
# Protocolo de Redes

# Índice

# Presentación

El presente material ha sido diseñado en función de semanas. Por cada semana se ha contemplado tema, objetivo, contenido y actividades, de tal manera que, al finalizarla, se pueda verificar si se ha logrado el objetivo.

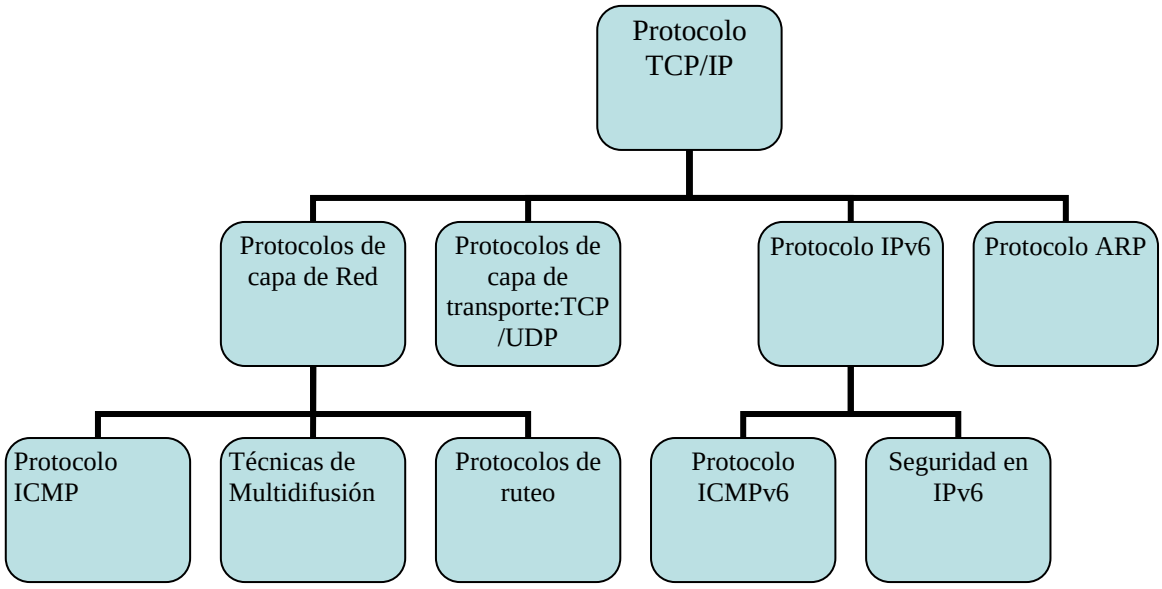
El contenido de este manual trata de describir la suite TCP/IP y desarrolla cada uno de sus elementos de manera paulatina.

Las redes basadas en el protocolo TCP/IP constituyen un tema al que se ha ido dando mayor atención conforme han pasado los años. Este desarrollo de TCP/IP se ha dado, principalmente, por el hecho de constituir el protocolo fundamental sobre el cual descansa Internet. Todas las aplicaciones que son utilizadas por millones de usuarios diariamente, tales como las páginas web, el e-mail y las salas de chat, funcionan porque, silenciosamente, TCP/IP hace su trabajo de manera eficiente.

Desde hace una década aproximadamente, TCP/IP empezó a tener vigencia también a nivel de las redes locales, tal es así que, actualmente, constituye el protocolo de transporte más utilizado a nivel de todos los sistemas operativos de redes locales, así no es raro encontrarlo en plataformas tan diversas como Linux, Windows 2003 y Netware.

El presente manual buscar allanar el camino en esta materia que, muchas veces, debido a su profundidad, puede resultar un tanto árido. Se ha buscado presentar los temas tomando como referencia el modelo TCP/IP desde sus capas iniciales. Esa es la razón por la cual se empieza con la capa de acceso a la red, para luego ir estudiando los diversos protocolos que se encuentran a nivel de la capa de Inter.-red y, posteriormente, llegar a las aplicaciones que trabajan en las capas más altas.

# Red de contenidos



SEMANA 1

# Suite TCP/IP

**TEMA**

Introducción a la Suite TCP/IP

Origen de Internet

Conmutación de paquetes

**OBJETIVOS ESPECÍFICOS**

- Conocer las condiciones iniciales que dieron inicio a Internet
- Identificar las organizaciones que supervisan y norman el crecimiento de Internet
- Conocer los distintos tipos de estándares manejados en Internet
- Conocer la técnica de Conmutación de paquetes

**CONTENIDOS**

- Introducción
- Origen de TCP/IP
- INTERNET: Reseña Histórica
- Organizaciones detrás de Internet
- Protocolos Internet
- Borradores de Internet
- Conmutación de paquetes

**ACTIVIDADES**

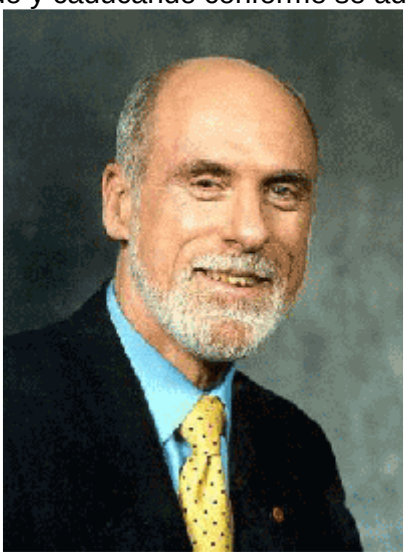
- Hacen uso de la técnica de lluvia de ideas para identificar las características de la suite TCP/IP.

## 1. Introducción

Hace 20 años las computadoras eran aparatos novedosos: equipos bastante caros y que, principalmente, se les utilizaba como un elemento que suplantaba a las máquinas de escribir, a las calculadoras y, algo importante, traían juegos incorporados. En esa época hablar de redes de computadoras era bastante extraño para el común de la gente.
Si se quería compartir información entre varias personas, la solución era el disquete. La mayoría de programas cabían en un solo disquete e incluso se podían ejecutar desde ellos. Sin embargo, esto ha cambiado. Hoy es posible, a través de las computadoras, comunicarnos con cualquier persona en el mundo. La integración que se ha logrado es impresionante, el video en tiempo real, la telefonía sobre Internet y los bajos precios de la tecnología informática han hecho que la computación cobre una vigencia inusitada y constituya el motor de la llamada nueva economía. Sin embargo, existen ciertos detalles técnicos que muchos no se detienen a analizar y que logran que esta revolución funcione. Es el caso del protocolo TCP/IP.

### 1.1. Origen de TCP/IP

TCP/IP fue desarrollado por el Departamento de Defensa de los EEUU, con el objetivo de comunicar distintas redes con el objetivo de formar una red mucho más grande, que se denominó ARPANET. Detrás de su desarrollo estuvieron muchas personas; sin embargo, Vinton Cerf es reconocido como uno de los principales programadores detrás de la suite TCP/IP. Si bien se podría pensar que TCP/IP constituye únicamente 2 protocolos, en realidad se trata de toda una suite completa de protocolos, que se van enriqueciendo, mejorando y caducando conforme se adapta a los cambios que le exige la tecnología.



Vinton Cerf

Entre muchas de las características de TCP/IP se tienen dos que son muy importantes:

- **Flexibilidad**
  Esto significa que puede adaptarse a distintas configuraciones de software y hardware.
- **Código abierto**
  Se trata de una especificación abierta, lo que significa que cualquiera puede escribir software que haga uso de TCP/IP. Este último hecho y su naturaleza de protocolo robusto es el que motivó a que se escribieran muchos programas que lo utilizaban como protocolo de red básico.

Con el paso del tiempo, ARPANET creció hasta abarcar a las universidades y, luego, dio un salto hacia las empresas convirtiéndose en el Internet actual.
A continuación, se detallan mediante una reseña, cuales fueron las etapas por las que pasó Internet y cómo es que se relacionó con TCP/IP.

**INTERNET: Reseña Histórica**

| | |
|---|---|
| 1968 | El DoD crea el proyecto ARPA<br>Se inicia la investigación de la tecnología de Conmutación de Paquetes.<br>Primera red experimental ARPAnet, une 4 nodos:<br>UCLA, UCSB, Universidad de Utah, SRI International. |
| 1972 | ARPA net presenta 20 hosts.<br>El objetivo inicial: Comunicación entre el DoD. Va cambiando y se usa para comunicación no relacionada con el DoD. |
| 1980 | Inicios de los 80's, ARPAnt es la espina dorsal de una interred que conecta instituciones educativas y contratistas del DoD, así como la MIL net (red militar, 1983). |
| 1983 | TCP/IP se desarrolla a inicios de los 80's, y en este año, se convierte en Norma para ARPAnet.<br>TCP/IP se incorpora a la versión 4.2 del UNIX de BSD, gana gran popularidad.<br>Al darse esta relación, todos los sistemas UNIX usan TCP/IP.<br>Aunque el ejército de EU auspició la investigación de Internet y luego eligió usarla, el trabajo entre redes se desarrolló y probó en localidades civiles. |
| 1986 | Comercialización de ARPAnet.<br>Se aíslan las redes militares de ARPAnet.<br>Se desmantela ARPAnet y se sustituye por una red financiada por la NSF. |
| 1987 | La NSF decide potenciar la red, pues desea que todo investigador de EU pueda acceder a la red.<br>Se escogen a 3 organizaciones :<br>• IBM : Se encarga del equipamiento (PCs)<br>• MCI : Llamadas de larga distancia<br>• MERIT : Experiencia en instalación y administración de redes de escuelas en Michigan.<br>Las 3 nuevas empresas cooperan para establecer una nueva red de área amplia (WAN), que constituye el backbone de Internet en 1988. |
| 1991 | En esta fecha, la red NSFnet, anteriormente citada, estaba por alcanzar su capacidad máxima.<br>El gobierno federal no podía sufragar los costos de Internet siempre. Se decide privatizarla.<br>IBM, MCI, MERIT forman una compañía sin fines de lucro llamada ANS (Advanced Network Services) |
| 1992 | ANS construye una red WAN que constituye el backbone actual.<br>Se le conoce como ANSnet. Es una WAN mucho más rápida.<br>ANS, y no el gobierno federal, es dueña de las líneas de transmisión y de las computadoras que utiliza la red. |

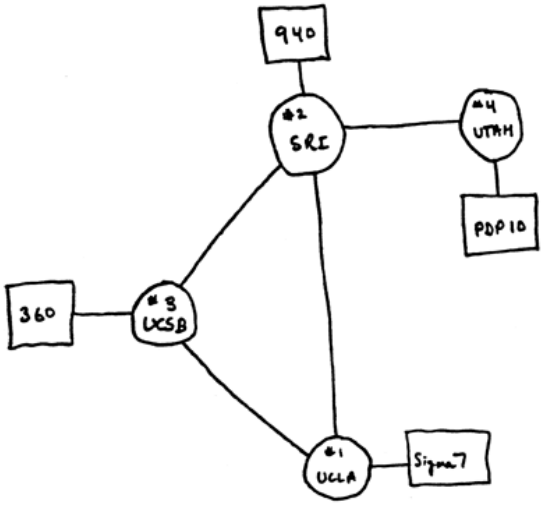



Diagrama original de Vinton Cerf: Los 4 nodos origen de Arpanet

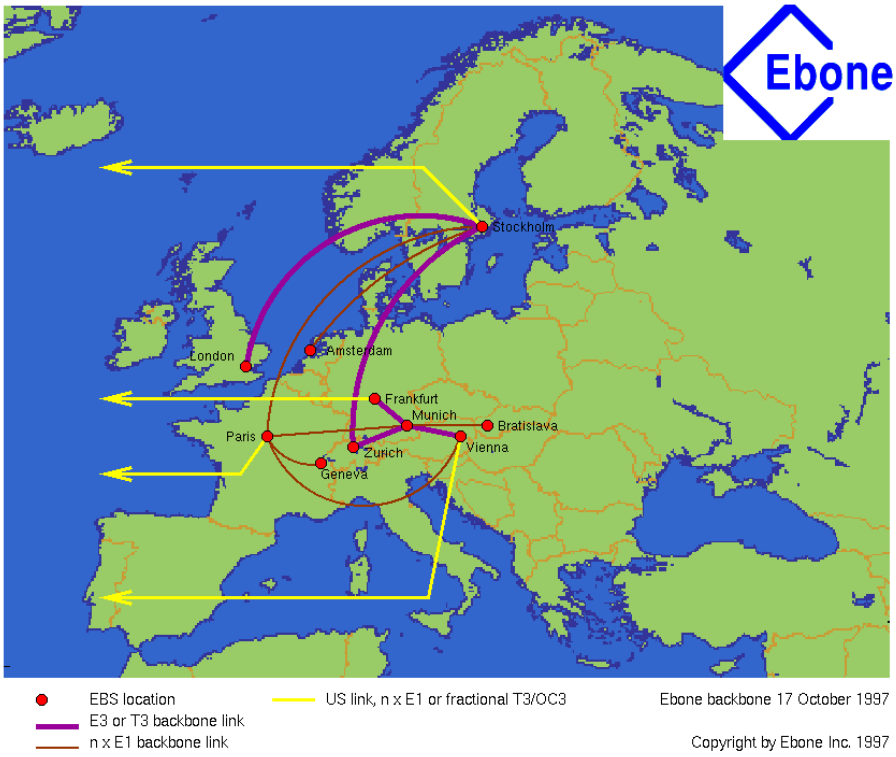
Si bien ARPA unía computadoras dentro de EU, también utilizó conexiones existentes fuera de EU para probar a gran escala la tecnología de Internet.

### 1.2. INTERNET: El caso de Europa

En Europa, el uso masivo de Internet demoró un poco en aplicarse y, y recién a inicios de los 90´s, se empezó a establecer una red europea que pudiera unirse al Internet del lado americano. El PTT (Post Telegraph and Telephone ) es una organización que abarca toda Europa y tiene control sobre muchas formas de comunicación. Además, es la que se encargó de crear una organización de estándares, el ITUT (Telecommunication Section of the International Union). Este último produjo un estándar para ser utilizado en redes de computadoras y lo llamó X.25.

### 1.3. EBONE: (Europe Bone)

En 1991, únicamente redes experimentales de Europa trabajan con TCP/IP, pero solo algunas se conectan a Internet.
Se crea una cooperativa para formar un backbone europeo de alta velocidad, que conectará a sus miembros y tendrá salida a Internet.
La organización del EBONE contaba con 21 miembros que pagan una cuota anual. El dinero es para mantener la red, las líneas de transmisión rentadas con EU y el grupo de operarios que administra la red.



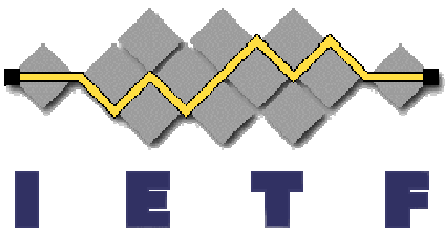

## 1.4. Organizaciones detrás de Internet

Detrás de Internet existe una gama de organizaciones, principalmente, sin fines de lucro, cuyos objetivos son técnicos y netamente administrativos. Entre las más importantes se tienen los siguientes:

### 1.4.1. Internet Activities Board (IAB)

Esta junta fue creada en 1983. Es un comité independiente de investigadores y profesionales con interés técnico en la salud y la evolución del sistema Internet. Además coordina el diseño, la ingeniería y la administración de Internet. Asimismo, la IAB publica información bajo la forma de RFC (Request for comments).
Los RFC constituyen el medio para desarrollar y publicar las normas que se utilizan en Internet. Presenta 2 grupos de trabajo:

**a. IETF: Internet Engineering Task Force :**




Se responsabiliza de la especificación de la arquitectura y los protocolos de Internet. Se compone de voluntarios. No es una organización tradicional de normalización. El trabajo del IETF se organiza en áreas que cambian de acuerdo con las necesidades técnicas del momento.

Los directores de las áreas técnicas componen el IESG (Internet Engineering Steering Group) Grupo director de Ingeniería de Internet.
Algunas áreas de actual ocupación son las siguientes:

- Aplicaciones IP : Siguiente generación
- Encaminamiento
- Transporte, etc.

**b. IRTF: Internet Research Task Force dedicada a la investigación**

Al margen de estos 2 organismos que son netamente técnicos, también existen 2 organizaciones que tienen influencia sobre el IAB:
La Internet Society

Organización abierta compuesta por investigadores, profesores, corporaciones, usuarios y agencias gubernamentales que promueven el uso de Internet. Tiene injerencia en el proceso de Normalización de Internet y, también, sobre el Federal Networking Council, que es una entidad del gobierno federal de los Estados Unidos que coordina con las agencias gubernamentales que prestan su apoyo a Internet.

## 1.5. Protocolos Internet

Los protocolos de Internet pueden denominarse de distintas formas, dependiendo de su estado en el proceso de normalización. Así, se tienen los siguientes:

- Propuesta de Norma (Proposed Standard)
  Protocolo en fase de estudio para su futura Normalización
- Borrador de Norma (Draft Estándar)
  Protocolo en las fases de estudio previas a su aprobación como norma
- Estándar o Norma
  Protocolo estándar oficial de Internet
- Experimental
  Protocolo en fase de pruebas que no ha iniciado su proceso de normalización
- Histórico
  Protocolo que ha sido superado o que ya no se considera estándar
  Las normas en Internet se clasifican sobre la base de los siguientes niveles de requisito
- Requerido:
  Todos los sistemas conectados a Internet deben implementarlo
- Recomendado:
  Debería implementarse
- Electivo:
  Puede implementarse si se desea
- Uso Limitado:
  Puede ser utilizado para algunos sistemas. Los protocolos históricos, especializados e históricos pueden recibir esta clasificación

- No Recomendado:
  Protocolos históricos, especializados o experimentales no recomendados para Internet.

### 1.6. Borradores de Internet

El IETF continuamente trabaja en gran cantidad de proyectos que no están suficientemente maduros para ser un RFC.
Estos proyectos se encuentran en los Internet-Drafts.

## 2. Conmutación de paquetes

Paul Baran fue uno de los impulsores de las redes de conmutación de paquetes junto a Donald Davies y Leonard Kleinrock. Baran desarrolló esta idea mientras trabajaba para la Corporación RAND que, luego, sería utilizada en ARPAnet.
El arreglo para que varios dispositivos compartan una sola vía de transmisión reduce el costo, ya que se utilizan menos cables y menos máquinas de conmutación. Sin embargo, existe un problema que se da si se quiere compartir un medio.

Paul Baran: Conmutación de paquetes

Así se tiene que:
Concederle a una parte el acceso exclusivo a una vía compartida de transporte resulta poco práctico, puesto que puede retrasar las otras partes.
De la misma forma, cuando dos computadoras conectadas a una red transfieren datos, todas las demás computadoras se ven forzadas a esperar hasta que termine la transferencia.
Se han ideado muchas soluciones para resolver el problema de los recursos compartidos. Los sistemas de televisión por cable utilizan uno de ellos. Una compañía de TV-cable transmite muchas señales en un solo cable al utilizar varios canales (transmisión en banda ancha).

### 2.1. Compartir esperando turno

Aunque es posible construir una tecnología de red de computadoras que utilice varios canales para mezclar señales en un cable compartido, casi ninguna de las tecnologías de red lo hace. En lugar de ello, utilizan una variación de la idea convencional de esperar turno.
Las reglas para compartir se deben definir, cuidadosamente, para que una sola computadora no retrase a las otras al utilizar el cable compartido por un periodo indeterminadamente largo.

La idea vislumbrada en los sesenta se llama conmutación de paquetes (packet switching), y la unidad de datos que se puede transferir a la vez se llama paquete (packet).

## 2.2. Características

La conmutación de paquetes evita demoras:
Tanto las LAN como las WAN utilizan conmutación de paquetes. En consecuencia, los mensajes cortos no necesitan esperar a que se terminen transferencias largas.

**Capa paquete se debe etiquetar**

Cada paquete que se envía a través de una red se origina en una computadora y se destina a otra. El hardware observa mientras los paquetes pasan a través de la red. Al detectar un paquete destinado a su máquina local, lo captura. Luego, coloca una copia del paquete en la memoria y le avisa que llegó. Para hacer posible que el hardware de la red distinga los paquetes, cada uno tiene el mismo formato.

El paquete incluye un encabezado al principio y datos al final. Piense como si el encabezado fuera una etiqueta que especifica qué computadora envió el paquete y cuál debe recibirlo. Las computadoras, en una red, contienen un número único, conocido como dirección de la computadora. El paquete de datos contiene dos direcciones importantes: una dirección origen y una dirección destino. No todos los paquetes son del mismo tamaño.
Aunque las tecnologías de conmutación de paquetes limitan la cantidad de datos dentro de un paquete, al que envía le permiten trasmitir cualquier tamaño de paquete, mientras que no rebase el tamaño máximo.

**La transmisión de paquetes parece instantánea**

Una LAN común puede transferir mil paquetes grandes por segundo entre dos computadoras y le toma un poco menos de tiempo enviar paquetes pequeños.
Lo interesante de esto es que, para un ser humano, los hechos que ocurren en milésimos de segundo parecen instantáneos.

En resumen, un sistema de conmutación de paquetes permite que varios pares de computadoras se comuniquen con retrasos mínimos a través de una red compartida, debido a que divide cada conversación en paquetes pequeños y a que hace que las computadoras, que comparten una red, tomen turnos para enviar paquetes.

## 2.3. Conmutación de Paquetes en ARPANET

Físicamente, ARPANET consistía en aproximadamente 50 mini computadores C30 y C300 de la BBN Corporation, llamadas Packet Switching Nodes (nodos de conmutación de paquetes o PSN) distribuidas en el territorio continental de Estados Unidos y de Europa Occidental (MILNET contiene unas 160 PSN).
Una PSN se ubica en cada localidad que participa en la red y está dedicada a la tarea de la conmutación de paquetes.
Desde las compañías de telecomunicaciones se conectaban los circuitos arrendados de datos de tipo punto a punto junto con las PSN para formar una red.
Por ejemplo, los circuitos arrendados de datos conectaban la PSN de ARPANET de la universidad de Purdue con la PSN de ARPANET en la Universidad de Wisconsin.
Inicialmente, estos circuitos arrendados operaban a 56 KBPS, una velocidad considerada alta en 1968, pero baja para los estándares actuales.
Para asegurar la fiabilidad de ARPANET ante posibles fallas de las líneas de transmisión, cada PSN debía tener al menos dos líneas de conexión arrendadas hacia otra PSN, y el software debía adaptarse, automáticamente, a las fallas y seleccionar rutas alternativas. En consecuencia, ARPANET continuaba funcionando

incluso si uno de los circuitos de datos fallaba. Hacia 1991, la NSF y otras dependencias gubernamentales comenzaron la ampliación de Internet más allá del dominio académico y científico original. El tráfico de NSFnet había crecido cerca de un billón de paquetes por día y la capacidad de 1.5 Mbps comenzó a ser insuficiente en el caso de varios de los circuitos. La NSF decidió transferir la red de columna vertebral a una compañía privada y comenzar a cobrar a las instituciones por la conexión.

IBM, MERIT y MCI conformaron una compañía sin fines de lucro llamada ANS (Advanced Networks and Services) y decidieron, en 1993, construir una nueva columa vertebral que reemplazaba a NSFnet, llamada ANSnet. Esta nueva red operaría en DS3 (codificación T3), es decir, a 45 Mbps.

## 2.4. Flexibilidad del protocolo TCP/IP

Una de las mayores cualidades del TCP/IP radica en la variedad de tecnologías de red física sobre las que se puede utilizar. Por ejemplo, cuando se decidió proporcionar el acceso a Internet a la industria y a pequeñas escuelas, se utilizó una variante del protocolo X.25 llamado x25NET. Puede parecer contradictorio el utilizar X.25 exclusivamente, mientras que Internet utiliza TCP/IP. Cuando se usa el TCP/IP para transportar tráfico, sin embargo, la red X.25 subyacente sólo proporciona una ruta sobre la cual el tráfico de Internet puede transferirse. Esto corrobora lo anteriormente dicho: que muchas tecnologías subyacentes pueden ser empleadas para acarrear tráfico de Internet.

Esta técnica llamada tunneling tan solo significa que el TCP/IP trata a un sistema de red complejo con sus propios protocolos como cualquier otro hardware de sistema de transmisión. Para enviar tráficos de información del TCP/IP a través de un túnel X.25, se hace una conexión con X.25 y, entonces, se envían paquetes TCP/IP como si estos fueran datos. Debido a que la red pública X.25 opera de manera independiente a Internet, se debe proporcionar un punto de contacto entre las dos. Tanto en ARPA como en Csnet operan máquinas dedicadas que proporcionan la interconexión entre X.25 y ARPANET. La primera conexión se conoció como VAN gateway.

# Autoevaluación

1. ¿Qué características del TCP/IP ayudaron mucho al desarrollo de Arpanet hacia una red global?

2. ¿Qué funciones cumple el IETF y la Internet Society?

3. ¿En qué momento el protocolo TCP/IP se relaciona con ARPANET?

4. ¿Dependiendo de su proceso de normalización, cómo se clasifican los protocolos Internet?

5. ¿Qué organización se encarga de la administración de los RFC?

# Para recordar

- TCP/IP fue desarrollado por el Departamento de Defensa de los EEUU con el objetivo de comunicar distintas redes y formar una red mucho más grande, que se denominó ARPANET.

- En Europa, el uso masivo de Internet demoró un poco en aplicarse y, recién a inicios de los 90 se empezó a establecer una red europea que pudiera unirse al Internet del lado americano.

- Detrás de Internet existe una gama de organizaciones principalmente sin fines de lucro, cuyos objetivos son técnicos y netamente administrativos: **la Internet Society Internet Activities Board (IAB) .**

- Las reglas para compartir se deben definir cuidadosamente para que una sola computadora no retrase a las otras al utilizar el cable compartido por un periodo indeterminadamente largo.

- Tanto las LAN como las WAN utilizan conmutación de paquetes.

SEMANA

2

# Modelo OSI - TCP/IP

**TEMA**

Modelo OSI y TCP/IP

**OBJETIVOS ESPECÍFICOS**

- Conocer las características del modelo OSI
- Identificar las funciones de las capas del modelo OSI
- Identificar las funciones del modelo TCP/IP

**CONTENIDOS**

- Modelo OSI
- Capas del Modelo OSI
- El Modelo TCP/IP

**ACTIVIDADES**

- Reconocen las características del modelo OSI y TCP-IP.
- Identifican las ventajas del TCP/IP frente a OSI.

# 2 Modelo OSI

El modelo OSI proporciona una visualización abstracta del funcionamiento de una red, desde el cableado que conecta las computadoras hasta los programas que se emplearán para la comunicación. Las capas o niveles constituyen los componentes clave del modelo OSI. Un nivel del modelo de red es, simplemente, una pieza funcional del total de la red. Este nivel utiliza un total de 7 niveles para describir la red desde los cimientos: capa física, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. Cada nivel se basa en el siguiente y sería completamente inútil por sí solo, o si faltara uno de los niveles anteriores. En su especificación del modelo OSI, la ISO no vincula el modelo a ningún estándar de red determinado, como TCP/IP.

Al estar diseñados los niveles tomando como base su funcionamiento, en lugar de algún estándar de red existente, la ISO ha proporcionado un modelo robusto y abierto, que es útil para explorar las especificaciones de red ya existentes y diseñar los estándares del futuro. Las capas de protocolos se enumeran desde la base hasta la cima. A continuación, se describirán las capas siguiendo un orden ascendente.

## 2.1 Capas del Modelo OSI

### 2.1.1 La capa física

Este nivel proporciona los cimientos sobre los que se construirán el resto de niveles. Se refiere a las computadoras, al cableado de red, las antenas de satélite o a cualquier dispositivo que se use para unir dos o más computadoras.

Se comunica directamente con el medio de comunicación y tiene dos responsabilidades: enviar bits y recibir bits.

Los bits se representan por cambios en las señales del medio de la red, algunos los representan con distintos voltajes, otros utilizan tonos de audio distintos y otras transiciones de estado (cambios de alto a bajo voltaje).

Se utiliza una gran variedad de medios en la comunicación de datos: cables eléctricos, fibras ópticas, ondas de luz o de radio y microondas.

Las capas superiores son totalmente independientes del proceso utilizado para transmitir los bits a través del medio de la red.

Las especificaciones de la capa física describen el modo en que los datos se codifican en señales del medio y las características de la interface de conexión con el medio, pero no describen el medio en sí.

### 2.1.2 La capa de enlace de datos

Esta capa es responsable de proporcionar la comunicación nodo a nodo en una misma LAN. Para ello, realiza dos funciones:

- Al recibir los mensajes de las capas superiores,le da formato para transformarlo en un marco de datos (paquete de datos).

- También, se encarga de regular la transmisión de datos desde el nivel físico. En función del tipo de red que se está configurando, existen una serie de condiciones que determinan si la máquina deberá esperar su

turno para transmitir datos, o esperar un tiempo para hacerlo nuevamente.
La capa de enlace de datos constituye el puente entre el hardware y el software.

En una computadora, la capa de enlace de datos suele estar representada por el driver de la tarjeta de red y se suele suministrar en un disquete con la tarjeta.


Modelo OSI

### 2.1.3 La capa de red

Las redes pequeñas constan de una sola LAN, pero la mayoría de las redes deben subdividirse. Una red que consta de varios segmentos de red se denomina *interred.*

Cuando las redes se subdividen, no es posible dar por sentado que los mensajes se entregan en la LAN. Es necesario recurrir a un mecanismo que dirija los mensajes de una red a otra.

Para entregar mensajes en una interred, cada red debe estar identificada de manera única por una dirección de red.

Al recibir un mensaje de las capas superiores, la capa de red añade una cabecera al mensaje que incluye las direcciones de red de origen y destino. Esta combinación de datos sumada a la capa de red se denomina *paquete*.

El proceso de hacer llegar los paquetes a la red correcta se denomina ***encaminamiento***, y los dispositivos que encaminan los paquetes se denominan encaminadores **(router).**

Los encaminadotes, proporcionan mecanismos especiales para realizar el encaminamiento. Dado que se trata de una tarea compleja, los encaminadores son dispositivos dedicados que no proporcionan servicios a los usuarios finales.

Los encaminadores al pertenecer a la capa de red, pueden utilizarse para intercambiar paquetes entre distintas redes físicas.

### 2.1.4 La capa de transporte

Todas las tecnologías de red establecen un tamaño máximo para los marcos que pueden ser enviados a través de la red. Por ejemplo, Ethernet tiene como límite de tamaño a 1500 bytes. La razón de este límite obedece a lo siguiente:

Los marcos de tamaño pequeño mejoran el rendimiento de una red compartida por muchos dispositivos. Al utilizar marcos pequeños, es necesario volver a transmitir menos datos cuando se produce un error.
Una de las responsabilidades de la capa de transporte consiste en dividir los mensajes en fragmentos que coincidan con el límite del tamaño de la red.
Cuando un mensaje se divide en varios fragmentos, aumenta la posibilidad de que los segmentos no se reciban en el orden correcto. Al recibir los paquetes, la capa de transporte debe recomponer el mensaje reensamblando los fragmentos en el orden correcto. Para ello, la capa de transporte incluye un número de secuencia en la cabecera del mensaje.

Muchas computadoras son multitarea y ejecutan varios programas simultáneamente. Por ejemplo, la estación de trabajo de un usuario puede estar ejecutando al mismo tiempo un proceso de transferencia de archivos a otra computadora, recuperando el e-mail y accediendo a una base de datos de la red. La capa de transporte debe entregar los mensajes del proceso de una computadora al proceso correspondiente de la computadora de destino.

**Según el modelo OSI, la capa de transporte asigna una identificación de *punto de acceso a servicio* (SAP) a cada paquete (puerto es el término TCP/IP correspondiente a un *punto de acceso a servicio*). La ID de un SAP es una dirección que identifica el proceso que ha originado el mensaje.**

La ID permite que la capa de transporte del nodo receptor encamine el mensaje al proceso adecuado.
La identificación de mensajes de distintos procesos para posibilitar su transmisión a través de un mismo medio de red se denomina *multiplexación*.
El procedimiento de recuperación de mensajes y de su encaminamiento a los procesos adecuados se denomina *demultiplexación.*
Aunque la capa de enlace de datos y de red pueden encargarse de detectar errores en los datos transmitidos, esta responsabilidad suele recaer sobre la capa de transporte. A este nivel es posible realizar dos tipos de detección de error:

- **Entrega fiable**
  Entrega fiable no significa que los errores no puedan ocurrir, sino que los errores se detectan cuando ocurren. En este caso, lo usual es pedir que los datos se envíen nuevamente.

- **Entrega no fiable**
  No significa que los errores puedan producirse, sino que la capa de transporte no los verifica. Este tipo de entrega es la usual en las redes LAN, y cuando los mensajes constan de un alto número de paquetes. A menudo se le llama entrega de datagramas y a cada paquete transmitido se le llama datagrama.

### 2.1.5 La capa de sesión

Esta capa se encarga del diálogo entre los distintos nodos de la red.

Un diálogo es una conversación formal en la que dos nodos acuerdan un intercambio de datos.

Existen tres posibilidades para el diálogo:

- Simple (Simplex)
  Un nodo transmite de manera exclusiva mientras otro recibe de manera exclusiva.
- Semidúplex (Half-duplex)
  Un solo nodo puede transmitir en un momento dado y los nodos se turnan para transmitir.
- Dúplex total (Full duplex)
  Los nodos pueden transmitir y recibir simultáneamente. Esta comunicación suele requerir un control de flujo que asegura que ninguno de los dispositivos envíen datos a mayor velocidad de la que el otro dispositivo puede recibir.

La sesión permite que los nodos se comuniquen de manera ordenada.

Cada sesión tiene tres fases:

- Establecimiento de la conexión
  Los nodos establecen contacto. Negocian las reglas de la comunicación incluyendo los protocolos utilizados y los parámetros de comunicación.
- Transferencia de datos
  Los nodos inician un diálogo para intercambiar datos.
- Liberación de la conexión
  Cuando ya no se requiere la comunicación, se inicia la liberación ordenada de la sesión.

Cuando una red administra varios dispositivos, envía periódicamente un breve informe de estado que suele constar de un solo marco. Si todos estos mensajes se enviaran como parte de una sesión formal, las fases de establecimiento y liberación de la conexión transmitirían más datos que los propios mensajes.

En estas situaciones se comunica sin conexión. El nodo emisor se limita a transmitir los datos asumiendo que el receptor está disponible.

### 2.1.6 La capa de presentación

Se responsabiliza de presentar los datos a la capa de aplicación. En ciertos casos, esta capa traduce los datos directamente de un formato a otro.

Los equipos grandes IBM utilizan un código de caracteres denominado EBCDIC, mientras que el común de PC's utilizan el código ASCII. Si se transmiten datos desde un equipo EBCDIC a otro ASCII, la capa de presentación traduce de un conjunto de caracteres al otro.

Una aplicación de esta capa que está en continuo crecimiento es el de proporcionar comunicaciones seguras en una red. Los datos pueden encriptarse a este nivel, antes de pasarlos a los niveles inferiores para su transmisión. También, se pueden comprimir los datos a este nivel.

### 2.1.7 La capa de aplicación

Esta capa proporciona la interfase definitiva con la que el usuario utilizará para acceder a los servicios de red.

Esta capa constituye el producto final que se ha estado construyendo, es decir, la aplicación global que oculta todo el trabajo de la red.

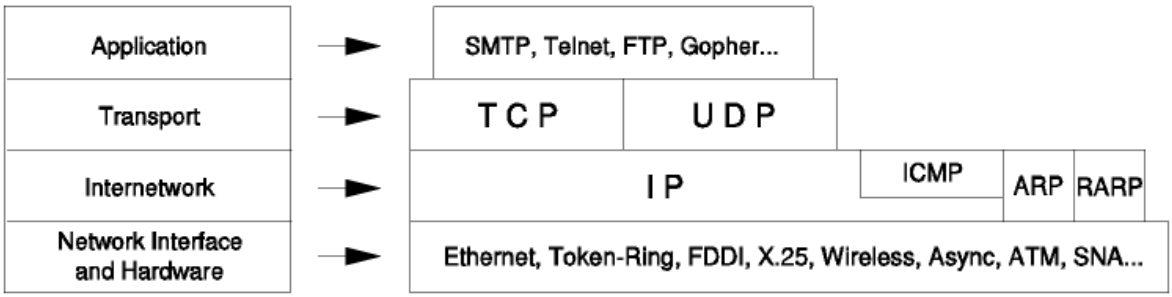
Es frecuente encontrar el término ***interface de programa de aplicación*** **(API**). Un API es un conjunto de reglas que permiten que las aplicaciones escritas por los usuarios puedan acceder a los servicios de un sistema de software.

Los diseñadores de programas y protocolos suelen proporcionar varias APIs para que los programadores puedan adaptar fácilmente sus aplicaciones y utilizar los servicios disponibles en sus productos.

Un API habitual de UNIX es Berkeley Sockets; Microsoft lo ha implementado denominándolo **Windows Socket.**

## 2.2. El modelo TCP/IP

La arquitectura del protocolo TCP/IP fue definida por el IETF, organismo encargado de establecer los protocolos y la arquitectura de Internet. Este modelo se remonta a la ARPANET y se suele denominar modelo DoD. La arquitectura del protocolo DoD es anterior a la del modelo de referencia OSI, que data de 1979. Por ello, no es posible establecer una correspondencia sin ambiguedades entre los modelos DoD y OSI. En la figura, se aprecia el modelo de Internet de cuatro capas estableciendo las posibles correspondencias con el modelo OSI.




En el modelo arriba definido, no cabe una equivalencia exacta entre el modelo OSI y el modelo TCP/IP; sin embargo, es posible realizar una aproximación y hablar de un modelo TCP/IP de 4 capas. Así se tiene la Capa de acceso a la red, Capa de interred, la capa host-host y la capa Proceso-aplicación.

### 2.2.1 Capa de acceso a la red

Capa que se encarga de conectar al host con el hardware de red local. Para ello hace uso de conectores que le permiten realizar la conexión al medio físico. La data viaja a este nivel bajo la forma de una secuencia de bits. También, hace uso de un protocolo adecuado que le permite acceder al canal de comunicaciones de manera exitosa. La ubicación de las computadoras se realiza a través del uso de direcciones físicas.

### 2.2.2 Capa de interred

Segunda capa del modelo TCP/IP, muy importante porque a este nivel se realiza el direccionamiento o ubicación de computadoras sobre la base de direcciones lógicas o IP, que permiten la posibilidad de reconocer direcciones de red y de un host en particular dentro de dicha red. También, a este nivel, la información se encapsula bajo la forma de datagramas IP, las que a su vez se encapsularán en las tramas de la capa de acceso a la red. Se hace uso de un servicio de datagramas sin conexión. La selección de las rutas que le permitirán alcanzar a un destino determinado se realiza en función de un algoritmo de ruteo. Este ruteo es vital y realizado por los ruteadores que constituyen dispositivos encargados de efectuar la selección de las rutas más óptimas para alcanzar un destino cualquiera.

### 2.2.3 Capa de transporte

Esta capa se encuentra orientada a la conexión y proporciona una transmisión confiable de datos mediante la detección y corrección de datos de extremo a extremo. Garantiza que los datos sean transferidos a través de una red de manera exacta y en el orden apropiado. Retransmite cualquier dato no recibido por el nodo destino. Para ello trabaja con los llamados acuses de recibo. También, otorga garantía contra la duplicación de datos entre los nodos emisor y receptor.

### 2.2.4 Capa de proceso-aplicación

Es muy parecida a la capa de aplicación del modelo OSI. Sirve como interfaz de comunicación y proporciona servicios de aplicación específicos. A este nivel se encuentran las aplicaciones típicas de Internet como el e-mail, transferencia de archivos, WWW y los terminales virtuales.

# Autoevaluación

1. Enumere las  funciones de la capa de transporte del modelo TCP/IP.
2. ¿Qué capas del modelo OSI no se encuentran presentes en el modelo TCP/IP?
3. ¿En qué capa del modelo TCP/IP se garantiza el acceso al canal de comunicaciones?
4. Enumere las aplicaciones de Internet presentes en la capa de aplicación de la suite TCP/IP.
5. Enumere las principales características del modelo  OSI.
6. ¿Qué funciones cumple la capa de red?
7. Brevemente, defina el concepto de SAP.
8. ¿Qué es una API? Defina brevemente.

# Para recordar

- La arquitectura del protocolo TCP/IP fue definida por el IETF, organismo encargado de establecer los protocolos y la arquitectura de Internet.

- El modelo TCP/IP presenta cuatro capas. Así se tiene la Capa de acceso a la red, Capa de interred, la capa host-host y la capa Proceso-aplicación.

- La capa de interred se encarga de la distribución de los datos a través de una interred.

- OSI proporciona una visualización abstracta del funcionamiento de una red, desde el cableado que conecta las computadoras hasta los programas que se emplearán para la comunicación.

- Según el modelo OSI, la capa de transporte asigna una identificación de punto de acceso a servicio (SAP) a cada paquete (puerto es el término TCP/IP correspondiente a un punto de acceso a servicio). La ID de un SAP es una dirección que identifica el proceso que ha originado el mensaje.

- Un API es un conjunto de reglas que permiten que las aplicaciones escritas por los usuarios puedan acceder a los servicios de un sistema de software.
- Los diseñadores de programas y protocolos suelen proporcionar varias APIs para que los programadores puedan adaptar fácilmente sus aplicaciones y utilizar los servicios disponibles en sus productos.

- Un API habitual de UNIX es Berkeley Sockets; Microsoft lo ha implementado denominándolo Windows Sockets.

SEMANA

3

# Protocolo IP

**TEMA**

Protocolo IP

**OBJETIVOS ESPECÍFICOS**

- Conocer la estructura de capas del Protocolo IP
- Conocer el esquema de direccionamiento IP

**CONTENIDOS**

- Direccionamiento IP
- Datagrama IP

**ACTIVIDADES**

- Revisan el esquema de direccionamiento classfull IP.
- Hacen uso de la técnica de lluvia de ideas para enumerar las etapas del proceso de fragmentación de los datagramas IP.

# 3 Introducción

La capa de interred se encarga de la distribución de los datos a través de una interred. IP (protocolo Internet) es el protocolo principal de esta capa y asume la mayor cuota de responsabilidad.

El RFC 791 contiene las especificaciones actuales de IP que han sido ampliadas en los RFC 919,922 y 950.

IP utiliza otros protocolos para llevar a cabo tareas específicas. El protocolo de mensajes de control de Internet (ICMP – Internet Control Messaging Protocol) se utiliza para entregar los mensajes a la capa host-host. También, se utilizan protocolos de encaminamiento para hacer más eficaz a IP.

Las principales funciones llevadas a cabo por IP son las siguientes:

- Direccionamiento
- Fragmentación y reensamblaje de datagramas
- Entrega de datagramas a través de la interred

De todas estas funciones, el direccionamiento es la más importante.

## 3.1. Direccionamiento IP

TCP/IP utiliza una dirección que emplea el protocolo IP siguiendo un esquema que permite identificar de manera única cada nodo de la red.

La identificación de un nodo en una interred requiere de dos datos: la red específica a la que está conectado el nodo y la identificación del nodo en esa red.

Los protocolos superiores de TCP/IP no utilizan directamente las direcciones hardware de la red. En vez de eso, se hacen uso de direcciones lógicas para identificar los hosts; además, estas direcciones contienen las direcciones de la red.

Las direcciones lógicas permiten que TCP/IP sea resistente a los cambios del hardware de la red, pues si se cambia la tarjeta de red, la dirección física también cambia.

### 3.1.1 Características del direccionamiento IP

Un sistema de comunicaciones proporciona un *servicio universal de comunicaciones* si permite que cualquier computadora host se comunique con cualquier otro host, así que para que el sistema de comunicaciones sea universal, necesita un método aceptado de manera global para identificar cada computadora que se conecte a él.

Este fue el esquema seguido por los diseñadores de Internet y desembocó en las llamadas direcciones IP.

### 3.1.2. Formato de una dirección IP

Las direcciones IP tienen una longitud de 32 bits y constan de dos campos:

- Un campo identificador de red (**netid),** que identifica la red a la que esta conecta
- Un campo identificador de host (**hostid**), que identifica a cada host de una red específica

Según TCP/IP, una red consiste en un grupo de hosts que pueden comunicarse directamente sin utilizar un encaminador.

Todo host TCP/IP que forma parte de la misma red debe tener asignado el mismo identificador de red.

Los hosts con distintos identificadores de red deben comunicarse a través de un encaminador.

### 3.1.3. Clases de Direcciones

Al momento de crear las direcciones IP, se partió del supuesto de que existirían los siguientes tipos de red:

- Una pequeña cantidad de redes compuestas por un gran número de hosts
- Una cantidad moderada de redes compuesta por un número intermedio de hosts
- Una gran cantidad de redes compuestas por un pequeño número de hosts

Fue esta la razón por la que se tomó la decisión de definir clases de direcciones IP adaptadas a estas situaciones. Para ello, se asignó un número distinto de bits a los identificadores de red de las distintas clases.

Las direcciones se organizan en 4 octetos.

- **REDES CLASE A (/8)**

  Las direcciones de clase A comienzan con un bit 0.

  El primer octeto de la dirección IP comprende el identificador de red y los 3 octetos restantes son el identificador del host.

- **REDES CLASE B (/16)**

  Las direcciones de clase B comienzan con los bits 10.

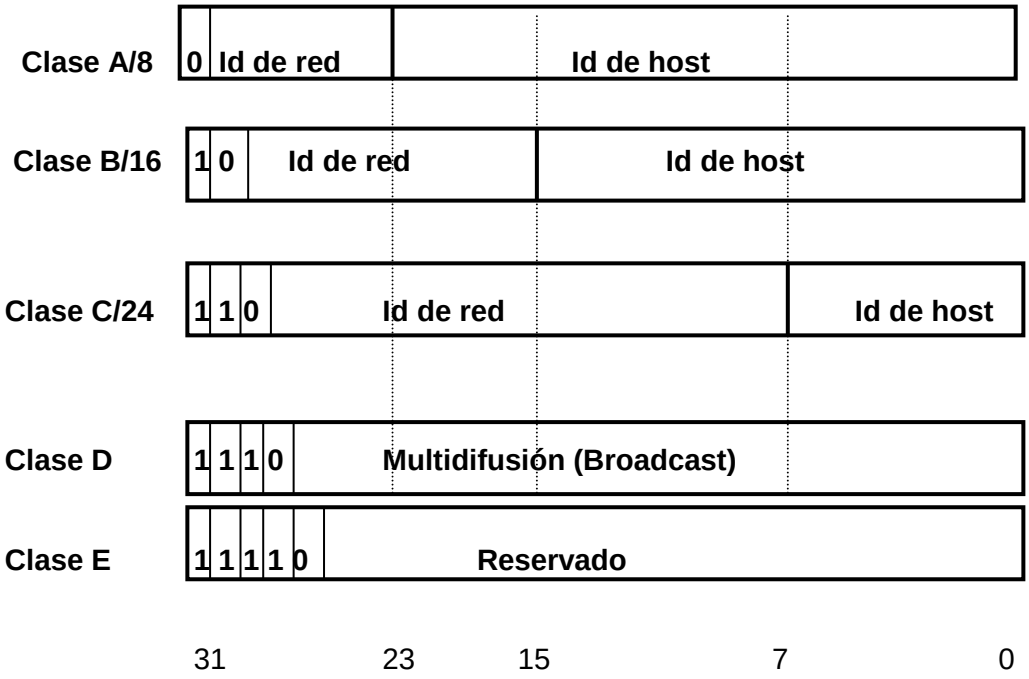
  Los dos primeros octetos de la dirección IP comprende el identificador de red y los dos octetos restantes son los identificadores del host.

- **REDES CLASE C (/24)**
  Las direcciones de clase C comienzan con los bits 110.

  Los tres primeros octetos de la dirección IP comprende el identificador de red y el octeto restante es el identificador del host.

- **REDES CLASE D**
  Las direcciones de clase D comienzan con los bits 1110. Este tipo de dirección no se asigna a un host, sino que es utilizado para identificar grupos de multidifusión. Por lo tanto, son muy usadas para transmisiones de tipo multicast. Ejemplo de esto son las direcciones multicast utilizadas por los protocolos OSPF, EIGRP para enviar información de ruteo.

- Las direcciones de clase E comienzan con los bits 11110. Su uso es experimental.




Todas las redes que se conectan a Internet deben configurarse con direcciones IP asignadas por InterNIC.

Actualmente, las direcciones clase C son las únicas disponibles. Las direcciones de clase A se agotaron hace mucho tiempo. Las pocas direcciones de clase B que quedan disponibles están reservadas para empresas corporativas de la industria. Lo negativo es que las direcciones de clase C están disminuyendo; además, tienen el impacto negativo de incrementar el tamaño de las tablas de ruteo globales de Internet. Si se desean utilizar los servicios de un proveedor para conectarse a Internet, este proporcionará sus direcciones IP. Para tal efecto, los proveedores disponen de bloques de direcciones IP.

Está muy difundido el uso de las direcciones IP en notación decimal, por lo que cada octeto se representa en forma decimal entre 0 y 255.

### 3.1.4. Restricción de las direcciones IP

Al momento de asignar las direcciones IP, se observa que existen algunas direcciones que se encuentran reservadas por tener un uso especial y no pueden utilizarse para identificar redes ni hosts. Entre estas tenemos las siguientes:

- Los identificadores de red y de hosts con valor 0 (00000000 binario) no están permitidos, ya que significan "esta red". La dirección IP 155.123.0.0 identifica la red 155.123. La dirección 0.0.0.35 identifica el host 35 de la red local.

- El identificador de red 127 (01111111) tiene un uso especial. Es una dirección de retorno utilizada para verificar la configuración de la red. Los mensajes dirigidos a 127 se reflejan en lugar de enviarse a la red.

- Los identificadores de host con valor 255 quedan restringidos para las difusiones. Un mensaje dirigido a 255.255.255.255 se envía a todos los hosts de la red. Un mensaje dirigido a 183.20.255.255 se envía a todos los hosts de la red 183.20.

- El último octeto de una dirección IP no puede tener los valores 0 ni 255.

| Clase | Desde | Hasta | Id. De red | Id. De Host |
|---|---|---|---|---|
| A | 1 | 126 | 126 | 16'777,214 |
| B | 128 | 191 | 16,384 | 65,534 |
| C | 192 | 223 | 2'097,152 | 254 |

## 3.2 Datagrama IP

Como se había descrito anteriormente, el protocolo IP cumple tres funciones importantes:

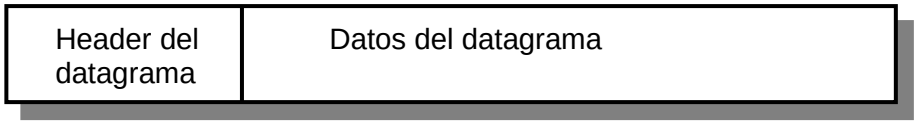
1. Definir la unidad básica para la transferencia de datos utilizada a través de una inter-red TCP/IP

2. Realizar la función de ruteo, seleccionando la ruta por la que los datos serán enviados

3. Además de aportar especificaciones formales para el formato de los datos y el ruteo, el IP incluye un conjunto de reglas que le dan forma a la idea de entrega de paquetes no confiable. Las reglas caracterizan la forma en que los

anfitriones y ruteadores deben procesar los paquetes, cómo y cuándo se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados.

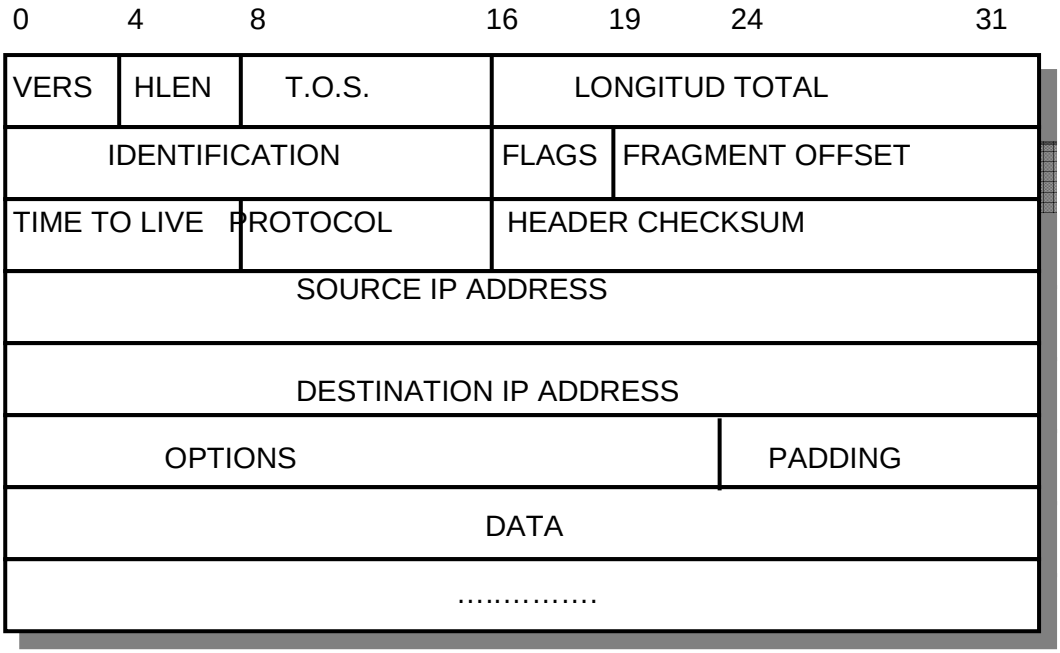
Esta parte tratará sobre la forma que tienen las unidades básicas de transferencia manejadas por IP. Estas constan de un encabezado y datos, donde el encabezado contiene información sobre la dirección de la fuente y la del destino. Estas unidades son los datagramas internet o datagramas IP.
El encabezado de un datagrama contiene direcciones IP, en tanto que el encabezado de la trama contiene direcciones físicas.




### 3.2.1. Formato del datagrama

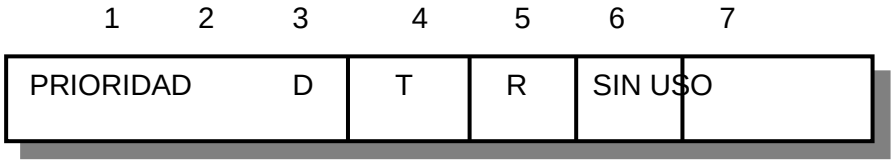
Una vez descrita la disposición general de un datagrama, se verá su contenido en mayor detalle.
Debido a que el procesamiento de los datagramas se da en el software, el contenido y el formato no está condicionado por ningún tipo de hardware.

- **VERS :**
  Este primer campo de 4 bits contiene la versión del protocolo IP utilizado para crear el datagrama.
  Todo software IP debe verificar el campo de versión antes de procesar un datagrama para asegurarse de que el formato corresponde al tipo de formato que espera el software.
- **HLEN :**
  Campo Longitud de Encabezado de 4 bits que proporciona la longitud del encabezado. Todos los campos del encabezado tienen longitudes fijas excepto para el campo OPTIONS de IP y su correspondiente campo PADDING.



- **TOTAL LENGHT :**
  Proporciona la longitud del datagrama IP medido en bytes, incluyendo los bytes del encabezado y los datos. Dado que el campo TOTAL LENGHT tiene una longitud de 16 bits, el tamaño máximo posible de un datagrama IP es de $2^{16}$ o 64 kb. En la mayor parte de las aplicaciones, esta no es una limitación severa, pero puede volverse una consideración importante en el futuro, si las redes de alta velocidad llegan a transportar paquetes de datos superiores a los 64Kb.

- **TYPE OF SERVICE (ToS) :**
  Conocido informalmente como el campo Type of Service, Este es un campo de 8 bits que especifica cómo debe manejarse el datagrama. Así mismo, está subdividido en 5 subcampos.




- **PRIORIDAD :**
  Estos tres bits especifican la prioridad del datagrama, con valores que abarcan desde 0 (prioridad normal) hasta 7 (control, de red). Co ello, permite indicar al emisor la importancia de cada datagrama.
  Los bits D, T y R especifican el tipo de transporte deseado para el datagrama:

  **D:** Solicita procesamiento con retardos cortos.
  **T:** Solicita alto desempeño.
  **R:** Solicita alta confiabilidad.

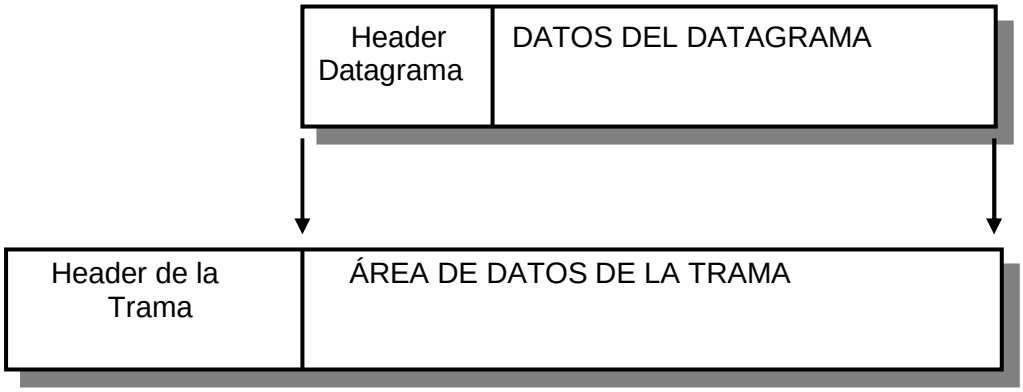
  Sin embargo, no es posible para una inter-red garantizar siempre el tipo de transporte solicitado. Por lo tanto, se debe pensar en una solicitud de transporte como en una simple indicación para los algoritmos de ruteo y no como en un requerimiento obligatorio. Si un ruteador conoce más que una posible ruta para alcanzar un destino determinado, puede utilizar el campo de tipo de transporte para seleccionar una con las características más cercanas a la petición deseada.
  Por ejemplo, si se acepta que un ruteador puede seleccionar entre una línea arrendada de baja capacidad y una conexión vía satélite con un gran ancho de banda(pero con un retardo alto); además, si cierto datagrama tiene el bit D activado, solicitando que la entrega sea lo mas rápida posible, el router encaminará este datagrama a través de la línea arrendada de baja capacidad pero poco retardo; mientras que otro datagrama que forma parte de un archivo de datos grande podría tener activado el bit T, que solicitará que el recorrido se haga a través de una ruta que incluya un satélite de alta capacidad.

  Por lo tanto, el campo TYPE OF SERVICE constituye una indicación para el algoritmo de ruteo que ayuda en la selección de una ruta entre varias hacia un destino. No obstante, una inter-red, eso si no garantiza la realización del tipo de transporte solicitado.

### 3.2.2 Encapsulación de datagramas

Los siguientes campos del datagrama IP tienen que ver con la manera en que estos últimos se relacionan con las tramas de las redes físicas.

A diferencia de las tramas de las redes físicas que pueden ser reconocidas por el hardware, los datagramas son manejados por el software. Estos pueden tener cualquier longitud seleccionado por el diseño del protocolo. Así se tiene que el CAMPO TOTAL LENGHT, al tener 16 bits de tamaño, limita al datagrama a un máximo de 64 kb. Sin embargo, este límite puede modificarse en versiones de protocolos recientes.
Como los datagramas se mueven de una máquina a otra deben transportarse siempre a través de una red física subyacente; por lo tanto, cada datagrama debe estar en capacidad de viajar en tramas físicas distintas. Debido a ello el datagrama IP deberá viajar encapsulado dentro de la trama Ethernet.

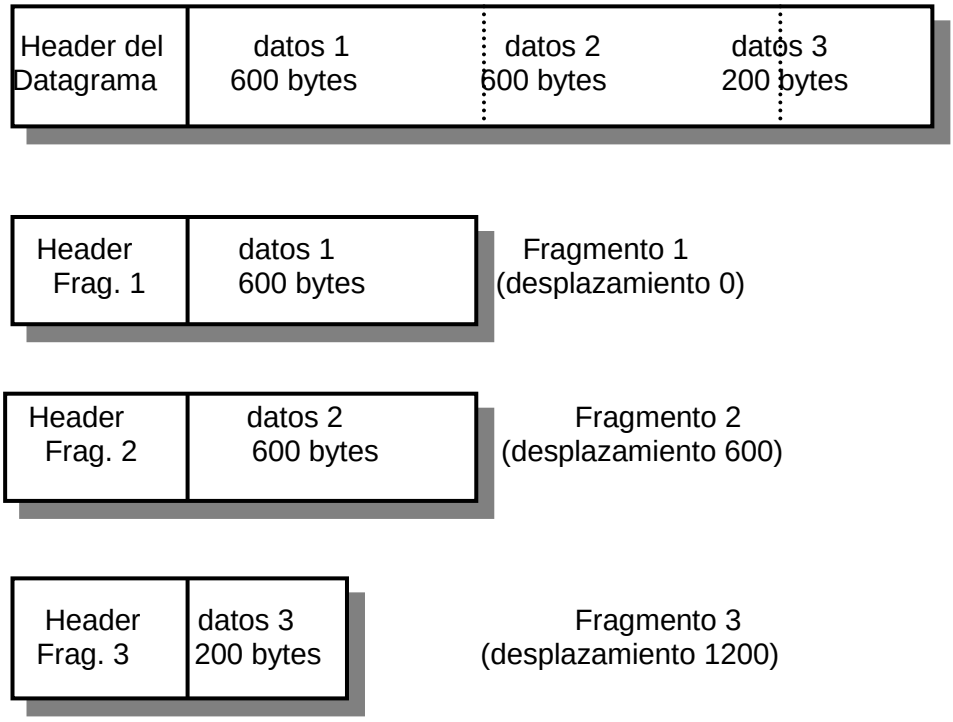



Encapsulación del datagrama IP en una trama Ethernet. La red física trata al datagrama entero, incluyendo el encabezado, como si se trataran de datos.

### 3.2.3 Fragmentación

En un caso ideal, el datagrama IP se ajusta dentro de la trama física haciendo que la transmisión a través de la red física sea eficiente. El campo Ethertype utiliza el valor 0800 hex para especificar un datagrama IP encapsulado.
El tamaño del datagrama IP depende del tipo de trama a utilizarse; por ello, las tramas Ethernet soportan la transferencia de 1500 bytes, mientras que FDDI soporta un promedio de 4,470 bytes por trama. Estos límites de transferencias son los llamados MTU y pueden ser muy pequeños (algunas tecnologías de hardware limitan la transferencia a 128 bytes o menos). La mayoría de las veces los datagramas IP son más grandes que las tramas IP, es decir, estos no se ajustan dentro de una sola trama. Por lo tanto, TCP/IP establece una forma para dividir datagramas en pequeños fragmentos, cuando el datagrama necesita viajar a través de una red que tiene un MTU pequeño. Las pequeñas piezas dentro de un datagrama se conocen como fragmentación.
Generalmente, la fragmentación se da en un ruteador a lo largo del trayecto entre la fuente del datagrama y su destino final. El ruteador recibe un datagrama de una red con una MTU grande y debe enviarlo a una red en la que la MTU es más pequeña que el tamaño del datagrama. IP define un tamaño de fragmento múltiplo de 8. Esta es la razón por la que los últimos fragmentos de un datagrama no encajan perfectamente en una trama.

Luego, los fragmentos se deben reensamblar para producir una copia completa del datagrama original, antes de que pueda procesarse en su lugar de destino.
El protocolo IP no limita los datagramas a un tamaño pequeño ni garantiza que los datagramas grandes serán entregados sin fragmentación. La fragmentación y el reensamblado se dan automáticamente sin que la fuente deba realizar ninguna acción especial.
Fragmentar un datagrama significa dividirlo en varios segmentos; sin embargo, cada fragmento tiene el mismo formato que el datagrama original.




Cada fragmento contiene un encabezado de datagrama que duplica la mayor parte del encabezado del datagrama original (excepto por un bit en el campo FLAGS que muestra que este es un fragmento), seguido por tantos datos como puedan ser acarreados en el fragmento, siempre y cuando la longitud total se mantenga en un valor menor a la MTU de la red en la que debe viajar.

### 3.2.4. Reensamblado de fragmentos

Luego que un datagrama ha sido fragmentado, los fragmentos viajan como datagramas separados hacia su destino final donde serán reensamblados. Hacer esto tiene dos desventajas:
Dado que los datagramas no son reensamblados inmediatamente después de pasar a través de una red con un MTU pequeña, los fragmentos pequeños deben transportarse en esa forma desde el punto de fragmentación hasta el destino final. Reensamblar los datagramas en el destino final puede implicar, también, que el proceso se realice con cierta ineficiencia.
Si se pierde cualquier fragmento, el datagrama no podrá reensamblarse. La máquina de recepción hace que arranque un temporizador de reensamblado

cuando recibe un fragmento inicial. Si el temporizador termina antes que todos los fragmentos lleguen, la máquina de recepción descartará los fragmentos sin procesar el datagrama. Aun con estas desventajas, la realización del reensamblado en el destino final trabaja bien. Esto permite que cada fragmento se pueda rutear de manera independiente sin necesidad de que ruteadores intermedios almacenen o reensamblen fragmentos.

### 3.2.5. Control de fragmentación

La fragmentación del datagrama IP es controlado a través de tres campos: IDENTIFICATION, FLAGS y FRAGMENT OFFSET.

- **IDENTIFICATION :**

  Contiene un entero único que identifica el datagrama. Cuando un ruteador fragmenta un datagrama , éste copia la mayor parte de los campos del encabezado del datagrama dentro de cada fragmento. El campo IDENTIFICATION debe copiarse. El propósito principal es permitir que el destino tenga información acerca de qué fragmentos pertenecen a qué datagramas.

  Conforme llega cada fragmento , el destino utiliza el campo IDENTIFICATION junto con la dirección de la fuente del datagrama para identificar el datagrama.

  Las computadoras que envían datagramas IP deben generar un valor único para el campo IDENTIFICATION de cada datagrama.

  Una de estas técnicas consiste en que IP establezca un contador global en memoria, y lo incremente cada vez que se crea un datagrama nuevo y asigna el resultado al campo IDENTIFICATION del datagrama.

- **FRAGMENT OFFSET :**

  Para un fragmento, el campo FRAGMENT OFFSET especifica el desplazamiento en el datagrama original de los datos que se están acarreando en el fragmento, medido en unidades de 1 byte, y comienza con un desplazamiento igual a cero.

  Para reensamblar el datagrama, el destino debe obtener todos los fragmentos comenzando con el fragmento que tiene asignado un desplazamiento igual a cero, hasta el fragmento con el desplazamiento de mayor valor.

  Los fragmentos no necesariamente llegarán en orden: además, no existe comunicación entre el ruteador que fragmentó el datagrama y el destino que trata de reensamblarlo.

- **FLAGS :**

  Los dos bits de orden menor del campo FLAGS controlan la fragmentación.

  La fragmentación y reensamblado son procedimientos automáticos que se dan a bajo nivel en el sistema operativo, invisible para el usuario final. Sin embargo, para probar el software de inter-red o depurar problemas operacionales, es importante probar el tamaño de los datagramas en los que se presenta la fragmentación.

- **Bit de no fragmentación**

El primer bit de control ayuda en esta prueba especificando en qué momento se debe fragmentar en datagrama. Cuando está puesto a 1 especifica que el datagrama no debe fragmentarse.

- **Bit de más fragmentos**

  El bit de orden inferior en el campo FLAGS específica si el fragmento contiene datos intermedios del datagrama original o de la parte final.
  La utilidad de este bit se nota cuando estamos en el extremo receptor y el software IP trata de reensamblar un datagrama. En este caso, el IP necesitará saber si ha recibido todos los fragmentos del datagrama. Si efectúa la consulta en el campo TOTAL LENGHT del fragmento, este le informa acerca del tamaño del fragmento y no del datagrama original, así que no es posible utilizar este campo para saber si ha reunido a todos los fragmentos.
  El bit more fragments resuelve este problema con facilidad: cuando el destino recibe un fragmento con el bit more fragments desactivado, sabe que este fragmento acarrea datos del extremo final del datagrama original.
  A partir de los campos FRAGMENT OFFSET y TOTAL LENGHT es posible calcular la longitud total del datagrama original.

- **Tiempo de vida ( time to live o ttl)**

  Este campo especifica la duración, en segundos, del tiempo que el datagrama tiene permitido permanecer en el sistema de red de redes.
  Cuando un datagrama es introducido en una red, se establece un tiempo máximo durante el cual el datagrama puede permanecer allí.
  Los ruteadores y los hosts que procesan los datagramas deben decrementar el campo TIME TO LIVE cada vez que pasa un datagrama y eliminarlo de la red cuando su tiempo ha concluido.
  La técnica utilizada para llevar a cabo esto es bastante simple. Los ruteadores, a lo largo de un trayecto, desde una fuente hasta un destino, es configurado para decrementar por 1 el campo TIME TO LIVE cuando se procesa el encabezado del datagrama.
  Cada vez que un campo TIME TO LIVE llega a cero, el ruteador descarta el datagrama y envía un mensaje de error a la fuente. La idea de establecer un temporizador para los datagramas es interesante, ya que garantiza que los datagramas no viajarán a través de la red de redes de manera indefinida.

- **Protocolo :**

  Este campo es parecido al campo Ethetype utilizado en una trama de red.
  El valor en el campo PROTOCOL especifica qué protocolo de alto nivel se utilizó para crear el mensaje que se está transportando en el área DATA de un datagrama, es decir, especifica el formato del área DATA.

- **Header checksum :**

  Este campo asegura la integridad de los valores del encabezado. La suma de verificación IP se forma considerando al encabezado como

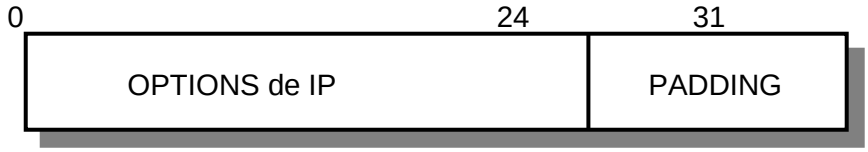
una secuencia de enteros de 16 bits, sumándolos juntos mediante el complemento aritmético a uno y, después, toma el complemento a uno del resultado.
Para propósito de cálculo de la suma de verificación, el campo HEADER CHECKSUM se asume como igual a cero.
Esta suma de verificación sólo se aplica a los valores del encabezado y no a los datos. Esta separación de la suma de verificación del encabezado y los datos, permite que el tiempo de procesamiento y ruteo disminuya, pues los routers sólo deben calcular la suma del encabezado, dejando a los protocolos de alto nivel su propio esquema de verificación de error.

- **Source IP address y destination IP address**

  Estos campos de 32 bits cada uno contienen las direcciones IP de os equipos transmisores y receptores involucrados. Estos campos fuente y destino nunca cambian.
  El campo DATA es a donde viajan, efectivamente, los datos. Su longitud es variable y dependiente de la cantidad de información que se esté enviando.

- **Campo options y padding**

  El campo OPTIONS de IP tiene una longitud variable y el campo PADDING depende de las opciones seleccionadas. Este representa un grupo de bits puestos a cero que podrían ser necesarios para asegurar que la extensión del encabezado sea un múltiplo exacto de 32 bits.




- **Campo options :**

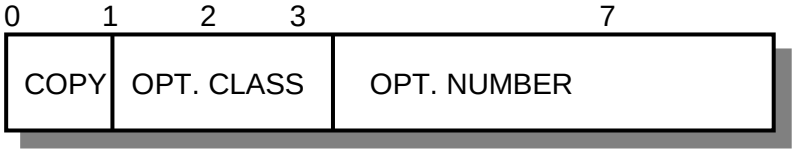
  Este campo aparece a continuación de la dirección destino y no se requiere en todos los datagramas; las opciones se incluyen en principio para pruebas de red o depuración. Sin embargo, el procesamiento de las opciones es parte integral del protocolo IP.
  Su longitud es variable dependiendo de lo que se esté seleccionando.
  Algunas opciones tienen una longitud de un octeto; estas consisten en un solo octeto de código de opción. Otras tienen longitudes variables.
  Cuando las opciones están presentes en un datagrama, aparecen contiguas, sin separadores especiales entre ellas.
  El byte de código de opción se divide en tres campos:

  - **Copy :**

    Flag de un bit que controla la forma en que los ruteadores tratan las opciones durante la fragmentación.
    Bit COPY = 1, específica que la opción se debe copiar en todos los fragmentos.

  Bit COPY = 0, la opción solo se debe copiar en el primer fragmento y no en el resto.

- **Option class y option number :**
  Especifican la clase general de opción y establecen una opción específica en esta clase.




División del byte de código de opción en tres campos

Así, se tiene una serie de opciones que se encuentran definidas en la tabla:

| OPTION CLASS | Significado |
|---|---|
| 0 | Control de red o datagrama |
| 1 | Reservado para uso futuro |
| 2 | Depuración y medición |
| 3 | Reservado para uso futuro |

En la siguiente tabla, se listan las opciones de número u OPTION NUMBER, que acompañan a los datagramas IP. Como se aprecia, existen 8 opciones posibles IP con una clase en forma numérica y los códigos de número.

| Option Class | Option Number | Longitud | Descripción |
|---|---|---|---|
| 0 | 0 | - | Fin de la lista de opciones. Se utiliza si las opciones no terminan al final del encabezado. |
| 0 | 1 | - | No operación (se utiliza para alinear octetos en una lista de opciones) |
| 0 | 2 | 11 | Seguridad y restricciones de manejo (para aplicaciones militares) |
| 0 | 3 | Var | Ruteo no estricto de fuente<br>Se utiliza para rutear un datagrama a través de una trayectoria específica. |
| 0 | 7 | var | Registro de ruta<br>Se utiliza para registrar el trayecto de una ruta. |
| 0 | 8 | 4 | Identificador de flujo. Se utiliza para transportar un identificador de flujo SATNET (Obsoleto) |
| 0 | 9 | Var | Ruteo estricto de fuente<br>Se utiliza para establecer la ruta de un datagrama en un trayecto específico. |
| 2 | 4 | Var | Sello de tiempo de internet.<br>Se usa para registrar sellos de hora a lo largo de una ruta. |

- **Opción de registro de ruta**

Las opciones de ruteo y sello de hora (timestamp) son las más interesantes, porque proporcionan una manera de monitorear o controlar la forma en que la red de redes maneja las rutas de los datagramas.
Esta opción permite a la fuente crear una lista de direcciones IP y arreglarla para que cada ruteador que maneje el datagrama añada su propia dirección IP a la lista.

- **Opción de ruta fuente**

  La opción de ruta fuente permite proporcionar al emisor una forma en la que este puede determinar una ruta a través de internet.
  Por ejemplo, para probar el desempeño de una red física dada N, el administrador de la red puede utilizar la ruta de fuente para forzar a los datagramas IP a viajar a través de la red N, incluso si los ruteadores normalmente seleccionan una ruta que no está incluida en esa trayectoria.

  Existen dos formas de ruteo de fuente: Ruteo estricto de fuente y ruteo no estricto de fuente.

  1. **Ruteo estricto de fuente**
     Este ruteo especifica las direcciones exactas que los datagramas deben seguir para llegar a su destino. La ruta entre dos direcciones sucesivas de la lista debe consistir en una sola red física. Se producirá un error si el ruteador no puede seguir una ruta estricta de fuente.
  2. **Ruteo no estricto de fuente**
     También, incluye una secuencia de direcciones IP. Esta especifica que el datagrama debe seguir la secuencia de direcciones IP, pero permite múltiples saltos de redes entre direcciones sucesivas de la lista.
     Ambas opciones de ruteo de fuente requieren que los ruteadores, a lo largo de la trayectoria, anoten su propia dirección de red local en la lista de direcciones. Así, cuando un datagrama llega a su destino, contiene una lista con todas las direcciones recorridas, igual que la lista producida por la opción de registro de ruta.

- **Opción de sello de hora**

  El sello de hora define la hora y la fecha en la que un ruteador manejó el datagrama, expresado en milisegundos de acuerdo con la hora GMT.
  El sello de hora (timestamp) debe considerarse como una estimación, independientemente de la representación, pues cada máquina reportará una hora de acuerdo con su reloj local y los relojes pueden diferir. En este caso, los ruteadores registran sus direcciones IP con sellos de horas dados.

# Autoevaluación

1. Enumere las capas del modelo TCP/IP. Brevemente, definir a cada uno de ellas.
2. Identifique cada una de las clases de direcciones IP.
3. ¿Qué direcciones IP no es posible asignar y por qué razones?
4. Brevemente, defina las funciones llevadas a cabo por el protocolo IP.
5. ¿Qué funciones cumple el protocolo IP? Responda brevemente.
6. ¿Si no existiera el campo TYPE OF SERVICE (TOS) del datagrama IP, que errores se darían en su funcionamiento?
7. ¿Qué valor numérico contiene el campo Ethertype de la trama Ethernet cuando transporta un datagrama IP?
8. Brevemente defina qué es el MTU de una red local.
9. Enumere los campos que controlan el proceso de fragmentación.
10. Explique la razón de tener un campo TTL en el datagrama IP.

# Para recordar

- La arquitectura del protocolo TCP/IP fue definida por el IETF, organismo encargado de establecer los protocolos y la arquitectura de Internet.

- El modelo TCP/IP presenta cuatro capas. Así se tiene la capa de acceso a la red, capa de interred, la capa de transporte y la capa proceso-aplicación.

- La capa de interred se encarga de la distribución de los datos a través de una interred.

- Además de aportar especificaciones formales para el formato de los datos y el ruteo, el IP incluye un conjunto de reglas que le dan forma a la idea de entrega de paquetes no confiable. Las reglas caracterizan la forma en que los anfitriones y ruteadores deben procesar los paquetes, cómo y cuándo se deben generar los mensajes de error y las condiciones bajo las cuales los paquetes pueden ser descartados.

- Como los datagramas se mueven de una máquina a otra, deben transportarse siempre a través de una red física subyacente; por lo tanto cada datagrama debe estar en capacidad de viajar en tramas físicas distintas. Debido a ello el datagrama IP deberá viajar encapsulado dentro de la trama Ethernet.

- El campo Ethertype utiliza el valor 0800 hex para especificar un datagrama IP encapsulado.

- El campo TTL especifica la duración, en segundos, del tiempo que el datagrama tiene permitido permanecer en el sistema de red de redes.

- El campo Header Checksum asegura la integridad de los valores del encabezado. La suma de verificación IP se forma considerando al encabezado como una secuencia de enteros de 16 bits.

SEMANA

4

# Direccionamiento IP - Subredes

**TEMA**

Direccionamiento basado en subredes

**OBJETIVOS ESPECÍFICOS**

- Conocer el concepto de subred
- Conocer las pautas de diseño de subredes
- Identificar las restricciones en el diseño de subredes

**CONTENIDOS**

- Subredes
- Prefijo de Red Extendida
- Consideraciones para el diseño de subredes

**ACTIVIDADES**

- Calculan las máscaras de subred dadas ciertas condiciones de hosts.

## 4. Subredes

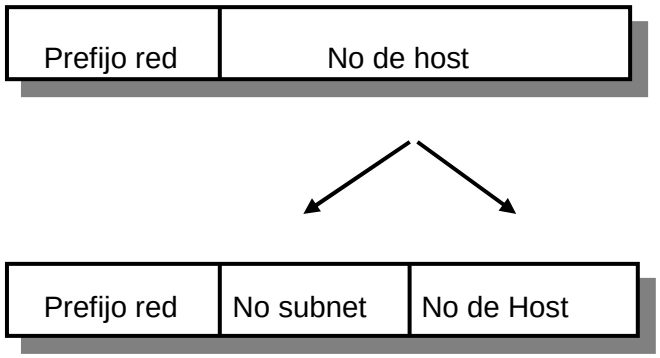
En 1985, el RFC 950 definió un procedimiento homogéneo para apoyar el desarrollo de las subredes, o la división de una red de Clase A, B o C en pequeñas partes. Las subredes se desarrollaron con la finalidad de solucionar algunos problemas que Internet estaba empezando a experimentar con la estructura de direccionamiento de dos direcciones:

- Las tablas de ruteo de Internet empezaron a crecer demasiado.
- Los administradores de red debían solicitar otro número de red de Internet antes que una nueva red pudiera ser instalada en su sitio.

Además de solucionar estos inconvenientes, las subredes permiten lo siguiente:

- Pueden utilizarse distintas tecnologías LAN en distintos lugares.
- Las conexiones de las LAN son limitadas.
  Un cable de red admite un número limitado de dispositivos. Si se supera el límite, pueden utilizarse encaminadores para conectar redes adicionales.
- Congestión
  Cuando una red se satura, su rendimiento puede caer en picada. En este caso es posible crear una interred para reducir el tráfico en determinados segmentos de la red.

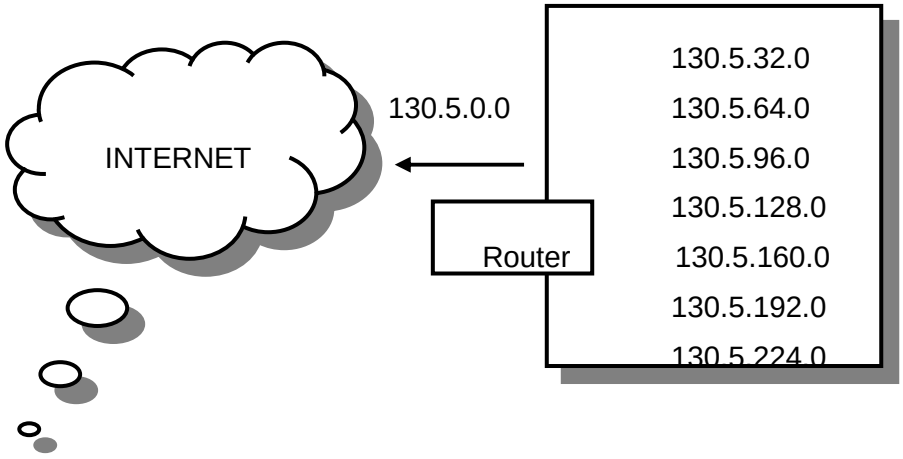
Estos problemas fueron atacados agregando otro nivel de jerarquía a la estructura de dirección IP. En lugar de la jerarquía de dos niveles, las subredes utilizan una jerarquía de tres niveles.




Las subredes atacan el problema del crecimiento de las tablas de ruteo asegurando que la estructura de la subred de una red no es visible fuera de la red privada de la organización. El ruteo desde Internet a una subred de una dirección IP cualquiera es la misma, sin importar en qué subred se encuentra el host destino. Esto es así pues todas las subredes de una dirección IP usan el mismo prefijo de red, pero diferentes números de subnet.

Los routers dentro de la organización necesitan diferenciar entre todas las subredes, pero en el caso de los routers de Internet todas las subredes están dentro de un solo registro de una tabla de ruteo.

Esto permite al administrador de la red introducir de manera arbitraria mayor complejidad dentro de la red privada sin afectar el tamaño de las tablas de ruteo de Internet. La organización puede, por lo tanto, asignar distintos números de subred para cada una de sus redes internas. Esto permite a la empresa implementar subredes adicionales sin la necesidad de obtener un nuevo número de red de Internet.




Red Privada

En la figura, se puede apreciar cómo un sitio con varias redes lógicas usan un direccionamiento basado en subredes para cubrir a todas ellas con una sola dirección de red Clase B (/16). El router acepta todo el tráfico de Internet a la red 130.5.0.0 y direcciona el tráfico hacia las redes interiores basándose en el tercer octeto de la dirección IP.

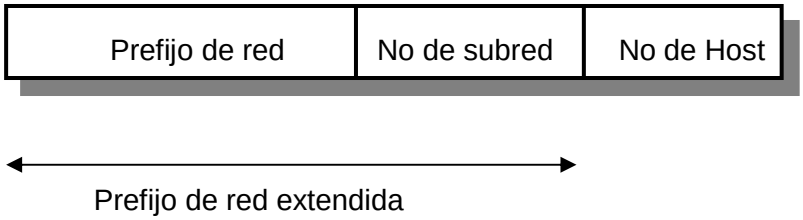
El uso de las subredes dentro de las redes privadas proporciona varios beneficios:

- El tamaño de las tablas de ruteo de Internet no crecen, porque el sitio no necesita obtener direcciones adicionales y los avisos de ruteo para todas las subredes interiores están combinadas en una solo registro de la tabla de ruteo.
- El administrador local tiene la flexibilidad de implementar subredes adicionales sin la necesidad de obtener un nuevo número de Internet.
- El Route Flapping (rápido cambio de rutas ) dentro de la red privada no afecta las tablas de ruteo de Internet, dado que los routers de Internet no saben acerca de la accesibilidad de las subredes individuales. Estos solo conocen de la accesibilidad de la dirección de la red inicial.

### 4.1. Prefijo de Red Extendida

Los routers de Internet solo usan el prefijo de red de la dirección destino para rutear el tráfico hacia entornos con subredes. Los routers dentro del entorno de las subredes usan el ***prefijo de red extendida*** para rutear el tráfico entre las subredes individuales.

El prefijo de red extendida está compuesto por el prefijo de red y el número de subred.

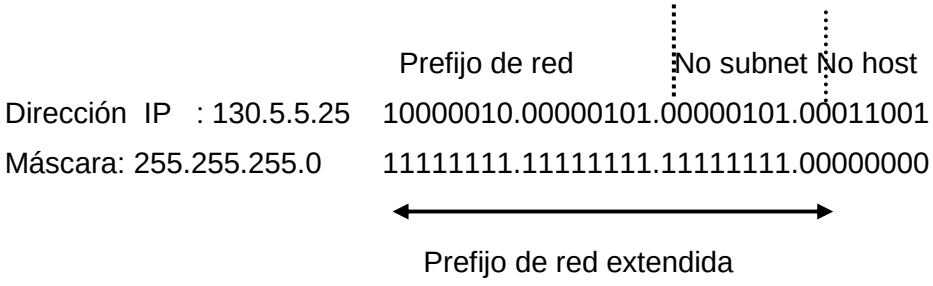



El prefijo de red extendida ha sido tradicionalmente identificado como la máscara de subred.

Por ejemplo, si se tiene la dirección /16, 130.5.0.0 y se desea utilizar todo el tercer octeto para representar el número de subred, se requiere de una máscara 255.255.255.0.

Los bits de la máscara de subred y la dirección de Internet tienen una correspondencia de uno-a-uno.

Los bits de la máscara de subred están puestos en 1 si el sistema que examina la dirección debe tratar el correspondiente bit de la dirección IP como parte del prefijo de red extendido. Los bits de la máscara están puestos en 0 si el sistema debe tratar a los bits como parte del número de host.




Los protocolos de ruteo modernos, frecuentemente, usan el término de ***longitud de red extendida*** en lugar de máscara de subred.

La longitud de prefijo es igual al número de bits contiguos de la máscara tradicional.

Esto significa que especificar una dirección de red 130.5.5.25 con una máscara de subred 255.255.255.0 puede ser también expresada como 130.5.5.25/24. La notación **/<longitud>** es más compacta y fácil de entender que escribir la máscara en su forma tradicional.

Asi por ejemplo :

130.5.5.25 10000010.00000101.00000101.00011001

255.255.255.0 11111111.11111111.11111111.00000000

o

130.5.5.25/24 10000010.00000101.00000101.00011001

prefijo de red extendida: 24 bits

Sin embargo, es importante notar que todos los protocolos de ruteo modernos todavía utilizan la máscara de subred. No existen todavía estándares de ruteo que tengan un campo de un byte en su cabecera para colocar el prefijo de longitud de red extendida. Es más, todos los protocolos de ruteo todavía requieren la máscara de subred completa con sus 4 octetos completos.

### 4.2. Consideraciones para el diseño de subredes

La implementación de un sistema basado en subredes requiere de un planeamiento muy cuidadoso por parte del administrador de la red. Existen 4 preguntas básicas que deben ser respondidas antes que todo diseño sea llevado a cabo.

1. Cuántas subredes totales necesita la organización hoy?
2. Cuántas subredes totales necesitará la organización del futuro?
3. Cuántos host existen en la subred más grande actualmente?
4. Cuántos host existirán en la subred más grande en el futuro?

Luego de haber respondido estas preguntas, el proceso de planeamiento se puede realizar en tres pasos:

1. El primer paso consiste en tomar el número máximo de subredes requeridas y redondearlo a la más próxima potencia de 2.Así, si la organización necesita 9 subredes, 2 a la 3 (8) no será suficiente, así que mejor será redondear a 2 a la 4 (16). Esto significa que siempre es importante dejar suficiente espacio para un futuro crecimiento de la organización.
2. El segundo paso es asegurarse que existen suficientes direcciones para los host de la subred más grande. Si la subred más grande necesita actualmente 50 direcciones de host actualmente, 2 a la 5 (32) no proporcionará suficientes direcciones de host, así que el redondeo se realizará en 2 a la 6 (64).

3. El paso final es asegurarse que la dirección asignada a la organización proporciona suficientes bits para implementar el plan de direccionamiento de subredes. En caso de encontrar problemas en este paso, una alternativa de solución sería utilizar números de red del espacio de direcciones privadas (RFC 1918) usados para la conectividad interna y usar un **Network Address Translator (NAT)** para proporcionar acceso externo a Internet.

### 4.3. La subnet Todo-0s y la subnet Todo-1s

Cuando las subredes fueron definidas en el RFC 950, se prohibió el uso de las subredes todo-0s y todo-1s. La razón para esta restricción fue el de eliminar toda posible situación que pudiera, potencialmente, confundir un router de clase total (classful). Hay que hacer notar que actualmente los routers pueden ser classless y classful al mismo tiempo, pueden estar corriendo RIP-1 ( protocolo classful) y BGP-4 (un protocolo classles) .

### 4.4. Subred todo-0s :

En relación a la subred todo-0s, un router requiere que cada tabla de ruteo incluya el prefijo de longitud de ruteo /<longitud> para poder diferenciar entre un ruteo a la subnet todo-0s o un ruteo a toda la red.

Por ejemplo, si se usa RIP-1 que no proporciona una máscara o un prefijo de longitud para cada ruteo, la información de ruteo par la subred 193.1.1.0/27 y para la red 193.1.1.0/24 son idénticas e iguales a 193.1.1.0. Sin algo que le informe acerca del prefijo de longitud o la máscara, un router no puede reconocer la diferencia entre un ruteo a la subnet todo-0s o un ruteo a toda la red.

Subnet Route : 193.1.1.0/27 11000001.00000001.00000001.00000000

Prefijo de 27 bits

Network

Route : 193.1.1.0/24 11000001.00000001.00000001.00000000

Prefijo de 24 bits

### 4.5. Subred todo-1s:

Respecto a la subred todo-1s, un router requiere que cada registro en la tabla de ruteo incluya el prefijo de longitud para que así pueda determinar si una señal de broadcast (dirigida o general a todas las subredes) pueda ser enviada sólo a la subred todo-1s o a toda la red.

Así, cuando la tabla de ruteo no contiene una máscara o un prefijo de longitud para cada ruta, puede darse la confusión por el hecho de que la misma dirección de broadcast (193.1.1.255) es usada tanto para toda la red 193.1.1.0/24 y para la subnet todo-1s 193.1.1.224/27.

Broadcast

A la subnet : 193.1.1.224/27 11000001.00000001.00000001.11111111

Prefijo de 27 bits

Broadcast

A la red : 193.1.1.224/24 11000001.00000001.00000001.11111111

Prefijo de 24 bits

# Autoevaluación

1. Si se asume que se tiene la dirección de red 200.35.1.0 /24, defina el prefijo extendido de red que permita la creación de 20 hosts en cada subred.
   El número de subredes no es pertinente para el diseño.
   Calcule lo siguiente:
   a. Máscara de subred (notación decimal)
   b. Longitud de prefijo extendida de red
   c. Número de subredes resultantes
   d. Obtener las primeras 6 subredes resultantes
   e. Obtener la dirección de broadcast para todas las subredes

2. Se le ha asignado una dirección de red 132.45.0.0/16. Se desean obtener 8 subredes. El número de hosts no es pertinente.
   Calcule lo siguiente:
   a) Máscara de subred (notación decimal)
   b) Longitud de prefijo extendida de red
   c) Número de subredes resultantes
   d) Obtener las primeras 6 subredes resultantes
   e) Obtener la dirección de broadcast para todas las subredes

# Para recordar

- Las subredes atacan el problema del crecimiento de las tablas de ruteo asegurando que la estructura de la subred de una red no es visible fuera de la red privada de la organización.

- Los routers dentro de la organización necesitan diferenciar entre todas las subredes, pero en el caso de los routers de Internet todas las subredes están dentro de un solo registro de una tabla de ruteo.

- Los routers de Internet solo usan el prefijo de red de la dirección destino para rutear el tráfico hacia entornos con subredes. Los routers dentro del entorno de las subredes usan el prefijo de red extendida para rutear el tráfico entre las subredes individuales.

SEMANA

5

# Direccionamiento VLSM

**TEMA**

- Direccionamiento VLSM

**OBJETIVOS ESPECÍFICOS**

- Definir VLSM y describir brevemente las razones para su utilización
- Definir la unificación de rutas y su resumen a medida en relación con VLSM

**CONTENIDOS**

- Ventajas de utilizar VLSM

**ACTIVIDADES**

- Utilizan los  medios interactivos.
- Calculan las direcciones VLSM.

**5. Ventajas de utilizar VLSM**

Cuando se trabaja bajo el esquema de direccionamiento basado en subredes anteriormente visto, se observa que las longitudes de las máscaras tienen un tamaño fijo independientemente del número de equipos que se requieran realmente por cada subred. Esto, en algunos casos, desperdicia direcciones; por ejemplo, en el caso que las necesidades de subredes no sean homogéneas.
Por lo tanto, se hizo necesario realizar una corrección al anterior esquema. Esto dio origen al direccionamiento basado en VLSM.

Con el VLSM, un administrador puede usar:

- Una máscara grande en una red con pocos hosts
- Una máscara corta en una red con muchos hosts

Para poder usar VLSM, es necesario que se utilice un protocolo que soporte este esquema de direccionamiento:
Los ruteadores CISCO soportan los siguientes protocolos de ruteo classless: OSPF, EIGRP, RIPv2 y el ruteo estático.

VLSM permite que una organización utilice más de una máscara de subred con el mismo valor de de dirección de red.
La implementación de VLSM es muchas veces llamada como “subnetting de una subred”.

IPv4 ofreció una estrategia de direccionamiento escalable durante un tiempo, pero que pronto dio como resultado una asignación de direcciones totalmente ineficiente. Es posible que IPv4 pronto sea reemplazado por IP versión 6 (IPv6) como protocolo dominante de Internet. IPv6 posee un espacio de direccionamiento prácticamente ilimitado y algunas redes ya han empezado a implementarlo.
Durante los últimos veinte años, los ingenieros del IETF han modificado con éxito el protocolo IPv4 para que pueda sobrevivir al crecimiento exponencial de Internet. Producto de tal esfuerzo es el esquema de direccionamiento VLSM, que constituye una de las modificaciones que ha ayudado a reducir la brecha entre los protocolos IPv4 e IPv6.
Un concepto y requisito muy importante en las redes modernas es la escalabilidad. Cuando una red es escalable, puede crecer de manera lógica, eficiente y económica. El protocolo de enrutamiento utilizado en una red ayuda a determinar la escalabilidad de la red. Es importante elegir bien el protocolo de enrutamiento. La versión 1 del Protocolo de Información de Enrutamiento (RIP v1) es adecuada en el caso de redes pequeñas. Sin embargo, no es escalable para las redes de gran envergadura. La versión 2 de RIP (RIP v2) se desarrolló para superar estas limitaciones.

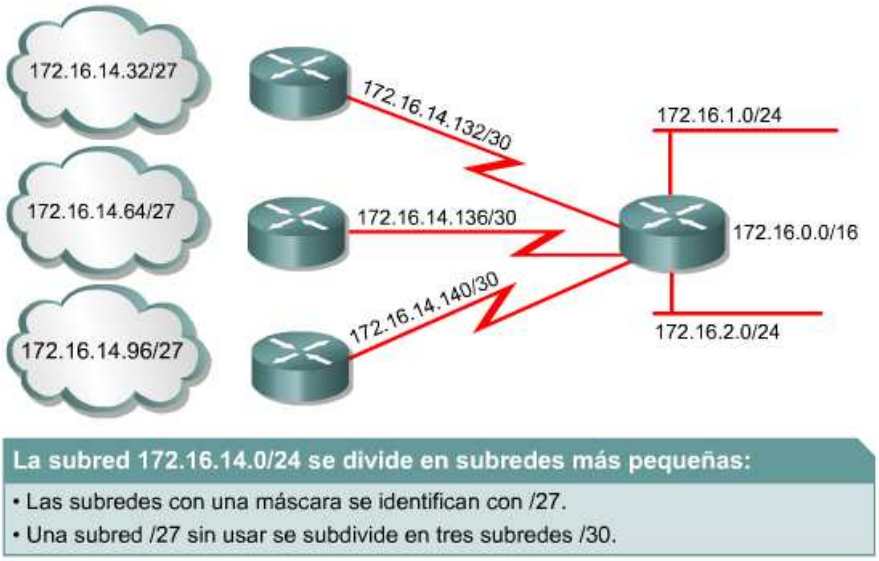
## 5.1 VLSM

### 5.1.1 ¿Qué es VLSM y por qué se usa?

Conforme las subredes IP han crecido, los administradores han buscado formas de utilizar su espacio de direccionamiento con más eficiencia.
Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts, y una máscara corta en las subredes que tienen muchos hosts. Sin embargo, para usar VLSM un administrador de red debe usar un protocolo de enrutamiento que brinde soporte para él. Los routers Cisco admiten VLSM con los protocolos de enrutamiento OSPF, IS-IS integrado, EIGRP, RIP v2 y el enrutamiento estático.
VLSM permite que una organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM

maximiza la eficiencia del direccionamiento y realmente consiste en la división de subredes en subredes.

Un protocolo de enrutamiento que utiliza VLSM le confiere al administrador de red la libertad para usar distintas máscaras de subred para redes que se encuentran dentro de un sistema autónomo.

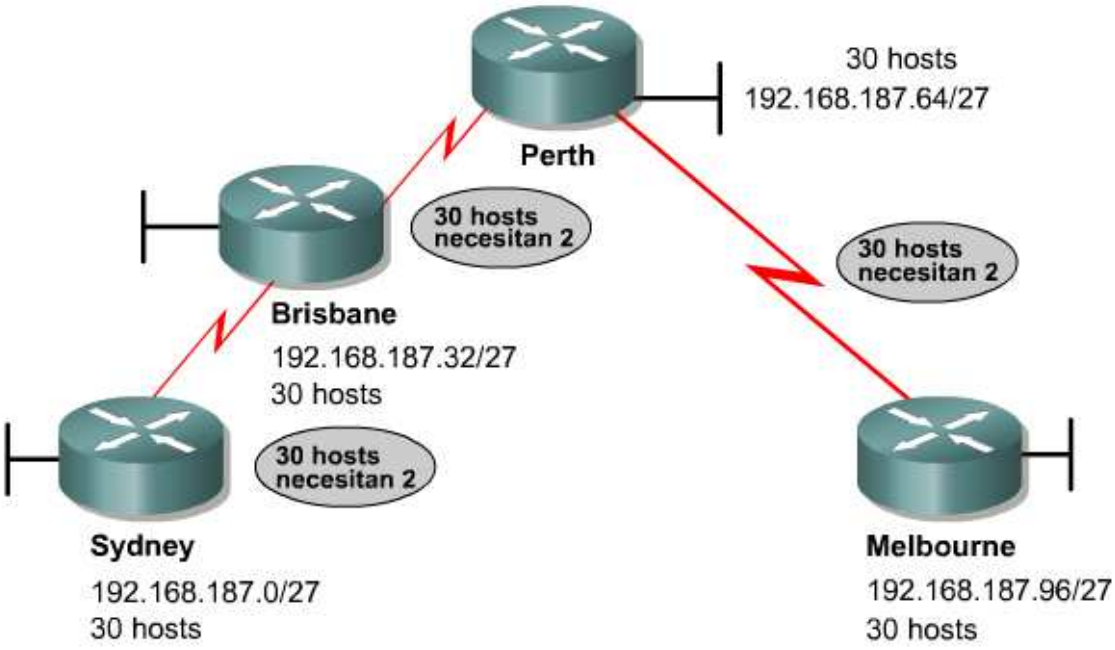



La Figura 2 muestra un ejemplo de cómo un administrador de red puede usar una máscara de 30 bits para las conexiones de red, una máscara de 24 bits para las redes de usuario e incluso una máscara de 22 bits para las redes con hasta 1000 usuarios.

| Máscaras de subred | | |
|---|---|---|
| 255.255.255.252 | 11111111 11111111 11111111 11111100 | 30 bits |
| 255.255.255.0 | 11111111 11111111 11111111 00000000 | 24 bits |
| 255.255.252.0 | 11111111 11111111 11111100 00000000 | 22 bits |

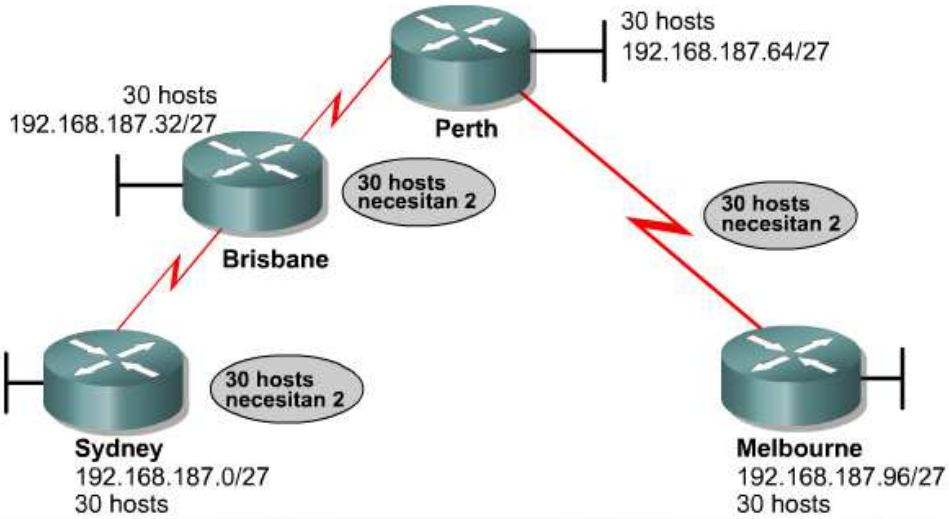
### 5.1.2 Un desperdicio de espacio

Cada una de las oficinas remotas de Sydney, Brisbane, Perth y Melbourne puede tener 30 hosts. El equipo se da cuenta que tiene que direccionar los tres enlaces WAN punto a punto entre Sydney, Brisbane, Perth y Melbourne. Si el equipo utiliza las tres últimas subredes para los enlaces WAN, se usarán todas las direcciones disponibles y no habrá más espacio para el crecimiento. El equipo, también, habrá desperdiciado las 28 direcciones de host de cada subred simplemente para direccionar tres redes punto a punto.




### 5.1.3 Cuándo usar VLSM

El equipo de administración de red ha decidido evitar el desperdicio debido al uso de la máscara /27 en los enlaces punto a punto. El equipo aplica VLSM al problema de direccionamiento.




Use VLSM en los enlaces punto a punto que sólo necesitan dos direcciones de host válidas en lugar de 30.

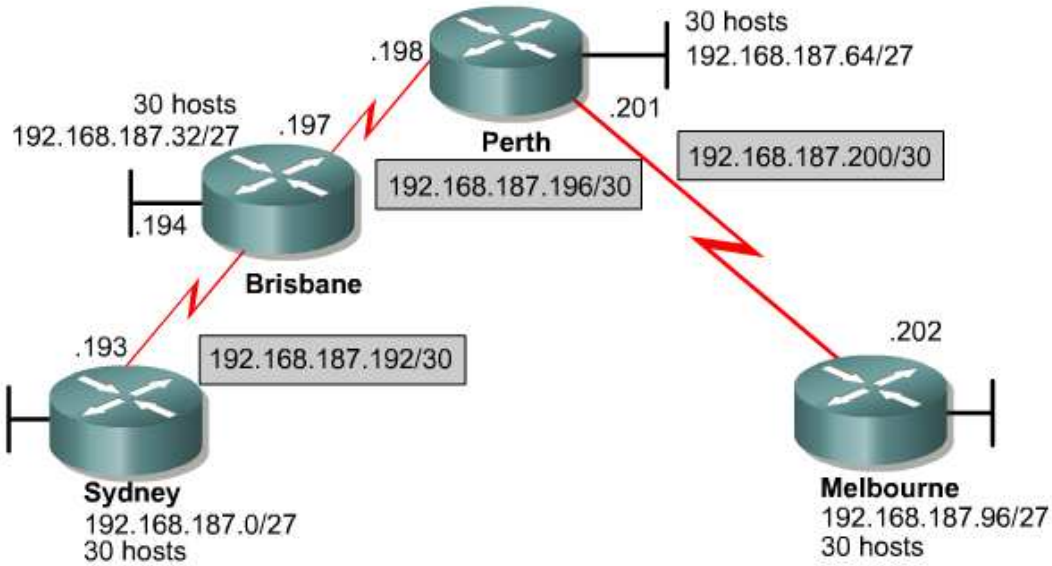
Para aplicar VLSM al problema de direccionamiento, el equipo divide la dirección Clase C en subredes de distintos tamaños. Subredes más grandes se crean para las LAN. Se crean subredes muy pequeñas para los enlaces WAN y otros casos especiales. Una máscara de 30 bits se utiliza para crear subredes con sólo dos direcciones de host válidas. Ésta es la mejor solución para las conexiones punto a

punto. El equipo tomará una de las tres subredes que anteriormente quedaba asignada a los enlaces WAN y la volverá a dividir en subredes con una máscara de 30 bits.

| Número de subred | Dirección de subred | |
|---|---|---|
| subred 0 | 192.168.187.0 | /27 |
| subred 1 | 192.168.187.32 | /27 |
| subred 2 | 192.168.187.64 | /27 |
| subred 3 | 192.168.187.96 | /27 |
| subred 4 | 192.168.187.128 | /27 |
| subred 5 | 192.168.187.160 | /27 |
| subred 6 | 192.168.187.192 | /27 |
| subred 7 | 192.168.187.224 | /27 |

| Número de subred | Dirección de subred | |
|---|---|---|
| sub-subred 0 | 192.168.187.192 | /30 |
| sub-subred 1 | 192.168.187.196 | /30 |
| sub-subred 2 | 192.168.187.200 | /30 |
| sub-subred 3 | 192.168.187.204 | /30 |
| sub-subred 4 | 192.168.187.208 | /30 |
| sub-subred 5 | 192.168.187.212 | /30 |
| sub-subred 6 | 192.168.187.216 | /30 |
| sub-subred 7 | 192.168.187.220 | /30 |

En el ejemplo, el equipo ha tomado una de las últimas tres subredes, la subred 6, y la ha dividido nuevamente en varias subredes. Esta vez, el equipo utiliza una máscara de 30 bits. Después de aplicar VLSM, el equipo posee ocho intervalos de direcciones que se pueden usar para los enlaces punto a punto.

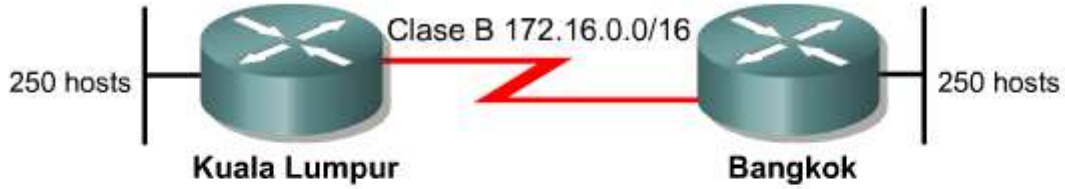



Observe la máscara /27 para las LAN y la máscara /30 para los enlaces seriales.

### 5.1.4 Cálculo de subredes con VLSM

Una máscara de subred debe satisfacer los requisitos de una LAN con una máscara de subred y los requisitos de una WAN punto a punto con otra máscara de subred.

El ejemplo incluye una dirección Clase B de 172.16.0.0 y dos LAN que requieren al menos 250 hosts cada una. Si los routers usan un protocolo de enrutamiento con clase, el enlace WAN debe formar una subred de la misma red de Clase B. Los protocolos de enrutamiento con clase, como RIP v1 e IGRP, no admiten VLSM. Sin VLSM, el enlace WAN necesitaría la misma máscara de subred que los segmentos LAN. La máscara de 24 bits de 255.255.255.0 puede admitir 250 hosts.

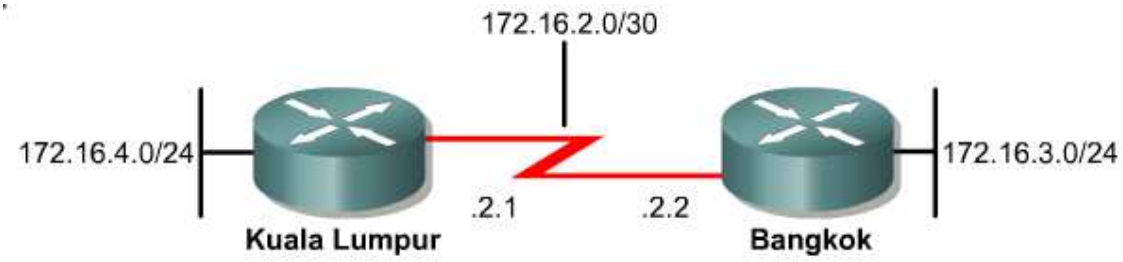



Cada LAN debe admitir más de 250 hosts. La red Clase B 172.16.0.0/16 se puede dividir en subredes con una máscara de 24 bits de 255.255.255.0 para crear subredes lo suficientemente grandes para cada LAN.

El enlace WAN sólo necesita dos direcciones, una para cada router. Esto significa que se han desperdiciado 252 direcciones.

Si se hubiera utilizado VLSM, todavía se podría aplicar una máscara de 24 bits en los segmentos LAN para los 250 hosts. Se podría usar una máscara de 30 bits para el enlace WAN dado que sólo se necesitan dos direcciones de host.

Los enlaces WAN usan direcciones de subred con un prefijo de /30. Este prefijo sólo permite dos direcciones de host, que es lo que se necesita para una conexión punto a punto entre un par de routers.




El /30 significa que se pierden menos direcciones.

Hay que aclarar que las direcciones de subred utilizadas se generan cuando la subred 172.16.32.0/20 se divide en subredes /26. Para calcular las direcciones de

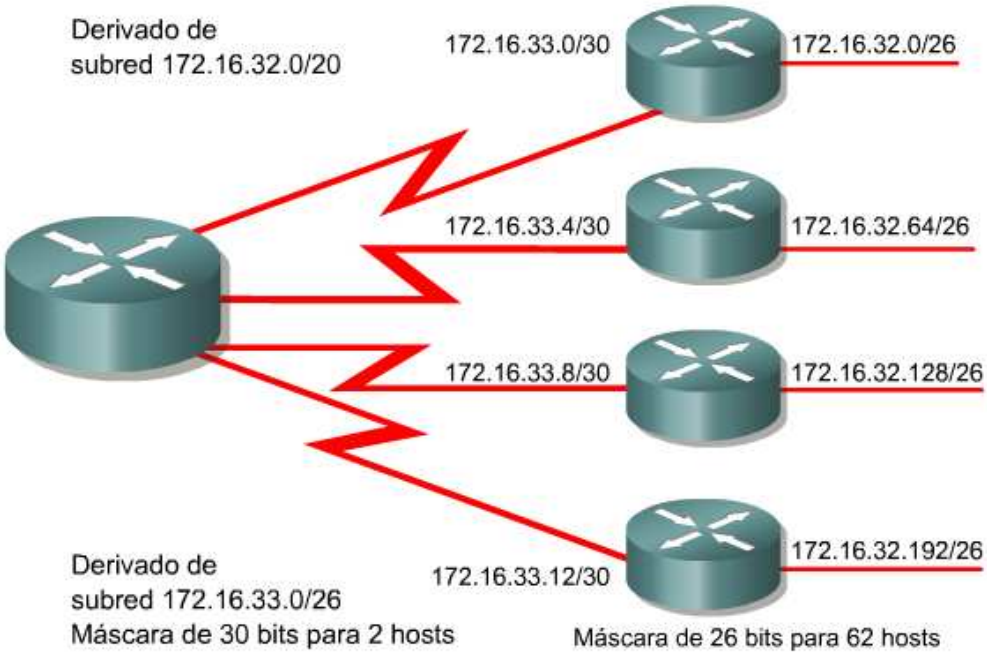
subred que se utilizan en los enlaces WAN, siga subdividiendo una de las subredes /26 que no se utilizan. En este ejemplo, 172.16.33.0/26 se sigue subdividiendo con un prefijo de /30. Esto permite obtener cuatro bits de subred adicionales y, por lo tanto, 16 ($2^4$) subredes para las WAN.

La dirección dividida en subredes es 172.16.32.0/20
La forma binaria es 10101100.00010000.00100000.00000000

La dirección VLSM es 172.16.32.0/26
La forma binaria es 10101100.00010000.0010 0000.00 000000

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **subred 1:** | 172 | • | 16 | .0010 | 0000.00 | 000000 = | 172.16.32.0/26 |
| **subred 2:** | 172 | • | 16 | .0010 | 0000.01 | 000000 = | 172.16.32.64/26 |
| **subred 3:** | 172 | • | 16 | .0010 | 0000.10 | 000000 = | 172.16.32.128/26 |
| **subred 4:** | 172 | • | 16 | .0010 | 0000.11 | 000000 = | 172.16.32.192/26 |
| **subred 5:** | 172 | • | 16 | .0010 | 0001.00 | 000000 = | 172.16.33.0/26 |
| | **Red** | | | **Subred** | **Subred VLSM** | **Host** | |

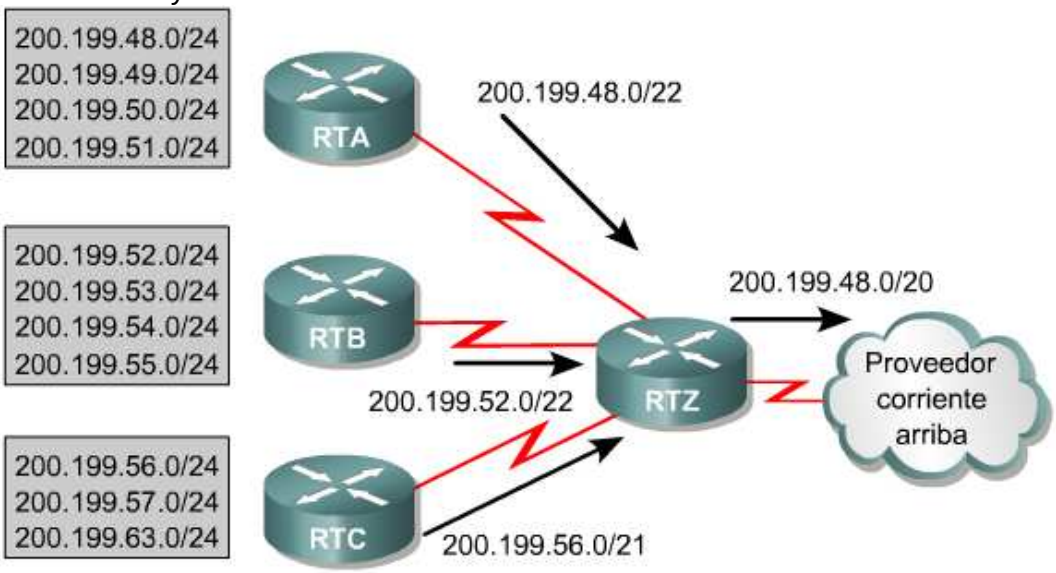
VLSM se puede usar para dividir en subredes una dirección que ya está dividida en subredes. Se puede tomar a modo de ejemplo, dirección de subred 172.16.32.0/20 y una red que necesita diez direcciones de host. Con esta dirección de subred, existen 212 – 2 ó 4094 direcciones de host, la mayoría de las cuales quedarán desperdiciadas. Con VLSM es posible dividir 172.16.32.0/20 en subredes para crear más direcciones de red con menos hosts por red. Cuando 172.16.32.0/20 se divide en subredes dando como resultado 172.16.32.0/26, existe una ganancia de 26 ó 64 subredes. Cada subred puede admitir 26 – 2 ó 62 hosts.



### 5.1.5 Unificación de rutas con VLSM

Existe un concepto muy importante que permite simplificar el número de direcciones de red que se agregan a una tabla de ruteo, la "sumarización" de direcciones. Cuando se utiliza VLSM, es importante mantener la cantidad de subredes agrupadas en la red para permitir la unificación o "sumarización". Por ejemplo, redes como 172.16.14.0 y 172.16.15.0 deberían estar cerca de manera que los routers sólo tengan que poseer una ruta para 172.16.14.0/23.

Sin el resumen de rutas, es probable que el enrutamiento por el backbone de Internet hubiera colapsado antes de 1997. Esta compleja jerarquía de redes y subredes de varios tamaños se resume en diferentes puntos con una dirección prefijo, hasta que la red completa se publica como sola ruta unificada de 200.199.48.0/22. El resumen de ruta o la superred, sólo es posible si los routers de una red utilizan un protocolo de enrutamiento sin clase, como OSPF o EIGRP. Los protocolos de enrutamiento sin clase llevan un prefijo que consiste en una dirección IP de 32 bits y una máscara de bits en las actualizaciones de enrutamiento.




El resumen de rutas reduce el tamaño de la tabla de enrutamiento al agregar rutas a varias redes en una sola superred.

El resumen de rutas que finalmente llega al proveedor contiene un prefijo de 20 bits común a todas las direcciones de la organización. Esa dirección es 200.199.48.0/22 ó 11001000.11000111.0011. Para que el resumen funcione, las direcciones se deben asignar cuidadosamente de manera jerárquica para que las direcciones resumidas compartan la misma cantidad de bits de mayor peso.

VLSM aumenta la flexibilidad del resumen de ruta, porque utiliza los bits de mayor peso compartidos a la izquierda, aun cuando las redes no sean contiguas.

| Direcciones | Primer octeto | Segundo octeto | Tercer octeto | Cuarto octeto |
|---|---|---|---|---|
| 192.168.98.0 | 11000000 | 10101000 | 01100010 | 00000000 |
| 192.168.99.0 | 11000000 | 10101000 | 01100011 | 00000000 |
| 192.168.100.0 | 11000000 | 10101000 | 01100100 | 00000000 |
| 192.168.101.0 | 11000000 | 10101000 | 01100101 | 00000000 |
| 192.168.102.0 | 11000000 | 10101000 | 01100110 | 00000000 |
| 192.168.105.0 | 11000000 | 10101000 | 01101001 | 00000000 |

**La ruta resumida es 192.168.96.0/20**

| | | | | |
|---|---|---|---|---|
| 192.168.96.0 | 11000000 | 10101000 | 01100000 | 00000000 |

**Otro ejemplo:**

| Direcciones | Primer octeto | Segundo octeto | Tercer octeto | Cuarto octeto |
|---|---|---|---|---|
| 172.16.0.0 | 10101100 | 00010000 | 00000000 | 00000000 |
| 172.16.2.0 | 10101100 | 00010000 | 00000010 | 00000000 |
| 172.16.3.128 | 10101100 | 00010000 | 00000011 | 10000000 |
| 172.16.4.0 | 10101100 | 00010000 | 00000100 | 00000000 |
| 172.16.4.128 | 10101100 | 00010000 | 00000100 | 10000000 |

**Respuesta:**

| | | | | |
|---|---|---|---|---|
| 172.16.0.0/21 | 10101100 | 00010000 | 00000000 | 00000000 |

**Ejemplo 1:**

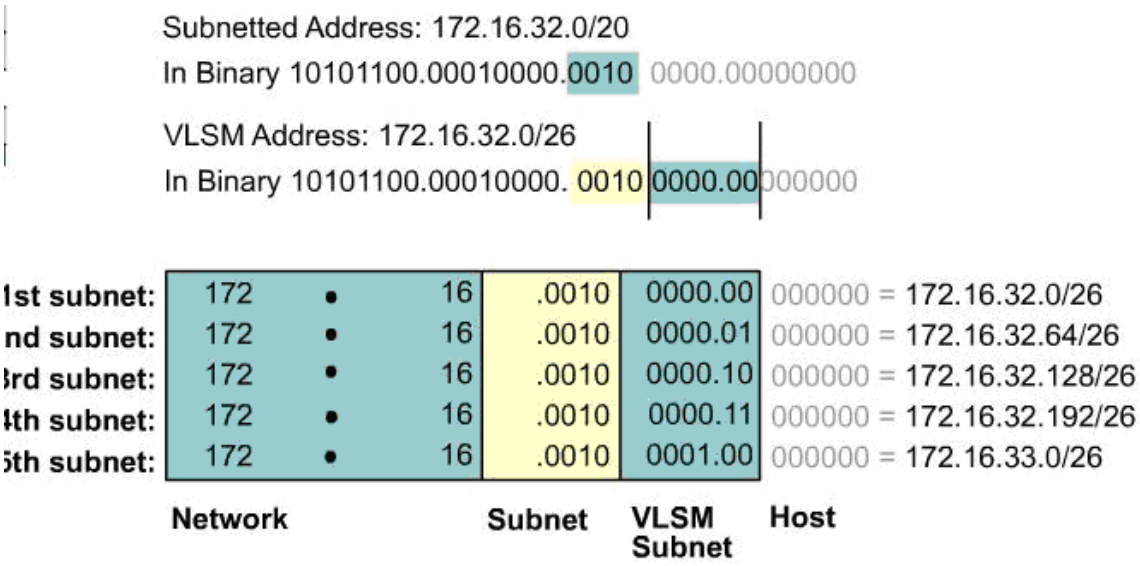
Dada una dirección de red Clase B: 172.16.0.0/16
Se busca obtener lo siguiente:

# de subnets = 12
# de hosts = 62 hosts por subnet

# de subnets = 2^N - 2 → se obtiene N=4

Sin embargo, se obtiene 12 bits para los hosts
# de hosts = 4096 hosts → sin embargo solo se quieren 62 hosts

Para no desperdiciar tantas IP, la solución es efectuar una reasignación de IPs mediante VLSM:
A partir de la subnet1: 172.168.32.0/20
Se va a obtener 62 subnets adicionales con una capacidad de direccionamiento de 62 hosts por cada subnet.




| Subnet Number | Subnet Address | |
|---|---|---|
| subnet 0 | 192.168.187.0 | /27 |
| subnet 1 | 192.168.187.32 | /27 |
| subnet 2 | 192.168.187.64 | /27 |
| subnet 3 | 192.168.187.96 | /27 |
| subnet 4 | 192.168.187.128 | /27 |
| subnet 5 | 192.168.187.160 | /27 |
| subnet 6 | 192.168.187.192 | /27 |
| subnet 7 | 192.168.187.224 | /27 |

| Subnet Number | Subnet Address | |
|---|---|---|
| sub-subnet 0 | 192.168.187.192 | /30 |
| sub-subnet 1 | 192.168.187.196 | /30 |
| sub-subnet 2 | 192.168.187.200 | /30 |
| sub-subnet 3 | 192.168.187.204 | /30 |
| sub-subnet 4 | 192.168.187.208 | /30 |
| sub-subnet 5 | 192.168.187.212 | /30 |
| sub-subnet 6 | 192.168.187.216 | /30 |
| sub-subnet 7 | 192.168.187.220 | /30 |

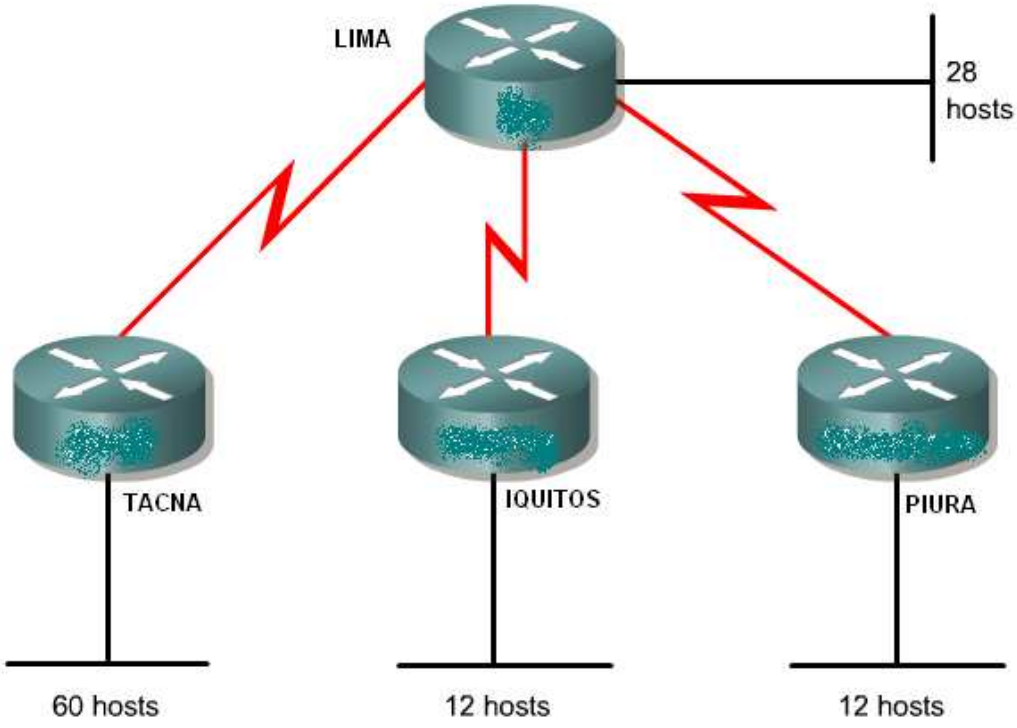
De esta manera, se ve que el utilizar VLSM en los enlaces WAN permite ahorrar direcciones IP para un posible crecimiento futuro.
Se utiliza una máscara /27 para las LAN, pero una máscara /30 para los enlaces WAN.

**Conclusión:**

Para solucionar este problema de direccionamiento, el equipo de diseño decide "subnetear" la dirección de red clase C, en subredes de tamaño variable. Subredes de solo 2 hosts son creadas para los enlaces WAN, a estas subredes se les llama también como subredes de 30-bit mask o de máscara de 30 bits.
Se observa que se tienen aún las subredes 4 y 5 disponibles para un posible crecimiento futuro.

**Ejemplo 3:**

Se cuenta con una dirección de red clase C: 192.168.10.0 /24
Tacna, Iquitos y Piura tienen enlaces WAN con Lima.
Tacna tiene 60 hosts.
Lima tiene 28 hosts.
Iquitos y Piura tienen 12 hosts cada una.
Se solicita efectuar un direccionamiento basado en VLSM para distribuir de manera más eficiente las direcciones IP que se tienen y reducir el tráfico de ruteo en el router de más alta jerarquía (LIMA).



# Autoevaluación

1. Dada una dirección de red: 140.25.0.0/16, se desea implementar un esquema de direccionamiento VLSM de tal manera que:

   a) De la red: 140.25.0.0/16 se obtengan 8 subredes (s0,s1,s2,…s7)
   b) De la s1, se desean obtener 32 subredes de igual número de hosts.
   c) De la s6, se desean obtener 16 subredes de igual número de hosts.

   Halle las direcciones de subredes VLSM resultantes, y el número de hosts que se tendrán para cada una de las subnets VLSM.

# Para recordar

- Con VLSM, un administrador de red puede usar una máscara larga en las redes con pocos hosts y una máscara corta en las subredes con muchos hosts.

- VLSM permite que una organización utilice más de una máscara de subred dentro del mismo espacio de direccionamiento de red. La implementación de VLSM maximiza la eficiencia del direccionamiento y, con frecuencia, se la conoce como división de subredes en subredes.

SEMANA

6

# Direccionamiento CIDR

**TEMA**

Direccionamiento de CIDR

**OBJETIVOS ESPECÍFICOS**

- Conocer el esquema de direccionamiento basado en CIDR
- Identificar las diferencias entre el direccionamiento IP y CIDR

**CONTENIDOS**

- Ruteo CIDR
- Características de funcionamiento
- CIDR: Implicaciones al asignarlo a Hosts
- Ventajas del CIDR

**ACTIVIDADES**

- Conocen las técnicas de direccionamiento CIDR.
- Utilizan el direccionamiento CIDR para “sumarizar” rutas.

## 6. RUTEO CIDR

(Classless Inter-Domain Routing)

Aproximadamente a mediados de 1992, el crecimiento exponencial de Internet comenzó a preocupar al IETF acerca de la posibilidad de que el sistema de ruteo utilizado en esa fecha pudiera adecuarse al crecimiento futuro de Internet.
Los problemas detectados eran los siguientes:

- El casi próximo agotamiento de las direcciones Clase B.
- El rápido crecimiento en el tamaño de las tablas de ruteo globales de Internet.
- El eventual agotamiento del espacio de direccionamiento basado en 32 bits de Ipv4.

El crecimiento proyectado para Internet hacía preveer que los primeros problemas arriba mencionados llegarían a ser críticos aproximadamente por 1994 ó 1995.
La respuesta a estos dos inmediatos desafíos fue el desarrollo del concepto de Superredes (Supernetting) o CIDR.
El tercer problema, el cual era de mayor proyección, se dejó para más adelante y resultó en el Ipv6, actualmente ya desarrollado. El protocolo CIDR fue documentado en 1993 en el RFC 1517, 1518, 1519 y 1520. CIDR proporciona dos características muy importantes que benefician el sistema global de ruteo.
CIDR elimina el concepto tradicional de redes de dirección Clase A, Clase B y Clase C. Esto permite la asignación eficiente del espacio de direccionamiento de IPV4. CIDR permite que un solo registro de la tabla de ruteo pueda representar el espacio de direccionamiento de miles de redes tradicional del tipo clasfull. Esto permite a un solo registro de la tabla de ruteo especificar cómo rutear el tráfico a muchas direcciones de red. Haciendo esto se puede reducir la información de ruteo en los routers de los backbones. Sin el rápido desarrollo de CIDR en 1994, las tablas de ruteo de Internet hubieran tenido un exceso de 70,000 rutas e Internet, muy probablemente, ya no hubiera estado funcionando actualmente.

### 6.1. Características de funcionamiento:

CIDR elimina el tradicional concepto de Clase A, Clase B y Clase C, y los reemplaza con el concepto de prefijo de red (network prefix).
Los routers utilizan el prefijo de red, en lugar de los 3 bits iniciales de las direcciones IP para determinar el punto de división entre el número de red y el número de host. Como resultado, CIDR soporta el uso de redes de tamaño arbitrario en lugar que los números de red de 8, 16 ó 24 bits asociados a las redes de tipo “classful”.
En el modelo CIDR, cada parte de la información de ruteo es anunciada con un bit de máscara (o longitud de prefijo). La longitud de prefijo es una manera de especificar el número de bits contiguos desde la izquierda hasta el punto de división de los valores de red y de host. Así se tiene que una red con un valor de número de red igual a 20 y 12 bits para el número de host puede ser identificada como (/20).
La parte inteligente de este enfoque es que una dirección IP identificada con un prefijo /20 puede ser una red Clase A, Clase B o Clase C. Los routers que usan CIDR no realizan presunciones basados en los 3 bits de la dirección, ellos confían en la información dada por el prefijo de longitud de red proporcionada con la ruta.
En un entorno “classless”, los prefijos son vistos como blocks contiguos de bits del espacio de direccionamiento IP. Por ejemplo, todas las redes con un prefijo /20 representan la misma cantidad de direcciones de hosts (2¨12 ó 4,096 direcciones). Mas aún, un prefijo /20 puede ser asignado a una red tradicional Clase A, Clase B o Clase C.

Así, se tiene lo siguiente:

| | | | |
|---|---|---|---|
| Clase A | 11.24.64.0 | /20 | 00001011.00011000.01000000.00000000 |
| Clase B | 130.5.0.0 | /20 | 10000011.00000101.00000000.00000000 |
| Clase C | 203.14.128.0 | /20 | 11001011.00001110.10000000.00000000 |

En la siguiente tabla, se proporciona información acerca de los bloques de direcciones CIDR comúnmente utilizados.
Si se presta atención al bloque /15, se puede ver que, utilizando la notación tradicional, el valor que se obtendría sería 255.254.0.0.
También, un bloque de direcciones CIDR /15 puede ser interpretado como 2 direcciones Clase B o 512 redes Clase C.

| Longitud de prefijos CIDR | Notación Decimal | # Direcciones individuales | # de Redes de tipo Classful |
|---|---|---|---|
| /13 | 255.248.0.0 | 512K | 8 Bs o 2048 Cs |
| /14 | 255.252.0.0 | 256K | 4 Bs o 1024 Cs |
| /15 | 255.254.0.0 | 128K | 2 Bs o 512 Cs |
| /16 | 255.255.0.0 | 64K | 1 B o 256 Cs |
| /17 | 255.255.128.0 | 32K | 128 Cs |
| /18 | 255.255.192.0 | 16K | 64 Cs |
| /19 | 255.255.224.0 | 8K | 32 Cs |
| /20 | 255.255.240.0 | 4K | 16 Cs |
| /21 | 255.255.248.0 | 2K | 8 Cs |
| /22 | 255.255.255.0 | 1K | 4 Cs |
| /23 | 255.255.254.0 | 512 | 2 Cs |
| /24 | 255.255.255.0 | 256 | 1 C |
| /25 | 255.255.255.128 | 128 | ½ C |
| /26 | 255.255.255.192 | 64 | ¼ C |
| /27 | 255.255.255.224 | 32 | 1/8C |

**Bloques de Direcciones CIDR**

## 6.2. CIDR: Implicaciones al asignarlo a Hosts

Es bueno saber que existen algunos cuidados a tomar en cuenta cuando se asignan direcciones CIDR a host de una red de tipo “classful”. En este caso, las interfaces de usuario de estos hosts no permitirán asignar una máscara más corta que la natural a una dirección tradicional de tipo classful.
Por ejemplo, se presentarán problemas si se desea asignar la siguiente dirección 200.25.16.0 con un prefijo /20 para definir una red capaz de soportar 4,094 hosts. El software que se ejecuta en el host no permitirá asignar una dirección tradicional Clase C (200.25.16.0) con una máscara /20 (255.255.240.0), dado que la máscara tradicional para ese tipo de dirección es de 24 bits.
Si el software del host soporta CIDR, este permitirá definir máscaras más cortas. Sin embargo, no habrán problemas a nivel de los hosts si es que se implementa la dirección 200.25.16.0/20 (Clase C) como un bloque de 16 redes /24, dado que los host no-CIDR interpretarán estas direcciones /24 como del tipo Clase C.
De la misma manera, es posible escribir una dirección 130.14.0.0/16 (una dirección Clase B), como un bloque de 255 redes /24, dado que el host interpretará el prefijo /24 como subnets /16.
Todos estos artilugios se podrían evitar si es que el software del host pudiera permitir máscaras más cortas que lo normal.

## 6.3. Ventajas del CIDR

Lo que se analizará a continuación son las ventajas derivadas del uso del direccionamiento CIDR frente a las direcciones basadas en clases.
En un entorno classfull, un CPI (Centro Proveedor de Información) puede, únicamente, asignar direcciones de tipo /8, /16, o /24.
En un entorno CIDR, el CPI puede escoger, libremente, un bloque de su espacio registrado de direcciones y que, además, estas satisfagan exactamente las necesidades de cada cliente. Esto permite gestionar de manera más eficiente el espacio de direcciones registradas y no desperdicia inútilmente estos recursos.
Para entender esto mejor se usará el siguiente ejemplo.
Supóngase que un CPI tiene asignado el bloque de direcciones 206.0.64.0/18. Este bloque representa 16,384 direcciones IP, las cuales pueden ser interpretadas como 64 redes de clase /24. Si un cliente requiere 800 direcciones de host, en lugar de asignar una dirección Clase B (y desperdiciar aproximadamente 64,700 direcciones) o 4 redes individuales Clase C (e introducir 4 nuevas rutas en las tablas globales de ruteo), el CPI podria asignar al cliente el bloque de direcciones 206.0.68.0/22, un bloque de 1,024 direcciones IP ( 4 contiguas redes /24).

Bloque del CPI: 11001110.00000000.01000000.00000000 206.0.64.0/18
Bloque del cliente: 11001110.00000000.01000100.00000000 206.0.68.0/22
Clase C #1 : 11001110.00000000.01000100.00000000 206.0.68.0/24
Clase C #2 : 11001110.00000000.01000101.00000000 206.0.69.0/24
Clase C #3 : 11001110.00000000.01000110.00000000 206.0.70.0/24
Clase C #4 : 11001110.00000000.01000111.00000000 206.0.71.0/24

### Ejercicio1: Asignación de direcciones CIDR

En este caso, se asumirá que un CPI posee el bloque de direcciones 200.25.0.0/16. Este bloque representa 65,536 direcciones IP (o 256 redes de tipo /24). De todo este bloque 200.25.0.0/16, solo se quiere asignar el bloque de direcciones 200.25.16.0/20. Este bloque más pequeño solo representa 4,096 direcciones IP (o 16 redes de tipo /24).
SE procede a realizar la asignación:

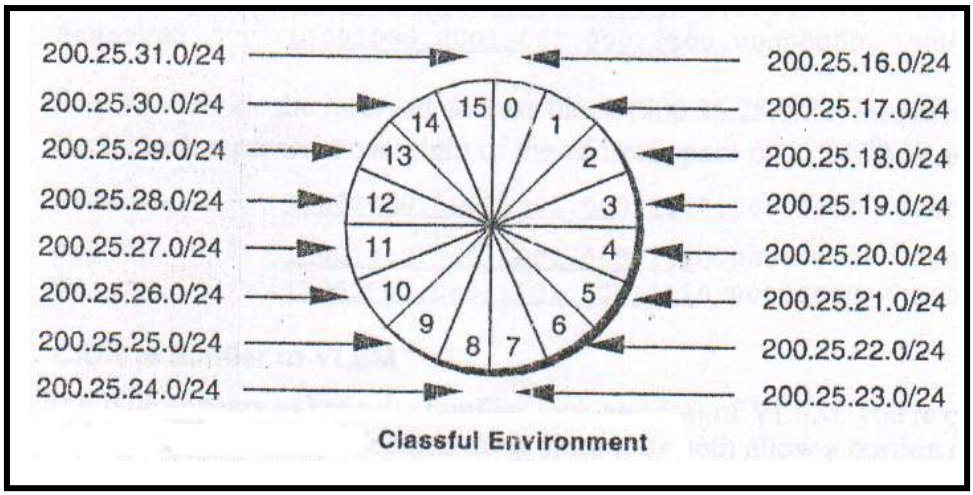
Dado el bloque de direcciones:

11001000.00011001.00010000.00000000 200.25.16.0/20

En un entorno de direccionamiento basado en clases (classful), el CPI es forzado a usar el bloque de direcciones /20 como 16 redes del tipo /24.

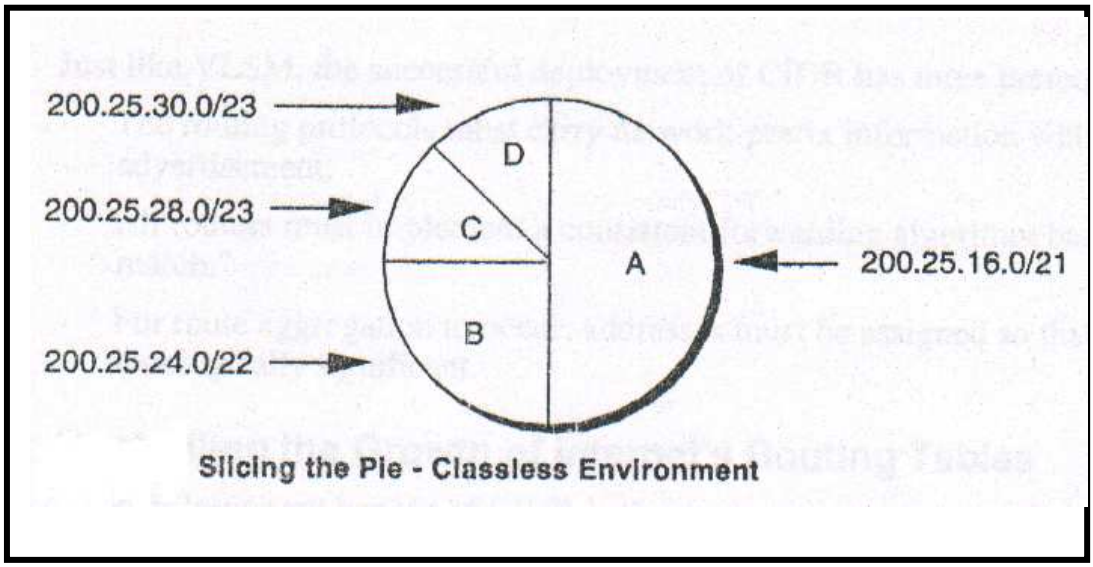
Red #1: 110010000.00011001.00010000.00000000 200.25.16.0/24
Red #2: 110010000.00011001.00010001.00000000 200.25.17.0/24
Red #3: 110010000.00011001.00010010.00000000 200.25.18.0/24
Red #4: 110010000.00011001.00010011.00000000 200.25.19.0/24
Red #5: 110010000.00011001.00010100.00000000 200.25.20.0/24
:
:
Red #14: 110010000.00011001.00011101.00000000 200.25.29.0/24
Red #15: 110010000.00011001.00011110.00000000 200.25.30.0/24
Red #16: 110010000.00011001.00011111.00000000 200.25.31.0/24

Si se visualiza el bloque de direcciones /20 del CPI como si se tratara de un pastel, se vería que en un entorno “classful” este bloque de direcciones solo puede ser cortado en 16 partes del mismo tamaño.



Classful Environment

Esto es en un entorno “classfull”; sin embargo, en un entorno CIDR, el CPI es libre de “cortar” el pastel en las partes que quiera. Esto significa que si se quisiera se podría asignar el bloque de direcciones en 2 bloques, y luego, dividir el segundo bloque en dos sub-bloques y así sucesivamente. Así, por ejemplo, se podría tener una asignación de direcciones representada como en el gráfico.



Slicing the Pie - Classless Environment

**Paso #1 :**
Dividir el bloque de direcciones 200.25.16.0/20 en dos partes iguales . Cada bloque representa una mitad del espacio de direccionamiento total o 2,048 direcciones IP.

Bloque del CPI : 11001000.00011001.00010000.00000000 200.25.16.0/20
Organización A : 11001000.00011001.00010000.00000000 200.25.16.0/21
Reservada : 11001000.00011001.00011000.00000000 200.25.24.0/21

**Paso #2 :**
Dividir el bloque reservado (200.25.24.0/21) en dos partes iguales . Cada bloque representa un cuarto del espacio de direccionamiento total o 1,024 direcciones IP.

Reservado : 11001000.00011001.00011000.00000000 200.25.24.0/21
Org. B : 11001000.00011001.00011000.00000000 200.25.24.0/22
Reservado : 11001000.00011001.00011100.00000000 200.25.28.0/22

**Paso #3 :**
Dividir el bloque de direcciones reservado (200.25.28.0/22) en dos partes iguales del mismo tamaño. Cada bloque representa un octavo del espacio de direcciones, es decir, 512 direcciones IP.

Reservado : 11001000.00011001.00011100.00000000 200.25.28.0/22
Org. C : 11001000.00011001.00011100.00000000 200.25.28.0/23
Org. D : 11001000.00011001.00011110.00000000 200.25.30.0/23

CIDR, como la creación de subredes de tamaño variable, requiere que los protocolos de enrutamiento publiquen las máscaras de subred junto con el ID de red. RIP versión 2, OSPF y BGPv4 admiten los entornos CIDR. RIP versión 1 no se puede utilizar en entornos con CIDR. InterNIC asigna las direcciones públicas dentro del espacio público de direcciones que consisten en todas las posibles direcciones “unicast” en la Internet mundial. Históricamente, InterNIC asignaba los ID de red con clase a las organizaciones conectadas a Internet sin tomar en consideración su ubicación geográfica. Hoy en día, lo que InterNIC hace es asignar bloques CIDR a los CPI según su ubicación geográfica. Luego, los CPI subdividen los bloques CIDR asignados entre sus clientes.

# Autoevaluación

1. Liste las direcciones de red individuales Clase C que pueden ser obtenidas a partir del bloque CIDR 200.56.168.0/21.

2. Liste las direcciones de red individuales Clase C que pueden ser obtenidas a partir del bloque CIDR 195.24.0.0/13

3. A partir de las siguientes direcciones de red Clase C. obtenga la dirección CIDR de máximo valor de longitud de prefijo de red extendida que las pueda contener.

212.56.132.0/24
212.56.133.0/24
212.56.134.0/24
212.56.135.0/24

4. A partir de las siguientes direcciones de red Clase C, obtenga la dirección CIDR de máximo valor de longitud de prefijo de red extendida que las pueda contener.

212.56.146.0/24
212.56.147.0/24
212.56.148.0/24
212.56.149.0/24

5. Un CPI presenta un bloque de direcciones CIDR: 210.0.60.0/18.
Cuatro (4) clientes le solicitan direcciones IP de la siguiente manera:

A → 500
B → 250
C → 125
D → 125

a. Calcule el bloque CIDR que se le asignará a cada uno de los clientes.
b. Las direcciones en formato CLASSSFULL Clase C que se asignarán a los dos primeros clientes.

6. Un CPI tiene el siguiente bloque de direcciones CIDR 225.60.0.0/16.
Una empresa que desea disponer de 4000 direcciones IP le solicita un rango de direcciones IP al CPI.
La empresa, a su vez, desea que las 4,000 direcciones se distribuyan en 4 grupos de direcciones CIDR.

Grupo A: 2000 direcciones
Grupo B: 1000 direcciones
Grupo C y D: 500 direcciones

¿Qué bloque de direcciones CIDR separará el CPI para asignárselas a la empresa?.
Obtenga cada una de las 4 direcciones CIDR que separará el CPI para cada grupo de direcciones (A, B, C y D).
¿Cada dirección CIDR obtenida a cuántas direcciones Clase C equivale?

# Para recordar

- CIDR elimina el concepto tradicional de redes de dirección Clase A, Clase B y Clase C. Esto permite la asignación eficiente del espacio de direccionamiento de IPV4.

- CIDR permite que un solo registro de la tabla de ruteo pueda representar el espacio de direccionamiento de miles de redes tradicional del tipo clasfull. Esto permite a un solo registro de la tabla de ruteo especificar cómo rutear el tráfico a muchas direcciones de red, lo que redice la información de ruteo en los routers de los backbones.

- En un entorno CIDR, el CPI puede escoger, libremente, un bloque de su espacio registrado de direcciones y que, además, estas satisfagan exactamente las necesidades de cada cliente. Esto permite gestionar de manera más eficiente el espacio de direcciones registradas y no desperdicia inútilmente estos recursos.

SEMANA

8

# Protocolo ARP

**TEMA**

Protocolo ARP

**OBJETIVOS ESPECÍFICOS**

- Conocer el funcionamiento del protocolo ARP

**CONTENIDOS**

- Protocolo ARP
- Asociación de direcciones
- Definición mediante enlace dinámico
- Mecanismo de funcionamiento
- Evitar la duplicación de direcciones IP
- Encapsulación e identificación de ARP
- Formato del protocolo ARP

**ACTIVIDADES**

- Reconocen el funcionamiento del protocolo ARP

# 8. PROTOCOLO ARP

Hasta ahora, se ha utilizado el esquema de direccionamiento lógico de TCP/IP y se ha visto que es posible con una dirección lógica de 32 bits identificar de manera inequívoca un host en una interred. También, se ha visto que las tecnologías de red física utilizan direcciones hardware o direcciones físicas de red. Lo que se verá a continuación es la manera en que un host o un ruteador transforma una dirección IP en una dirección física correcta.

## 8.1. Asociación de Direcciones

Si se considera dos máquinas, A y B, que comparten una red física, cada una de ellas tiene asignada una dirección IP, Ipa e Ipb. Así mismo, cada una de ellas tiene una dirección física, Hwa y HWb. Al desarrollar el modelo de interconexión de interredes utilizando la capa de red como base, se propuso diseñar un software de bajo nivel que oculte las direcciones físicas y permita qué programas de un nivel más alto trabajen sólo con direcciones IP.

Sin embargo, la comunicación debe llevarse a cabo por medio de redes físicas, utilizando cualquier esquema de direcciones físicas proporcionadas por el hardware.

El problema que se plantea es cómo hace un host para enviar un paquete de datos a otro host a través de la red física, utilizando solamente direcciones IP, es decir, cómo transforma la máquina A la dirección lógica en dirección física.

Esta transformación de direcciones se realiza en cada fase a lo largo del camino, desde la fuente original hasta el destino final.

En particular surgen dos casos:

1. En la última fase de la entrega de un paquete, éste se debe enviar a través de una red física hacia su destino final. La computadora que envía el paquete tiene que transformar la dirección IP del destino final en su dirección hardware.
2. En cualquier punto del camino, de la fuente al destino, que no sea la fase final, el paquete se debe enviar hacia un router intermedio. Por lo tanto, el equipo transmisor tiene que transformar la dirección IP del router en una dirección física.

Este problema de transformar direcciones de alto nivel en direcciones físicas se conoce como problema de asociación de direcciones y, en este caso, se estudiará una manera de resolverlo a través del protocolo ARP.

## 8.2. Definición mediante enlace dinámico

Se sabe que la tecnología Ethernet utiliza una interfaz que tiene asignada una dirección física de 48 bits asignada por el fabricante. Por lo tanto, cuando una tarjeta falla y se necesita reemplazar, la dirección física de la máquina cambia. También, debido a que una dirección Ethernet es de 48 bits, no hay posibilidad de codificarla en una dirección IP de 32 bits.

La manera en que se soluciona este problema es utilizando un protocolo de bajo nivel para asignar las direcciones en forma dinámica.

Este protocolo es conocido como ARP (*Protocolo de Asociación de Direcciones),* es razonablemente eficaz y fácil de mantener.

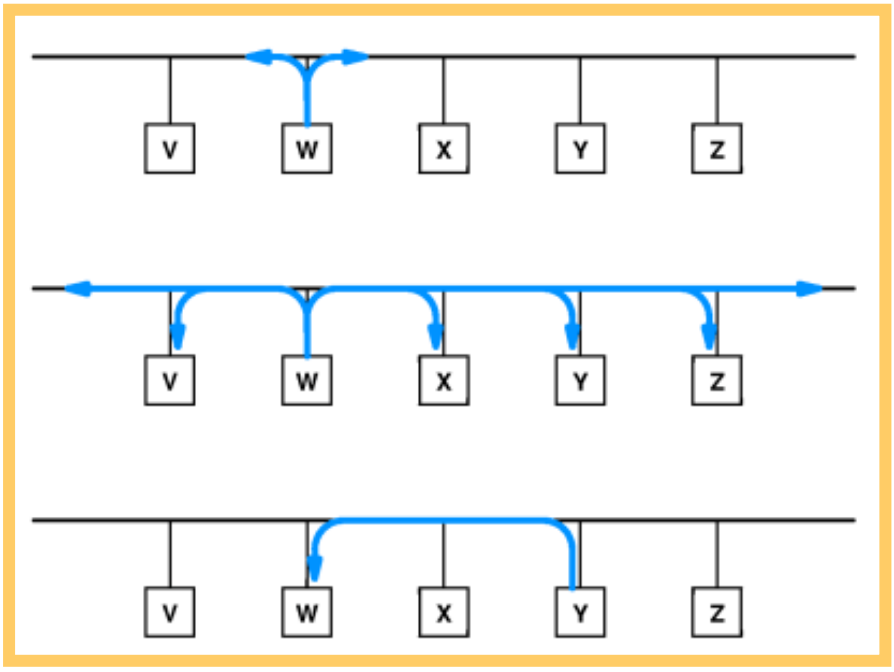
### 8.3. ARP: Mecanismo de funcionamiento

ARP es un protocolo de bajo nivel que oculta el direccionamiento físico subyacente de red, al permitir que se asigne una dirección IP arbitraria a cada máquina. Por lo tanto, ARP es más parte del sistema físico de red, y no tanto como parte de los protocolos de internet.

De manera funcional, ARP está dividido en dos partes:

La primera parte transforma una dirección IP en una dirección física cuando se envía un paquete.

La segunda parte responde solicitudes de otras máquinas.



1. El protocolo ARP del host 1400.1.1.3 envía un marco de solicitud ARP difundiéndolo a la red local. En Ethernet, los mensajes se envían a la dirección FF:FF:FF:FF. El marco de solicitud ARP incluye las direcciones IP y HW del emisor y la dirección IP del destino.
2. Todos los hosts de la red reciben el marco de solicitud ARP y comparan la dirección IP de destino con la suya.
3. Si un host determina que las direcciones coinciden, crea un marco de respuesta ARP que contiene su dirección HW y lo devuelve al host que ha emitido la solicitud.
4. Cuando el protocolo ARP de 140.1.1.3 recibe el marco de respuesta ARP, pasa la información a IP.

Si cada host tuviera que difundir un marco de solicitud ARP cada vez que fuera necesario enviar un datagrama, el tráfico colapsaría la red. Por lo tanto, ARP mantiene una *tabla caché* con las direcciones recibidas recientemente para reducir el número de solicitudes de direcciones. La tabla caché se consulta antes de difundir solicitudes ARP.

### 8.4. Evitar la duplicación de direcciones IP

Muchos clientes que utilizan TCP/IP utilizan ARP, para evitar que se dupliquen las direcciones IP en la red. Cuando un host entra por primera vez en la red, difunde un marco de solicitud ARP con su propia dirección ARP para anunciar su presencia. Si otro host responde al marco de solicitud ARP, el nuevo host sabe que su dirección IP ya está siendo utilizada y se impide su entrada a la red. El nuevo host, y el que ya está establecido, reciben mensajes de error que informan acerca del conflicto de direcciones.

### 8.5. Paquetes ARP que llegan a un terminal

Cuando llega un paquete ARP por medio de la red, el software extrae la dirección IP del transmisor y la dirección del hardware; luego, examina la memoria temporal local para verificar si ya existe un registro para el transmisor. SI es así, el controlador actualiza el registro al sobre escribir la dirección física con la dirección obtenida del paquete. Después, el receptor procesa el resto del paquete ARP.

El receptor debe manejar dos tipos de paquetes ARP entrantes:

Si llega una solicitud ARP, la máquina receptora debe verificar si es el objetivo de la solicitud (si alguna otra máquina transmitió por difusión una solicitud de la dirección física del receptor). Si es así, el software ARP formula una respuesta al proporcionar su dirección física de hardware y la envía directamente al solicitante. El receptor, también, agrega el par de direcciones del transmisor a su memoria temporal si éstas no están presentes. Si la dirección IP mencionada en la solicitud ARP no corresponde a la dirección IP local, el paquete solicitará la transformación de alguna otra máquina en la red, aunque podría ser ignorado

El otro caso sucede cuando llega una respuesta ARP. Dependiendo de la implantación, el controlador quizá necesite crear un registro en su memoria temporal o el registro se puede crear cuando se genere la solicitud. En cualquiera de estos casos, una vez que se actualiza la memoria temporal, el

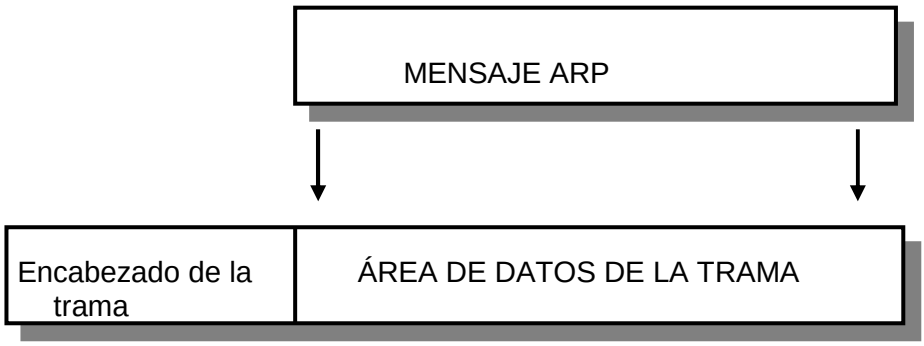
receptor intenta encontrar una correspondencia entre la respuesta y una solicitud expedida con anterioridad.

Por lo general, las respuestas llegan obedeciendo a una solicitud que se generó, porque la máquina tiene que entregar un paquete.

Entre el tiempo en que una máquina transmite por difusión su solicitud ARP y recibe la respuesta, los programas de aplicación o los protocolos de un nivel más alto pueden generar solicitudes adicionales para la misma dirección; el software debe recordar que ya envió una solicitud para no enviar más.

## 8.6. Encapsulación e identificación de ARP

Cuando los mensajes ARP viajan de una máquina a otra, se deben transportar en tramas físicas.




Mensaje ARP encapsulado en una trama de red física

Para identificar que la trama transporta un mensaje ARP, el transmisor asigna un valor especial al campo de tipo en el encabezado de la trama y coloca el mensaje ARP en el campo de datos de la misma.

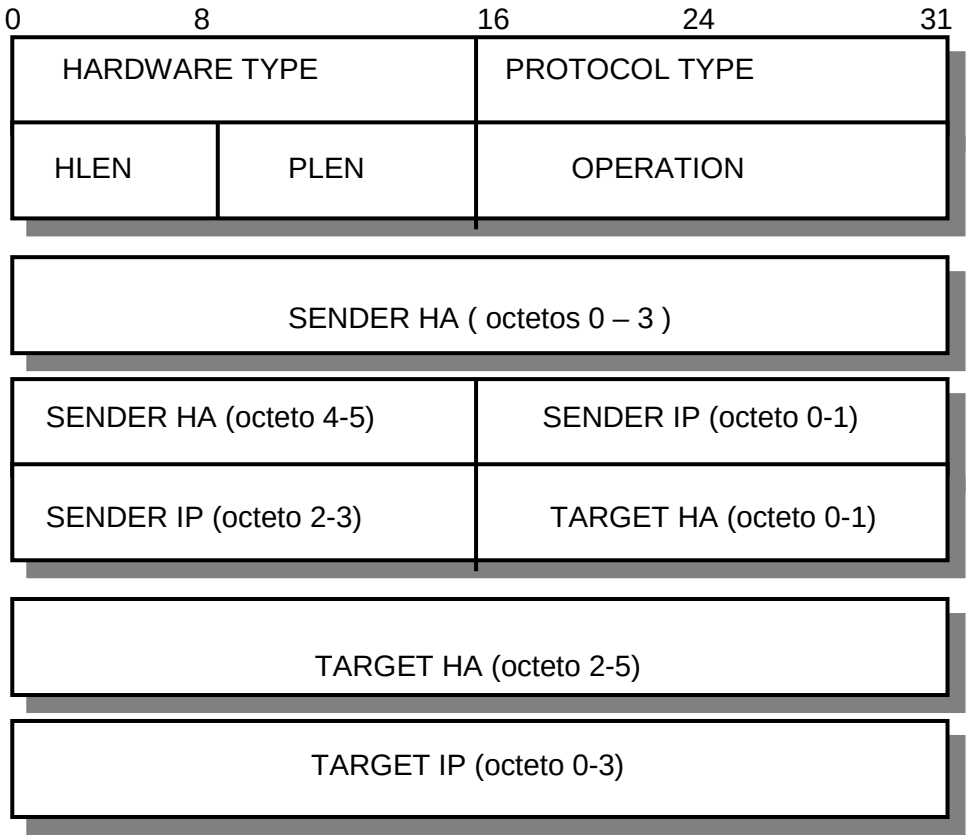
Cuando llega una trama a una computadora, el software de red utiliza el campo de tipo de trama para determinar su contenido. En el caso de las tramas Ethernet, las tramas que transportan mensajes ARP tienen un campo de tipo de 0806hex. Este es un valor estándar asignado para Ethernet. Otras tecnologías de hardware de red utilizan otros valores.

## 8.7. Formato del protocolo ARP

A diferencia de la mayor parte de los protocolos, los datos en los paquetes ARP no tienen un encabezado con formato fijo. Para hacer que ARP sea útil para varias tecnologías de red, la longitud de los campos que contienen direcciones depende del tipo de red. Sin embargo, para hacer posible la interpretación de un mensaje ARP arbitrario, el encabezado incluye campos fijos cerca del comienzo, que especifican la longitud de las direcciones que se encuentran en los campos siguientes.

Se discutirá el formato de 28 bytes de un mensaje ARP que se utiliza en el hardware Ethernet (donde las direcciones físicas tienen una longitud de 48 bits o 6 bytes) y que se asocia con direcciones IP (longitud de 32 bits o 4 bytes).

En el diagrama, se puede ver un mensaje ARP con 32 bits por línea, formato estándar; sin embargo, a diferencia de la mayor parte de los otros protocolos, los campos de longitud variable en los paquetes ARP no se alínean firmemente en fronteras de 32 bits, lo cual causa que el diagrama sea difícil de leer. Por ejemplo, la dirección de hardware del transmisor, etiquetada como SENDER HA, ocupa 6 bytes contiguos, por lo que abarca dos líneas en el diagrama.



Formato de mensaje ARP/RARP utilizado para la transformación de una dirección IP en una dirección Ethernet

| CAMPO | FUNCIÓN |
|---|---|
| | Tipo de interfaz de hardware |
| HARDWARE TYPE | Ethernet : 1 |
| PROTOCOL TYPE | Tipo de dirección de protocolo de alto r |
| | IP : 0800 hex |
| OPERATION | 1 : Solicitud ARP |
| | 2 : Respuesta ARP |
| | 3 : Solicitud RARP |
| | 4 : Respuesta RARP |
| HLEN | Longitud de la dirección hardware |
| PLEN | Longitud de la dirección del protocol alto nivel |
| SENDER HA | Dirección hardware del transmisor |
| SENDER IP | Dirección lógica del transmisor |
| TARGET HA | Dirección hardware del receptor |
| TARGET IP | Dirección IP del receptor |

Por lo tanto, para enviar un paquete de inter-red a través de una re física desde una máquina hacia otra, el software de red debe transformar la dirección IP en una dirección física de hardware y utilizar esta última para transmitir las tramas.

ARP permite que las máquinas asocien direcciones sin tener un registro permanente de asignaciones. Además, una máquina utiliza ARP para encontrar la dirección de hardware de otra máquina al transmitir por difusión una solicitud ARP.

La solicitud contiene la dirección IP de la máquina de la que se necesita la dirección de hardware. Todas las máquinas en una red reciben la solicitud ARP. Si la solicitud corresponde a la dirección IP de una máquina, ésta responde al enviar una respuesta que contiene la dirección de hardware requerida.

Las respuestas se dirigen a una sola máquina; no se transmiten por difusión. Para lograr que ARP sea eficiente, cada máquina guarda en su memoria temporal las asignaciones de dirección IP a dirección física.

## 8.7 ARP-SPOOFING

Cuando se dio la posibilidad de segmentar las redes mediante el uso de switches, dio la apariencia que los problemas de sniffer habían terminado. Sin embargo, es posible aprovechar una inseguridad en el protocolo ARP para espiar en la red. Para ello se aclararán algunos conceptos básicos.

El protocolo ethernet fue concebido en torno a una idea principal: todas las máquinas de una misma red local comparten el mismo medio (el cable). Todas las máquinas son capaces de "ver" todo el tráfico de la red. Debido a esto, las tarjetas ethernet incorporan un filtro que ignora todo el tráfico que no está destinado a él. Esto se consigue ignorando aquellos paquetes cuya dirección MAC (Media Access Control) no coincide con la suya. Un sniffer elimina este filtro de la tarjeta de red y la coloca en modo promiscuo. De esta forma la tarjeta es capaz de "ver" todo el tráfico que pasa por la red. Solo es cuestión de colocar los filtros adecuados y comenzar a capturar los paquetes que más interesen (login/passwd de conexiones de telnet, POP3, etc).
El empleo de switches soluciona este problema. Mediante la segmentación de la red, el único tráfico que se podrá ver será el nuestro, ya que el Switch se encarga de enrutar hacia este segmento solo aquellos paquetes destinado a la dirección MAC.

Todas las computadoras de una misma red comparten el mismo medio, por lo que debe de existir un identificador único para cada equipo, o mejor dicho para cada tarjeta de red. Esto no sucede en una conexión telefónica mediante modem, ya que se supone que cualquier dato que se envía está destinado al equipo que se encuentra al otro lado de la línea. Pero cuando se envían datos en una red local, hay que especificar claramente a quién van dirigidos. Esto se consigue mediante la dirección MAC, un número compuesto por 12 dígitos hexadecimales que identifica de forma única a cada dispositivo ethernet. La dirección MAC se compone de 48 bits. Los 24 primeros bits identifican al fabricante del hardware y los 24 bits restantes corresponden al número de serie asignado por el fabricante, lo que garantiza que dos tarjetas no puedan tener la misma dirección MAC. Direcciones MAC duplicadas causarían problemas en la red.
Ahora que ha quedado claro que, para comunicarse en una red ethernet con otro equipo de la misma, es necesario conocer su dirección MAC, la cual es única, se verá cómo se puede conocer las direcciones MAC de los equipos de la red.
Asúmase que se trabaja con una computadora que utiliza Linux, por lo que la configuración de la tarjeta del equipo se obtendrá con el comando ifconfig -a. La salida de este comando se asemejará al siguiente:

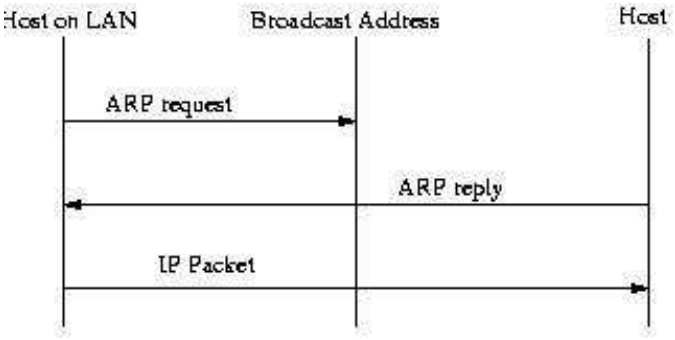
```
eth0 Link encap:Ethernet HWaddr 00:C0:4F:68:BA:50
inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:31658 errors:0 dropped:0 overruns:0 frame:0
TX packets:20940 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
Interrupt:19 Base address:0xdc00
```

Donde la dirección MAC es 00:C0:4F:68:BA:50.
Si se quiere conocer las direcciones de otros equipos de la red, se hará uso de la cache arp del equipo, mediante el comando arp -a. Este comando mostrará la relación IP/MAC de los equipos que la cache tiene almacenados en ese momento (Si se quiere obtener la dirección ethernet de una máquina, primero se le hará un ping. De esta forma se almacenará la dirección MAC en la cache y mediante arp -a se podrá obtener su dirección MAC). Cada vez que se comunique con un equipo de la red, se debe de conocer su dirección MAC. Para ello, se enviará un arp-request a la dirección de Broadcast, que solicite la MAC de la ip del equipo con el que se quiere contactar. Este responderá con un arp-reply informando de su MAC. Esta quedará almacenada el la cache arp, durante algunos minutos, para futuras comunicaciones. De esta forma no se tendrá que volver a solicitar la dirección MAC. Aquí es donde comienza el problema.

### 8.7.1 Funcionamiento de ARP

Se sabe que el protocolo arp (address resolution protocol) es el encargado de "traducir" las direcciones ip de 32 bits a las correspondientes direcciones de hardware. En ethernet &

Token ring, estas direcciones suelen tener 48 bits. La traducción inversa la hace el protocolo RARP o Reverse ARP.
Cuando un ordenador necesita resolver una dirección IP a una MAC, lo que hace es efectuar una petición arp (Arp request) a la broadcast de dicho segmento de red, FF:FF:FF:FF:FF:FF, solicitando que el equipo con dicha IP responda con su dirección ethernet (MAC).

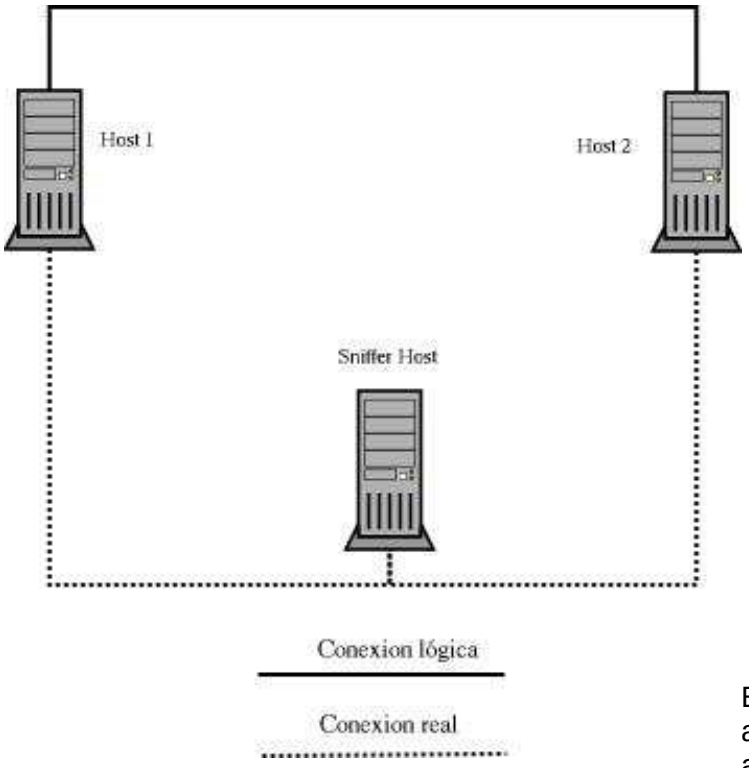



Esquemáticamente el proceso es el siguiente:

Con el fin de reducir el tráfico en la red, cada arp-reply que llega a la tarjeta de red es almacenado en la cache, incluso si la petición no la realizamos nosotros. Es decir, todo arp-reply que llega es almacenado en la cache. Este factor es el que utilizaremos para realizar arp-spoofing.

### 8.7.2 Arp-Spoofing

Este método no pone la interfaz de red en modo promiscuo. Esto no es necesario porque los paquetes serán dirigidos hacia el host que realizará el sniffer y el switch enrutará los paquetes hacia ese host  A continuación se verá como esto es posible.
El método consiste en “envenenar” la cache arp de las dos máquinas que se quiere sniffear. Una vez que las caches estén envenenadas, los dos hosts comenzarán la comunicación, pero los paquetes serán enviados hacia el host que sniffeará la comunicación y luego lo enrutará de nuevo al host apropiado. De esta forma, la comunicación es transparente para los dos hosts. La única forma de descubrir que existe “a man in the middle” en la conexión, sería ver la cache arp de la máquina origen y comprobar si existen dos máquinas con la misma dirección MAC. El esquema de la comunicación es sencillo:
Desde la máquina que intercepta la comunicación se enviará paquetes de tipo arp-reply falsos a las dos host que se quieren sniffear. En estos reply’s se le debe  decir al host 1 que la dirección ethernet del segundo host es la del host interceptor, quedando esta información almacenada en su cache arp. Este equipo enviará ahora los paquetes al host 2 pero con la dirección MAC del interceptor. Los paquetes ya están en el host interceptor. El switch se encargará de hacernos llegar los datos.
Imagínese la siguiente situación:




Enviamos un flujo constante de arp-reply (para evitar que la cache arp de las máquinas se refresque con la información verdadera al host 1 y host 2 con los siguientes datos:

HOST 1 : arp-reply informando que 192.168.0.2 tiene dirección MAC 03:03:03:03:03:03
HOST 2 : arp-reply informando que 192.168.0.1 tiene dirección MAC 03:03:03:03:03:03

De esta forma, estamos “envenenando” las cache arp. A partir de ahora lo paquetes que se envíen entre ambas nos llegarán a nosotros, pero para que ambos hosts no noten nada extraño, deberemos de hacer llegar los paquetes a su destino final. Para ello, deberemos de tratar los paquetes que recibamos en función del host de origen:

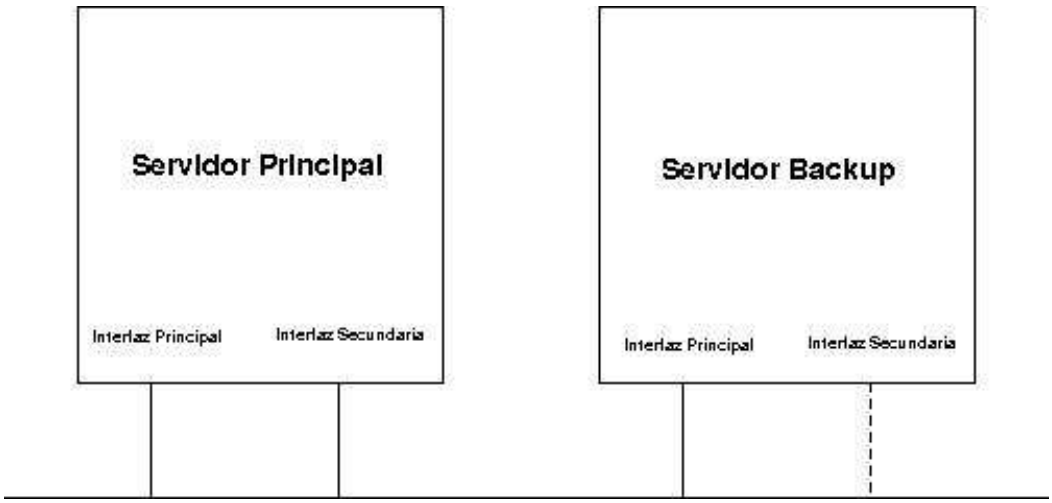
Paquetes procedentes de HOST 1 ----------> reenviar a 02:02:02:02:02:02
Paquetes procedentes de HOST 2 ----------> reenviar a 01:01:01:01:01:01

De esta forma, la comunicación entre ambos no se ve interrumpida y podemos “ver” todo el tráfico entre ellos. Solo tendremos que utilizar un sniffer para poder capturar y filtrar el tráfico entre ambos, ya sea login/passwd de telnet, ftp, POP3 o incluso la sesión completa. Eso ya depende de la habilidad y el interés de cada cual.
Como se puede comprobar, el proceso no es complicado, pero ¿qué utilidades tenemos disponibles para poder enviar los paquetes arp falsificados?
Existen varios programas para intentar el arp-spoofing: Arptool, Arp-Fun, ettercap. Este último está muy completo, ya que permite varios tipos de sniffeo: Por IP, MAC y Arp-Spoofing. Pudiendo ejecutarse bien en modo comando, o mediante un entorno de ventanas, en este entorno se nos mostrará, al inicio, un listado de los hosts encontrados en la LAN. Para realizar esta búsqueda, el programa envía un ARP-REQUEST de las IP teniendo en cuenta la IP del host donde se está ejecutando y la máscara de red. Obteniendo a continuación los ARP-REPLYs, podremos componer la lista de los hosts presentes en la red. Hay que tener mucho cuidado con la máscara de red que usemos, porque si es de clase B (255.255.0.0) el programa realizará 255*255=65025 ARP-REQUEST, lo cual le llevará su tiempo ya que el retardo entre cada petición es de 1 milisegundo.

Hasta aquí hemos visto la forma en la que se pueden utilizar las vulnerabilidades del protocolo ARP para poder espiar en nuestra red. Pero las posibilidades son múltiples: ataques DoS (Denegación de servicio); si "envenenamos" la cache arp de una máquina haciéndonos pasar por el gateway de la red, toda comunicación con el exterior pasará por nosotros. Si desechamos los paquetes procedentes de este host y no los reenviamos al gateway, el host no podrá comunicarse con el exterior. Algunos switches pueden ser manipulados mediante paquetes ARP para que en vez de actuar en modo "bridging" lo hagan en modo "repetición". Es decir que, en vez de enviar los paquetes por la "boca o puerto" adecuado del switch, los enviará por todos, a todas las máquinas les llegarán todo los paquetes de la red. Esto se consigue inundando la tabla de direcciones con gran cantidad de direcciones MAC falsas. El switch al recibir un paquete cuya dirección MAC de destino no tenga en su cache, lo enviará a todos los equipos, y esperará la respuesta del equipo para poder almacenar su MAC en la cache. Pero como estamos "bombardeándola" con direcciones MAC falsas, esto no ocurrirá.

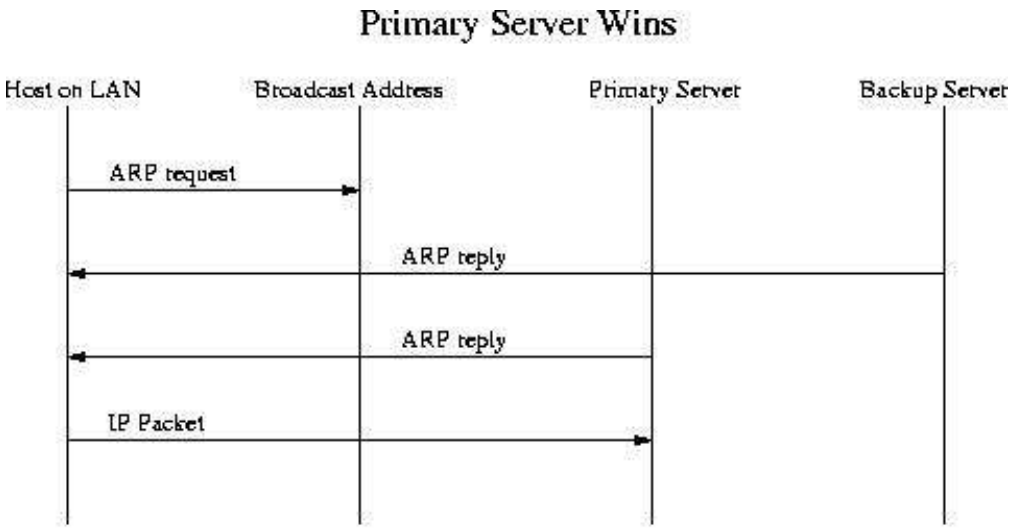
### 8.7.3 ARP-SPOOFING y servidores redundantes

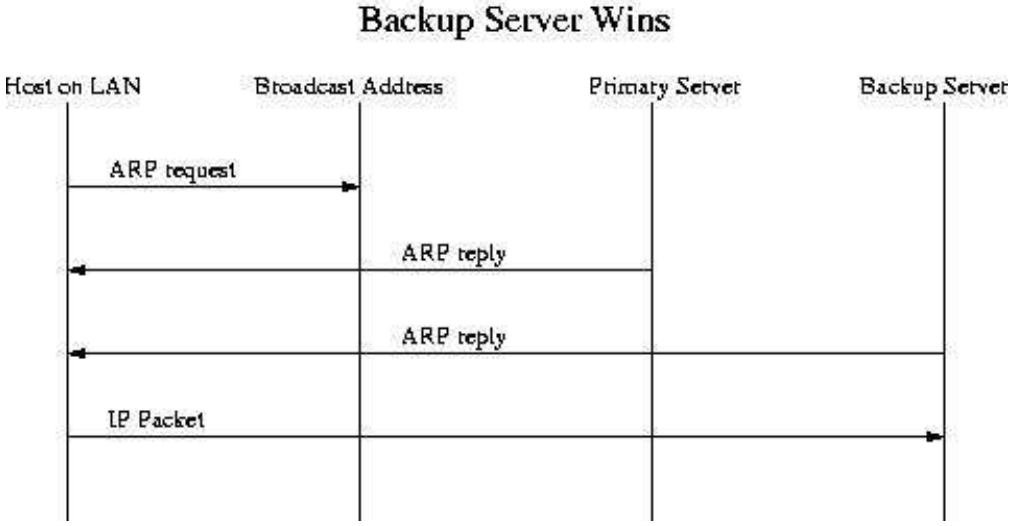
El ARP-SPOOFING no solo sirve como herramienta para espiar en una red o realizar ataques DoS. También, se puede utilizar para crear servidores redundantes, servidores con tolerancia fallos. La idea consiste en crear un servidor auxiliar que tome la identidad del servidor que ha dejado de funcionar. Para ello, se hará uso de IP alias y de ARP-SPOOFING. Es una solución rápida y no muy formal, pero puede ser útil.
En muchas ocasiones, es vital la redundancia en un determinado servicio: HTTP, FTP, SMTP, POP3. Los equipos que permiten la redundancia en un servicio suelen ser bastante caros, por lo que este método puede solucionar el problema. La situación es la siguiente:




Se tiene un servidor principal con dos interfaces de red (la segunda permitirá acceder al servidor cuando el backup esté funcionando) y un servidor de backup también con dos tarjetas de red (o bien puede utilizarse una sola en el redundante y emplear IP Alias para poder disponer de dos direcciones IP).
El servidor de backup debe de configurarse de forma que cuando se active (porque el principal ha sufrido algún problema y deja de funcionar) configure su tarjeta de red con la IP del servidor principal que debe de sustituir (bien configurando la única tarjeta con IP Alias o configurando una segunda tarjeta). A continuación, el servidor de backup utilizará ARP SPOOFING para asegurarse de que recibe todos los paquetes destinados al servidor que está sustituyendo. Los paquetes ARP que se enviarán informarán que la dirección MAC correspondiente a la IP del servidor principal es ahora la MAC del servidor de backup. Este envío debe de producirse de manera continua, mientras dure la caída del

principal, lo que evita que las cache arp se refresquen con la dirección MAC verdadera del servidor principal. Si la cache arp expirase y se actualizase con la MAC verdadera del servidor principal, se produciría un “race condition”, como se verá a continuación:




Como se aprecia en la figura, si el servidor de backup responde al ARP REQUEST con su ARP REPLY antes que el servidor principal, el ARP REPLY del backup se “machacará” con el del principal. Mientras que si es al contrario, será el ARP REPLY del principal el que será sustituido por el del servidor de backup. Esto no debe de llegar a producirse, ya que sino el proceso de redundancia sería inútil.
La activación del servidor de backup deberá de producirse de forma automática, ya que estos problemas suelen producirse de madrugada (no siempre claro) y no serviría de nada que fuésemos nosotros los que tuviésemos que activarlo manualmente.
Utilizar un servidor de NFS para ambos equipos sería lo más conveniente, ya que de esta forma se podrá acceder a los mismos contenidos desde ambos servidores, una solución interesante para servicios como HTTP, POP3, FTP.

# Autoevaluación

1. ¿Cuál es la función principal del protocolo ARP?

2. ¿En qué capa del modelo TCP/IP se encuentra definido el protocolo ARP?

3. Mediante un diagrama identifique los campos de los mensajes ARP.

4. ¿Cuál es el valor numérico del campo Ethertype cuando la trama Ethernet transporta un mensaje ARP?

# Para recordar

- ARP es un protocolo de bajo nivel que oculta el direccionamiento físico subyacente de red, al permitir que se asigne una dirección IP arbitraria a cada máquina. Por lo tanto, ARP es más parte del sistema físico de red y no tanto como parte de los protocolos de internet.

- De manera funcional, ARP está dividido en dos partes:
  La primera parte transforma una dirección IP en una dirección física cuando se envía un paquete.
  La segunda parte responde solicitudes de otras máquinas.

- Cuando los mensajes ARP viajan de una máquina a otra, se deben transportar en tramas físicas.

- En el caso de las tramas Ethernet, las tramas que transportan mensajes ARP tienen un campo de tipo de 0806hex. Este es un valor estándar asignado para Ethernet. Otras tecnologías de hardware de red utilizan otros valores.

SEMANA

9

# Protocolo ICMP

**TEMA**

Protocolo ICMP

**OBJETIVOS ESPECÍFICOS**

- Conocer el esquema de mensajes ICMP
- Identificar los distintos mensajes de error

**CONTENIDOS**

- Protocolo ICMP
- Protocolo de Mensajes de control de Internet
- Entrega de mensajes ICMP
- Prueba de accesibilidad y estado de un destino (Ping)
- Mensajes de error ICMP

**ACTIVIDADES**

- Reconocen los mensajes de control y error utilizados por ICMP.

## 9. PROTOCOLO ICMP

En aquellos casos en los que durante el proceso de ruteo un router no pudiera entregar un datagrama, o si el ruteador detectara una condición anormal que pudiera afectar su capacidad para direccionarlo (tráfico en la red), se necesita de un mecanismo que permita informar a la fuente original para que este evite o corrija el problema.
En esta parte se estudiará un mecanismo que permita hacer este trabajo.
Los ruteadores utilizan el mecanismo para reportar problemas, mientras que los hosts lo emplean para comprobar si los destinos son accesibles.

### 9.1. Protocolo de Mensajes de control de Internet

No hay que olvidar que el sistema de comunicación utilizado en Internet es uno sin conexión; por lo tanto, cada ruteador trabaja de manera autónoma, ruteando o entregando los datagramas que llegan sin ninguna coordinación con el transmisor original.
Este sistema es susceptible a fallas, de las cuales las más importantes se deben a lo siguiente:

- Fallas en las líneas de comunicación y en los procesadores
- Fallas cuando la PC destino está desconectada temporal o permanentemente de la red
- Cuando el TTL expira
- Cuando los ruteadores intermedios se congestionan tanto que no pueden procesar el tráfico entrante

En una red de redes en la que no es posible valerse de un mecanismo que le permita indicar si ocurrió una falla en la entrega, originada por un mal funcionamiento local o de red, la depuración de errores se vuelve muy difícil. El protocolo IP, por sí mismo, no contiene nada para ayudar al transmisor a comprobar la conectividad ni para ayudarle a aprender sobre dichas fallas. Por lo tanto, para permitir que los ruteadores en una inter red reporten los errores o proporcionen información sobre las circunstancias inesperadas, los diseñadores agregaron al TCP/IP un mecanismo de mensajes de propósito especial. Este protocolo es el ICMP y se considera como parte obligatoria del IP y, por lo tanto, está incluido en todas las implantaciones IP.
Los mensajes ICMP viajan a través de la red en la porción de datos de los datagramas IP. Sin embargo, el destino final de un mensaje ICMP no es un programa de aplicación ni un usuario en la máquina destino, sino el IP de dicha máquina.Cuando llega un mensaje de error ICMP, el módulo de ICMP lo maneja. En conclusión, el Protocolo de Mensajes de Control Internet permite que los ruteadores envíen mensajes de error o de control hacia otros ruteadores o anfitriones; el ICMP proporciona comunicación entre el software del Protocolo Internet en una máquina y el mismo software en otra. Algo interesante es que el ICMP no se restringe solo a los ruteadores, pues aunque con algunas restricciones cualquier PC puede enviar un mensaje ICMP a cualquier otra.
Así, un host puede usar el ICMP para comunicarse con un router o con un host.

### 9.2. ICMP: Reporte de errores

Técnicamente, el ICMP es un mecanismo de reporte de errores. Otorga una manera para que los ruteadores que encuentran un error lo reporten a la fuente original.
Si bien el protocolo subraya los usos deseables del ICMP y sugiere posibles acciones para responder a los reportes de error, el ICMP no especifica del todo las acciones que deben tomarse para cada posible error. Esto significa que cuando un datagrama causa un error, el ICMP solo puede reportar la condición del error a la fuente original del datagrama; la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema. La mayoría de los errores se originan en la fuente original; pero otros, no. Sin embargo, debido a que el ICMP reporta los problemas a

la fuente original, no se pueden utilizar para informar los problemas a los ruteadores intermedios. ¿Cuál es la razón por la que solo se informan de los errores al origen?
Un datagrama solo contiene campos que especifican la fuente original y el último destino; no contiene un registro completo de su viaje a través de la red. Los ruteadores pueden establecer y cambiar sus propias tablas de ruteo, no existe un conocimiento global de las rutas. Si un ruteador detecta un problema, no puede saber qué grupo de máquinas intermedias procesaron el datagrama, así que no puede informarles del problema.

### 9.3. Entrega de mensajes ICMP

Los mensajes ICMP requieren dos niveles de encapsulamiento:
Los datagramas que llevan mensajes ICMP se rutean exactamente como los que llevan información de usuario; no presentan una prioridad adicional. Así que, también, pueden perderse o descartarse.
Los mensajes ICMP no se generan por errores resultantes de datagramas que llevan mensajes de error ICMP.
Si bien el mensaje ICMP se encapsula y envía mediante el IP; el ICMP no se considera como un protocolo de nivel más alto, sino como una parte obligatoria de IP.
ICMP se debe encapsular dentro de IP, pues es muy probable que estos mensajes necesiten viajar a través de muchas redes físicas para llegar a su destino.

### 9.4. Formato de los mensajes ICMP

Si bien cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos 3 campos:

- **Campo TYPE :**
  De 8 bits y números enteros, que identifica el mensaje.
- **Campo CODE :**
  De 8 bits, da información sobre el tipo de mensaje.
- **Campo CHECKSUM :**
  De 16 bits (en este caso aplicable solamente al mensaje ICMP)

Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.
La razón de regresar el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa qué protocolo y qué programa de aplicación son responsables del datagrama.
Como se verá luego, los protocolos de más alto nivel de TCP/IP están diseñados para codificar información crucial en los primeros 64 bits.

El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos son los siguientes:

| Campo de tipo (TYPE) | Tipo de mensaje ICMP |
|---|---|
| 0 | Respuesta de Eco |
| 3 | Destino inaccesible |
| 4 | Disminución de origen |
| 5 | Redireccionar (cambiar una ruta) |
| 8 | Solicitud de eco |
| 11 | Tiempo excedido para un datagrama |
| 12 | Problema de parámetros en un datagrama |
| 13 | Solicitud de timestamp |
| 14 | Respuesta de timestamp |
| 15 | Solicitud de información (obsoleto) |

| | |
|---|---|
| 16 | Respuesta de información (obsoleto) |
| 17 | Solicitud de máscara de dirección |
| 18 | Respuesta de máscara de dirección |

### 9.5. Prueba de accesibilidad y estado de un destino (Ping)

Una de las herramientas de depuración más utilizadas incluyen los mensajes ICMP de *echo request* (solicitud de eco) y echo reply (respuesta de eco).
Un host o un ruteador envía un mensaje ICMP de solicitud de eco hacia un destino específico. Cualquier máquina que recibe una solicitud de eco formula una respuesta y la regresa al transmisor original. La solicitud de eco y su respuesta asociada se pueden utilizar para comprobar si un destino es alcanzable y si responde.
Muchos sistemas implementan las solicitudes de eco bajo el comando PING.
Las versiones mas sofisticadas de PING envían varias solicitudes de eco ICMP, capturan las respuestas y proporcionan estadísticas sobre las pérdidas de datagramas. Permiten que el usuario especifique la longitud de los datos que se envían, así como el intervalo entre solicitudes.

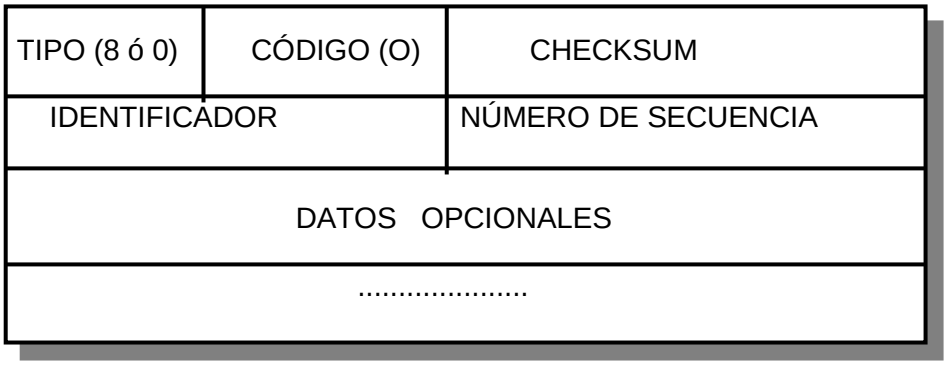
**Ping de la Muerte:**

Hacer pings no es malo; sin embargo, hay ocasiones en que puede ocasionar problemas. La más famosa de estas situaciones es el “ping de la muerte”, que envía paquetes muy grandes a un host remoto y puede hacer que este colapse. Sin embargo, la mayoría de los NOS actuales están actualizados contra este tipo de contingencia.

### 9.6. Mensajes de error ICMP

A continuación, pasará revista a los distintos mensajes de error posibles en ICMP.

#### 9.6.1 Formato del mensaje ICMP de solicitud de eco y de respuesta




- **Datos opcionales (optional data)**
  Campo de longitud variable. Contiene los datos que se regresarán al transmisor.
  Una respuesta de eco siempre regresa exactamente los mismos datos que se recibieron en la solicitud.
- **Identificador y número de secuencia**
  Se utilizan por el transmisor para responder a las solicitudes.

### 9.6.2 Formato del mensaje ICMP de reporte de destinos no accesibles

Cuando un ruteador no puede direccionar o entregar un datagrama IP, envía un mensaje de destino no accesible a la fuente original.


- **Código :**

  Contiene un entero que describe con más detalle el problema.

  Los valores posibles son los siguientes:

| VALOR DE CÓDIGO | SIGNIFICADO |
|---|---|
| 0 | Red inaccesible |
| 1 | Host inaccesible |
| 2 | Protocolo inaccesible |
| 3 | Puerto inaccesible |
| 4 | Se necesita fragmentación |
| 5 | Falla en la ruta de origen |
| 6 | Red de destino desconocida |
| 7 | Host de destino desconocido |
| 8 | Host de origen aislado |
| 9 | Comunicación con la red de destino administrativamente prohibida |
| 10 | Comunicación con el host de destino administrativamente prohibido |
| 11 | Red inaccesible por el tipo de servicio |
| 12 | Host inaccesible por el tipo de servicio |

Siempre que un error evite que un ruteador direccione o entregue un datagrama, el ruteador envía al origen un mensaje de destino no accesible y luego descarta el datagrama.
Los errores de red inaccesible ( 0 ), por lo general, implican fallas en el ruteo .
Los destinos pueden no ser accesibles ya sea porque el hardware esté temporalmente fuera de servicio (Host inaccesible=1) o porque el transmisor haya especificado una direccion de destino no existente (Falla en la ruta de origen=5). También, porque el ruteador no tenga una ruta para la red destino (Host de destino desconocido=7).
Si un ruteador necesita fragmentar un datagrama, pero está activado el bit de “no fragmentar”, el ruteador enviará un mensaje de “Se necesita fragmentación = 4”.

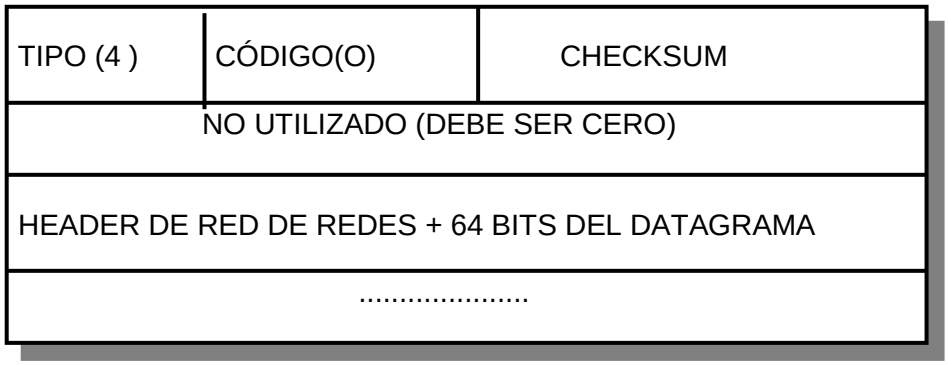
Si bien un ruteador envía mensajes de destino no accesible cuando encuentra un datagrama que no se puede direccionar o entregar, no puede detectar la totalidad de dichos errores.

### 9.6.3 Control de congestionamientos y de flujo de datagramas

Como IP funciona sin conexión, un ruteador no puede reservar memoria o recursos de comunicación antes de recibir datagramas. Por ello, los ruteadores se pueden saturar con el tráfico, condición conocida como congestionamiento.
El congestionamiento puede darse por dos razones:
Una computadora de alta velocidad puede ser capaz de generar tráfico de forma más rápida de lo que una red puede ser capaz de transferir.
Muchas computadoras necesitan enviar datagramas al mismo tiempo a través de un solo router, sin embargo, este se puede congestionar. Una máquina utiliza mensajes ICMP de disminución de tasa al origen (source quench) para reportar el congestionamiento a la fuente original. Este mensaje de disminución de tasa al origen es una solicitud para que la fuente reduzca la velocidad de transmisión de los datagramas. Se envía un mensaje de disminución de tasa al origen por cada datagrama que se descarta.

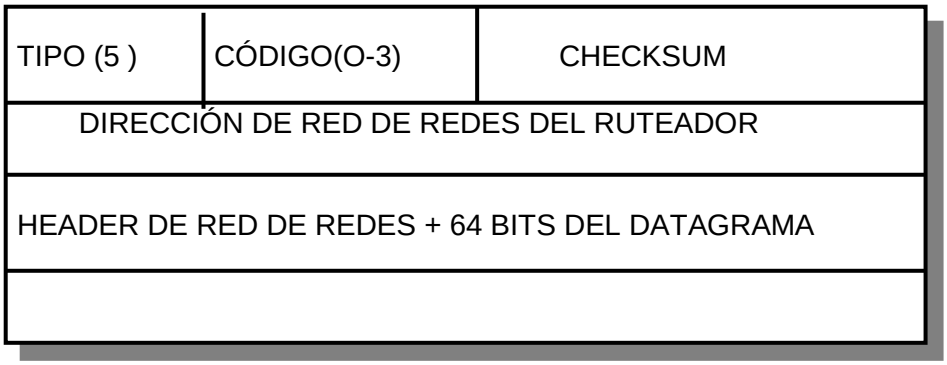
### 9.6.4 Formato del mensaje ICMP de disminución de tasa al origen

De manera adicional a los campos normales propios de ICMP, en este caso se utiliza un campo que contiene un prefijo de datagrama que identifica al que descartó.




### 9.6.5 Solicitudes para cambio de ruta desde los ruteadores

Las tablas de ruteo de una red de redes se mantienen sin cambios por grandes periodos de tiempo. Los hosts las inician desde un archivo de configuración en el arranque del sistema y los administradores de sistema, muy esporádicamente, hacen cambios de ruteo durante la operación normal.
Los ruteadores intercambian en forma periódica información de ruteo para incorporar los cambios en la red y para mantener actualizadas sus rutas.
Se asume que los ruteadores conocen rutas correctas; los hosts comienzan con información mínima de ruteo y aprenden nuevas rutas de los ruteadores.
Todo host arranca con información mínima y confía en los ruteadores para actualizar su tabla de ruteo. Cuando un ruteador detecta un host que utiliza una ruta no óptima, le envía al host un mensaje ICPM, llamado redireccionar (redirect), solicitándole que cambie sus rutas. El ruteador también direcciona el datagrama original hacia su destino.

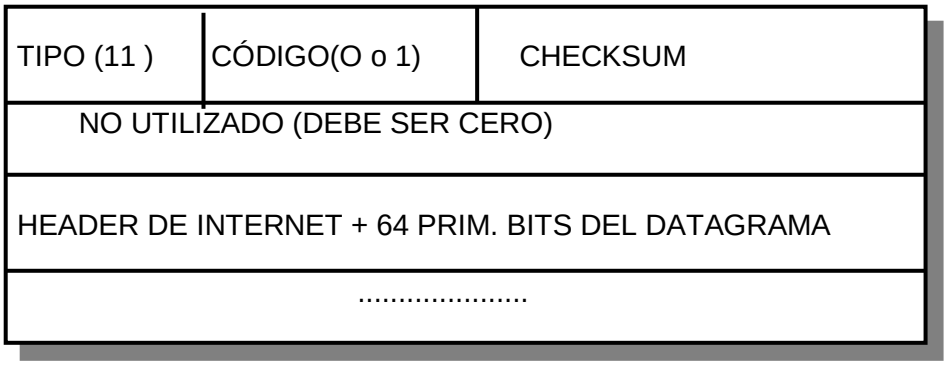



Además de los campos obligatorios de TYPE, CODE y CHECKSUM, cada mensaje de redireccionamiento contiene un campo de 32 bits llamado ROUTER INTERNET ADDRESS. Este campo contiene la dirección de un ruteador que el host utilizará para alcanzar el destino mencionado en el encabezado del datagrama.
El campo INTERNET HEADER contiene el encabezado IP , más los siguientes 64 bits del datagrama que activó el mensaje. De esta forma, un host que recibe el redireccionamiento ICMP examina el prefijo de datagrama para determinar la dirección de destino.

| Valor del Código (CODE) | Significado |
|---|---|
| 0 | Redireccionar datagramas para la red (obsoleto) |
| 1 | Redireccionar datagramas para el host |
| 2 | Redireccionar datagramas para el TOS y la red |
| 3 | Redireccionar datagramas para el TOS y el host |

### 9.6.6 Detección de rutas circulares o excesivamente largas :

Es posible que, debido a errores en las tablas de ruteo, se puedan generar ciclos de ruteo para algún destino.
Un ciclo de ruteo puede consistir en dos ruteadores, cada uno ruteando al otro un datagrama para el destino, D, o puede consistir en muchos ruteadores haciendo lo mismo. Cuando muchos ruteadores forman un ciclo, cada uno rutea un datagrama para el destino D y hacia el siguiente ruteador dentro del ciclo. Si un datagrama entra en un ciclo de ruteo, recorrerá indefinidamente y de manera circular todos los ruteadores.
Para evitar esto, existen los contadores de salto en cada datagrama IP. Siempre que un ruteador descarta un datagrama ya sea porque su conteo de saltos llega a cero o porque ocurre una terminación de tiempo mientras espera fragmentos de un datagrama, envía un mensaje ICMP de tiempo excedido a la fuente del datagrama.




En el campo CODE se explica la naturaleza de la terminación del tiempo.

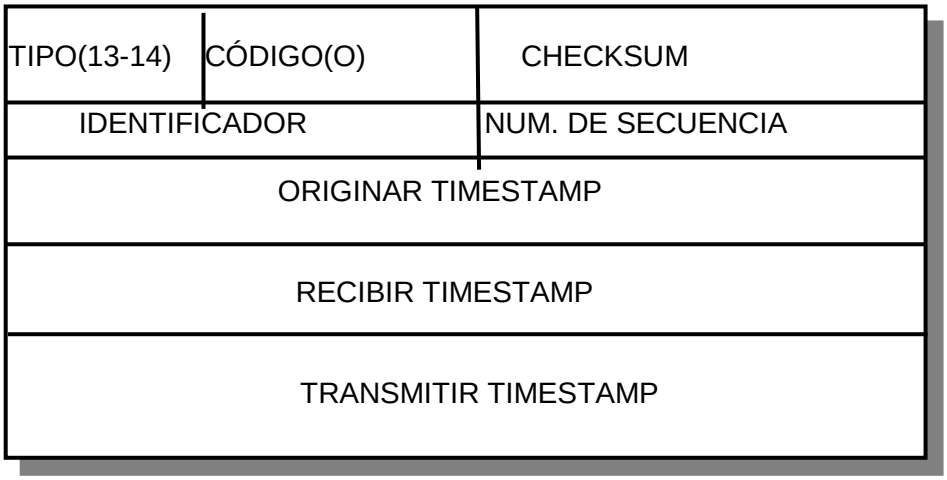
| Valor de Código | Significado |
|---|---|
| 0 | Conteo de tiempo de vida excedido |
| 1 | Tiempo para el reensamblado de fragmentos excedido. |

El reensamblado de fragmentos se refiere a la tarea de recolectar todos los fragmentos de un datagrama. Cuando llega el primer fragmento de un datagrama, el host que lo recibe arranca un temporizador y considera como error que dicho temporizador expire antes de que lleguen todas las piezas del datagrama.

### 9.6.7 Sincronización de relojes y estimación del tiempo de tránsito

Si bien las máquinas en una red se pueden comunicar, generalmente operan de forma independiente, y cada máquina mantiene su propia noción de la hora actual. Los relojes que varían demasiado pueden confundir a los usuarios de ciertos programas de sistemas distribuidos.

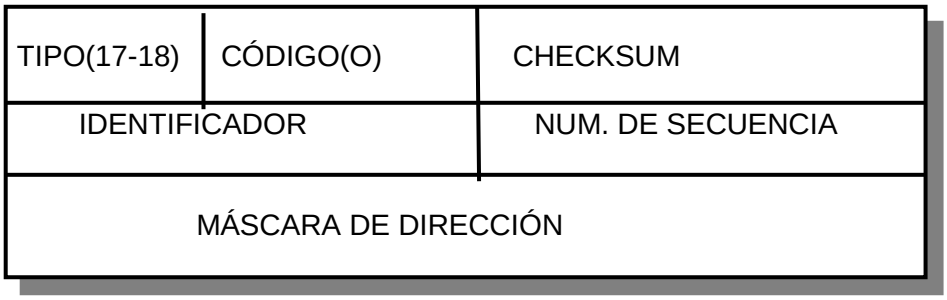
Por lo tanto, TCP/IP incluye varias técnicas para sincronizar los relojes, una de estas justamente utiliza los mensajes ICMP.
Una máquina solicitante envía un mensaje ICMP de solicitud de timestamp (marca de hora) a otra, solicitándole que informe su valor actual para la hora del día.



El campo TYPE identifica el mensaje como solicitud (13) o como respuesta(14): los campos IDENTIFIER y SEQUENCE NUMBER los utiliza la fuente para asociar las solicitudes con las respuestas.
Los campos restantes especifican la hora, en milisegundos desde la medianoche, en Tiempo Universal (GMT).
El campo ORIGINATE TIMESTAMP es llenado por la fuente original justo antes de transmitir el paquete; el campo RECEIVE TIMESTAMP se llena inmediatamente al recibir una solicitud; y el campo TRANSMIT TIMESTAMP se llena justo antes de transmitir la respuesta.
Los host utilizan estos tres campos para computar estimaciones del tiempo de retraso entre ellos y para sincronizar sus relojes.

### 9.6.8 Obtención de una máscara de subred

Para participar en el direccionamiento de subred, un host necesita saber qué bits de la dirección de red de redes de 32 bits corresponden a la red física, así como qué bits corresponden a los identificadores del host. La información necesaria para interpretar la dirección se representa en una cantidad de 32 bits llamada máscara de subred (subset mask).
Para aprender la máscara de subred utilizada para la red local, una máquina puede enviar un mensaje de solicitud de máscara de subred a un ruteador y recibir una respuesta de máscara de subred. La máquina que hace la solicitud puede enviar directamente el mensaje, si conoce la dirección del ruteador, o transmistir el mensaje por difusión.




El campo TYPE, en un mensaje de máscara de dirección, especifica si el mensaje es una solicitud (17) o una respuesta (18). Una respuesta contiene la máscara de dirección de subred en el campo ADDRESS MASK. Los campos IDENTIFIER y SEQUENCE NUMBER permiten que una máquina asocie las solicitudes con las respuestas.

# Autoevaluación

1. ¿Cuál es la necesidad de utilizar los mensajes ICMP?
2. Enumere las principales características de funcionamiento del ICMP.
3. Dibuje el formato del mensaje ICMP.
4. Enumere y describa los tipos de mensajes ICMP más utilizados.

# Para recordar

- En aquellos casos en los que durante el proceso de ruteo un router no pudiera entregar un datagrama, o si el ruteador detectara una condición anormal que pudiera afectar su capacidad para direccionarlo (tráfico en la red), se necesita de un mecanismo que permita informar a la fuente original para que este evite o corrija el problema.

- El protocolo IP, por sí mismo, no contiene nada para ayudar al transmisor a comprobar la conectividad ni para ayudarle a aprender sobre dichas fallas.

- Para permitir que los ruteadores en una interred reporten los errores o proporcionen información sobre las circunstancias inesperadas, los diseñadores agregaron al TCP/IP un mecanismo de mensajes de propósito especial.

  Este protocolo es el ICMP y se considera como parte obligatoria del IP y, por lo Tanto, está incluido en todas las implantaciones IP.

- Los mensajes ICMP viajan a través de la red en la porción de datos de los datagramas IP. Sin embargo, el destino final de una mensaje ICMP no es un programa de aplicación ni un usuario en la máquina destino, sino el IP de dicha máquina.

SEMANA

10

# Técnicas de Multidifusión

**TEMA**

Mensajes ICMP

**OBJETIVOS ESPECÍFICOS**

- Conocer el esquema de mensajes ICMP
- Identificar los distintos mensajes de error

**CONTENIDOS**

- La Multidifusión
- Multidifusión por hardware
- Multidifusión IP
- Direcciones de Multidifusión IP
- Conversión de direcciones de multidifusión IP en direcciones de multidifusión
- Protocolo de Administración de Grupos en Internet – IGMP
- Instalación del software IGMP
- Formato de los mensajes IGMP

**ACTIVIDADES**

- Hacen uso de la técnica de lluvia de ideas para identificar las características de las técnicas de Multidifusión.

## 10 La Multidifusión

La multidifusión es útil para entregas de punto-multipunto en una interred.
Es posible utilizar tres maneras para la entrega punto-multipunto:

1. Enviar la información individualmente usando direcciones de tipo unicast.
   La desventaja de este método es la duplicación del tráfico de la red y la sobrecarga de tener que mantener una lista de destinos unicast.
2. La otra alternativa es enviar la información en un solo paquete usando una dirección de difusión general (broadcast). Las ventajas de este método son el envío de un solo paquete y el no tener que mantener una lista de destinos de unicast.
   Las desventajas son el uso de paquetes de difusión (que molestan a todos los nodos) y el hecho que los ruteadores no retransmiten mensajes de broadcast.
   Un paquete de difusión alcanza a todos los equipos en una red, pero no a todos los equipos en una Inter-red.
3. La tercera posibilidad es enviar un paquete usando una dirección de multidifusión. Las ventajas de este método son el uso de un solo paquete y no tener que sobrecargar al equipo manteniendo un listado de destinos posibles.
   A diferencia de los paquetes de difusión, el tráfico de tipo multicast no molesta a los otros equipos que no están en escucha de los paquetes.
   Los ruteadores pueden soportar multidifusiones y reenviar los paquetes multicast a todos aquellos nodos que están en modo escucha. La técnica de multicast es la mejor opción para enviar tráfico de tipo punto-multipunto.

### 10.1 Multidifusión por hardware

A diferencia de la difusión, la multidifusión permite que cada máquina elija si quiere participar en ella. Generalmente, una tecnología de hardware reserva un conjunto extenso de direcciones para usarse con la multidifusión. Cuando un grupo de máquinas quiere comunicarse selecciona una dirección de multidifusión en particular para utilizarla durante la comunicación.
El direccionamiento de multidifusión puede considerarse como una generalización de todas las otras formas de difusión.
Así, puede considerarse una dirección de unidifusión como una forma de direccionamiento de multidifusión en la que hay exactamente una máquina en el grupo de multidifusión. Ethernet proporciona el mejor ejemplo de multidifusión en hardware. Ethernet utiliza el bit de menor orden del byte de mayor orden para distinguir la dirección de unidifusión convencional (con valor 0) de la dirección de multidifusión (con valor 1). En la notación hexadecimal con puntos, el bit de multidifusión se toma de la siguiente forma:

01.00.00.00.00.0 (hex)

Inicialmente, el hardware de interfaz de red está configurado para aceptar paquetes destinados a la dirección de difusión de Ethernet o la dirección de hardware de la máquina. Sin embargo, una interfaz puede reconfigurarse con facilidad para permitir el reconocimiento de un pequeño conjunto de direcciones de multidifusión.

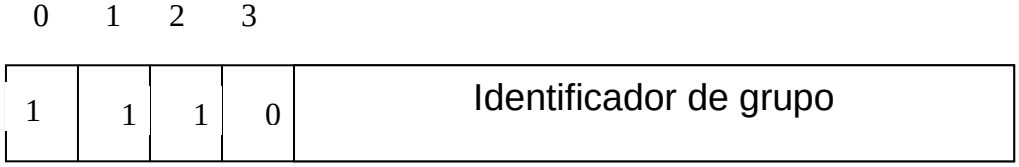
## 10.2 Multidifusión IP

La multidifusión IP es la abstracción inter-red del hardware de multidifusión. Permite la transmisión de un datagrama IP a un conjunto de hosts que forman un solo grupo de multidifusión.
La pertenencia a un grupo de multidifusión es un proceso dinámico. Así mismo, un host puede unirse o abandonar un grupo en cualquier momento. Además, un host puede ser miembro de un número indeterminado de grupos de multidifusión. Los miembros de un grupo determinan si el host recibirá datagramas enviados hacia el grupo de multidifusión: un host puede enviar datagramas hacia un grupo de multidifusión sin ser un miembro.
Cada grupo de multidifusión tiene una dirección de multidifusión única (de clase D). Como los puertos del protocolo TCP, algunas direcciones de multidifusión IP son asignadas por la autoridad de Internet (IANA) y corresponden a grupos que siempre existen aun cuando, actualmente, quizás no tengan miembros. Estas son las llamadas direcciones bien conocidas.
Otras direcciones de multidifusión están disponibles para usos temporales. Corresponden a grupos transitorios de multidifusión que se crean cuando son necesarios y se descartan cuando el número de miembros llega a cero.
La multidifusión IP puede utilizarse en una sola red física o a través de una Interred. En este último caso, se requieren ruteadores de multidifusión para enviar los datagramas de multidifusión.
Si un ruteador de multidifusión está presente, recibirá el datagrama y lo enviará hacia otra red conforme sea necesario.

## 10.3 Direcciones de Multidifusión IP

Al igual que el hardware de red, la multidifusión IP se vale de la dirección de destino de datagrama para especificar una entrega de multidifusión. La multidifusión IP utiliza direcciones clase D.

Los primeros 4 bits contienen 1110 e identifican la dirección como una multidifusión. Los 28 bits restantes especifican un grupo de multidifusión particular. Los bits del 4 al 31 identifican la dirección como una multidifusión.




El rango de direcciones de multidifusión abarca de:

224.0.0.0 a 239.255.255.255

La dirección 224.0.0.0 está reservada, no se puede asignar a ningún grupo.
La dirección 224.0.0.1 está asignada permanentemente ***al grupo de todos los anfitriones***, el cual incluye a todos los hosts y ruteadores que participan en la multidifusión IP.

La dirección del grupo de todos los host se utiliza para alcanzar todas las máquinas que participan en la multidifusión IP en una red local. No hay direcciones de multidifusión IP que hagan referencia a todos los hosts en la interred.
Las direcciones de multidifusión IP solo pueden emplearse como direcciones de destino.
Estas direcciones nunca aparecerán en el campo de dirección de la fuente de un datagrama.
No hay manera de generar mensajes de error ICMP relacionados con datagramas de multidifusión.

## 10.4 Conversión de direcciones de multidifusión IP en direcciones de multidifusión Ethernet

Para transformar una dirección de multidifusión IP en una dirección de multidifusión Ethernet, se deben colocar los 23 bits de orden menor de la dirección de multidifusión IP dentro de los 23 bits de orden inferior de la dirección de multidifusión Ethernet especial 01.00.5E.00.00.00 (hex).

De esta forma la dirección de multidifusión IP 224.0.0.1 se convierte en la dirección de multidifusión Ethernet 01.00.5E.00.00.01 (hex).

### Extensión de IP para manejar la multidifusión

Un hosts trabaja en un entorno de multidifusión en cualquiera de los 3 niveles:

| Nivel | Significado |
|---|---|
| 0 | El host no puede ni enviar ni recibir multidifusión IP. |
| 1 | El host puede enviar pero no recibir multidifusión IP. |
| 2 | El host puede enviar y recibir multidifusión IP. |

Para enviar mensajes de multidifusión IP, el software IP debe permitir a un programa de aplicación especificar una dirección de multidifusión como una dirección IP de destino y el software de interfaz de red debe ser capaz de transformar una dirección de multidifusión IP en la correspondiente dirección de multidifusión hardware.
Recibir datagramas de multidifusión IP es más complejo. El software IP en el host debe tener una interfaz que permita a un programa de aplicación declarar si desea unirse o abandonar un grupo de multidifusión en particular. Si diversos programas de aplicación se unen al mismo grupo, el software IP debe recordar cada uno de ellos para transferir una copia de los datagramas que llegan destinados para este grupo. Si todos los programas de aplicación abandonan un grupo, el host debe recordar que no quedan participantes en el grupo. También, se hace necesario que el host debe ejecutar un programa que informe a los ruteadores de multidifusión locales del estado de los miembros de un grupo.

## 10.5 Protocolo de Administración de Grupos en Internet – IGMP

Para participar en la multidifusión IP dentro de una red local, un host debe tener el software que le permita enviar y recibir datagramas de multidifusión.
Para participar en una multidifusión que cubra varias redes, el host debe informar a los ruteadores de multidifusión local.
El ruteador local se pone en contacto con otros ruteadores de multidifusión, pasando información hacia los miembros y estableciendo rutas.

Previamente a que un ruteador de multidifusión pueda difundir información a los miembros de multidifusión, debe determinar si uno o más hosts en la red local han decidido unirse a un grupo de multidifusión. Para realizar esto, los ruteadores de multidifusión y los hosts que implantan la multidifusión deben utilizar el Protocolo de Administración de Grupos de Internet (IGMP), para poder comunicar información a los miembros del grupo.
El IGMP es análogo al ICMP, así como este utiliza datagramas IP para transportar mensajes.
El IGMP es un estándar para el TCP/IP. Este es requerido en todas las máquinas que participan en multidifusión IP en el nivel 2.
Conceptualmente, el IGMP tiene 2 fases:

**Fase 1:**

Cuando un host se une a un nuevo grupo de multidifusión envía un mensaje IGMP para la dirección de multidifusión "todos los hosts", declarando su pertenencia a dicho grupo.
Los ruteadores de multidifusión local reciben el mensaje y establecen el ruteo necesario para difundir la información de pertenencia del grupo hacia otros ruteadores de multidifusión a través de la interred.

**Fase 2:**

Debido a que la pertenencia a un grupo es dinámica, los ruteadores de multidifusión local muestrean de manera periódica a los hosts en la red local para determinar qué hosts se mantienen como miembros y de qué grupos.
Si en un grupo no se reportan miembros después de varios muestreos, el ruteador de multidifusión asume que no hay hosts en la red que se mantengan en el grupo y deja de anunciar miembros del grupo a otros ruteradores de multidifusión.

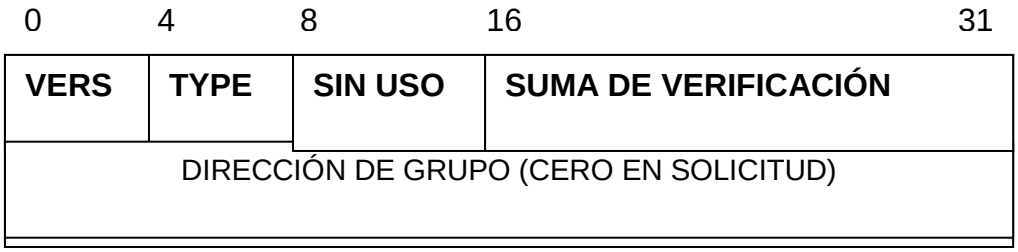
### 10.5.1 Instalación del software IGMP

Este protocolo está diseñado para evitar congestionamiento en una red local.
Toda la comunicación entre hosts y ruteadores de multidifusión utilizan multidifusión IP. Esto significa que cuando los mensajes IGMP están encapsulados en un datagrama IP para su transmisión, la dirección de destino IP es la dirección de multidifusión de todos los hosts.
Esto significa que, en las redes en las que el hardware soporta la multidifusión, los hosts que no participan en la multidifusión IP nunca reciben mensajes IGMP.

Un ruteador de multidifusión no enviará mensajes de solicitud individuales para cada grupo de multidifusión, sino un mensaje de muestreo para solicitar información relacionada con la membresía en todos los grupos. La cantidad de muestreos está restringida, a lo sumo, a una solicitud por minuto.

Los hosts, que son miembros de varios grupos, no envían respuestas múltiples al mismo tiempo. Cuando llega un mensaje de solicitud IGMP desde un ruteador de multidifusión, el host asigna un retardo aleatorio de entre 0 y 10 segundos para cada grupo en el que tiene miembros, y envía una respuesta para este grupo después del retardo. Así, un host separa sus respuestas aleatoriamente dentro de un lapso de 10 segundos.

### 10.5.2 Formato de los mensajes IGMP




VERS: Conserva la versión del protocolo.

TYPE: Identifica el mensaje como
Una solicitud enviada por un ruteador de multidifusión (1).
Una respuesta enviada por un anfitrión (2).

CHECKSUM:
Contiene una suma de verificación para el mensaje IGMP de 8 bytes.

DIRECCIÓN DE GRUPO:
Los hosts contienen una dirección que define la pertenencia a un grupo de multidifusión determinado.
En solicitudes, el campo contiene ceros y no tiene significado.

# Autoevaluación

1. Identifique el rango de direcciones Clase D.

2. Mediante un diagrama, identifique los campos que forman parte de los mensajes IGMP.

3. Identifique la diferencia entre un envío de tipo Multicast frente a mensaje de tipo Broadcast.

4. Indique si es cierto que los envíos Unicast pueden ser interpretados como un tipo particular de Multidifusión.

5. ¿Los grupos de Multidifusión pueden abarcar computadoras de redes distintas?

# Para recordar

- Para enviar mensajes de multidifusión IP, el software IP debe permitir a un programa de aplicación especificar una dirección de multidifusión como una dirección IP de destino.

- La multidifusión IP es la abstracción inter-red del hardware de multidifusión.

- El tráfico de tipo multicast no molesta a los otros equipos que no están en escucha de los paquetes.

- El IGMP es un estándar para el TCP/IP. Este es requerido en todas las máquinas que participan en multidifusión IP en el nivel 2.

- Un ruteador de multidifusión no enviará mensajes de solicitud individuales para cada grupo de multidifusión, sino un mensaje de muestreo para solicitar información relacionada con la membresía en todos los grupos.

SEMANA

11

# Capa de Transporte

**TEMA**

Capa de transporte

**OBJETIVOS ESPECÍFICOS**

- Conocer las funciones específicas de la capa de transporte
- Identificar los procesos que garantizan las entregas confiables y de control de flujo

**CONTENIDOS**

- Mecanismo de multiplexación
- Protocolo TCP
- Datagrama TCP
- Protocolo UDP

**ACTIVIDADES**

- Identifican el proceso de entregas seguras utilizada en la capa de transporte.

## 11. Capa de Transporte

La capa de transporte ofrece a la capa de aplicación dos servicios: un servicio orientado a conexión protocolo TCP "Transmition Control Protocol" y un servicio no orientado a conexión protocolo UDP "User Datagram Protocol". La unidad de envío o recepción datos del protocolo TCP se conoce con el nombre de segmento TCP, y la unidad de envío o recepción de datos del protocolo UDP es conocido como segmento UDP. La función del protocolo TCP consiste en ofrecer un servicio de envío y recepción de datos orientados a conexión que sea seguro y que goce de los siguientes mecanismos:

- Multiplexamiento
- Conexiones
- Fiabilidad
- Control de flujo y congestión

### 11.1. Mecanismo de multiplexación

El mecanismo de multiplexamiento consiste en que más de una aplicación pueda utilizar los servicios del protocolo TCP. El protocolo TCP hace uso de los parámetros de control: Puerto destino y Puerto origen incluidos en una cabecera TCP y los parámetros de control: Dirección IP Destino y Dirección IP Origen incluidos en una cabecera IP con el fin de satisfacer el mecanismo de multiplexamiento. Cuando los números de puerto son concatenados con las direcciones IP de la capa de enrutamiento, conforman lo que se denomina un conector "socket". Un par de conectores identifica de forma única la conexión bidireccional entre una aplicación cliente y una aplicación servidor.

### 11.1.2. Mecanismo de cotrol de flujo

El protocolo TCP está diseñado para controlar el envío y recepción de segmentos TCP a fin de evitar momentos de congestión en la red. Las principales técnicas de control de flujo implementadas en el protocolo TCP son los siguentes:

- Desplazamiento de ventana "Sliding Window"
- Comienzo lento "Slow Start" y control de congestión

La técnica de desplazamiento de ventana es una técnica de control del flujo impuesta por el receptor de segmentos TCP con el fin de evitar momentos de congestión en el computador receptor. Durante el proceso de inicialización de una conexión TCP, el proceso TCP de cada computador da a conocer los parámetros de control ventana y MSS. Con estos dos parámetros el proceso de envío de segmentos del protocolo TCP puede calcular el máximo número de segmentos que puede recibir el proceso de recepción del protocolo TCP en un momento determinado. El parámetro ventana incluido en una cabecera TCP es un registro de 16 bits y el valor del mismo puede variar durante el envío y recepción de segmentos TCP hasta llegar al punto de que sea igual a cero. Cuando esto ocurre, indica que el proceso de recepción de segmentos no está en capacidad de recibir ningún segmento TCP, ya que el buffer de recepción se encuentra completamente lleno. Esto obliga al proceso de envío de segmentos TCP del computador remoto no transmitir ningún segmento hasta que el parámetro de control ventana sea mayor o igual a un segmento. Esta técnica funciona si la conexión TCP se establece en una red local, pero cuando la conexión TCP se establece a través de una red WAN los enrutadores pueden experimentar momentos de congestión, ya que los mismos interactúan con un servicio de no orientado a la conexión. Además la capacidad de envío y recepción de datos de un enlace WAN en la mayoría de los casos es mucho menor que el de una red LAN. Para

resolver este inconveniente, el protocolo TCP hace uso de la técnica comienzo lento "Slow Start" y control de congestión. Estas técnicas son de control de flujo impuestas en el emisor para evitar momentos de congestión en la red.
Las técnicas slow start y control de congestión consisten en que el transmisor de segmentos TCP hace uso de los parámetros de control: ventana de congestión y umbral de congestión. El parámetro de control de ventana de congestión es utilizado para calcular el máximo número de segmentos que pueden ser transmitidos por el transmisor en un momento determinado. Y el parámetro umbral de congestión es utilizado para detectar momentos de congestión en la red.
El valor inicial del parámetro congestión de ventana es igual al parámetro MSS y el valor inicial del umbral de congestión es igual a 65535. Por cada número de acuse recibido de cada segmento transmitido, el parámetro congestión de ventana se incrementa a un MSS; esto implica un posible crecimiento exponencial de este parámetro. El máximo número de segmentos TCP que el transmisor puede enviar en un momento dado es seleccionado por el mínimo valor de la comparación de los parámetros Ventana y Congestión de ventana, es decir, que si el valor del parámetro Ventana es igual a 4096 bytes y el parámetro Congestión de ventana es igual a 2048 bytes, el transmisor de segmentos TCP hará uso del parámetro congestión de ventana para determinar el máximo número de segmentos que pueden ser transmitidos en un momento dado. El crecimiento del parámetro congestión de ventana se detiene hasta que el mismo sea igual al parámetro de control ventana. Si el transmisor de segmentos TCP detecta un posible momento de congestión en la red debido a que el tiempo de espera de un número de acuse recibido expiró, el protocolo slow start se inicia nuevamente inicializando la ventana de congestión con el valor asignado al MSS y el parámetro umbral de congestión se le asigna un valor igual a la mitad de la ventana de transmisión, pero nunca por debajo de dos segmentos. Esto implica que el umbral de congestión es determinado por la siguiente fórmula:

Umbral de congestión = máx. [2 segmentos, 1 / 2 min. (Ventana, ventana de congestión)]

Luego, la técnica **slow start** entra en acción hasta que el parámetro congestión de ventana sea mayor que el umbral de la congestión. Cuando esto ocurre, el crecimiento de la ventana de congestión deja de ser exponencial, ya que se incrementa a uno no por cada número de acuse recibido por segmento, sino por el grupo de números de acuse recibido del rango de segmentos que son incluidos en la ventana de congestión en ese momento. Se dice que el protocolo de transmisión TCP se encuentra en el estado **slow start** si la ventana de congestión es menor o igual al umbral de congestión. Y si la ventana de congestión es mayor que el umbral de congestión se dice que el protocolo de transmisión se encuentra en un estado de control de congestión.

### 11.1.3. Control de flujo para aplicaciones interactivas

Ejemplo: Telnet hace uso de los servicios de la capa de transporte por cada caracter a ser enviado, el protocolo TCP crea un segmento TCP de 21 Bytes que al ser encapsulado por la capa de enrutamiento (Red en OSI o Interned en TCP/IP) tenemos un paquete de 41 Bytes. Una vez que este paquete es recibido y procesado, el computador destino envía un paquete IP de 40 bytes, el cual incluye el número de acuse recibido del segmento enviado. Esto implica que por cada caracter a ser enviado se requieren como mínimo de 81 Bytes. Para optimizar esta situación en el receptor, muchas de las aplicaciones retardan el envío de los números de acuse recibido o las actualizaciones de ventanas a un tiempo fijo, el cual varía dependiendo de la aplicación TCP. Este retardo se encuentra en el rango de 200mseg - 500mseg. Para el transmisor se hace uso del algoritmo de Nagle, el cual consiste en enviar el primer carácter y almacenar en un buffer los posibles nuevos caracteres que serán enviados cuando se reciba el número de acuse recibido del primer carácter.

### 11.1.4. Tiempo de espera de retransmisión

Debido a la variabilidad de las redes que componen el sistema de redes de la red Internet y la gran cantidad de casos de conexiones TCP, el tiempo de espera de retransmisión se debe determinar dinámicamente, ya que el tiempo de ida y vuelta es distinto para cada conexión TCP.
Se verá una manera de determinar un tiempo de espera de retransmisión.

- Mídase el tiempo transcurrido entre el envío de un octeto de datos con un número de secuencia determinado y la recepción de un acuse de recibo que incluya ese número de secuencia (los segmentos enviados no tienen por qué concordar con los segmentos recibidos). Este tiempo medido es la muestra del tiempo de ida y vuelta 'Round Trip Time' o RTT.
- Calcular un promedio ponderado del **RTT:**
- **RTT-Estimado** = alpha x RTT-Estimado + Beta * RTT-Muestra. Donde alpha + beta = 1. alpha entre 0.8 y 0.9 y beta entre 0.1 y 0.2.
- El tiempo de espera de retransmisión => RTO = 2 * RTT-Estimado.

El inconveniente de este algoritmo es que no se distingue entre un ACK del segmento enviado y un ACK de retransmisión.
Los algoritmos de Karn y Partridge solucionan este problema no tomando muestras del RTT al retransmitir un segmento y duplicando el RTO después de cada retransmisión.

## 11.2 Protocolo TCP

TCP define el segundo servicio más importante y mejor conocido de nivel de red, la entrega de flujo confiable. Además, TCP añade una funcionalidad substancial a los protocolos que ya se han analizado, pero, a su vez, su implantación es substancialmente más compleja. Si bien forma parte de TCP/IP, es cierto que puede ser adaptado para ser utilizado con otros sistemas de entrega.

### 11.2.1. Necesidad de la entrega de flujo

En el nivel más bajo, las redes de comunicación por PC proporcionan una entrega de paquetes no confiable. Esto significa que los paquetes se pueden perder o destruir, cuando falla el hardware de red o cuando las redes se sobrecargan. También, los paquetes se pueden entregar en desorden, con retraso o duplicados.
En el nivel más alto, los programas de aplicación, a menudo, necesitan enviar grandes volúmenes de datos de una PC a otra. Utilizar un sistema de entrega sin conexión y no confiable para las transferencias de gran volumen se vuelve tedioso, molesto y requiere que los programadores incorporen, en cada programa de aplicación, la detección y solución de errores.

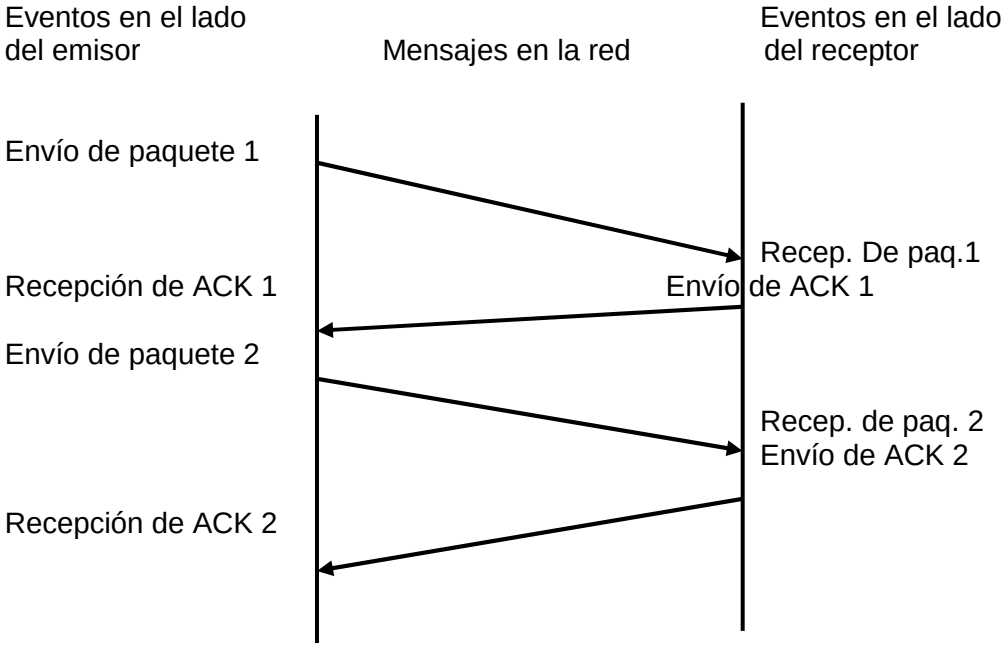
### 11.2.2 Características del servicio de entrega fiable

- Orientación de flujo
- Se refiere al servicio de entrega de flujo que se da entre la máquina de destino y la máquina de origen.
- Conexión de circuito virtual
- Transferencia con memoria intermedia
- Flujo no estructurado
- Conexión Full Duplex

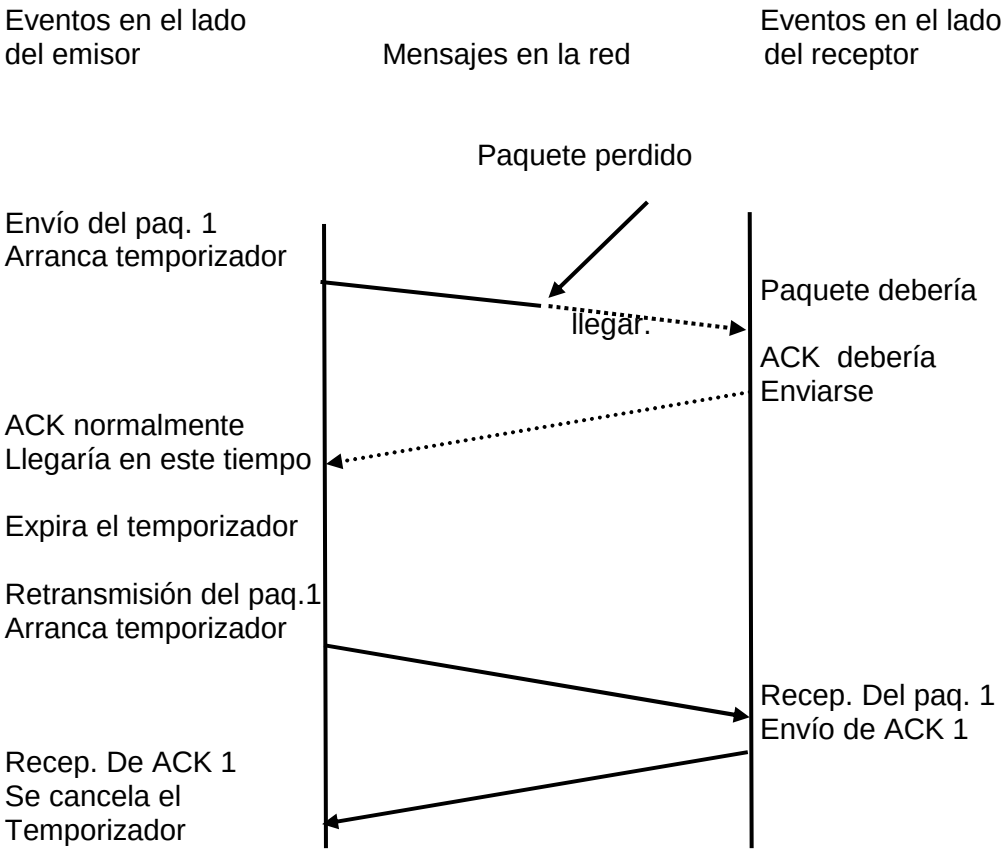
### 11.2.3. Características de confiabilidad

El problema es el de proporcionar un protocolo confiable sobre un sistema subyacente de comunicación no confiable. La solución es utilizar una técnica conocida como acuse de recibo positivo con retransmisión. Esta técnica requiere que un receptor se comunique con el origen y le envíe un mensaje de acuse de recibo (ACK) conforme recibe los datos. El transmisor guarda un registro de cada paquete que envía y espera un acuse de recibo antes de enviar el siguiente paquete. El transmisor, también arranca un temporizador cuando, envía un paquete y lo retransmite si dicho temporizador expira antes de que llegue un acuse de recibo.

En el gráfico, se aprecia el modo de operar de un protocolo que se vale de reconocimientos o acuses de recibo positivos, con retransmisión, en la cual el emisor espera un acuse de recibo para cada paquete enviado. La distancia vertical bajo la figura representa el incremento en el tiempo y las líneas que cruzan en diagonal representan la transmisión de paquetes de red.




La figura siguiente muestra qué sucede cuando se pierde o corrompe un paquete. El transmisor arranca un temporizador después de enviar el paquete. Cuando termina el tiempo, el transmisor asume que el paquete se perdió y lo vuelve a enviar. En el gráfico inferior, se ve el tiempo excedido y la retransmisión que ocurre cuando un paquete se pierde. La línea punteada muestra el tiempo que podría ocuparse para la transmisión de un paquete y su acuse de recibo, si no se perdiera el paquete. Otro problema que se da es el de los paquetes duplicados. Los duplicados pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión prematura. La solución de la duplicación requiere acciones cuidadosas, ya que tanto los paquetes como los acuses de recibo se pueden duplicar.




### 11.2.4. La técnica de las ventanas deslizantes

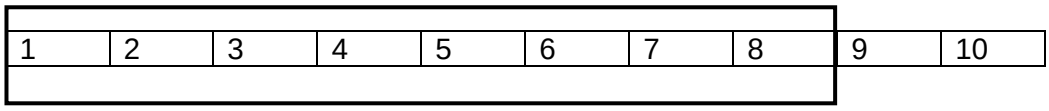
Para lograr que el flujo de transmisión sea eficiente, se hace necesario introducir el concepto de ventana deslizable. Si se analiza la manera cómo se da el mecanismo de transmisión de datos, se verá que estos datos solo fluyen entre las máquinas en una dirección a la vez, inclusive si la red tiene capacidad para comunicación simultánea en ambas direcciones. Esto demuestra que la red tiene periodos ociosos durante el tiempo en que las máquinas retrasan sus respuestas. Así se tiene que un protocolo simple de acuses de recibo positivos ocupa una cantidad sustancial de ancho de banda de red debido a que debe retrasar el envío de un nuevo paquete hasta que reciba un acuse de recibo del paquete anterior. La técnica de ventana deslizable es una forma más compleja de acuse de recibo positivo y retransmisión que el sencillo método mencionado antes. Esta técnica utiliza el ancho de banda de mejor forma, ya que permiten que el trasmisor envíe varios paquetes sin esperar un acuse de recibo.

El protocolo coloca una ventana pequeña y de tamaño fijo en la secuencia, y transmite todo los paquetes que residan dentro de la ventana.

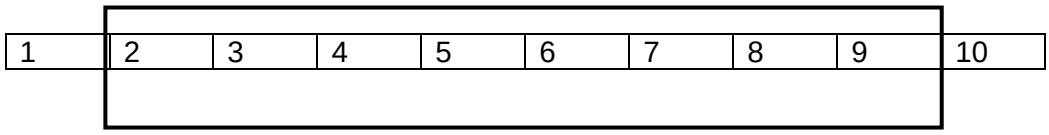
En el gráfico se puede ver un protocolo de ventana deslizante con 8 paquetes en la ventana en el caso A.

En el caso B, la ventana que se desliza hacia el paquete 9 puede enviarse cuando se recibe un acuse de recibo del paquete 1. Únicamente se retransmiten los paquetes sin acuse de recibo.

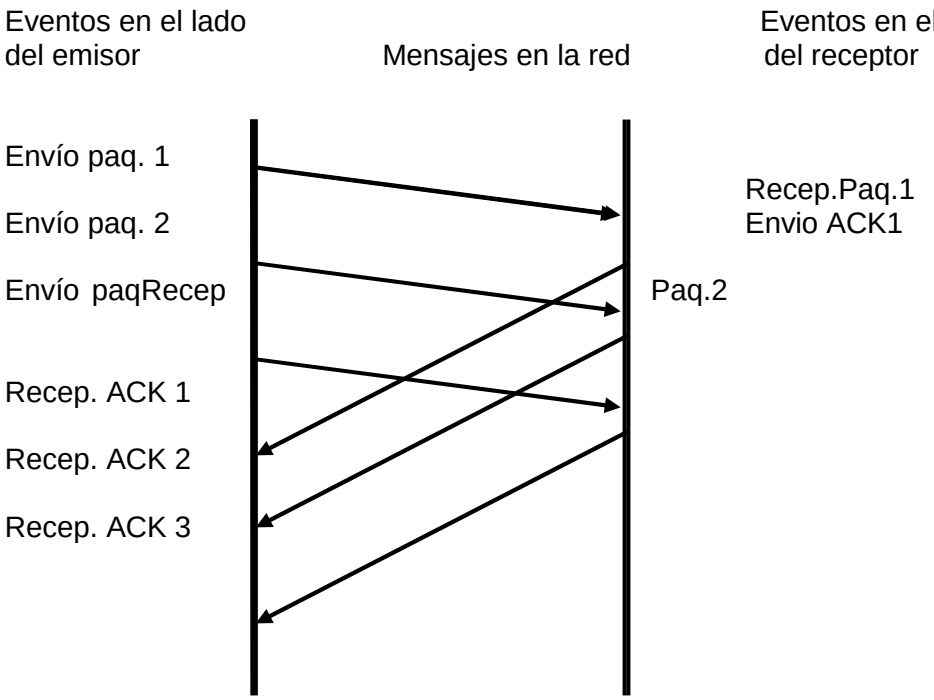
**A. Ventana inicial**




**B. Deslizamiento de la ventana**




Un paquete es *unacknowledged* o sin acuse de recibo si se transmitió, pero no se recibió ningún acuse de recibo. Una vez que el transmisor recibe un acuse de recibo para el primer paquete dentro de la ventana, mueve la misma y envía el siguiente paquete. La ventana continua, moviéndose en tanto se reciban acuses de recibo. El desempeño de los protocolos de ventana deslizable dependen del tamaño de la ventana y de la velocidad en que la red acepta paquetes. Con un tamaño de ventana de 1, un protocolo de ventana deslizable sería idéntico a un protocolo simple de acuse de recibo positivo. Al aumentar el tamaño de la ventana, es posible eliminar completamente el tiempo ocioso de la red. Lo importante aquí es ver que como un protocolo de ventana deslizable bien establecido mantiene la red completamente saturada de paquetes, con él se obtiene una generación de salida substancialmente más alta que con un protocolo simple de acuse de recibo positivo. A continuación, se puede ver el ejemplo de tres paquetes transmitidos mediante un protocolo de ventana deslizante. El concepto clave es que el emisor puede transmitir todos los paquetes de la ventana sin esperar un acuse de recibo.



### 11.2.5. Protocolo de control de transmisión

El TCP es un protocolo de comunicación, no una pieza de software.
Las funciones precisas proporcionadas por el TCP son las siguientes:

- Especificar el formato de datos y los acuses de recibo que intercambian dos computadoras para lograr una transferencia confiable.
- Implementar procedimientos que la computadora utiliza para asegurarse de que los datos lleguen de manera correcta.
- Especificar técnicas para distinguir entre muchos destinos en una misma máquina.
- Dada la comunicación, resolver problemas tales como la pérdida o duplicación de paquetes.

### 11.2.6. Puertos, conexiones y puntos extremos

El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el demultiplexado del tráfico TCP entrante entre los programas de aplicación. Al igual que el UDP, el TCP utiliza números de puerto de protocolo para identificar el destino final dentro de una máquina.
Sin embargo, los puertos TCP son mucho más complejos, ya que un número de puerto no corresponde a un solo objeto. De hecho, el TCP se diseñó según la abstracción de conexión, en la que los objetos que se van a identificar son conexiones de circuito virtual, no puertos individuales. Entender que el TCP utiliza la noción de conexiones es crucial, ya que ayuda a explicar el significado y la utilización de los números de puerto TCP. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos.
Ahora lo importante es saber qué son exactamente los puntos extremos de una conexión.
Una conexión consiste en un circuito virtual entre 2 programas de aplicación, por lo que puede ser natural asumir que un programa de aplicación sirve como el punto extremo de la conexión. Sin embargo, no es así. El TCP define que un punto extremo es un par de números enteros (host,puerto), en donde host es la dirección IP de un host y puerto es un puerto TCP en dicho host.
Por ejemplo, el punto extremo (128.10.2.3, 25), se refiere al puerto TCP 25 en las máquinas con dirección IP 128.10.2.3.
Luego, la conexión está definida por dos puntos extremos.
La abstracción de conexión permite que varias conexiones compartan un punto extremo. Como el TCP identifica una conexión por medio de un par de puntos extremos, varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

### 11.2.7. Aperturas pasivas y activas

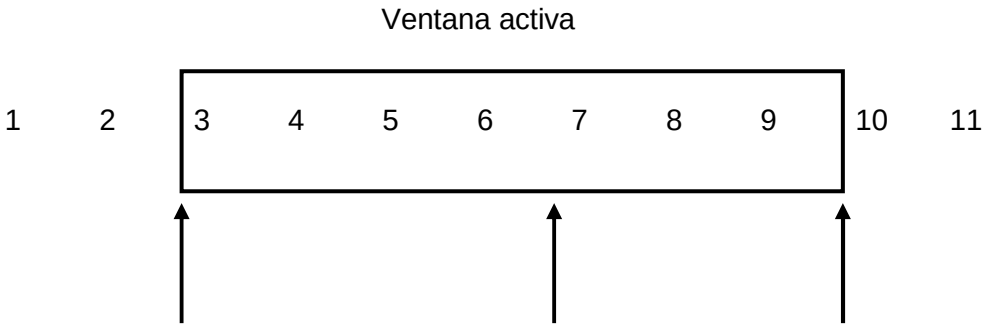
El TCP es un protocolo orientado a la conexión, que requiere que ambos puntos extremos estén de acuerdo en participar. Para ello, el programa de aplicación en un extremo realiza una función de apertura pasiva al contactar su sistema operativo e indicar que aceptará una conexión entrante. En ese momento, el sistema operativo asigna un número de puerto TCP a su extremo de la conexión. El programa de aplicación en el otro extremo debe contactar a su sistema operativo mediante una solicitud de apertura activa para establecer una conexión. Una vez que se crea ésta, los programas de aplicación pueden comenzar a transferir datos; los módulos de software TCP en cada extremo intercambian mensajes que garantizan la entrega confiable.

### 11.2.8. Segmentos, flujos y números de secuencia

El TCP visualiza el flujo de datos como una secuencia de bytes que divide en segmentos para su transmisión.
Generalmente, cada segmento viaja a través de una red como un sólo datagrama IP.
El TCP utiliza un mecanismo especializado de ventana deslizable para solucionar 2 problemas importantes:

- La transmisión eficiente
- El control de flujo

De manera similar al caso anterior, el mecanismo de ventana del TCP hace posible enviar varios segmentos antes de que llegue un acuse de recibo.
La forma TCP de un protocolo de ventana deslizable también soluciona el problema de control de flujo de extremo a extremo, al permitir que el receptor restrinja la transmisión hasta que tenga espacio suficiente en memoria intermedia para incorporar más datos.
El mecanismo TCP de ventana deslizable opera a nivel de byte, no a nivel de segmento ni de paquete.



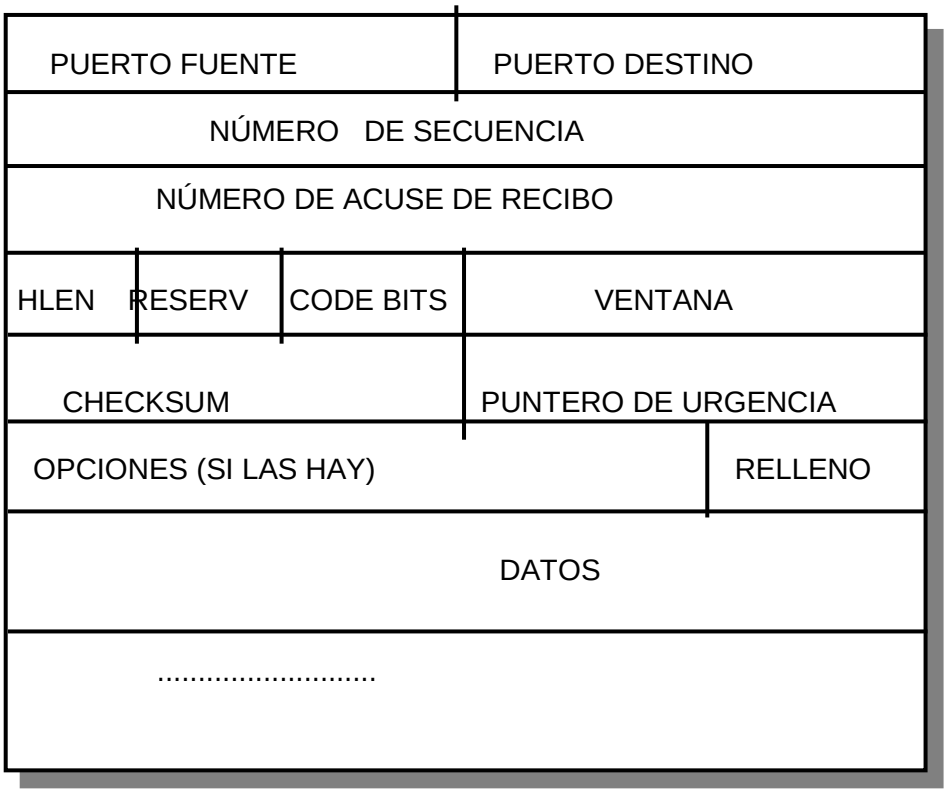

Este es el ejemplo de una ventana deslizante del TCP. Los bytes hasta el 2 se han enviado y reconocido, los bytes del 3 al 6 han sido enviados pero no reconocidos, los bytes del 7 al 9 no se han enviado pero serán enviados sin retardo y los bytes del 10 en adelante no pueden ser enviados hasta que la ventana se mueva.

### 11.2.9. Tamaño variable de ventana y control de flujo

Una diferencia entre el protocolo TCP de ventana deslizable y el protocolo simplificado de ventana deslizable es que el TCP permite que el tamaño de la ventana varíe. Cada acuse de recibo, que informa cuántos bytes se recibieron, contiene un aviso de ventana, que especifica cuántos bytes adicionales de datos está preparado para aceptar el receptor.
En respuesta a un aumento en el aviso de ventana, el transmisor aumenta el tamaño de su ventana deslizable y procede al envío de bytes de los que todavía no se tiene un acuse de recibo. La ventaja de utilizar una ventana de tamaño variable es que ésta proporciona control de flujo así como una transferencia confiable.
Si la memoria intermedia del receptor se llena, no puede aceptar más paquetes, así que envía un anuncio de ventana más pequeño. En caso extremo, el receptor anuncia un tamaño de ventana igual a cero para detener toda la transmisión. Después, cuando hay memoria intermedia disponible, el receptor anuncia un tamaño de ventana distinto a cero para activar de nuevo el flujo de datos.

### 11.3. Formato del segmento TCP

La unidad de transferencia entre el software TCP de 2 máquinas se conoce como segmento.
Los segmentos se intercambian para establecer conexiones, transferir datos, enviar acuses de recibo, anunciar los tamaños de las ventanas y para cerrar conexiones.




- **Sequence number (número de secuencia)**
  Identifica la posición de los datos del segmento en el flujo de datos del transmisor.
- **Acknowledgement number (no de acuse de recibo)**
  Identifica el número de bytes que la fuente espera recibir después.
- **Hlen**
  Especifica la longitud del encabezado del segmento. Es necesario porque el campo OPTIONS varía en su longitud dependiendo de las opciones utilizadas.
- **Reservado**
  Reservado para uso futuro

- **Window (ventana)**
  Usado para que TCP informe cuántos datos está dispuesto a aceptar cada vez que envía un segmento. Esto se hace al especificar el tamaño de memoria intermedia en este campo.

- **Code bits**
  Utilizado para determinar el propósito y contenido del segmento.

Los 6 bits indican cómo interpretar otros campos en el encabezado de acuerdo con la tabla:

**Bits del campo CODE en el encabezado TCP**

| Bit (de izquierda a derecha) | Significado si el bit está puesto a 1 |
|---|---|
| URG | El campo de puntero de urgente es válido. |
| ACK | El campo de acuse de recibo es válido. |
| PSH | Este segmento solicita una operación push. |
| RST | Iniciación de la conexión |
| SYN | Sincronizar números de secuencia |
| FIN | El emisor ha llegado al final de su flujo de bytes. |

### 11.3.1. Datos fuera de banda

Algunas veces es importante que el programa en un extremo de la conexión envíe datos fuera de banda, sin esperar a que el programa en el otro extremo de la conexión consuma los bytes que ya están en flujo. Las señales se deben enviar sin esperar a que el programa lea los bytes que ya están en el flujo TCP.
Para lograr esto, el TCP permite que el transmisor especifique los datos como urgentes, dando a entender que se debe notificar su llegada al programa receptor tan pronto como sea posible, sin importar su posición en el flujo. El protocolo específica que cuando se encuentra con datos urgentes, el TCP receptor debe notificar al programa de aplicación, que esté asociado con la conexión, que entre en "modalidad urgente". Después de asimilar todos los datos urgentes, el TCP indica al programa de aplicación que regrese a su posición normal. El mecanismo utilizado para marcar los datos urgentes, cuando se transmiten en un segmento, consiste en un bit de código URG y en un campo URGENT POINTER (PUNTERO DE URGENCIA).
Cuando se activa el bit URG, el indicador urgente especifica la posición dentro del segmento en la que terminan los datos urgentes.

### 11.3.2. Opción de tamaño máximo de segmento

No todos los segmentos que se envían a través de una conexión serán del mismo tamaño. Por ello, ambos extremos necesitan acordar el tamaño máximo de los segmentos que transferirán.
Para esto se utiliza el campo OPTIONS. Este campo es usado por TCP para negociar con el otro extremo las condiciones del intercambio. De esta manera, cada máquina puede especificar el tamaño máximo de segmento (MSS) que está dispuesto a recibir.
Para las computadoras conectadas por redes LAN es especialmente importante escoger un tamaño máximo de segmento que llene los paquetes o no harán un buen uso del ancho de banda.
Si los dos puntos extremos residen en la misma red física, el TCP, por lo general, computará un tamaño máximo de segmento de tal forma que los datagramas IP resultantes correspondan con la MTU de la red.
No hay que olvidar que los segmentos TCP viajan encapsulados dentro de datagramas IP, que a su vez están encapsulados en tramas de red física.

## 11.4 Protocolo UDP

UDP permite agregar un mecanismo con el que se logre distinguir entre muchos destinos dentro de un host. De esta forma, permitiendo que varios programas de aplicación que se ejecutan en una computadora envíen y reciban datagramas en forma independiente.

### 11.4.1. Identificación del destino final

La mayoría de sistemas operativos aceptan el esquema de multitarea, lo que significa que varios programas de aplicación se ejecuten al mismo tiempo. Esto significa que varios programas pueden ejecutarse al mismo tiempo.

Cada programa en ejecución es conocido como un proceso, tarea, programa de aplicación o proceso a nivel de usuario. A estos sistemas se les llama sistemas multitarea. Puede parecer natural decir que un proceso es el destino final de un mensaje. Sin embargo, especificar que un proceso en una máquina particular es el destino final para un datagrama es un poco confuso.

1. Los procesos se crean y destruyen de una manera dinámica. Los transmisores rara vez saben lo suficiente para identificar un proceso en otra máquina.
2. Seria deseable poder reemplazar los procesos que reciben los datagramas sin tener que informar a todos los transmisores.
3. Se necesitan identificar los destinos de las funciones que implantan sin conocer el proceso que implanta la función.

En lugar de pensar en un proceso como destino final, imaginaremos que cada máquina contiene un grupo de puntos abstractos de destino, llamados puertos de protocolos. Cada puerto de protocolo se identifica por medio de un número entero positivo. El sistema operativo local proporciona un mecanismo de interfaz que los procesos utilizan para especificar o accesar un puerto.

La mayoría de los NOS proporcionan un acceso síncrono a los puertos. Desde el punto de vista de un proceso en particular, el acceso síncrono significa que los cómputos se detienen durante una operación de acceso a puerto.

Por ejemplo, si un proceso intenta extraer datos de un puerto antes de que llegue cualquier dato, el sistema operativo detiene temporalmente el proceso hasta que lleguen datos. Luego que sucede esto, el NOS pasa los datos al proceso y lo vuelve a iniciar. Todos los puertos tienen memoria intermedia, para que los datos que llegan antes de que un proceso esté listo para aceptarlos no se pierdan.

Para comunicarse con un puerto externo, un transmisor necesita saber tanto la dirección IP de la máquina de destino como el número de puerto de protocolo del destino dentro de la máquina. Cada mensaje debe llevar el número del puerto de destino de la máquina a la que se envía, así como el número de puerto de origen de la máquina fuente a la que se deben direccionar las respuestas.

### 11.4.2. Características

Dentro del grupo de protocolos TCP/IP, UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina.

Esto es que cada mensaje UDP contiene tanto el número de puerto de destino como el número de puerto de origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que este envíe una respuesta.

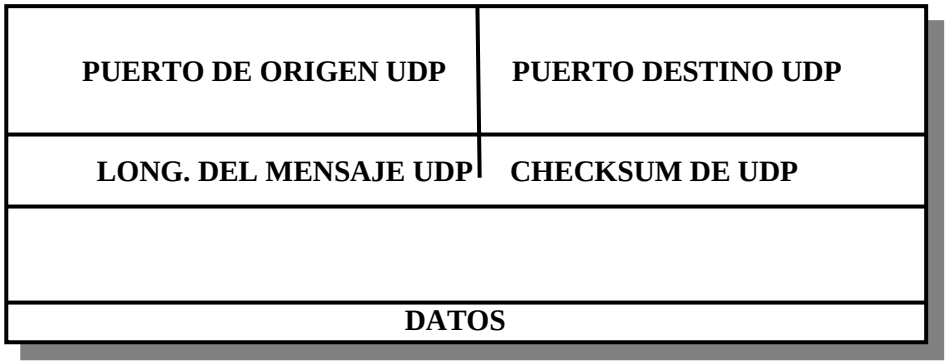
UDP no emplea acuses de recibo para asegurarse de que lleguen mensajes, no ordena los mensajes entrantes ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las máquinas.

Por lo tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. También, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. Un programa de aplicación que utiliza UDP acepta toda la responsabilidad por el manejo de problemas de confiabilidad, incluyendo la pérdida, duplicación y retraso de los mensajes, la entrega fuera de orden y la pérdida de conectividad. Por

esta razón, muchos programas que confían en UDP trabajan bien en un ambiente de red LAN, pero fallan cuando se utilizan en Internet.

### 11.4.3. Formato de mensajes UDP

Un datagrama UDP consta de dos partes: un encabezado UDP y un área de datos UDP. El encabezado se divide en 4 campos de 16 bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación.




- **El puerto de origen**
  Es opcional. Cuando se utiliza, sirve para especificar la parte a la que se deben enviar las respuestas, de lo contrario, puede tener valor de cero.
- **El campo checksum UDP**
  Es opcional y no es necesario utilizarla; un valor de cero en el campo de CHECKSUM significa que la suma no se computó.

### 11.4.4. Encapsulación de UDP

La encapsulación significa que el UDP adjunta un encabezado a los datos que un usuario envía y lo pasa al IP. La capa IP solo es responsable de transferir datos entre un par de hosts dentro de una red de redes, mientras que la capa UDP solamente es responsable de diferenciar entre varias fuentes o destinos dentro de un anfitrión.
Por lo tanto, el encabezado IP identifica a los hosts de origen y destino; solo la capa UDP identifica a los puertos de origen y destino dentro de un host.

# Autoevaluación

1. Explique brevemente el mecanismo de control de flujo mediante el método de la ventana deslizante.

2. Enumere las funciones básicas proporcionadas por la capa de transporte.

3. Brevemente defina lo siguiente:
   - Slow Start
   - Round Trip Time (RTT)

4. Identifique el mecanismo que permite garantizar entregas confiables.

5. Identifique el problema que es solucionado por los algoritmos de Karn y Partridge.

6. ¿Cuáles son las funciones más importantes ejecutadas por TCP?

7. ¿En qué capa del modelo TCP/IP se encuentra TCP?

8. ¿Qué desventaja se encuentra en la técnica de acuse de recibo simple?

9. Brevemente describa en qué consiste la técnica de ventanas deslizables.

10. ¿Cuáles son las principales diferencias entre UDP y TCP?

11. Elabore un diagrama e identifique cada una de las partes del segmento UDP.

12. Defina brevemente el concepto de puertos y sockets.

13. ¿En qué consiste el proceso de encapsulación en UDP?

# Para recordar

- El mecanismo de multiplexamiento consiste en que más de una aplicación pueda utilizar los servicios del protocolo TCP.

- Cuando los números de puerto son concatenados con las direcciones IP de la capa de enrutamiento, conforman lo que se denomina un conector "socket".

- La técnica de desplazamiento de ventana es una técnica de control del flujo impuesta por el receptor de segmentos TCP con el fin de evitar momentos de congestión en el computador receptor.

- El máximo número de segmentos TCP que el transmisor puede enviar en un momento dado es seleccionado por el mínimo valor de la comparación de los parámetros Ventana y Congestión de ventana.

- TCP define el segundo servicio más importante y mejor conocido de nivel de red, la entrega de flujo confiable.
- TCP añade una funcionalidad substancial a los protocolos que ya se han analizado, pero a su vez su implantación es substancialmente más compleja.

- Para lograr que el flujo de transmisión sea eficiente, se hace necesario introducir el concepto de ventana deslizable. Si se analiza la manera cómo se da el mecanismo de transmisión de datos, se verá que los datos solo fluyen entre las máquinas en una dirección a la vez, inclusive si la red tiene capacidad para comunicación simultánea en ambas direcciones. Esto demuestra que la red tiene periodos ociosos durante el tiempo en que las máquinas retrasan sus respuestas.

- Al igual que el UDP, el TCP utiliza números de puerto de protocolo para identificar el destino final dentro de una máquina. Sin embargo, los puertos TCP son mucho más complejos, ya que un número de puerto no corresponde a un solo objeto.

- El TCP visualiza el flujo de datos como una secuencia de bytes que divide en segmentos para su transmisión.

- Generalmente, cada segmento viaja a través de una red como un solo datagrama IP.

SEMANA

12

# Protocolos de ruteo

## TEMA

Protocolos de ruteo

## OBJETIVOS ESPECÍFICOS

- Comprender las técnicas de encaminamiento basadas en RIP
- Identificar las características del ruteo estático y dinámico
- Comprender las técnicas de encaminamiento basadas en OSPF

## CONTENIDOS

- Protocolo RIP
- Problemas que pueden existir con RIP
- Protocolo OSPF

## ACTIVIDADES

- Identifican las características del protocolo RIP y del OSPF.

## 12. PROTOCOLO RIP

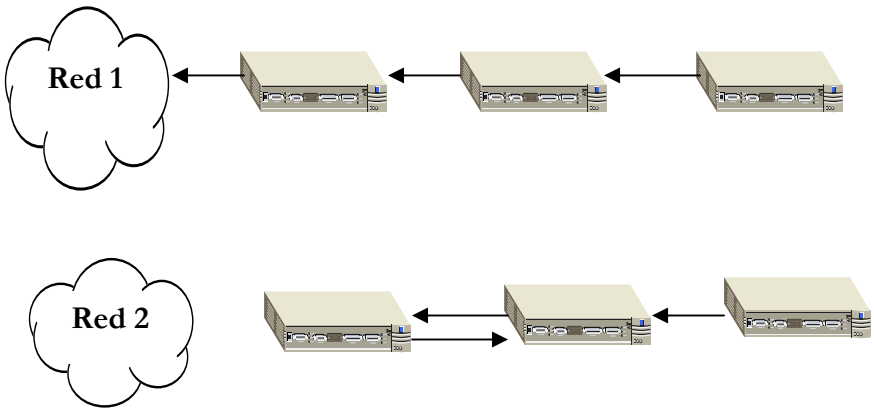
Uno de los protocolos más ampliamente utilizados es el Protocolo de Información de Ruteo (RIP,Routing Information Protocol), también conocido con el nombre de un programa que lo implementa, **routed.** El routed fue originalmente diseñado en la Universidad de Berkeley, en California, para proporcionar información consistente de ruteo y accesibilidad entre las máquinas de su red local.
Tomando como base a las primeras investigaciones de enlaces de redes realizadas en la corporación Xerox en el centro de investigación de Palo Alto (PARC), el routed implementa un protocolo derivado del protocolo derivado del Protocolo de Información de ruteo NS de Xerox. La popularidad de RIP, como un IGP, no se debe a sus méritos técnicos; al contrario es el resultado de que Berkeley distribuyó el software routed junto con su popular sistema 4BSD de Unix. Una vez instalado y corriendo se convirtió en la base del ruteo local y varios grupos de investigadores lo adaptaron para redes amplias.
Un dato sorprendente es que RIP fue construido y adoptado antes de que se escribiera un estándar formal. El protocolo RIP es consecuencia directa de la implantación del ruteo de vector distancia para redes locales. En principio, divide las máquinas participantes en activas y pasivas.

- Los ruteadores activos anuncian sus rutas a los otros.
- Los ruteadores pasivos listan y actualizan sus rutas con base a estos anuncios, pero no anuncian.

Solo un ruteador puede correr RIP de modo activo; los hosts deben utilizar el modo pasivo. Un ruteador que corre RIP de modo activo difunde un mensaje cada **30 segundos**. Cada mensaje consta de un par de datos, donde cada par contiene una dirección de red IP y un entero que representa la distancia hacia esa red.
RIP utiliza una métrica de **conteo de saltos (hop count metric) para medir la distancia hacia un destino.** En la métrica RIP, un ruteador define un salto desde la red conectada directamente, dos saltos desde la red que está al alcance a través de otro ruteador, y así sucesivamente. Usar el conteo de saltos para calcular la trayectoria más corta no siempre produce resultados óptimos. Muchas implantaciones RIP permiten que los administradores configuren artificialmente los contadores de saltos con valores altos cuando deban anunciar conexiones hacia redes lentas. RIP especifica unas cuantas reglas para mejorar el desempeño y la confiabilidad. Una vez que un ruteador aprende una ruta desde otro ruteador, debe conservar esta ruta hasta que aprenda otra mejor.

## 12.1 Problemas asociados a RIP

### 12.1.1 Problema de la cuenta infinita




**R**1 tiene una conexión directa hacia la red 1, de esta forma se tiene una ruta en su tabla con la distancia 1. Este incluye la ruta en sus difusiones periódicas. El ruteador R2 ha aprendido la ruta desde R1, instala la ruta en su tabla de ruteo y anuncia la ruta con una distancia igual a 2. Finalmente, R3 ha aprendido la ruta de R2 y la anuncia con una distancia 3.

Supóngase que la conexión de R1 hacia la red 1 falla. R1 actualizará su tabla de ruteo inmediatamente para hacer la distancia igual a 16(infinita). En la siguiente difusión, R1 reportará el alto costo de la ruta.

Sin embargo, a menos que el protocolo incluya mecanismos extra para prevenirlo, cualquier otro ruteador podría difundir sus rutas antes que R1.

En particular, supóngase que R2 logra anunciar sus rutas justo después de que la conexión de R1 falló. Si esto sucede, R1 recibirá los mensajes de R2 y seguirá el algoritmo usual de vector-distancia. Este notará que R2 ha anunciado una ruta hacia la red 1 a un costo bajo, calculando que ahora se encuentra a 3 saltos para alcanzar la red 1(2 para que R2 alcance la red 1, más 1 para alcanzar R2) e instalará una nueva ruta a través de R2.

En este punto, si R1 o R2 reciben un datagrama destinado para la red 1, rutearán el datagrama de regreso y así, sucesivamente, hasta que su tiempo de vida límite se cumpla.

En el siguiente ciclo de intercambio de ruteo, R1 difundirá sus tablas de rutas completas. Cuando R2 aprenda que las rutas de R1 hacia la Red 1tienen una longitud a 3, esta calculará una nueva longitud para tal ruta, haciéndola igual a 4.

Este problema es posible resolverlo mediante una técnica conocida como ***actualización de horizonte separado*** **(split horizon update).**

Cuando se utilizan horizontes separados, un ruteador registra la interfaz por la que ha recibido una ruta particular y no difunde esta información acerca de la ruta de regreso sobre la misma interfaz. En este caso, el ruteador R2 anunciará su ruta de longitud 2 hacia la red 1 de regreso hacia el ruteador R1, así, si R1 pierde su conexión hacia la red 1, podrá detener el anuncio de la ruta.

### 12.1.2. Técnica Hold Down

Esta técnica obliga a los ruteadores participantes a ignorar información acerca de una red durante un periodo de tiempo fijo luego de la recepción de un mensaje que afirma que la red es inaccesible. Generalmente, el periodo hold down se establece en 60 segundos. La idea es esperar lo suficiente como para asegurar que todas las máquinas reciban las malas noticias y no acepten un mensaje erróneo que esté fuera de fecha.

## 12.2. FORMATO DEL MENSAJE RIP

Los mensajes RIP pueden ser clasificados en dos grupos:
Mensajes de información de ruteo y mensajes utilizados para solicitar información. Ambos se valen del mismo formato:

| Comando | Significado |
|---|---|
| 1 | Solicitud para información parcial o completa de ruteo |
| 2 | Respuesta con distancias de red de pares desde la tabla de ruteo del emisor |

| | | |
|---|---|---|
| COMANDO | VERSIÓN | DEBE ESTAR PUESTO A CERO |
| FAMILIA DE RED1 | | DEBE ESTAR PUESTO A CERO |
| DIRECCIÓN IP DE LA RED1 | | |
| DEBE ESTAR PUESTO A CERO | | |
| DEBE ESTAR PUESTO A CERO | | |
| DISTANCIA HACIA LA RED1 | | |
| FAMILIA DE RED2 | | DEBE ESTAR PUESTO A CERO |
| DIRECCIÓN IP DE LA RED1 | | |
| DEBE ESTAR PUESTO A CERO | | |
| DISTANCIA HACIA LA RED2 | | |
| …….. | | |

Los mensajes RIP no contienen un campo de longitud explícito. De hecho, RIP asume que los mecanismos de entrega subyacentes dirán al receptor la longitud de un mensaje entrante. Los mensajes RIP dependen del UDP para informar al receptor la longitud del mensaje. RIP opera el puerto 520 en UDP.

## 12.3 PROTOCOLO OSPF

Este protocolo fue desarrollado por el IETF a partir del algoritmo SPF. Las características de este protocolo son las siguientes:

- Constituye un estándar abierto, por lo que cualquiera puede implantarlo sin pagar por una licencia de uso. Es el reemplazo de los protocolos abiertos.
- Utiliza un ruteo de tipo de servicio. Esto es que se pueden definir múltiples rutas hacia un destino dado, uno por cada tipo de servicio (retardo bajo o rendimiento alto). El OSPF está entre los primeros protocolos que utiliza esta característica.
- OSPF proporciona balanceo de carga. Esto significa que si existen múltiples rutas hacia un destino dado con el mismo costo, OSPF distribuye el tráfico entre todas las rutas.
- OSPF permite que una localidad divida sus redes y ruteadores en subconjuntos llamados áreas. Cada área es autónoma, el conocimiento de la topología de un área se mantiene oculto para las otras áreas.
- El intercambio de datos entre ruteadores debe ser previamente autenticado. La idea es que solo ruteadores confiables difundan información de ruteo.
- OSPF permite a los ruteadores intercambiar información de ruteo aprendida desde otras localidades (externas).

### 12.3.1. Formato del mensaje OSPF

Todo mensaje OSPF empieza con un encabezado de 24 bytes.

| | | |
|---|---|---|
| VERSIÓN | TIPO | LONGITUD DE MENSAJE |
| DIRECCIÓN IP DEL RUTEADOR FUENTE | | |
| ÁREA ID | | |
| SUMA DE VERIFICACIÓN | | TIPO DE AUTENTICACIÓN |
| AUTENTICACIÓN (bytes 0 – 3) | | |
| AUTENTICACIÓN (bytes 4-7) | | |

El campo VERSIÓN especifica la versión del protocolo.
El campo TYPE identifica el tipo de mensaje según la tabla siguiente:

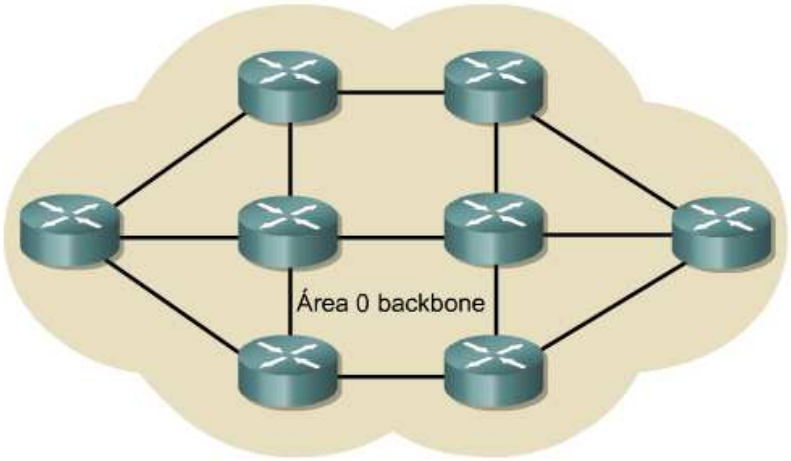
| TIPO | SIGNIFICADO |
|---|---|
| 1 | Hello (para pruebas de accesibilidad) |
| 2 | Descripción de Base de datos (topología) |
| 3 | Solicitud de estado de enlace |
| 4 | Actualización de estado de enlace |
| 5 | Acuse de recibo de estado de enlace |

El campo DIRECCIÓN IP DEL RUTEADOR FUENTE, tiene la dirección del emisor y el campo con el nombre AREA ID tiene un número de identificación de 32 bits para el área.

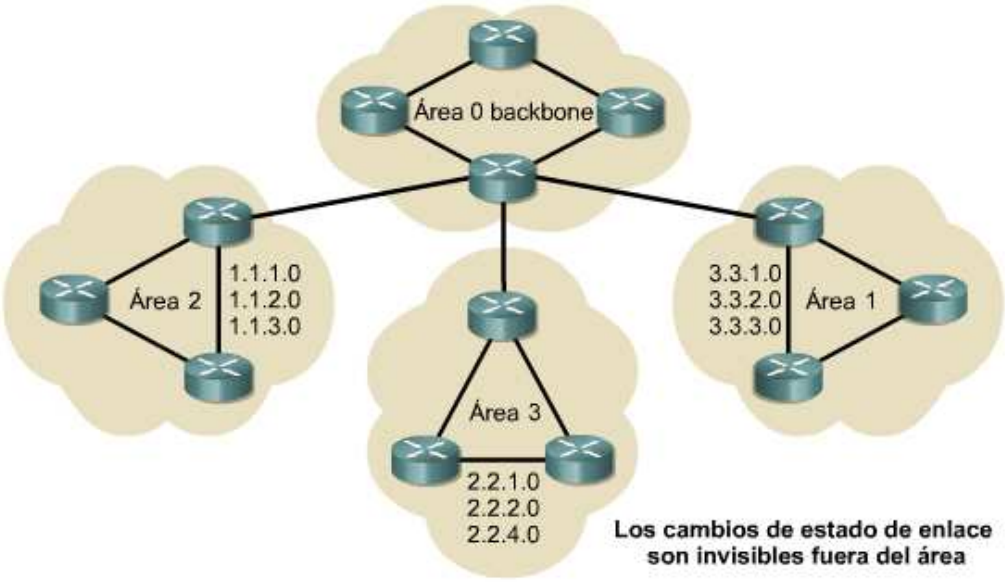
El campo TIPO DE AUTENTICACIÓN especifica qué esquema de autenticación se está utilizando ( 0 significa que no está utilizando ningún esquema de autenticación)

### 12.3.2 Descripción general de OSPF

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. El término "libre" en "Primero la ruta libre más corta" significa que está abierto al público y no es propiedad de ninguna empresa. En comparación con RIP v1 y v2, OSPF es el IGP preferido porque es escalable. Una desventaja de usar OSPF es que solo soporta el conjunto de protocolos TCP/IP.  OSPF se puede usar y configurar en una sola área en las redes pequeñas.

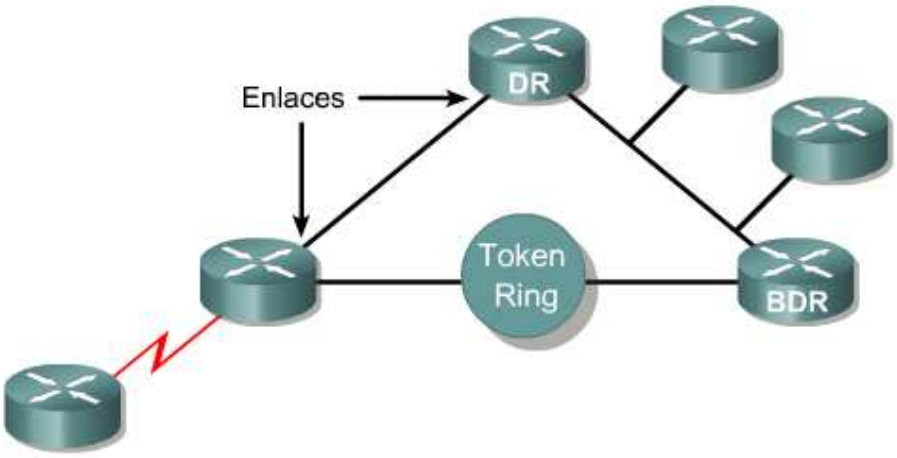



Pero su flexibilidad permite que también se pueda utilizar en las redes grandes. En este caso hacen uso de un diseño jerárquico.
Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento.




### 12.3.3 Terminología de OSPF

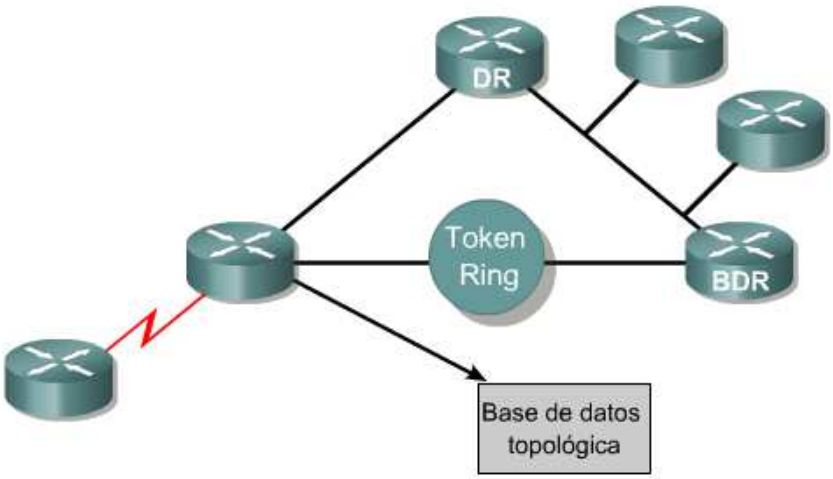
El protocolo OSPF tiene su propia terminología. OSPF reúne la información de los routers vecinos acerca del estado de enlace de cada router OSPF.



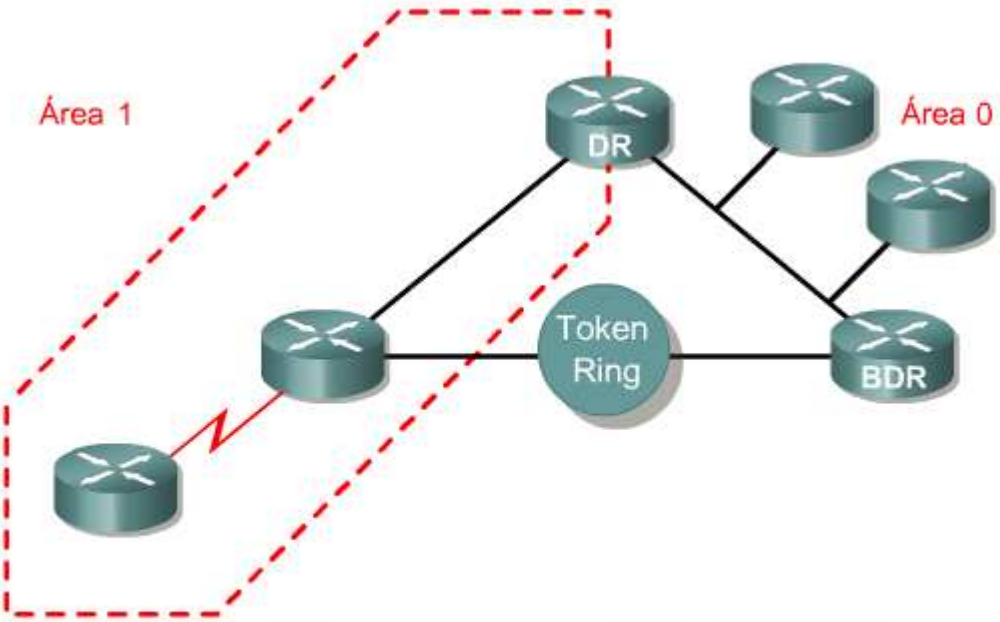

**Enlace** - Una interfaz en un router

**Estado de enlace** - El estado de un enlace entre dos routers. Además, una interfaz de router y su relación con los routers vecinos.

Un router OSPF publica sus propios estados de enlace y, a su vez, envía los estados de enlace recibidos. De esta manera, los routers procesan la información acerca de los estados de enlace y crean una base de datos del estado de enlace. Cada router del área OSPF tendrá la misma base de datos del estado de enlace. Por lo tanto, cada router tiene la misma información sobre el estado del enlace y los vecinos de cada uno de los demás routers.

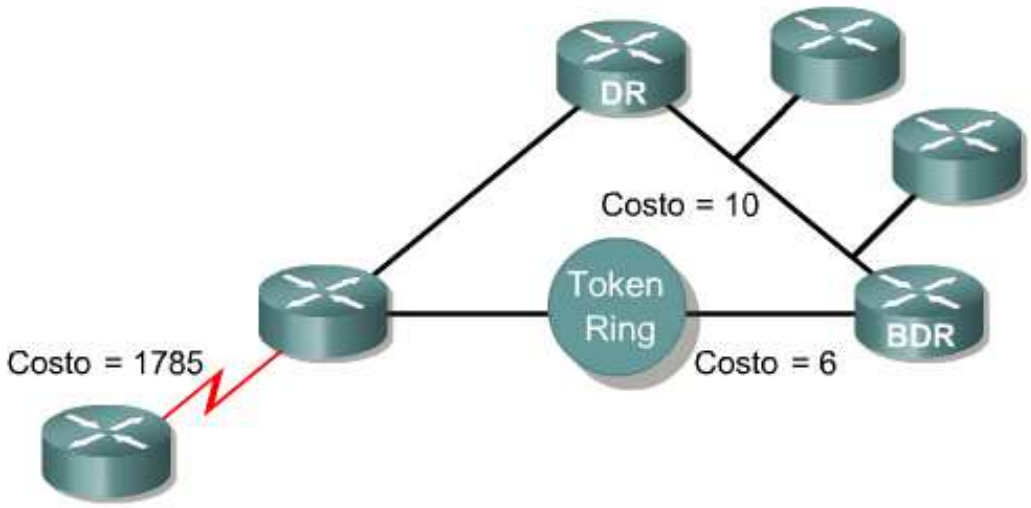



**Base de datos de estado de enlace (o base de datos topológica)** - Una lista de información acerca de todos los demás routers en una internetwork.




**Área** - Una colección de redes y routers que tiene la misma identificación de área. Cada router dentro de un área tiene la misma información de estado de enlace. Un router dentro de un área se denomina router interno.

Cada router luego aplica el algoritmo SPF a su propia copia de la base de datos. Este cálculo determina la mejor ruta hacia un destino. El algoritmo SPF va sumando el costo, un valor que se corresponde generalmente al ancho de banda.




**Costo** - El valor asignado a un enlace. Los protocolos de estado de enlace asignan un costo a un enlace, a base del ancho de banda del enlace o la velocidad de transmisión. Esto se usa en lugar de los saltos.

La ruta de menor costo se agrega a la tabla de enrutamiento, que se conoce también como la base de datos de envío.

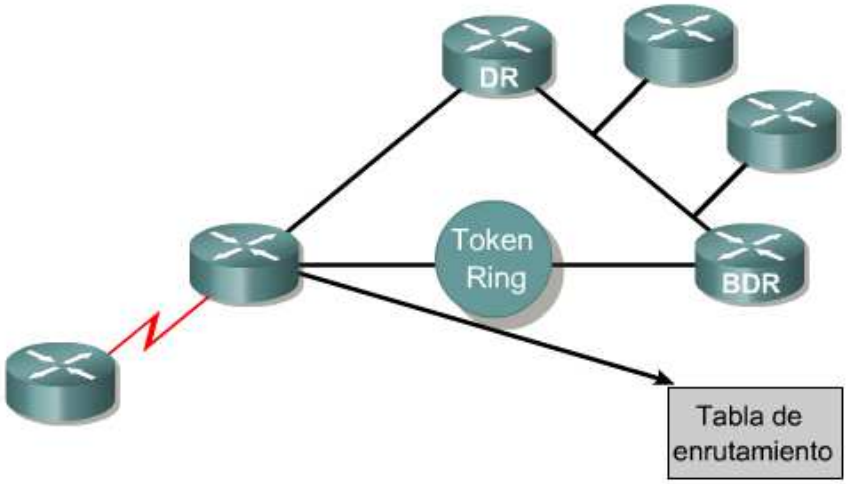
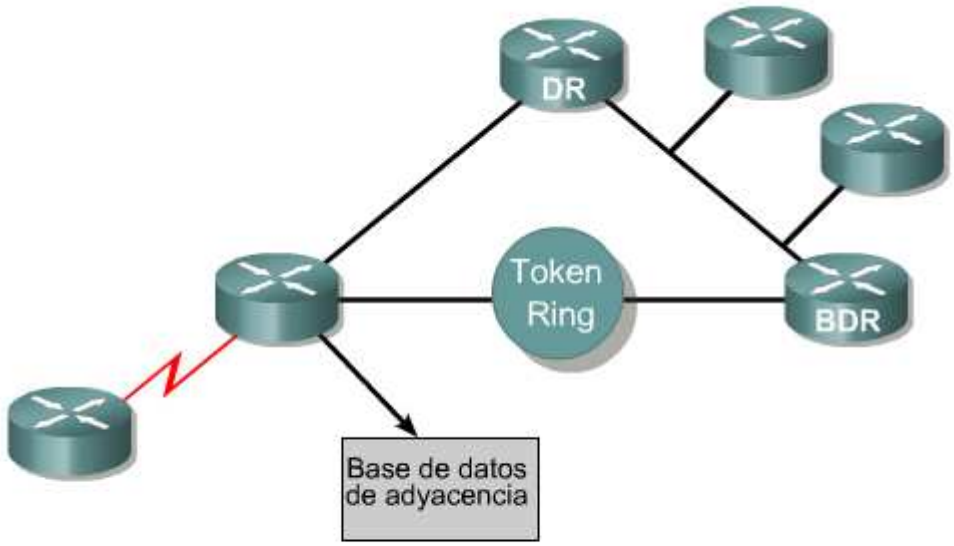


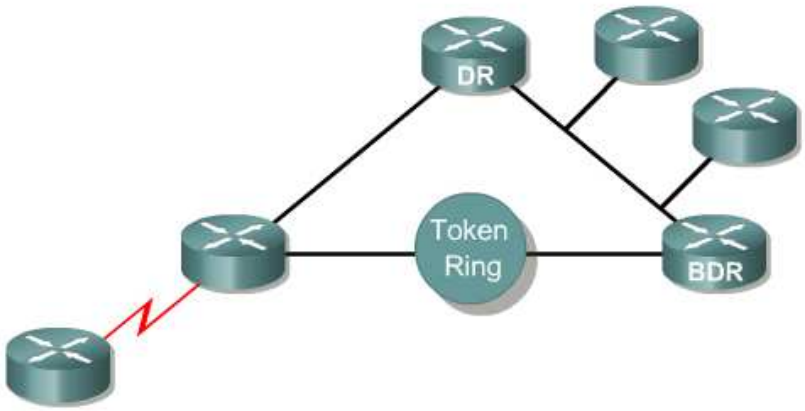

**Tabla de enrutamiento** - También se denomina base de datos de envío. Una tabla de enrutamiento se genera cuando un algoritmo se ejecuta en una base de datos de estado de enlace. La tabla de enrutamiento de cada router es única.

Cada router mantiene una lista de vecinos adyacentes que se conoce como base de datos de adyacencia. La base de datos de adyacencia es una lista de todos los routers vecinos con los que un router ha establecido comunicación bidireccional. Esta base de datos es exclusiva de cada router.




**Base de datos de adyacencia** - Una lista de todos los routers vecinos con los que un router ha establecido comunicación bidireccional. Esto es exclusivo de cada router.

Para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los routers de OSPF seleccionan un router designado (DR) y un router designado de respaldo (BDR), que sirven como puntos de enfoque para el intercambio de información de enrutamiento.

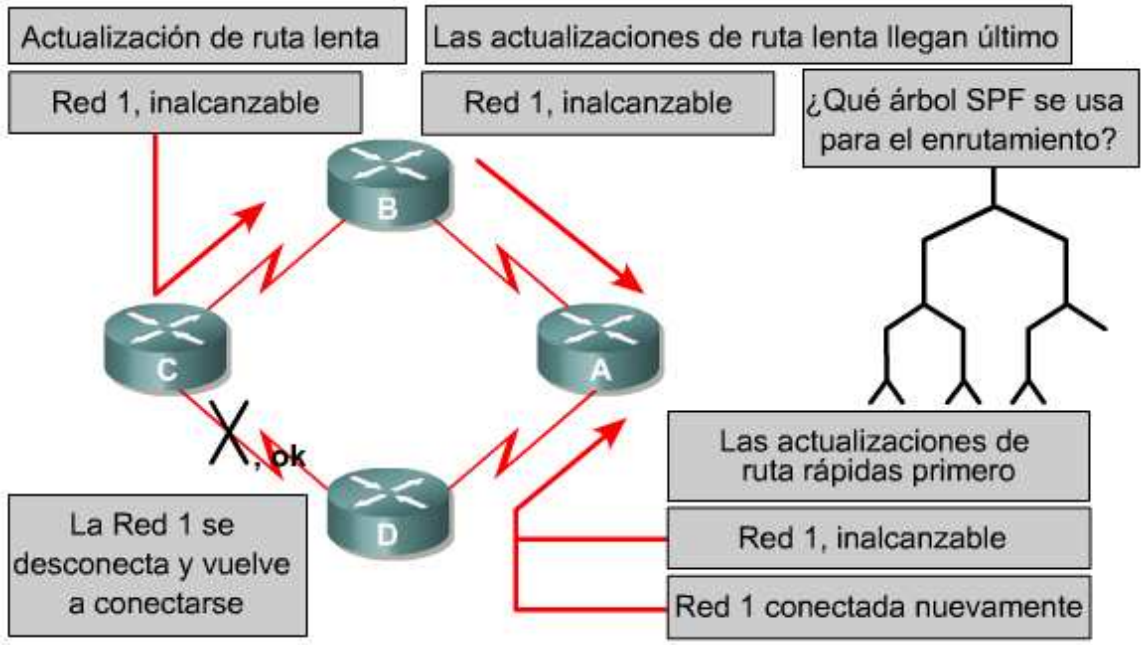



**Router designado (DR) y router designado de respaldo (BDR)** - Un router elegido por todos los demás routers de la misma LAN para representar a todos los routers. Cada red tiene un DR y BDR.

### 12.3.4 Comparación de OSPF con los protocolos de vector-distancia

Los routers de estado de enlace mantienen una imagen común de la red e intercambian información de enlace en el momento de la detección inicial o de efectuar cambios en la red. Los routers de estado de enlace no envían las tablas de enrutamiento en broadcasts periódicos como lo hacen los protocolos de vector-distancia.

Por lo tanto, los routers de estado de enlace utilizan menos ancho de banda para garantizar el mantenimiento de la tabla de enrutamiento.
Así como RIP es adecuado para pequeñas redes y la mejor ruta se basa en el menor número de saltos, OSPF es apropiado para internetworks grandes y escalables, y la mejor ruta se determina sobre la base de la velocidad del enlace.
Los routers que implementan los protocolos de vector-distancia necesitan menos memoria y menos potencia de procesamiento que los que implementan el protocolo OSPF. OSPF selecciona las rutas sobre la base del costo, lo que se relaciona con la velocidad. Cuanto mayor sea la velocidad, menor será el costo del enlace para OSPF. También, selecciona la ruta más rápida y sin bucles del árbol SPF como la mejor ruta de la red. Asimismo, garantiza un enrutamiento sin bucles, mientras que los protocolos de vector-distancia pueden provocar bucles de enrutamiento.




OSPF ofrece soluciones a los siguientes problemas:

- Velocidad de convergencia
- Admite la máscara de subred de longitud variable (VLSM)
- Tamaño de la red
- Selección de ruta
- Agrupación de miembros

Después de la convergencia OSPF inicial, el mantenimiento de un estado convergente es más rápido, porque se inundan a los otros routers del área con los cambios en la red. OSPF admite VLSM y, por lo tanto, se conoce como un protocolo sin clase. RIP v1 no admite VLSM, pero RIP v2 sí la admite. RIP considera inalcanzable a una red que se encuentra a más de 15 routers de distancia, porque el número de saltos se limita a 15. Esto limita el RIP a pequeñas topologías. OSPF no tiene límites de tamaño y es adecuado para las redes intermedias a grandes. RIP selecciona una ruta hacia una red agregando uno al número de saltos informado por un vecino. Compara los números de saltos hacia un destino y selecciona la ruta con la distancia más corta o menos saltos. Este algoritmo es sencillo y no requiere ningún router poderoso ni demasiada memoria, ya que RIP no toma en cuenta el ancho de banda disponible en la determinación de la mejor ruta.

OSPF selecciona la ruta mediante el costo, una métrica basada en el ancho de banda. Todos los routers OSPF deben obtener información acerca de la redes de cada router en su totalidad para calcular la ruta más corta. Éste es un algoritmo complejo. Por lo tanto, OSPF requiere routers más poderosos y más memoria que RIP.
RIP utiliza una topología plana. Los routers de una región RIP intercambian información con todos los routers. OSPF utiliza el concepto de áreas. Una red puede subdividirse en grupos de routers. De esta manera, OSPF puede limitar el tráfico a estas áreas. Los cambios en un área no afectan el rendimiento de otras áreas. Este enfoque jerárquico permite el eficiente crecimiento de una red.

# Autoevaluación

1. Brevemente defina cuál es la característica principal del ruteo dinámico.
2. ¿Cuál es el algoritmo de funcionamiento del protocolo RIP?
3. ¿Qué problemas pueden presentase al trabajar con RIP?
4. Brevemente explique el proceso de autentificación de ruteadores OSPF
5. ¿En qué campo del mensaje OSPF se ve qué esquema de identificación se está utilizando?
6. Brevemente defina un área OSPF.
7. Brevemente enuncie cuatro características de funcionamiento del protocolo OSPF.

# Para recordar

- Con el encaminamiento dinámico, los *routers* automáticamente intercambian los caminos conocidos para ir de una a otra red. Si el camino cambia, los protocolos de *routing* automáticamente actualizan las tablas de rutas e informan a los otros *routers* de estos cambios. En las grandes redes (y en Internet), las tablas de rutas dinámicas juegan un papel importante en las comunicaciones de la red.

- El protocolo RIP (***R****outing* ***I****nformation* ***P****rotocol*) para el IP facilita el intercambio de información de encaminamiento en una red IP. Todos los mensajes RIP se envían bajo el puerto 520 de UPD.

- Cuando existe la caída de un *router*, pueden pasar varios minutos hasta que los cambios se propagan en la red. Esto es conocido como *slow convergence problem* o el problema de la lenta convergencia.

- OSPF permite que una localidad divida sus redes y ruteadores en subconjuntos llamados áreas. Cada área es autónoma. El conocimiento de la topología de un área se mantiene oculto para las otras áreas.

- El intercambio de datos entre ruteadores debe ser previamente autenticado. La idea es que solo ruteadores confiables difundan información de ruteo.

SEMANA

13

# Protocolo BOOTP-DHCP

**TEMA**

Protocolo BOOTP y DHCP

**OBJETIVOS ESPECÍFICOS**

- Conocer el esquema de direccionamiento dinámico
- Identificar las características del protocolo BOOTP y DHCP

**CONTENIDOS**

- Protocolo BOOTP Y DHCP
- BOOTP
- Protocolo DHCP

**ACTIVIDADES**

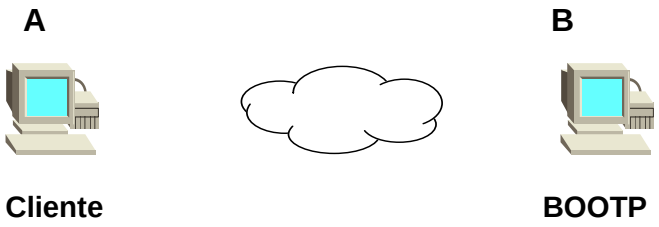
- Realizan la comparación entre un direccionamiento estático y uno dinámico, y resaltan las ventajas de este ultimo caso.

## 13. Protocolo BOOTP Y DHCP

Se sabe que cada computadora conectada a una red TCP/IP requiere de una dirección IP para poder comunicarse. La manera de agenciarse una dirección IP, cuando no se tiene de disco duro, se puede resolver mediante el protocolo RARP; sin embargo esto no es lo mejor, así que existen 2 posibilidades extras que son BOOTP y DHCP. El primero fue utilizado ampliamente, pero actualmente ha sido desplazado por DHCP completamente. Véase cómo trabajan estos protocolos.

### 13.1 BOOTP

(Boot Strap Protocol)
BOOTP utiliza al UDP y al IP. BOOTP debe implantarse como un programa de aplicacion. Al igual que RARP, BOOTP opera dentro de un paradigma cliente-servidor y requiere solo de un intercambio de paquetes. Sin embargo, es mas eficiente que RARP, pues un solo mensaje BOOTP especifica muchos aspectos necesarios para el arranque, incluyendo una dirección IP para la computadora, la dirección de un ruteador y la dirección de un servidor. También, incluye un campo de vendedor específico en la respuesta que permite ingresar información especial como la máscara de subred.
Dado que BOOTP se vale de UDP para transportar mensajes y los mensajes UDP a su vez están encapsulados en los datagramas IP para su entrega, y para que un datagrama IP pueda viajar se requiere que un equipo conozca su dirección IP, resulta todo una paradoja. Sin embargo, la paradoja es solo aparente, pues hay varias direcciones IP de casos especiales. En particular, cuando se usa como una dirección de destino, la dirección IP está formada solo por unos (255.255.255.255), que especifican el límite para la difusión. El software IP puede aceptar y difundir datagramas que especifican la dirección de difusión límite. Por lo tanto, un programa de aplicación puede utilizar la dirección IP de difusión límite para obligar al IP a difundir un datagrama en la red local, antes de que el IP haya descubierto la dirección IP de la red local o la dirección IP de la máquina.



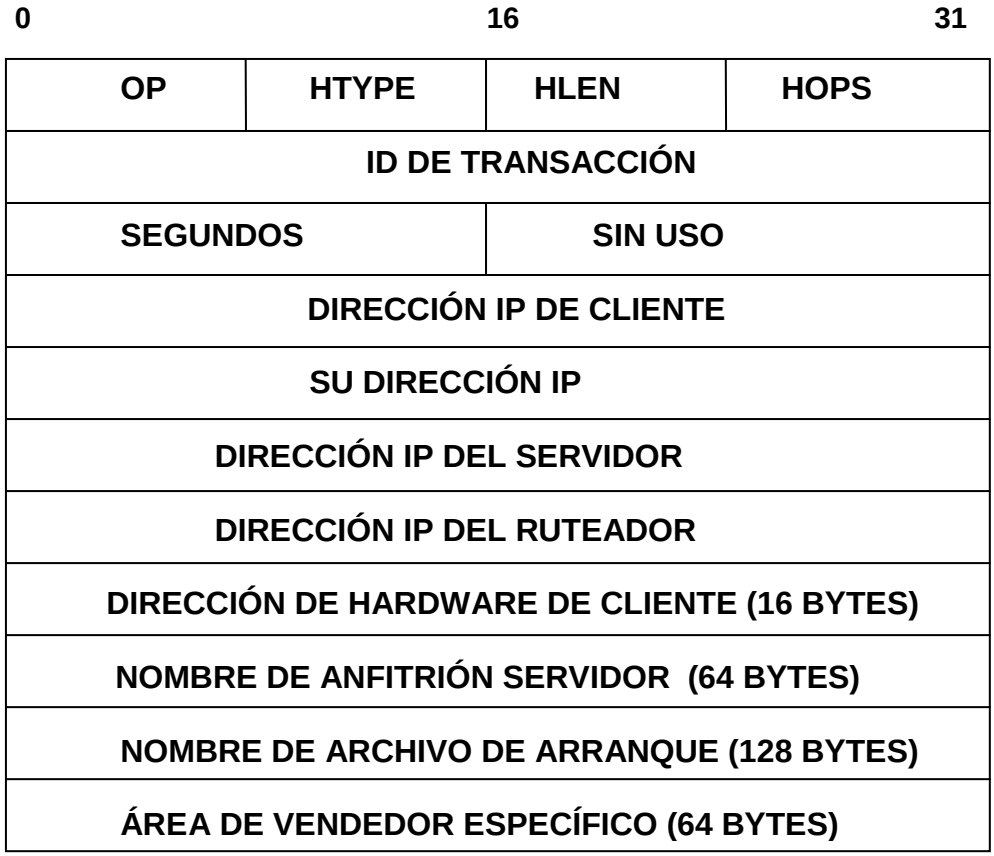

- La máquina A utiliza BOOTP para localizar información de arranque (incluida la dirección IP).
- B es el servidor en la misma red física que responderá a la solicitud.
- A no conoce la dirección IP de B; por lo tanto, debe difundir en su BOOTP inicial la solicitud para utilizar la dirección IP de difusión limite.
- B no envía una réplica directa, sino que utiliza una dirección de difusión límite para su réplica, aunque conoce la dirección IP de A.

### 13.2 Elementos de seguridad usados por BOOTP

Debido a que el BOOTP utiliza UDP y estos a su vez IP, los mensajes pueden retrasarse, perderse, entregarse fuera de orden o duplicarse. Además, debido a que IP no proporciona una suma de verificación, el datagrama UDP puede llegar con bytes alterados. Para contrarrestar, esto BOOTP utiliza sumas de verificación para los datos. Para manejar datagramas perdidos, BOOTP utiliza la técnica convencional de tiempo límite (time out) y retransmisión (retransmission).

Cuando el cliente transmite una solicitud, inicia un temporizador. Si no llega ninguna réplica antes de que el tiempo expire, el cliente debe retransmitir la solicitud.

### 13.3 Formato del mensaje BOOTP




Los mensajes tienen campos de longitud fija y las réplicas poseen el mismo formato que las solicitudes.

- OP : Define si el mensaje es una solicitud (valor 1) o una réplica (valor 2).
- HTYPE: Tipo de hardware de red. Ethernet = 1
- HLEN : Longitud de la dirección de hardware
- HOPS : El cliente coloca HOPS = 0. Si un servidor BOOTP recibe la solicitud y la transfiere hacia otra máquina, incrementa en 1 el valor de HOPS.
- SEGUNDOS: Reporta el número de segundos desde que el cliente comenzó el arranque.
- ID DE TRANSACCIÓN: Contiene un entero que la PC sin disco utiliza para cotejar las respuestas con las solicitudes.
- DIRECCIÓN IP DEL CLIENTE: Será llenada si un cliente conoce su dirección IP.
- NOMBRE DE ANFITRIÓN SERVIDOR
- DIRECCIÓN IP DEL RUTEADOR

- DIRECCIÓN IP DEL SERVIDOR: Si se conoce la dirección de un servidor BOOTP específico así como su nombre, estos dos campos son editados de tal forma que solo se recibirán las direcciones de este servidor.
- SU DIRECCI´ÓN IP : Valor devuelto por el servidor BOOTP
- NOMBRE DE ARCHIVO DE ARRANQUE: Información necesaria para obtener una imagen. Luego, el cliente utiliza otro protocolo (TFTP) para obtener la imagen de memoria.
- ÁREA DE VENDEDOR ESPECÍFICO: Información opcional para su transferencia del servidor al cliente.

### 13.4 INCONVENIENTES:

BOOTP fue diseñado para un ambiente relativamente estático en el que cada anfitrión tiene una conexión de red permanente.
Con la llegada de laptops y redes inalámbricas, es posible cambiar rápidamente la posición de las máquinas. En este contexto BOOTP no se acomoda bien.
No se debe olvidar que el archivo de configuración es creado y actualizado por un administrador; por lo tanto, es de difícil actualización.

### 13.5 Protocolo DHCP

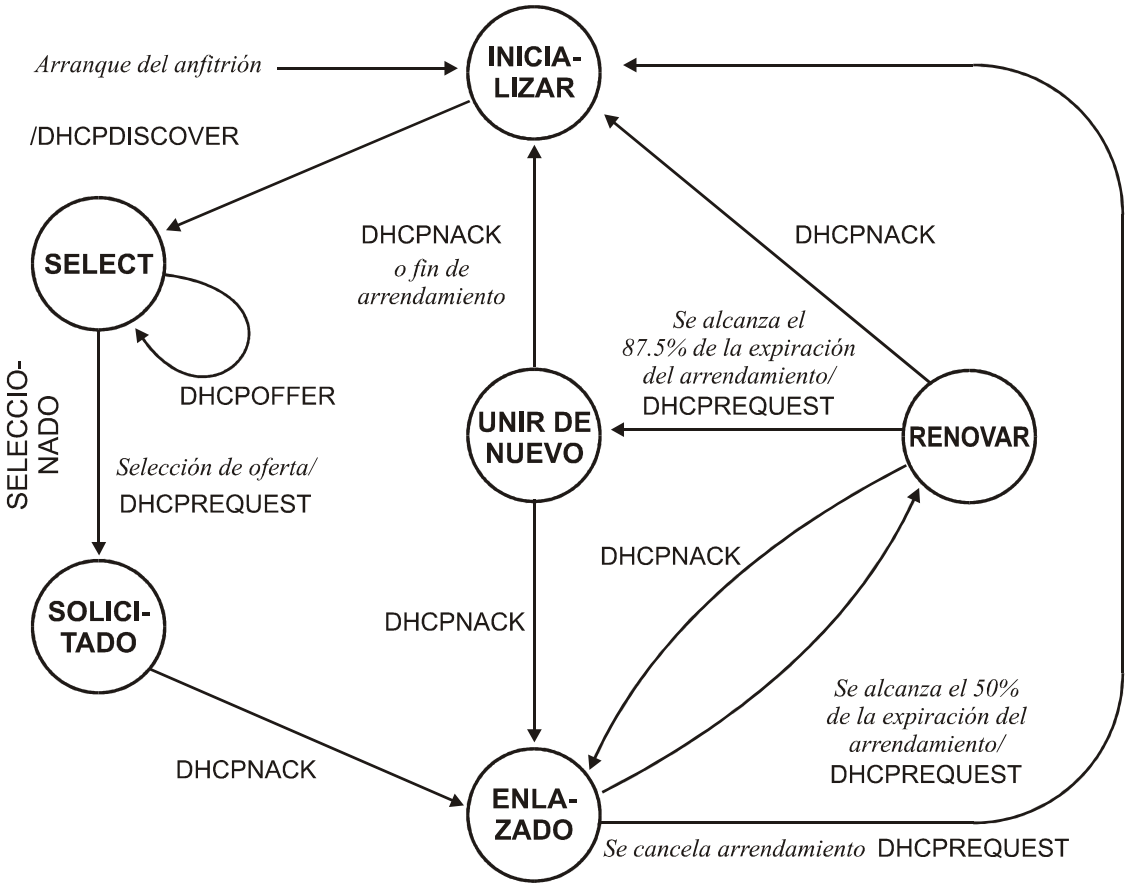
Para solucionar estos problemas, el IETF creó un nuevo protocolo: el DHCP (Protocolo de configuración dinámica de anfitrión).
DHCP es mejor que BOOTP en dos formas:

- El DHCP permite que una computadora adquiera toda la información que necesita en un solo mensaje.
- DHCP permite que una computadora posea una dirección IP en forma rápida y dinámica.

A diferencia de la asignación de direcciones estáticas, que asigna permanentemente cada dirección IP a un host específico, la asignación de direcciones dinámicas es temporal. Se dice que un servidor DHCP arrienda una dirección a un cliente por un periodo de tiempo finito.
El servidor especifica el periodo de arrendamiento cuando asigna la dirección.
Al final del periodo de arrendamiento, sin embargo, el cliente debe renovar el arrendamiento o dejar de usar la dirección.

### PROCESO DE ADQUISICIÓN DE DIRECCIONES

1. Cuando un cliente recién inicia, entra en el estado **INITIALIZE (INICIALIZAR)** para adquirir una dirección IP. Para lograr ello, el cliente difunde un mensaje **DHCPDISCOVER** a toda la red.
2. Al hacer esto, cambia al estado **SELECT**. El mensaje **DHCPDISCOVER** es enviado en un datagrama UDP con puerto **destino 67.**
3. Los servidores que reciben el mensaje responden con un mensaje **DHCPOFFER.**
4. Estando en el modo **SELECT,** el cliente reúne respuestas **DHCPOFFER** desde los servidores DHCP. Cada mensaje contiene información de configuración para el cliente junto con una dirección IP que el servidor ofrece en arrendamiento.




5. El cliente debe seleccionar una de las respuestas y negociar con el servidor un arrendamiento. Para ello, el cliente envía al servidor un mensaje **DHCPREQUEST** y entra al estado **REQUEST**.
6. El servidor responde con un mensaje **DHCPACK.** Esto significa que empieza el arrendamiento por parte del servidor.
7. El cliente pasa al estado **BOUND**, en el cual el cliente procede a utilizar la dirección.

# Autoevaluación

1. Identifique los mensajes utilizados por DHCP para entregar la dirección IP a un host remoto.

2. ¿En qué casos es mejor el protocolo DHCP frente a BOOTP?

3. Identifique las ventajas del protocolo BOOTP frente al protocolo ARP.

4. ¿De qué protocolos se vale UDP para enviar su data?

# Para recordar

- Al igual que RARP, BOOTP opera dentro de un paradigma cliente-servidor y requiere solo de un intercambio de paquetes.

- Un programa de aplicación puede utilizar la dirección IP de difusión limite para obligar al IP a difundir un datagrama en la red local, antes de que el IP haya descubierto la dirección IP de la red local o la dirección IP de la máquina.

- Para manejar datagramas perdidos, BOOTP utiliza la técnica convencional de tiempo límite (time out) y retransmisión (retransmission).

- La asignación de direcciones dinámicas es temporal. Se dice que un servidor DHCP arrienda una dirección a un cliente por un periodo de tiempo finito.

SEMANA

14

# Protocolo Ipv6

**TEMA**

Direccionamiento IPv6

**OBJETIVOS ESPECÍFICOS**

- Conocer el esquema de direccionamiento dinámico
- Identificar las características del protocolo BOOTP y DHCP

**CONTENIDOS**

- Características del Ipv6
- Forma general de un datagrama Ipv6
- Formato del encabezado base del IPV6
- Fragmentación y reensamblaje del IPv6
- Direcciones IPv6

**ACTIVIDADES**

- Hacen uso de la técnica de lluvia de ideas para identificar las características del protocolo IPv6 frente a la versión anterior.

## 14. Protocolo Ipv6

La tecnología básica de IP ha trabajado bien durante una década; sin embargo, existen algunos problemas que están empezando a surgir con el IPV4.

- El agotamiento del espacio de direccionamiento en IPV4 basado en 32 bits
- El creciente interés en utilizar aplicaciones de multimedia
- La posibilidad de mantener comunicación en tiempo real de audio y video

### 14.1 Características del Ipv6

Este protocolo conserva muchas de las características que hicieron al IPv4 un protocolo exitoso. Se tienen dos características:

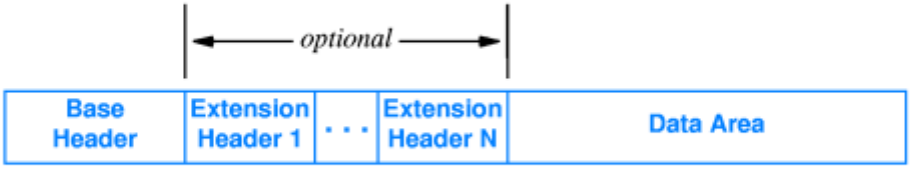
- El IPv6 todavía soporta la entrega sin conexión (cada datagrama puede ser ruteado independientemente).
- También, mantiene sus capacidades de fragmentación y ruteo de fuente.

Los principales cambios pueden organizarse de la siguiente manera:

- **Direcciones más largas :**
  El Ipv6 cuadriplica el tamaño de las direcciones de Ipv4, esto es que va de 32 bits a 128 bits.
- **Formato de encabezados flexible**
  Ipv6 utiliza un formato de datagrama incompatible y completamente nuevo. A diferencia del IPv4 que utiliza un encabezado de datagrama de formato fijo en el que todos los campos excepto las opciones ocupan un número fijo de octetos en un desplazamiento fijo, el Ipv6 utiliza un conjunto de encabezados opcionales.
- **Opciones mejoradas**
  Así como el Ipv4 , el Ipv6 permite que un datagrama incluya información de control opcional.
- **Soporte para asignación de recursos**
  El Ipv6 reemplaza la especificación de tipo de servicio del Ipv4 con un mecanismo que permite la preasignación de recursos de red. Este nuevo mecanismo permite soportar aplicaciones como video en tiempo real que requieren de una garantía de ancho de banda y retardo.
- **Provisión para extensión de protocolo**
  El cambio más significativo del Ipv6 se refiere al hecho de que se cambia de un protocolo que especifica completamente todos los detalles a un protocolo que puede permitir características adicionales. Esta capacidad de extensión tiene la posibilidad de permitir que el IETF se adapte a los protocolos para cambiar al hardware de red subyacente o a nuevas aplicaciones.

14.2. Forma general de un datagrama Ipv6

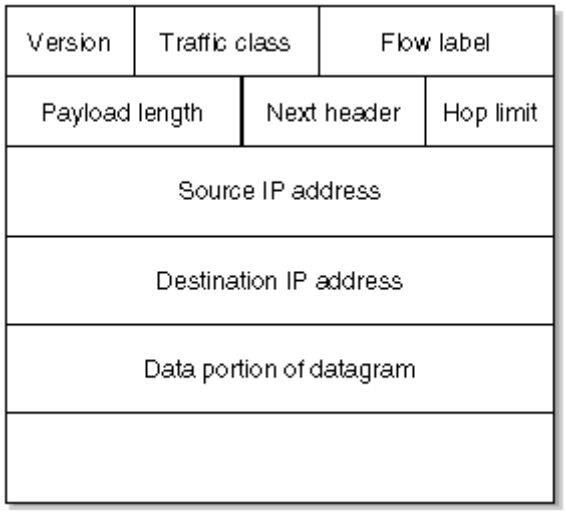
El Ipv6 cambia completamente el formato de un datagrama. Un datagrama Ipv6 tiene un encabezado base de tamaño fijo, seguido por ceros o encabezados de extensión, seguidos a su vez por datos.




## 14.3. Formato del encabezado base del IPV6

El encabezado base Ipv6 contiene menos información que un encabezado de datagrama Ipv4. Las opciones y algunos de los campos fijos que aparecen en un encabezado de datagrama del Ipv4 se han cambiado por encabezados de extensión en Ipv6.

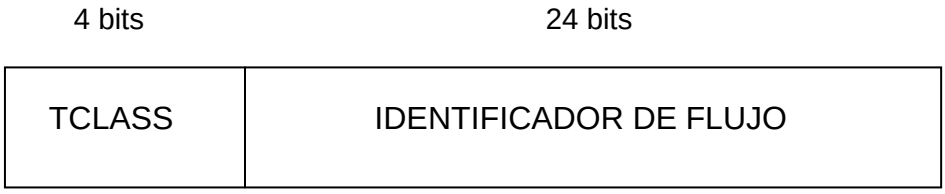
- Los campos de longitud de encabezado se han eliminado y el campo de longitud de datagrama ha sido reemplazado por el campo PAYLOAD LENGTH de 16 bits. Por lo tanto, el tamaño máximo de un datagrama IPv6, incluyendo el encabezado mismo (40 bytes), es de 64Kbytes.
- El tamaño de los campos de dirección origen y destino se ha incrementado a 128 bits.
- La información de fragmentación se ha movido de los campos fijos en el encabezado base, hacia un *encabezado de extensión*.
- El campo TIME-TO-LIVE (LÍMITE DE SALTO) ha sido reemplazado por el HOP LIMIT.
  Este campo es interpretado como el número máximo de saltos que puede dar un datagrama antes de ser desechado.
- El campo SERVICE TYPE ha sido reemplazado por el campo FLOW LABEL (ETIQUETA DE FLUJO).
  El campo FLOW LABEL, en el encabezado base, contiene información que los ruteadores utilizan para asociar un datagrama con una prioridad y un flujo específicos .
- El campo PROTOCOL ha sido reemplazado por un campo que especifica el tipo del próximo encabezado.




Encabezado Ipv6

### 14.3.1 CAMPO FLOW LABEL o ETIQUETA DE FLUJO

El campo está subdividido en dos subcampos:




Este nuevo mecanismo en el Ipv6 soporta reservación de recursos y permite a un ruteador asociar cada datagrama con una asignación de recursos dados. La abstracción subyacente, un flujo, consiste en una trayectoria a través de una red de redes a lo largo de la cual ruteadores intermedios garantizan una calidad de servicio específica. Así dos aplicaciones que necesitan enviar video pueden establecer un flujo en el que el retardo y el ancho de banda estén garantizados.

### 14.3.2 Subcampo TCLASS:

Campo de 4 bits especifica la clase de tráfico para el datagrama.
Los valores del 0 al 7 se emplean para especificar la sensibilidad al tiempo del tráfico controlado por flujo. Los valores del 8 al 15 se utilizan para especificar una prioridad para tráfico que no es de flujo.

### 14.3.3. Subcampo IDENTIFICADOR DE FLUJO:

La fuente selecciona un identificador de flujo cuando establece el flujo.
No hay conflicto potencial entre las computadoras debido a que un ruteador utilice la combinación de direcciones fuente de datagramas e identificadores de flujo cuando asocia un datagrama con un flujo específico.
Por ellos, cada datagrama IP comienza con un encabezado base de 40 bytes que incluye campos para las direcciones de fuente y de destino, el límite máximo de saltos, la etiqueta de flujo y el tipo del próximo encabezado.
Todo datagrama Ipv6 debe, contener por lo menos, 40 bytes además de los datos.

## 14.4 Encabezados de extensión del Ipv6

Para ser totalmente general, el Ipv6 necesita incluir mecanismos para soportar funciones como la **fragmentacion, el ruteo de fuente y la autenticación**. Sin embargo, elegir la asignación de campos fijos en el encabezado de datagrama para todos los mecanismos es ineficiente, pues la mayor parte de los datagramas no utilizan todos los mecanismos. El gran tamaño de las direcciones Ipv6 aumenta la ineficiencia. Un emisor puede elegir qué encabezados de extensión incluir en un datagrama determinado y cuáles omitir. De esta manera, los encabezados de extensión proporcionan una flexibilidad máxima. Los encabezados de extensión Ipv6 funcionan en forma similar a las opciones del Ipv4. Cada datagrama incluye encabezados de extensión solo para los recursos que el datagrama utilice.

## 14.5. Fragmentación y reensamblaje del IPv6

Según el esquema de trabajo de IPv4, se requiere un ruteador intermedio para fragmentar cualquier datagrama que sea demasiado largo para la MTU de la red en la que viaja.
En IPv6, la fragmentación está restringida a la fuente original. Antes de enviar tráfico de información, las fuentes deben implementar una técnica de ***Path MTU Discovery (Descubrir la MTU de la ruta)*** para descubrir la MTU mínima a lo largo de la trayectoria hasta el destino.
Antes de enviar un datagrama, la fuente fragmenta el datagrama de manera que cada fragmento sea menor que el Path MTU. Así, la fragmentación es de extremo a extremo: no son necesarias fragmentaciones adicionales en ruteadores intermedios.
Cuando la fragmentación es necesaria, la fuente inserta un pequeño encabezado de extensión luego del encabezado base en cada fragmento.


Encabezado de extensión de fragmento

### 14.5.1 Características de la fragmentación de IPv6

IPv6 conserva mucho de la fragmentación del IPv4, de manera que cada fragmento debe ser múltiplo de 8 bytes.

- MF : Si presenta 1 bit indica que es el último fragmento.
- IDENTIFICACIÓN DE DATAGRAMA: transporta una ID que el receptor utiliza para el grupo de fragmentos.
- DESPLAZAMIENTO DE FRAGMENTO: Determina el orden adecuado de cada fragmento.

### 14.5.2 Consecuencias de la fragmentación de extremo a extremo

Esta técnica permite reducir la sobrecarga en los ruteadores y deja que cada ruteador maneje más datagramas por unidad de tiempo.
Para poder asimilar las consecuencias de este comportamiento, se debe recordar que el Ipv4 está diseñado para que los ruteadores cambiar en cualquier momento. Si una red o un ruteador falla, el tráfico puede ser redireccionado hacia diferentes trayectorias alternativas. En Ipv6, los ruteadores no pueden cambiar tan fácilmente, pues un cambio en una ruta puede cambiar el Path MTU.Si el Path MTU a lo largo de una nueva ruta es menor que el Path MTU a lo largo de la ruta original, un router intermedio deberá fragmentar el datagrama original. Para resolver este problema, el Ipv6 permite a los ruteadores intermedios hacer un túnel de Ipv6 a través del Ipv6. Cuando un ruteador necesita fragmentar un datagrama, el ruteador no inserta un encabezado de extensión de fragmento ni cambia los campos en el encabezado base.
En lugar de eso, el router crea un datagrama completamente nuevo que encapsula el datagrama original como dato. Luego, divide el nuevo datagrama en fragmentos reproduciendo el encabezado base e insertando un encabezado de extensión de fragmento en cada uno. Luego, el router envía cada uno de los fragmentos hacia el destino final.

## 14.6. Tamaño del espacio de direccionamiento del IPv6

En IPv6, cada dirección ocupa 16 bytes (128 bits), 4 veces el tamaño de una direccion IPv4. Este amplio esquema de direcciones garantiza que el IPv6 pueda tolerar cualquier esquema de asignación de direcciones razonable.
El número total es de 2 ^128 = 3.4 x 10 ^38. Esto significa que si las direcciones se asignaran a razón de un millón de direcciones por milisegundo, tomaría alrededor de 20 años asignar todas las direcciones posibles.

## 14.7. Notación hexadecimal con dos puntos del IPv6

Si bien IPv6 resuelve el problema de tener una capacidad insuficiente, el gran tamaño de direcciones plantea un problema nuevo: los usuarios que administran las redes deben leer, introducir y manipular estas direcciones.
Como se puede ver, la notación binaria no es práctica. La notación decimal tampoco hace las direcciones lo suficientemente compactas.

Por ejemplo si se tiene una dirección en formato decimal:

104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255

y se convierte en el formato hexadecimal con 2 puntos, se obtiene lo siguiente:

68E6:8C64:FFFF:FFFF:0:1180:96A:FFFF

Además, la notación hexadecimal con 2 puntos presenta dos técnicas que la hacen muy útil.

**Primero:**
La notación hexadecimal con 2 puntos permite la ***compresión 0*** que permite que una cadena de ceros repetidos se reemplacen por un par de dos puntos.

Por ejemplo, la dirección:

FA07:0:0:0:0:0:0:A5

Puede escribirse:
**FA07:: A5**
Para asegurar que la compresión cero produce una interpretación sin ambigüedades, la propuesta especifica que puede aplicarse sólo una en cualquier dirección.

**Segundo :**
Esta notación hexadecimal con dos puntos incorpora sufijos decimales con puntos; como se verá, esta combinación tiene el propósito de utilizarse durante la transición del Ipv4 al Ipv6.
Así, la siguiente dirección Ipv4:
128.10.2.1

Se convierte en la siguiente cadena hexadecimal :

0:0:0:0:0:0:128.10.2.1

O también:

**::128.10.2.1**

## 14.8 Direcciones Ipv6

Existen 3 tipos de direcciones Ipv6:

1. **Unicast**
   Identifica una sola interfase dentro del ámbito de las direcciones unicast. Es parecido al esquema actual de direccionamiento.
2. **Multicast**
   Esta dirección identifica múltiples interfaces. Con un adecuado ruteo, los paquetes diseccionados a una dirección multicast son enviados a todas las interfaces que son identificadas mediante la dirección.
3. **Anycast**
   Una dirección multicast identifica múltiples interfaces. Con un adecuado ruteo, los paquetes direccionados a una dirección anycast son enviados a una sola interfase., la más cercana en términos de distancia de ruteo.

**a. Direcciones Unicast**

Un campo de longitud variable denominado **Prefijo de formato, FP (Format Prefix),** permite identificar el tipo de dirección de Ipv6.
Las direcciones unicast pueden ser:

- a.1 Direcciones unicast reservadas
- a.2 Direcciones unicast globales agregables
- a.3 Direcciones unicast de uso local
  - a.3.1 Direcciones de Enlace-local
  - a.3.2 Direcciones de Sitio-local

a.4 Direcciones de compatibilidad

## a.1 Direcciones unicast reservadas

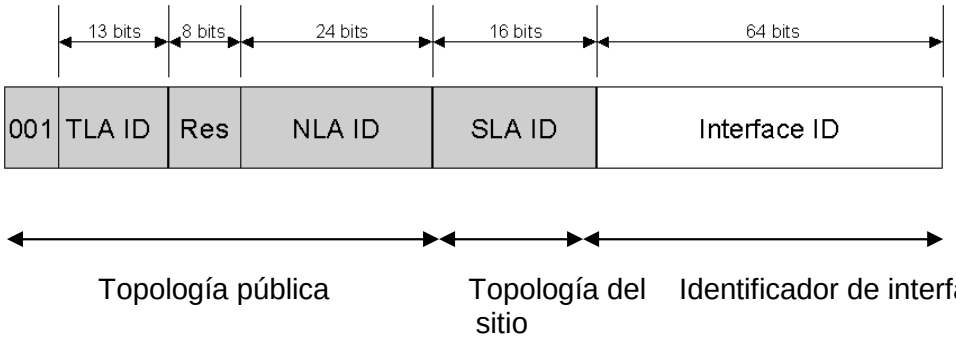
**Dirección no específica:**
La dirección 0:0:0:0:0:0:0:0 o (::) solo es utilizada para indicar la ausencia de una dirección. Normalmente, se usa mientras los nodos inicializan Ipv6 e indica que aún no ha conseguido conocer su propia dirección.

**Dirección de loopback:**
La dirección 0:0:0:0:0:0:0:1 o (::1) es usada para identificar la interfase de lazo cerrado (loopback), permitiendo a un nodo enviar paquetes a sí mismo. Es la equivalente de la dirección 127.0.0.1 de Ipv4.

## a.2 Direcciones unicast globales agregables

Bajo el ruteo entre dominios sin clases, CIDR, los CPI´s asignan direcciones en pools o bloques. Las direcciones unicast globales agregables funcionan de forma similar, y se usarán para la comunicación global en la parte activa con Ipv6.
A diferencia de Ipv4, que actualmente trabaja con una mezcla de direcciones planas y jerárquicas, las direcciones Ipv6 han sido diseñadas desde un inicio para soportar un ruteo eficiente y un direccionamiento jerárquico.
El ámbito en el cual la dirección unicast global agregable Ipv6 es única es en todo el Internet.

**Estructura del datagrama unicast global agregable**




| Abrev. | Campo | Tamaño | Descripción |
|---|---|---|---|
| FP | Prefijo de formato (FP) | 3 bits | "001" : indica que es una dirección unicast global agregable |
| TLA ID | ID de agregación de nivel superior (Top Level aggregation) | 13 bits | Son administrados por la IANA y asignados a los CPI´s. Los ruteadores en el más alto nivel de la jerarquía de ruteo no tienen rutas por defecto, sino solo rutas para un determinado TLA ID. |

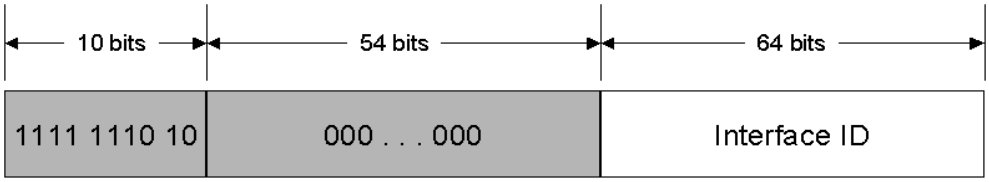
| | | | |
|---|---|---|---|
| Res | Reservado | 8 bits | Para permitir la expansión de los campos TLA y NLA. |
| NLA ID | ID de agregación de siguiente nivel (Next Level aggregation) | 24 bits | Utilizado por las organizaciones que tienen un TLA para crear una jerarquía interna de direccionamiento y permitir a los proveedores de Internet identificar a los sitios que sirven .<br>Cada TLA puede dar servicio a 16 millones de sitios aprox. si se utiliza plano. |
| SLA ID | ID de agregación del nivel del sitio | 16 bits | Permite que las organizaciones creen una estructura interna de enrutamiento independiente de las estructuras externas. |
| ID de interfaz | | 64 bits | Los IDs de interfaz deben ser únicos en el enlace. Permiten identificar a los nodos. |

**a.3 Direcciones unicast de uso local:**

Estas direcciones son de uso local, es decir, se usan para la comunicación dentro del mismo enlace.
Existen dos tipos de direcciones unicast de uso local:

- Direcciones de enlace local (Link-local addresses)
- Direcciones de sitio local (Site-local addresses)

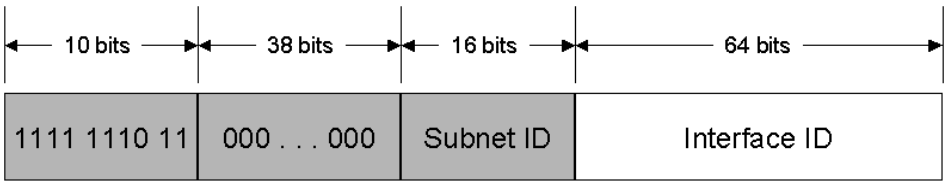
1. **Direcciones de enlace local**
   Usadas entre equipos vecinos en el mismo enlace y para implementar los procesos de Neighbor Discovery .
   Se identifican por presentar un FP : 1111 1110 10, y son usadas por los nodos cuando se comunican con otros nodos en el mismo enlace. En el caso de una red local sin un router, estas direcciones permiten la comunicación entre los equipos del enlace.
   Estas direcciones son equivalentes a las direcciones APIPA (Automatic Private IP Addressing) de Windows que usan el valor 169.254.0.0/16.
   Estas direcciones son utilizadas, también, para el proceso de Neighbor Discovery, que permite encontrar otros nodos en un enlace.




Dirección de enlace local

2. **Direcciones de sitio local**:
   Se identifican por presentar un FP : 1111 1110 11, y son equivalentes a las direcciones IP privadas. Se recomienda su uso en intranets que no tienen una salida hacia Internet a través de un router. Estas direcciones

no pueden ser alcanzadas desde otros sitios. A diferencia de las direcciones de enlace local no se asigna automáticamente, sino que deben ser asignadas manualmente o por un servidor DHCP.

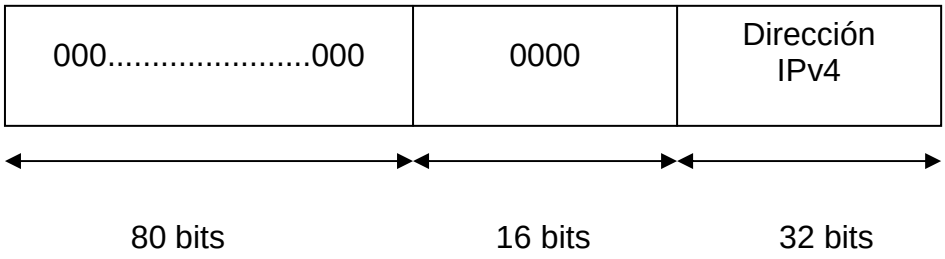



Dirección de sitio local

Los primeros 48 bits están siempre fijados para las direcciones de sitio local. Luego de los 48 bits, sigue un identificador de subset que proporciona 16 bits que se pueden utilizar para crear un esquema de subred en la organización.

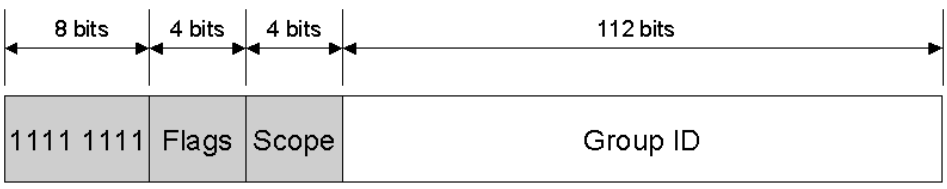
### a.4 Direcciones de compatibilidad

Para facilitar la transición desde IPv4 hasta IPv6, se han desarrollado mecanismos para crear túneles de paquetes de IPv6 sobre una infraestructura de IPv4. Estas direcciones tienen el siguiente formato.




### b. Direcciones Multicast

Definidas en el RFC 2373 y 2375, estas direcciones se usan para el tráfico de IPv6 de multidifusión y sustituyen a las direcciones de difusión en IPv6.
Una dirección de multicast se asigna a un grupo de nodos, pero al contrario que las direcciones *anycast*, todos los configurados con la dirección de multidifusión recibirán los paquetes enviados a dicha dirección.
Un nodo puede pertenecer a más de un grupo de multidifusión.
Ningún nodo puede utilizar una dirección de multidifusión como dirección de origen en ningún paquete ni se puede utilizar en las cabeceras de enrutamiento.

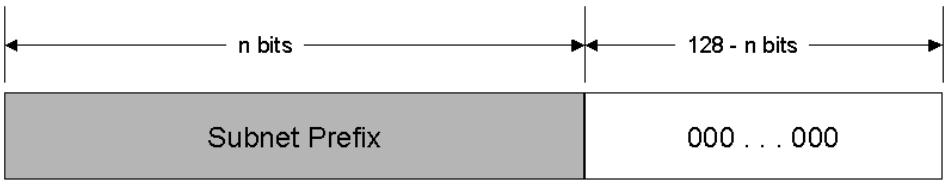



Dirección multicast IPv6

<table>
<tr><th>Abrev.</th><th>Tamaño</th><th>Descripción</th></tr>
<tr><td>FP</td><td>8</td><td>“11111111”<br>dirección de multidifusión</td></tr>
<tr><td>Flags</td><td>4</td><td>Los 3 primeros bits están a CERO.<br>Último Bit :<br>0 → Dirección permanente, asignada por la IANA<br>1 → Dirección Temporal</td></tr>
<tr><td>Ámbito (Scope)</td><td>4</td><td>
<table>
<tr><th>Valor</th><th>Ambito</th></tr>
<tr><td>0</td><td>Reservado</td></tr>
<tr><td>1</td><td>Ámbito de Nodo-local</td></tr>
<tr><td>2</td><td>Ámbito de enlace-local</td></tr>
<tr><td>5</td><td>Ámbito de sitio-local</td></tr>
<tr><td>8</td><td>Ámbito de Organization-local</td></tr>
<tr><td>E</td><td>Ámbito Global</td></tr>
<tr><td>F</td><td>Reservado</td></tr>
</table>
</td></tr>
<tr><td>ID de grupo</td><td>112</td><td>Identificador único para el ID del grupo de multidifusión que aceptará paquetes enviados a esta dirección.</td></tr>
</table>

### c. Direcciones Anycast:

Las direcciones *anycast* son asignadas a múltiples interfaces. Los paquetes enviados a una dirección *anycast* son reenviados por el router a la interfase más cercana.
Para facilitar la entrega, los routers deben estar al tanto de las interfases con direcciones *anycast* y su distancia en términos de métrica de ruteo. Actualmente, las direcciones *anycast* son utilizadas únicamente como direcciones destino y son solo asignadas a los ruteadores.



# Autoevaluación

1. Identifique los distintos tipos de direcciones ipv6. Defina cada una de ellas.

2. Mediante un diagrama, identifique los campos del encabezado base del datagrama ipv6.

3. Numéricamente, calcule la cantidad total de direcciones que es posible generar utilizando direcciones ipv6.

4. Defina la función del campo de encabezado “FRAGMENT OFFSET”.

5. ¿Cuál es la ventaja de trabajar con la técnica del PATH MTU Discovery?

# Para recordar

- El encabezado base Ipv6 contiene menos información que un encabezado de datagrama Ipv4. Las opciones y algunos de los campos fijos que aparecen en un encabezado de datagrama del Ipv4 se han cambiado por encabezados de extensión en Ipv6.

- Cada datagrama IP comienza con un encabezado base de 40 bytes que incluye campos para las direcciones de fuente y de destino, el límite máximo de saltos, la etiqueta de flujo y el tipo del próximo encabezado.

- Para ser totalmente general, el Ipv6 necesita incluir mecanismos para soportar funciones como la **fragmentacion, el ruteo de fuente y la autenticación.**

- En IPv6, la fragmentación está restringida a la fuente original. Antes de enviar tráfico de información, las fuentes deben implementar una técnica de ***Path MTU Discovery (Descubrir la MTU de la ruta)*** para descubrir la MTU mínima a lo largo de la trayectoria hasta el destino.

- En IPv6, cada dirección ocupa 16 bytes (128 bits), 4 veces el tamaño de una dirección IPv4.

SEMANA

15

# Protocolo ICMPv6

## TEMA

Protocolo ICMPv6

## OBJETIVOS ESPECÍFICOS

- Conocer las características nuevas del protocolo ICMPv6
- Identificar los distintos tipos de mensajes ICMPv6

## CONTENIDOS

- Tipos de mensajes ICMPv6:
- Encabezado ICMPv6
- Mensajes de error:
- Mensajes informativos:
- Técnica del Path MTU Discovery

## ACTIVIDADES

- Hacen uso de la técnica de lluvia de ideas para identificar las características del protocolo ICMPv6 frente a la versión anterior.

## 15 Protocolo ICMPv6

Al igual que el protocolo IPV4, Ipv6 tampoco proporciona facilidades para reportar errores. En lugar de ello, Ipv6 utiliza una versión actualizada del Internet Control Message Protocol (ICMP). Icmpv6 cumple las funciones más comunes realizadas por Icmpv4, pero también sirve de base para cumplir las siguientes funciones:

1. **Multicast Listener Discovery (MLD)**
   MLD es un proceso que hace uso de 3 tipos de mensajes ICMP y reemplaza al protocolo IGMPv2 utilizado en IPv4 para administrar la pertenencia a un determinado grupo de multicast.

2. **Neighbor Discovery (ND)**
   ND es un proceso que hace uso de 5 tipos de mensajes ICMP que gestionan la comunicación nodo-a-nodo en un enlace. ND reemplaza al protocolo ARP, ICMPv4 Router Discovery y al mensaje ICMPv4 Redirect.

### 15.1. Tipos de mensajes ICMPv6:

Existen dos grupos de mensajes Icmpv6:

a. Mensajes de error
b. Mensajes informativos

**a. Mensajes de error**

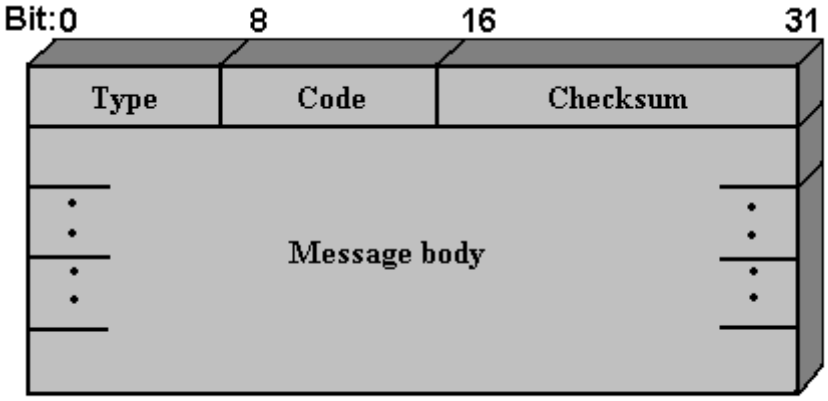
Estos mensajes son usados para reportar errores en la entrega o re-envío de los paquetes IPv6 por parte de nodos destinos o routers intermedios.
El valor del campo TYPE de 8 bits está en el rango de 0 a 127.
Algunos mensajes de error son los siguientes: Destino no alcanzable, Paquete muy grande (Packet too big), Time exceded, etc.

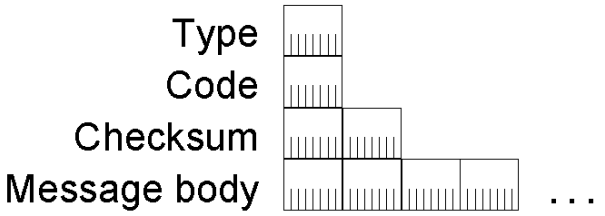
**b. Mensajes informativos :**

Estos mensajes son utilizados para proporcionar funciones de diagnóstico y funciones adicionales del host, tales como MLD y Neighbor Discovery.
Dentro de estos mensajes se encuentran los mensajes de Echo Request y Echo Reply.

### 15.2. Encabezado ICMPv6

Un encabezado ICMPv6 es anunciado a través del valor 58 en el campo Next Header del encabezado previo.




**Encabezado ICMPv6**

| Campo | Descripción |
|---|---|
| Type | Indica el tipo de mensaje ICMPv6. Su tamaño es de 8 bits.<br>El bit de mayor orden es :<br><br>Mensaje de error = 0<br>Mensajes informativos = 1 |
| Code | Permite diferenciar múltiples mensajes dentro de un tipo de mensaje dado.<br>Si solo hay un mensaje para un tipo dado, asume el valor 0. |
| Checksum | Utilizado para la suma de verificación del mensaje ICMPv6. |
| Cuerpo del mensaje | Contiene la data del mensaje ICMPv6. |

## 15.3 Mensajes de error

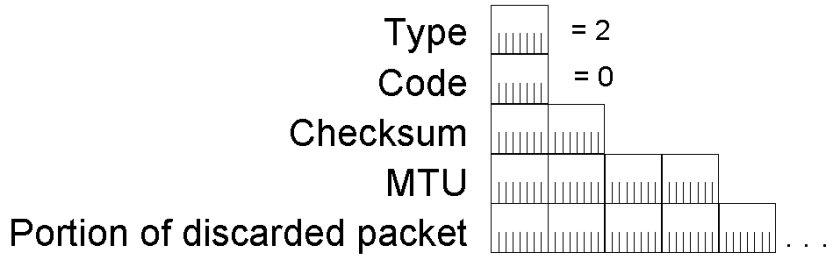
Estos mensajes son usados para reportar errores en la entrega o re-envío de los paquetes IPv6 por parte de nodos destinos o routers intermedios.

Para conservar ancho de banda los mensajes de error no son enviados por cada error encontrado, sino en función a una tasa de envío.

El límite de tasa de envío puede estar basado en un mensaje por determinado número(T) de milisegundos.

### 15.3.1 Mensaje Paquete muy grande (Packet Too big )

Este tipo de mensaje ICMPv6 es enviado cuando el paquete de datos no puede ser re-enviado por un router porque el enlace del router de re-envío tiene un MTU más pequeño que el de los datagramas IPv6.
Este mensaje es el utilizado por el proceso IPv6 Path MTU Discovery.



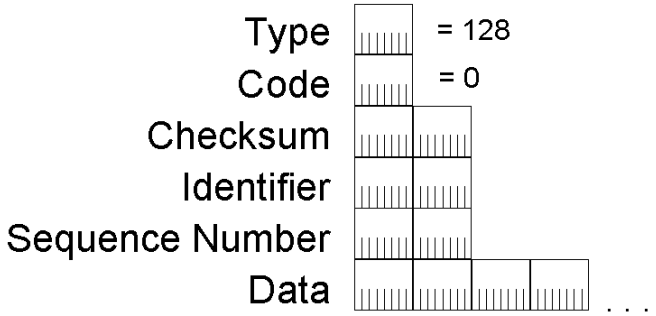

| Campo | Descripción |
|---|---|
| Type | Valor = 2 |
| Code | Código = 0 |
| Checksum | Suma de verificación de error |
| MTU | Almacena el valor de MTU del enlace que no pudo ser re-enviado por ser más pequeño que el paquete original. |
| Portion of discarded packet | Porción del paquete que no pudo ser re-enviado, hasta un tamaño igual a 1280 bytes |

## 15.4 Mensajes informativos

Estos mensajes ICMPv6 proporcionan capacidades de diagnóstico para ayudar a solucionar diversos problemas de interconectividad.

### 15.4.1 Mensaje Echo Request

Estos mensajes son enviados a un destino para solicitar un mensaje de Echo Request inmediato. Los mensajes Echo Request/Echo Reply proporcionan la capacidad de resolver problemas sencillos de accesibilidad y ruteo.



| Campo | Descripción |
|---|---|
| Type | Echo Request → Type = 128<br>Echo Reply → Type = 129 |
| Code | Código = 0 |
| Checksum | Suma de verificación de error |
| Identifier | Permite identificar el mensaje enviado |
| Sequence Number | Proporciona la secuencia de los mensajes enviados. |
| Data | Normalmente es CERO, o puede almacenar data opcional enviada por el host transmisor. |

## 15.5 Técnica del Path MTU Discovery

El PATH MTU es la ruta con el MTU más pequeño de todas las posibles rutas entre un equipo origen y otro destino.
Para descubrir el PATH MTU, el equipo transmisor utiliza los mensajes ICMPv6 Packet Too Big.

# Autoevaluación

1. Defina brevemente en qué consisten los mensajes informativos de tipo ICMPv6.

2. Describa el proceso denominado Path MTU Discovery.

3. Describa brevemente el mensaje de tipo Packet Too Big e identifique para qué se le utiliza.

4. Identifique para qué se utilizan los mensajes Echo Request.

# Para recordar

- Neighbor Discovery es el proceso que hace uso de 5 tipos de mensajes ICMP y que permiten gestionar la comunicación nodo-a-nodo en un enlace. Esta técnica reemplaza al protocolo ARP en su integridad, y los mensajes ICMPv4 Router Discovery y al mensaje ICMPv4 Redirect.

- Los mensajes de error ICMP son usados para reportar errores en la entrega o re-envío de los paquetes IPv6 por parte de nodos destinos o routers intermedios. Para conservar más convenientemente el ancho de banda los mensajes de error, no son enviados por cada error encontrado, sino en función a una tasa de envío.

- La técnica denominada PATH MTU es la ruta con el MTU más pequeño de todas las posibles rutas entre un equipo origen y otro destino. Esta técnica minimiza la cantidad de fragmentaciones intermedias realizadas por los routers que se encuentran en la trayectoria de los paquetes.

SEMANA

16

# Seguridad en IPv6

**TEMA**

Seguridad en IPv6

**OBJETIVOS ESPECÍFICOS**

- Conocer las características de seguridad del protocolo IPv6
- Identificar los componentes del IPSec

**CONTENIDOS**

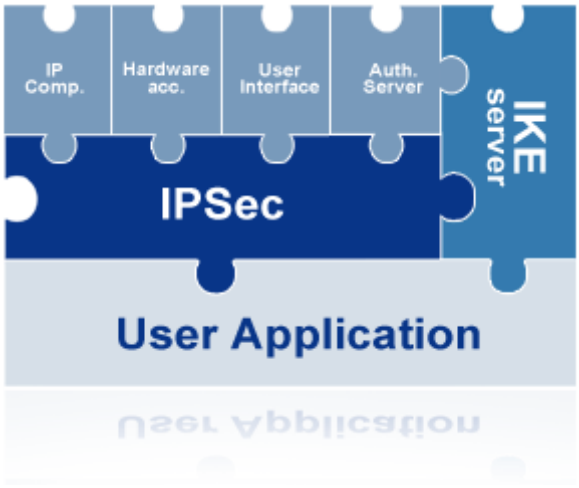
- Seguridad en IPv6
- Cabecera de Autenticación (AH)
- Estructura de un encabezado AH
- Encabezado ESP

**ACTIVIDADES**

- Hacen uso de la técnica de lluvia de ideas para identificar las características de seguridad del protocolo IPv6.

## 16 Seguridad en Ipv6

La necesidad de utilizar actualmente Internet para realizar transacciones comerciales, ha hecho que se tengan que desarrollar una serie de protocolos de seguridad que permitan garantizar la autenticación de la información transmitida, así como la integridad de los mismos. Estas características no contempladas en Ipv4 han tenido que ser implementadas a través de protocolos adicionales; sin embargo, en el caso de IPv6, estos esquemas están contemplados e integrados mediante el uso de cabeceras de extensión.
IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a Ipv4. La arquitectura IPsec se describe en el RFC2401. Los siguientes párrafos dan una pequeña introducción a IPsec.
IPsec (la abreviatura de Internet Protocol security) es una extensión al protocolo IP que añade cifrado fuerte para permitir servicios de autenticación y, de esta manera, asegurar las comunicaciones a través de dicho protocolo. Inicialmente, fue desarrollado para usarse con el nuevo estándar Ipv6, aunque posteriormente se adaptó a Ipv4.




IPsec actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes en la comunidad IPsec. No está ligado a ningún algoritmo de cifrado o autenticación, tecnología de claves o algoritmos de seguridad específico. Es más, IPsec es un marco de estándares que permite que cualquier nuevo algoritmo sea introducido sin necesitar de cambiar los estándares. También, está formado por un conjunto de protocolos de cifrado para asegurar flujos de paquetes de datos e intercambiar claves de la siguiente forma:

- Encapsulating Security Payload (ESP), que provee autenticación, confidencialidad de datos e integridad del mensaje
- Authentication Header (AH), que provee de autenticación e integridad de datos, pero no de confidencialidad.

Debido a ello existen dos cabeceras de extensión muy importantes:

- La cabecera AH o Encabezado de Autenticación (Authentication header)
- La cabecera ESP o Encapsulamiento de seguridad de carga útil (Encapsulating Security Payload)

## 16.1. Cabecera de Autenticación (AH)

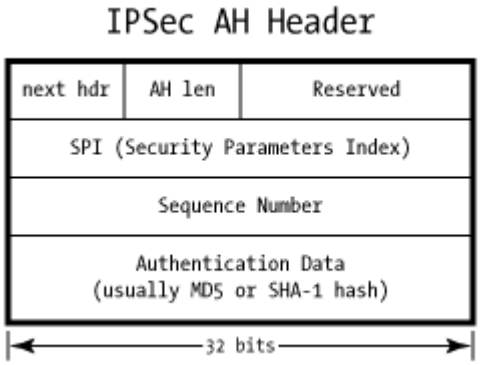
Este encabezado se encarga de garantizar la integridad y autenticación de los datagramas IPv6. Esto significa que proporciona un medio al equipo receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados durante el tránsito. Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos podrían ser vistos por terceros. La cabecera de Autenticación es identificada por el valor 51 en la cabecera Next Header, del encabezado previo.

El funcionamiento de AH se basa en el uso de un código de autenticación de mensajes. Este algoritmo consiste en aplicar una ***función hash*** a la combinación de unos datos de entrada junto con una clave o llave AH, siendo el resultado una pequeña cadena de caracteres a la que se le denomina extracto. Este extracto deviene en una huella digital asociada a los datos y al equipo que lo ha generado. Este extracto del mensaje original se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete.

Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en el tránsito y que procede efectivamente del equipo origen esperado.

Al analizar el mecanismo de funcionamiento del encabezado AH se puede concluir que su seguridad reside en el hecho de que el cálculo del extracto es imposible sin conocer la clave (llave), y que dicha llave solo la conocen el emisor y el receptor.

## 16.2. Estructura de un encabezado AH



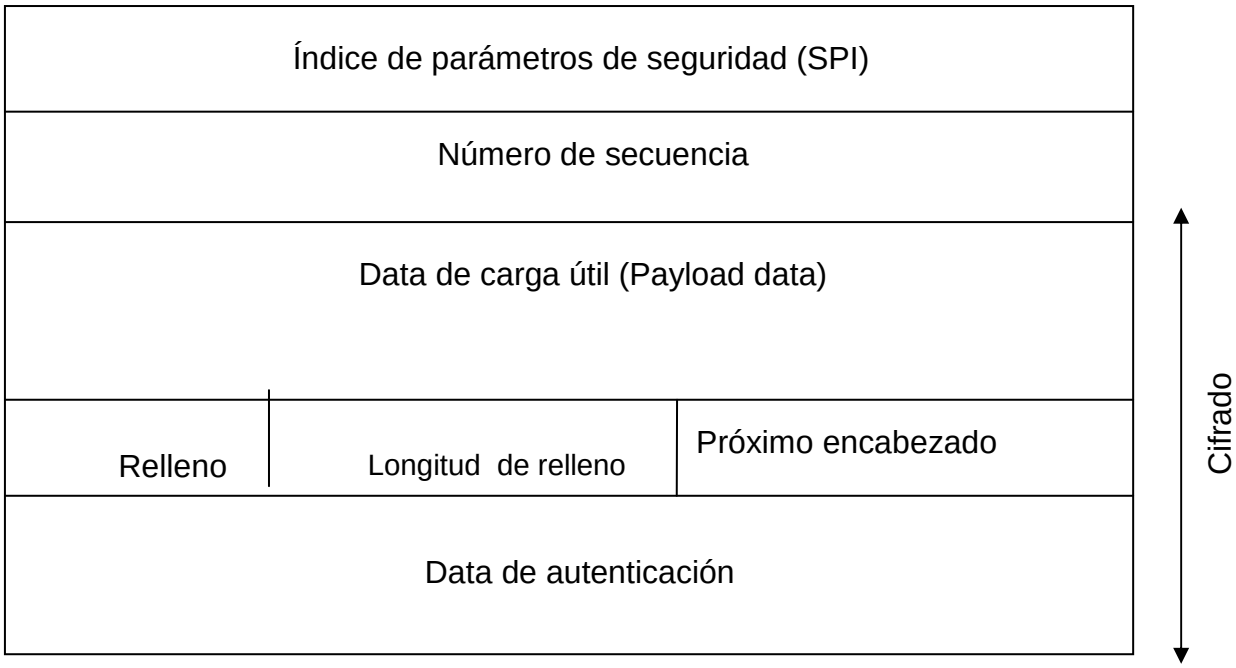

1. Próximo encabezado :
   Valor que identifica el encabezado siguiente
2. Longitud de carga útil:
   Tamaño de la cabecera de extensión
3. Índice de parámetros de seguridad:
   Campo que identifica una asociación especifica de seguridad
4. Número de secuencia:
   Proporciona la protección contra re-envíos innecesarios
5. Campo de autenticación :

Contiene un valor de chequeo de integridad o ICV (extracto). Este valor permite garantizar la autenticación y la integridad de los datos.

El encabezado de autenticación (AH) solo proporciona autenticación e integridad de la data, y no confidencialidad de la data enviada. Para lograr lo último, se requiere que el encabezado AH se use en asociación con el encabezado ESP.

### 16.3. Encabezado ESP

Este encabezado de extensión proporciona confidencialidad de la data transmitida, autenticación y servicios de integridad de la totalidad de la data encapsulada en el datagrama IPv6.
El encabezado ESP es identificado por el valor 50 en el campo Próximo encabezado del encabezado previo.




1. Índice de parámetros de seguridad (SPI):
   Este campo permite identificar el IPSec o algoritmo criptográfico.

2. Número de secuencia:
   Campo para proporcionar la secuencia de los datagramas cifrados

3. Data de carga útil:
   La información real que se desea enviar. Este campo presenta agregados los campos Relleno, Longitud de Relleno y Próximo Encabezado.

4. Data de autenticación :
   Proporciona la data que permitirá garantizar la confidencialidad de la información transmitida.

   Para ocultar aún más la información enviada se agregan caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, dificultar aún más la posibilidad de la desencriptación de la información.

# Autoevaluación

1. Identifique las características de funcionamiento del algoritmo hashing.
2. Identifique los campos del mensaje AH.
3. Enumere las diferencias entre el protocolo AH y ESP.
4. Brevemente describa las características importantes del protocolo IPSec.

# Para recordar

- El funcionamiento de AH se basa en el uso de un código de autenticación de mensajes. Este algoritmo consiste en aplicar una ***función hash*** a la combinación de unos datos de entrada junto con una clave o llave AH, de ahí que el resultado sea una pequeña cadena de caracteres a la que se le denomina extracto.

- El encabezado de autenticación ( AH) solo proporciona autenticación e integridad de la data, y no confidencialidad de la data enviada. Para lograr lo último, se requiere que el encabezado AH se use en asociación con el encabezado ESP.

- Este encabezado se encarga de garantizar la integridad y autenticación de los datagramas Ipv6. Esto significa que proporciona un medio al equipo receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados durante el tránsito.