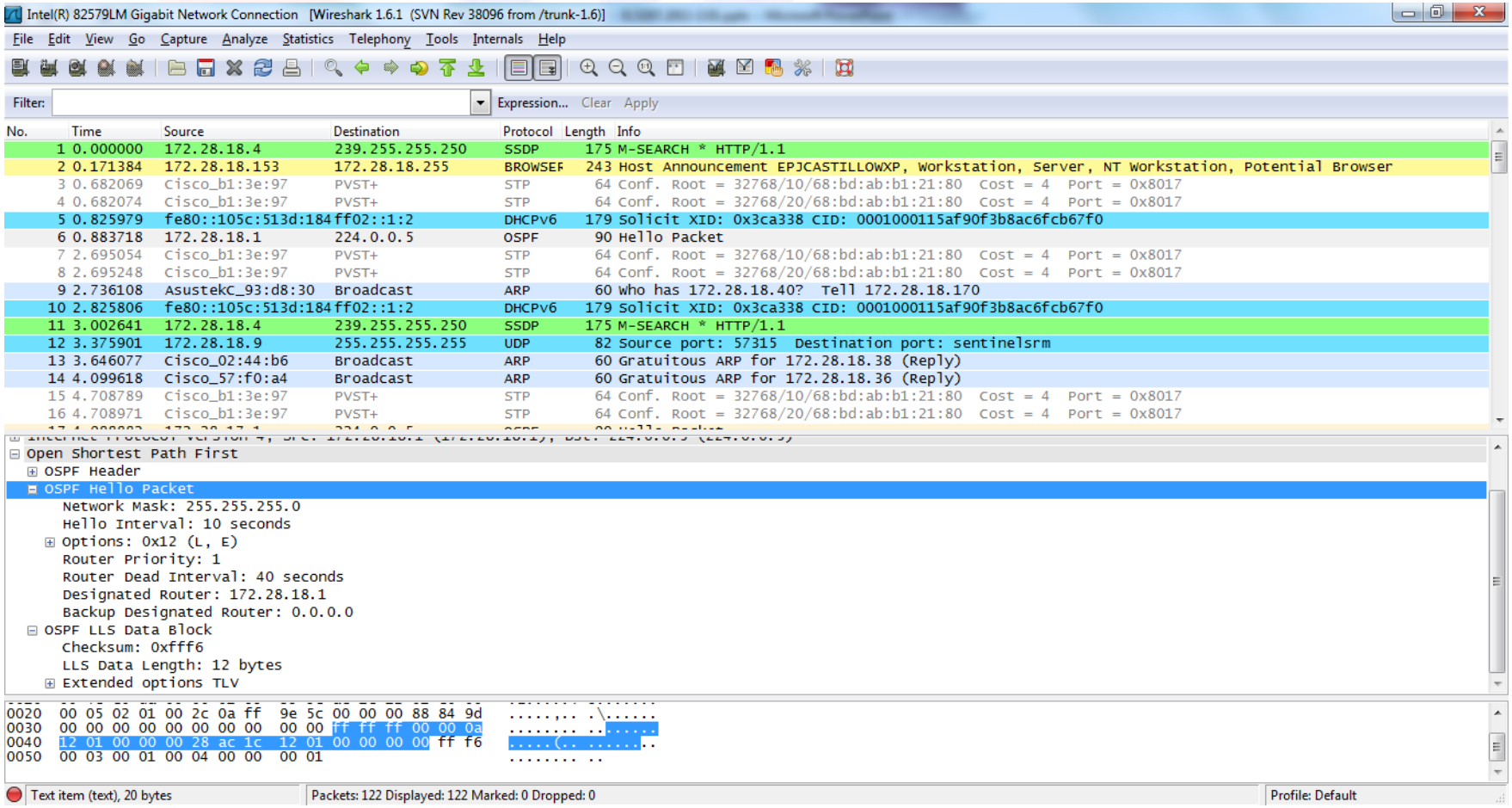
```
zone "1.0.10.in-addr.arpa" IN {
 type master;
 file "example.com.rr.zone";
 allow-update { none; };
};
```

```
$ORIGIN 1.0.10.in-addr.arpa.
$TTL 86400
@ IN SOA dns1.example.com. hostmaster.example.com. (
                            2001062501 ; serial
                            21600 ; refresh after 6 hours
                            3600 ; retry after 1 hour
                            604800 ; expire after 1 week
                            86400 ) ; minimum TTL of 1 day
        IN      NS dns1.example.com.
        IN      NS dns2.example.com.
20      IN      PTR alice.example.com.
21      IN      PTR betty.example.com.
22      IN      PTR charlie.example.com.
23      IN      PTR doug.example.com.
24      IN      PTR ernest.example.com.
25      IN      PTR fanny.example.com.
```

# Herramientas

# wireshark

- www.wireshark.org



# Herramientas nativas

- Snoop
- Tcpdump
- Ping
- Traceroute (tracert)
- netstat