

Tema 2: IP

- Funciones IP
 - Routed vs Routing protocols
 - Tipos de datagramas: unicast, multicast, broadcast
- Formato cabecera IP
- Direcciones IP, máscaras y subredes
 - Classfull addresses
 - Clase A, B, C, D
 - Subnetting
 - Classless addresses: CIDR y supernetting
 - Interficie loopback
 - DHCP
 - Cabeceras IPv6
- Detección de errores: checksum
- Resolución de direcciones: ARP/RARP

Tema 2: IP

- **Nivel de red**
 - Routed Protocols (protocolos encaminados):
 - Encapsulan información de nivel 4 (transporte)
 - Definen un esquema de direcciones jerarquizado
 - Usan un protocolo de nivel de enlace para transmitir la información a un dispositivo de nivel 3 (router)
 - E.g: IP, IPX, ...
 - Routing Protocols (protocolos de encaminamiento):
 - Buscan rutas óptimas para que los protocolos encaminados sepan a donde dirigir la información
 - E.g: RIP, IGRP, OSPF, EIGRP, BGP, ...
 - Otros (en pila TCP/IP)
 - ARP/RARP: mapeo de direcciones IP y MAC y viceversa
 - ICMP: control de mensajes de IP

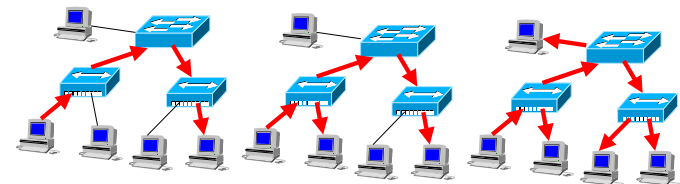
Tema 2: IP

- Unidad de información: datagrama IP
- Protocolo no-orientado a la conexión (conectionless Protocol)
 - IP no mantiene ningún tipo de estado de información entre sucesivos datagramas
 - Cada datagrama IP es tratado independientemente respecto a otros datagramas (de la misma/distinta conexión)
 - No fases de establecimiento – mantenimiento – cierre de la conexión
 - Datagramas IP pueden ser entregados sin un orden determinado
 - Control de errores: si algo va mal (detector de errores en los datagramas IP), IP descarta los datagramas y envía un aviso al origen a través del protocolo ICMP
- IP es totalmente independiente de la tecnología de red, debajo puede haber cualquier nivel de enlace (ATM, PPP, Ethernet, Token Ring, Frame Relay, ISDN,)

Tema 2: IP

• Tipos de datagramas

- **Unicast:** se envía el datagrama a un solo destinatario de la red
- **Multicast:** se envía el datagrama a un grupo de destinatarios de la red
- **Broadcast:** se envía el datagrama a todos los destinatarios de la red



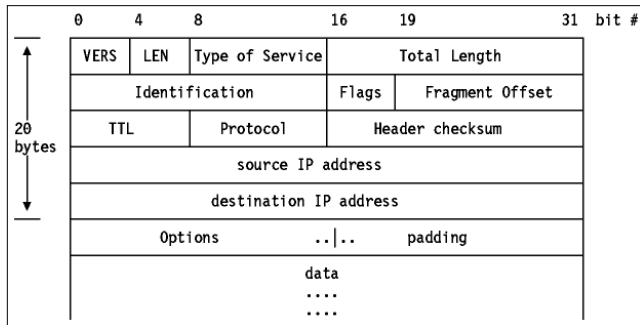
Unicast

Multicast

Broadcast

Tema 2: IP

Datagrama IP:



Tema 2: IP

• IP datagram

- **Version:** 4 (IPv4), 6 (IPv6)
- **Header Length:** 4.n bytes (límite 60 bytes)
- **TOS (Type of Service):** 3 bits of precedence + 4 bits de TOS + 1 bit a 0. Los 4 bits se activan para indicar:
 - Precedence: 8 niveles (no usados en IPv4)
 - minimum delay, maximum throughput, maximum reliability, minimum cost
 - Actualmente estos 8 bits se usan de manera diferente definidos por nuevos protocolos, e.g. Servicios Diferenciados (Diff Serv) para proporcionar Calidad de Servicio (QoS) en Internet
- **Total length:** max is 65535 bytes, pero típico MTU (Maximum Transfer Unit) es 576 bytes de datagrama IP (viene de X.25)
- **Identification:** incrementado en uno por cada datagrama enviado

Tema 2: IP

• IP datagram

- **Flags + fragment offset:** para fragmentar datagramas
- **TTL (Time To Live):** restado en uno por cada router atravesado
- **Protocol:** contenido del datag. IP, e.g datag. IP (0), mensajes ICMP (1), seg. TCP (6), datag. UDP (17), datag. IPv6 (41) ...
- **Header Checksum:** detector de errores
- **Source/Destination IP addresses**
- **Options (máximo 40 bytes)**
 - **Timestamp**
 - **Loose source routing**
- **Data:** contenido del nivel superior u otros
 - Segmentos TCP, datagramas UDP, mensajes de otros protocolos de transporte como RSVP, mensajes ICMP, datagramas IP (tunneling) ...
 - Cada protocolo es identificado por el campo "protocolo", e.g. TCP = 6

Tema 2: IP

• Direcciones IP:

- Son de 32 bits divididos en 4 octetos expresados en decimal acompañados de una máscara de red
- El formato decimal es del tipo xxx.xxx.xxx.xxx
- Contienen una parte que identifica la red (o subred) a la que pertenecen (NetID) y una parte que identifica la máquina (hostID)
- El primer valor decimal determina la clase de direcciones IP
 - 001 - 126 = Clase A
 - 128 - 191 = Clase B
 - 192 - 223 = Clase C
 - 224 - 239 = Clase D

Tema 2: IP

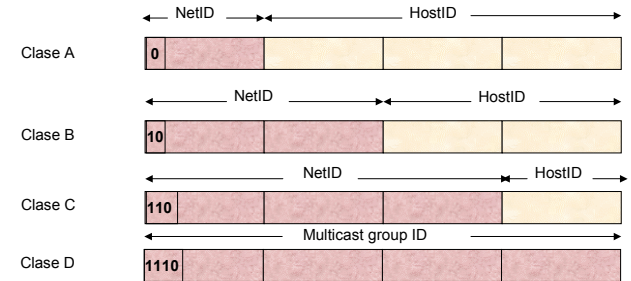
Direcciones IP

- Las direcciones IP son únicas.
- El organismo encargado de su asignación es IANA (Internet Assigned Numbers Authority), dependiente de ICANN.
- En Europa el organismo encargado de la asignación de direcciones IP es RIPE (Reseaux IP Europeenes).
- RIPE asigna grupos de direcciones IP a las Operadoras (Telefonica, BT, etc..) que a su vez las asignan a los ISP.
- Cuando un ISP se convierte en AS (Autonomous System) las direcciones se las asigna RIPE.
- La petición de direcciones se hace a RIPE mediante los formularios 140, 139, y 138.

Tema 2: IP

Direcciones IP:

- Classfull addresses:** son aquellas direcciones IP que definen una clase de tipo A (8 bits de Mask), tipo B (16 bits de Mask) y C (24 bits de Mask) y clase D para multicast



Tema 2: IP

IP addresses:

Classfull addresses

- Clase A:** 0.0.0.0 a 126.0.0.0 con máscaras 255.0.0.0
 - $2^{(8-1)} - 2 = 2^7 - 2 = 126$ redes
 - $2^{24} - 2 = 16.777.214$ hosts/red
- Clase B:** 128.0.0.0 a 191.255.0.0 con máscara 255.255.0.0
 - $2^{(16-2)} - 2 = 2^{14} - 2 = 16.382$ redes
 - $2^{16} - 2 = 65.534$ hosts/red
- Clase C:** 192.0.0.0 a 223.255.255.0 con máscara 255.255.255.0
 - $2^{(24-3)} - 2 = 2^{21} - 2 = 2.097.150$ redes
 - $2^8 - 2 = 254$ host/red
- Clase D (Multicast):** 224.0.0.0 a 239.255.255.255
 - Hay direcciones especiales multicast definidas por IANA

Tema 2: IP

IP addresses:

Direcciones con un significado especial

- Dirección de red:** HostID = todo 0s, e.g. 147.83.0.0, nunca se utilizan como dirección de dispositivos.
- Dirección broadcast:** HostID=todo 1s, e.g. 147.83.255.255
- Dirección 0.0.0.0** = este host en esta red (Nunca como dirección destino. Sólo sentido al arrancar el sistema como dirección origen), e.g. BOOTP
- Interficie loopback:** permite a un cliente comunicarse con un servidor dentro de la misma máquina sin tener que usar una tarjeta de red. Se usa la clase A 127.0.0.0, de la que utilizamos la dirección 127.0.0.1 como dirección loopback.
- Direcciones privadas:** son direcciones que no son enrutables en Internet, por tanto no son "vistas" por nadie fuera esa red
 - Clase A: 10.0.0.0
 - Clase B: 172.16.0.0 a 172.31.0.0
 - Clase C: 192.168.0.0 a 192.168.255.0

Tema 2: IP

• Subnetting

- El subnetting aparecio a medida que los sitios Web empezaron a desarrollarse
- Una red puede ser dividida en redes más pequeñas llamadas subredes
- Las mascararas de subred se utilizan para determinar la parte de la dirección IP que se utiliza para red, la subred y los host
- E.g. para la clase B 147.83.0.0. las subredes se pueden representar de la siguiente forma:
 - Decimal con putos : 147.83.0.0 255.255.0.0
 - Recuento de bits : 147.83.0.0/16 donde 16 es el númro de unos que hay en la mascara de subred.
 - Hexadecimal : 147.16.0.0xFFFF0000

13

Tema 2: IP

• CIDR: Classless InterDomain Routing:

- Son aquellas direcciones que no mantienen el concepto de clase y por tanto tienen una máscara que puede ser cualquier número de bits
- Intentan resolver el problema de agotamiento de direcciones con clase que se considera que es un sistema que “desperdicia” direcciones
- E.g. 147.83.128.0 255.255.255.0 (147.83.128.0 /24) la máscara tiene $8+8+8 = 24$ bits. Notar que es una clase B con máscara de clase C, aunque aquí el concepto de clase deja de existir
- Las máscaras no tienen porqué ser múltiplos de 8 bits: 147.83.128.0 /22 (máscara:255.255.252.0), en este caso los primeros 22 bits identifican al número de red teniendo 10 bits para identificar los hosts
- IANA da una dirección con una mascara y permite que los administradores de red gestionen esta dirección de red creando tantas subredes como quieran, es decir, asignando nuevas mascararas de mayor valor a la otorgada (subnetting o lo que se llama VLSM: Variable Length Subnetting Mask)

14

Tema 2: IP

• Supernetting

- Es la utilización de bloques contiguos de espacios de dirección de clase C para simular un único espacio de direcciones.
- Cuando se utiliza se usan bloques contiguos de Clases C para emular una red más grande de lo que permite la clase
- Se da una clase con una máscara menor que la de la clase
- Raramente se utiliza esta técnica
- E.g. Disponemos de las Clase C 220.220.1.0/24 a 220.220.255.0/24, asumir que la compañía usa hasta la red 100 (de la 220.220.1.0/24 a la 220.220.100.0/24). Su router de salida debería anunciar 100 redes en la tabla de encaminamiento. Pero si anuncia la 220.220.0.0/16 sólo anuncia 1.

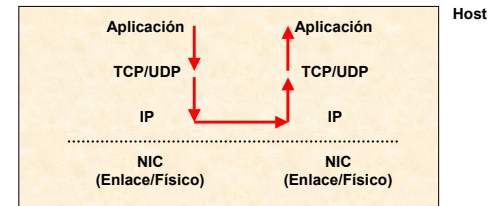
IP	Interficie	IP	Interficie
220.220.1.0	atm0	220.220.0.0	atm0
220.220.2.0	atm0		
.....			
220.220.100.0	atm0		

15

Tema 2: IP

• Interficie Loopback

- Interficie que permite comunicarse a dos procesos dentro de un mismo host
- Los datos de la aplicación bajan los niveles de transporte y de red (niveles 4 y 3) pero no llegan al nivel de enlace (nivel 2)
- En el caso de IP, la dirección IP loopback está estandarizada y es la IP = 127.0.0.1



16

Tema 2: IP

- **DHCP (Dynamic Host Configuration Protocol)**
 - Permite manejar rangos de direcciones IP de forma dinámica y automatizada.
 - DHCP está construido sobre el modelo cliente servidor, donde el servidor DHCP designado asigna direcciones de red y suministra parámetros de configuración dinámicamente a un host.
 - El formato de los mensajes DHCP está basado en el formato de mensajes BOOTP, para capturar el comportamiento del agente de transmisión BOOTP
 - El protocolo BOOTP utilizaba una estructura de tramas muy sencilla y el tráfico generado era mínimo pero su eficacia es muy baja.
 - A principios de la década de los 90, la IETF (Internet Engineering Task Force) desarrolló el protocolo DHCP (Dynamic Host Configuration Protocol). Su objetivo principal era superar las limitaciones de BOOTP, ampliándolo y permitiendo que los administradores de redes se olvidaran, casi por completo, de la asignación de direcciones IP a las decenas o centenares de PC's y otras máquinas de su organización.

Tema 2: IP

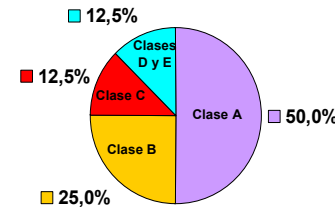
- **DHCP (Dynamic Host Configuration Protocol)**
 - DHCP se basa en el conocido modelo Cliente-Servidor.
 - Utiliza un protocolo de comunicaciones muy sencillo (basado en UDP sobre IP).
 - Los clientes de una red que utilicen este protocolo utilizan direcciones IP que les "alquila" un servidor (no tiene porqué ser local). Cada vez que un cliente se inicia, pide una dirección IP o una renovación de la que tiene alquilada actualmente.
 - El cliente recibe, junto con la dirección, algunos parámetros adicionales:
 - pasarela (gateway) por defecto,
 - servidor WINS,
 - servidor DNS, etc...
 - Lo que DHCP consigue es que la asignación y liberación de las direcciones IP en una red sea dinámica y automática

Tema 2: IP

- **DHCP (Dynamic Host Configuration Protocol)**
 - DHCP soporta tres mecanismos para la asignación de direcciones:
 - **Asignación automática:** en la cual DHCP asigna una dirección IP permanente a un cliente.
 - **Asignación dinámica:** DHCP asigna una dirección IP a un cliente por período de tiempo específico, o un período de tiempo especificado por el cliente. Este mecanismo es el único de los tres que permite automáticamente re usar direcciones que no están siendo más necesitadas por un cliente al cual fue asignada, por lo tanto este mecanismo es útil para asignar una dirección a un cliente que estará temporalmente conectado a la red o para compartir un grupo limitado de direcciones IP de un conjunto de clientes que no necesitan direcciones IP permanentes.
 - **Asignación Manual:** La dirección IP de un cliente es asignado por el administrador de la red y DHCP solo es utilizado para transmitir la dirección asignada al cliente. Este mecanismo es usado para corregir errores en redes que por alguna razón no usan DHCP.

Tema 2: IP

- **IPv6**
 - Crisis en el esquema de direcciones de IPv4
 - Clases A y B: suponen un 75 % de las direcciones pero sólo permiten 17000 organizaciones
 - Clases C permiten más organizaciones pero pocos hosts por red (254 hosts)
 - El hecho de que haya más clases A, B o C no mejora la situación (demasiadas direcciones en las tablas de routing)



Tema 2: IP

- **IPv6**
 - Debido a la falta de direcciones IP es necesario encontrar soluciones
 - **Subnetting**: mejora la distribución de direcciones pero no soluciona el problema a corto plazo
 - **VLSM (Variable-Length Subnet Masks)**: significa "subnetting a subnet", sucede lo mismo que el punto anterior
 - **CIDR (Classless Inter-Domain Routing)**:
 - Eliminar el concepto de clases y mejora la agregación de rutas para una mejor eficiencia del encaminamiento (CPU y memoria en los routers)
 - Supernetting: consiste en asignar bloques contiguos de direcciones C a una única red siguiendo criterios geográficos
 - **IP privadas + NAT (Network Address Translation)**: usar direcciones privadas y efectuar una translación de direcciones privadas a públicas (solución provisional o a corto plazo)

Tema 2: IP

- **IPv6:**
 - Compatibles con IPv4
 - Direcciones de 128 bits
 - Las opciones se envían en la cabecera como una extensión. La cabecera tiene un campo ("next header") que indica cual es la siguiente cabecera (una opción, o un protocolo de transporte,)
 - Las direcciones IP se detectan automáticamente (no tienen que ser asignadas por el administrador de sistema). Cuando se conecta el host, se configuran las direcciones "link local" y "global scope"
 - Incorpora mecanismos de seguridad informática (IPsec) que permiten autenticar y encriptar la información, que también se pueden utilizar en IPv4
 - Define el concepto de flujo (secuencia de datagramas IPv6) para permitir QoS en comunicaciones en tiempo real, que también se pueden utilizar en IPv4

Tema 2: IP

- **IPv6:**
 - Direcciones de 128 bits expresadas en Hex organizados en grupos de 8 words de 16-bits

1080:0000:0000:0000:0008:0080:1AF0:453D
 1080:0:0:0:8:80:1AF0:453D
 1080::8:80:1AF0:453D

- Una dirección IPv6 incluye 3 niveles jerárquicos

Bits 3 13 8 24 16 64

FP	TLA Id	Resv	NLA Id	SLA Id	Interf Id
Public Topology				Site Topology	Interface Identifier

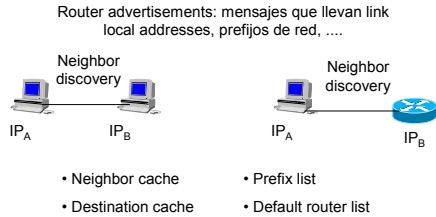
Tema 2: IP

- **IPv6:**
 - Topologías jerárquicas en una dirección IPv6
 - **Topología Pública (48 bits)**: identifica a los proveedores de la conexión a Internet
 - **FP (Formal Prefix)**: identifica si la IPv6 es unicast, anycast o multicast
 - **TLA Id (Top-Level Aggregation)**: identifica a la autoridad de mayor nivel dentro de la jerarquía de encaminamiento
 - **Res**: Reservado para futuras expansiones de las direcciones
 - **NLA Id (Next-Level Aggregation)**: identifica ISP
 - **Topología de la Organización (16 bits)**: identifica a la organización a la que pertenece el nodo IP
 - **SLA Id (Site Level Aggregation)**: permite a una organización crear su propia jerarquía de direcciones
 - **Identificador de la interficie (64 Bits)**: identifica inequívocamente a un nodo. Notar que coincide con los bits de una dirección típica MAC

Tema 2: IP

Neighbor Discovery for IPv6

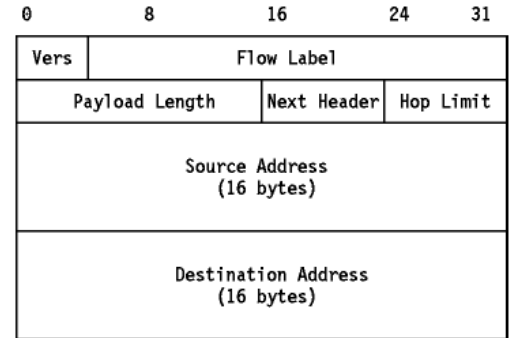
- Proceso por el cual un host IPv6 descubre automáticamente su dirección IP. Tipos de direcciones:
 - Link local: direcciones que se usan en aquellas interfaces que no están conectadas a ningún router
 - Global scope: direcciones que se usan en aquellas interfaces que están conectadas a un router



Tema 2: IP

Formato del datagrama IPv6

- Incrementa la longitud de la cabecera IP de 20 bytes a 40 bytes



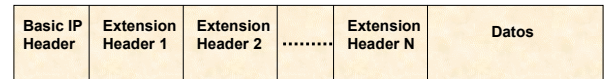
Tema 2: IP

IPv6:

- Por ejemplo la cabecera básica contendría las direcciones IPv6 y campos típicos de IPv6
 - version
 - flow label: tipo de manipulación de los paquetes, control o no de flujo, tipo de tráfico
 - payload length
 - Next header: tipo de cabecera
 - Hop limit (TTL o tiempo de vida): que se mide en saltos ya que hay más de un salto por segundo.
 - , ...)
- El campo DATOS contendría las cabeceras de extensión:
 - La información para autenticar el datagrama (Protocolo AH)
 - La información para encriptar los datos (Protocolo ESP)
 - Información relacionada con un terminal móvil
 - La cabecera TCP ya que el resto del campo DATOS son un segmento TCP
 -

Tema 2: IP

Extensiones básicas de cabecera (IPv6 Extension Headers) (EH)



(NO se puede alterar el orden de las opciones)

- Hop-by-hop Options Header
- Destination Options Header (1)
- Routing Header
- Fragment Header
- Authentication Header (AH protocol)
- Encapsulating Security Payload Header (ESP protocol)
- Destination Options Header (2)
- Upper Layer Header (e.g.; TCP, UDP,)

Tema 2: IP

- **Gestión en la asignación de IP**
 - ICANN se encarga de asignar IP o bloques de IP
 - RFCs relevantes:
 - RFC 2050: Internet Registry IP Allocation Guidelines
 - RFC 1918: Address Allocation for private Internets
 - RFC 1518: An Architecture for IP Address Allocation with CIDR
 - Distinción entre Reserva de bloques de IP (para ISPs que lo soliciten) y Asignación de bloques de IP (los ISPs asignan a sus clientes bloques de IP)

Tema 2: IP

- **Gestión en la asignación de IP**
 - Jerarquía de organizaciones de registro (**Internet Registry: IR**)
 - Nodo Raíz: IANA
 - Debajo: **IRs regionales** atendiendo a diversas zonas del mundo
 - **RIPE NCC** (Reseau IP Europeens) <http://www.ripe.net>
 - **1600 IRs locales**
 - Mantiene Base Datos con las redes Europeas
 - **APNIC** (Asia-Pacific Network Information Center) <http://www.apnic.net>
 - **ARIN** (American Registry for Internet Numbers) <http://www.arin.net>
 - **IRs locales (LIRs)**: establecidos bajo el consentimiento de los regionales que delegan ciertas tareas en ellos
 - Hay cierta componente geográfica en la reserva de IP
 - Las ISPs solicitan a sus IRs regionales la reserva de bloques de IP. Condiciones:
 - Conectado a un nodo neutro
 - Conectado a Internet a través de dos conexiones

Tema 2: IP

- **Gestión en la asignación de IP**
 - Consideraciones:
 - Se recomienda que las ISPs no asignen IP estáticas a usuarios conectados vía modem
 - Asignación de bloques de IP
 - Proceso por el cual una empresa consigue que se le delegue la autoridad sobre un bloque determinado de direcciones, de forma que es ella quien establece el reparto de tales direcciones entre sus máquinas
 - No puede subdelegar la autoridad sobre estas direcciones
 - Empresas que requieren mucho espacio de IP deberían contactar directamente con la IR regional
 - En caso contrario deben contactar con algún ISP y solicitar un bloque de IP
 - Asignación de IP por RIPE
 - Ver <http://www.ripe.net/ripe/docs/ir-policies-procedures.html> doc RIPE-185: "European Internet Registry Policies and Procedures"

Tema 2: IP

- **Detección de errores en IP:**
 - Checksum en la cabecera de cada datagrama IP
 - Los datos están protegidos por otro checksum que se aplica en el nivel de transporte (sobre todo el segmento TCP o datagrama UDP)
 - El checksum SOLO protege la cabecera IP
 - Acción si error detectado: descarta la trama y envía un mensaje ICMP al origen
 - Checksum (es software) = $\sum \text{Words}_i$
 - Alinear en palabras de 16 bits
 - Inicializar el checksum a 0
 - Sumar palabras de la cabecera en complemento a 1s
 - Calcular el complemento a 1 del resultado
 - Rellenar el campo del checksum con el valor calculado
 - Se tiene que recalcularse cada vez que se atraviesa un router (ya que hay campos de la cabecera que son mutables, e.g. TTL)

Tema 2: IP

Detección de errores en IP:

- E.g. Checksum de una cabecera:
a% tcpdump -x -s 512 -i eth0

```
45 10
05 dc
64 78
00 00
40 06
00 00
93 53
23 50
93 53
23 51
```

Si añadimos el checksum, la suma dará 0

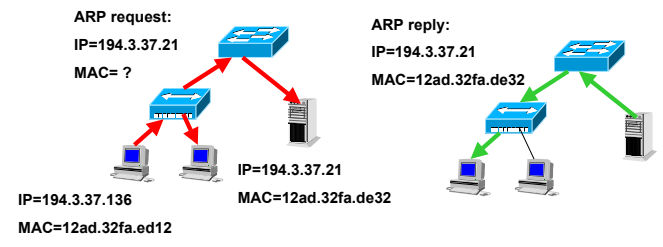
- **Version:** 4 (0x04)
- **Hdr Length:** 20 bytes (0x05)
- **TOS:** (0x10)
- **Total length:** 1500 bytes (0x05dc)
- **Ident:** (0x6478)
- **Flags:** 000 (3 bits)
- **offset:** 0 (13 bits)
- **TTL:** 64 (0x40)
- **Protocolo:** el 6 es TCP (0x06)
- **Hdr checksum:** (0x0000)
- **IPorg:** 147.83.35.80 (0x9353 2350)
- **IPdest:** 147.83.35.81 (0x9353 2351)

2 5c b1 → acumular el 2 y hacer complemento a 1
5c b3 → checksum = a3 4c

Tema 2: IP

• ARP (Address Resolution Protocol) (RFC 826)

- Protocolo de capa 3
- ARP permite que un terminal encuentre la dirección MAC de otro terminal que esta asociada a una dirección IP
- Se encarga de mapear IP con MAC
- Host A envía una trama broadcast a la subred, el servidor responde con la respuesta



Tema 2: IP

• ARP (Address Resolution Protocol)

- ARP cache: tabla que mantiene cada dispositivo con los mapeos más recientes entre IP y MAC
- Recordar que las IP son dinámicas y pueden cambiar, en cambio las direcciones físicas son permanentes a las tarjetas
- En UNIX: se puede usar el comando arp -a para obtener el contenido de la tabla ARP
- En Windows la utilidad winipcfg.exe muestra las direcciones MAC en uso por parte del PC
- La duración de una entrada es de 20 minutos

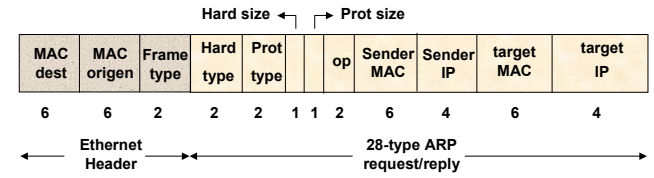
- **arp [-vn] [-H type] [-i if] -a [hostname]**
- **aucanada% arp -a**

```
teix.ac.upc.es (147.83.35.110) at 00:20:E1:10:4f:34 [ether] on eth0
arenys5.ac.upc.es (147.83.35.2) at 00:10:F8:B3:E4:00 [ether] on eth0
```

Tema 2: IP

• Formato del paquete ARP

- Usa tramas de nivel 2 (e.g. Ethernet)



MAC dest = broadcast
Frame type = 0x0806 (ARP)

Hard type = ethernet
Prot type = IP
Hard/prot size in bytes
Op: (1) ARP request, (2) ARP reply, (3) RARP request, (4) RARP reply

Tema 2: IP

- **Otras redes que no sean Broadcast:**

- Actualmente la mayoría de las grandes redes están basadas en ATM.
- ATM es una WAN que usa distintas arquitecturas de las de las LAN estándar.
- Como es una WAN el concepto de broadcast no existe, las conexiones son punto a punto (unicast) o punto a multipunto (multicast)
- No se puede hacer un ARP request (broadcast)
- Solución:
 - Usar servidores dedicados, LIS (Logical IP Subnetwork), que sean capaces de resolver IP con direcciones ATM (formato distinto a una dirección MAC Ethernet)
 - El host se comunica con este servidor dedicado (uno por subred) que le devuelve la dirección ATM de la IP que le interesa
 - El host puede establecer un Circuito Virtual (VC) con el destino
 - A esta técnica se le llama ATMARP definida en la RFC 1577.

Tema 2: IP

- **ARP**

- ¿Qué ocurre si el host buscado no existe?
 - Se reintenta porque TCP reintenta la conexión varias veces hasta que salte su Timeout (ver tema 3WHS de TCP)
- Proxy ARP
 - Permite que un router conteste por el host destino. El host origen "piensa" que está hablando directamente con el destino pero es el router el que está enviando la respuesta ARP.
 - CUIDADO !!! Normalmente los hosts se comunican con el router porque su tabla de encaminamiento se lo indica, y no por Proxy ARP
- Gratuitous ARP
 - Un host hace un ARP request para averiguar su propia IP
 - Para qué?
 - Para saber si otro host tiene configurada la misma IP
 - Hacer un update de ARP caches cuando cambias tu @Física

Tema 2: IP

- **RARP (Reverse ARP)**

- Cálculo de direcciones inversas del mismo modo que en ARP
- Averigua IP a partir de una dirección MAC destino
- Permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red.
- Los dispositivos que usan RARP necesitan un servidor RARP en la red que responda a sus peticiones.
- Se usa en Xterminals o Diskless workstations (no tienen IP originalmente) pero saben su dirección MAC
- Funciona igual que ARP pero con "frame type = 0x8035" y "op= 3 (request), 4 (reply)"
- En el caso de que haya múltiples servidores RARP en la red, el cliente RARP solo hará uso de la primera respuesta RARP que reciba de su broadcast