O nivel de rede

Sumario

Introdución

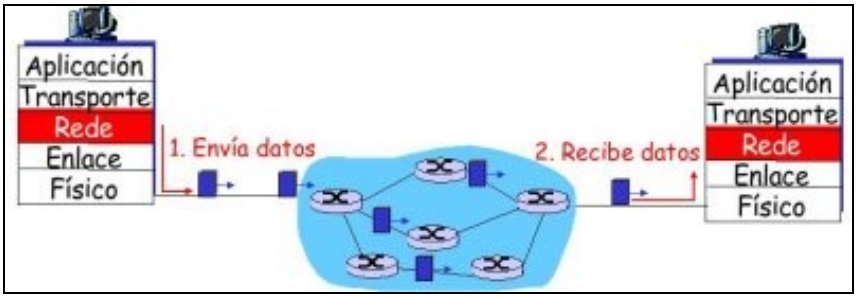
No capítulo anterior vimos que o nivel de enlace xoga un papel fundamental nas redes locais. Nesta unidade estudaremos o nivel de rede que é necesario para a comunicación nas redes de área extensa (*Wide Area Networks* ou WAN).

As redes locais utilizan un medio compartido a través do cal as estacións están conectadas directamente (mediante un *switch*, ou un *hub*), polo que existe unha única ruta posible para comunicar dúas estacións. O nivel de enlace dunha estación realiza, entre outras, a tarefa de comprobar se as tramas que circulan pola rede local van destinadas a ela e, se procede, capturalas. Para elo, comproba a dirección MAC do destinatario na trama de datos.

Con todo, se queremos enviar datos a unha estación fóra da LAN a situación cambia, xa que pode haber múltiples camiños para levar a información dende a orixe ao destino. É dicir, podemos querer enviar datos dende unha estación conectada a unha LAN a outra estación conectada a outra LAN distinta, posiblemente, noutro lugar. O nivel de enlace non está preparado para facer este traballo. É o nivel de rede o encargado de facelo.

O nivel de rede divide a información en paquetes que se envían por distintos camiños. A esta técnica chámaselle **conmutación de paquetes** e é a que usa o IP e, polo tanto, Internet. Para que a información chegue dende o emisor ao receptor pasará por distintas estacións intermedias, característica

que diferencia a esta capa do nivel de enlace, que só se preocupa da comunicación entre estacións conectadas á mesma LAN.



Pola contra, na **conmutación de circuítos**, primeiro se establece unha conexión, é dicir, resérvase unha ruta determinada entre a orixe e o destino para uso exclusivo desa transmisión. Unha vez establecida a ruta, a información circula toda xunta por ese camiño e, cando xa non hai nada que transmitir, é necesario liberar esa conexión. O gran inconveniente da conmutación de circuítos é que consume os mesmos recursos da rede con independencia de se están usando ou non, ou da cantidade de información enviada. Isto non acontece na conmutación de paquetes.

Servizos típicos do nivel de rede

As funcións principais que levan a cabo os protocolos do nivel de rede son as seguintes:

- **Encamiñamento da información**
- **Control da conxestión**
- **Direccionamento**

Igual que acontecía no nivel de enlace, non todos os protocolos do nivel de rede implementan todas as funcións. De feito, o Internet Protocolo (IP) non soporta control de conxestión.

Encamiñamento

Nunha rede WAN as estacións que se queren comunicar non van estar conectadas directamente. Existen equipos intermedios, chamados **nodos**, que poden ser destinatarios dos datos pero que tamén se encargan de "guiar? correctamente a información cando non son os destinatarios finais. A esta tarefa denomínaselle encamiñamento.

A elección dunha determinada ruta faise seguindo criterios de rendemento e usando **táboas de encamiñamento**, como se verá máis adiante.

Control de conxestión

Cada nodo necesita un intervalo de tempo para procesar os paquetes que lle chegan. Pode chegar un novo paquete ao nodo mentres este está procesando algún outro. Existe un *buffer* (memoria temporal) que impide a perda de datos neses casos. Se o nodo procesa os paquetes con máis lentitude da que son recibidos pode haber perda de paquetes.

Nesta tesitura as estratexias poden ser:

1. Rexeitar os novos paquetes que van chegando, que é o que fai o IP, seguindo un principio de mínimo esforzo.
2. Impedir que os nodos veciños envíen novos paquetes, que pode empeorar a situación, xa que se incrementa o tráfico de control entre os nodos xa conxestionados en detrimento dos datos.

Direccionamento

Cada estación debe ter unha dirección que a identifique de xeito único do resto para que se poida especificar a orixe e destino da información. Este mecanismo é o direccionamento no nivel de rede que coexiste na pila de protocolos co direccionamento no nivel de enlace. Este último utilízase para distinguir entre estacións conectadas á mesma LAN pero non serve para equipos conectados en LAN distintas. Ambos mecanismos de direccionamento son necesarios. Facendo unha analoxía co mundo real podemos pensar na dirección MAC dunha estación como o DNI dunha persoa e na dirección IP coma na súa dirección postal.

O Internet Protocol

O IP ou Internet Protocol é un protocolo de interconexión de redes que utiliza a conmutación de paquetes. Por iso dise que é un protocolo **orientado a datagrama** (paquete) e **non orientado á conexión**.

O IP non ten control de conxestión nin de erros polo que non é capaz de recuperar datos perdidos, nin de garantir que as tramas se entregarán na orde correcta (recordemos que os paquetes poden seguir camiños diferentes e sufrir atrasos diferentes); tampouco garante que o ritmo de recepción sexa o adecuado para que o receptor procese convenientemente os datos. Por todo isto, dise que IP é un protocolo de tipo *best effort* que poderiamos traducir como ?quen fai o que pode non está obrigado a máis?. O traballo que non fai IP delégase nas capas superiores, xa que esta política de mínimo esforzo non sempre vale se hai erros, polo que é o TCP (*Transmission Control Protocol*) o responsable de conseguir que a información chegue nas condicións de fiabilidade desexadas.

Direccionamento en IP

As direccións IP permiten identificar un equipo en Internet (Internet é unha gran rede formada por redes máis pequenas), así como a subrede á que pertence. Cada interface de rede (NIC ou *Network Interface Card*) dun equipo ten unha dirección IP (pode ter varias), aínda que esta pode cambiar, non como no caso das direccións MAC en Ethernet. Se unha máquina ten dúas interfaces de rede terá, polo menos, dúas direccións IP.

Unha dirección IP represéntase con 4 bytes en decimal separados por puntos. Por exemplo:

```
194.83.153.100
```

O Internet Network Information Center ou InterNIC (actual ICANN) adícase á tarefa de asignar rangos de direccións IP. Na actualidade, esta entidade delega a responsabilidade da asignación de direccións a entidades rexionais (en España, a red.es)

Un enderezo IP divídese en dúas partes:

- Unha parte identifica o **número de rede** (identificador de rede)
- Outra parte identifica o **número de equipo** dentro desa rede (identificador de equipo)

Existen tres clases de direccións IP (A, B e C) en función do número de equipos e redes que poden direccionar:

- **Clase A**. Reservan o primeiro byte (8 bits) para o identificador da rede e os tres restantes (24 bits) para identificadores de equipos. O primeiro bit do primeiro byte vale 0. Polo tanto, só pode haber 2^7 direccións de clase A con 2^24 equipos cada unha (xa non se asignan direccións deste tipo). Por exemplo:

```
Dirección IP: 30.1.2.3
Identificador de rede (o primeiro byte): 30
Identificador de equipo (os tres bytes seguintes): 1.2.3
```

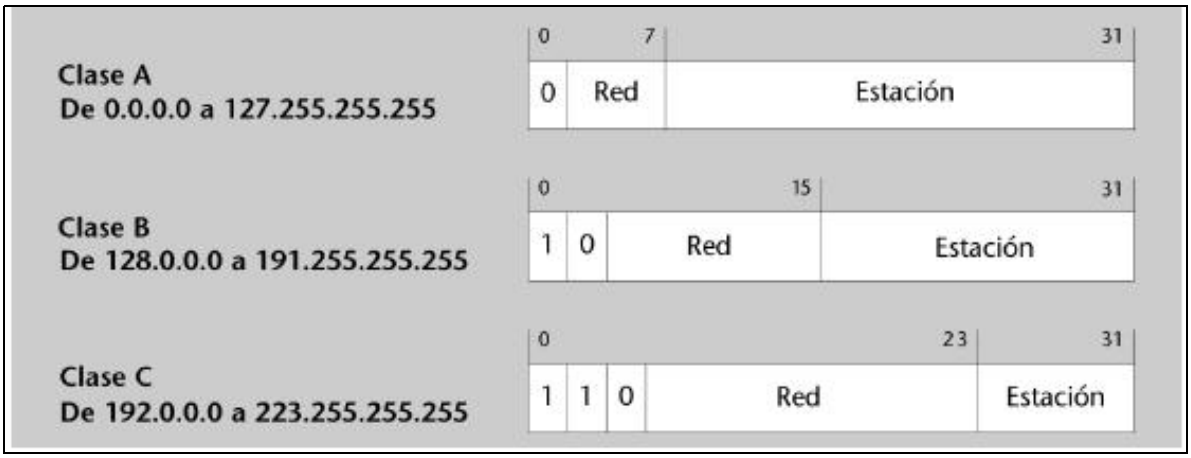
- **Clase B**. Teñen 2 bytes para redes e 2 bytes para equipos. Os dous primeiros bits do identificador de rede sempre valen 10 (en binario), xa que logo, pode haber 16.384 redes (2^14) con 65.536 estacións cada unha. De clase B tampouco queda ningunha dirección libre para asignar. Por exemplo:

```
Dirección IP: 140.1.2.3
Identificador de rede: 140.1
Identificador de equipo dentro desa rede: 2.3
```

- **Clase C**. Reservan 3 bytes (24 bits) para o identificador de rede e 1 byte (8 bits) para o identificador de estación. Os tres primeiros bits do identificador de rede teñen o valor 110 (en binario). Por exemplo:

```
Dirección IP: 194.144.35.5
Identificador de rede: 194.144.35
Identificador de equipo dentro desa rede: 5
```

Hai menos direccións IP útiles das posibles, xa que algunhas están reservadas. Unha vez que se coñece unha dirección é fácil saber se corresponde a unha rede de clase A, B ou C:



Na imaxe anterior non hai ningunha dirección que empece con tres bits 111. Estas direccións (chamadas clase D e clase E) son de propósito especial e non se asignan a máquinas concretas.

Máscaras de rede

O concepto de máscara é fundamental para entender o funcionamento das redes IP. A máscara permite a unha estación decidir se o destino ao que debe transmitir se atopa dentro da mesma LAN ou nunha LAN remota. Neste último caso debe delegar a súa transmisión a algún equipo da súa mesma LAN (o encamiñador) para que se encargue de facer chegar o paquete ao seu destino.

O que determina se dous equipos están na mesma LAN é o **identificador de rede**. O identificador de rede dunha dirección IP non está determinado polo primeiro byte da dirección IP (ou primeiros), senón pola máscara. A máscara son 4 bytes que oscilan entre 0 e 255 cada un separados por puntos, como nunha dirección IP. Por medio da máscara definimos os bits que identifican a rede (bits a 1 da máscara) e os que identifican a estación (bits a 0). Así, o identificador de rede é a parte da dirección IP que encaixa cos bits a 1 da máscara (**AND lóxico**). Analogamente, o **identificador de equipo** é a parte da dirección IP que encaixa cos bits a 0 da máscara (**OR lóxico**). Vexámolo cuns exemplos:

```
Obter o identificador de rede e identificador de equipo dun enderezo IP
Exemplo I:
 ? Enderezo IP: 69.51.117.3 (01000101.51.117.3)
 ? Máscara: 255.0.0.0 (11111111.0.0.0)
 ? Rede: 69.0.0.0
 ? Equipo: 51.117.3

Exemplo II:
 ? Enderezo IP: 69.51.117.3
 ? Máscara: 255.255.0.0
 ? Rede: 69.51.0.0
 ? Equipo: 117.3

Exemplo III:
? Enderezo IP: 69.51.117.3
? Máscara: 255.255.255.0
? Rede: 69.51.117.0
? Equipo: 3
```

Para que dous equipos se poidan comunicar entre si no nivel de rede deben pertencer á mesma rede IP, senón terán que comunicarse a través dun encamiñador. Para comprobar se dous equipos pertencen ou non á mesma LAN basta con aplicarlles a máscara de rede ás súas direccións IP mediante un AND lóxico e así obteremos o identificador da rede. Vexámolo cun exemplo:

```
Exemplo:
Se temos dúas estacións coas direccións:
- Equipo I: 147.83.153.100
- Equipo II: 147.83.153.200,
- Máscara de rede 255.255.255.0
Podemos ver que están na mesma LAN, aplicándolle a máscara:
- Equipo I: 10010011.01010011.10011001.01100100
- Máscara:  11111111.11111111.11111111.00000000
-----------------------------------------------
AND:        10010011.01010011.10011001.00000000
```

O identificador de rede é, en ambos casos, 147.83.153.0. Se facemos un OR lóxico entre a parte que está a 0 da máscara e a dirección IP obteriamos o identificador do equipo.

No exemplo anterior, con todo, deduciriamos que non están conectadas á mesma LAN se a máscara fose, por exemplo, 255.255.255.128. Vexámolo. Para o equipo I:

```
- Equipo I: 10010011.01010011.10011001.01100100
- Máscara:  11111111.11111111.11111111.10000000
-----------------------------------------------
AND:        10010011.01010011.10011001.00000000
```

O identificador de rede é:

```
147.83.153.0
```

Para o equipo II:

```
- Equipo II: 10010011.01010011.10011001.11001000
- Máscara:   11111111.11111111.11111111.10000000
-----------------------------------------------
AND:         10010011.01010011.10011001.10000000
```

O identificador de rede é:

```
147.83.153.128
```

Unha notación alternativa para a máscara é proporcionar o número de bits a 1 da mesma. Así pois, a máscara 255.255.255.0 é unha máscara de 24 bits e a 255.255.255.128 é unha máscara de 25 bits. É habitual ver unha dirección co engadido da máscara e coa seguinte notación:

```
147.83.153.100/24
```

Direccións especiais

Existen algunhas direccións IP de propósito especial. Todas as direccións dos seguintes rangos son privadas:

```
10.0.0.0/8
Da 172.16.0.0/16 á 172.31.0.0/16
Da 192.168.0.0/24 á 192.168.255.0/24
```

Asemade, as clases D e E están reservadas.

Subnetting

Cando un administrador dunha rede recibe o encargo de xestionar un conxunto de direccións, é posible que necesite configurar internamente diferentes LAN con este conxunto. Xa vimos que isto se fai coa máscara de rede. Por exemplo, podemos usar máis bits dos que corresponderían para a máscara nunha rede de clase C (25 bits en lugar de 24 que sería o "normal" ou **máscara natural**). Isto permite crear máis redes ?roubando? bits aos bits correspondentes aos equipos. Poderemos direccionar menos equipos pero cunha única dirección IP teremos máis redes. A isto chámaselle *subnetting* e ás redes que se crean utilizando esta técnica chámaselles **subredes**.

Por exemplo, a dirección 212.45.10.0/27 permite crear 6 subredes distintas dentro da rede de clase C 212.45.10.0 porque rouba 3 bits do identificador de estación, xa que a máscara natural sería de 24 bits, é dicir, 212.45.10.0/24, e 2^3 ? 2 = 6 redes. Vemos que se restan dúas subredes das posibles. Isto é así porque a dirección con todos os bits a 0 coincide co identificador de rede e a dirección con todos os bits a 1 coincide coa dirección de broadcast. Xa que logo, as subredes posibles serían:

```
000 (non se usa)
001
010
011
100
101
110
111 (non se usa)
```

Supernetting

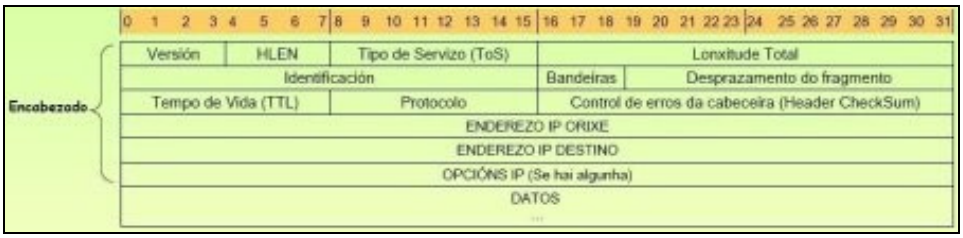
Se en lugar de roubar bits da parte da dirección IP que identifica aos equipos, collemos bits da parte da dirección IP que identifica ás redes estaremos facendo *supernetting*. O mecanismo é idéntico ao anterior pero o que se fai é obter unha super-rede que permite direccionar varias subredes IP

utilizando unha única ruta e aforrando espazo nas táboas de routing. Á rede (ou ruta) resultante chámaselle **super-rede**.

Ambas técnicas, subnetting e supernetting, xunto co uso de máscaras variables dan lugar ao que se chama **Classless Inter-Domain Routing** (CIDR).

O formato do paquete IP

Á **PDU** (*Unidade de Datos do Protocolo*) do nivel de rede chámaselle paquete ou datagrama. Para entender moitas das funcionalidades do IP hai que estudar o formato do paquete. Este, igual que a trama Ethernet, ten unha cabeceira e uns datos (**payload**). O formato da cabeceira é o seguinte:

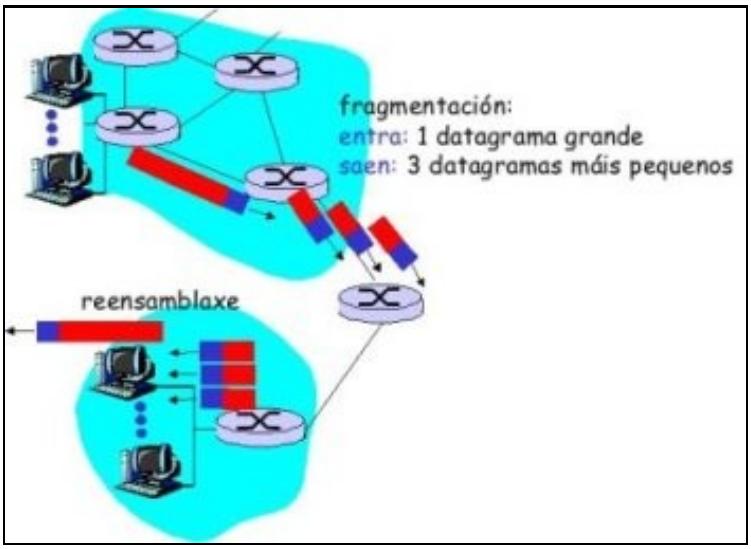


E o significado dos campos é o que segue:

- **Version**: Versión do protocolo IP do datagrama. Normalmente será IPv4.
- **HLEN**: Lonxitude da cabeceira medida en palabras de 32 bits (1 palabra de 32 bits é igual a unha fila do debuxo).
- **Lonxitude total**: Medido en bytes. Inclúe os bytes de cabeceira e dos datos. O campo ten 16 bits, polo tanto, o paquete IP poderá ter, como máximo, 2^16 = 65536 bytes ou 64KBytes
- **Tipo de servizo**: Para especificar a **prioridade** do datagrama, **fiabilidade**, **retardo**, etc. Os routers non fan moito caso deste campo.
- **Tempo de vida** (*Time To Live*): Especifica o tempo que o datagrama pode estar na rede. Ao pasar polos routers, estes van decrementando este valor. Se chega a 0 e o datagrama non chegou ao destino descartarase.
- **Protocolo**: O protocolo do nivel de transporte que encapsula (TPC, UDP, ICMP)
- **Checksum**: Úsase para comprobar que a cabeceira chegou correctamente.
- **Direccións IP**: De orixe e destino do paquete.
- **Opcións**: Úsase para probar de rede, depuración, etc.
- **Datos**: Contén a PDU do nivel superior, por exemplo, un segmento TCP.

Fragmentación

Un paquete IP normalmente vai inserido (encapsulado) nunha trama Ethernet. Polo tanto, un host emisor debe pasar un datagrama do nivel 3 ao nivel 2 para poder transmitilo. Isto é, debe meter o datagrama IP no campo de datos dunha trama Ethernet. En Ethernet o paquete máximo que pode transmitir unha estación é de 1.500 bytes, é dicir, a **MTU** (*Maximun Transfer Unit*) é de 1500, incluída a cabeceira IP. Co cal, se se ten un datagrama de tamaño maior que a MTU, terase que dividir noutros máis pequenos. A isto chámaselle **fragmentación**. Cando o paquete chegue ao receptor, este terá que reensamblalo.



Os campos da cabeceira dun paquete IP que se ven afectados pola fragmentación son:

- **Identificación**: determina o número do paquete. Se este se fragmenta, cada fragmento levará a mesma identificación, así o receptor saberá que fragmentos se corresponden a cada paquete orixinal.
- **Flags**: son un conxunto de bits da cabeceira que indican se o paquete se pode fragmentar ou non (bit "Don't Fragment*). Se se pode fragmentar, indican se é un fragmento intermedio ou o último (bit* More Fragments*).*
- **Desprazamento** ou *offset*: cando se fragmenta un paquete cada fragmento leva un anaco do datagrama orixinal. O campo desprazamento indica a posición dos bytes que leva un fragmento no datagrama orixinal. É dicir, é como se fose a numeración de cada fragmento.

O resto dos campos da cabeceira cópianse integramente do paquete orixinal aos fragmentos que resultan da fragmentación, excepto a lonxitude e o *checksum*. Vexámolo cun exemplo: se se queren enviar 4000 bytes (incluída a cabeceira IP) nunha rede cunha MTU de 1500 bytes, como no exemplo da anterior figura, sería como segue:

Fragmento	Bytes datos	Quedan por enviar	Identificador	Flag MF
1º fragmento	1480	3980 – 1480 = 2500	777	1
2º fragmento	1480	2500 – 1480 = 1020	777	1
3º fragmento	1020	1020	777	0
TOTAL:	3980			

Pero **onde e cando se fragmenta**? Un datagrama pódese fragmentar no emisor ou en calquera dos routers intermedios, sempre e cando o esixa a MTU da rede a atravesar.

E **onde se reensambla**? Só no receptor final, nunca nos encamiñadores, pois cada fragmento puido ir por camiños distintos ata chegar ao receptor final, e el será o único que reciba todos os anacos nos que se dividiron os fragmentos.

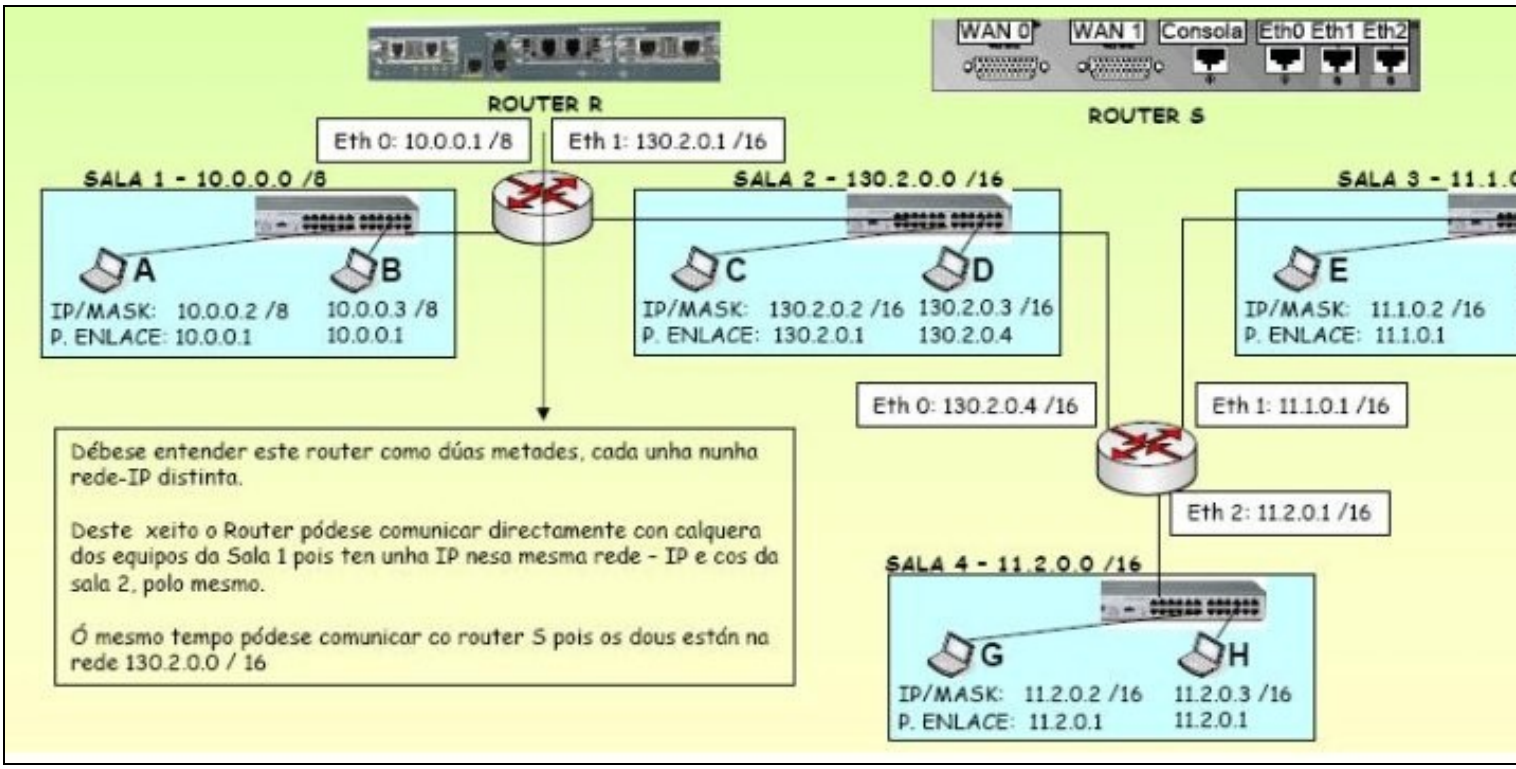
Encamiñamento ou *routing*

Para entender o concepto de encamiñamento en IP imos facer unha analoxía coas rotondas de tráfico onde, en función dos sinais de dirección, os coches encamíñanse por distintas estradas. As rotondas de tráfico serven, polo tanto, para:

1. Encamiñar o tráfico, grazas aos sinais que indican cara a onde están os destinos
2. Unir estradas de distintos tipos e velocidades. Por exemplo, unha vía rápida cunha estrada normal

De xeito similar, no ámbito das redes o encamiñamento permite dirixir o tráfico cara a outras estacións remotas ou destinos. A un router (tamén chamado encamiñador, porta de enlace ou *gateway*) chegan paquetes que serán encamiñados por unha ou outra liña en función da súa táboa de encamiñamento (os sinais da rotonda). Así como un condutor, para acadar o seu destino, pode atravesar moitas rotondas, un paquete, para acadar o seu destino, pode atravesar moitos routers, tal e como se ve na primeira figura deste tema.

Así, se un computador ten que enviar un datagrama a outro que non está na mesma rede IP ca el, debe enviar ese paquete ao router da súa rede. Esta é a razón pola que se configura unha porta de enlace no propio equipo. A porta de enlace estará na mesma rede que o equipo, é dicir, as direccións IP do equipo e a porta de enlace pertencen á mesma rede. Vexámolo cun exemplo:



No gráfico anterior temos catro redes (nunha delas faise *subnetting*) e dous routers. Cada computador ten que ter configurada unha porta de enlace á que enviar os paquetes que non vaian para a súa rede.

Táboas de encamiñamento

O routing lévase a cabo a partir de táboas de encamiñamento con información que permite a interconexión das distintas redes. Cada router ten unha táboa de encamiñamento. Asemade, cada equipo conectado a unha rede IP necesita unha táboa de encamiñamento para saber se unha determinada dirección está ou non na súa rede e enviar o paquete ao router en caso de que non sexa así. Unha táboa de encamiñamento ten o seguinte aspecto:

	Dirección	Máscara	Direccionador	Interfaz
1	147.83.153.5	255.255.255.255	127.0.0.1	*Loopback*
2	147.83.30.2	255.255.255.255	127.0.0.1	*Loopback*
3	127.0.0.0	255.0.0.0	127.0.0.1	*Loopback*
4	147.83.153.0	255.255.255.0	147.83.153.5	ether1
5	147.83.30.0	255.255.255.0	147.83.30.2	ether0
6	255.255.255.255	255.255.255.255	147.83.153.5	ether1
7	0.0.0.0	0.0.0.0	147.83.30.1	ether0

Esta táboa é dun router que conecta a rede 147.83.153.0/24 co exterior por medio da rede 147.83.30.0/24.

A **primeira**, **segunda** e **terceira** entrada permiten transmitir paquetes IP ás direccións 147.83.153.5, 147.83.30.2 e a todas as direccións que empecen por 127 (fixádevos na máscara das entradas). En ambos os tres casos os paquetes envíanse á interface virtual loopback. Ningún dos paquetes que se direccione con algunha destas tres regras sairá á rede.

A **cuarta** e **quinta** entrada serán adoptadas por todos os paquetes destinados ás rede 147.83.153.0 e 147.83.30.0, respectivamente.

A **sexta** entrada ten unha importancia relativa. Indícanos que os broadcasts IP restrinxiranse á rede local.

Na táboa anterior hai unha fila especial que permite que non se teñen que contemplar nunha táboa de encamiñamento todos os posibles destinos (tanto da intranet como de Internet, que sería imposible). É a dirección 0.0.0.0 ou dirección por defecto (default). Xa que calquera IP AND 0.0.0.0 vai dar 0.0.0.0, esa entrada sempre se debe poñer ó final da táboa.

Algoritmos de encamiñamento

Indican a forma en que se constrúe a táboa de encamiñamento dun router. Hai dous tipos:

- **Non adaptativos ou estáticos**: non se adaptan ás situacións cambiantes da rede (unha liña saturada, unha liña que cae, etc). Cando cheguen varios paquetes para o mesmo destino sempre os vai encamiñar polo mesmo sitio. Hai que configuralos manualmente. Equivalen a unha rotonda na que só hai sinais indicativas e onde non se sabe en que situación se atopan cada unha das saídas.
- **Adaptativos ou dinámicos**: adáptanse aos cambios e situacións da rede. Poden ser de tres tipos:
    - **Centralizados**, que equivalen á sala de control de tráfico dunha cidade onde teñen a información do que está a pasar en cada unha das rotondas, que rúas están saturadas, cales cortadas, etc. Con toda esa información elaboran as accións que deben levar a cabo cada un dos gardas de tráfico que están nas rotondas. Existe un nó central ao que cada router lle envía información (cal é a liña máis solicitada, de onde lle veñen paquetes devoltos, se ten enlace cos demais routers, etc). Con esa información o nó elabora a táboa de cada router e logo envíalla.
    - **Illados**, que equivalen a poñer un garda en cada rotonda e que este dirixa o tráfico como lle pete sen ter en conta nada de nada, nin se está saturada unha saída, se hai un incidente, etc.
    - **Distribuídos**. É onde se encadran os principais protocolos de enrutamento en TCP/IP (RIP v01 e v02, e OSPF). equivalen a ter gardas nas rotondas pero cada un comunícase cos gardas das rotondas próximas a el, deste xeito trata de tomar as decisións adaptándose ao que pasa ao seu arredor.

O comando route

O comando route permite establecer as regras de encamiñamento que serán consultadas polo noso equipo para decidir por que interface de rede enviar os paquetes coa finalidade de que cheguen ao seu destino. Para coñecer ditas regras execútase o seguinte comando:

```
route -n
```

Algunhas regras da táboa de encamiñamento configúranse automaticamente cando traballamos co comando ifconfig. A sintaxe do comando é a seguinte:

```
route add/del -net/host dirección_IP netmask máscara gw gateway dev interface_de_rede
```

Por exemplo, para que o noso equipo se poida comunicar cos equipos da rede 172.22.0.0/16 (net 172.22.0.0, netmask 255.255.0.0) supoñendo que o noso gateway sexa o 192.168.100.2 na interface eth3, teclearemos o seguinte comando:

```
route add -net 172.22.0.0 netmask 255.255.0.0 gw 192.168.100.2 dev eth3
```

O Address Resolution Protocol (ARP)

O ARP **é un protocolo do nivel de rede** encargado de traducir direccións IP a direccións MAC. Para entender por que é necesaria esta tradución hai que recordar que cada nivel da pila de protocolos engade información (cabeceiras) aos datos para poder desenvolver as súas funcións. Cando se transmite un paquete IP dende o nivel de rede ao nivel de enlace a trama do nivel de enlace que se constrúe contén, entre outros campos, a dirección MAC de orixe e a dirección MAC de destino. Para saber a MAC de orixe non hai problema, xa que está na propia tarxeta de rede do equipo, pero como sabe a estación que quere transmitir cal é a MAC de destino dunha IP determinada? Grazas ao ARP que mantén unha táboa que mapea as direccións IP do nivel de rede coas do nivel de enlace (direccións MAC). Devandita táboa denomínase **cache ARP**.

Paquetes ARP

O ARP baséase en dous únicos paquetes que **van encapsulados sobre tramas Ethernet**: a petición ARP e a resposta ARP.

A petición ARP

Este paquete (ARP-Request) equivale a preguntar: ?Pódeme dicir o computador con IP X.Z.Y.Z cal é a súa MAC?

Xa que logo, o paquete transporta a dirección IP da que se quere coñecer a dirección MAC. Levará como dirección de destino a dirección broadcast (FF:FF:FF:FF:FF:FF), deste xeito, todas as estacións locais da LAN procesarán esta trama. Con todo, só contestará a posuidora da dirección IP de destino.

Cando se coñece esta correspondencia IP<->MAC, o receptor da petición ARP tamén actualiza a súa caché ARP.

A resposta ARP

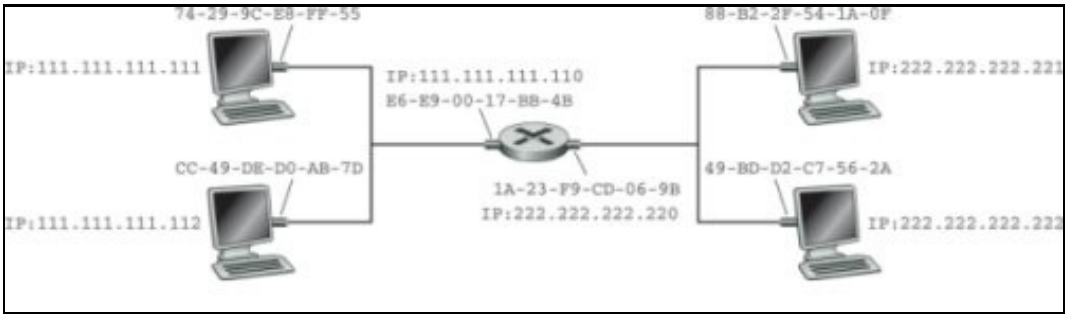
O outro paquete existente, ARP-Reply, é a resposta ARP que comunica a dirección MAC a quen a pediu (é o paquete resposta do anterior). É interesante observar como o formato deste paquete é case irrelevante, posto que o único interesante é a trama MAC e, en particular, a súa dirección de orixe.

Funcionamento

Cando efectuamos a transmisión dun paquete entre dúas estacións dunha mesma LAN, facémolo indicando as direccións IP dos equipos. A táboa ou caché ARP permite coñecer a correspondencia entre direccións IP e direccións MAC. Aínda que esta táboa pode modificarse manualmente (co comando arp), o máis normal é que ditas entradas se actualicen dinamicamente polo funcionamento do protocolo.

O ARP entra en funcionamento no momento en que o nivel de rede necesita transmitir un paquete IP destinado a unha dirección IP da que se descoñece a dirección MAC. Temos dúas situacións:

1. Se a dirección IP de destino está na mesma rede o computador correspondente enviará un ARP-Reply como resposta ao ARP-Request.
2. Se a dirección IP non está na mesma rede envíaselle o paquete ao router quen se encargará de transmitilo. Este paquete terá como dirección IP de destino a do equipo correspondente pero **a dirección MAC de destino será a do router**.



Os routers cortan o tráfico broadcast. Son como firewalls para este tipo de tráfico por iso crean un **dominio de broadcast** por cada interface que teñan, fronte as switches que crean un **dominio de colisión**, por cada porto que teñan. Na imaxe anterior, hai dous dominios de broadcast diferentes, un por cada interface do router.

O comando arp

O comando ARP permite manipular a cache ARP do computador. Para ver a táboa ARP hai que teclear:

```
arp -n
```

A opción -n amosa as direccións IP e non os nomes de dominio.

Para engadir unha entrada de forma estática hai que teclear o seguinte:

```
sudo arp -s <dir_ip> <dir_mac>
```

Para eliminala:

```
sudo arp -d <dir_ip>
```

O ICMP

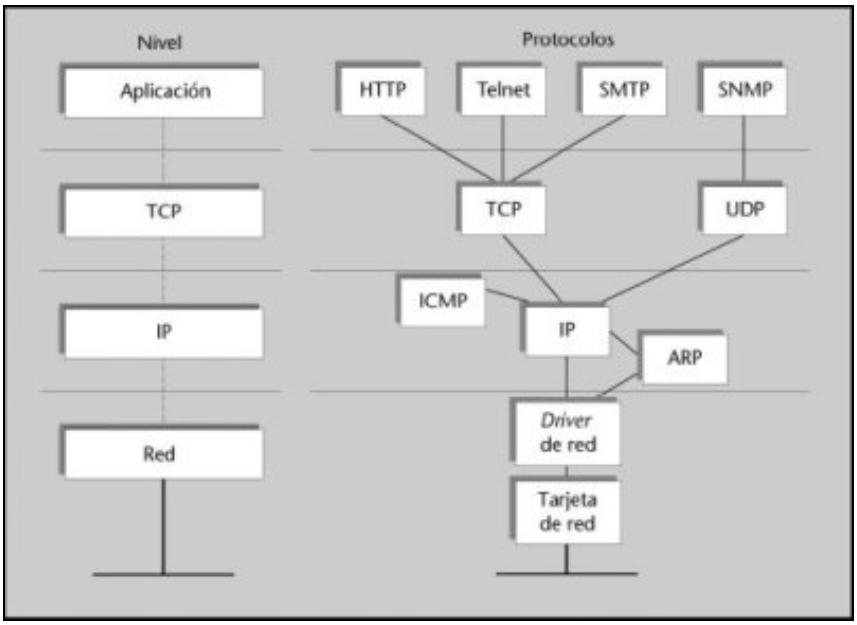
O Protocolo de Mensaxes de Control de Internet (*Internet Control Message Protocol* ou ICMP) está especificado no RFC 792 e proporciona un mecanismo para xestionar incidencias básicas nunha rede IP. Por exemplo: Se un datagrama co bit DF (*Don?t Fragment*) a 1 (é dicir, un paquete IP que non se pode fragmentar) non pode pasar por unha determinada rede, o router onde se produce o problema debe devolver unha mensaxe ao emisor indicándolle o acontecido.

Funcionamento

O ICMP pode verse como un protocolo específico da pila TCP/IP ou coma unha ferramenta que usa IP para notificar erros. De feito, o seu

funcionamento está baseado no intercambio de **mensaxes ICMP** que viaxan dentro de paquetes IP, encapsulados como se fosen datos (ao contrario do que acontecía con ARP que ten paquetes ARP específicos).

O campo *Protocolo* da cabeceira do paquete IP vale 1 se encapsula un paquete ICMP (consulta o formato do paquete IP). Recorda que IP pode encapsular outras PDU de niveis superiores, como TCP ou UDP. Neses casos o campo Protocolo vale 6, se encapsula TCP, e 17 se encapsula UDP.



As mensaxes ICMP xéraas o equipo que detecta o problema pero a quen llas envía? Pois ben, o paquete IP recibido ten na súa cabeceira a dirección IP de orixe, polo tanto, é a este equipo a quen se lle envían as mensaxes ICMP. As mensaxes ICMP inclúen un código de erro que facilita a identificación do problema. Existen trece tipos de mensaxes ICMP, cada unha cos seus propios códigos de erro, pero os máis importantes son os seguintes:

- **ECHO REQUEST** e **ECHO REPLY**. Úsanse para detectar se un equipo determinado está operativo. Ao recibir a mensaxe ICMP ECHO REQUEST o equipo responde coa mensaxe ICMP ECHO REPLY.
- **DESTINATION UNREACHABLE**. Xérase cando non se pode entregar o datagrama no seu destino, por exemplo: Datagramas co bit DF a 1 que non "collen" na MTU da rede pola que se enviaron; cando un router non atopa nas súas táboas ningunha ruta pola que poida chegar á dirección para a que vai dirixido un datagrama.
- **TIME EXCEEDED**. Envíase ao emisor unha mensaxe deste tipo cando se descarta un paquete porque o seu TTL (*Time to Live*) chegou a cero. Isto pode se síntoma de que se produciu algún bucle na rede, ou que o valor do TTL utilizado é demasiado baixo.
- **REDIRECT**. Utilízase para avisar ao emisor cando se sospeita de que un paquete se está a encamiñar incorrectamente. Por exemplo: Cando un router recibe dun equipo datagramas que van dirixidos a outro equipo que se atopa na mesma LAN.

A ferramenta `ping`

O programa ping proporciona información do tempo de ida e volta (*Round Trip Time* ou RTT) dun paquete, así como da porcentaxe de datagramas perdidos. Polo tanto permite coñecer con bastante facilidade o estado da rede nun intre determinado. O comando ping utiliza o protocolo ICMP enviando unha mensaxe ICMP do tipo 8 (petición de eco ou ECHO REQUEST) co destino indicado. O receptor da petición debe responder cunha resposta de eco, ECHO REPLY, que unha mensaxe ICMP de tipo 0. Cando ping a recibe, indica en pantalla que a estación está activa. Para executar o comando ping basta con escribir o seguinte:

```
ping nome_equipo
```

Para obter axuda sobre as opcións do comando pódese teclear `man ping` en Linux ou `ping /help` en Windows.

A ferramenta `traceroute`

Este programa permite atopar a ruta entre un equipo orixe e un destino. Utiliza un ocorrente mecanismo que se basea no uso de dúas mensaxes ICMP:

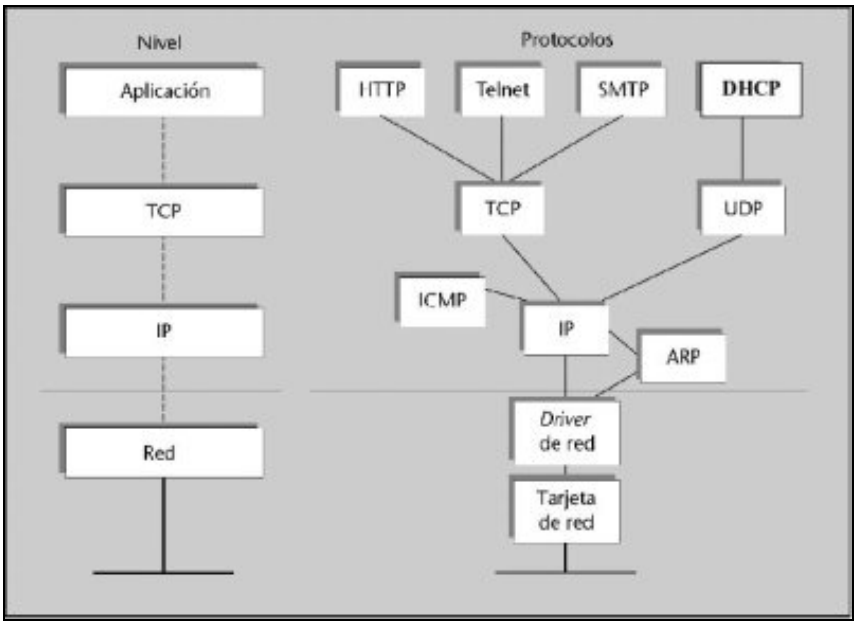
- **TIME EXCEEDED** (TTL superado). Cando un router recibe un paquete reduce nunha unidade o valor do campo TTL da cabeceira IP. O paquete elimínase se o valor é 0. Esta eliminación non é silenciosa, senón que o router responsable envía unha notificación da mesma ao orixinador do paquete por medio dunha mensaxe ICMP TIME EXCEEDED (tempo de vida esgotado). Este paquete ICMP contén a cabeceira do paquete IP que se eliminou e, polo tanto, a dirección do equipo que o envía.

- **UNREACHEABLE PORT** (porto inalcanzable). Para saber que se chegou ao destino, traceroute inclúe coa mensaxe ICMP (na versión de Linux vai nun paquete UDP) un intento de conexión a un porto da máquina que non contén ningún servizo, polo que a máquina de destino enviará unha mensaxe ICMP de porto inalcanzable.

O DHCP

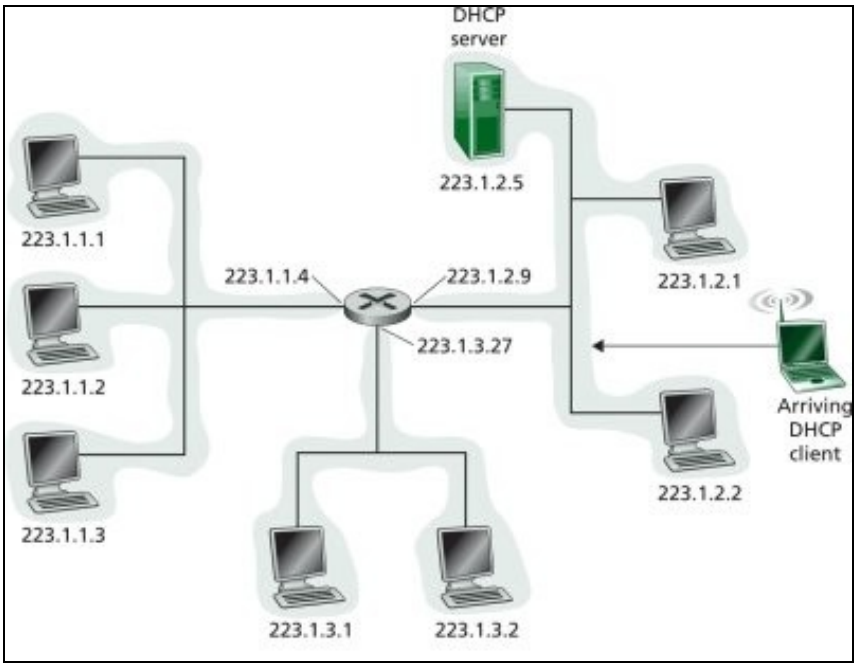
O *Dynamic Host Configuration Protocolo* (DHCP) está especificado no RFC 2131 . Este protocolo permite que un equipo nunha rede obteña unha dirección IP automaticamente, así como outra información importante como a súa máscara de rede, a dirección IP do seu encamiñador (gateway) e as direccións do seus DNS. Polo tanto, é o máis semellante a autoconfiguración en IPv4 (*plug-and-play*), polo que é moi interesante para simplificar as tarefas de administración da rede, que terían que facerse de xeito manual. Por iso, úsase amplamente en LAN domésticas, empresas, ISP, redes wifi, universidades, etc.

Foi deseñado no ano 1993 e complementa e mellora outros protocolos similares como RARP (*Reverse ARP*) e BOOTP.



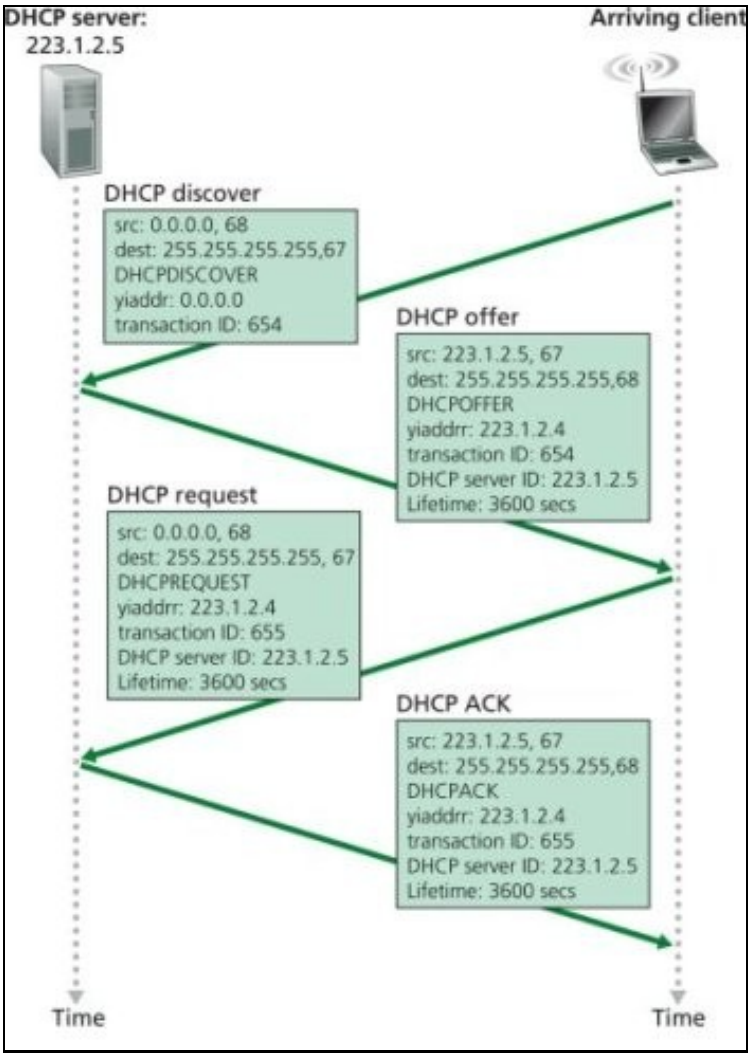
Funcionamento

DHCP está baseado na arquitectura cliente / servidor (como case todos os servizos de Internet), polo que debe existir un servidor DHCP (dhcpd) e un cliente DHCP para o seu funcionamento. No caso máis simple existirá un servidor DHCP na subrede ao cal o cliente solicitará a asignación da dirección IP. Se non existe tal servidor na subrede necesitarase un **axente DHCP de reenvío** (normalmente un router) que coñeza a dirección do servidor DHCP.



Como podemos ver na seguinte figura, o protocolo funciona en catro pasos:

1. DHCP discover
2. DHCP offer
3. DHCP request
4. DHCP ACK



DHCP pode configurarse para realizar a asignación dos parámetros aos equipos de distintas formas. Así, distinguimos tres tipos de asignación:

- **Asignación manual**. Neste modo de funcionamento DHCP compórtase como BOOTP. A asignación dos parámetros faise manualmente e cada vez que un equipo se conecte á rede asígnaselle automaticamente eses parámetros.
- **Asignación persistente**. Neste caso, a asignación tamén é automática e cada vez que o equipo se conecta a esa rede obtén a mesma dirección IP, con todo, non precisa que o administrador estableza unha configuración inicial dos parámetros.
- **Asignación dinámica** (aluguer de direccións). O cliente recibe a dirección IP do servidor durante un tempo limitado, pasado o cal o cliente debe renovar a súa solicitude ou a concesión expirará. Así, unha mesma dirección pode ser reutilizada por diferentes máquinas en momentos diferentes.

Un caso típico de uso de DHCP é nos provedores de acceso a Internet ou ISP. Por exemplo, se o ISP dá servizo a 2000 clientes e calcúlase que nunca haberá máis de 200 computadores simultaneamente conectados, en principio, poderiamos dar servizo cunha rede IP de clase C (254 direccións) e usando DHCP con asignación dinámica.

Clientes DHCP

En calquera momento podemos executar o cliente DHCP para renovar a nosa dirección IP:

- En GNU/Linux. Co comando `dhclient` renovamos a dirección IP. 1.Se se precisa borrar a configuración do cliente:

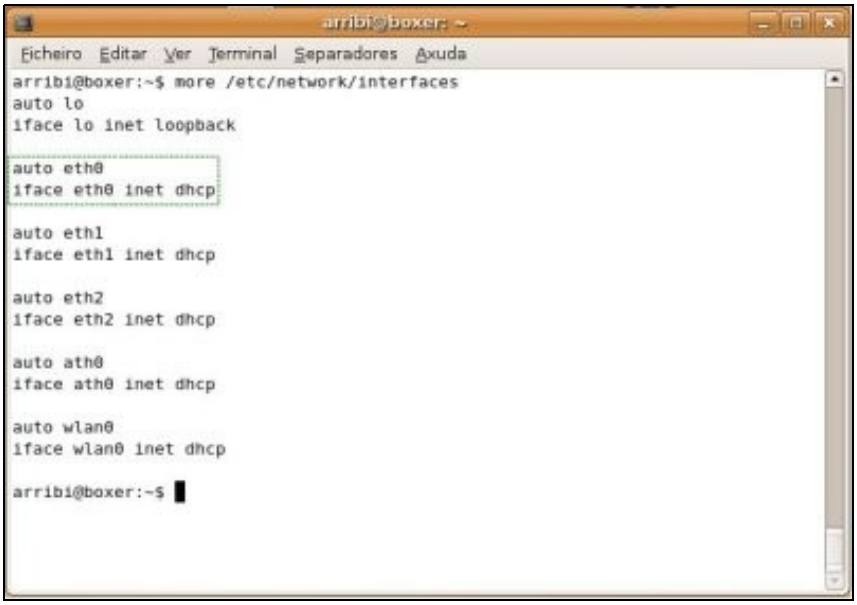
```
sudo dhclient -r
```

- En MS-Windows. Para borrar a IP actual:

```
ipconfig /release
ipconfig /renew. Renova a IP
```

En ambos casos, cando apaguemos o computador perderase a configuración. Se o que queremos é manter a configuración permanentemente para que o noso computador se conecte mediante DHCP sempre farémolo do seguinte xeito:

- **En modo gráfico**:
  - En GNU/Linux: Depende do contorno de escritorio que teñamos instalado. En Gnome: Sistema->Administración->Rede
  - En MS-Windows: En propiedades de rede pode seleccionarse asignación automática de dirección IP e DNS
- **En modo texto**. En GNU/Linux hai que editar o ficheiro /etc/network/interfaces tal e como se amosa na seguinte figura:



Inconvenientes de DHCP

Non todo son vantaxes. Entre os principais inconvenientes podemos destacar:

- **Problemas de trazabilidade**. Se se desexa rastrexar un problema e só se dispón da dirección IP resulta máis difícil (ás veces imposible) pescudar que computador ou usuario foi o causante do problema.
- **Inconsistencias cos nomes de dominio**. Outro problema que pode aparecer é a asociación de direccións e nomes no DNS. Coa asignación dinámica diferentes máquinas poden recibir o mesmo nome en diferentes momentos provocando inconsistencias. Este problema pode solventarse con programas como WinIP, DNS2GO, etc.

Anexo: Configuración da rede en Linux

Normalmente, a configuración da rede pode realizarse a través de aplicacións gráficas, como en MS-Windows. Con todo, neste apartado veremos como facelo desde a liña de comandos que é o método máis frecuente cando configuramos, por exemplo, un servidor. O seguinte aplícase ao sistema operativo Ubuntu, sendo moi similar para outras distribucións (Debian, OpenSuse, etc.).

Moitos dos aspectos de configuración relacionados coas interfaces de rede están no ficheiro `/etc/network/interfaces`. Se o computador non ten dispositivos ethernet este ficheiro só conterá a interface *loopback*, tal e como se amosa a continuación:

```
# Este ficheiro describe as interfaces de rede dispoñibles no sistema
# e como activalas. Para máis información: man interfaces.

# A interface de rede loopback
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Para ver o ficheiro de interfaces pódese teclear o seguinte:

```
more /etc/network/interfaces
```

Configuración mediante DHCP

Se o computador ten só un dispositivo ethernet, eth0, que se activa automaticamente ao arrincar o sistema e que se configura mediante un servidor DHCP, o ficheiro interfaces terá dúas liñas máis::

```
auto eth0
iface eth0 inet dhcp
```

A primeira liña indica que o dispositivo eth0 se activa automaticamente durante o arrinque do sistema. A segunda liña indica que a interface (?iface?) eth0 ten unha dirección IPv4. Se substituímos ?inet? con ?inet6? teríamos unha dirección IPv6. Se o servidor DHCP está correctamente configurado non se precisa facer nada máis para ter a rede funcionando. O servidor DHCP proporcionará o encamiñador por defecto (*gateway*), a dirección IP e os servidores DNS. Para editar o ficheiro interfaces pódese usar o editor de textos `nano` tecleando o seguinte:

```
nano /etc/network/interfaces
```

Para máis información sobre o `nano` consulta as páxinas de manual tecleando:

```
man nano
```

Tamén se poden configurar os parámetros anteriores mediante a ferramentas **dhclient** pero os cambios non se manterán se apagamos o computador.

Configuración manual

Se non temos un servidor DHCP hai que configurar os parámetros anteriores manualmente. O ficheiro `/etc/network/interfaces` úsano os scripts de configuración **ifup**/**ifdown** scripts. Tamén se poden configurar os parámetros anteriores mediante as ferramentas **ifconfig** e **route** pero os cambios non se manterán se apagamos o computador.

Direccións IP: o ficheiro `interfaces`

Supoñamos que queremos asignar a dirección IP 192.168.0.2 ao dispositivo eth1, cunha máscara natural 255.255.255.0. O encamiñador por defecto é o 192.168.0.1. Habería que editar o ficheiro `/etc/network/interfaces` para que incluíra o seguinte información:

```
iface eth1 inet static
        address 192.168.0.2
        netmask 255.255.255.0
        gateway 192.168.0.1
```

Servidor de nomes: o ficheiro `resolv.conf`

A continuación hai que especificar o servidor DNS cales serán os servidores DNS. Esta información está almacenada no ficheiro `/etc/resolv.conf`, que ten o seguinte aspecto:

```
search iessanclemente.net
nameserver 192.168.0.1
nameserver 4.2.2.2
```

A palabra **search** engade o dominio iessanclemente.net ás consultas para tentar resolver os nomes dentro da nosa rede. Por exemplo, se o noso dominio é iessanclemente.net e tentamos facer un ping ao equipo pc1 dentro da nosa rede, non será necesario teclear o nome completo, é dicir, ping pc1.iessanclemente.net, senón que automaticamente a consulta DNS será pc1.iessanclemente.net se tecleamos ping pc1. A palabra **nameserver** especifica os servidores DNS que se usarán para resolver nomes a direccións IP. Pode haber varios servidores DNS e consultaranse na orde especificada.

Se o servidor DNS se obtén dinamicamente mediante DHCP as entradas no ficheiro resolv.conf se sobrescribirán.

O ficheiro `hosts`

O ficheiro `/etc/hosts` contén direccións IP e os seus correspondentes nomes de equipo. Cando o computador tenta averiguar a dirección IP dun equipo primeiro acudirá a este ficheiro antes que ao servidor de nomes DNS. Xa que logo, se a dirección IP está no ficheiro `/etc/hosts` o DNS non se usará (isto pode cambiarse editando o ficheiro `/etc/nsswitch.conf`).

Se a nosa rede ten computadores con direccións IP que non están no DNS recoméndase engadilas ao ficheiro `/etc/hosts`.

Reinicio manual do servizo de rede

En calquera momento podemos reiniciar o servizo de rede tecleando o seguinte:

```
sudo /etc/init.d/networking restart
```

--Arribi 10:13 6 oct 2009 (BST)