

## INTRODUCCIÓN

En la actualidad el direccionamiento basado en direcciones IP versión 4 se han ido agotando y más aun con la adopción de las nuevas tecnologías como son los dispositivos móviles y las redes de Área personal, en la cual toda persona requiere de cuando menos 4 a 5 direcciones IP lo que ha ocasionado que en poco tiempo más colapse toda la infraestructura de red de las empresas proveedoras de internet y hosting para el mismo.

IPv6 ya no es un protocolo en fase de diseño y experimentación. Tras años de inversión en la creación de backbones, todas las ventajas que introduce este nuevo protocolo (espacio virtualmente ilimitado de direcciones, seguridad a nivel de red, movilidad, multicast) aparecen disponibles ante un mundo que todavía no deja de sorprenderse por el impacto de una tecnología, IPv4, que fue concebida en los años 60 con unos objetivos muy distintos de aquellos a los cuales sirve en la actualidad.

La mayoría de sistemas operativos están preparados para el nuevo protocolo y la emigración al mismo no debería suponer problemas al usuario final. No obstante, desde el punto de vista del profesional existe aún cierto recelo a la introducción de esta nueva tecnología, temor que con este trabajo pretendemos disipar describiendo esta sencilla propuesta para la introducción de IPv6 en una compleja red. En nuestra opinión, la convergencia tecnológica a medio plazo hacia el nuevo protocolo IPv6 es inevitable. En este contexto las universidades y demás centros de investigación deberían desplegar servicios de red como apoyo a la docencia y la investigación, constituyéndose así como un seminario ideal para la innovación y experimentación con tecnologías que en un futuro no lejano se encontrara integradas plenamente en el resto de la sociedad.

Miles de dispositivos móviles surgen día tras día con un único objetivo; que podamos estar conectados a la red en cualquier momento y desde cualquier lugar.

Así la compañía de encuestas e Investigación Internacional (IDC) señala que más de 260 millones de personas tienen actualmente acceso a internet. Cifra que se elevara, puesto que cada segundo ingresan siete usuarios nuevos a internet. A las puertas de tamaño de revolución, la pregunta obligada es: ¿está preparado internet para todo esto?, dar cabida a más usuarios y dispositivos. Ese es el reto al que se enfrenta actualmente internet y que ha dado lugar a su revisión y renovación.

Los organismos encargados de velar por el correcto funcionamiento de la red impulsaron en 1994 un debate conocido como IP Next Generation. El objetivo no era otro que encontrar una nueva arquitectura un nuevo internet que hiciese frente a las necesidades de la Sociedad de la información.

El resultado de esta investigación y los estudios realizados sobre el IPv6, ha dado como resultado al “Internet del nuevo milenio”.

El nuevo protocolo de comunicación representa un paso más allá, una clara y necesaria evolución de IPv4, el estándar que se utiliza actualmente y que tras 20 años de vida, se ha visto desbordado por el crecimiento de la red.

IPv4 tiene una historia de gran éxito, con cerca de 200 millones de usuarios alrededor del mundo. Los cimientos de tan exitosa industria no pueden ser cambiados de la noche a la mañana. El cambio solo puede hacerse gradualmente, y con extremo cuidado para evitar cualquier impacto del tráfico vía IPv4.

En referencia a lo expuesto anteriormente con el nivel actual en el desarrollo del protocolo una de las áreas que mayor preocupación está teniendo es la creación de aplicaciones IPv6 y también la migración de aplicaciones desde IPv4 a IPv6, es por esto que el proyecto de investigación será un aporte a los esfuerzos globales por hacer de la implementación definitiva de IPv6 una realidad.

El requisito de seguridad en el nivel de IP, requiere un medio público como internet requiere servicios de cifrado que impidan que los datos enviados se

puedan ver o modificas durante el transito Aunque en la actualidad existe un estándar que proporciona seguridad para los paquetes IPv4 denominados IPSec, este estándar es opcional y prevalece las soluciones propietarias.

En base a lo anteriormente expuesto en el trabajo de investigación se ha planteado el estudio de este novedoso tema en 3 capítulos los mismos que se encuentran desarrollados de la siguiente manera:

En el capítulo I se realiza un análisis de todos los conceptos que se van a tratar dentro del trabajo de investigación tomando como fuente principal el internet y la bibliografía actualizada que cuenta la Universidad.

En el capítulo II está la investigación de campo basado en fuentes bibliográficas, las entrevistas y encuestas tanto a directivos de la empresa como a empleados técnicos y los clientes que son el motor fundamental de toda empresa.

En el Capítulo III de la investigación, la compatibilidad con el tráfico en tiempo real depende del campo Tipo de servicio (ToS, Type of Service) de IPv4 y la identificación de la carga, que suele utilizar un puerto UDP o TCP. Por desgracia, el campo tiene una funcionalidad limitada y diferentes interpretaciones.

Por todas estas razones es que se ha desarrollado investigaciones como la presente para ser un aporte en el desarrollo de protocolos y estándares IP versión 6 ya que esta incorpora los conceptos de muchos métodos propuestos para la actualización del protocolo IPv4 a IPv6, está diseñado con la intención de reducir al mínimo el impacto en los protocolos de nivel superior e inferior al evitar la adición arbitraria de nuevas características.

Finalmente la investigación cuenta con conclusiones y recomendaciones que pueden ser de gran ayuda para las futuras promociones de la Universidad.

## CAPITULO I

### 1 FUNDAMENTACION TEÓRICA SOBRE USO DE HERRAMIENTAS DE COMUNICACIÓN.

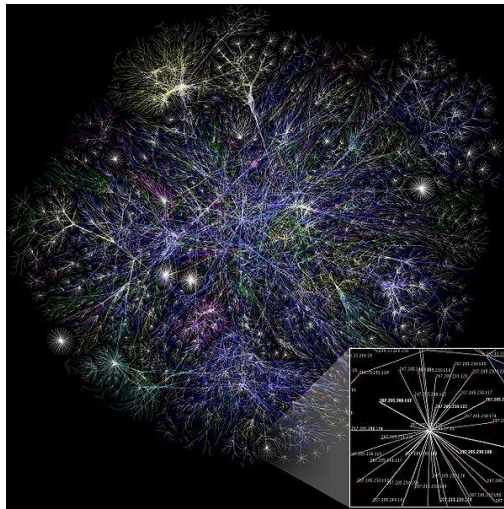
#### 1.1 INTERNET

**Internet** es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencia, la transmisión de contenido y comunicación multimedia -telefonía (VoIP), televisión (IPTV)-, los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea.

**Gráfico 1.1.:** El Internet



**Fuente:** [http://es.wikipedia.org/wiki/Archivo:Internet\\_map\\_1024.jpg](http://es.wikipedia.org/wiki/Archivo:Internet_map_1024.jpg)

### **1.1.1 Antecedentes**

Sus orígenes se remontan a la década de 1960, dentro de ARPA (hoy DARPA), como respuesta a la necesidad de esta organización de buscar mejores maneras de usar los computadores de ese entonces, pero enfrentados al problema de que los principales investigadores y laboratorios deseaban tener sus propios computadores, lo que no sólo era más costoso, sino que provocaba una duplicación de esfuerzos y recursos.<sup>5</sup> Así nace ARPANet (Advanced Research Projects Agency Network o Red de la Agencia para los Proyectos de Investigación Avanzada de los Estados Unidos), que nos legó el trazado de una red inicial de comunicaciones de alta velocidad a la cual fueron integrándose otras instituciones gubernamentales y redes académicas durante los años 70.

Investigadores, científicos, profesores y estudiantes se beneficiaron de la comunicación con otras instituciones y colegas en su rama, así como de la posibilidad de consultar la información disponible en otros centros académicos y de investigación. De igual manera, disfrutaron de la nueva habilidad para publicar y hacer disponible a otros la información generada en sus actividades.

En el mes de julio de 1961 Leonard Kleinrock publicó desde el MIT el primer documento sobre la teoría de conmutación de paquetes. Kleinrock convenció a Lawrence Roberts de la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red. El otro paso fundamental fue hacer dialogar a los ordenadores entre sí. Para explorar este terreno, en 1965, Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida.

- 1969: La primera red interconectada nace el 21 de noviembre de 1969, cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, y gracias a los trabajos y estudios anteriores de varios científicos y organizaciones desde 1959 (*ver: Arpanet*). El mito de que ARPANET, la primera red, se construyó simplemente para sobrevivir a ataques nucleares sigue siendo muy popular. Sin embargo, este no fue el único motivo. Si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables, tal y como se atestigua en la siguiente cita:

A raíz de un estudio de RAND, se extendió el falso rumor de que ARPANET fue diseñada para resistir un ataque nuclear. Esto nunca fue cierto, solamente un estudio de RAND, no relacionado con ARPANET, consideraba la guerra nuclear en la transmisión segura de comunicaciones de voz. Sin embargo, trabajos posteriores enfatizaron la robustez y capacidad de supervivencia de grandes porciones de las redes subyacentes. (Internet Society, A Brief History of the Internet)<sup>1</sup>

- 1972: Se realizó la Primera demostración pública de ARPANET, una nueva red de comunicaciones financiada por la DARPA que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva

---

<sup>1</sup> Tomado de: [www.monografias.com/internet/arpanet.html](http://www.monografias.com/internet/arpanet.html)

arquitectura sirvió para que, en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

- 1983: El 1 de enero, ARPANET cambió el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet. Por otra parte, se centró la función de asignación de identificadores en la IANA que, más tarde, delegó parte de sus funciones en el Internet registry que, a su vez, proporciona servicios a los DNS.
- 1986: La NSF comenzó el desarrollo de NSFNET que se convirtió en la principal *Red en árbol* de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.
- 1989: Con la integración de los protocolos OSI en la arquitectura de Internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En 1990 el CERN crea el código HTML y con él el primer cliente World Wide Web. En la imagen el código HTML con sintaxis coloreada.

En el CERN de Ginebra, un grupo de físicos encabezado por Tim Berners-Lee creó el lenguaje HTML, basado en el SGML. En 1990 el mismo equipo construyó el primer cliente Web, llamado WorldWideWeb (WWW), y el primer servidor web.

A inicios de los 90, con la introducción de nuevas facilidades de interconexión y herramientas gráficas simples para el uso de la red, se inició el auge que actualmente le conocemos al Internet. Este crecimiento masivo trajo consigo el surgimiento de un nuevo perfil de usuarios, en su mayoría de personas comunes no ligadas a los sectores académicos, científicos y gubernamentales.

Esto ponía en cuestionamiento la subvención del gobierno estadounidense al sostenimiento y la administración de la red, así como la prohibición existente al uso comercial del Internet. Los hechos se sucedieron rápidamente y para 1993 ya se había levantado la prohibición al uso comercial del Internet y definido la transición hacia un modelo de administración no gubernamental que permitiese, a su vez, la integración de redes y proveedores de acceso privados.

- 2006: El 3 de enero, Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la Red aumentará a 2.000 millones.

El resultado de todo esto es lo que experimentamos hoy en día: la transformación de lo que fue una enorme red de comunicaciones para uso gubernamental, planificada y construida con fondos estatales, que ha evolucionado en una miríada de redes privadas interconectadas entre sí. Actualmente la red experimenta cada día la integración de nuevas redes y usuarios, extendiendo su amplitud y dominio, al tiempo que surgen nuevos mercados, tecnologías, instituciones y empresas que aprovechan este nuevo medio, cuyo potencial apenas se comienza a descubrir.

### **1.1.2 Definición**

Internet tiene un impacto profundo en el mundo laboral, el ocio y el conocimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo de esto es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) por ejemplo GNU, Linux, Mozilla y OpenOffice.org.



Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos. En este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano, el espacio virtual es actualizado constantemente de información, fidedigna o irrelevante.

### **1.1.3 Importancia**

Inicialmente el Internet tenía un objetivo claro. Se navegaba en Internet para algo muy concreto: búsquedas de información, generalmente. Ahora quizás también, pero sin duda algún hoy es más probable perderse en la red, debido al inmenso abanico de posibilidades que brinda. Hoy en día, la sensación que produce Internet es un ruido, una serie de interferencias, una explosión de ideas distintas,

de personas diferentes, de pensamientos distintos de tantas posibilidades que, en ocasiones, puede resultar excesivo. El crecimiento o más bien la incorporación de tantas personas a la red hace que las calles de lo que en principio era una pequeña ciudad llamada Internet se conviertan en todo un planeta extremadamente conectado entre sí entre todos sus miembros. El hecho de que Internet haya aumentado tanto implica una mayor cantidad de relaciones virtuales entre personas. Es posible concluir que cuando una persona tenga una necesidad de conocimiento no escrito en libros, puede recurrir a una fuente más acorde a su necesidad. Como ahora esta fuente es posible en Internet. Como toda gran revolución, Internet augura una nueva era de diferentes métodos de resolución de problemas creados a partir de soluciones anteriores. Algunos sienten que Internet produce la sensación que todos han sentido sin duda alguna vez; produce la esperanza que es necesaria cuando se quiere conseguir algo. Es un despertar de intenciones que jamás antes la tecnología había logrado en la población mundial. Para algunos usuarios Internet genera una sensación de cercanía, empatía, comprensión y, a la vez, de confusión, discusión, lucha y conflictos que los mismos usuarios consideran la vida misma.

## **1.2 PROTOCOLOS**

En el campo de las telecomunicaciones, un protocolo de comunicaciones es el conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación. Un ejemplo de un protocolo de comunicaciones simple adaptado a la comunicación por voz es el caso de un locutor de radio hablando a sus radioyentes.

Los protocolos de comunicación para la comunicación digital por redes de computadoras tienen características destinadas a asegurar un intercambio de datos fiable a través de un canal de comunicación imperfecto. Los protocolos de comunicación siguen ciertas reglas para que el sistema funcione apropiadamente.

Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma. El protocolo TCP/IP fue creado para las comunicaciones en Internet. Para que cualquier computador se conecte a Internet es necesario que tenga instalado este protocolo de comunicación.

- Estrategias para mejorar la seguridad (autenticación, cifrado).
- Cómo se construye una red física.
- Cómo los computadores se conectan a la red.

Si bien los protocolos pueden variar mucho en propósito y sofisticación, la mayoría especifica una o más de las siguientes propiedades:

- Detección de la conexión física subyacente (con cable o inalámbrica), o la existencia de otro punto final o nodo.
- *Handshaking*.
- Negociación de varias características de la conexión.
- Cómo iniciar y finalizar un mensaje.
- Procedimientos en el formateo de un mensaje.
- Qué hacer con mensajes corruptos o formateados incorrectamente (corrección de errores).
- Cómo detectar una pérdida inesperada de la conexión, y qué hacer entonces.
- Terminación de la sesión y/o conexión

En el campo de las redes informáticas, los protocolos se pueden dividir en varias categorías, una de las clasificaciones más estudiadas es la OSI.

Según la clasificación OSI, la comunicación de varios dispositivos ETD se puede estudiar dividiéndola en 7 niveles, que son expuestos desde su nivel más alto hasta el más bajo:<sup>2</sup>

**Gráfico 1.2.:** Capas del modelo OSI

<i>Nivel</i>	<i>Nombre</i>	<i>Categoría</i>
<i>Capa 7</i>	Nivel de aplicación	Aplicación
<i>Capa 6</i>	Nivel de presentación	
<i>Capa 5</i>	Nivel de sesión	
<i>Capa 4</i>	Nivel de transporte	
<i>Capa 3</i>	Nivel de red	Transporte
<i>Capa 2</i>	Nivel de enlace de datos	de datos
<i>Capa 1</i>	Nivel físico	

**Fuente:** Las Tesistas

- A su vez, esos 7 niveles se pueden subdividir en dos categorías, las capas superiores y las capas inferiores. Las 4 capas superiores trabajan con problemas particulares a las aplicaciones, y las 3 capas inferiores se encargan de los problemas pertinentes al transporte de los datos.
- Otra clasificación, más práctica y la apropiada para TCP/IP, podría ser esta:

**Gráfico 1.3.:** Capas del Modelo TCP

<i>Nivel</i>
<i>Capa de aplicación</i>
<i>Capa de transporte</i>
<i>Capa de red</i>
<i>Capa de enlace de datos</i>
<i>Capa física</i>

**Fuente:** Las Tesistas

<sup>2</sup> **Tomado de:** Curso de Cisco CCNA 1 Exploration

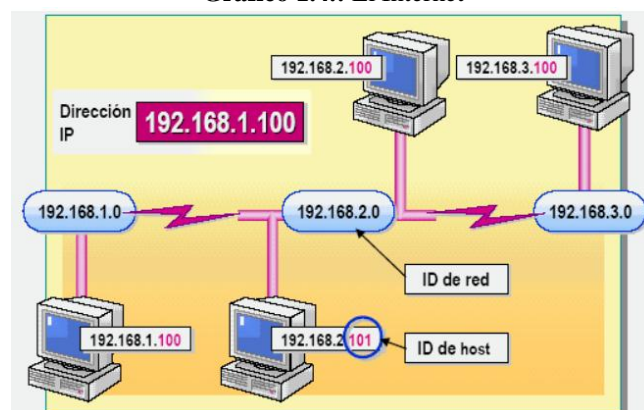
Los protocolos de cada capa tienen una interfaz bien definida. Una capa generalmente se comunica con la capa inmediata inferior, la inmediata superior, y la capa del mismo nivel en otros computadores de la red. Esta división de los protocolos ofrece abstracción en la comunicación

Una aplicación (capa nivel 7) por ejemplo, solo necesita conocer cómo comunicarse con la capa 6 que le sigue, y con otra aplicación en otro computador (capa 7). No necesita conocer nada entre las capas de la 1 a la 5. Así, un navegador web (HTTP, capa 7) puede utilizar una conexión Ethernet o PPP (capa 2) para acceder a la Internet, sin que sea necesario cualquier tratamiento para los protocolos de este nivel más bajo. De la misma forma, un router sólo necesita de las informaciones del nivel de red para enrutar paquetes, sin que importe si los datos en tránsito pertenecen a una imagen para un navegador web, un archivo transferido vía FTP o un mensaje de correo electrónico

### 1.3 DIRECCIONAMIENTO IP (INTERNET PROTOCOL)

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que aplicaremos cuando proporcionemos direcciones IP a los equipos y otros hosts de nuestra red.

Gráfico 1.4.: El Internet



Fuente: [www.mundomagico.com/internet.htm](http://www.mundomagico.com/internet.htm)

La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comuniquen mediante TCP/IP.

La dirección IP identifica la ubicación de un equipo en la red, al igual que el número de la dirección identifica una casa en una ciudad. Al igual que sucede con la dirección de una casa específica, que es exclusiva pero sigue ciertas convenciones, una dirección IP debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255.<sup>3</sup>

### **Componentes de una dirección IP**

Al igual que la dirección de una casa tiene dos partes (una calle y un código postal), una dirección IP también está formada por dos partes: el ID de host y el ID de red. **ID de red** La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo.

Todos los equipos del mismo segmento deben tener el mismo ID de red, al igual que las casas de una zona determinada tienen el mismo código postal. **ID de host** La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

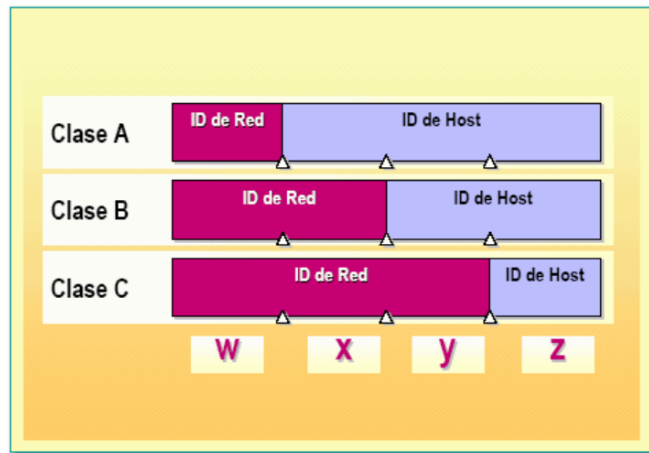
El ID de cada host debe ser exclusivo en el ID de red, al igual que la dirección de una casa es exclusiva dentro de la zona del código postal.

Es importante observar que al igual que dos zonas de código postal distinto pueden tener direcciones iguales, dos equipos con diferentes IDs de red pueden tener el mismo ID de host. Sin embargo, la combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí.

---

<sup>3</sup> **Tomado de:** Curso de Cisco CCNA 1 Exploration

**Gráfico 1.6.:** Direccionamiento IPv4.



Fuente: [www.mundomagico.com/ipv4.html](http://www.mundomagico.com/ipv4.html)

Las clases de direcciones se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones también se utilizan para definir el punto de división entre el ID de red y el ID de host.

Se asigna a una organización un bloque de direcciones IP, que tienen como referencia el ID de red de las direcciones y que dependen del tamaño de la organización. Por ejemplo, se asignará un ID de red de clase C a una organización con 200 hosts, y un ID de red de clase B a una organización con 20.000 hosts.

### **Clase A**

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

### **Clase B**

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red.

Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

### Clase C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

### Clases D y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.<sup>4</sup>

### Determinación de la clase de dirección

El direccionamiento IP en clases se basa en la estructura de la dirección IP y proporciona una forma sistemática de diferenciar IDs de red de IDs de host. Existen cuatro segmentos numéricos de una dirección IP. Una dirección IP puede estar representada como  $w.x.y.z$ , siendo  $w$ ,  $x$ ,  $y$  y  $z$  números con valores que oscilan entre 0 y 255. Dependiendo del valor del primer número,  $w$  en la representación numérica, las direcciones IP se clasifican en cinco clases de direcciones como se muestra en la siguiente tabla:

**Gráfico 1.7.:** Valores de las direcciones IP en rangos

Clase de dirección IP	Dirección IP	ID de red	Valores de $w$
A	$w.x.y.z$	$w.0.0.0$	1 - 126*
B	$w.x.y.z$	$w.x.0.0$	128 - 191
C	$w.x.y.z$	$w.x.y.0$	192 - 223
D	$w.x.y.z$	No disponible	224 - 239
E	$w.x.y.z$	No disponible	240 - 255

\*El ID de red 127.0.0.0 está reservado para las pruebas de conectividad.

**Fuente.:** las Tesistas

<sup>4</sup> **Tomado de:** Curso de Cisco CCNA 1 Exploration



## **Determinación de los ID de red y de host**

En las direcciones IP de clase A, el ID de red es el primer número de la dirección IP. En la clase B, el ID de red son los dos primeros números; y en la clase C, el ID de red son los tres primeros números de la dirección IP. Los números restantes identifican el ID de host.

El ID de red tiene una estructura de cuatro números al igual que la dirección IP. Por tanto, si el primer número,  $w$ , de una dirección IP representa el ID de red, la estructura del ID de red es  $w.0.0.0$ , siendo 0 los tres números restantes. La estructura del ID de host es  $x.y.z$ . Observe que el host no va precedido de un 0.

Por ejemplo, la dirección IP 172.16.53.46 sería una dirección de clase B ya que  $w=172$  y está entre 128 y 191. El ID de red sería 172.16.0.0 y el ID de host 53.46 (sin punto al final).

## **SUBDIVISIÓN DE UNA RED**

Podemos ampliar una red utilizando dispositivos físicos, como routers y puentes, para añadir segmentos de red. También podemos utilizar dispositivos físicos para dividir una red en segmentos más pequeños para incrementar la eficacia de la red.

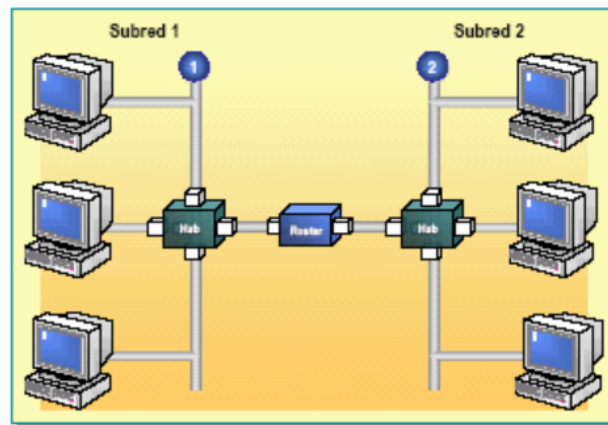
Los segmentos de red separados por routers se denominan *subredes*. Cuando creamos subredes, debemos dividir el ID de red para los hosts de las subredes. La división del ID de red utilizado para comunicarse en Internet en IDs de red más pequeños (en función del número de direcciones IP identificadas) para una subred se denomina *subdivisión* de una red.

Para identificar el nuevo ID de red de cada subred, debemos utilizar una máscara de subred para especificar qué parte de la dirección IP va a ser utilizada por el nuevo ID de red de la subred. Podemos localizar un host en una red analizando su ID de red.

Los IDs de red coincidentes muestran qué hosts se encuentran en la misma subred. Si los IDs de red no son los mismos, sabremos que están en distintas subredes y que necesitaremos un router para establecer comunicación entre ellos.<sup>5</sup>

## SUBREDES

Gráfico 1.8.: Subredes



Fuente.: Las Tesistas

A medida que crece el número de equipos y el volumen de tráfico en una red Ethernet, se produce un crecimiento de la colisión de datos y se reduce el rendimiento de la red. Para solucionar este problema, los equipos de una red Ethernet se agrupan juntos en divisiones físicas, denominadas segmentos, separadas por un dispositivo físico, como un router o un puente.

En un entorno TCP/IP, los segmentos separados por routers se denominan subredes. Todos los equipos que pertenecen a una subred tienen el mismo ID de red en sus direcciones IP. Cada subred debe tener un ID de red distinto para comunicarse con otras subredes. Basándose en el ID de red, las subredes definen las divisiones lógicas de una red. Los equipos que se encuentran en distintas subredes necesitan comunicarse a través de routers.<sup>6</sup>

<sup>5</sup> Tomado de: Curso de Cisco CCNA 1 Exploration

<sup>6</sup> Tomado de: Curso de Cisco CCNA 3 Navigation

## MÁSCARAS DE SUBRED

**Gráfico 1.9.:** Valores de las subredes en las mascarar

Dirección IP	10.50.100.	200
Máscara de subred	255.255.255.	0
ID de red	10.50.100.	0

**Fuente:** Las Tesistas

En el método de direccionamiento en clases, el número de redes y hosts disponibles para una clase de dirección específica está predeterminado. En consecuencia, una organización que tenga asignado un ID de red tiene un único ID de red fijo y un número de hosts específico determinado por la clase de dirección a la que pertenezca la dirección IP.

Con el ID de red único, la organización sólo puede tener una red conectándose a su número asignado de hosts. Si el número de hosts es grande, la red única no podrá funcionar eficazmente. Para solucionar este problema, se introdujo el concepto de subredes.

Las subredes permiten que un único ID de red de una clase se divida en IDs de red de menor tamaño (definido por el número de direcciones IP identificadas). Con el uso de estos múltiples IDs de red de menor tamaño, la red puede segmentarse en subredes, cada una con un ID de red distinto, también denominado ID de subred.

### **Estructura de las máscaras de subred**

Para dividir un ID de red, utilizamos una máscara de subred. Una máscara de subred es una pantalla que diferencia el ID de red de un ID de host en una dirección IP pero no está restringido por las mismas normas que el método de

clases anterior. Una máscara de subred está formada por un conjunto de cuatro números, similar a una dirección IP.

El valor de estos números oscila entre 0 y 255.

En el método de clases, cada uno de los cuatro números sólo puede asumir el valor máximo 255 o el valor mínimo 0. Los cuatro números están organizados como valores máximos contiguos seguidos de valores mínimos contiguos. Los valores máximos representan el ID de red y los valores mínimos representan el ID de host. Por ejemplo, 255.255.0.0 es una máscara de subred válida, pero 255.0.255.0 no lo es. La máscara de subred 255.255.0.0 identifica el ID de red como los dos primeros números de la dirección IP.

### **Máscaras de subred predeterminadas**

En el método de clases, cada clase de dirección tiene una máscara de subred predeterminada. La siguiente tabla lista las máscaras de subred predeterminadas para cada clase de dirección.

**Gráfico 1.10.:** Valores de la Máscara de subred

<b>Clase de dirección IP</b>	<b>Dirección IP</b>	<b>Máscara de subred</b>	<b>ID de red</b>	<b>ID de host</b>
A	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z
B	w.x.y.z	255.255.0.0	w.x.0.0	x.y
C	w.x.y.z	255.255.255.0	w.x.y.0	z

**Fuente:** Las tesis

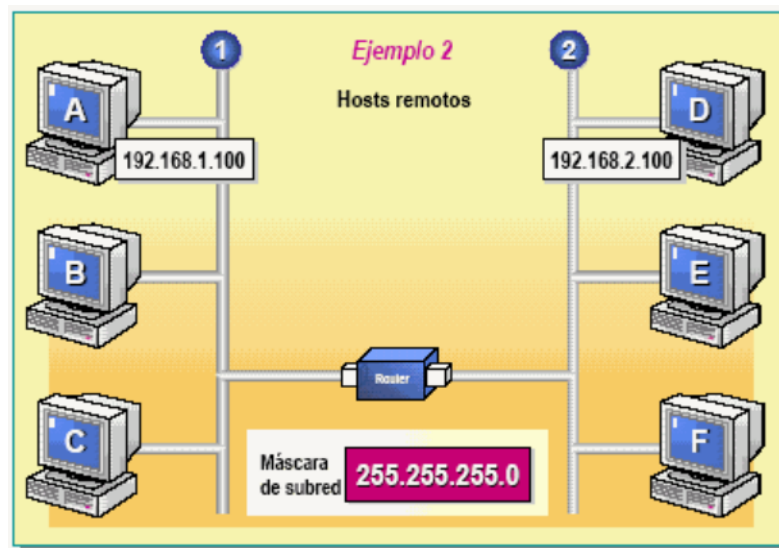
### **Máscaras de subred personalizadas**

Cuando dividimos un ID de red existente para crear subredes adicionales, podemos utilizar cualquiera de las máscaras de subred anteriores con cualquier

dirección IP o ID de red. Así, la dirección IP 172.16.2.200 podría tener la máscara de subred 255.255.255.0 y el ID de red 172.16.2.0 o la máscara de subred predeterminada 255.255.0.0 con el ID de red 172.16.0.0. Esto permite a una organización dividir en subredes un ID de red de clase B existente 172.16.0.0 en IDs de red más pequeños para que coincida con la configuración real de la red.

## DETERMINACIÓN DE HOSTS LOCALES Y REMOTOS

**Gráfico 1.11.:** Subneteo con concentradores compartidos



**Fuente:** Las tesis

Después de que el ID de red de un host ha sido identificado, es fácil determinar si otro host es local o remoto respecto a él. Para ello, comparamos los IDs de red de ambos hosts. Si coinciden, los dos hosts se encuentran en la misma subred. Si no coinciden, significa que los hosts se encuentran en distintas subredes y es necesario un router para transmitir datos entre ellos.

### Ejemplo 1

Supongamos los dos equipos A y B con las direcciones IP 192.168.1.100 y 192.168.2.100 y una máscara de subred 255.255.0.0. Como se muestra en la

siguiente tabla, los IDs de red de sus direcciones IP coinciden. Por tanto, los equipos A y B son locales.

**Gráfico 1.12.:** Configuraciones de la red

	<b>Equipo A</b>	<b>Equipo B</b>
Dirección IP	192.168.1.100	192.168.2.100
Máscara de subred	255.255.0.0	255.255.0.0
ID de red	<b>192.168.0.0</b>	<b>192.168.0.0</b>

**Fuente.:** Los Tesistas

## Ejemplo 2

Otro ejemplo serían los equipos A y D con las direcciones IP 192.168.1.100 y 192.168.2.100 y una máscara de subred 255.255.255.0. Los IDs de red de estas direcciones IP no coinciden, como muestra la siguiente tabla. Por tanto, el equipo A es remoto respecto al equipo D.

**Gráfico 1.13.:** Ids de red

	<b>Equipo A</b>	<b>Equipo D</b>
Dirección IP	192.168.1.100	192.168.2.100
Máscara de subred	255.255.255.0	255.255.255.0
ID de red	<b>192.168.1.0</b>	<b>192.168.2.0</b>

**Fuente.:** Las tesistas

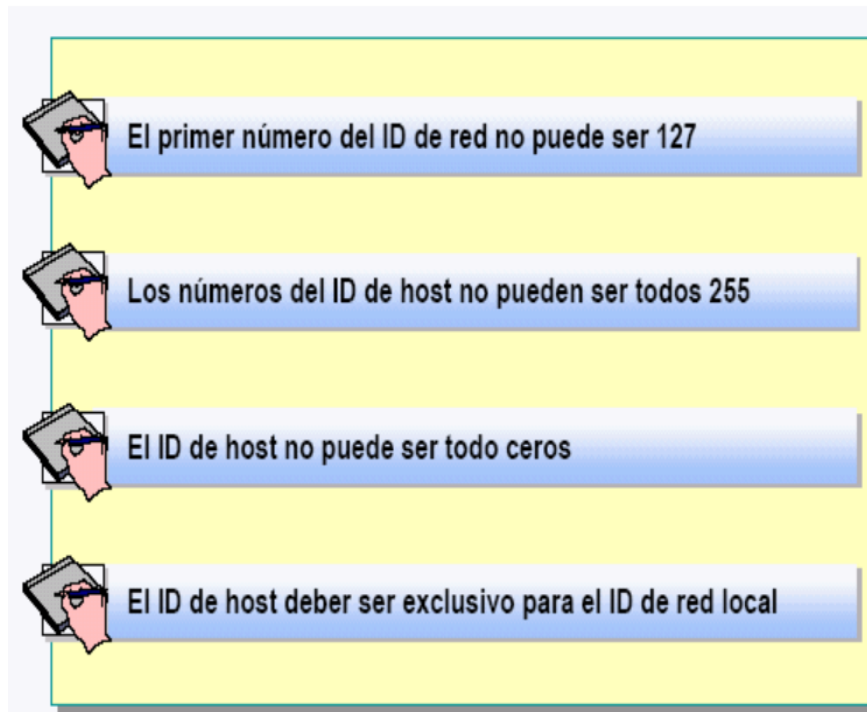
## PLANIFICACIÓN DEL DIRECCIONAMIENTO IP

Una vez establecida una red, todos los equipos que se encuentran en ella necesitan una dirección IP; parecido a las viviendas de un edificio, que necesitan direcciones asignadas a ellas. Sin una dirección IP, un equipo no recibe los datos que van dirigidos a él. Y al igual que las direcciones de una vivienda, el formato de la dirección IP debe seguir ciertas directrices para garantizar que los datos se transmiten al equipo correcto.

Esta sección explica las directrices para asignar IDs de red y de host.

## DIRECTRICES DE DIRECCIONAMIENTO

Gráfico 1.14.: Direccionamiento IPv4



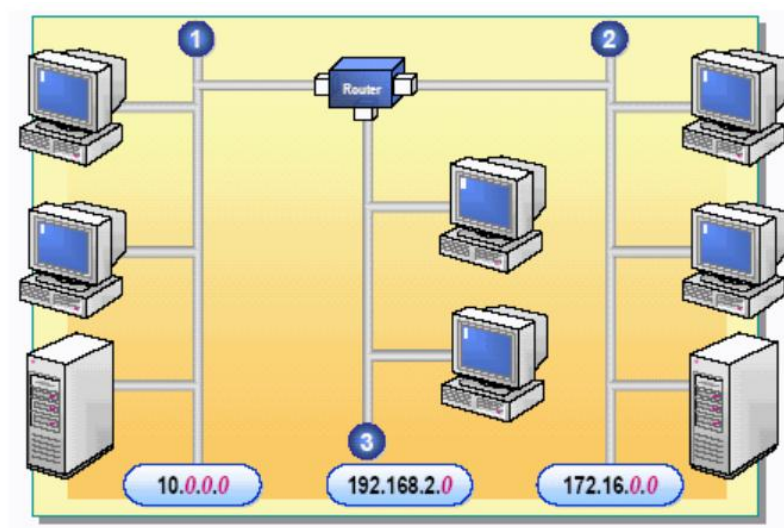
Fuente.: Las tesisas

Debemos tener en cuenta algunas directrices sobre los números utilizados para el ID de red y el ID de host cuando asignemos una dirección IP utilizando clases. Estas directrices son las siguientes:

- El primer número del ID de red no puede ser 127. Este número de ID está reservado para pruebas de conexión, como realizar un bucle local.
- Los números del ID de host no pueden ser todos 255, ya que esta dirección se utiliza como dirección de difusión IP.
- El ID de host no puede ser todo ceros (0s), ya que esta dirección se utiliza para indicar un ID de red.
- El ID de host deber ser exclusivo para el ID de red local.

## ASIGNACIÓN DE IDs DE RED

Gráfico 1.15.: Identificación de redes



Fuente.: Las Tesistas

El ID de red identifica los hosts TCP/IP ubicados en la misma subred física. Todos los hosts de la misma subred deben tener asignado el mismo ID de red para que puedan comunicarse entre sí.

Todas las subredes deben tener un ID de red exclusivo. Por ejemplo, la subred A podría tener el ID de red 10.0.0.0, la subred B podría tener el ID de red 192.168.2.0, y la subred C podría tener el ID de red 172.16.0.0. La siguiente tabla muestra una lista de intervalos válidos de IDs de red para una red.

Gráfico 1.16.: Intervalos de clases en IPv4.

Clase de dirección	Inicio del intervalo	Fin del intervalo
Clase A	1.0.0.0	126.0.0.0
Clase B	128.0.0.0	191.255.0.0
Clase C	192.0.0.0	223.255.255.0

Fuente.: Las Tesistas

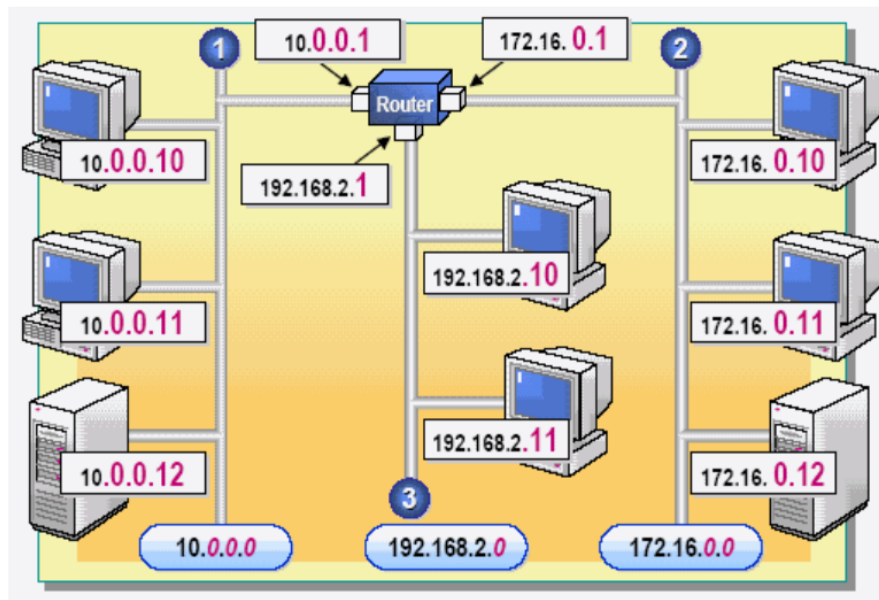
**Nota:** Si tiene previsto conectar su red a Internet, debe asegurarse de que la parte de ID de red de la dirección IP es exclusiva respecto al resto de redes en Internet. Para obtener



una asignación de un número válido de red IP, puede contactar con su proveedor de servicios de Internet. Puede dividir en subredes su red utilizando máscaras de subred.

## ASIGNACIÓN DE IDs DE HOST

Grafico 1.17.:Direccionamientos



Fuente.: Las tesisas

El ID de host identifica a un host TCP/IP de una red y debe ser exclusivo para un ID de red determinado. Todos los hosts TCP/IP, incluyendo los routers, requieren IDs de host exclusivos. No existen normas para la asignación de IDs de host en una subred. Por ejemplo, podemos numerar todos los hosts TCP/IP consecutivamente, o podemos numerarlos para que puedan ser identificados fácilmente, por ejemplo asignando al router de cada subred el número 1 para el último número del ID de host.

**IDs de host válidos** La siguiente tabla muestra una lista de intervalos válidos de IDs de host para cada clase de red.

Grafico 1.18.: Clases de Redes

<b>Clase de dirección</b>	<b>Inicio del intervalo</b>	<b>Fin del intervalo</b>
Clase A	w.0.0.1	w.255.255.254
Clase B	w.x.0.1	w.x.255.254
Clase C	w.x.y.1	w.x.y.254

**Fuente.:** Las Tesistas

### **Puerta de enlace predeterminada**

Para un host específico, la dirección IP del router que se encuentra en el mismo segmento que el host recibe el nombre de la puerta de enlace predeterminada del host. Toda la información que el host necesite enviar a segmentos distintos de los suyos, es enrutada a través de la puerta de enlace predeterminada. Como un host y su puerta de enlace predeterminada se encuentran en el mismo segmento, tienen el mismo ID de red pero diferentes IDs de host. Por ejemplo, para el host con la dirección IP 192.168.2.11, la dirección IP de la puerta de enlace predeterminada es 192.168.2.1.

### **ASIGNACIÓN DE DIRECCIONES TCP/IP**

Podemos establecer direcciones IP utilizando el método estático o el método automático. Si decidimos establecer la dirección IP de forma estática, deberemos configurar manualmente la dirección de cada equipo de la red. Si decidimos establecer la dirección IP automáticamente, podremos configurar las direcciones IP para toda una red desde una sola ubicación y asignarlas dinámicamente a cada equipo.

Una vez hemos establecido la dirección IP, podemos ver su configuración TCP/IP utilizando el cuadro de diálogo Propiedades del protocolo de Internet (TCP/IP) o la utilidad *Ipconfig*.

#### **1.4 IP V4. (Protocolo de Internet versión 4).<sup>7</sup>**

<sup>7</sup> Tomado de: ADICTOS AL TRABAJO: [www.adictosaltrabajo.com/ipv4](http://www.adictosaltrabajo.com/ipv4) ; CEDIA: [www.cedia.org](http://www.cedia.org)

El **Internet Protocol versión 4 (IPv4)** (en español: *Protocolo de Internet versión 4*) es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791.

IPv4 usa direcciones de 32 bits, limitándola a = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4.

Las direcciones disponibles en la reserva global de IANA pertenecientes al protocolo IPv4 se agotaron el jueves 3 de Febrero de 2011 oficialmente<sup>[1]</sup> Los Registros Regionales de Internet deben, desde ahora, manejarse con sus propias reservas, que se estima, alcanzaran hasta Septiembre de 2011

Actualmente no quedan direcciones IPv4 disponibles para compra, por ende se está en la forzosa y prioritaria obligación de migrar a IPv6, Los sistemas operativos Windows Vista, 7, Unix/like (Gnu/linux, Unix, Mac OSX), BSD entre otros, tienen soporte nato para IPv6, mientras que Windows XP requiere utilizar el prompt y digitar `ipv6 install`, para instalarlo, y sistemas anteriores no tienen soporte para este

El **Internet Protocol versión 4 (IPv4)** (en español: *Protocolo de Internet versión 4*) es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala. Definida en el RFC 791.

IPv4 usa direcciones de 32 bits, limitándola a = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs). Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones en muchos casos (ver abajo), ya hace varios años se vio que escaseaban las direcciones IPv4.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4.

Las direcciones disponibles en la reserva global de IANA pertenecientes al protocolo IPv4 se agotaron el jueves 3 de Febrero de 2011 oficialmente<sup>[1]</sup> Los Registros Regionales de Internet deben, desde ahora, manejarse con sus propias reservas, que se estima, alcanzaran hasta Septiembre de 2011

Actualmente no quedan direcciones IPv4 disponibles para compra, por ende se está en la forzosa y prioritaria obligación de migrar a IPv6, Los sistemas operativos Windows Vista, 7, Unix/like (Gnu/linux, Unix, Mac OSX), BSD entre otros, tienen soporte nato para IPv6, mientras que Windows XP requiere utilizar el prompt y digitar `ipv6 install`, para instalarlo, y sistemas anteriores no tienen soporte para éste.

## **1.5 IP V6. (Protocolo de Internet versión 6)<sup>8</sup>**

El Internet Protocol versión 6 (IPv6) (en español: Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4 (IPv4) RFC 791, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes.

---

<sup>8</sup>Tomado de: [www.6deploy.org](http://www.6deploy.org)

A principios de 2010, quedaban menos del 10% de IPs sin asignar. En la semana del 3 de febrero del 2011, la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó el último bloque de direcciones disponibles (33 millones) a la organización encargada de asignar IPs en Asia, un mercado que está en auge y no tardará en consumirlas todas.

IPv4 posibilita 4.294.967.296 ( $2^{32}$ ) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. En cambio, IPv6 admite 340.282.366.920.938.463.463.374.607.431.768.211.456 ( $2^{128}$  o 340 sextillones de direcciones) —cerca de  $6,7 \times 10^{17}$  (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales en el año 2008.

### **1.5.1 Motivación y orígenes de los IP**

Durante la primera década de operación de Internet basado en TCP/IP, a fines de los 80s, se hizo aparente que se necesitaba desarrollar métodos para conservar el espacio de direcciones. A principios de los 90s, incluso después de la introducción del rediseño de redes sin clase, se hizo claro que no sería suficiente para prevenir el agotamiento de las direcciones IPv4 y que se necesitaban cambios adicionales. A comienzos de 1992, circulaban varias propuestas de sistemas y a finales de 1992, la IETF anunció el llamado para white papers (RFC 1550) y la creación de los grupos de trabajo de "IP de próxima generación" ("IP Next Generation") o (IPng).

IPng fue propuesto por el Internet Engineering Task Force (IETF) el 25 de julio de 1994, con la formación de varios grupos de trabajo IPng. Hasta 1996, se publicaron varios RFCs definiendo IPv6, empezando con el RFC 2460.

La discusión técnica, el desarrollo e introducción de IPv6 no fue sin controversia. Incluso el diseño ha sido criticado por la falta de interoperabilidad con IPv4 y otros aspectos, por ejemplo por el científico de computación D. J. Bernstein.

Incidentalmente, IPng (IP Next Generation) no pudo usar la versión número 5 (IPv5) como sucesor de IPv4, ya que ésta había sido asignada a un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio.

Se espera ampliamente que IPv6 sea soportado en conjunto con IPv4 en el futuro cercano. Los nodos solo-IPv4 no son capaces de comunicarse directamente con los nodos IPv6, y necesitarán ayuda de un intermediario; vea Mecanismos de Transición más adelante.

### **1.5.2 Cambios y nuevas características**

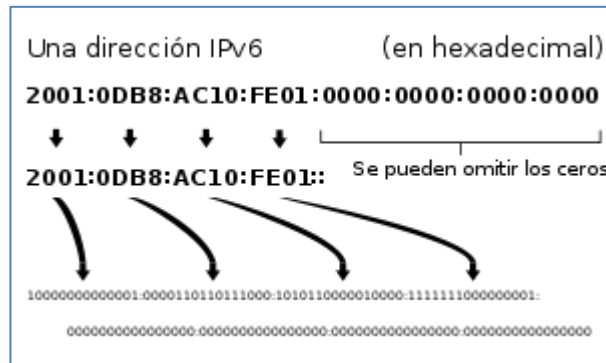
En muchos aspectos, IPv6 es una extensión conservadora de IPv4. La mayoría de los protocolos de transporte -y aplicación- necesitan pocos o ningún cambio para operar sobre IPv6; las excepciones son los protocolos de aplicación que integran direcciones de capa de red, como FTP o NTPv3, NTPv4.

IPv6 especifica un nuevo formato de paquete, diseñado para minimizar el procesamiento del encabezado de paquetes. Debido a que las cabeceras de los paquetes IPv4 e IPv6 son significativamente distintas, los dos protocolos no son interoperables.

Algunos de los cambios de IPv4 a IPv6 más relevantes son:

Capacidad extendida de direccionamiento.

**Grafico 1.19.:** Dirección IP (versión 6), en hexadecimal y binario.



**Fuente:** [www.monografias.com/redes/comunicacionesipv6.html](http://www.monografias.com/redes/comunicacionesipv6.html)

El interés de los diseñadores era que direcciones más largas permiten una entrega jerárquica, sistemática y en definitiva mejor de las direcciones y una eficiente agregación de rutas. Con IPv4, se desplegaron complejas técnicas de Classless Interdomain Routing (CIDR) para utilizar de mejor manera el pequeño espacio de direcciones. El esfuerzo requerido para reasignar la numeración de una red existente con prefijos de rutas distintos es muy grande, como se discute en RFC 2071 y RFC 2072. Sin embargo, con IPv6, cambiando el prefijo anunciado por unos pocos routers es posible en principio reasignar la numeración de toda la red, ya que los identificadores de nodos (los 64 bits menos significativos de la dirección) pueden ser auto-configurados independientemente por un nodo.

El tamaño de una subred en IPv6 es de  $2^{64}$  (máscara de subred de 64-bit), el cuadrado del tamaño de la Internet IPv4 entera. Así, las tasas de utilización del espacio de direcciones será probablemente menor en IPv6, pero la administración de las redes y el ruteo serán más eficientes debido a las decisiones de diseño inherentes al mayor tamaño de las subredes y la agregación jerárquica de rutas.

Autoconfiguración de direcciones libres de estado

Los nodos IPv6 pueden configurarse a sí mismos automáticamente cuando son conectados a una red ruteada en IPv6 usando los mensajes de descubrimiento de

routers de ICMPv6. La primera vez que son conectados a una red, el nodo envía una solicitud de router de link-local usando multicast (router solicitación) pidiendo los parámetros de configuración; y si los routers están configurados para esto, responderán este requerimiento con un "anuncio de router" (router advertisement) que contiene los parámetros de configuración de capa de red.

Si la autoconfiguración de direcciones libres de estado no es adecuada para una aplicación, es posible utilizar Dynamic Host Configuration Protocol para IPv6 (DHCPv6) o bien los nodos pueden ser configurados en forma estática.

Los routers presentan un caso especial de requerimientos para la configuración de direcciones, ya que muchas veces son la fuente para información de autoconfiguración, como anuncios de prefijos de red y anuncios de router. La configuración sin estado para routers se logra con un protocolo especial de reenumeración de routers.

## **Multicast**

Multicast, la habilidad de enviar un paquete único a destinos múltiples es parte de la especificación base de IPv6. Esto es diferente a IPv4, donde es opcional (aunque usualmente implementado).

IPv6 no implementa broadcast, que es la habilidad de enviar un paquete a todos los nodos del enlace conectado. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos (all hosts). Por lo tanto, no existe el concepto de una dirección de broadcast y así la dirección más alta de la red (la dirección de broadcast en una red IPv4) es considerada una dirección normal en IPv6.

Muchos ambientes no tienen, sin embargo, configuradas sus redes para rutear paquetes multicast, por lo que en éstas será posible hacer "multicasting" en la red local, pero no necesariamente en forma global.

El multicast IPv6 comparte protocolos y características comunes con IPv4, pero también incorpora cambios y mejoras. Incluso cuando se le asigne a una



organización el más pequeño de los prefijos de ruteo global IPv6, ésta también recibe la posibilidad de usar uno de los 4.2 billones de grupos multicast IPv6 ruteables de fuente específica para asignarlos para aplicaciones multicast intradominio o entre-dominios (RFC 3306). En IPv4 era muy difícil para una organización conseguir incluso un único grupo multicast ruteable entre-dominios y la implementación de las soluciones entre-dominios eran anticuadas (RFC 2908). IPv6 también soporta nuevas soluciones multicast, incluyendo Embedded Rendezvous Point (RFC 3956), el que simplifica el despliegue de soluciones entre dominios.

### **1.5.3 Direccionamiento IPv6**

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374 pero fue redefinida en abril de 2003 en la RFC 3513 , son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de  $2^{128} \approx 3.4 \times 10^{38}$ . Este número puede también representarse como  $16^{32}$ , con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores (véase combinatoria).

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

## **1.6 Windows 2008**

Windows Server 2008 es el nombre de un sistema operativo de Microsoft diseñado para servidores.

Es el sucesor de Windows Server 2003, distribuido al público casi cinco años antes. Al igual que Windows 7, Windows Server 2008 se basa en el núcleo Windows NT 6.1. Entre las mejoras de esta edición, se destacan nuevas funcionalidades para el Active Directory, nuevas prestaciones de virtualización y administración de sistemas, la inclusión de IIS 7.5 y el soporte para más de 256 procesadores. Hay siete ediciones diferentes: Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server y para Procesadores Itanium.

### **1.6.1 Historia**

Fue conocido como Windows Server "Longhorn" hasta el 16 de mayo de 2007, cuando Bill Gates, presidente de Microsoft, anunció su título oficial (Windows Server 2008) durante su discurso de apertura en WinHEC. Windows Aero está deshabilitado y usa la interfaz clásica de versiones anteriores de Windows.

La beta 1 fue lanzada el 27 de julio de 2005. La beta 2 fue anunciada y lanzada el 23 de mayo de 2006 en WinHEC 2006, y la beta 3 fue lanzada al público el 25 de abril de 2007. Su lanzamiento fue el 27 de febrero de 2008

### **1.6.2 Características**

Hay algunas diferencias (unas sutiles y otras no tanto) con respecto a la arquitectura del nuevo Windows Server 2008, que pueden cambiar drásticamente la manera en que se usa este sistema operativo. Estos cambios afectan a la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de forma remota y cambiar de forma radical la política de seguridad. Entre las mejoras que se incluyen, están:

- Nuevo proceso de reparación de sistemas NTFS: proceso en segundo plano que repara los archivos dañados.

- Creación de sesiones de usuario en paralelo: reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.
- Cierre limpio de Servicios.
- Sistema de archivos SMB2: de 30 a 40 veces más rápido el acceso a los servidores multimedia.
- Address Space Load Randomization (ASLR): protección contra malware en la carga de controladores en memoria.
- Windows Hardware Error Architecture (WHEA): protocolo mejorado y estandarizado de reporte de errores.
- Virtualización de Windows Server: mejoras en el rendimiento de la virtualización.
- PowerShell: inclusión de una consola mejorada con soporte GUI para administración.
- Server Core: el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

### **1.6.3 Ediciones**

La mayoría de las ediciones de Windows Server 2008 están disponibles en x86-64 (64 bits) y x86 (32 bits). Windows Server 2008 para sistemas basados en Itanium soporta procesadores IA-64. La versión IA-64 se ha optimizado para escenarios con altas cargas de trabajo como servidores de bases de datos y aplicaciones de línea de negocios (LOB). Por ende no está optimizado para su uso como servidor de archivos o servidor de medios. Microsoft ha anunciado que Windows Server 2008 será el último sistema operativo para servidores disponible en 32 bits.<sup>2</sup> Windows Server 2008 está disponible en las ediciones que figuran a continuación, similar a Windows Server 2003.

- Windows Server 2008 Standard Edition (x86 y x86-64)
- Windows Server 2008 Todas las Ediciones (Solo 64Bit)

- Windows Server 2008 Enterprise Edition (x86 y x86-64)
- Windows Server 2008 Datacenter Edition (x86 y x86-64)
- Windows Server 2008 R2 Standard Edition (Solo 64Bit)
- Windows Server 2008 R2 Todas las Ediciones (Solo 64Bit)
- Windows Server 2008 R2 Enterprise Edition (Solo 64Bit)
- Windows Server 2008 R2 Datacenter Edition (Solo 64Bit)
- Windows HPC Server 2008 (reemplaza Windows Compute Cluster Server 2003)
- Windows Web Server 2008 R2 (Solo 64Bit)
- Windows Storage Server 2008 (x86 y x86-64)
- Windows Small Business Server 2008 (Nombre clave "Cougar") (x86-64) para pequeñas empresas
- Windows Essential Business Server 2008 (Nombre clave "Centro") (x86-64) para empresas de tamaño medio<sup>3</sup>
- Windows Server 2008 para sistemas basados en Itanium
- Windows Server 2008 R2 Foundation Server

*Server Core* está disponible en las ediciones Web, Standard, Enterprise y Datacenter, aunque no es posible usarla en la edición Itanium. *Server Core* es simplemente una opción de instalación alterna soportada y en sí no es una edición propiamente dicha. Cada arquitectura dispone de un DVD de instalación independiente.

Windows Server 2008 Standard Edition, y Windows Server 2008 R2 Standard Edition estaban disponibles gratuitamente para estudiantes a través del programa Microsoft DreamSpark.

Actualmente Windows Server 2008 Standard Edition (32 y 64bits), Windows Server 2008 Enterprise Edition (32 y 64bits), Windows Server 2008 Datacenter Edition (32 y 64bits), Windows Server 2008 R2 Standard Edition (con y sin SP1), Windows Server 2008 R2 Web Edition (con y sin SP1), Windows Server 2008 R2 Enterprise Edition (con y sin SP1), y Windows Server 2008 R2 Datacenter

Edition (con y sin SP1), están disponible gratuitamente para estudiantes a través del programa Microsoft DreamSpark, al renovarse la licencia.

**Grafico 1.120:** Logotio Windows 2008 Server .



**Fuente:** Microsoft Inc.

## 1.7 Linux Centos<sup>9</sup>

CentOS (Community ENTERprise Operating System) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise Linux y está libremente disponible para ser bajado y usado por el público, pero no es mantenido ni asistido por Red Hat. Existen otras distribuciones también derivadas de las fuentes de Red Hat.

---

<sup>9</sup> [www.linuxparatodos.com](http://www.linuxparatodos.com)

CentOS usa yum para bajar e instalar las actualizaciones, herramienta también utilizada por Fedora.

## 1.8 Free BSD<sup>10</sup>

FreeBSD es un sistema operativo libre para computadoras basado en las CPU de arquitectura Intel, incluyendo procesadores Intel 80386, Intel 80486 (versiones SX y DX), y Pentium. También funciona en procesadores compatibles con Intel como AMD y Cyrix. Actualmente también es posible utilizarlo hasta en once arquitecturas distintas como Alpha, AMD64, IA-64, MIPS, PowerPC y UltraSPARC.

FreeBSD está basado en la versión 4.4 BSD-Lite del Computer Systems Research Group (CSRG) de la University of California, Berkeley siguiendo la tradición que ha distinguido el desarrollo de los sistemas BSD. Además del trabajo realizado por el CSRG, el proyecto FreeBSD ha invertido miles de horas en ajustar el sistema para ofrecer las máximas prestaciones en situaciones de carga real.

La mascota del sistema operativo es Beastie.

**Grafico 1.21.:** Logotipo FreeBSD



**Fuente.:** [www.freebsd.org](http://www.freebsd.org)

---

<sup>10</sup> [www.freebsd.org](http://www.freebsd.org)

### 1.8.1 Características

FreeBSD es un sistema operativo multiusuario, capaz de efectuar multitarea con apropiación y multiproceso en plataformas compatibles con múltiples procesadores; el funcionamiento de FreeBSD está inspirado, como ya se dijo, en la variante 4.4 BSD-Lite de UNIX. Aunque FreeBSD no puede ser propiamente llamado UNIX, al no haber adquirido la debida licencia de The Open Group, FreeBSD sí está hecho para ser compatible con la norma POSIX, al igual que varios otros sistemas "clones de UNIX".

El sistema FreeBSD incluye el núcleo, la estructura de ficheros del sistema, bibliotecas de la API de C, y algunas utilidades básicas. La versión 6.1<sup>2</sup> trajo importantes mejoras como mayor apoyo para dispositivos Bluetooth y controladores para tarjetas de sonido y red.

La versión 7.0, lanzada el 27 de febrero del año 2008, incluye compatibilidad con el sistema de archivos ZFS de Sun y a la arquitectura ARM, entre otras novedades

### 1.8.2 Gestión de Programas

FreeBSD al igual que varios otros sistemas inspirados en BSD, provee de manejo semi-automatizado de paquetes distribuidos en formato comprimido (en formato tar.bz o .tbz). Además de eso, y al igual que NetBSD y OpenBSD, FreeBSD provee para conveniencia del usuario, de un eficiente sistema de gestión de paquetería llamado **ports**. Los ports son un conjunto de comandos por lotes, que especifican exactamente los requisitos, lo que se debe hacer para compilar el código fuente y lo necesario para instalar la versión ejecutable de un determinado paquete de software en el sistema. Existen miles de programas libres y comerciales hechos para sistemas como GNU/Linux, que también tienen versiones en FreeBSD. Debido a que muchos de los paquetes están ya compilados y preparados por los participantes del proyecto FreeBSD, éstos pueden ser instalados simplemente seleccionándolos en una interfaz provista por el sistema operativo, y copiados directamente desde un servidor HTTP o FTP.

### 1.8.3 Compatibilidad con GNU/Linux

FreeBSD es compatible con binarios de varios sistemas operativos de tipo Unix, incluyendo GNU/Linux. La razón de esto es la necesidad de ejecutar algunas aplicaciones desarrolladas para ser ejecutadas en sistemas con el núcleo Linux en las que el código fuente no se distribuye públicamente y, por tanto, no pueden ser portadas a FreeBSD.

Algunas de las aplicaciones usadas bajo esta compatibilidad son la versión de GNU/Linux de Adobe Flash Player, Linux-Firefox, Linux-Opera, Netscape, Adobe Acrobat, RealPlayer, VMware, Oracle, WordPerfect, Skype, Doom 3, Quake 4, Unreal Tournament, SeaMonkey y varias más.

Generalmente no se siente pérdida de rendimiento, y funcionan igual de rápido que las versiones nativas. Incluso puede ser más veloz ejecutar un binario de GNU/Linux en FreeBSD, que un binario nativo (como en el caso de Firefox, no obstante es muy relativo ya que FreeBSD compila el código y GNU/Linux en la mayoría de los casos no, pero si compilara, obtendría una funcionalidad similar al de FreeBSD, unos programas funcionan mejor en GNU/Linux mientras que otros en FreeBSD).

Si bien algunas aplicaciones funcionan perfectamente, otras se ven limitadas debido a que la capa de compatibilidad solo incluye las llamadas de sistema del núcleo Linux 2.4.2, una versión antigua. Una emulación incompleta del núcleo Linux 2.6 está incluida en FreeBSD 7.x, aunque todavía no viene activada por defecto. FreeBSD 8.x implementa compatibilidad con las llamadas nativas del núcleo linux 2.6 y el conjunto de librerías base de Fedora 10.