Configuración del protocolo de red

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está por debajo de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua y un lugar donde vivir.

Los métodos que el ser humano ha utilizado para compartir ideas e información han cambiando a lo largo de la historia y están en constante evolución. Mientras que la red humana ha sido limitada a conversaciones cara a cara, el progreso de los medios ha ampliado el alcance de nuestras comunicaciones. Desde la prensa escrita hasta la televisión, cada nuevo avance ha mejorado la comunicación.

Como con cada avance en la tecnología de la comunicación, la creación y la interconexión de redes de datos sólidos tiene un efecto profundo y han permitido que el ser humano realice de forma más eficiente su trabajo facilitando que las empresas exijan día a día mayores retos a los que los desarrollan. De esta forma, se ha llegado a alternativas de gran impacto a través del tiempo como el correo electrónico, Internet, televisión por cable, etc.

Redes de área local

Las infraestructuras de red pueden variar mucho en los siguientes aspectos:

* Tamaño del área cubierta
* Cantidad de usuarios conectados
* Cantidad y tipo de servicios disponibles

LAN : acrónimo del inglés *local area network* o red de área local.

Una red individual cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Este tipo de red se denomina **red de área local** (LAN). Como norma general, una LAN está administrada por una única organización. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el ámbito de red.

Internet

Aunque el uso de una LAN aporta beneficios, la mayoría de usuarios necesita comunicarse con recursos de otras redes fuera de la organización local.

Los ejemplos de este tipo de comunicación incluyen:

* Enviar un correo electrónico a un amigo de otro país
* Acceder a noticias o productos de un sitio web
* Obtener un archivo del ordenador del vecino
* Enviar un mensaje instantáneo a un familiar de otra ciudad
* Seguir una actividad de un equipo deportivo con el teléfono móvil.

Internetwork

Una malla global de redes interconectadas (*Internetworks*) cubre estas necesidades de comunicación humanas. Algunas de estas redes interconectadas pertenecen a grandes organizaciones públicas o privadas como agencias gubernamentales o empresas industriales, y están reservadas para su uso exclusivo.

La *Internetwork* más conocida, ampliamente utilizada ya la que accede el público en general es Internet.

Internet se crea por la interconexión de redes que pertenecen a los proveedores de servicios de Internet (ISP). Estas redes ISP se conectan entre ellas para proporcionar acceso a millones de usuarios en todo el mundo. Garantizar la comunicación efectiva por medio de esta infraestructura diversa requiere la aplicación de tecnologías y protocolos consistentes y reconocidos comúnmente, así como la cooperación de muchas agencias de administración de redes.

protocolos

Toda comunicación, cara a cara o por una red, está regida por reglas predeterminadas denominadas *protocolos*.

Estos protocolos son específicos de las características de la conversación. En nuestras comunicaciones personales cotidianas, las reglas que aplicamos para comunicarnos utilizando un medio, como el teléfono, no son necesariamente las mismas que los protocolos que se utilizan en un medio diferente, como escribir una carta.

Una *suite* de protocolos es un conjunto de protocolos de comunicación que implementan la pila ( *stack* ) de protocolos de las redes en que se ejecutan.

El éxito de la comunicación entre los *hosts* de una red requiere la interacción de una gran cantidad de protocolos diferentes. Un grupo de protocolos interrelacionados que son necesarios para llevar a cabo una función de comunicación se denomina **suite de protocolos**. Estos protocolos se implementan en el software y en el hardware que está cargado en cada *host* y dispositivo de red.

Las *suites* de protocolos de *networking* describen procesos como los siguientes:

* El formato o estructura del mensaje.
* El método por el cual los dispositivos de *networking* comparten información sobre rutas con otras redes.
* Cómo y cuándo se pasan los mensajes de error y del sistema entre dispositivos.
* El inicio y el final de las sesiones de transferencia de datos.
* Los protocolos individuales de una *suite* de protocolos pueden ser específicos de un fabricante o de propiedad exclusiva. En este contexto, *propietario* significa que una compañía o proveedor controla la definición del protocolo y cómo funciona.
* Uno de los protocolos más comunes es el protocolo de Internet (IP, del inglés *Internet Protocol*). IP es responsable de tomar segmentos de datos, encapsularse en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta para enviar los datos al *host* de destino.

Modelo TCP / IP

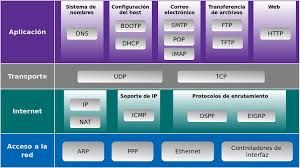
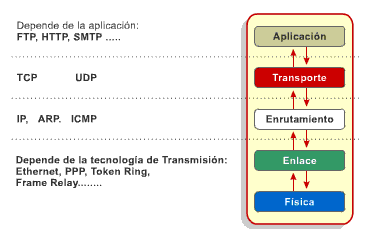
El primer modelo de protocolo en capas para la comunicación de *Internetworks* se creó al principio de la década de los setenta y se conoce con el nombre de *modelo de Internet*. Define cuatro categorías de funciones que deben tener lugar para que las comunicaciones tengan éxito. La arquitectura de la *suite* de protocolos TCP / IP sigue la estructura de este modelo. Por esta razón, es común que el modelo de Internet se conozca como *modelo TCP / IP* (véase la [figura .1](file:///E:\ElLago_2019_20\SistemasInformaticos\Sistemas%20inform%C3%A1ticos_WEB_Catalan\WebContent\u4\a2\continguts.html#Figure10) ).

Cuando una compañía no controla la definición de un protocolo, se denomina un estándar abierto.

La gran mayoría de los modelos de protocolos describen una pila de protocolos específicos del proveedor. Sin embargo, el modelo TCP / IP es un estándar abierto: no hay una compañía que controle la definición del modelo. Las definiciones del estándar y los protocolos TCP / IP se explican en un foro público y se definen en un conjunto de documentos disponibles para el público. Estos documentos se denominan *solicitudes de comentarios* ( RFC ). Contienen las especificaciones formales de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC también contienen documentos técnicos y organizacionales sobre Internet, incluyendo las especificaciones técnicas y los documentos de las políticas producidos por el grupo de trabajo de ingenieros de Internet (IETF).

**Figura** Modelo TCP IP



Proceso de comunicación

El modelo TCP / IP describe la funcionalidad de los protocolos que forman la *suite* de protocolos TCP / IP. Estos protocolos, que se implementan tanto en el *host* emisor como en el receptor, interactúan para entregar aplicaciones de extremo a extremo utilizando la Red.

Un proceso completo de comunicación incluye estos pasos:

1. Creación de datos en la capa de aplicación del dispositivo de origen.
2. Segmentación y encapsulación de datos cuando pasan por la pila de protocolos en el dispositivo de origen.
3. Generación de los datos sobre el medio en la capa de acceso a la Red.
4. Transporte de los datos para la Red, que está formada por los medios y cualquier dispositivo intermediario.
5. Recuperación de los datos en la capa de acceso a la Red del dispositivo de destino.
6. Desencapsulació y rearme de los datos al pasar por la pila en el dispositivo final.
7. Traspaso de estos datos a la aplicación de destino correspondiente a la capa de aplicación del dispositivo de destino.

Direccionamiento en la Red

El modelo TCP/IP describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la Red. Un flujo de datos que se envía desde un origen a un destino se puede dividir en partes y entrelazar con los mensajes que viajan desde otros *hosts* hasta otros destinos. Miles de millones de estas partes de información viajan por una red en cualquier momento. Es muy importante que cada parte de los datos contenga información de identificación suficiente para llegar al destino correcto.

Hay diferentes tipos de direcciones que se deben incluir para entregar satisfactoriamente los datos desde una aplicación de origen que se ejecuta en un *host* hasta la aplicación de destino correcto que se ejecuta en el otro. Al utilizar el modelo TCP / IP como guía, se pueden observar diferentes direcciones e identificadores necesarios en cada capa.

Los protocolos de capa 2 del modelo TCP / IP están diseñados principalmente para mover datos desde una red local a otra dentro de una *Internetwork* o por Internet. Las direcciones de capa 2 deben incluir identificadores que permitan a dispositivos de red intermediarios ubicar los *hosts* en diferentes redes. En la *suite* de protocolos TCP / IP, cada dirección IP de *host* contiene información sobre la red en la que está ubicado el *host*.

En los límites de cada red local, un dispositivo de red intermediario, generalmente un router, desencapsula la trama para leer la dirección *host* de destino situada en la cabecera del paquete, la PDU (*unidad de datos de protocolo*  de capa 2. Los routers utilizan la porción del identificador de red de esta dirección para determinar la ruta a utilizar para llegar al *host* de destino. Una vez se ha determinado la ruta, el router vuelve a encapsular el paquete en una nueva trama y la envía por su trayecto hasta el dispositivo final. Cuando la trama llega al destino, la trama y las cabeceras del paquete se eliminan y los datos se envían a las capas superiores.

Protocolos de capa 2 de TCP / IP

La capa de Internet debe proveer de un mecanismo para dirigir los dispositivos finales de origen y de destino. Si las secciones individuales de datos deben dirigirse a un dispositivo final, éste debe tener una dirección única.

En una red IPv4, cuando esta dirección se agrega a un dispositivo, el dispositivo se denomina *host*.

Los protocolos implementados en la capa de Internet que llevan datos de usuario son:

* versión 4 del protocolo de Internet (IPv4)
* versión 6 del protocolo de Internet (IPv6)
* intercambio novel de paquetes de *Internetwork* (IPX)
* AppleTalk
* servicio de red sin conexión (CLNS / usando DECNet).

Los protocolos de Internet (IPv4 e IPv6) son los protocolos de transporte de datos de capa 2 utilizados más ampliamente y, concretamente, el IPv4 será el que se tratará en este módulo.

direccionamiento IPv4

Cada dispositivo de red se debe definir de manera exclusiva. En la capa de Internet es necesario identificar los paquetes de la transmisión con direcciones de origen y de destino de los sistemas finales. En IPv4, esto significa que cada paquete tiene una dirección de origen de 32 bits y una dirección de destino de 32 bits.

Estas direcciones se utilizan en las redes de datos como patrones binarios. Dentro de los dispositivos, se aplica la lógica digital para su interpretación. Para los que formamos parte de la red humana, una serie de 32 bits es difícil de interpretar y recordar, por tanto, representamos las direcciones IPv4 utilizando el formato decimal punteado.

Conversión binaria / decimal

Para comprender el funcionamiento de un dispositivo en una red, es necesario considerar las direcciones y otros datos de la manera en que lo hace un dispositivo: en notación binaria. Esto significa que es necesario ser hábil en la conversión de binario a decimal.

Los datos representados en el sistema binario pueden representar muchas formas diferentes de datos en la red humana. En este tema, haremos referencia al sistema binario por estar relacionado con el direccionamiento IPv4.

**Notación de posición**

El Aprendizaje de la notación de posición para convertir binario a decimal requiere una comprensión de los fundamentos matemáticos de un sistema de numeración llamado notación de posición. Notación de posición significa que un dígito representa diferentes valores según la posición que ocupa. Más específicamente, el valor que un dígito representa es el valor multiplicado por la potencia de la base o raíz representado por la posición que el dígito ocupa. Para ayudar a entender esto, vamos a ver algunos ejemplos:

Para el número decimal 245, el valor que el 2 representa es 2 \* 10 ^ 2 (2 multiplicado por 10 elevado a la segunda potencia). El 2 se encuentra en lo que comúnmente llamamos la posición "100".

Usando la notación de posición en el sistema de numeración en base 10, 245 representa:

245 = (2 \* 10 ^ 2) + (4 \* 10 ^ 1) + (5 \* 10 ^ 0)

o

245 = (2 \* 100) + (4 \* 10) + (5 \* 1)

**Sistema de numeración binaria**

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa potencias incrementadas de 2. En números binarios de 8 bits, las posiciones representan estas cantidades:

2 ^ 7 2 ^ 6 2 ^ 5 2 ^ 4 2 ^ 3 2 ^ 2 2 ^ 1 2 ^ 0

o, lo que es lo mismo:

128 64 32 16 8 4 2 1

El sistema de numeración de base 2 tiene solamente dos dígitos: 0 y 1.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esta posición representa si el dígito es 1 y no se obtiene la cantidad si el dígito es 0.

1 1 1 1 1 1 1 1

128 64 32 16 8 4 2 1

Un 1 en cada posición significa que el valor para esta posición se añade al total. Si tenemos el número binario 11111111, obtendremos su valor decimal realizando la suma de:

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Un 0 en cada posición indica que el valor para esta posición no se suma al total. Un 0 en cada posición produce un total de 0. Es decir, el valor binario 00000000 equivale a sumar:

128 64 32 16 8 4 2 1

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

Ejemplo: ¿Qué valor tiene el octeto binario 10010110?

128 \* 1 + 64 \* 0 + 32 \* 0 + 16 \* 1 + 8 \* 0 + 4 \* 1 + 2 \* 1 + 1 \* 0 = 150

Es decir, podemos afirmar que 10010110 en binario, equivale al valor 150 en formato decimal.

**Tabla**Tabla de conversión decimal / binario

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Decimal / Binario** |  |  |  |  |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 1 | 0 |
| 3 | 0 | 0 | 1 | 1 |
| 4 | 0 | 1 | 0 | 0 |
| 5 | 0 | 1 | 0 | 1 |
| 6 | 0 | 1 | 1 | 0 |
| 7 | 0 | 1 | 1 | 1 |
| 8 | 1 | 0 | 0 | 0 |
| 9 | 1 | 0 | 0 | 1 |
| 10 | 1 | 0 | 1 | 0 |
| 11 | 1 | 0 | 1 | 1 |
| 12 | 1 | 1 | 0 | 0 |
| 13 | 1 | 1 | 0 | 1 |
| 14 | 1 | 1 | 1 | 0 |
| 15 | 1 | 1 | 1 | 1 |

punto decimal

Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se dice octeto debido a que cada número decimal representa un byte u 8 bits.

Por ejemplo, la dirección IPv4 de un *host* de red en formato binario es el siguiente:

10101100000100000000010000010100

Si dividimos la dirección en bytes mediante puntos obtendremos:

10101100.00010000.00000100.00010100

En formato decimal punteado, sólo hay que traducir cada octeto en formato decimal, por lo que se obtiene un resultado como el siguiente:

10101100 = 172

00010000 = 16

00000100 = 4

00010100 = 20

Por tanto, la dirección IPv4 en formato decimal punteado se representaría así:

172.16.4.20

Porciones de red y de host

Cada dirección IPv4 tiene una porción que representa la parte de red y una porción que representa la parte de *host* . En la capa 2, se define una red como un grupo de *hosts* con patrones de bits idénticos a la porción de red. Por ejemplo, en la dirección 192. 168. 2. 6, la parte de red estaría definida por los tres primeros octetos, y la parte de *host* para el último.

* Dirección de red. Parte de la dirección IP en la que se hace referencia en la red
* Direcciones de *host*. Parte de la dirección IP asignada a los dispositivos finales de la red. Cada dispositivo final necesita una dirección única para enviar datos a otra red.

Dentro del rango de direcciones IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit en la porción de *host* de la dirección.

**Máscara de red**

Para poder identificar correctamente qué parte de la dirección IPv4 pertenece a la red y qué pertenece al *host* utiliza una tira de 32 bits que siempre acompañan la dirección IPv4 y que se denomina *máscara de red*. Cada uno de estos bits debe estar asignado a 1 si la parte equivalente de la dirección IPv4 pertenece a la red, ya 0 si pertenece al *host*. Por ejemplo:

Dirección IPv4 en binario:

10101100000100000000010000010100

Máscara IPv4 en binario:

11111111111111110000000000000000

Como se puede ver, los dieciséis primeros bits de la máscara de red están establecidos a 1, con lo que los dieciséis primeros bits de la dirección IP identifican la red en que se encuentra el *host* , y los últimos dieciséis bits representan el *host* en concreto.

Si traducimos de bits a decimal obtendremos:

Dirección IPv4 en decimal:

172.16.4.20

Máscara IPv4 en decimal:

255.255.0.0

Por lo tanto, los dos primeros octetos de la dirección de la red (172.16.) Representan la red, y los dos últimos el *host* (04:20).

La máscara de red se puede representar de dos maneras diferentes: el formato tradicional con cuatro bytes que tienen 1 binario en la parte de red y 0 binario en la parte de *host*. ejemplo:

255.0.0.0

255.255.0.0

255.255.255.0

O se puede especificar la longitud del prefijo, que es la cantidad de bits de la máscara que identifica la parte de red (forma resumida). ejemplo:

* **255. 0. 0. 0** se representa como **/ 8** (8 bits).
* **255. 255. 0. 0** se representa como **/ 16** (16 bits).
* **255. 255. 255. 0** se representa como **/ 24** (24 bits).

Por ejemplo, en la dirección 10. 6. 7. 11 con máscara 255. 0. 0. 0, podemos decir que el primer octeto identifica la red (10. 0. 0. 0) y los últimos tres bytes identifican el *host*. En la dirección 192. 168. 11. 27/24, podemos decir que los primeros tres bytes identifican la red (192. 168. 11. 0) y el último octeto identifica el *host*.

Tipo de direcciones IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

* **Dirección de red**: la dirección en la que se hace referencia en la red.
* **Dirección de broadcast**: una dirección especial utilizada para enviar datos a todos los hosts de la red.
* **Direcciones host**: las direcciones asignadas a los dispositivos finales de la red tales como PCs, PDAs, impresoras en red, etc.

**Dirección de red**

La dirección de red es una manera estándar de hacer referencia a una red. Por ejemplo: se podría hacer referencia a la una red como "red 10. 0. 0. 0". Esta es una forma mucho más conveniente y descriptiva de referirse a la red que utiliza un término como "la red del primer piso". Todos los hosts de la red 10. 0. 0. 0 tendrán los mismos bits de red.

Dentro del rango de direcciones IPv4 de una red, la dirección más baja se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección.

**Dirección de broadcast**

La dirección de broadcast es una dirección especial para permitir la comunicación a todos los host en esta red. Para enviar datos a todos los hosts de una red, un host puede enviar un solo paquete dirigido a la dirección de broadcast de la red.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Esta es la dirección en la que los bits de la porción de host son todos 1. Para la red 10. 0. 0. 0, la dirección de broadcast sería 10. 255. 255. 255.

**Direcciones host**

Como habéis visto anteriormente, cada dispositivo final requiere una dirección única para enviar un paquete a un host concreto. En las direcciones IPv4, se asignan los valores entre la dirección de red y la dirección de broadcast a los dispositivos en esta red.

**Ejemplo**

Tenemos la red 172. 16. 0. 0/16. ¿Cuál sería la dirección de red? ¿Cuál la de broadcast? ¿Qué direcciones podríamos asignar a los hosts?

* Dirección de red: 172. 16. 0. 0
* Dirección de broadcast: 172. 16. 255. 255
* Rango de direcciones asignables: 172. 16. 0. 1 a 172. 16. 255. 254

Clases IPv4

Históricamente, la RFC1700 agrupaba rangos de de direcciones IPv4 en tamaños específicas denominadas direcciones de clase A, de clase B y de clase C. También definía a las direcciones de clase D (multicast) y de clase E (experimentales).

Las direcciones de clases A, B y C definían redes de tamaños específicas, así como bloques de direcciones específicos para estas redes. De esta forma, se asignaban a compañías u organizaciones todo un bloque de direcciones de clase A, clase B o clase C. Este uso de espacio de dirección es denominado *direccionamiento con clase*.

**tabla**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Clases de direcciones** | **Rango primer octeto** | **Partes de red y de host** | **Máscara por defecto** | **Número de redes y de hosts totales** |
| A | 1-127 | XHHH | 255.0.0.0 | 128 redes / 16777214 hosts |
| B | 128-191 | XXHH | 255.255.0.0 | 16.384 redes / 65.534 hosts |
| C | 192-223 | XXXH | 255.255.255.0 | 2.097.150 redes / 254 hosts |

Bloques de clase A

Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo/8 fijo, donde el primer byte indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host.

Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que sólo había 128 redes de clase A posibles, de 0. 0. 0. 0/8 a 127. 0. 0. 0/8, antes de excluir los bloques de direcciones reservadas. Aunque las direcciones de clase A reservaban la mitad del espacio de direcciones, debido al límite de 128 redes, sólo podían ser asignadas a aproximadamente 120 compañías u organizaciones.

Bloques de clase B

El espacio de direcciones de clase B fue diseñado para satisfacer las necesidades de las redes de tamaño moderado a grande con más de 65.000 hosts. Una dirección IP de clase B utilizaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las direcciones de host. Al igual que con la clase A, había que reservar espacio de direcciones para las clases de direcciones restantes.

Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran 10. De esta forma, se restringía el bloque de direcciones para la clase B a 128. 0. 0. 0/16 hasta 191. 255. 0. 0/16. La clase B tenía una asignación de direcciones un poquito más eficiente que la clase A ya que dividía equitativamente el 25% del total del espacio de direcciones IPv4 entre aproximadamente 16.000 redes.

Bloques de clase C

El espacio de direcciones de clase C era la clase de direcciones antiguas más utilizadas. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts.

Los bloques de direcciones de clase C utilizaban el prefijo/24. Esto significaba que una red de clase C sólo utilizaba el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red.

Los bloques de direcciones de clase C reservaban espacio de direcciones para la clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringió el bloque de direcciones para la clase C de 192.0.0.0/24 a 223.255.255.0/24. Aunque ocupaba sólo el 12.5 % del total del espacio de direcciones IPv4, podía suministrar direcciones a 2 millones de redes.

Limitaciones del sistema basado en clases

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. La asignación con clase de espacio de direcciones menudo desperdiciaba muchas direcciones, lo que agotaba la disponibilidad de direcciones IPv4. Por ejemplo: una compañía con una red con 260 hosts necesitaría que se le asignara una dirección de clase B con más de 65.000 direcciones ya que una clase C (máximo 254 hosts) se hacía pequeña.

Aunque este sistema con clase no fue abandonado hasta finales de la década del 90, es posible ver restos de estas redes en la actualidad. Por ejemplo: en asignar una dirección IPv4 a un host, el sistema operativo examina la dirección que se está asignando para determinar si es de clase A, clase B o clase C. Después, el sistema operativo adopta el prefijo utilizado para esta clase y realiza la asignación de la máscara de subred adecuada.

Direcciones IPv4 públicas y privadas

**InterNIC ...**

fue el primer organismo gubernamental encargado de las direcciones IP y nombres de dominio. Actualmente, de estas funcionalidades, se encarga la ICANN (del inglés Internet Corporation for Assigned Names and Numbers, Corporación de Internet para la Asignación de Nombres y Números).

Aunque la mayoría de direcciones IPv4 de *host* son direcciones públicas designadas para el uso en redes a las que se accede desde Internet, hay bloques de direcciones que se utilizan en redes que requieren acceso a Internet o no. Estas direcciones se denominan *direcciones privadas*.

Las direcciones públicas son designadas por InterNIC (del inglés *Internet Network Information Center*) y están compuestas por identificadores de red basados en clases o bloques que son universalmente únicos para Internet.

direcciones privadas

Las direcciones privadas son direcciones utilizadas para redes internas. Estas direcciones están definidas en el documento RFC -1918. No son encaminables en Internet.

Los bloques de direcciones privadas son:

* Desde 10. 0. 0. 0 a 10. 255. 255. 255 (red 10. 0. 0. 0/8)
* Desde 172. 16. 0. 0 a 172. 31. 255. 255 (red 172. 16. 0. 0/16)
* Desde 192. 168. 0. 0 a 192. 168. 255. 255 (red 192. 168. 0. 0/24)

En nuestro caso, habitualmente trabajaremos con direcciones privadas, ya que son las que podemos asignar a los *hosts* de la red. Las direcciones públicas son asignadas habitualmente por nuestro ISP (del inglés *Internet service provider*, proveedor de servicios de Internet).

Direccionamiento estático o dinámico para dispositivos de usuario final

A la hora de configurar el direccionamiento de la capa 2, se puede utilizar un direccionamiento estático (configurado manualmente) o dinámico (configurado utilizando un servidor específico). En este apartado, podrá aprender las características de cada uno de estos métodos.

Direccionamiento para dispositivos de usuario

Es necesario que la asignación de direcciones IP en una red esté bien diseñada. En la mayoría de redes de datos, la mayoría de *hosts* incluye dispositivos finales como PC, teléfonos IP, impresoras y organizadores personales o PDA ( *personal digital assistant* ). Por este motivo, se asignarán a estos dispositivos la mayoría de direcciones IPv4.

Las direcciones IP se pueden asignar de forma estática o dinámica.

Asignación estática de direcciones IPv4

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un *host* concreto, tal y como puede ver en la [figura .4](file:///E:\ElLago_2019_20\SistemasInformaticos\Sistemas%20inform%C3%A1ticos_WEB_Catalan\WebContent\u4\a2\continguts.html#Figure13) . Como mínimo, esto implica ingresar la dirección IP del *host* y su máscara de red. Además, se puede configurar la pasarela (*gateway*) por defecto y los servidores DNS.

La pasarela se utiliza para acceder a otras redes externas a la nuestra y, típicamente, contiene la dirección de la interfaz interna del router que conecta con Internet. Los servidores DNS permiten resolver nombres de *host* ( [www. Iuego. Cat](http://www.ioc.cat) ) en la dirección IP correspondiente (85. 192. 111. 244).

Las direcciones estáticas tienen ciertas ventajas en comparación con las direcciones dinámicas. Por ejemplo, resultan útiles para impresoras, servidores y otros dispositivos que hay que identificar de la misma manera a cada momento. Si normalmente los *hosts* acceden a un servidor utilizando una dirección IP en particular, podrían aparecer ciertos problemas si se modificaba la dirección. Por otro lado, asignar direcciones manualmente puede hacer que los recursos de una red se controlen más. Sin embargo, es posible que para hacer esta configuración de cada *host* sea necesario más tiempo.

Al hacer el direccionamiento IP estático, se debe mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Estas deben ser las direcciones permanentes y normalmente no se pueden volver a utilizar en ningún otro *host*.

Asignación dinámica de direcciones IPv4

Debido a la complejidad asociada a la administración de direcciones estáticas, los dispositivos de usuarios finales suelen incluir direcciones asignadas dinámicamente. Para lograr esto, se utiliza un protocolo llamado **DHCP** (*Dynamic Host Configuration Protocol* o protocolo de configuración dinámica de *host* ).

El DHCP permite la asignación automática de información de direccionamiento como la dirección IP, la máscara de red, la pasarela o *gateway* por defecto y otra información de configuración. La configuración del servidor DHCP requiere que se defina un bloque de direcciones para ser asignado a los clientes DHCP en una red. Las direcciones asignadas a este bloque deben planificarse de manera que se excluyan las utilizadas para otros tipos de dispositivos como impresoras o servidores, los cuales deben tener una dirección IP estática.

Generalmente, el DHCP es el método preferido para asignar direcciones IP a los *hosts* de grandes redes, ya que reduce en gran parte la carga del personal de apoyo a la red y prácticamente elimina los errores de entrada.

Otro beneficio del DHCP es que no se asigna una dirección a un *host* de manera permanente, sino que sólo se alquila o presta durante un tiempo determinado. Si un *host* se apaga o se desconecta en la red, la dirección asignada devuelve al conjunto de direcciones disponibles del servidor DHCP y puede volver a ser utilizada. Esta configuración es muy útil para usuarios móviles que constantemente entran y salen de la red.