

# IP

## Internet Protocol

---

### Funcionalidades:

Permite la interconexión de redes heterogéneas mediante un esquema de direccionamiento apropiado y funciones de fragmentación de datos y ruteo de mensajes.

- Esquema global de direcciones
- Fragmentación / reensamblado
- Ruteo



# IP

## Dirección IP

---

### Direccionamiento IP

La dirección Internet (o dirección IP) está codificada en 32 bits (4 bytes).



Dotted Decimal Notation.

Ej: 211.15.24.143



# IP

## Clases de direcciones IP

- La dirección IP se descompone en un "Network number" y un "Host number".
- Las direcciones se dividen en "**clases**" en función del byte mas significativo.

	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
<b>A</b>	0	<b>Network bits</b>								<b>Host bits</b>																						
<b>B</b>	1	0	<b>Network bits</b>										<b>Host bits</b>																			
<b>C</b>	1	1	0	<b>Network bits</b>														<b>Host bits</b>														
<b>D</b>	1	1	1	0	<b>Multicast group</b>																											
<b>E</b>	1	1	1	1	0	<b>Reserved</b>																										

# IP

## Direccionamiento IP

---

Las direcciones de "**broadcast**" permiten la difusión de datagramas a todos los hosts de una misma red

Broadcast	Todos los bits de Host # en 1	Datagrama destinado a todos los host de la red
Red	Todos los bits de Host # en 0	Dirección que identifica la red
Red Loopback	127.0.0.0	
Loopback	127.0.0.1	

# IP

## Direccionamiento IP

---

- Direccionamiento Classful

- Definición del Net Number en función de la clase.
- Esquema poco flexible, ej.:
  - Necesidad de definir una nueva red debido a la utilización de otra tecnología de capa 2
  - Crecimiento de la cantidad de hosts de la red
  - Crecimiento de la red en distancia (nuevas sucursales)

- Subnetting

- Particionamiento del espacio de direcciones de una red en subredes del mismo tamaño.
- La dirección IP se particiona en: **Net# - SubNet# - Host#**

# IP

## Direccionamiento IP

---

- Direccionamiento ClassLess

- Utilización de la Máscara de Red (NETMASK)
- Definición del Net Number en función de la máscara
- Distinto tamaño de red para cada subred según las necesidades
- Redefinición del algoritmo de ruteo (CIDR)
- Utilización mas eficiente del espacio de direcciones
- Sumarización de redes



# IP

## Direccionamiento IP

**Mascara de red =**  
4 octetos binarios

**Dirección de red =**  
Dirección IP & Máscara  
de red.

### Ejemplo de planeamiento de subred clase C

Dirección IP de host: 192.168.5.121  
Máscara de subred: 255.255.255.248



- Dirección de subred = 192.168.5.120
- Dirección de host = 192.168.5.121 - 192.168.5.126
- Dirección de broadcast = 192.168.5.127
- Cinco bits de subredes

# IP

## IP Header

Header de IP: 20 bytes mínimo

0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
<b>Version</b>				<b>Header Length</b>				<b>TOS</b>								<b>Total length</b>															
<b>Identification</b>												<b>Flags</b>				<b>Fragment offset</b>															
<b>TTL</b>				<b>Protocol</b>								<b>Header checksum</b>																			
<b>Source IP address</b>																															
<b>Destination IP address</b>																															
<b>Options and padding :::</b>																															

# IP

## IP Header

---

<b>Campo</b>	<b>Longitud</b>	<b>Observación</b>
version	4 bits	Versión de IP (4)
header length	4 bits	Longitud del header en 32bits words
type of service	1byte	
total length	2 bytes	Tamaño total del datagrama IP
identifier	2 bytes	Para el reensamblado de los paquetes fragmentados
reserved	1bit	
don't fragment	1bit	en 0 puede ser fragmentado
more fragments	1bit	1: más fragmentos; 0: último fragmento.
fragment offset	13bits	Orden de los fragmentos
time to live	1byte	Especificado en <i>hops</i> , cada router decrementa este valor y al llegar a 0 es descartado

# IP

## IP Header

---

<b>Campo</b>	<b>Longitud</b>	<b>Observación</b>
protocol	1byte	IP=0, ICMP=1, TCP=6, UDP=17
header checksum	2bytes	Verificación de integridad del header IP
source address	4bytes	Dirección IP origen
destination address	4bytes	Dirección IP destino
options	Variable	
padding	variable	El header tiene una longitud múltiplo de 32bits
Data	variable	

# IP

## Fragmentación / Reensamblado

---

¿Por qué fragmentar?

IP Soporta un tamaño máximo de datagrama de 64 KBytes

IP es todo terreno,

- Redes con distintas tecnologías
- Distintos MTU

¿Cuándo se fragmenta?

Se fragmenta cuando el datagrama tiene mayor longitud que el MTU de la red por la cual se debe realizar el forwarding



# IP

## Fragmentación / Reensamblado

---

### ¿Quién fragmenta?

La fragmentación puede producirse tanto:

- Host origen
- Sistema intermedio

### ¿Quién reensambla?

El reensamblado de un datagrama fragmentado se realiza **únicamente en el host de destino.**

El host de destino inicializa un **reassembly timer**. Si dicho timer expira antes que todos los fragmentos hayan sido recibidos, *descartará todos los fragmentos.*

# IP

## Fragmentación / Reensamblado

---

¿Como se fragmenta?

El proceso de fragmentación utiliza el campo de “offset” y el flag de “more fragments” del header IP.

El campo “Identifier” para diferenciar fragmentos de dos datagramas IP distintos.

Este esquema permite la fragmentación de fragmentos.

Fragmento	Offset	More Fragments Flag
Primero	0	1
Intermedio	Distinto de 0	1
Último	Distinto de 0	0

# IP

## Routing - conceptos

---

### ***“Routing”***

es el proceso de transferencia de un datagrama desde un host a otro a través de nodos intermediarios (routers o gateways).

### ***“Direct routing”***

cuando el network number de la source address coincide con el network number de la destination address.

### ***“Indirect routing”***

cuando el network number de la source address difiere del network number de la destination address.



# IP

## Routing - conceptos

---

### **Ruteo clásico**

Utilizado para Clasful Addressing y para Subneting

La dirección de red destino se obtiene a partir del primer byte de la dirección IP destino.

### **CIDR (Classless Inter Domain Routing)**

Utilizado para VLSM

La dirección de red se obtiene mediante la dirección IP y la máscara de red registrada para cada entrada en la tabla de ruteo.



# IP

## Routing Tables

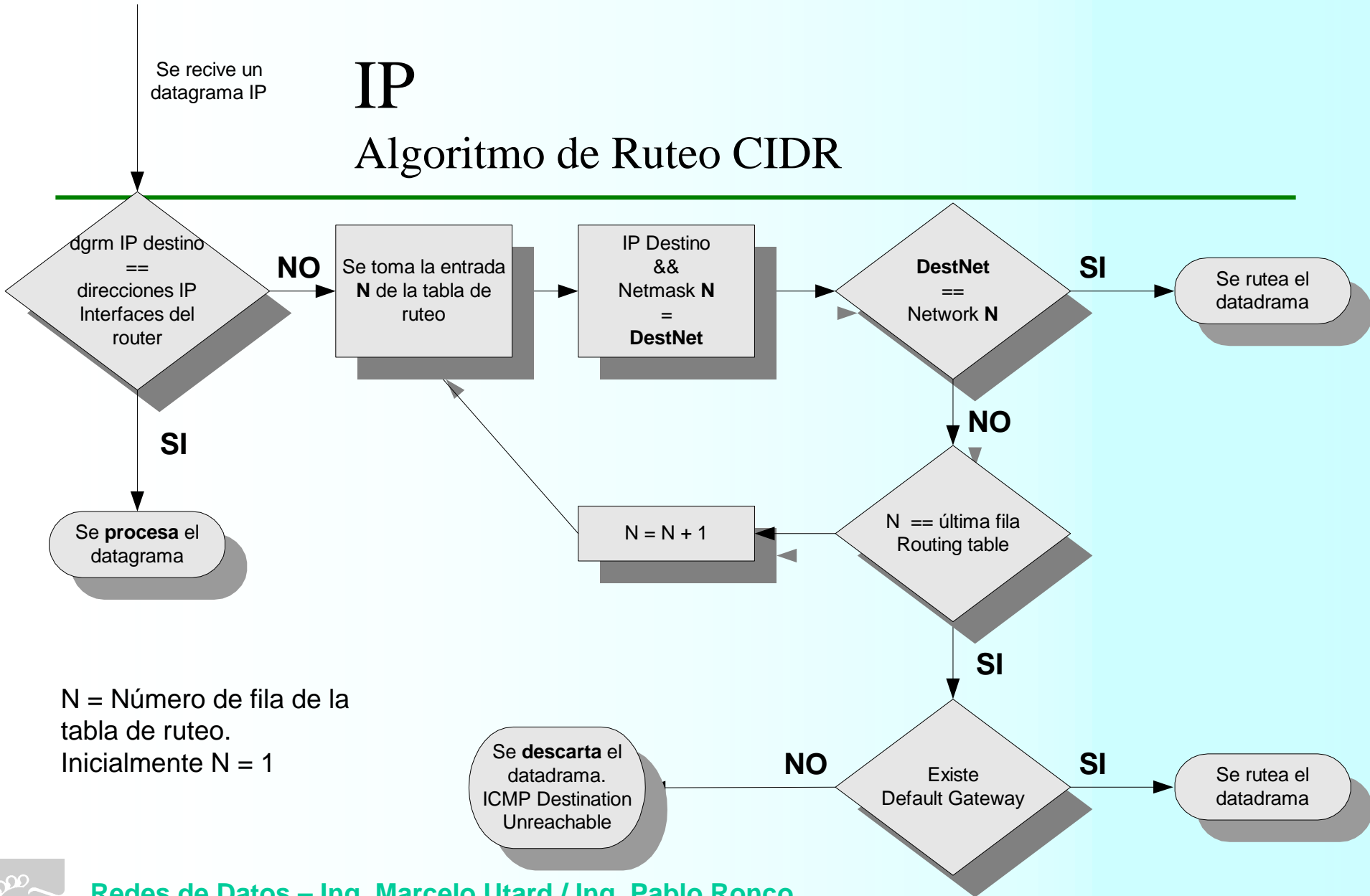
---

### Campos:

- Red
- Máscara de red
- Métrica
- Next Hop (Próximo salto) / Interfaz
- Tipo de ruta
- Entradas ordenadas
  - Se ordenan según la selectividad de la máscara de red
  - Las mas selectivas se analizan antes que las menos selectivas

# IP

## Algoritmo de Ruteo CIDR



# ARP

## Address Resolution Protocol

---

- El protocolo **ARP** (*Address Resolution Protocol*) permite establecer la dirección física correspondiente a la dirección lógica (Internet) de cada host en una red.
- Soporte de múltiples protocolos de capa 2
  - Hardware Type
  - Hardware address length

# ARP

## ARP PDU

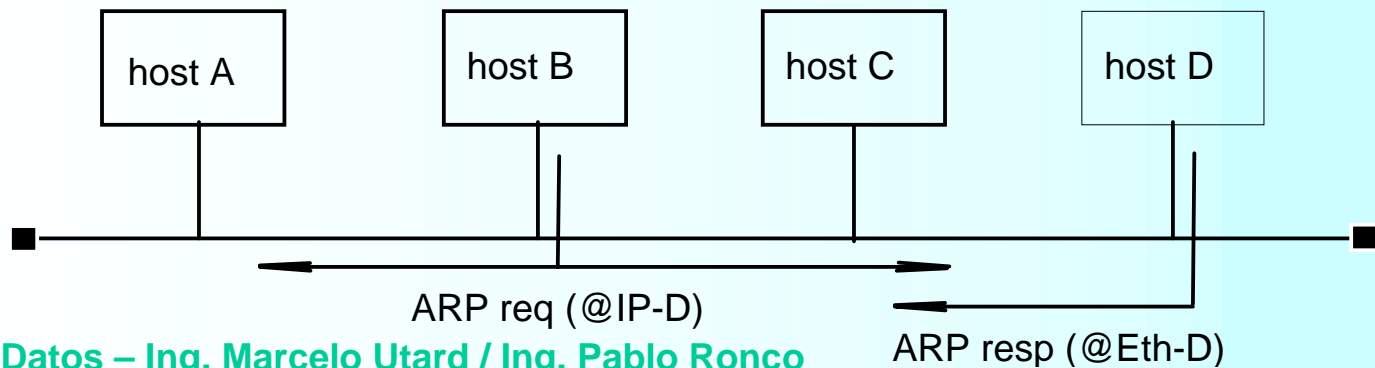
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
<b>Hardware type</b>																<b>Protocol type</b>															
<b>Hardware address length</b>						<b>Protocol address length</b>						<b>Opcode</b>																			
<b>Source hardware address :::</b>																															
<b>Source protocol address :::</b>																															
<b>Destination hardware address :::</b>																															
<b>Destination protocol address :::</b>																															
<b>Data :::</b>																															

# ARP

## Resolution Process

---

1. El hostB quiere enviar uno o más datagramas al hostD
2. El hostB conoce la dirección IP del hostD pero no la dirección Eth
3. El hostB envía un **broadcast ARP request** con la dirección IP de hostD
4. Todos los hosts de la red reciben el ARP request (sólo hostD responderá)
5. El hostD envía el **ARP response** al hostB con su dirección física Ethernet
6. El hostB actualiza su **ARP cache** temporalmente
7. El hostB envía el(los) datagrama(s)
8. Cada vez que hostB envíe un datagrama a hostD usará la tabla ARP



# ARP

## Extensiones

---

- RARP
  - Reverse Address Resolution Protocol
- Proxy ARP
  - Hosts que no soportan ARP
  - Dos redes que comparten el mismo Network Address

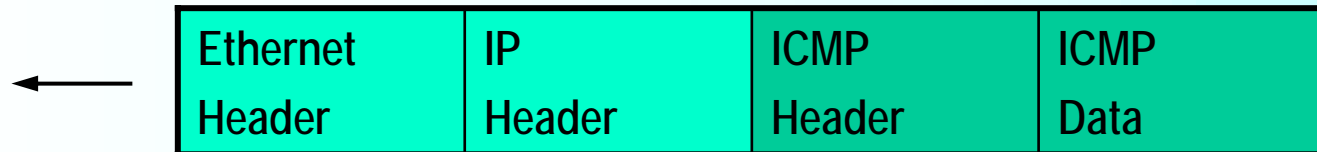


# ICMP

## Internet Control Message Protocol

---

- El Protocolo **IP** no es confiable
- El protocolo **ICMP** (*Internet Control Message Protocol*) es un mecanismo para pasar mensajes de error y de control a través de una red IP.
- **ICMP** es parte integral de IP.
- No generan mensajes nuevos **ICMP** a partir de mensajes **ICMP**
- **ICMP** sólo reporta errores al host remitente del datagrama
- El **mensaje ICMP** es encapsulado en un datagrama IP.



# ICMP

## Internet Control Message Protocol

---

Cada tipo de mensaje tiene su propio formato, pero todos tienen 3 campos en común:

- Type
- Code
- CheckSum

0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
<b>Type</b>								<b>Code</b>								<b>ICMP header checksum</b>															
<b>Data :::</b>																															

# ICMP

## Internet Control Message Protocol

---

**Tipos** de mensajes posibles:

<u>Type</u>	<u>Tipo de Mensaje</u>
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded

El comando "**ping**" envía un **ICMP\_ECHO REQUEST** y espera recibir como respuesta un **ICMP\_ECHO REPLY** antes que expire el tiempo de espera