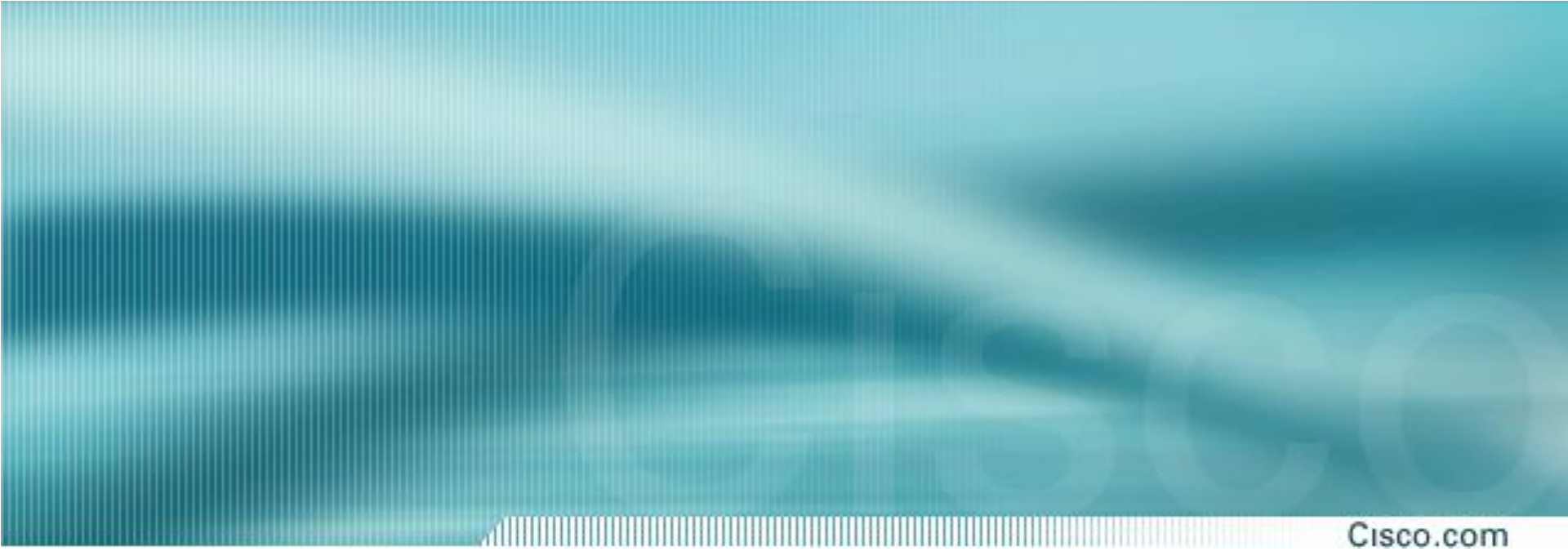


CCNA 1 v3.0 Módulo 9 Suite de Protocolos TCP/IP y Direccionamiento IP

Prof: Mg Robert Antonio, Romero Flores

Objetivos

- **Los estudiantes que completen este módulo deberán poder:**
- **Explicar por qué se desarrolló la Internet y cómo el TCP/IP se ajusta al diseño de la misma.**
- **Nombrar las cuatro capas del modelo TCP/IP.**
- **Describir las funciones de cada capa del modelo TCP/IP.**
- **Comparar el modelo OSI con el TCP/IP.**
- **Describir la función y la estructura de las direcciones IP.**
- **Comprender por qué es necesaria la división en subredes.**
- **Explicar la diferencia entre direccionamiento público y privado.**
- **Comprender la función de las direcciones IP reservadas.**
- **Explicar el uso del direccionamiento estático y dinámico para un dispositivo.**
- **Comprender cómo el direccionamiento dinámico puede realizarse con RARP, BootP y DHCP.**
- **Utilizar ARP para obtener direcciones MAC a fin de poder enviar un paquete a otro dispositivo.**
- **Comprender los problemas relacionados con el direccionamiento entre redes.**

Introducción al TCP/IP

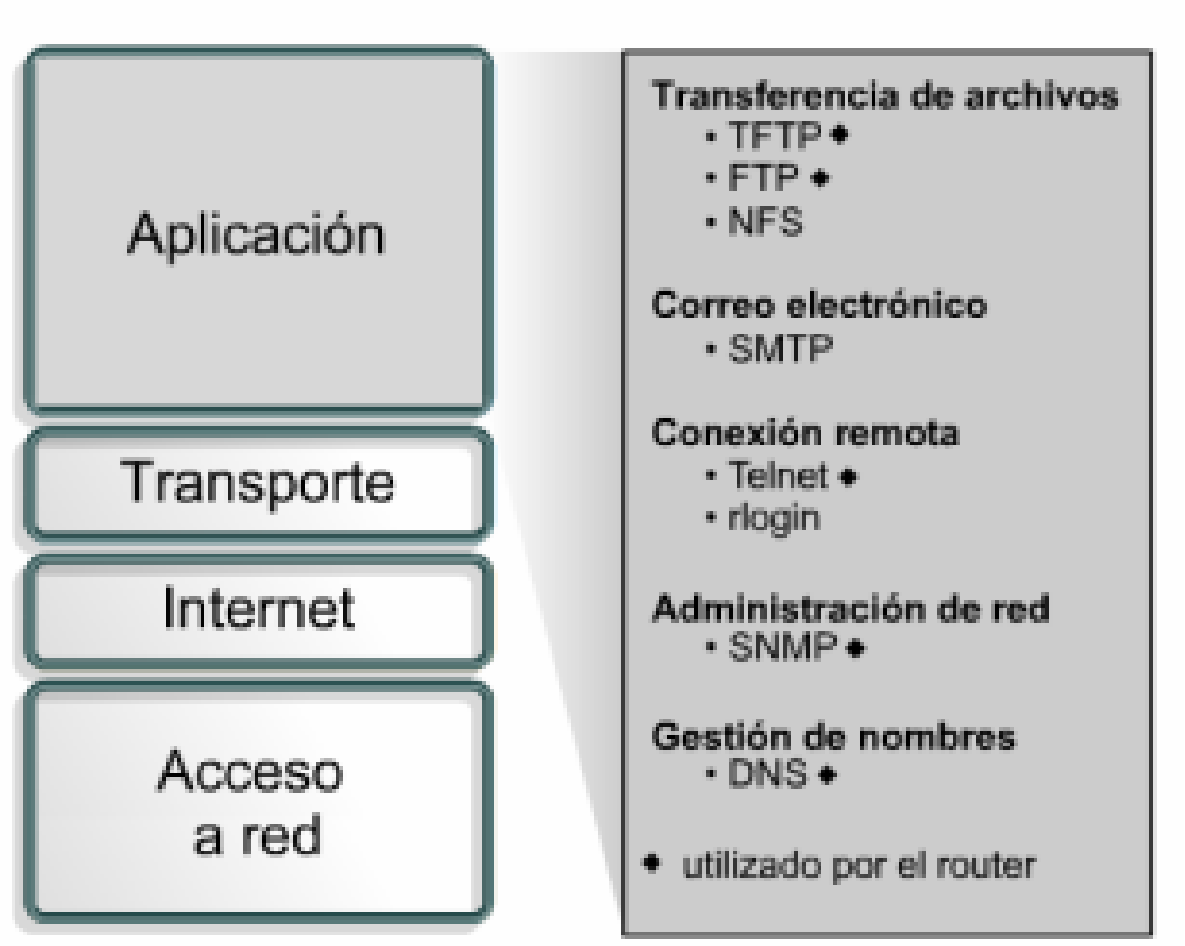
Historia y futuro de TCP/IP

- **El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba una red que pudiera sobrevivir ante cualquier circunstancia. Para tener una mejor idea, imagine un mundo, cruzado por numerosos tendidos de cables, alambres, microondas, fibras ópticas y enlaces satelitales.**
- **Entonces, imagine la necesidad de transmitir datos independientemente del estado de un nodo o red en particular. El DoD requería una transmisión de datos confiable hacia cualquier destino de la red, en cualquier circunstancia. La creación del modelo TCP/IP ayudó a solucionar este difícil problema de diseño.**
- **Desde entonces, TCP/IP se ha convertido en el estándar en el que se basa la Internet..**

La capa de aplicación

- **La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:**

Ejemplos de la Capa de Aplicación



La capa de aplicación

- **Protocolo de transferencia de archivos (FTP): es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.**
- **Protocolo trivial de transferencia de archivos (TFTP): es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP). Los Routers utilizan el TFTP para transferir los archivos de configuración e imágenes IOS de Cisco y para transferir archivos entre los sistemas que admiten TFTP. Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.**
- **Sistema de archivos de red (NFS): es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por Sun Microsystems que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.**
- **Protocolo simple de transferencia de correo (SMTP): administra la transmisión de correo electrónico a través de las redes informáticas. No admite la transmisión de datos que no sea en forma de texto simple.**
- **Emulación de terminal (Telnet): Telnet tiene la capacidad de acceder de forma remota a otro computador. Permite que el usuario se conecte a un host de Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.**
- **Protocolo simple de administración de red (SNMP): es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.**

La capa de aplicación

- **Sistema de denominación de dominio (DNS): es un sistema que se utiliza en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.**

La capa de transporte

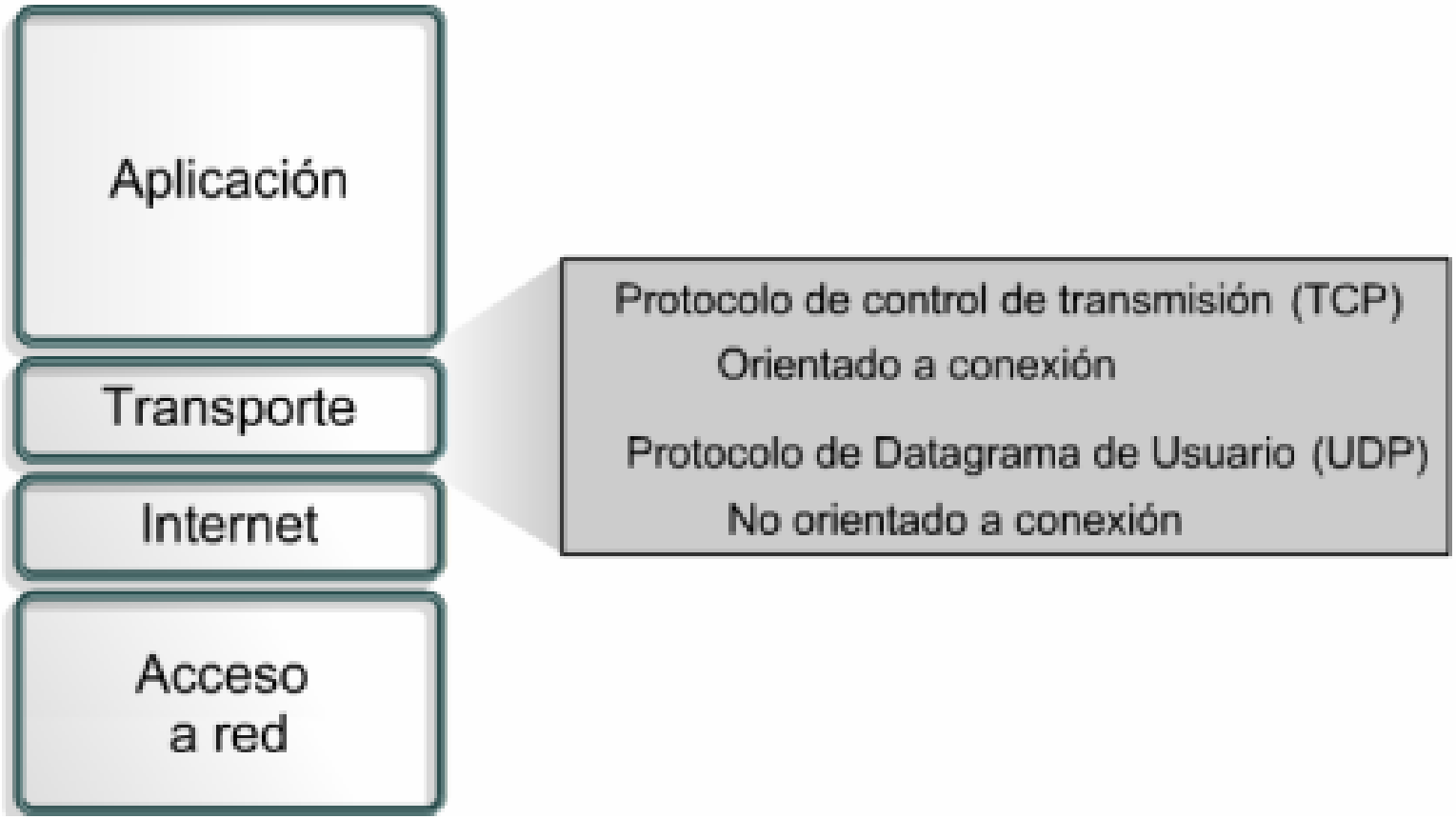
La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. Esta capa forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor.

Los protocolos de transporte segmentan y reensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

Soporta Cinco servicios básicos:

- **Segmentación de datos para la capa superior de aplicación.**
- **Establecer operaciones extremo a extremo.**
- **Enviar segmentos desde un host extremo a otro.**
- **Asegurar la confiabilidad de los datos.**
- **Proveer flujo de control.**

La capa de transporte



TCP y UDP

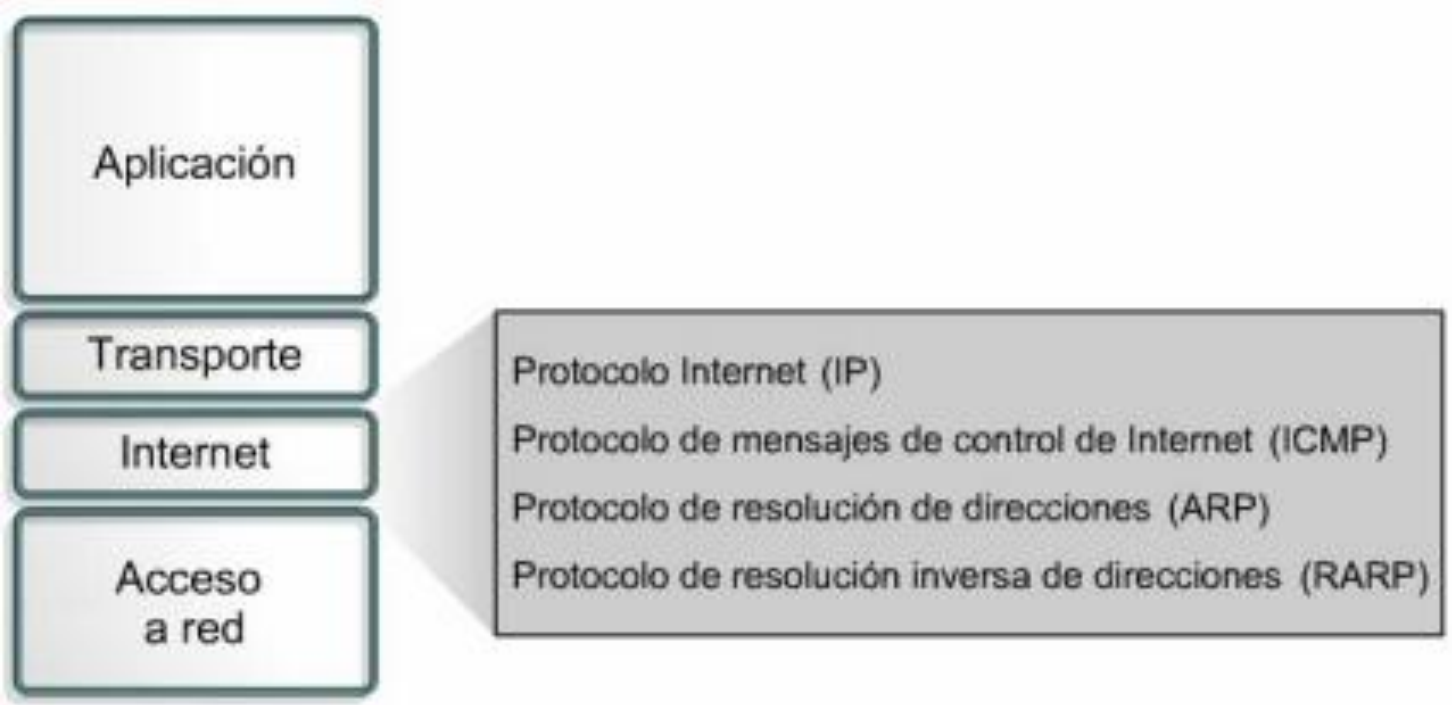
- **Segmentación de los datos de capa superior.**
- **Envío de los segmentos desde un dispositivo en un extremo a otro dispositivo en otro extremo.**

TCP solamente

- **Establecimiento de operaciones de punta a punta.**
- **Control de flujo proporcionado por ventanas deslizantes.**
- **Confiabilidad proporcionada por los números de secuencia y los acuses de recibo.**

La Capa de Internet

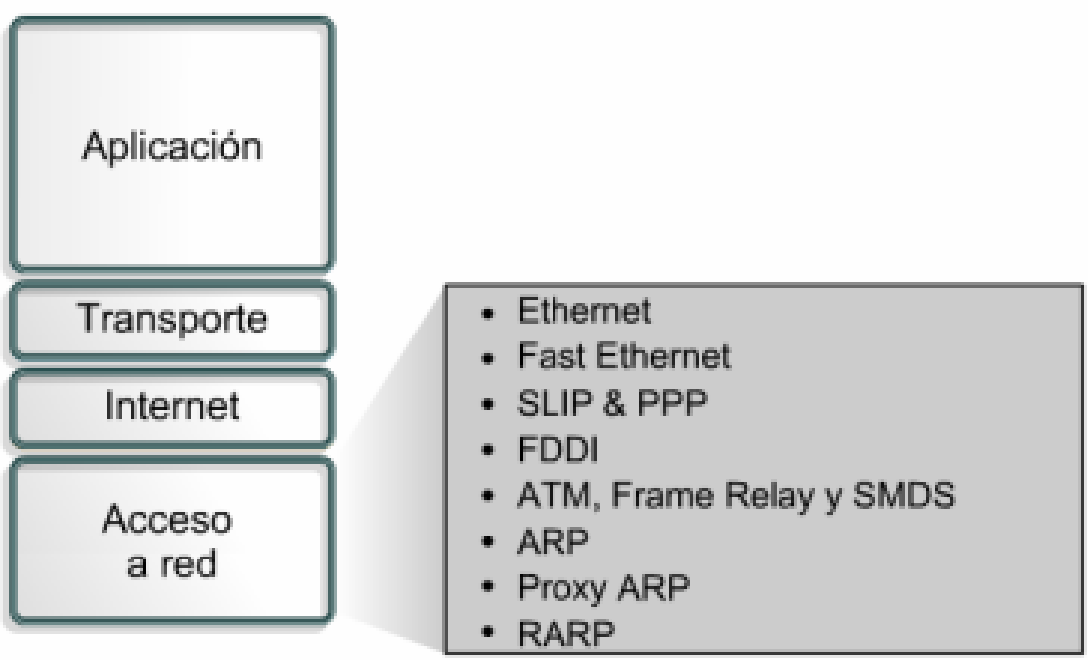
El propósito de la capa de Internet es seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurre en esta capa.



- **Los siguientes protocolos operan en la capa de Internet TCP/IP:**
- **IP proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.**
- **El Protocolo de mensajes de control en Internet (ICMP) suministra capacidades de control y envío de mensajes.**
- **El Protocolo de resolución de direcciones (ARP) determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.**
- **El Protocolo de resolución inversa de direcciones (RARP) determina las direcciones IP cuando se conoce la dirección MAC.**
- **Define un paquete y un esquema de direccionamiento.**
- **Transfiere los datos entre la capa Internet y las capas de acceso de red.**
- **Enruta los paquetes hacia los hosts remotos.**

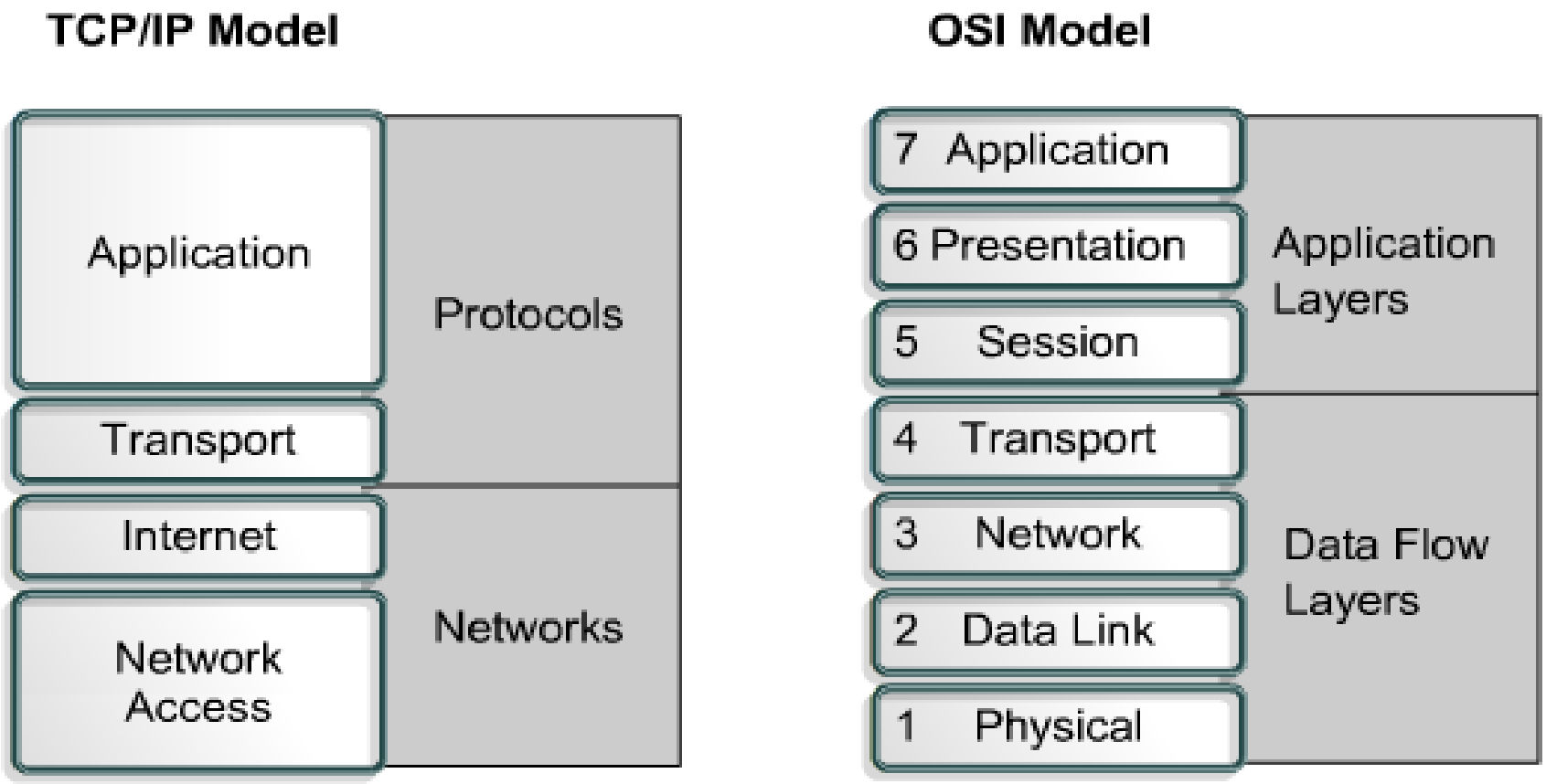
La capa de acceso de red

- **La capa de acceso de red también se denomina capa de host a red. La capa de acceso de red es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas física y de enlace de datos del modelo OSI.**



- **Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem tales como el Protocolo Internet de enlace serial (SLIP) y el Protocolo de punta a punta (PPP) brindan acceso a la red a través de una conexión por módem. Debido a un intrincado juego entre las especificaciones del hardware, el software y los medios de transmisión, existen muchos protocolos que operan en esta capa. Esto puede generar confusión en los usuarios. La mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet del modelo TCP/IP**

Comparación entre el modelo OSI y el TCP/IP



Similarities of the OSI and TCP/IP Models

Similitudes entre los modelos OSI y TCP/IP:

- **Ambos se dividen en capas.**
- **Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.**
- **Ambos tienen capas de transporte y de red similares.**
- **Se supone que la tecnología es de conmutación por paquetes y no de conmutación por circuito.**
- **Los profesionales de networking deben conocer ambos modelos.**

Diferencias entre los modelos OSI y TCP/IP:

- **TCP/IP combina las capas de presentación y de sesión en una capa de aplicación**
- **TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa**
- **TCP/IP parece ser más simple porque tiene menos capas**
- **La capa de transporte TCP/IP que utiliza UDP no siempre garantiza la entrega confiable de los paquetes mientras que la capa de transporte del modelo OSI sí.**

Arquitectura de Internet

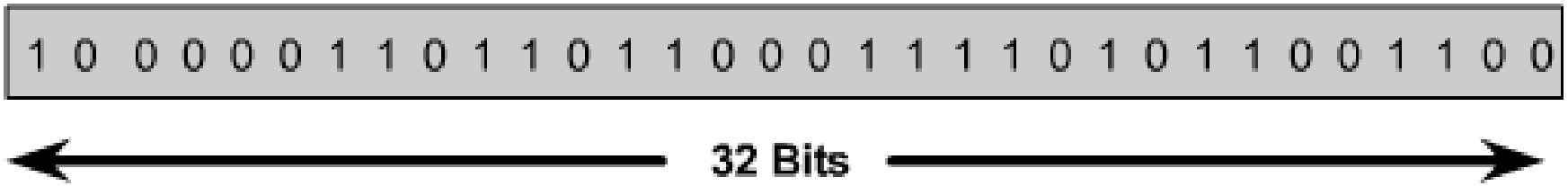
- **Aunque Internet es compleja, existen algunas ideas básicas que rigen su operación. Esta sección examinará la arquitectura básica de la Internet. La Internet es una idea que parece muy sencilla a primera vista, y cuando se repite a gran escala, permite la comunicación casi instantánea de datos por todo el mundo entre cualesquiera personas, en cualquier lugar, en cualquier momento.**
- **Las LAN son redes de menor tamaño que se limitan a un área geográfica. Muchas LAN conectadas entre sí permiten que funcione La Internet. Pero las LAN tienen sus limitaciones de tamaño. Aunque se han producido avances tecnológicos que mejoran la velocidad de las comunicaciones, tales como la Ethernet de 10 Gigabits, de 1 Gigabit y Metro Optical, la distancia sigue siendo un problema.**

- **Internet utiliza el principio de la interconexión en la capa de red. Con el modelo OSI a modo de ejemplo, el objetivo consiste en construir la funcionalidad de la red en módulos independientes. Esto permite que una variedad de tecnologías LAN existan en las Capas 1 y 2 y una variedad de aplicaciones funcionen en las**
- **Capas 5; 6 y 7. El modelo OSI proporciona un mecanismo en el cual se separan los detalles de las capas inferior y superior. Esto permite que los dispositivos intermedios de networking "retransmitan" el tráfico sin tener que molestarse con los detalles de la LAN.**

Dirección de Internet

Direccionamiento IP

- **Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura muestra un número de 32 bits de muestra. Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado. En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios. Por ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria.**



Conversión decimal y binaria

2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Decimal Number	Binary Number
204	11001100
Try New Number	Check Answer

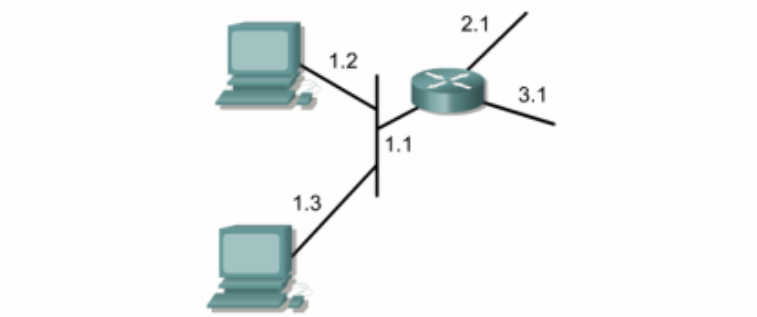
Binary Number	Decimal Number
11110111	247
Try New Number	Check Answer

Direccionamiento IPv4

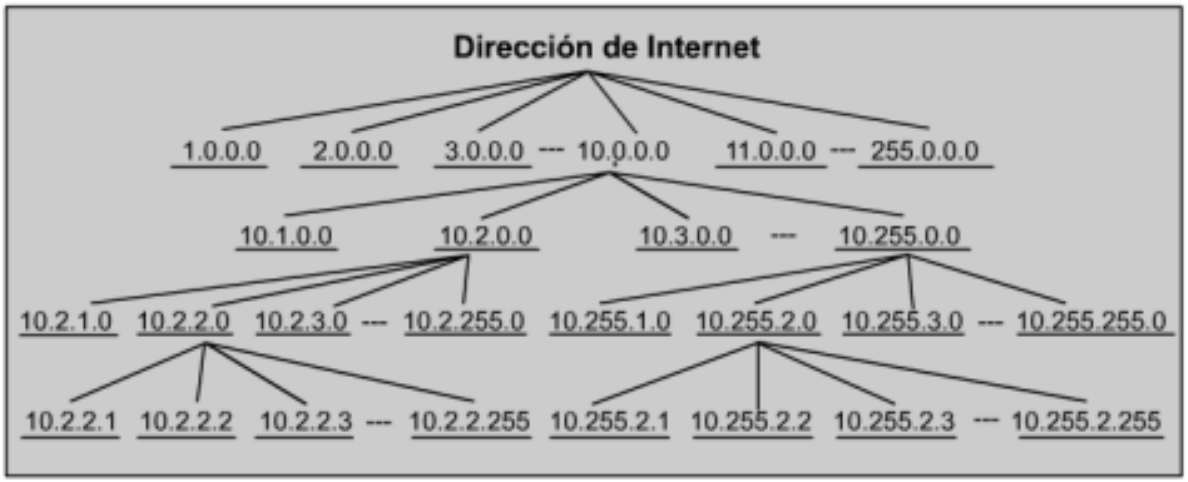
Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

* The 127.x.x.x address range is reserved as a loopback address, used for testing and diagnostic purposes.



Red	Host
1	1 2 3
2	1
3	1



Direcciones IP Clase, A, B, C, D y E

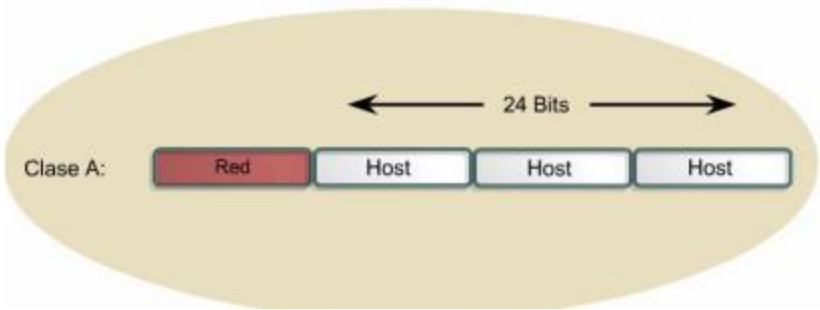
Class A	Network	Host		
Octet	1	2	3	4

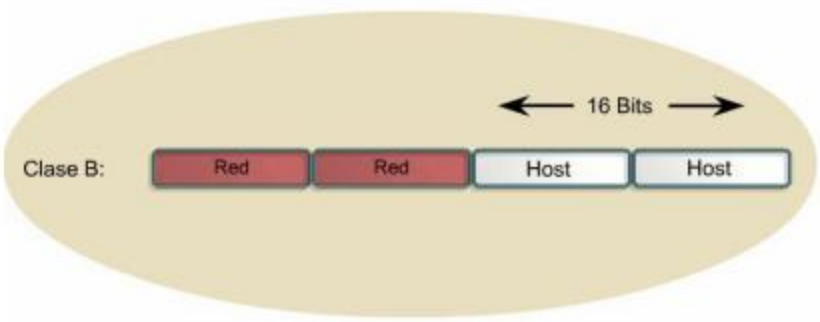
Class B	Network		Host	
Octet	1	2	3	4

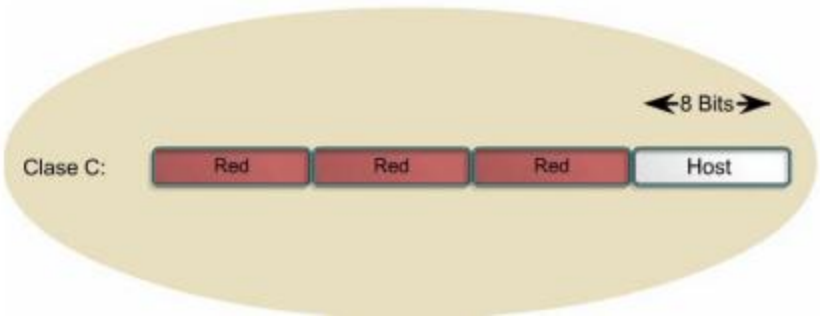
Class C	Network			Host
Octet	1	2	3	4

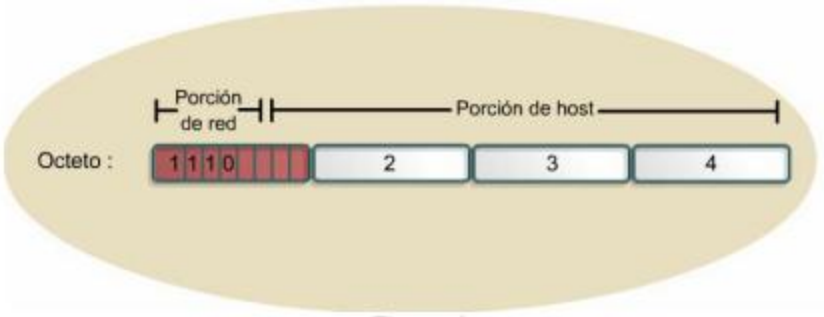
Class D	Host			
Octet	1	2	3	4

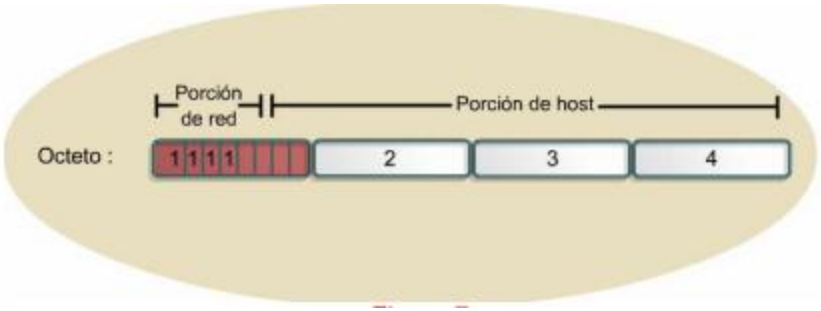
IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)





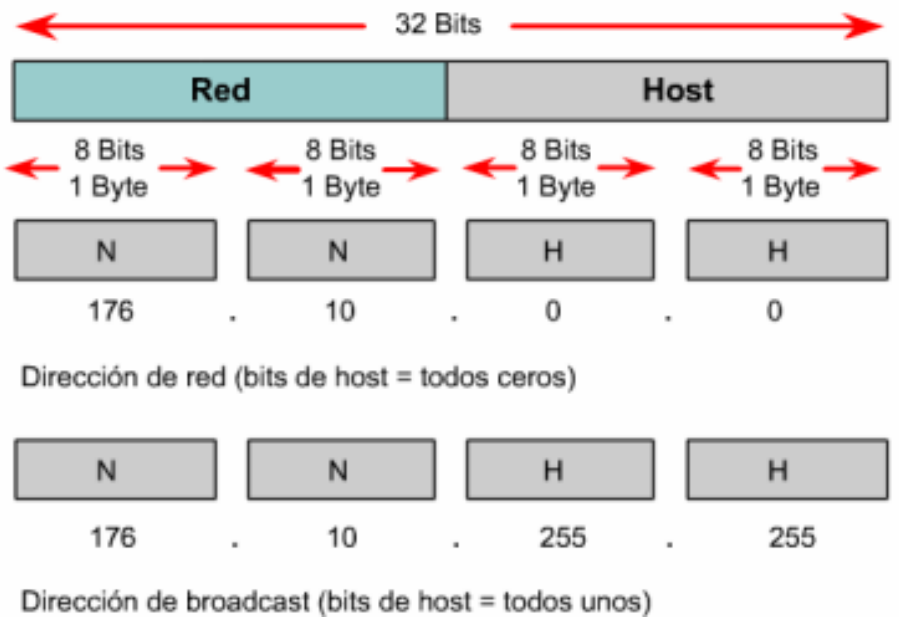


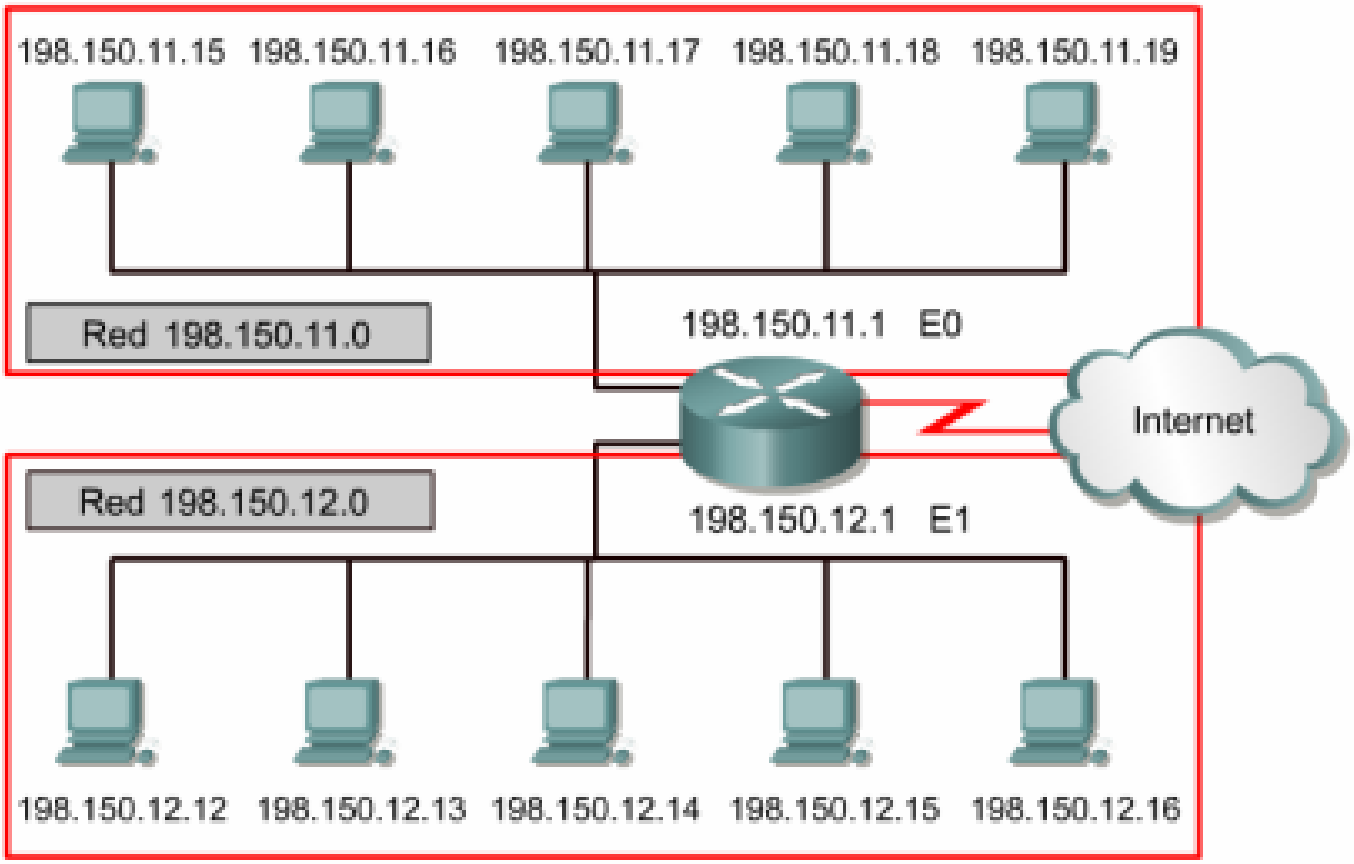




Direcciones IP reservadas

- **Ciertas direcciones de host son reservadas y no pueden asignarse a dispositivos de la red. Estas direcciones de host reservadas incluyen:**
- **Dirección de red: Utilizada para identificar la red en sí.**
- **En la Figura la sección que está identificada en el casillero superior representa la red 198.150.11.0. Los datos enviados a cualquier host de dicha red (198.150.11.1-198.150.11.254) se verá desde afuera de la red del área local con la dirección 198.159.11.0. Los números del host sólo tienen importancia cuando los datos se encuentran en una red de área local. La LAN contenida en el casillero inferior recibe el mismo tratamiento que la LAN superior, sólo que el número de la red es 198.150.12.0.**
- **Dirección de broadcast: Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de una red.**

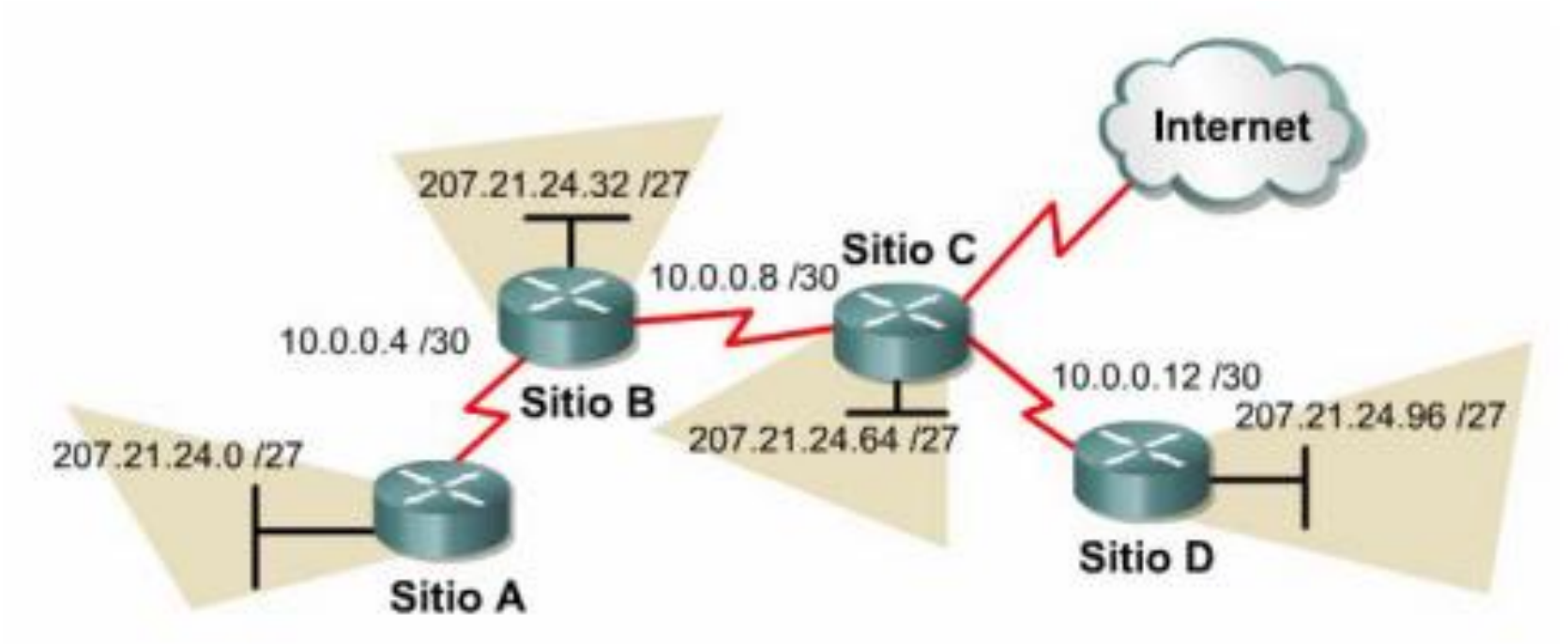




Direcciones IP públicas y privadas

- La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente. En la Figura , se muestran ciertos aspectos del esquema del direccionamiento de red. Al observar las redes, ambas tienen la dirección 98.150.11.0. El Router que aparece en esta ilustración no podrá enviar los paquetes de datos correctamente. Las direcciones IP de red repetidas hacen que el Router no pueda realizar su trabajo de seleccionar la mejor ruta. Es necesario que cada dispositivo de la red tenga
- El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado.
- La conección de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un Router es el dispositivo que realiza la NAT. NAT, junto con CIDR e IPv6 se describen con mayor detalle más adelante en el currículo.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255



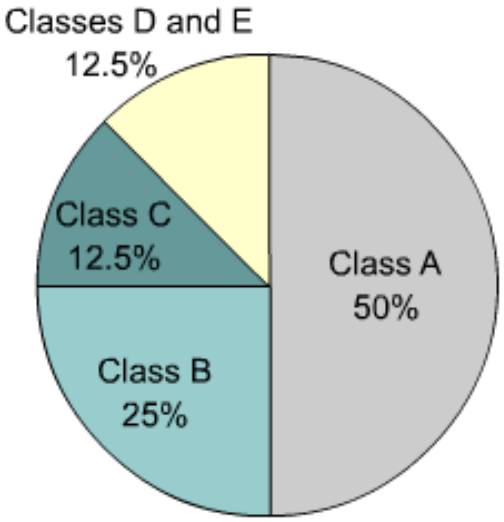
Introducción a la división en subredes

- **La división en subredes es otro método para administrar las direcciones IP. Este método, que consiste en dividir las clases de direcciones de red completas en partes de menor tamaño, ha evitado el completo agotamiento de las direcciones IP. Resulta imposible hablar sobre el TCP/IP sin mencionar la división en subredes.**

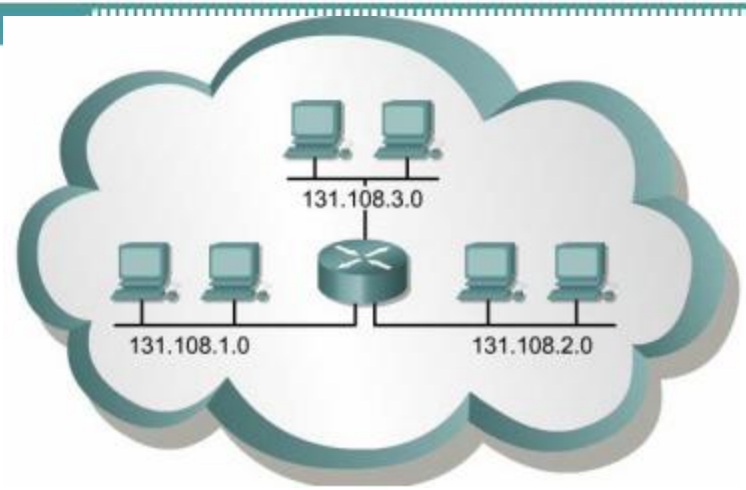
Notación decimal para el primer octeto de host	Número de subredes	Número de Hosts de clase A por subred	Número de Hosts de clase B por subred	Número de Hosts de clase C por subred
.192	2	4,194,302	16,382	62
.224	6	2,097,150	8,190	30
.240	14	1,048,574	4,094	14
.248	30	524,286	2,046	6
.252	62	262,142	1,022	2
.254	126	131,070	510	-
.255	254	65,534	254	-

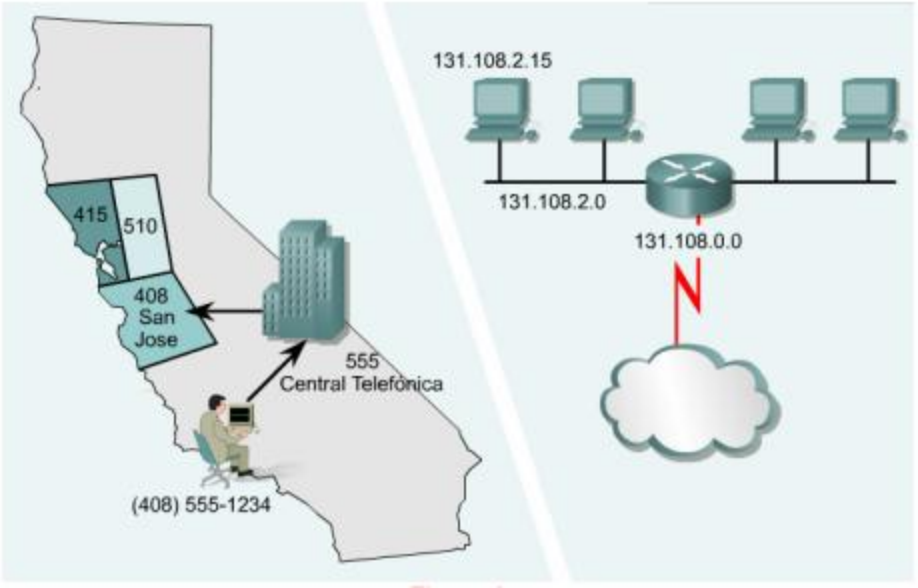
IPv4 en comparación con IPv6

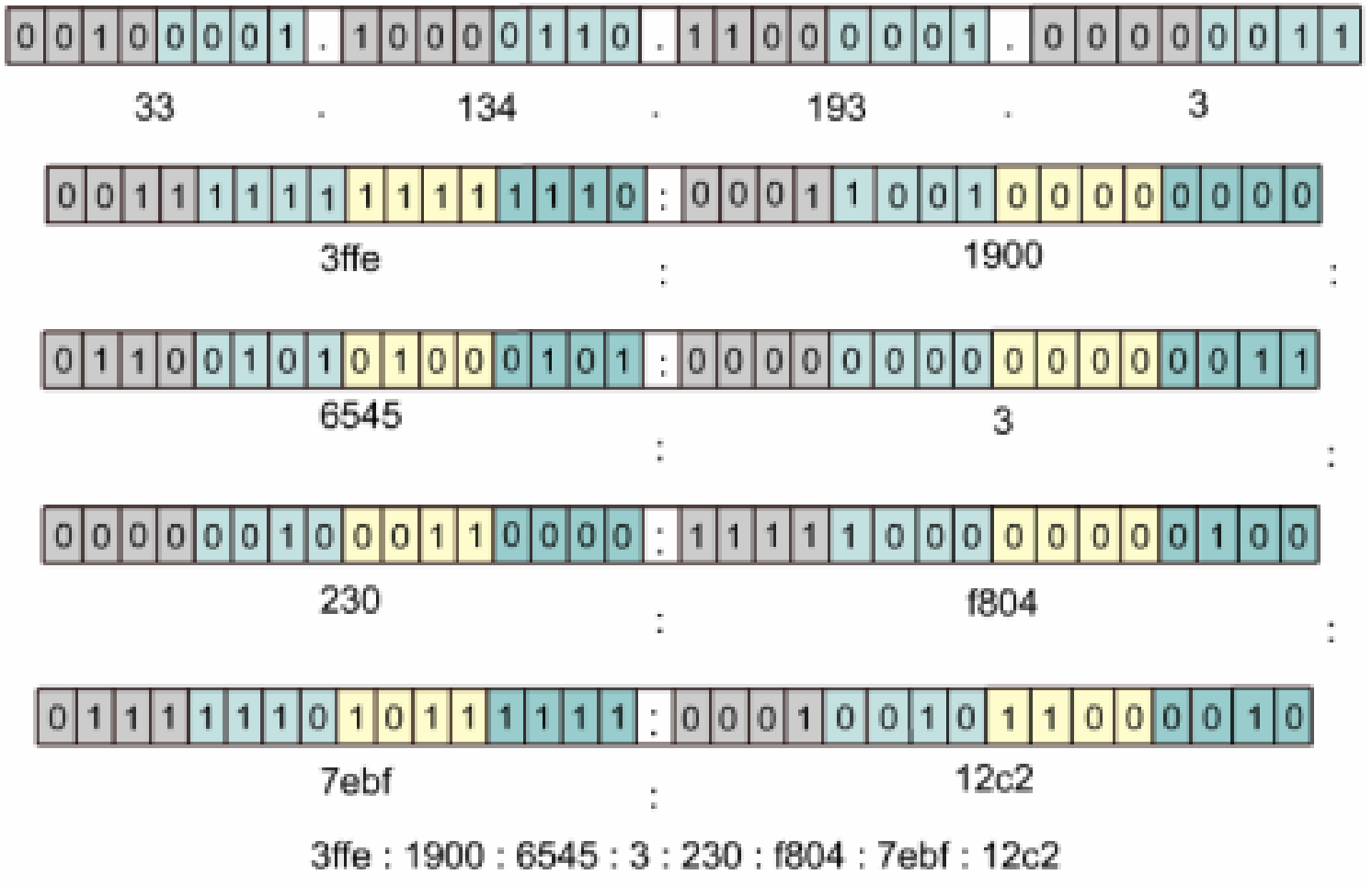
- **Cuando se adoptó TCP/IP en los años 80, dependía de un esquema de direccionamiento de dos niveles. En ese entonces, esto ofrecía una escalabilidad adecuada. Desafortunadamente, los diseñadores de TCP/IP no pudieron predecir que, con el tiempo, su protocolo sostendría una red global de información, comercio y entretenimiento. Hace más de viente años, la Versión 4 del IP (IPv4) ofrecía una estrategia de direccionamiento que, aunque resultó escalable durante algún tiempo, produjo una asignación poco eficiente de las direcciones.**
- **Las direcciones Clase A y B forman un 75 por ciento del espacio de direccionamiento IPv4, sin embargo, se pueden asignar menos de 17 000 organizaciones a un número de red Clase A o B. Las direcciones de red Clase C son mucho más numerosas que las direcciones Clase A y B aunque ellas representan sólo el 12,5 por ciento de los cuatro mil millones de direcciones IP posibles**



IPv4







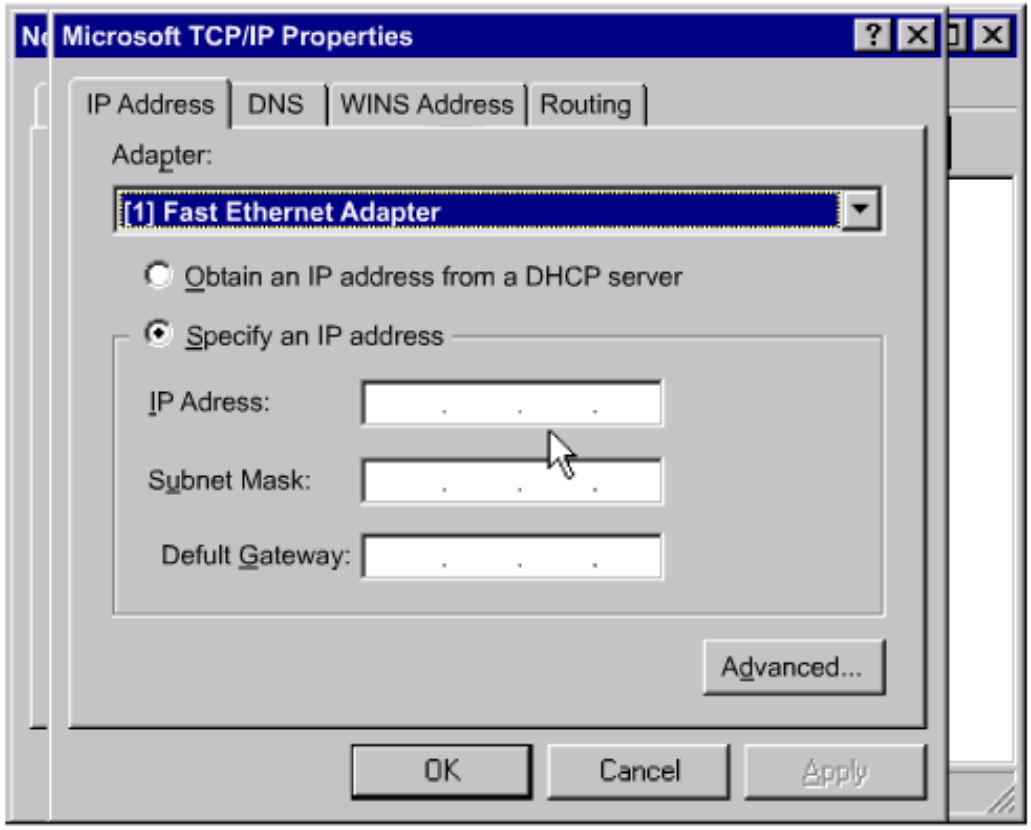
Obtener una dirección IP

Cómo obtener una dirección IP

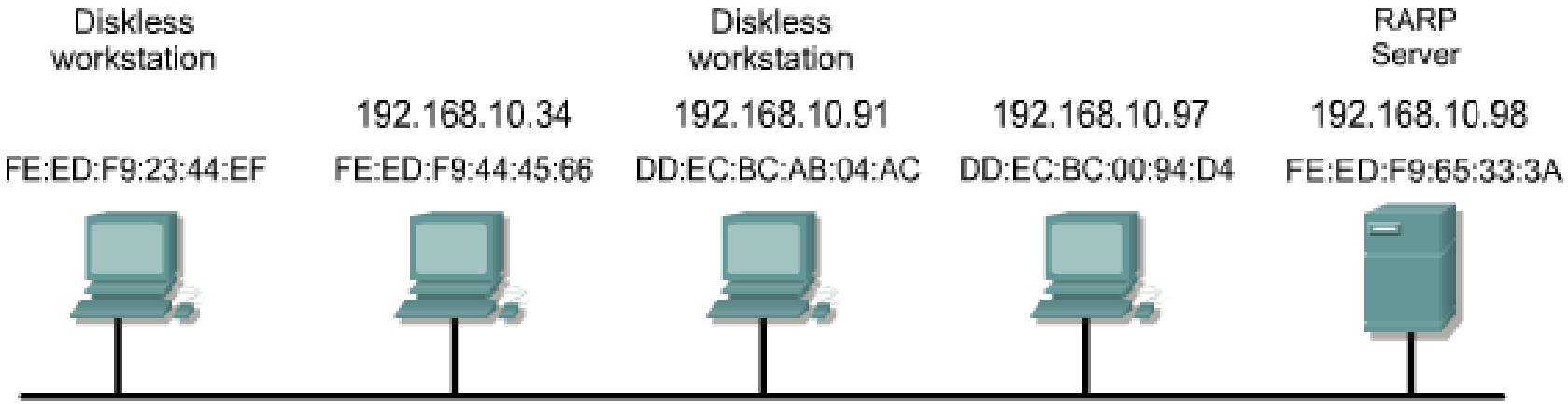
- **Los administradores de redes utilizan dos métodos para asignar las direcciones IP. Estos métodos son el estático y el dinámico. Más adelante, en esta lección, se tratará el direccionamiento estático y las tres variantes del direccionamiento dinámico. Independientemente del esquema de direccionamiento elegido, no es posible tener dos interfaces con la misma dirección IP. Dos hosts con la misma dirección IP pueden generar conflictos que hacen que ambos no puedan operar correctamente. Como muestra la Figura , los hosts tienen una dirección física ya que cuentan con una tarjeta de interfaz de red que les permite conectarse al medio físico.**

Asignación estática de una dirección IP

- **Cada dispositivo debe tener una dirección IP.**



Asignación de direcciones RARP IP



MAC HEADER	IP HEADER	RARP REQUEST MESSAGE
Destination FF-FF-FF-FF-FF-FF Source FE:ED:FD:23:44:EF	Destination 255.255.255.255 Source ????????	What is my IP address?

Asignación de direcciones BOOTP IP

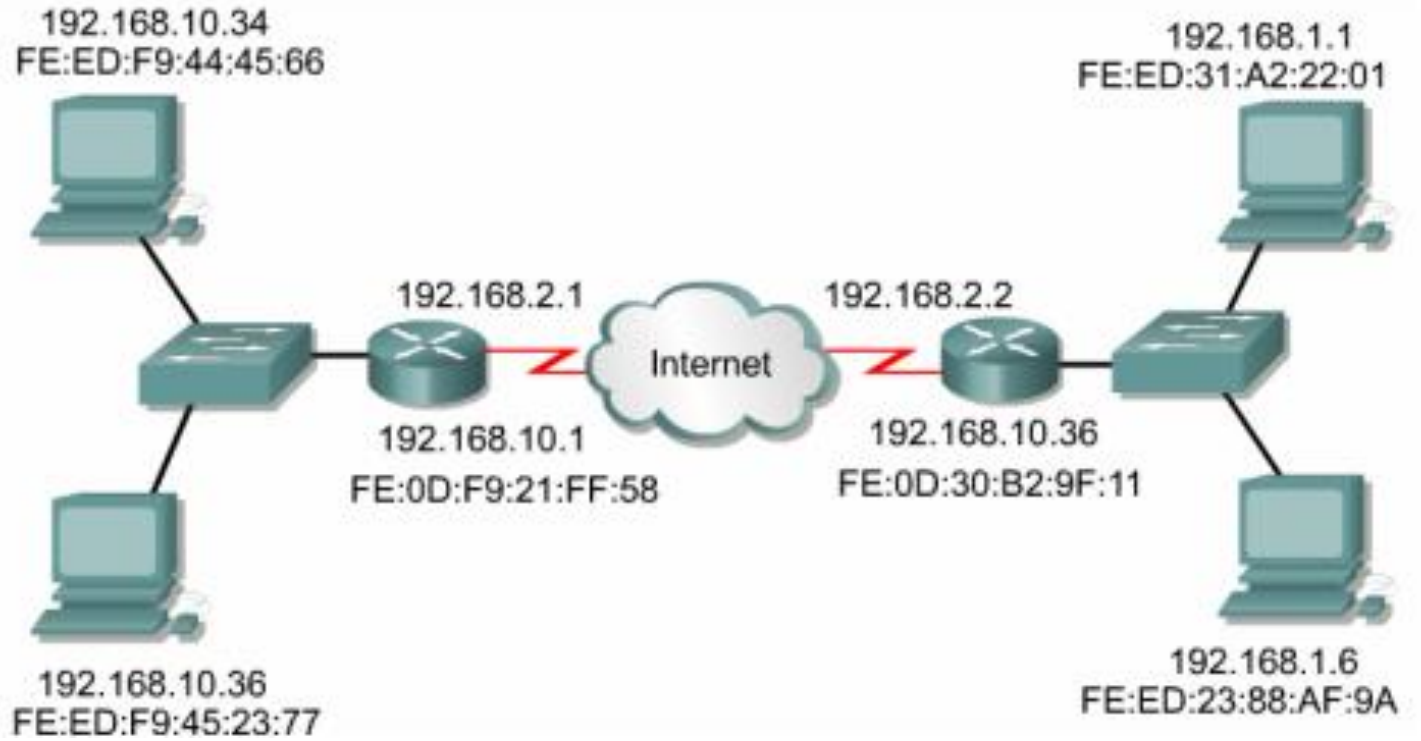
- **El protocolo bootstrap (BOOTP) opera en un entorno cliente-servidor y sólo requiere el intercambio de un solo paquete para obtener la información IP. Sin embargo, a diferencia del RARP, los paquetes de BOOTP pueden incluir la dirección IP, así como la dirección de un Router, la dirección de un servidor y la información específica del fabricante.**
- **Sin embargo, un problema del BOOTP es que no se diseñó para proporcionar la asignación dinámica de las direcciones. Con el BOOTP, un administrador de redes crea un archivo de configuración que especifica los parámetros de cada dispositivo. El administrador debe agregar hosts y mantener la base de datos del BOOTP. Aunque las direcciones se asignan de forma dinámica, todavía existe una relación exacta entre el número de direcciones IP y el número de hosts. Esto significa que para cada host de la red, debe haber un perfil BOOTP con una asignación de dirección IP en él. Dos perfiles nunca pueden tener la misma dirección IP. Es posible que estos perfiles se utilicen al mismo tiempo y esto quiere decir que dos hosts tendrían la misma dirección IP**

Administración de direcciones DHCP IP

- **El Protocolo de configuración dinámica del host (DHCP) es el sucesor del BOOTP. A diferencia del BOOTP, el DHCP permite que el host obtenga la dirección IP de forma dinámica sin que el administrador de red tenga que configurar un perfil individual para cada dispositivo. Lo único que se requiere para utilizar el DHCP es un rango definido de direcciones IP en un servidor DHCP. A medida que los hosts entran en línea, se comunican con el servidor DHCP y solicitan una dirección. El servidor DHCP elige una dirección y se la arrienda a dicho host. Con DHCP, la configuración completa de las red se puede obtener en un mensaje.**
- **Esto incluye todos los datos que proporciona el mensaje BOOTP más una dirección IP arrendada y una máscara de subred.**
- **La principal ventaja que el DHCP tiene sobre el BOOTP es que permite que los usuarios sean móviles. Esta movilidad permite que los usuarios cambien libremente las conexiones de red de un lugar a otro. Ya no es necesario mantener un perfil fijo de cada dispositivo conectado a la red como en el caso del sistema BOOTP. La importancia de este avance del DHCP es su capacidad de arrendar una dirección IP a un dispositivo y luego reclamar dicha dirección IP para otro usuario una vez que el primero la libera. Esto significa que DHCP puede asignar una dirección IP disponible a cualquiera que se conecte a la red.**

Problemas en la resolución de direcciones

- **Uno de los principales problemas del networking es cómo comunicarse con los otros dispositivos de la red.**
- **En la comunicación TCP/IP, el datagrama de una red de área local debe contener tanto una dirección MAC destino como una dirección IP destino. Estas direcciones deben ser correctas y concordar con las direcciones IP y MAC destino del dispositivo host. Si no concuerdan, el host destino descartará el datagrama. La comunicación dentro de un segmento de LAN requiere de dos direcciones. Debe haber una forma de mapear las direcciones IP a MAC de forma automática. Se necesitaría demasiado tiempo si el usuario creara los mapas de forma manual. El conjunto TCP/IP cuenta con un protocolo, llamado Protocolo de resolución de direcciones (ARP), que puede obtener las direcciones MAC, de forma automática, para la transmisión local. Pueden surgir diferentes problemas cuando se manda información fuera de la LAN.**
- **Las comunicaciones entre dos segmentos de LAN tienen una tarea extra. Tanto las direcciones IP como las MAC son necesarias para el dispositivo de enrutamiento intermedio y el host destino. TCP/IP tiene una variante en ARP llamada ARP proxy que proporciona la dirección MAC de un dispositivo intermedio para realizar la transmisión a otro segmento de la red fuera de la LAN.**



Protocolo de resolución de direcciones (ARP)

- En la red TCP/IP, el paquete de datos debe contener tanto la dirección MAC destino como la dirección IP destino. Si el paquete pierde alguna de las dos, los datos no pasarán de la Capa 3 a las capas superiores. De esta forma, las direcciones MAC e IP actúan como controles y balances entre sí. Una vez que los dispositivos determinan las direcciones IP de los dispositivos destino, pueden agregar las direcciones MAC de destino a los paquetes de datos.
- Algunos dispositivos guardan tablas que contienen las direcciones MAC e IP de otros dispositivos conectados a la misma LAN. Estas reciben el nombre de tablas del Protocolo de resolución de direcciones (ARP). Las tablas ARP se guardan en la memoria RAM, donde la información en caché se guarda automáticamente en cada uno de los dispositivos. Resulta muy inusual que un usuario tenga que entrar en la tabla ARP de forma manual