EL64E
Redes de Computadores

Introducción a Redes IP

Introducción a Redes IP

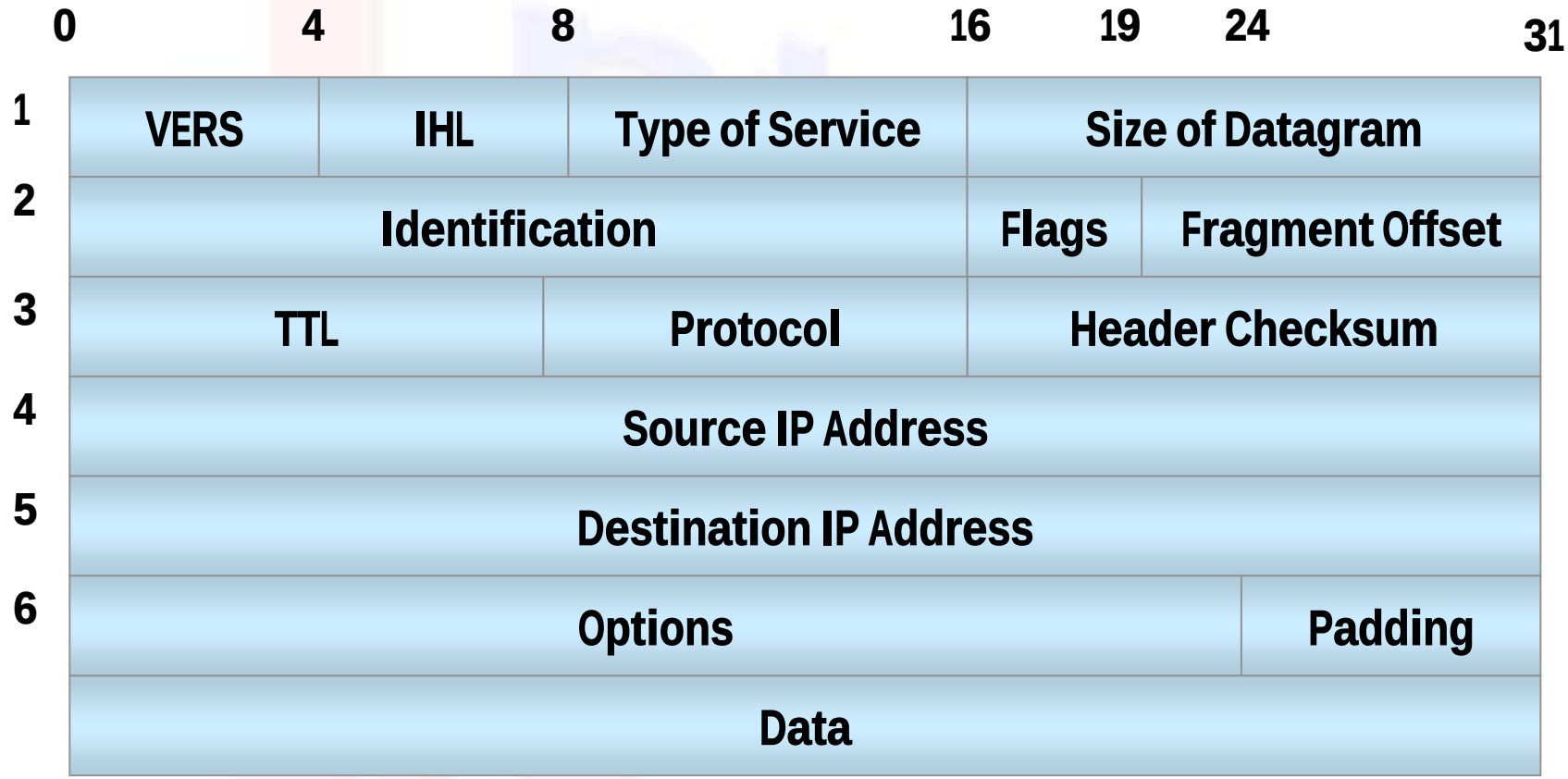
1. Formato de Paquetes IP
2. ARP. Address Resolution Protocol
3. ICMP. Internet Control Message Protocol
4. Tipos de direcciones
5. Jerarquía de Direcciones
6. Subnetting y CIDR, VLSM
7. NAT/NAPT

Formato de Paquetes IP

IP - Internet Protocol

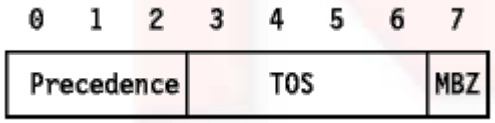
- Protocolo no orientado a la conexión.
- No transmite información de control.
- No establece una conexión end-to-end. antes de transmitir los datos.
- No es confiable.

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.

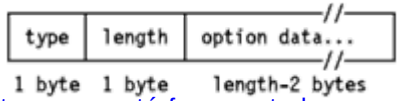
Descripción de Campos 3

- **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.

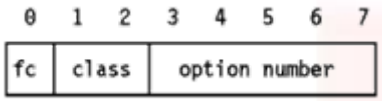
Descripción de Campos 4

- **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:
    1. 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.
    2. 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.
    3. 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.
    4. 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 1

- 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.

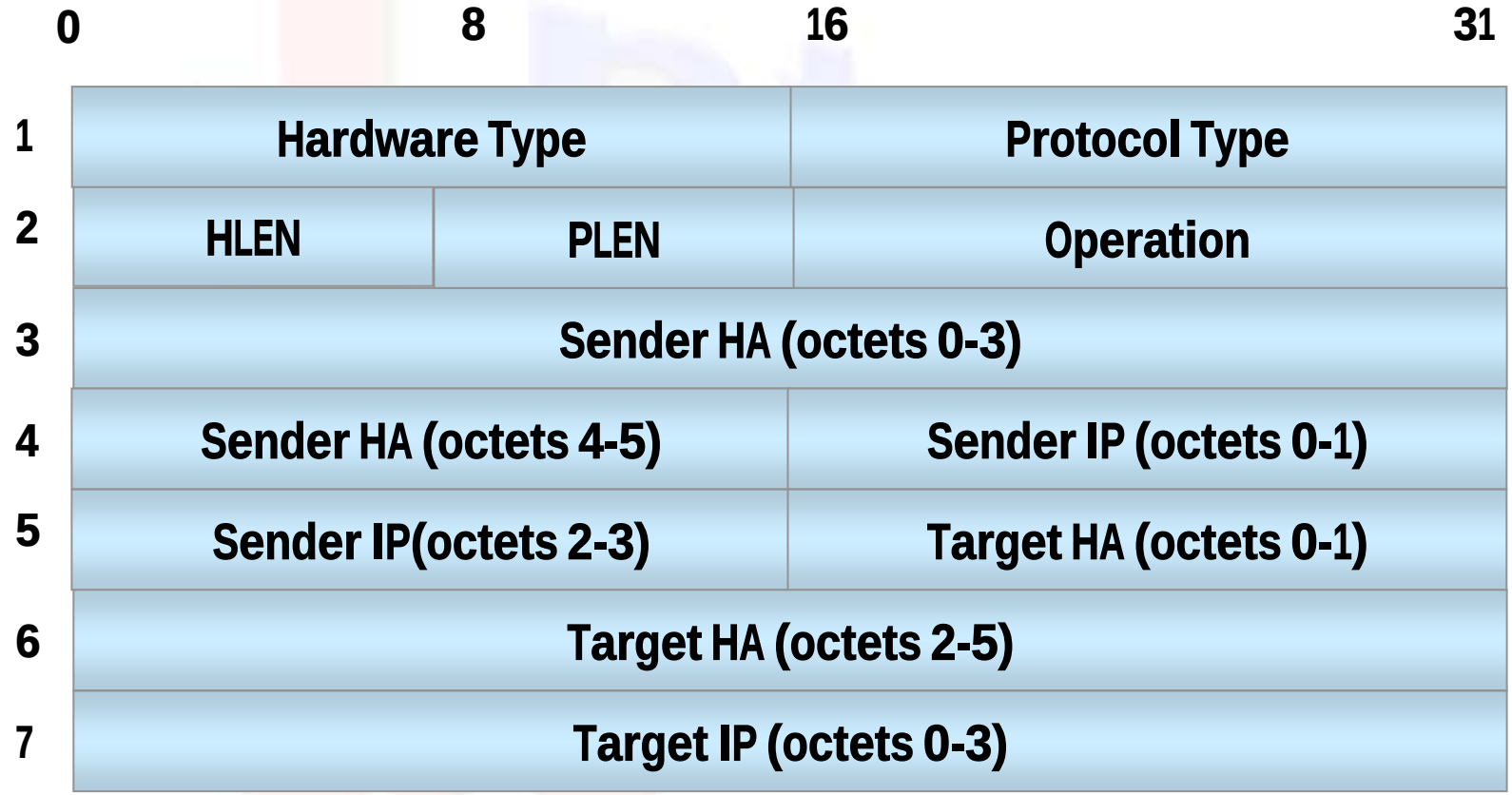
http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html

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

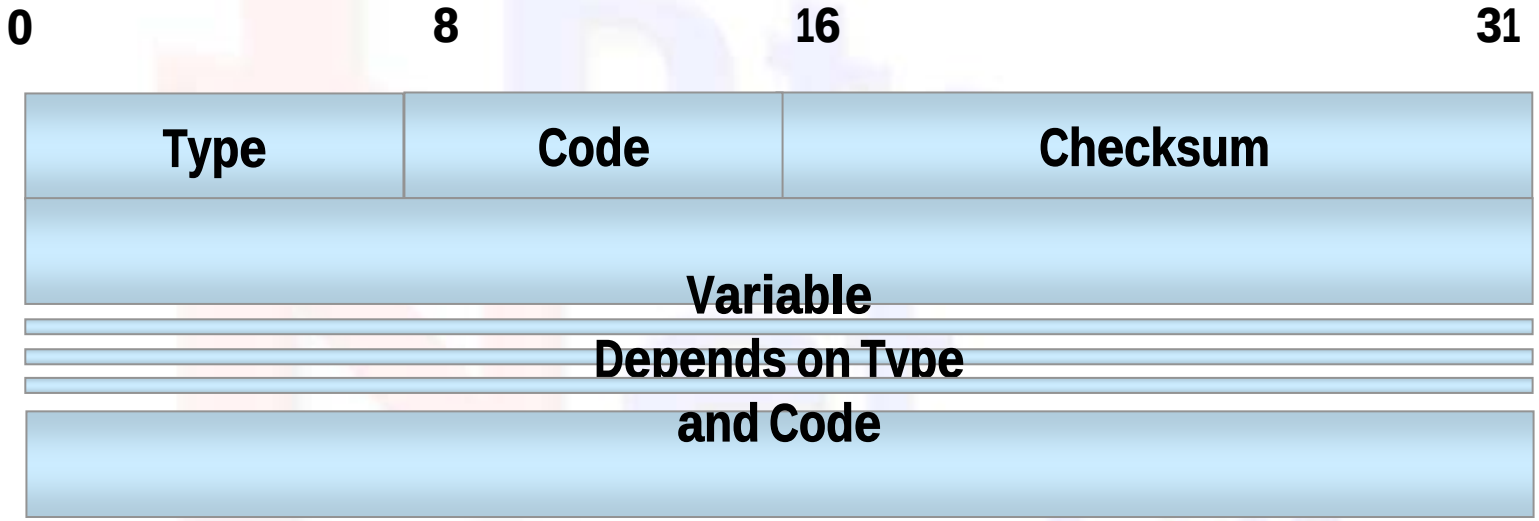
```
matrix% arp
Usage: arp hostname
       arp -a
       arp -d hostname
       arp -s hostname ether_addr [temp] [pub] [trail]
       arp -f filename
matrix% arp -a

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

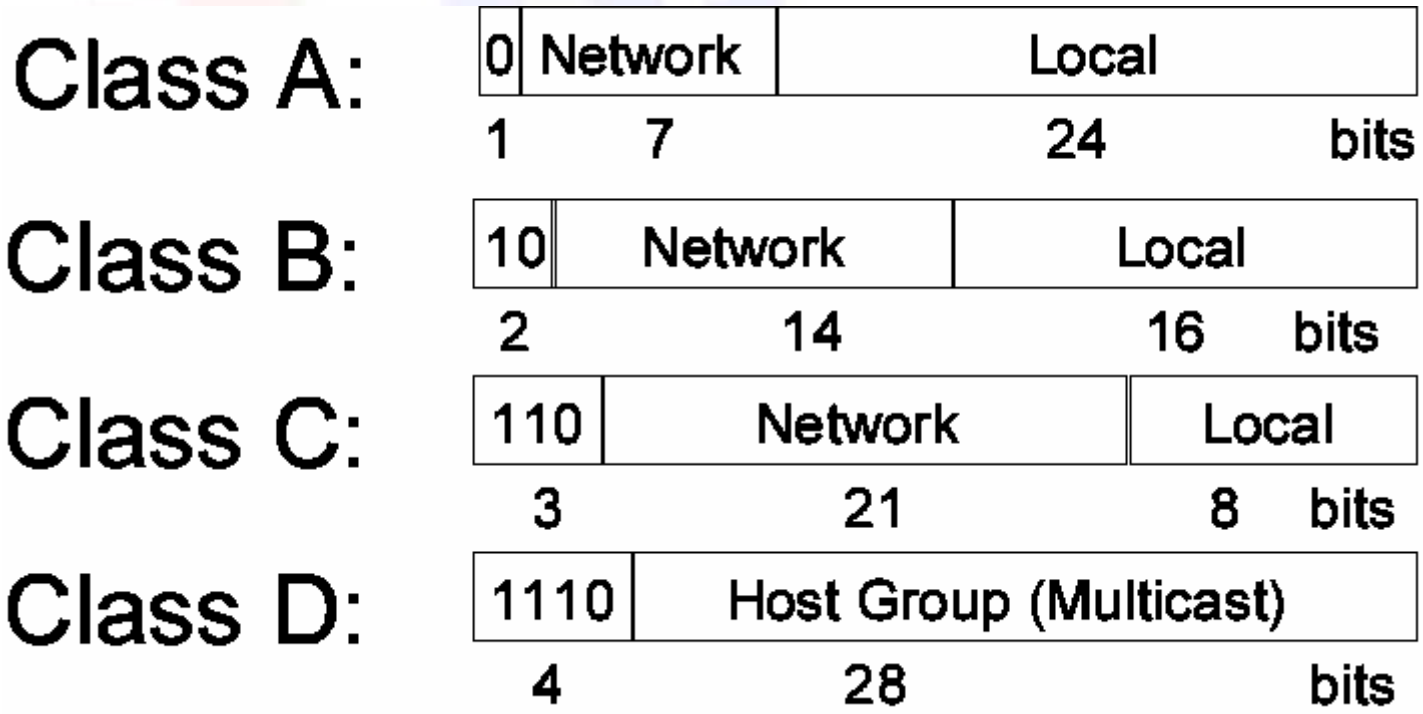
- Redirect Message
  - El router detecta que el próximo salto es un router dentro de la misma red del equipo que recibio el datagrama por lo que le informa que es mejor que se lo envie al otro router.
- Echo or Echo Reply Message.
  - La información recibida en un mensaje echo debe ser devuelta en un 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.

Tipos de Direcciones

¿Qué es un dirección IP?

- Una dirección IP es el identificador único de un host en una red IP.
- Está compuesto por 32 bit que usualmente se representa en cuatro decimales y cada uno de ellos representa 8 bit.
- Ejemplo:
  - 146.83.12.32
  - 1001 0010. 0101 0011. 0000 1100. 0010 0000

Clases de Direcciones IP



Clases de Direcciones

- Rangos de Direcciones
  - **A** 0.10.0.0-126.0.0.0
  - **B** 128.0.0.0-191.255.0.0
  - **C** 192.0.1.0-223.255.255.255
  - **D** 224.0.0.0-239.255.255.255 multicast
  - **E** 240.0.0.0-254.255.255.255 experimentación

- La encargada de la administración de las direcciones ip es la IANA (Internet Assigned Numbres Authority). LACNIC para latinoamérica y El Caribe

Direcciones IP Privadas

- Direcciones IP privadas (RFC 1597):
  - 10.0.0.0 1 clase A
  - 172.16.0.0 a la 172.31.0.0 16 clases B
  - 192.168.0.0 256 clases C
  - Las puede usar quien quiera. NO son ruteables en Internet

Jerarquía de Direcciones

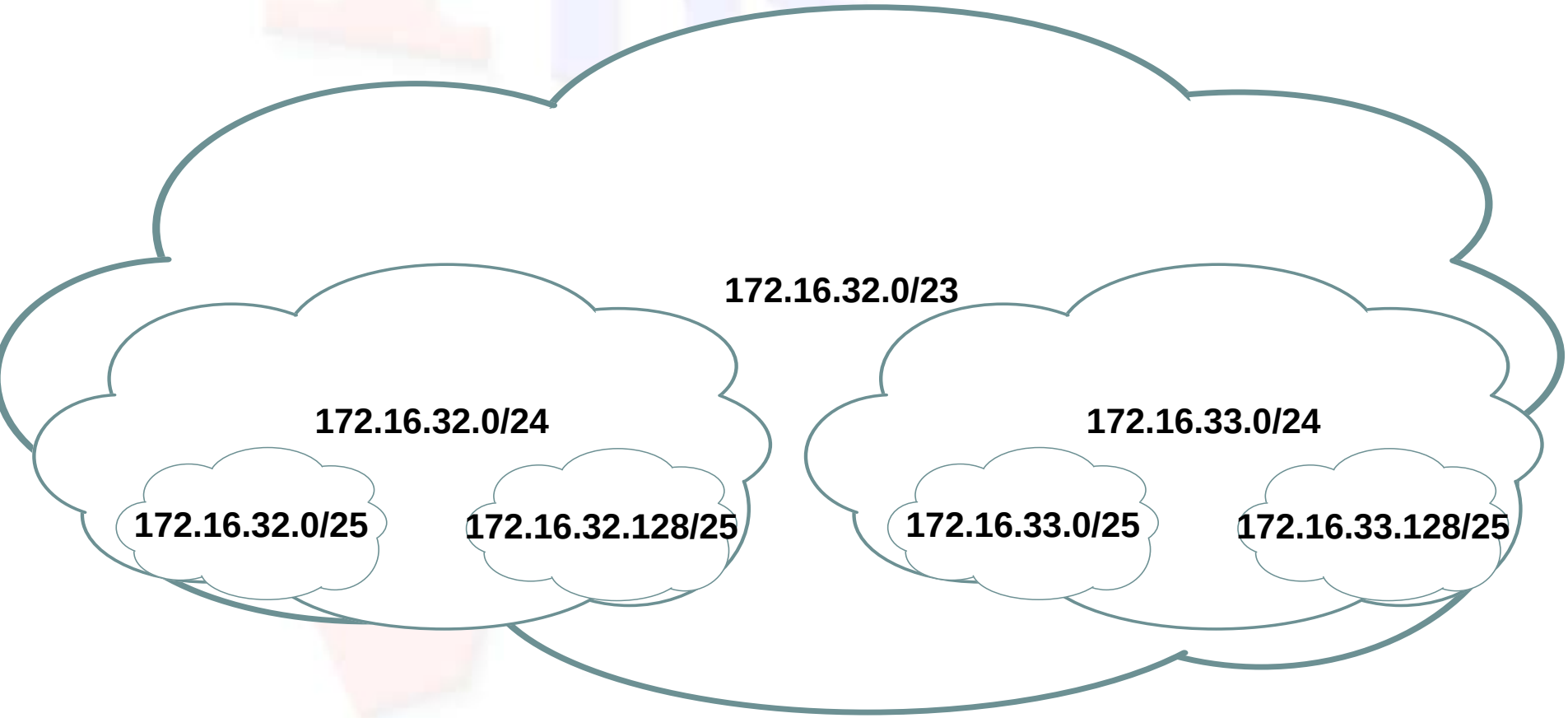
Jerarquía en Telefonía

Ejemplo de jerarquía telefónica:

+562 678 4207

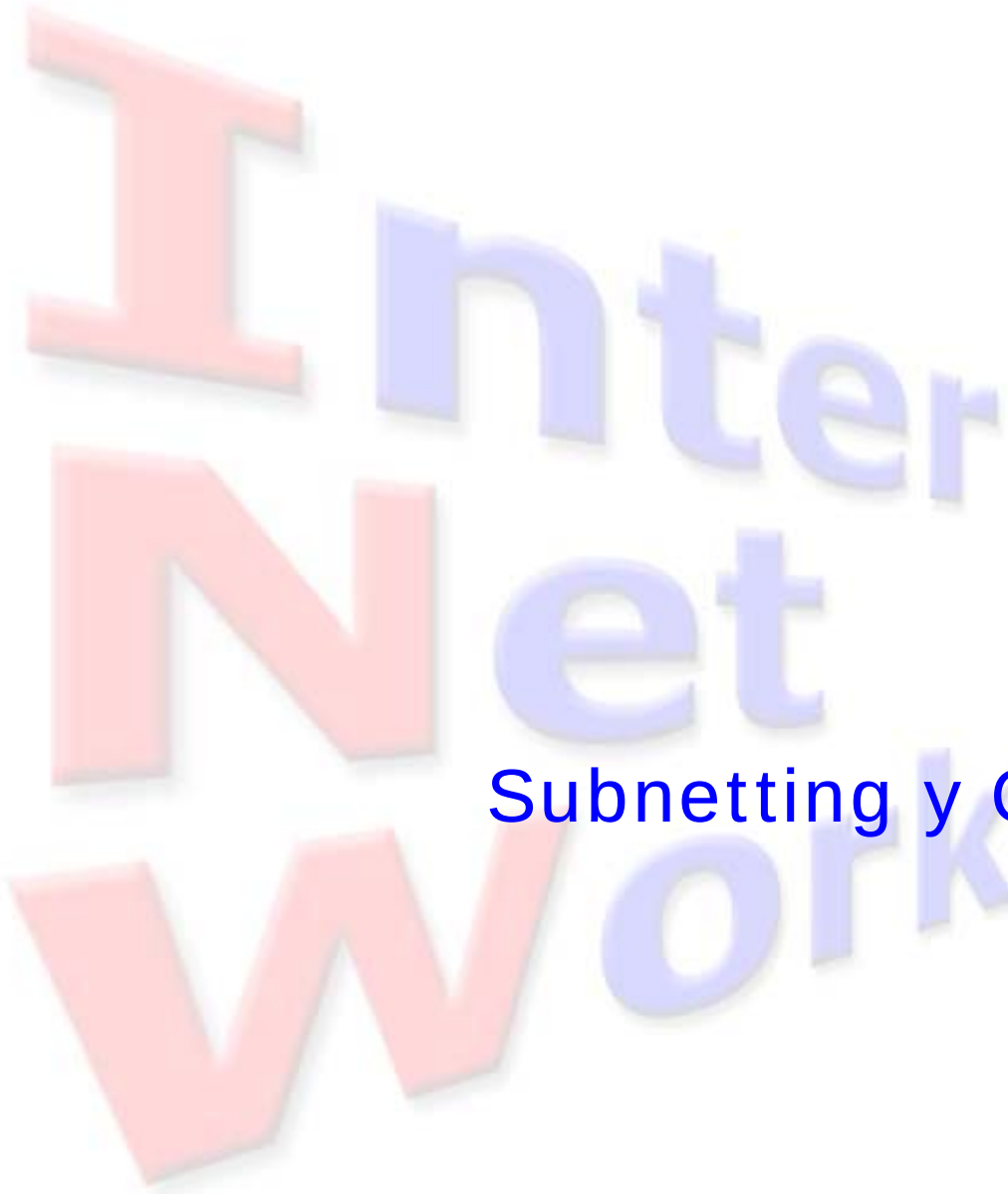
+562 678 4207 CHILE
+562 678 4207 SANTIAGO
+562 678 4207 UCHILE
+562 678 4207 FCFM
+562 678 4207 DIE

Jerarquía de Direcciones IP



Beneficios Jerarquía

- Reduce el número de entradas en las tablas de rutas. Resumiendo múltiples entradas en una ruta sumarizada.
- Localización eficiente de una dirección. La asignación de direcciones contiguas permite usar todas las direcciones disponibles.



Subnetting y CIDR, VLSM

Mascara por defecto 1

- La clase determina la máscara por defecto que tendrá la red y la cantidad de IPs que se pueden asignar a los host.
  - Clase A: **AAAAAAAA.xxxxxxxx.xxxxxxxx.xxxxxxxx**
    - **126 Redes**
    - **2^24 - 2=16.777.214 direcciones**
  - Clase B: **BBBBBBBB.BBBBBBBB.xxxxxxxx.xxxxxxxx**
    - **16.382 Redes**
    - **2^16 - 2=65.534 direcciones**
  - Clase C: **CCCCCCCC.CCCCCCCC.CCCCCCCC.xxxxxxxx**
    - **2.097.150 Redes**
    - **2^8 - 2=254 direcciones**

Mascara por defecto 2

- La mascara de red se utiliza para determinar el nombre de la red.
- Realizando la operación “and” lógico obtenemos el nombre de red.
  - Ejm.
  - Dirección IP: 146.83.12.32
  - Mascara Def: 255.255.0.0
  - Red: 146.83.0.0

Problemática

- Las clases de red determinan redes muy dispares.
  - Muy pocas redes con muchas direcciones para hosts.
  - Muchas redes con pocas direcciones para hosts.
- Solución Subdividir las redes.
  - Subnetting

Subnetting 1

- Si movemos mascara de red podemos generar subredes con un número de host adecuado a las necesidades de la Red.

Subnetting 2

- Ejemplo:
  - Red: 146.83.0.0
  - Mascara Def: 255.255.0.0

    1111 1111.1111 1111.0000 0000.0000 0000
  - Nueva Mascara: 255.255.224.0

    1111 1111.1111 1111.1110 0000.0000 0000
  - Número de Subredes: 2^3-2 = 6
  - Número de Hosts: 2^13-2 = 8190

  - Número de host útiles sin subnetting: 65.534
  - Número de Hosts útiles CON subnetting: 8190*6=49.140

Ejemplo

- IP address: 192.169.49.35
- Subnet Mask: 255.255.255.224
- Nº Subredes: $2^3-2=6$
- Nº Nodos/subred: $2^5-2=30$
- Subnet address: 192.169.49.32
- Direcciones válidas: 192.169.49.33-62
- Subnet broadcast: 192.169.49.63

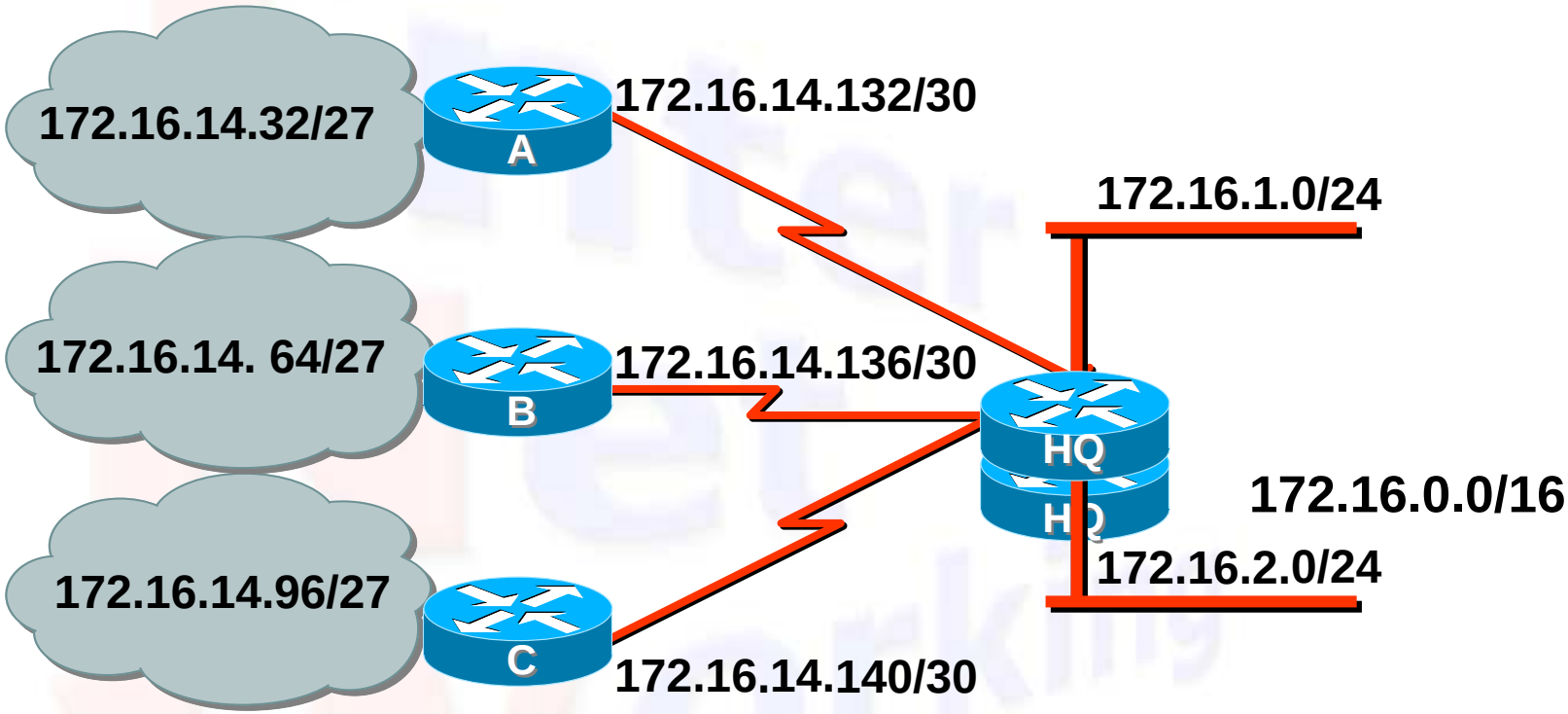
Ejemplo (cont.)

Numero de Red	Direcciones para Nodos	Dirección de Broadcast
192.169.49.0	Reservado	NA
192.169.49.32	.33 al .62	192.169.49.63
192.169.49.64	.65 al .94	192.169.49.95
192.169.49.96	.97 al .126	192.169.49.127
192.169.49.128	.129 al .158	192.169.49.159
192.169.49.160	.161 al 190	192.169.49.191
192.169.49.192	.193 al .222	192.169.49.223
192.169.49.224	Reservado	NA

VLSM

- Variable-Length Subnet Mask
- Al realizar subnetting quedan definidas redes que no son utilizables.
- Puede que la división realizada con subnetting contenga más direcciones IPs que las que se utilizarán (caso enlaces punto a punto)
- Para solucionar estos problemas se puede volver a dividir esas redes.

Ejemplo VLSM



Subred 172.16.14.0/24 is dividida en subredes más pequeñas:

- Subred con una máscara mayor (/27)
- Subredes más pequeñas se crean (/30)

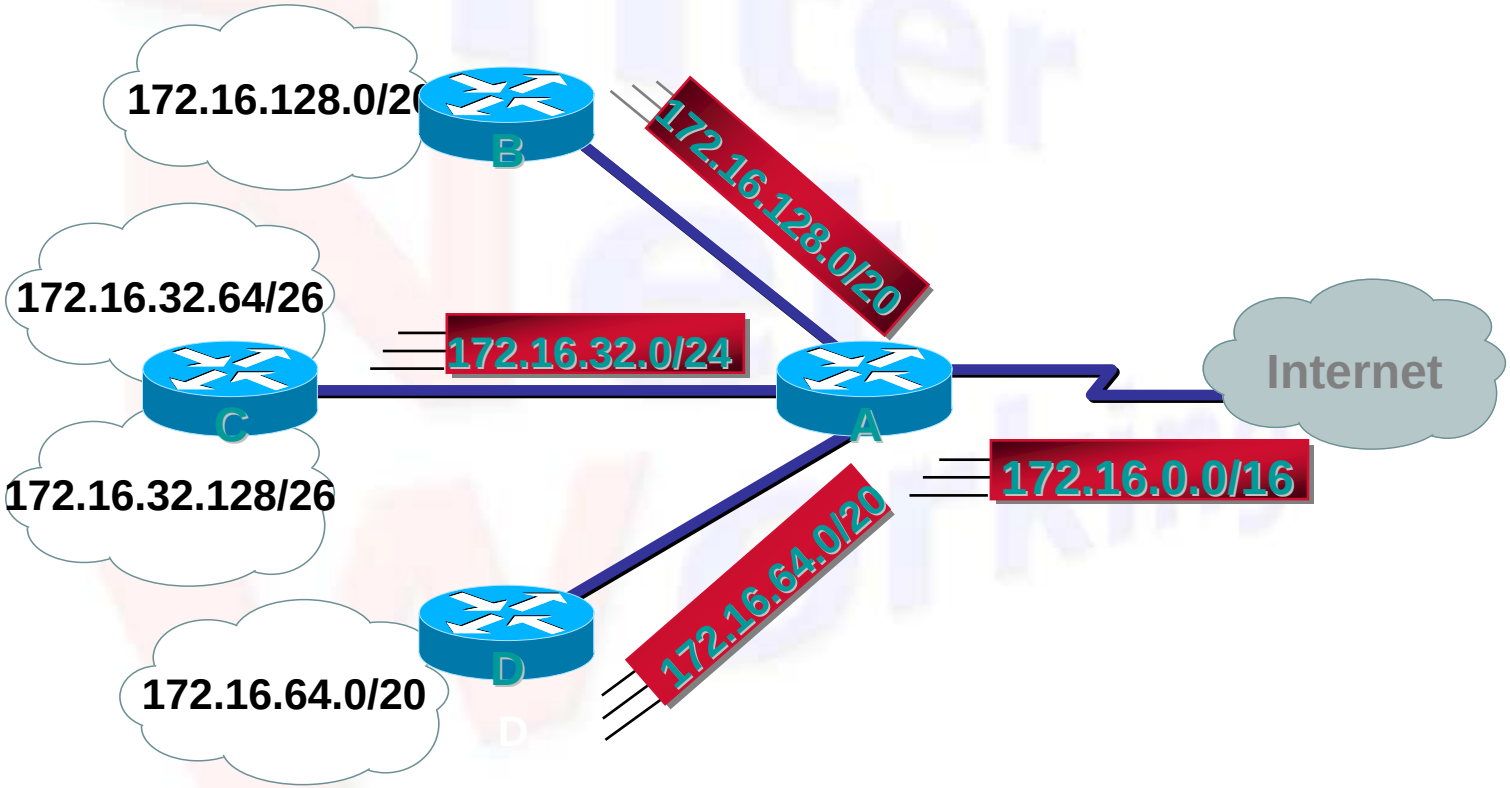
CIDR

- Classless InterDomain Routing
- Al definir las redes puede que estás no cumplan con las IPs necesaria.
- Es posible juntar redes y **sumarizarlas (supernetting).**
- Ejemplo:

  192.168.10.0/24
  192.168.11.0/24
  = 192.168.10.0/23
- Al sumarizar se puede controlar el crecimiento de las tablas de ruteos en los routers.

Sumarización (Supernetting)

Sumarización de direcciones en una red diseñada con VLSM



NAT/NAPT

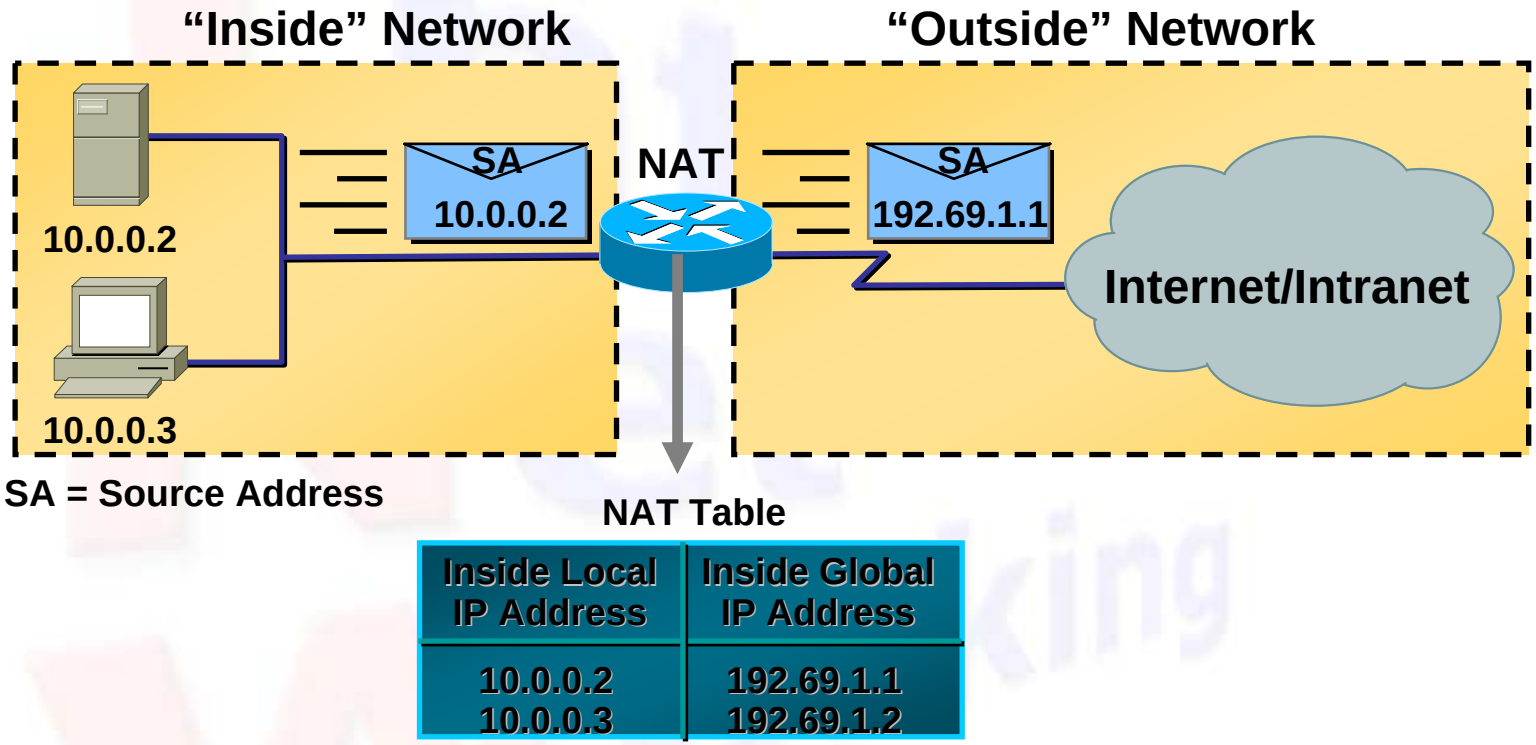
NAT

- Network Address Translation
- Está definido en el RFC 1631
- Tipos de NAT:
  - estático: mapeo uno a uno
  - dinámico: mapeo pool inside a pool outside
- Conceptos:
  - Dirección Local y Global

NAPT

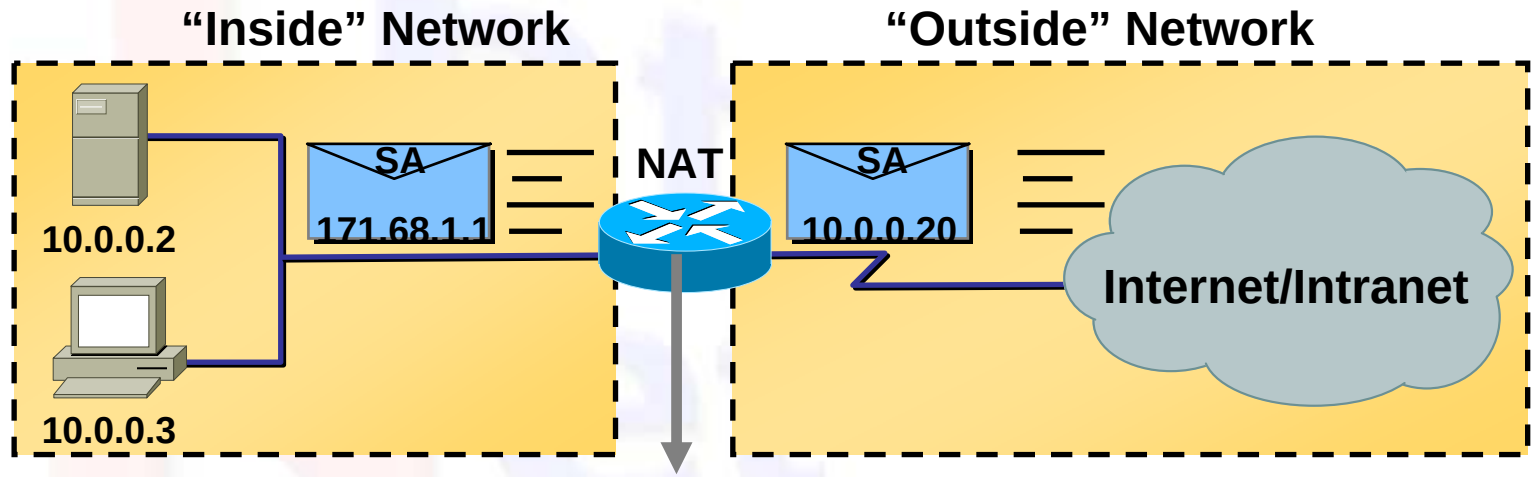
- Network Address Port Translation
- Mapeo de múltiples direcciones usan sólo una dirección Global
- Se trasladan los puertos UDP/TCP de las direcciones privadas a los puertos UDP/TCP de la IP global

“Inside Source” Address Translation



Los hosts internos usan diferentes direcciones ip que las que ven los hosts en la red “outside”

“Outside Source” Address Translation



NAT Table

Outside Local IP Address	Outside Global IP Address
171.68.1.1	10.0.0.20
171.68.1.2	10.0.0.21

- Habilita las direcciones para el uso de las direcciones traslapadas
- Equivale a trasladar el destino externo para el tráfico desde adentro hacia fuera.