tutoría Redes de Datos

Capítulo 3: Capa de red

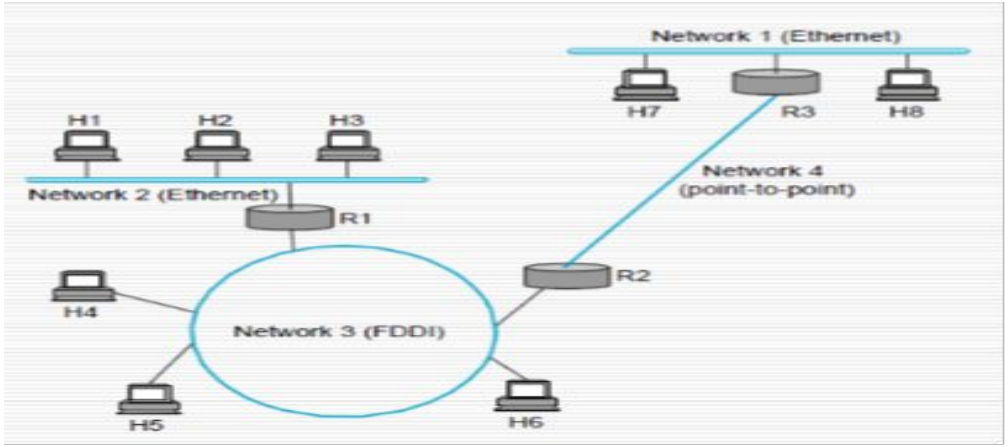
udp Escuela de Informática y Telecomunicaciones
FACULTAD DE INGENIERÍA Y CIENCIAS

Ph.D. Nicolás Boettcher

¿Para qué sirve?

El protocolo IP pretende resolver el problema de conectar diversas redes locales, que además pueden ser de diversos tipos.

A este concepto se le conoce como internet working.



No hay garantías...

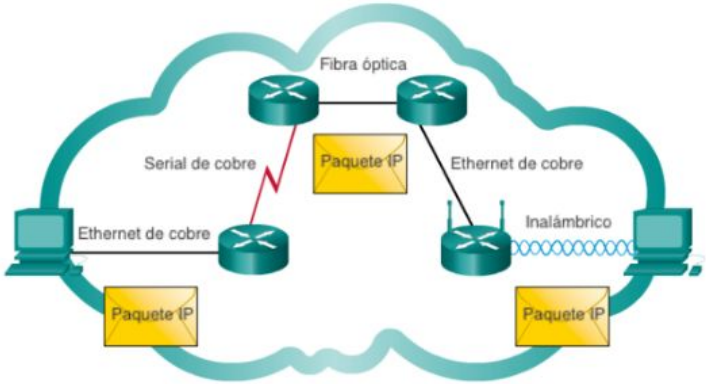
- A este esquema también se le llama orientado al mensaje (connection-less).
- Cada datagrama contiene suficiente información para permitir que la red se encargue de hacerlo llegar a destino independientemente.
- Si algo anda mal y el datagrama se pierde, corrompe, se despacha a otro lugar y cualquier otra cosa, la red no hace nada para corregirlo. Esto lo convierte en un servicio no confiable.

¿Por qué no hacerlo confiable?

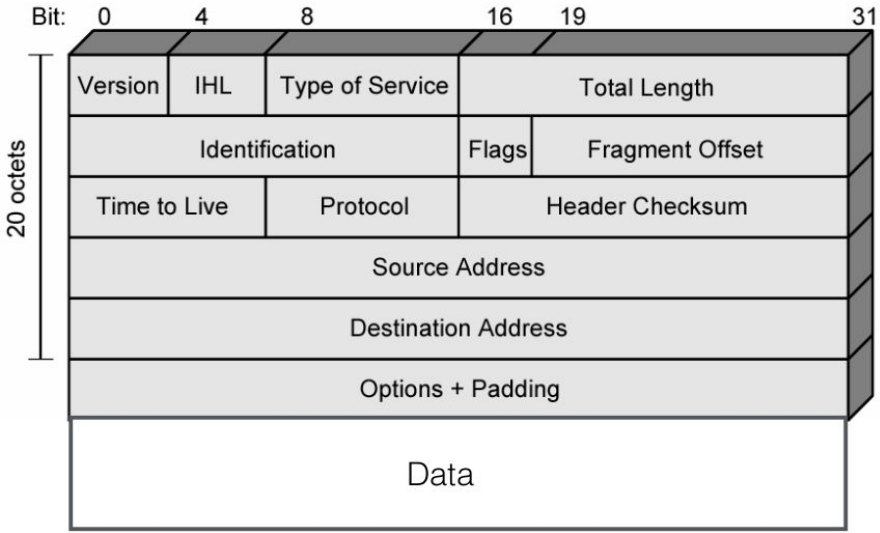
- Si se ofrece un servicio confiable sobre una red no confiable, es necesario colocar mucha inteligencia en los componentes para sobrellevar el problema.
- Hacer que los routers sean simples es uno de los objetivos iniciales de IP.
- La idea de “mejor esfuerzo” no sólo implica a veces que los datagramas se pierdan, sino que lleguen desordenados o duplicados. Se espera que las capas superiores se encarguen de dichas circunstancias.
- La habilidad de funcionar sobre cualquier cosa es otra de las fortalezas de IP.

Relación con L2

- IP funciona independiente del medio de comunicación.
- Capa de enlace de datos se encarga de prepararlo para su transmisión en la red.
- Hay una restricción! el tamaño máximo del paquete a transmitir.



Datagrama IP




```
Internet Protocol Version 4, Src: 192.168.1.129, Dst:
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN:
    Total Length: 68
    Identification: 0x1aca (6858)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  ▸ Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0xf841 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.129
    Destination Address: 192.112.36.4
```

```
0000  e4 ab 89 bb 06 a8 dc 21  48 24 f8 56 08 00 45 00
0010  00 44 1a ca 00 00 01 11  f8 41 c0 a8 01 81 c0 70
0020  24 04 50 0b 82 a0 00 30  a6 df 09 33 68 74 74 70
```

Fragmented ICMP packet

No.	Time	Source	Destination	Protocol	Length	Info
137	15.943…	192.168.31.178	1.1.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0,
138	15.943…	192.168.31.178	1.1.1.1	ICMP	35	Echo (ping) request id=0x0001, seq=1/256, t
139	15.954…	1.1.1.1	192.168.31.178	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0,
140	15.954…	1.1.1.1	192.168.31.178	ICMP	60	Echo (ping) reply id=0x0001, seq=1/256, t

```
▾ Internet Protocol Version 4, Src: 1.1.1.1, Dst: 192.168.31.178
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 21
    Identification: 0x7845 (30789)
  ▸ Flags: 0x00
    ...0 0101 1100 1000 = Fragment Offset: 1480
    Time to Live: 55
    Protocol: ICMP (1)
    Header Checksum: 0x288e [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 1.1.1.1
    Destination Address: 192.168.31.178
  ▾ [2 IPv4 Fragments (1481 bytes): #139(1480), #140(1)]
      [Frame: 139, payload: 0-1479 (1480 bytes)]
      [Frame: 140, payload: 1480-1480 (1 byte)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1481]
      [Reassembled IPv4 data: 0000bf46000100017ad58165000000003359
```

```
[redacted] ping -c 1 -s 1473 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 1473(1501) bytes of data.
1481 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=25.1 ms

--- 1.1.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 25.114/25.114/25.114/0.000 ms
```

Encuentre 2 inconsistencias!

Maximum Transmission Unit (MTU)

Source	Destination	Protocol	Length	Info
192.168.31.178	1.1.1.1	ICMP	35	Echo (ping) request id=0x0002, seq=1/256, ttl=64
1.1.1.1	192.168.31.178	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=c8
1.1.1.1	192.168.31.178	ICMP	60	Echo (ping) reply id=0x0002, seq=1/256, ttl=55
192.168.31.178	1.1.1.1	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=27
192.168.31.178	1.1.1.1	ICMP	60	Echo (ping) request id=0x0003, seq=1/256, ttl=64
1.1.1.1	192.168.31.178	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d8
1.1.1.1	192.168.31.178	ICMP	60	Echo (ping) reply id=0x0003, seq=1/256, ttl=55

ping -s 1473 vs ping -s 1498

Jumbo Packets

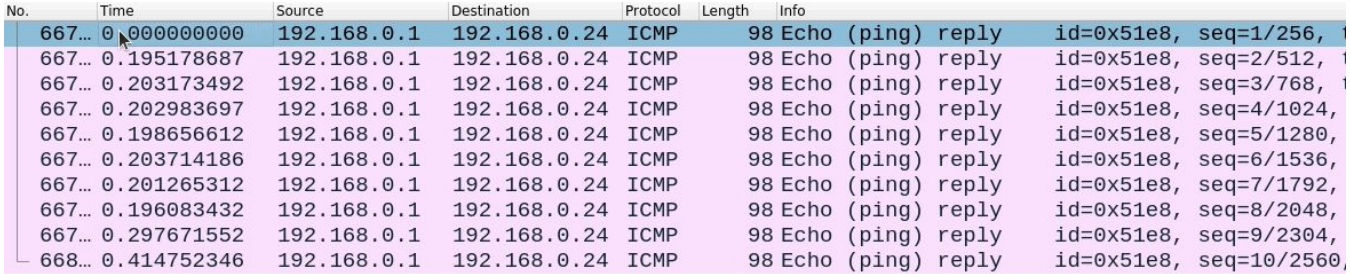
```
~ ifconfig lo
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
```

No.	Time	Source	Destination	Protocol	Length	Info
1154	0.00006…	127.0.0.1	127.0.0.1	TCP	65549	8000 → 59290
1155	0.00001…	127.0.0.1	127.0.0.1	TCP	66	59290 → 8000
1156	0.00000…	127.0.0.1	127.0.0.1	TCP	119	8000 → 59290
1157	0.00006…	127.0.0.1	127.0.0.1	TCP	65549	8000 → 59290

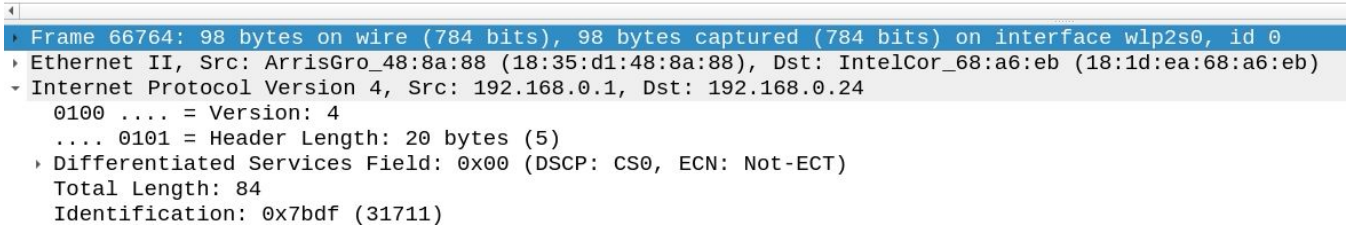
```
▸ Frame 1154: 65549 bytes on wire (524392 bits), 65549 bytes ca
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst
▾ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x02 (DSCP: CS0, ECN: ECT(0)
      0000 00.. = Differentiated Services Codepoint: Default (0
      .... ..10 = Explicit Congestion Notification: ECN-Capable
    Total Length: 65535
    Identification: 0x8946 (35142)
  ▸ Flags: 0x4000, Don't fragment
```

Estructura Datagrama IP

Identification: contiene el número del datagrama el cual identifica el fragmento para su reconstrucción.



No.	Time	Source	Destination	Protocol	Length	Info
667…	0.000000000	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=1/256,
667…	0.195178687	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=2/512,
667…	0.203173492	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=3/768,
667…	0.202983697	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=4/1024,
667…	0.198656612	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=5/1280,
667…	0.203714186	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=6/1536,
667…	0.201265312	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=7/1792,
667…	0.196083432	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=8/2048,
667…	0.297671552	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=9/2304,
668…	0.414752346	192.168.0.1	192.168.0.24	ICMP	98	Echo (ping) reply id=0x51e8, seq=10/2560,



```
Frame 66764: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0
Ethernet II, Src: ArrisGro_48:8a:88 (18:35:d1:48:8a:88), Dst: IntelCor_68:a6:eb (18:1d:ea:68:a6:eb)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x7bdf (31711)
```

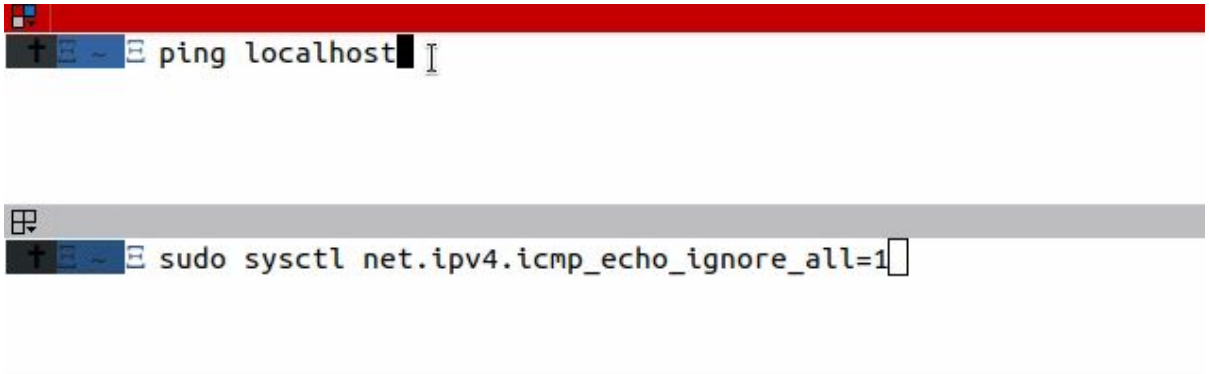
ICMP Broadcast

Source	Destination	Indentification	TTL	Protocol	Length	Info
192.168.1.129	192.168.1.255	0x0000 (0)	64	ICMP	98	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (no response found!)
192.168.1.181	192.168.1.129	0x27fd (10237)	64	ICMP	98	Echo (ping) reply id=0x0002, seq=1/256, ttl=64

Source	Destination	Indentification	TTL	Protocol	Length	Info
192.168.1.129	255.255.255.255	0x0000 (0)	64	ICMP	98	Echo (ping) request id=0x0003, seq=1/256, ttl=64 (broadcast)
192.168.1.181	192.168.1.129	0xb936 (47414)	64	ICMP	98	Echo (ping) reply id=0x0003, seq=1/256, ttl=64

```
[redacted] ping -b 192.168.1.255
WARNING: pinging broadcast address
PING 192.168.1.255 (192.168.1.255) 56(84) bytes of data.
64 bytes from 192.168.1.181: icmp_seq=1 ttl=64 time=20.8 ms
64 bytes from 192.168.1.181: icmp_seq=2 ttl=64 time=13.8 ms
```

Disable/Enable ICMP reply



¿Qué ventajas tiene segmentar?

- Eficiencia
  - Un segmento IP requiere estar en el mismo dominio de broadcast.
  - Si tenemos muchos nodos en el mismo segmento, aumentamos las posibilidades de colisión y disminuimos el rendimiento.
- Seguridad
  - Podemos aplicar reglas o filtros de tráfico entre segmentos IP.
- Administración
  - Definimos segmentos IP en base a funciones, que requieren tipos de servicio diferentes.
  - Cada red IP puede recibir un tratamiento diferente, distintos servicios, etc.

IPs para una LAN

- IANA define un bloque de IPs reservados que permiten a las organizaciones su utilización en redes privadas sin solicitud alguna.
- Estos bloques reservados se les conoce como **direcciones privadas**, pues está prohibido su uso en redes públicas como Internet.

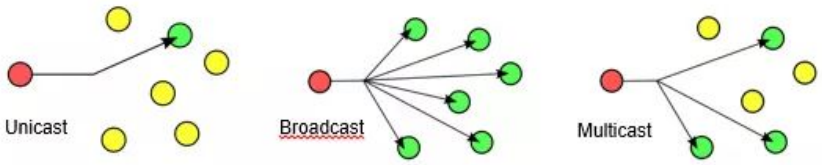
Podríamos decir que las frecuencias de libre uso del espacio radioeléctrico son una analogía a las ips privadas dentro del espacio de la totalidad de las ips.

	Octeto	Octeto	Octeto	Octeto
Binario	11000000	00000101	00100010	00001011
Decimal	192	5	34	11

Públicas vs Privadas

- **Direcciones IP públicas:** Son visibles en todo Internet. Un nodo con una IP pública es accesible (visible) desde cualquier otro nodo conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas):** Son visibles únicamente por otros nodos de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los nodos con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública.

Clases de direcciones IPs



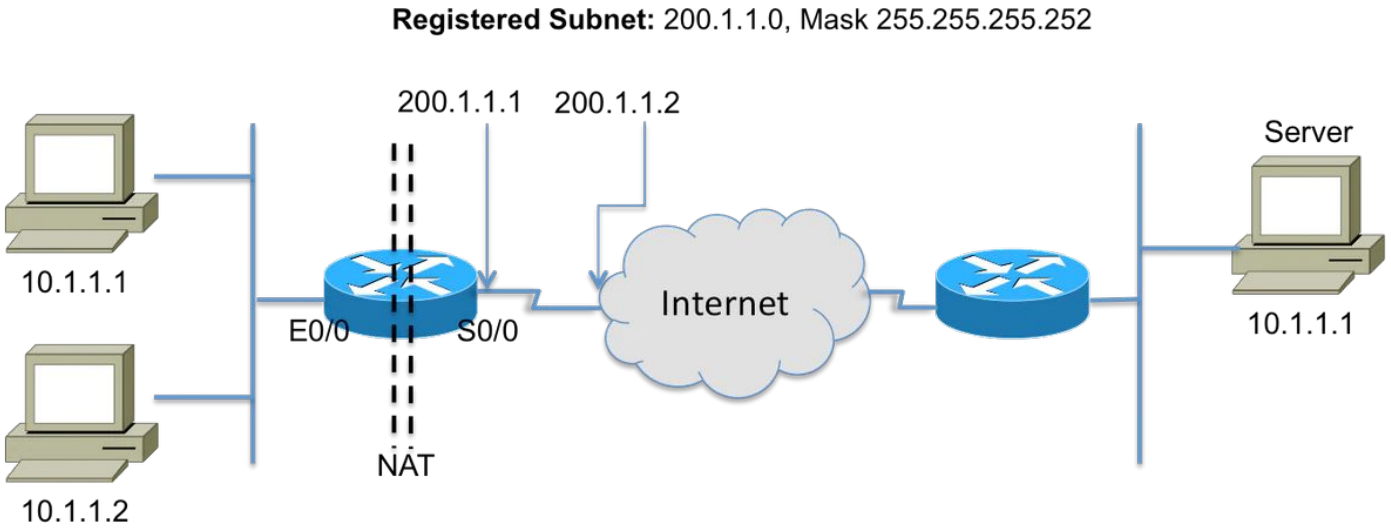
Red o rango	Uso
127.0.0.0	Reservado (fin clase A)
128.0.0.0	Reservado (ppio. clase B)
191.255.0.0	Reservado (fin clase B)
192.0.0.0	Reservado (ppio. clase C)
224.0.0.0	Reservado (ppio. clase D)
240.0.0.0 – 255.255.255.254	Reservado (clase E)
10.0.0.0	Privado clase A
172.16.0.0 – 172.31.0.0	Privado clase B
192.168.0.0 – 192.168.255.0	Privado clase C

```
curl ifconfig.me/ip
186.156.125.25%
ifconfig wlp2s0
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.24  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::49e7:4e54:dfa:4014  prefixlen 64  scopeid 0x20<link>
        ether 18:1d:ea:68:a6:eb  txqueuelen 1000  (Ethernet)
        RX packets 285150  bytes 303044989 (303.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 152143  bytes 41931840 (41.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

NAT: Network Address Translation

- Solución para la escasez de IPs
- ISP asigna 1 IP para cada hogar o empresa (o un número pequeño de estas)
- Dentro de la red, cada equipo tiene un IP único perteneciente a la red privada
- Para lograr comunicar con el resto de las redes, se realiza un proceso de traducción entre las IP privadas a la IP pública

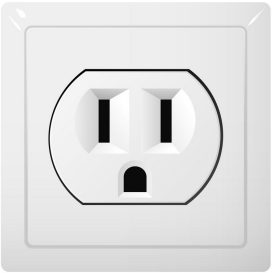
Dynamic NAT



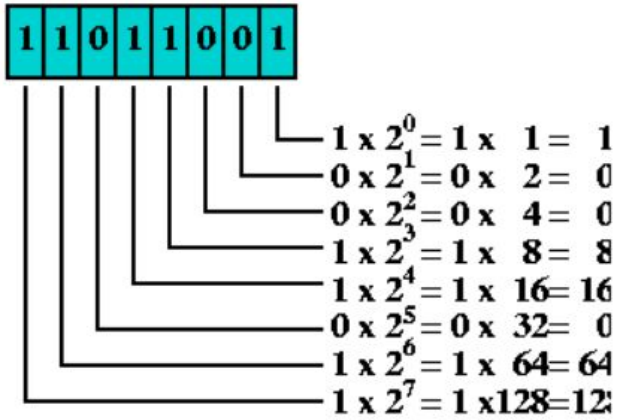
Inside Local	Inside Global
10.1.1.1:3212	200.1.1.1:3212
10.1.1.1:3213	200.1.1.1:3213
10.1.1.2:38913	200.1.1.1:38913

Inside

Outside



Binario & decimal



$$1 + 8 + 16 + 64 + 128 = 217$$

Decimal number 225

Division	Quotient	Remainder	
225 / 2	112	1	← LSB
112 / 2	56	0	
56 / 2	28	0	
28 / 2	14	0	
14 / 2	7	0	
7 / 2	3	1	
3 / 2	1	1	
1 / 2	0	1	

Binary number 1 1 1 0 0 0 0 1

Decimal number 8

Division	Quotient	Remainder	
8 / 2	4	0	← LSB
4 / 2	2	0	
2 / 2	1	0	
1 / 2	0	1	
		0	
		0	
		0	
		0	

Binary number 0 0 0 0 1 0 0 0

Decimal number 77

Division	Quotient	Remainder	
77 / 2	38	1	← LSB
38 / 2	19	0	
19 / 2	9	1	
9 / 2	4	1	
4 / 2	2	0	
2 / 2	1	0	
1 / 2	0	1	
		0	

Binary number 0 1 0 0 1 1 0 1

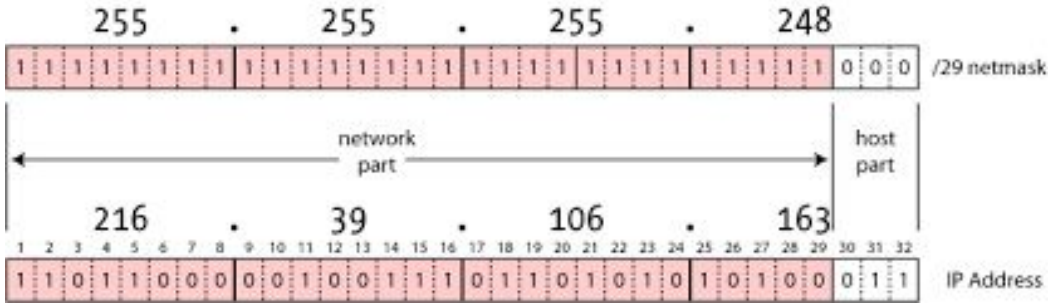
Decimal number 254

Division	Quotient	Remainder	
254 / 2	127	0	← LSB
127 / 2	63	1	
63 / 2	31	1	
31 / 2	15	1	
15 / 2	7	1	
7 / 2	3	1	
3 / 2	1	1	
1 / 2	0	1	

Binary number 1 1 1 1 1 1 1 0

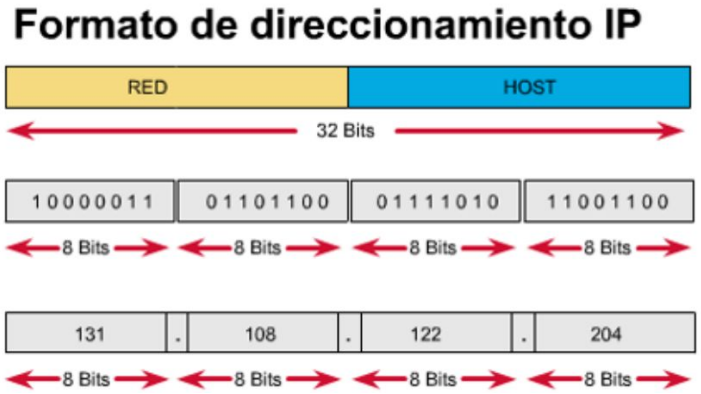
Máscara de red

- Está compuesta por una secuencia de 1s y 0s
- Permite conocer rangos de IPs
- Al hacer un AND con una dirección IP de una red, permite obtener la IP inicial y final de la red.



Prefijo

- Formado por IP/Mask
- Tamaño del prefijo no puede ser calculado solo con la IP
- IP + tamaño: 131.108.0.0 / 16, se debe enviar el tamaño igualmente
- Subnet Mask → 16 representa número de 1’s incluidos en la máscara
- IP AND Mask → Parte que representa la red



Ventajas del esquema jerárquico

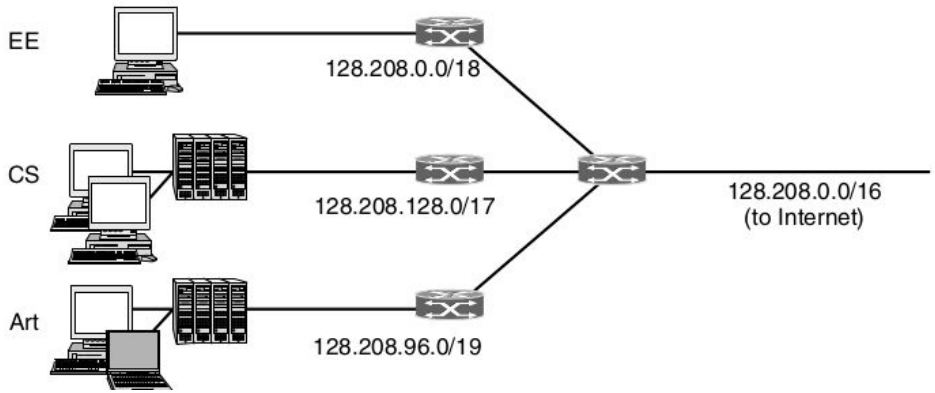
- Solo utiliza la parte de red para “rutear” paquetes disminuyendo los tamaños de las tablas de los routers
- Cuando llega a la red de destino, se utiliza la información del host para entregar el paquete
- Tamaño tablas del orden de 300.000 prefijos, con Internet actual, lo cual le permite escalar

Desventajas del esquema jerárquico

- Uso ineficiente de las IPs a menos que haya una cuidadosa administración
- Si se asignan bloques de direcciones muy grandes pueden quedar muchos IPs sin uso
- Con el crecimiento de internet las IPs son un bien escaso

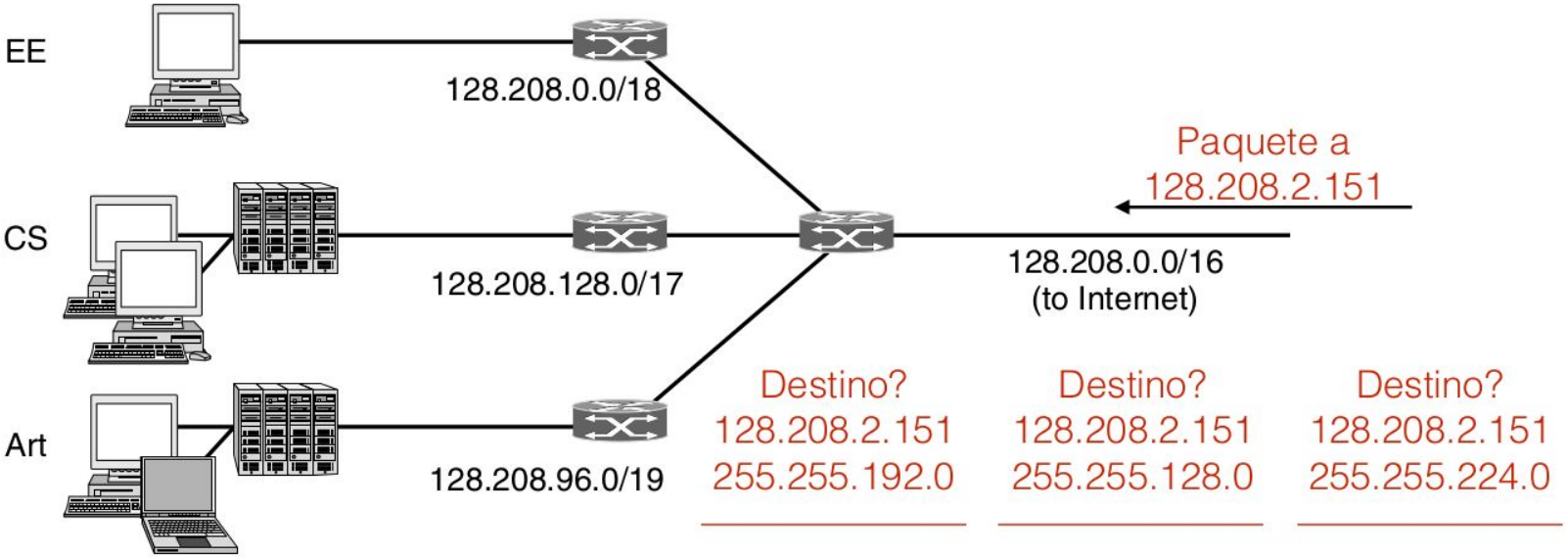
Subredes

- Subredes son segmentos de nodos de la red
- Cada segmento de la red está identificado por un prefijo de red
- Todos los host de dicho segmento poseen el mismo prefijo
- ¿Para qué sirven?



Ejemplo de subred

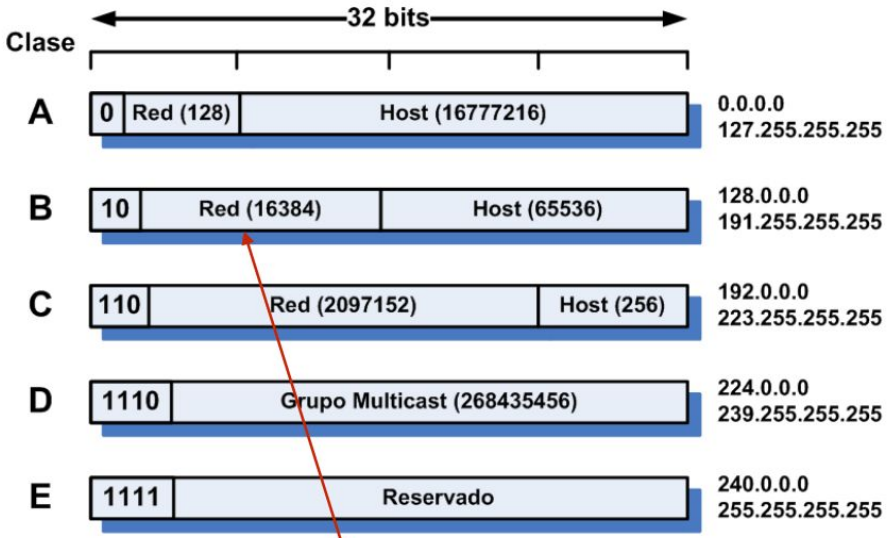
Computer Science:	10000000	11010000	1xxxxxxx	xxxxxxxx
Electrical Eng.:	10000000	11010000	00xxxxxx	xxxxxxxx
Art:	10000000	11010000	011xxxxx	xxxxxxxx



Classful Addressing

- Mecanismo predecesor del addressing Classless
- Router utiliza largo de prefijo fijo y acepta solo determinados prefijos definidos por clases
- No requiere de la transmisión de información del prefijo
- Para rutear un paquete, se busca en la tabla de rutas una dirección de red que coincida con el prefijo de la dirección de destino

Classful Addressing



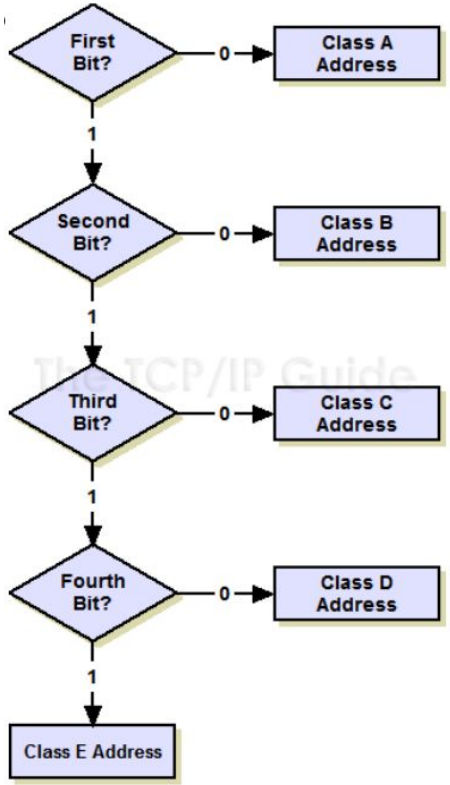
Class	Leading bits	Size of *network*	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127,255,255,255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191,255,255,255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223,255,255,255

Classful Addressing

- Al recibir un paquete el router analiza la IP de destino y clasifica el paquete en una clase
- Aplica máscara para la clase y determina la red de destino

Máscaras

- A: 255.0.0.0 (/8)
- B: 255.255.0.0 (/16)
- C: 255.255.255.0 (/24)



Classful addressing

Classful addressing se utilizó hasta el año 1993 por su problema de desperdicio de IPs.

Soluciones:

- CIDR (Classless Inter Domain Routing) se utiliza para combinar rutas y reducir los datos de enrutamiento transportados por los routers centrales
- VLSM (Variable Length Subnet Masking) ayuda a optimizar el espacio de direcciones disponible.

Beneficios

- Se puede modificar la división de la red modificando las máscaras
- En el exterior la subredes no son visibles por lo que no hay necesidad de informar o solicitar cambios a ICANN (Internet Corporation for Assigned Names and Numbers)
- Mejor uso de las IPs
- Permite escalar las redes, un segmento un dominio de broadcast
- Si tenemos muchos nodos en el mismo segmento, aumentamos las posibilidades de colisión y disminuimos el rendimiento
- Podemos aplicar reglas o filtros de tráfico entre segmentos IP
- Se puede definir segmentos IP en base a funciones, que requieren tipos de servicio diferentes

CIDR

Subnet Mask

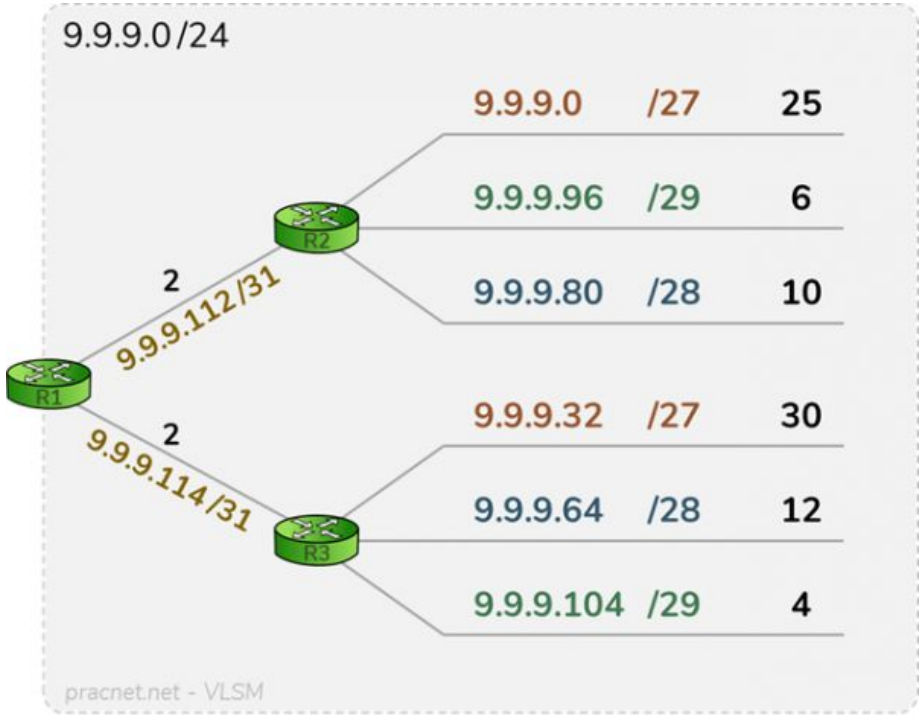
Suffix	Hosts	32-Borrowed=CIDR	2^Borrowed = Hosts	Binary=> dec = Suffix
.255	1	/32	0	11111111
.254	2	/31	1	11111110
.252	4	/30	2	11111100
.248	8	/29	3	11111000
.240	16	/28	4	11110000
.224	32	/27	5	11100000
.192	64	/26	6	11000000
.128	128	/25	7	10000000

Clase	Prefijo CIDR	Rango	
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255	1 dirección clase A
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255	16 direcciones clase B
C	192.168.0.0/16	192.168.0.0 - 192.168.255.255	256 direcciones clase C

Classless addressing

- Se aceptan prefijos variables (VLSM)
- Se rutea información junto con información del tamaño del prefijo (máscara)
- Router utiliza para decidir el envío el match más largo al momento de buscar en tabla
- Máscaras diferentes en cada subred

VLSM



- Lo que tradicionalmente se utiliza es un tamaño de máscara variable.
- Máscara variable permite adaptarse a las necesidades y reducir el desperdicio de IPs.
- La parte red y la parte host no son iguales en todas las subredes.
- Aunque las subredes pueden tener diferente tamaño no pueden solaparse.

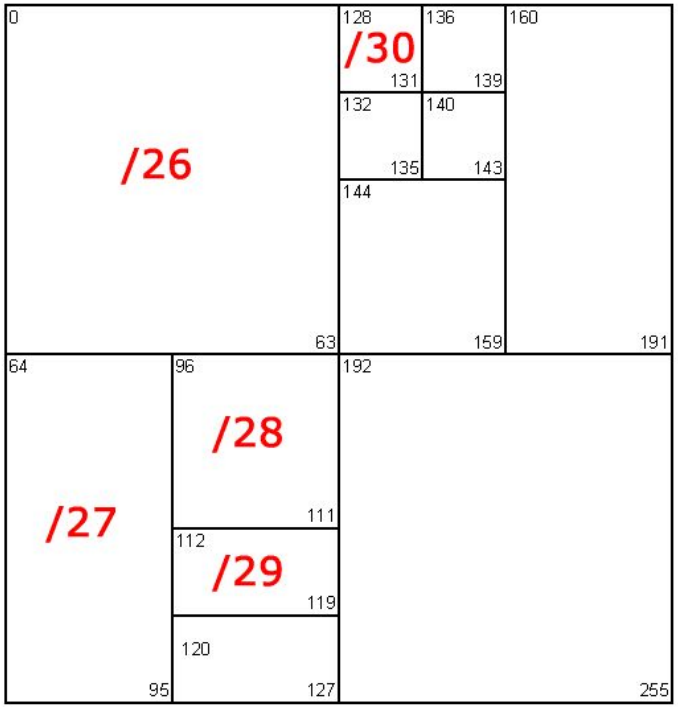
Ejemplo VLSM

Se tiene una red **clase C** cuya dirección base es **192.168.10.0/24**. Se quiere dividir dicha red en 4 subredes. Subred **A** con 50 host, subred **B** con 20 host, subred **C** con 10 host, y subred **D** con 10 host. Determine una manera de asignar direcciones utilizando VLSM. Identifique número de hosts, rango de IPs disponibles, dirección de broadcast, y máscara de cada subred.

Ejemplo VLSM

RED:#	Host (2^n)	n	Red	Mascara	Rango Util	Broadcast
A: 50	64	6	192.168.10.0	255.255.255.192 /26	192.168.10.1 - 192.168.10.62	192.168.10.63
B: 20	32	5	192.168.10.64	255.255.255.224 /27	192.168.10.65 - 192.168.10.94	192.168.10.95
C:10	16	4	192.168.10.96	255.255.255.240 /28	192.168.10.97 - 192.168.10.110	192.168.10.111
D:10	16	4	192.168.10.112	255.255.255.240 /28	192.168.10.113 - 192.168.10.126	192.168.10.127

VLSM - Técnica cuadro



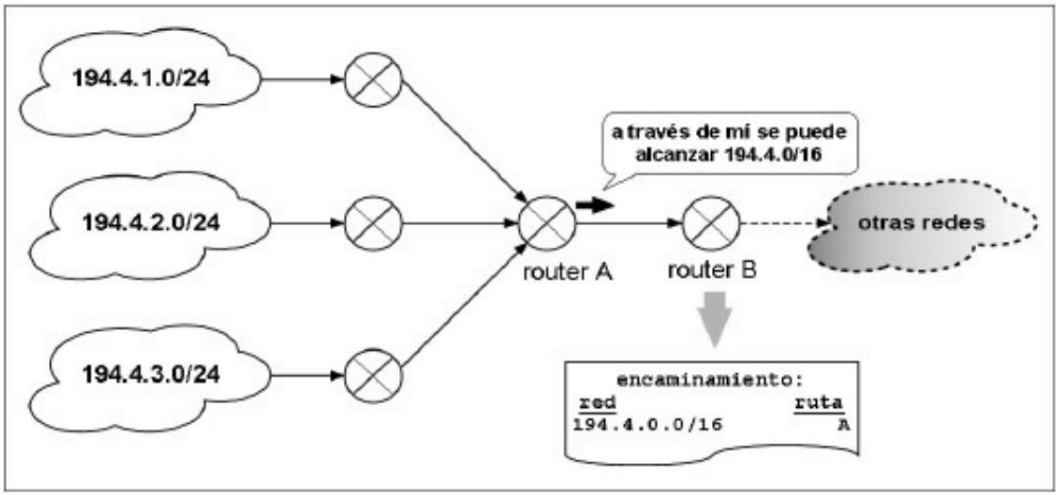
Agregación de dominios

Ventajas:

- Hace más pequeñas las tablas de enrutamiento.
- Esto hace que las búsquedas en la tabla sean más rápidas.
- Vuelve más legible la información.
- Oculta información específica acerca de las redes agregadas
- Las redes más pequeñas incluídas pueden caerse sin que esto afecte a publicación.
- Los protocolos de enrutamiento dinámico pueden evitar consumir ancho de banda para las actualizaciones.

Agregación de dominios

Proceso consiste en encontrar el máximo prefijo común entre las redes



Encontrar un prefijo que considere los 3 sub prefijos indicados y minimice la cantidad de IPs no disponibles.

Agregación de dominios

- Pasar a binario todas las redes a sumarizar.
- Identificar el número de bit n hasta el cual todos los bits de todas las redes son iguales. los bits contenidos entre este y los bits de host iniciales deben formar un recubrimiento completo.
- Para obtener el número de la super red se dejan los n bits primeros como están y el resto se pone a 0 obteniendo una red X.Y.Z.K
- La superred será X.Y.Z.K/n

Problema

Una organización recibe desde su ISP el bloque de direcciones 63.78.2.0/23 y necesita satisfacer los siguientes requerimientos:

- 8 equipos de comunicación
- 26 servidores de diversos tipos
- 1 router
- 12 equipos en finanzas
- 20 equipos en desarrollo
- 10 equipos en gerencia
- 40 equipos para administración y contabilidad
- 32 equipos de laboratorio de pruebas

Solución 1

- Mantener una jerarquía plana o único segmento IP. Así todos los equipos estarán configurados con la máscara 255.255.128.0
- Se ahorran interfaces de red en el router.
- Se ahorran problemas si hay que cambiar algún equipo de función.
- Todos los equipos tienen que estar en el mismo dominio de broadcast.

Solución 2

- Dividir el bloque usando máscaras más pequeñas.
- Se determina la máscara en base al número de hosts esperados en dicho bloque.