CAPÍTULO 1

PRINCIPIOS DE NETWORKING

MODELO DE REFERENCIA OSI

A principios de los años 80 los fabricantes informáticos más importantes del momento se reúnen para unificar diferencias y recopilar la mayor información posible acerca de cómo poder integrar sus productos hasta el momento no compatibles entres sí y exclusivos para cada uno de ellos. Como resultado de este acuerdo surge el modelo de referencia OSI, que sigue los parámetros comunes de hardware y software haciendo posible la integración multifabricante.

El modelo **OSI** (Modelo abierto de internetwork, no confundir con ISO) divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin tener necesidad de depender de otras áreas. Un programador crea una aplicación determinada sin importarle cuáles serán los medios por los que se trasladarán los datos, inversamente un técnico de comunicaciones proveerá comunicación sin importarle qué datos transporta.

En su conjunto el modelo OSI se compone de siete capas bien definidas que son: APLICACIÓN, PRESENTACIÓN, SESIÓN, TRANSPORTE, RED, ENLACE DE DATOS Y FÍSICA.

7	APLICACIÓN
6	PRESENTACIÓN
5	SESIÓN
4	TRANSPORTE
3	RED
2	ENLACE DE DATOS
1	FÍSICA

Las Siete Capas del Modelo OSI

Cada una de estas capas presta servicio a la capa inmediatamente superior, siendo la capa de aplicación la única que no lo hace ya que al ser la última capa su servicio está directamente relacionado con el usuario. A sí mismo cada una de estas siete capas del host origen se comunica directamente con su similar en el host de destino. Las cuatro capas inferiores también son denominadas capas de medios (en algunos casos capas de flujo de datos), mientras que las tres superiores capas se llaman de Host.

Modelo OSI:

- *Proporciona una forma de entender cómo opera los dispositivos en una red.*
- *Es la referencia para crear e implementar estándares de red, dispositivos y esquemas de internetworking.*
- *Separa la compleja operación de una red en elementos más simples.*
- *Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares ocupándose cada uno de su parte especifica.*
- *Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug-and-play" e integración multifabricante.*

Descripción de las siete capas

Capa de aplicación: Es la única capa que no presta servicio a otra puesto que es la capa de nivel superior del modelo OSI directamente relacionada con el usuario. La aplicación a través del software dialoga con los protocolos respectivos para acceder al medio. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa. Algunos protocolos relacionados con esta capa son: HTTP, Correo electrónico, telnet.

Capa de presentación: Los datos formateados se proveen de diversas funciones de conversión y codificación que se aplican a los datos provenientes de la capa aplicación. Estas funciones aseguran que estos datos enviados desde la capa de aplicación de un sistema origen podrán ser leídos por la capa de aplicación de otro sistema destino. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Por ejemplo los formatos de imágenes jpeg y gif que se muestran en páginas web. Este formato asegura que todos los navegadores web puedan mostrar las imágenes, con independencia del sistema operativo utilizado. Algunos protocolos relacionados con esta capa son: JPEG, MIDI, MPEG, QUICKTIME.

Capa de sesión: Es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La Comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

Capa de transporte: Es la encargada de la comunicación confiable entre host, control de flujo y de la corrección de errores entre otras cosas. Los datos son divididos en segmentos identificados con un encabezado con un número de puerto que identifica la aplicación de origen. En esta capa funcionan protocolos como UDP y TCP siendo este último uno de los más utilizados debido a su estabilidad y confiabilidad.

Capa de red: En esta capa se lleva a cabo el direccionamiento lógico que tiene carácter jerárquico, se selecciona la mejor ruta hacia el destino mediante el uso de tablas de enrutamiento a través del uso de protocolos de enrutamiento o por direccionamiento estático. Protocolos de capa de red: IP, IPX, RIP, IGRP, Apple Talk.

Capa de enlace de datos: Proporciona las comunicaciones entre puestos de trabajo en una primera capa lógica, transforma los voltios en tramas y las tramas en voltios. El direccionamiento físico y la determinación de si deben subir un mensaje a la pila de protocolo ocurren en esta capa. Esta dividida en dos subcapas, la **LLC** *Logical Link Control* y la subcapa ***MAC.*** Protocolos de capa 2, Ethernet, 802.2, 802.3, HDLC, Frame-Relay.

Capa física: Se encarga de los medios, conectores, especificaciones eléctricas, lumínicas y de la codificación. Los bits son transformados en pulsos eléctricos, en luz o en radio frecuencia para ser enviados según sea el medio en que se propaguen.

Proceso de encapsulación de los datos

El proceso desde que los datos son incorporados al ordenador hasta que se transmiten al medio se llama encapsulación. Estos datos son formateados, segmentados, identificados con el direccionamiento lógico y físico para finalmente ser enviados al medio. A cada capa del modelo OSI le corresponde una **PDU** (Unidad de Datos) siguiendo por lo tanto el siguiente orden de encapsulamiento:

DATOS-SEGMENTOS-PAQUETES-TRAMAS-BITS

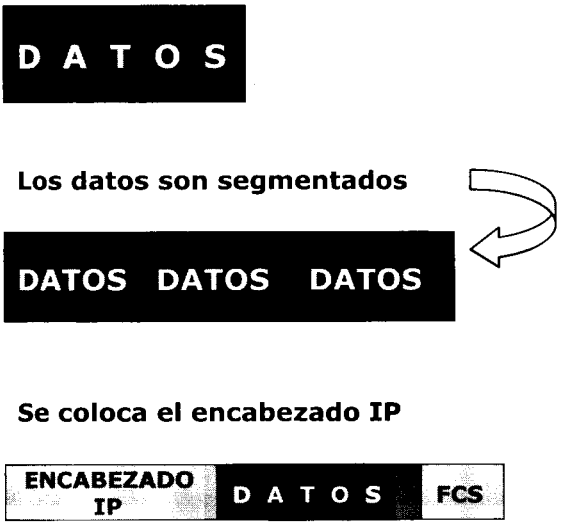
APLICACIÓN	
PRESENTACIÓN	**DATOS**
SESIÓN	
TRANSPORTE	**SEGMENTOS**
RED	**PAQUETES**
ENLACE DE DATOS	**TRAMAS**
FÍSICA	**BITS**

Relación entre capas del modelo OSI y su correspondiente PDU

Debido a que posiblemente la cantidad de los datos sea demasiada, la capa de transporte desde el origen se encarga de segmentarlos para así ser empaquetados debidamente, esta misma capa en el destino se encargara de reensamblar los datos y colocarlos en forma secuencial, ya que no siempre llegan a su destino en el orden en que han sido segmentados, así mismo acorde al protocolo que se esté utilizando habrá corrección de errores. Estos segmentos son empaquetados (paquetes o datagramas) e identificados en la capa de red con la dirección lógica o IP correspondiente al origen y destino. Ocurre lo mismo con la dirección MAC en la capa de enlace de datos formándose las tramas o frames para ser transmitidos a través de alguna interfaz. Finalmente las tramas son enviadas al medio desde la capa física.

El proceso inverso se llama desencapsulación de datos.

Secuencia de la encapsulación de datos:



Formato básico de una trama ethernet

PREÁMBULO	DIRECCIÓN DESTINO IP/MAC	DIRECCIÓN ORIGEN IP/MAC	NÚMERO DE PROTOCOLO	TAMAÑO DE LA TRAMA		FCS	FIN

Longitud máxima: **1518** Bytes
Longitud mínima: **64** Bytes

FUNCIONES DE LA CAPA FÍSICA

La capa física define el tipo de medio, el tipo de conector y el tipo de señalización. Se especifican los requisitos necesarios para la correcta transmisión de los datos. Se establecen las características eléctricas, mecánicas y funcionales para activar, mantener y desactivar la conexión física entre sistemas finales.

La capa física especifica también características tales como niveles de voltaje, tasas de transferencia de datos, distancias máximas de transmisión y conectores, cada medio de red posee a su vez su propio ancho de banda y unidad máxima de transmisión (**MTU**).

El medio físico y los conectores usados para conectar dispositivos al medio vienen definidos por estándares da la capa física.

Los estándares de cableado se identifican siguiendo los siguientes conceptos:

10 Base T

Donde:

- **10** hace referencia a la velocidad de transmisión en Mbps (mega-bits por segundo) en este caso 10 Mbps.
- **Base** es la tecnología de transmisión (banda base, analógica o digital) en este caso Digital.
- **T** se refiere al medio físico, en este caso par trenzado.

El enfoque principal de este libro esta asociado con los estándares e implementaciones Ethernet e IEE 802.3.

El siguiente cuadro muestra las características de los estándares más comunes:

ESTÁNDAR	MEDIO FÍSICO	DISTANCIA MÁXIMA	COMENTARIOS
10BASE 2	CABLE COAXIAL FINO DE 50 OHMS THINNET	185 METROS	CONECTORES BNC
10BASE 5	CABLE COAXIAL GRUESO DE 50 OHMS THINKNET	500 METROS	CONECTORES BNC
10BASE FB	FIBRA ÓPTICA	2000 METROS	CABLEADO DE BACKBONE
100BASE FX	FIBRA ÓPTICA MULTIMODO DE 62.5/125 MICRONES	400 METROS	CONECTORES ST, SC
100BASE FX	FIBRA ÓPTICA MONOMODO	10000 METROS	CABLEADO DE BACKBONE
1000BASE SX	FIBRA ÓPTICA MULTIMODO	260 METROS	VARIAS SEÑALES A LA VEZ
100BASE LX	FIBRA ÓPTICA MONOMODO DE 9 MICRONES	3000 A 10000 METROS	CABLEADO DE BACKBONE
10BASE T	UTP CATEGORÍA 3, 4, 5	100 METROS	CONECTORES RJ-45
100BASE T	UTP CATEGORÍA 5	100 METROS	CONECTORES RJ-45
100BASE TX	UTP, STP CATEGORÍA 6, 7	100 METROS	CONECTORES RJ-45
1000BASE T	UTP CATEGORÍA 5, 6	100 METROS	CONECTORES RJ-45 CAT 6

La Normativa **EIE/TIA 568**, creada en 1991, establece los estándares de cableado estructurado, ampliada posteriormente a **568-A** y **568-B.**

Norma de Cableado 568-A

PIN	PAR	FUNCIÓN	COLOR
1	3	TRANSMITE +	BLANCO/VERDE
2	3	TRANSMITE -	VERDE
3	2	RECIBE +	BLANCO/ NARANJA
4	1	TELEFONÍA	AZUL
5	1	TELEFONÍA	BLANCO/ AZUL
6	2	RECIBE -	NARANJA
7	4	RESPALDO	BLANCO/MARRÓN
8	4	RESPALDO	MARRÓN

Orden de los pines correspondiente a la norma 568-A sobre un conector RJ-45

Norma de Cableado 568-B

PIN	PAR	FUNCIÓN	COLOR
1	3	TRANSMITE +	BLANCO/ NARANJA
2	3	TRANSMITE -	NARANJA
3	2	RECIBE +	BLANCO/ VERDE
4	1	TELEFONÍA	AZUL
5	1	TELEFONÍA	BLANCO/ AZUL
6	2	RECIBE -	VERDE
7	4	RESPALDO	BLANCO/MARRÓN
8	4	RESPALDO	MARRÓN

Orden de los pines correspondiente a la norma 568-B sobre un conector RJ-45

Cable directo

El orden de los pines es igual en ambos conectores, se debe utilizar la misma norma en cada extremo

COLOR	COLOR
BLANCO/ NARANJA	BLANCO/ NARANJA
NARANJA	NARANJA
BLANCO/ VERDE	BLANCO/ VERDE
AZUL	AZUL
BLANCO/ AZUL	BLANCO/ AZUL
VERDE	VERDE
BLANCO/MARRÓN	BLANCO/MARRÓN
MARRÓN	MARRÓN

Cable directo 568 B

COLOR	COLOR
BLANCO/VERDE	BLANCO/VERDE
VERDE	VERDE
BLANCO/ NARANJA	BLANCO/ NARANJA
AZUL	AZUL
BLANCO/ AZUL	BLANCO/ AZUL
NARANJA	NARANJA
BLANCO/MARRÓN	BLANCO/MARRÓN
MARRÓN	MARRÓN

Cable directo 568 A

Cable cruzado

El orden de los pines varia en ambos extremos, se cruzan el 1-2 con el 3-6 y el 3-6 con el 1-2. El cable cruzado también es llamado **crossover**.

COLOR	COLOR
BLANCO/ NARANJA	BLANCO/ VERDE
NARANJA	VERDE
BLANCO/ VERDE	BLANCO/ NARANJA
AZUL	AZUL
BLANCO/ AZUL	BLANCO/ AZUL
VERDE	NARANJA
BLANCO/MARRÓN	BLANCO/MARRÓN
MARRÓN	MARRÓN

Orden de los colores en ambos extremos
de un cable cruzado

Cable consola

El orden de los pines es completamente inverso, 1-2-3-4-5-6-7-8 con el 8-7-6-5-4-3-2-1, respectivamente. El cable de consola también es llamado **rollover**.

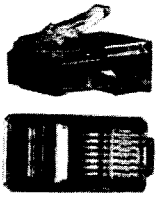
1	AL	8
2	AL	7
3	AL	6
4	AL	5
5	AL	4
6	AL	3
7	AL	2
8	AL	1

Dispositivos de la capa física

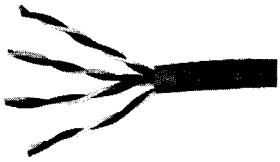
En la capa física comprende los medios, (cobre, fibra, RF), los conectores, transceivers, repetidores y Hubs. Ninguno de ellos manipula los datos transmitidos sino que solo se encargan de transportarlos y propagarlos por la red.

Los repetidores se encargan de retransmitir y de retemporizar los pulsos eléctricos cuando la extensión del cableado supera las medidas específicas.

Los hubs son repetidores multipuesto, también llamados concentradores. Al recibir una trama inundan todos sus puertos obligando a todos los dispositivos conectados a cada uno de sus puertos a leer dichas tramas. Los transceivers son adaptadores de un medio a otro.



Conector RJ-45



Cable UTP

Cable blincado STP

Fibra Óptica

DOMINIOS DE COLISIÓN Y DIFUSIÓN

Ethernet es una tecnología conflictiva, todos los equipos de trabajo que se conectan al mismo medio físico reciben las señales enviadas por otros dispositivos. Si dos estaciones transmiten a la vez, se genera una colisión. Si no existieran mecanismos que detectasen y corrigiesen los errores de estas colisiones, ethernet no podría funcionar.

En el diseño de una red se debe tener especial cuidado con los llamados Dominios de Colisión y Dominio de difusión (Broadcast)

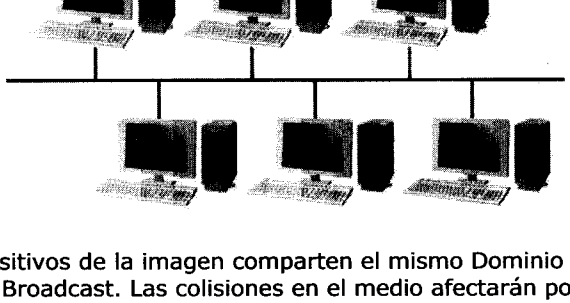
Dominio de colisión:

Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado será una colisión entre las dos señales. Como resultado de estas colisiones se produce un consumo inadecuado de recursos y de ancho de banda. Cuanto menor sea la cantidad de dispositivos afectados a un dominio de colisión mejor desempeño de la red.

Dominio de difusión:

Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos. Una cantidad excesiva de estos mensajes de difusión (broadcast) provocará un bajo rendimiento en la red, una cantidad exagerada (tormenta de broadcast) dará como resultado el mal funcionamiento de la red hasta tal punto de poder dejarla completamente congestionada.

Los hubs o concentradores tienen un único dominio de colisión, eso quiere decir que si dos equipos provocan una colisión en un segmento asociado a un puerto del hubs, todos los demás dispositivos aun estando en diferentes puertos se verán afectados. De igual manera se verían afectados si una estación envía un Broadcast, debido a que un hub también tiene un solo dominio de difusión.



Los dispositivos de la imagen comparten el mismo Dominio de Colisión y de Broadcast. Las colisiones en el medio afectarán por igual a todos los host del segmento.

CSM

La tecn
determi
de porta
varios p
acceder
ningún
procede
puestos
mismo t

A partir
asegura
que las e

El ejem

FUNC

La finalic
trabajo e
direccion
datos co
subir un

La capa
no basa
conocimi
de red (**N**

Está divi
de la ide
posterior
MAC (8
topología
ordenada
destino s

CSMA/CD

La tecnología Ethernet utiliza para controlar las colisiones dentro de un determinado segmento el protocolo **CSMA/CD** (acceso múltiple con detección de portadora (carrier) y detección de colisiones. En la práctica, esto significa que varios puestos pueden tener acceso al medio y que, para que un puesto pueda acceder a dicho medio, deberá detectar la portadora para asegurarse de que ningún otro puesto esté utilizándolo. Si el medio se encuentra en uso, el puesto procederá a mantener en suspenso el envío de datos. En caso de que haya dos puestos que no detectan ningún otro tráfico, ambos tratarán de transmitir al mismo tiempo, dando como resultado una colisión.

A partir de esta colisión las estaciones emiten una señal de congestión para asegurarse de que existe una colisión y se genera un algoritmo de espera con el que las estaciones retransmitirán aleatoriamente.

El ejemplo más claro de CSMA/CD es el de "escucho y luego transmito".

FUNCIONES DE LA CAPA DE ENLACE DE DATOS

La finalidad de esta capa es proporcionar las comunicaciones entre puestos de trabajo en una primera capa lógica que hay por encima de los bits del cable. El direccionamiento físico de los puestos finales se realiza en la capa de enlace de datos con el fin de facilitar a los dispositivos de red la determinación de si deben subir un mensaje a la pila de protocolo.

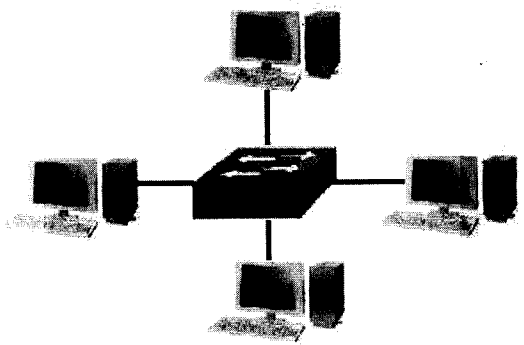
La capa de enlace de datos da soporte a servicios basados en la conectividad y no basados en ella, y proporciona la secuencia y control de flujo. Tiene conocimiento de la topología a la que está afectada y donde funciona la tarjeta de red (**NIC**).

Está dividida en dos subcapas, la **LLC** Logical Link Control (802.2), responsable de la identificación lógica de los distintos tipos de protocolos y el encapsulado posterior de los mismos para ser transmitidos a través de la red, y la subcapa **MAC** (802.3), responsable del acceso al medio, el direccionamiento físico, topología de la red, disciplina de la línea, notificación de errores, distribución ordenada de tramas y control óptimo de flujo. Las direcciones físicas de origen destino son representadas como direcciones de capa MAC.

Dispositivos de capa de enlace de datos

En la capa de enlace de datos se diferencian perfectamente los Dominios de Colisión y los Dominios de Difusión. Los puentes y los switches dividen a la red en segmentos, estos a su vez crean dominios de colisión. Una colisión producida en un segmento conectado a un switch no afectará a los demás segmentos conectados al mismo switch. Sin embargo los dispositivos de capa 2 no crean dominios de broadcast o difusión.

Un switch de 12 puertos utilizados tendrá 12 dominios de colisión y uno de difusión.



Los dispositivos de capa dos crean dominios de colisión pero mantienen un único Dominio de Broadcast.
Una colisión producida en un segmento NO afecta al resto.

En un switch, el reenvío de tramas se controla por medio de hardware (**ASIC**). Esta tecnología permite que las funciones de conmutación puedan llevarse a cabo a una velocidad mucho mayor que por software. Debido a la tecnología ASIC, los switches proporcionan escalabilidad a velocidades de gigabits con una latencia baja. Los puentes funcionan a nivel de software por lo que poseen mayor latencia comparados con un switch.

Un dispositivo de capa 2 almacena en una memoria de contenido direccionable (**CAM**) las direcciones físicas de los dispositivos asociados a un segmento de red conectado directamente a un puerto determinado. De esta manera identificará inmediatamente por qué puerto enviar la trama. Si el dispositivo de destino está en el mismo segmento que el origen el switch bloquea el paso de la trama a otro segmento. Este proceso se conoce como **filtrado**. Si el dispositivo de destino se encuentra en un segmento diferente, el switch envía la trama únicamente al segmento apropiado, técnica conocida como **conmutación** de capa dos. Si la dirección de destino es desconocida para el switch, o si se tratara de un **broadcast** este enviará la trama a todos los segmentos excepto a aquel de donde se ha recibido la información. Este proceso se denomina **inundación**.

La **NIC** o tarjeta de red se desempeña principalmente en la capa de enlace de datos, no debe confundirse con la capa física a pesar de estar directamente conectada al medio ya que sus principales funciones radican en la capa 2. La **NIC** almacena en su propia **ROM** la dirección **MAC** que consta de 48 bits y viene expresada en 12 dígitos hexadecimales. Los primeros 24 bits, o 6 dígitos hexadecimales, de la dirección MAC contienen un código de identificación del fabricante o vendedor **OUI** (Organizationally Unique Identifier). Los últimos 24 bits, o 6 dígitos hexadecimales, están administrados por cada fabricante y presentan, por lo general, el número de serie de la tarjeta. La dirección de la capa de enlace de datos no tiene jerarquías, es decir, que es un **direccionamiento plano**.

Ejemplo de una dirección MAC o dirección física

00-11-85-F2-32-E5

Donde:

00-11-85 representa el código del fabricante
F2-32-E5 representa el número de serie

Para verificar el correcto funcionamiento de la tarjeta de red se realiza un ping a la dirección IP de la misma.

En las redes punteadas/conmutadas observamos que:

- *Cada segmento genera su propio dominio de colisión.*
- *Todos los dispositivos conectados al mismo bridge o switch forman parte del mismo dominio de difusión.*
- *Todos los segmentos deben utilizar la misma implementación al nivel de la capa de enlace de datos como, por ejemplo, Ethernet o Token Ring. Si un puesto final concreto necesita comunicarse con otro puesto final a través de un medio diferente, se hace necesaria la presencia de algún dispositivo, como puede ser un router o un bridge de traducción, que haga posible al diálogo entre los diferentes tipos de medios.*
- *En un entorno conmutado, puede haber un dispositivo por segmento, y todos los dispositivos pueden enviar tramas al mismo tiempo, permitiendo de este modo que se comparta la ruta primaria.*

FUNCIONES DE LA CAPA DE RED

La capa de red define cómo transportar el tráfico de datos entre dispositivos que no están conectados localmente en el mismo dominio de difusión, es decir, que pertenecen a diferentes redes. Para conseguir esta comunicación se necesita conocer las direcciones lógicas asociadas a cada puesto de origen y de destino y una ruta bien definida a través de la red para alcanzar el destino deseado. La capa de red es independiente de la de enlace de datos y, por tanto, puede ser utilizada para conectividad de medios físicos diferentes.

Las direcciones de capa 3, o direcciones lógicas, son **direcciones jerárquicas**. Esta jerarquía define primero las redes y luego a los dispositivos (nodos) pertenecientes a esas redes. Un ejemplo para la comprensión de una dirección jerárquica sería un número telefónico, donde primero se define el código del país, luego el estado, y luego el número del usuario. Un esquema plano se puede ejemplificar con un número de carné de identidad donde cada número es único y personal.

Una dirección lógica cuenta con dos partes bien definidas, una que identifica de forma única a la red dentro de un Conjunto en la internetwork y la otra parte que representa al Host dentro de estas redes. Con la suma o combinación de ambas partes se obtiene un identificador único para cada dispositivo. El router identifica dentro de la dirección lógica la porción perteneciente a la red con el fin de identificar la red donde enviar los paquetes.

RECUERDE:

Existen muchos protocolos de red, todos cumplen las mismas funciones de identificar redes y hosts. TCP/IP es el protocolo común más usado.

Dirección de capa tres

Una dirección IP se identifica como:

- Una dirección de 32 bits, dividida en cuatro octetos. Este direccionamiento identifica una porción perteneciente a la red y otra al host.
- A cada dirección IP le corresponde una máscara de red de 32 bits dividida en cuatro octetos. El router determina las porciones de red y host por medio de la máscara de red.
- Las direcciones IP generalmente se representan en forma decimal para hacerlas más comprensibles. Esta forma se conoce como **decimal punteado o notación decimal de punto.**

Dirección IP 172.16.1.3
Máscara 255.255.0.0

172	16	1	3
10101100	**00010000**	**00000001**	**00000011**
255	255	0	0
11111111	**11111111**	**00000000**	**00000000**
Porción de red		Porción de Host	

Formato de una dirección IP

Operación AND

Los routers determinan la ruta de destino a partir de la dirección de RED, estos comparan las direcciones IP con sus respectivas máscaras efectuando la operación booliana **AND**. Los routers ignoran el rango de Host para encontrar la red destino a la que este pertenece.

La operación AND consiste en comparar bit a bit la dirección IP y la máscara utilizando el siguiente razonamiento:

1x1=1
1x0=0
0x1=0
0x0=0

Dirección de Host	**10101100.00100000.00000001.00000011**
Máscara de red	**11111111.11111111.00000000.00000000**
Dirección de red	**10101100.00100000.00000000.00000000**

En decimales:

Dirección de Host	**172.16.1.3**
Máscara de red	**255.255.0.0**
Dirección de red	**172.16.0.0**

Comparación entre el direccionamiento IPv4 e IPv6

Cuando se adoptó TCP/IP en los años 80, 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.

A mediados de los años 90 se comenzaron a detectar las siguientes dificultades sobre IPv4:

- Agotamiento de las restantes direcciones de red IPv4 no asignadas. En ese entonces, el espacio de Clase B estaba a punto de agotarse.

- Se produjo un gran y rápido aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Durante las últimas dos décadas, se desarrollaron numerosas extensiones al IPv4. Estas extensiones se diseñaron específicamente para mejorar la eficiencia con la cual es posible utilizar un espacio de direccionamiento de 32 bits como **VLSM** y **CIDR**.

Mientras tanto, se ha definido y desarrollado una versión más extensible y escalable del IP, la Versión 6 del IP (IPv6). IPv6 utiliza 128 bits en lugar de los 32 bits que en la actualidad utiliza el IPv4. IPv6 utiliza números hexadecimales para representar los 128 bits. IPv6 proporciona 640 sextillones de direcciones. Esta versión del IP proporciona un número de direcciones suficientes para futuras necesidades de comunicación.

Las direcciones IPv6 miden 128 bits y son identificadores de interfaces individuales y conjuntos de interfaces. Las direcciones IPv6 se asignan a interfaces, no a nodos. Como cada interfaz pertenece a un solo nodo, cualquiera de las direcciones unicast asignada a las interfaces del nodo se pueden usar como identificadores del nodo. Las direcciones IPv6 se escriben en hexadecimal, separados por dos puntos. Los campos IPv6 tienen una longitud de 16 bits.

Dirección IPv6:

24ae:0002:f2f3:b542:0001:5687:a2ff:6184

Para que las direcciones sean más fáciles de leer, es posible omitir los ceros iniciales de cada campo.

El campo: 0002: se escribe :2: el campo: 0001: se escribe :1:

24ae:2:f2f3:b542:1:5687:a2ff:6184

Dispositivos de la capa de RED

Los routers funcionan en la capa de red del modelo OSI separando los segmentos en dominios de colisión y difusión únicos. Estos segmentos están identificados por una dirección de red que permitirá alcanzar las estaciones finales. Los router cumplen dos funciones básicas que son la de **enrutar** y **conmutar** los paquetes. Para ejecutar estas funciones registran en **tablas de enrutamiento** los datos necesarios para esta función.

Además de identificar redes y proporcionar conectividad, los routers deben proporcionar estas otras funciones:

- Los routers no envían difusiones de Capa 2 ni tramas de multidifusión.
- Los routers intentan determinar la ruta más óptima a través de una red enrutada basándose en algoritmos de enrutamiento.
- Los routers separan las tramas de Capa 2 y envían paquetes basados en direcciones de destino Capa 3.
- Los routers asignan una dirección lógica de Capa 3 individual a cada dispositivo de red; por tanto, los routers pueden limitar o asegurar el tráfico de la red basándose en atributos identificables con cada paquete. Estas opciones, controladas por medio de listas de acceso, pueden ser aplicadas para incluir o descartar paquetes.
- Los routers pueden ser configurados para realizar funciones tanto de puenteado como de enrutamiento.
- Los routers proporcionan conectividad entre diferentes LAN virtuales (VLAN) en entornos conmutados.
- Los routers pueden ser usados para desplegar parámetros de calidad de servicio para tipos específicos de tráfico de red.

Una tabla de enrutamiento contiene la siguiente información:

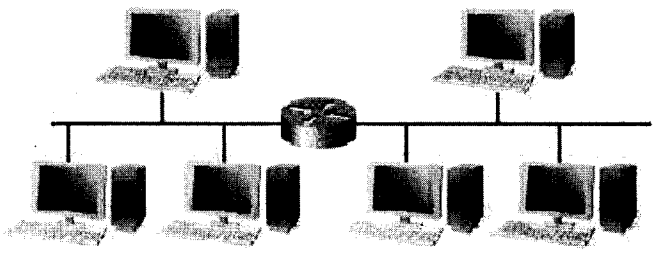
- **Dirección de red**. Representa redes conocidas por el router. La dirección de red es específica del protocolo. Si un router soporta varios protocolos, tendrá una tabla por cada uno de ellos.
- **Interfaz**. Se refiere a la interfaz usada por el router para llegar a una red dada. Esta es la interfaz que será usada para enviar los paquetes destinados a la red que figura en la lista.

- **Métrica**. Se refiere al coste o distancia para llegar a la red de destino. Se trata de un valor que facilita el router la elección de la mejor ruta para alcanzar una red dada. Esta métrica cambia en función de la forma en que el router elige las rutas. Entre las métricas más habituales figuran el número de redes que han de ser cruzadas para llegar al destino(conocido también como **saltos**), el tiempo que se tarda en atravesar todas las interfaces hasta una red dada(conocido también como **retraso**), o un valor asociado con la velocidad de un enlace(conocido también como **ancho de banda**).

En la siguiente salida del router se observa una tabla de enrutamiento con las Direcciones IP de destino (**172.25.25.6/32**), la métrica (**[120/2]**) y la correspondiente interfaz de salida **Serial0.1**.

```
Router2#show ip route rip
R     172.21.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R     172.22.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
      172.25.0.0/16 is variably subnetted, 6 subnets, 3 masks
R     172.25.25.6/32 [120/2] via 172.25.2.1, 00:00:01, Serial0.1
R     172.25.25.1/32 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R     172.25.1.0/24 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
R     172.25.0.0/16 [120/1] via 172.25.2.1, 00:00:01, Serial0.1
```

Además de las ventajas que aporta su uso en un campus, los routers pueden utilizarse también para conectar ubicaciones remotas con la oficina principal por medio de servicios WAN. Los routers soportan una gran variedad de estándares de conectividad al nivel de la capa física, lo cual ofrece la posibilidad de construir WAN. Además, pueden proporcionar controles de acceso y seguridad, que son elementos necesarios cuando se conectan ubicaciones remotas.



Los routers comunican redes diferentes creando Dominios de Difusión y de Colisión, los broadcast de un segmento no inundan a los demás ni las colisiones afectan al resto.

FUNCIONES DE LA CAPA DE TRANSPORTE

Para conectar dos dispositivos remotos es necesario establecer una conexión. La capa de transporte establece las reglas para esta interconexión. Permite que las estaciones finales ensamblen y reensamblen múltiples segmentos del mismo flujo de datos. Esto se hace por medio de identificadores que en TCP/IP reciben el nombre de **números de puerto**. La capa cuatro permite además que las aplicaciones soliciten transporte fiable entre los sistemas. Asegura que los segmentos distribuidos serán confirmados al remitente. Proporciona la retransmisión de cualquier segmento que no sea confirmado. Coloca de nuevo los segmentos en su orden correcto en el receptor. Proporciona control de flujo regulando el tráfico de datos.

En la capa de transporte, los datos pueden ser transmitidos de forma fiable o no fiable. Para IP, el protocolo TCP es fiable u orientado a conexión, mientras que UDP no es fiable, o no orientado a la conexión.

1 AL 1023	**Puertos bien conocidos**
1 AL 255	**Puertos públicos**
256 AL 1023	**Asignados a empresas**
Mayores al 1023	**Definidos por el usuario**

Números de puerto utilizados por TCP y UDP para identificar sesiones de diferentes aplicaciones

TCP utiliza una técnica llamada **Ventanas** donde se establece la cantidad de envío de paquetes antes de transmitir mientras que en el Windowing o de **Ventana deslizante**, el flujo de envío de datos es negociado dinámicamente entre el emisor y el receptor.

MODELO 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 **INTERNET**.

Al leer sobre las capas del modelo TCP/IP, tenga en cuenta el propósito original de Internet. Recordar su propósito ayudará a reducir las confusiones.

El modelo TCP/IP tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de acceso de red. Es importante observar que algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI. Resulta fundamental no confundir las funciones de las capas de los dos modelos ya que estas desempeñan diferentes funciones en cada modelo.

OSI	TCP/IP	PROTOCOLOS
APLICACIÓN PRESENTACIÓN SESIÓN	APLICACIÓN	TELNET, FTP, LPD, SNMP,TFTP, SMTP, NFS, X WINDOWS
TRANSPORTE	TRANSPORTE	TCP, UDP
RED	INTERNET	ICMP, BOOTP, ARP, RARP, IP
ENLACE DE DATOS FÍSICA	RED	ETHERNET, FAST-ETHERNET, TOKEN RING, FDDI

Comparativa entre el modelo OSI y el Modelo TCP/IP

RECUERDE:

1 AL 1023	PUERTOS BIEN CONOCIDOS
1 AL 255	PUERTOS PÚBLICOS
256 AL 1023	ASIGNADOS A EMPRESAS
MAYORES AL 1023	DEFINIDOS POR EL USUARIO

RECUERDE:

Nº	MODELO OSI	FUNCIONES	PROTOCOLOS
7	APLICACIÓN	Nivel usuario, Software, aplicaciones	HTTP, TELNET, SNMP,
6	PRESENTACIÓN	Representa Datos, Formateo, cifrado.	JPG, MP3, DOC
5	SESIÓN	Reglas, separar datos de las aplicaciones, establece sesiones entre aplicaciones	NFS, LINUX
4	TRANSPORTE	Comunicación confiable, Corrección de errores, control de flujo, establece, mantiene y finaliza comunicaciones	UDP,TCP
3	RED	Direccionamiento lógico, determinación de ruta	IP, IPX, RIP, ARP, ICMP
2	ENLACE DE DATOS	Direccionamiento físico, mapa topológico, acceso al medio	ETHERNET, PPP, HDLC
1	FÍSICA	Codificación, transmisión	EIE/TIA 568

RECUERDE:

La capa de Internet también es llamada capa de Interred o capa de red.

RECUERDE:

TCP protocolo confiable de capa de transporte orientado a conexión
UDP protocolo **NO** confiable de capa de transporte **NO** orientado a conexión
Un protocolo Orientado a conexión es el que previamente establece un saludo antes de enviar los datos, como es el ejemplo de una llamada telefónica, donde se establece un saludo de tres vías. Un protocolo No orientado a conexión es el que no establece saludo previo antes de enviar los datos como es el caso de un envío postal donde se establece un saludo de dos vías

RECUERDE:

OSI	TCP/IP	PROTOCOLOS
APLICACIÓN PRESENTACIÓN SESIÓN	APLICACIÓN	TELNET, FTP, LPD, SNMP,TFTP, SMTP, NFS, X WINDOWS
TRANSPORTE	TRANSPORTE	TCP, UDP
RED	INTERNET	ICMP, BOOTP, ARP, RARP, IP
ENLACE DE DATOS FÍSICA	RED	ETHERNET, FAST-ETHERNET, TOKEN RING, FDDI

Comparativa entre el modelo OSI y el Modelo TCP/IP

MOD

Con el
Cisco u
este m
importa
caracte

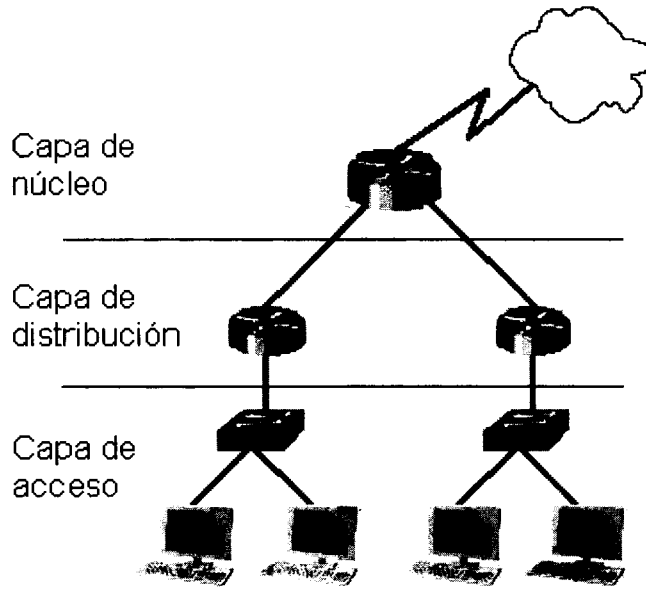
El mod

MODELO JERÁRQUICO

Con el fin de simplificar el diseño, implementación y administración de las redes, Cisco utiliza un modelo jerárquico para describir la red. Aunque la práctica de este método suele estar asociada con el proceso de diseño de una red, es importante comprender el modelo para poder determinar el equipo y características que van a necesitar en la red.

El modelo se compone de tres capas:

- ***Capa de acceso***
- ***Capa de distribución***
- ***Capa de núcleo***



Modelo Jerárquico de tres capas

RECUERDE:

TCP protocolo confiable de capa de transporte orientado a conexión
UDP protocolo **NO** confiable de capa de transporte **NO** orientado a conexión
Un protocolo Orientado a conexión es el que previamente establece un saludo antes de enviar los datos, como es el ejemplo de una llamada telefónica, donde se establece un saludo de tres vías. Un protocolo No orientado a conexión es el que no establece saludo previo antes de enviar los datos como es el caso de un envío postal donde se establece un saludo de dos vías

RECUERDE:

OSI	TCP/IP	PROTOCOLOS
APLICACIÓN PRESENTACIÓN SESIÓN	APLICACIÓN	TELNET, FTP, LPD, SNMP,TFTP, SMTP, NFS, X WINDOWS
TRANSPORTE	TRANSPORTE	TCP, UDP
RED	INTERNET	ICMP, BOOTP, ARP, RARP, IP
ENLACE DE DATOS FÍSICA	RED	ETHERNET, FAST-ETHERNET, TOKEN RING, FDDI

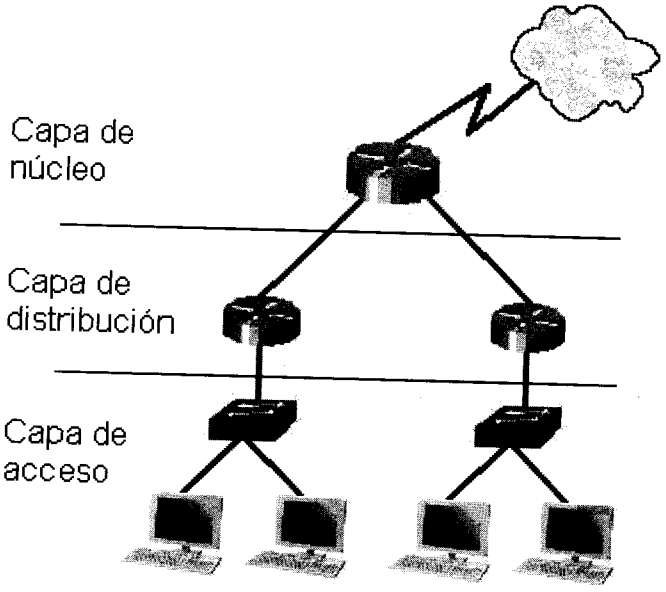
Comparativa entre el modelo OSI y el Modelo TCP/IP

MODELO JERÁRQUICO

Con el fin de simplificar el diseño, implementación y administración de las redes, Cisco utiliza un modelo jerárquico para describir la red. Aunque la práctica de este método suele estar asociada con el proceso de diseño de una red, es importante comprender el modelo para poder determinar el equipo y características que van a necesitar en la red.

El modelo se compone de tres capas:

- ***Capa de acceso***
- ***Capa de distribución***
- ***Capa de núcleo***



Modelo Jerárquico de tres capas

Capa de acceso

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red. Esta es la razón por la cual la capa de acceso se denomina a veces capa de puesto de trabajo, capa de escritorio o de usuario. Los usuarios así como los recursos a los que estos necesitan acceder con más frecuencia, están disponibles a nivel local. El tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales.

En la capa de acceso podemos encontrar múltiples grupos de usuarios con sus correspondientes recursos. En muchas redes no es posible proporcionar a los usuarios un acceso local a todos los servicios, como archivos de bases de datos, almacenamiento centralizado o acceso telefónico al Web. En estos casos, el tráfico de usuarios que demandan estos servicios se desvía a la siguiente capa del modelo: la capa de distribución.

Capa de distribución

La capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red. La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

En un entorno de campus, la capa de distribución abarca una gran diversidad de funciones, entre las que figuran las siguientes:

- Servir como punto de concentración para acceder a los dispositivos de capa de acceso.
- Enrutar el tráfico para proporcionar acceso a los departamentos o grupos de trabajo.
- Segmentar la red en múltiples dominios de difusión / multidifusión.
- Traducir los diálogos entre diferentes tipos de medios, como Token Ring y Ethernet.
- Proporcionar servicios de seguridad y filtrado.

La capa de distribución puede resumirse como la capa que proporciona una conectividad basada en una determinada política, dado que determina cuándo y cómo los paquete pueden acceder a los servicios principales de la red. La capa de distribución determina la forma más rápida para que la petición de un usuario (como un acceso al servidor de archivos) pueda ser remitida al servidor. Una vez que la capa de distribución ha elegido la ruta, envía la petición a la capa de núcleo. La capa de núcleo podrá entonces transportar la petición al servicio apropiado.

Capa de núcleo

La capa del núcleo, principal o Core se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos. Algunos de ellos pueden ser e-mail, el acceso a Internet o videoconferencia.

Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo. Este se limita a proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

RECUERDE:

CAPA	FUNCIONES	DISPOSITIVOS
NÚCLEO	Conmuta el tráfico hacia el servicio solicitado, comunicación rápida y segura	**ROUTERS, SWITCH MULTICAPA**
DISTRIBUCIÓN	Enrutamiento, filtrado, acceso WAN, seguridad basada en políticas, servicios empresariales, enrutamiento entre VLANS, definición de dominios de broadcast y multicast	**ROUTER**
ACCESO	Define Dominios de colisión, estaciones finales, ubicación de usuarios, servicios de grupos de trabajos, VLANS	**HUB, SWITCH**

Modelo jerárquico de tres capas

NÚMEROS BINARIOS

Los dispositivos emiten y reciben pulsos eléctricos o luminosos, estos pulsos poseen dos estados SÍ y NO, este sistema de dos signos se le llama binario, matemáticamente hablando un sistema binario está compuesto por dos estados de unos y ceros siendo por lo tanto una potencia en base 2. En informática llamamos bits a la unidad que tiene también dos estados, un byte es un grupo de ocho bits.

Un octeto o un bytes se expresa de la siguiente manera:

00000000

Cada uno de estos bits que componen el octeto posee dos estados, 1 y 0 obteniendo por lo tanto 256 estados con todas las combinaciones posibles.

00000000
00000001
00000010
00000011
00000100
.....
01111111
11111111

Para que estos bytes sean más entendibles conviene que los traslademos al modo decimal al que estamos más acostumbrados cotidianamente por lo tanto si son potencias de 2, su valor será:

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

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$

Los bits que resulten iguales a 1 tendrán el valor correspondiente a esa potencia, mientras que los que permanezcan en 0 tendrán un valor igual a cero, finalmente se suma el conjunto de los decimales resultantes y se obtiene el equivalente en decimal.

Ejemplo:

0000001 (en binario) = 0000002^0 (en decimal) = 1
(0+0+0+0+0+0+0+1)

01001001 (en binario) = $02^5002^3002^0$(en decimal) = 73
(0+64+0+0+8+0+0+1)

Para pasar de decimal a binario podemos utilizar la siguiente técnica:

Número decimal a convertir a binario 195

128	entra en **195**?	**SÍ**, le resto 128 a 195=67
64	entra en **67**?	**SÍ**, le resto 64 a 67=3
32	entra en **3**?	**NO**, siguiente
16	entra en **3**?	**NO**, siguiente
8	entra en **3**?	**NO**, siguiente
4	entra en **3**?	**NO**, siguiente
2	entra en **3**?	**SÍ**, le resto 2 a 3=1
1	entra en **1**?	**SÍ**

Donde los **SÍ** equivalen al valor binario **UNO** y los **NO** al valor binario **CERO**

Por lo tanto 195 es equivalente en binario a 11000011

NÚMEROS HEXADECIMALES

Los números hexadecimales se basan en potencias de 16, utilizando símbolos alfanuméricos, la siguiente tabla le ayudará a convertir números hexadecimales en binarios o en decimales:

NÚMERO DECIMAL	NÚMERO HEXADECIMAL	NÚMERO BINARIO
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Tabla de conversión decimal, hexadecimal y binario

Siguiendo el ejemplo anterior el número **195** es igual al número binario:

11000011

Divida este octeto en dos grupos de cuatro, **1100 0011**

Busque el valor correspondiente en la tabla de estos dos grupos de bits,
Al número binario **1100** le corresponde el número hexadecimal **C**
Al número binario **0011** le corresponde el número hexadecimal **3**

Por lo tanto **195** es igual a **11000011** en binario y al **C3** en hexadecimal. Para que no existan confusiones los números hexadecimales se identifican con un **0x** adelante, en este caso **0xC3**

El proceso inverso será si tenemos el número hexadecimal **0xAE** donde

A es igual a **1010**
E es igual a **1110**

Por lo tanto **0xAE** es igual el número binario **10101110** si convertimos este número a decimal

$$2^7+0+2^5+0+2^3+2^2+2^1+0 = 174$$

RECUERDE:

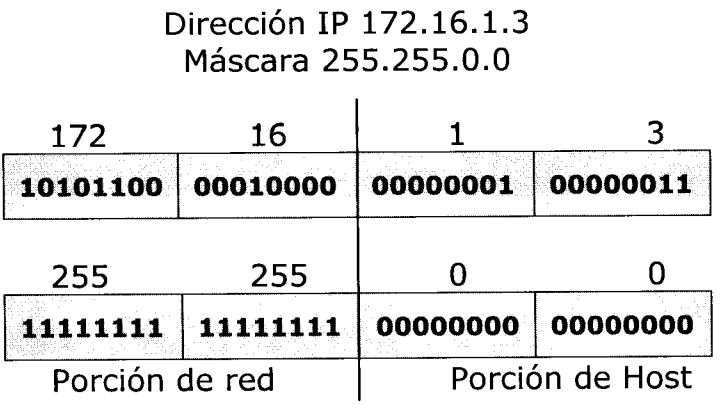
Existen varias técnicas para hacer conversiones de un sistema numérico a otro, un matemático, un físico o un informático podrían utilizar diferentes métodos de conversión con iguales resultados. El estudiante podrá utilizar el método que crea más conveniente según su propio criterio.

DIRECCIONAMIENTO IP

Para que dos dispositivos se comuniquen entre sí, es necesario poder identificarlos claramente. Una dirección IP es una secuencia de unos y ceros de 32 bits. Para hacer más comprensible el direccionamiento, una dirección IP aparece escrita en forma de cuatro números decimales separados por puntos. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros. Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.

Una dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red. Este tipo de dirección recibe el nombre de **dirección jerárquica** porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la del host, identifica qué máquina en particular de la red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones llamadas privadas para uso interno que no veremos en Internet. Las direcciones de clase D son de uso multicast y las de clase E, experimentales.



Ejemplo de una dirección IP

Clases de direccionamiento IP

Direccionamiento **Clase A:**

Rango de direcciones IP **1.0.0.0** a **127.0.0.0**
Máscara de red **255.0.0.0**

Direcciones privadas **10.0.0.0** a **10.255.255.255**

Direccionamiento **Clase B:**

Rango de direcciones IP: **128.0.0.0** a **191.255.0.0**
Máscara de red: **255.255.0.0**

Direcciones privadas **172.16.0.0** a **172.31.255.255**

Direccionamiento **Clase C:**

Rango de direcciones IP: **192.0.0.0** a **223.255.255.0**
Máscara de red: **255.255.255.0**

Direcciones privadas **192.168.0.0** a **192.168.255.255**

Direccionamiento **Clase D:**

Rango de direcciones IP: **224.0.0.0** a **239.255.255.255**
Uso multicast o multidifusión

Direccionamiento **Clase E:**

Rango de direcciones IP: **240.0.0.0** a **254.255.255.255**
Uso experimental o científico

La dirección **127.0.0.1** es llamada Dirección de loopback o interfaz virtual. La máscara **255.255.255.255** es llamada máscara de nodo y se utiliza para identificar un host específico.

En números binarios:

*Las clases **A** comienzan con **00**xxxxxx*
*Las clases **B** comienzan con **10**xxxxxx*
*Las clases **C** comienzan con **11**xxxxxx*
*Las clases **D** comienzan con **111**xxxxx*
*Las clases **E** comienzan con **1111**xxxx*

Dirección de broadcast

Existe un direccionamiento particular cuando los bits están todos en UNOS llamada dirección de broadcast, o de difusión. Este direccionamiento particular no debe utilizarse para identificar a los host. Una cantidad excesiva de estas difusiones provocará una tormenta de broadcast que hará ineficiente el uso de la red, consumiendo gran cantidad de ancho de banda y haciendo que los host utilicen demasiados recursos al estar "obligados" a leer esos paquetes ya que están dirigidos a todos los host que integran ese **Dominio de Broadcast**.

SUBREDES

Las redes se pueden dividir en redes más pequeñas, para el mayor aprovechamiento de las mismas, que llamaremos **subredes**, además de contar con esta flexibilidad, la división en subredes permite que el administrador de la red brinde contención de broadcast y seguridad de bajo nivel en la LAN. La división en subredes, además, ofrece seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un Router. Las clases de direcciones IP disponen de 256 a 16,8 millones de Hosts según su clase.

El proceso de creación de subredes comienza pidiendo "prestado" al rango de host la cantidad de bits necesaria para la cantidad subredes requeridas. Se debe tener especial cuidado en esta acción de pedir ya que deben quedar como mínimo dos bits del rango de host.

La máxima cantidad de bits disponibles para este propósito depende del tipo de clase:

- **Clase A** cantidad disponible **22** bits
- **Clase B** cantidad disponible **14** bits
- **Clase C** cantidad disponible **6** bits

Cada bit que se toma del rango de host posee dos estados **0** y **1** por lo tanto si se toman tres bit existirán 8 estados diferentes:

BITS PRESTADOS	BITS DE HOST	VALOR DECIMAL
000	00000	0
001	00000	32
010	00000	64
011	00000	96
100	00000	128
101	00000	160
110	00000	192
111	00000	224

El número de subredes que se puede usar es igual a: 2 elevado a la potencia del número de bits asignados a subred, menos 2. La razón de restar estos dos bits es por las direcciones que identifican a la red original, la **000** y la dirección de broadcast de esta subred, la **111** según el ejemplo anterior, que no se utilizarán.

$$2^N-2=\text{Número de subredes}$$

Donde **N** es la cantidad de bits tomados al rango de host

Por lo tanto si se quiere crear 5 subredes **VÁLIDAS** (preste atención al término validas), es decir cumpliendo la formula 2^N-2 tendrá que tomar del rango de host 3 bits:

$$2^3-2=6$$

*Observe que no siempre el resultado es exacto,
en este caso se pedían 5 subredes pero se obtendrán 6

Procedimiento para la creación de subredes

Paso 1-Piense en binarios.

Paso 2-Encuentre la máscara adecuada para la cantidad de subredes que le solicitan, independientemente de la dirección IP lo que nos importa es la clase de red.

Razone, red clase C, el primer octeto, el segundo y el tercero corresponden a la dirección de red por lo tanto trabaje con el cuarto octeto correspondiente a los host. De izquierda a derecha tome la cantidad de bits necesarios de la máscara para la cantidad de subredes que le solicitan:

Crear **10 subredes** a partir de una red clase **C**

Máscara de red 255.255.255.0

Rango de red Rango de host
11111111.11111111.11111111.00000000

Cuarto octeto **00000000**
11110000

Según la formula 2^N-2 debemos tomar 4 bits del rango de host, por lo tanto:

$$2^4-2=16-2=14$$

Recuerde que no siempre los valores son exactos

Coloque en **1** (uno) los bits que resultaron de la operación anterior y súmelos, recuerde el valor de cada bit dentro del octeto: 128, 64, 32, 16, 8, 4, 2, 1

Se obtiene:

11110000
128+64+32+16=240

La máscara de subred de clase C para obtener 10 subredes válidas es:

255.255.255.240

Paso 3- Identifique las correspondientes direcciones IP de las subredes restando a 256, que es la cantidad máxima de combinaciones que tiene un octeto, el valor de la máscara obtenida. Este número será la dirección de la primera subred utilizable que a su vez es el incremento o la constante para determinar las siguientes subredes.

256
240
016

El resultado indica la primera dirección valida de subred

NÚMERO DE SUBRED	VALOR DEL OCTETO	VALOR DECIMAL
0	00000000	0
1	00010000	16
2	00100000	32
3	00110000	48
4	01000000	64
5	01010000	80
6	01100000	96
7	01110000	112
8	10000000	128
9	10010000	144
10	10100000	160
11	10110000	176
12	11000000	192
13	11010000	208
14	11100000	224
15	11110000	240

El incremento constante en este caso será de 16

Paso 3- Identifique las correspondientes direcciones IP de las subredes restando a 256, que es la cantidad máxima de combinaciones que tiene un octeto, el valor de la máscara obtenida. Este número será la dirección de la primera subred utilizable que a su vez es el incremento o la constante para determinar las siguientes subredes.

_256
240
016

El resultado indica la primera dirección valida de subred

NÚMERO DE SUBRED	VALOR DEL OCTETO	VALOR DECIMAL
0	00000000	0
1	00010000	16
2	00100000	32
3	00110000	48
4	01000000	64
5	01010000	80
6	01100000	96
7	01110000	112
8	10000000	128
9	10010000	144
10	10100000	160
11	10110000	176
12	11000000	192
13	11010000	208
14	11100000	224
15	11110000	240

El incremento constante en este caso será de 16

Paso 4-Obtenga las direcciones IP de las Subredes (observe el cuadro anterior).

Dirección IP de la red original: 192.168.1.0 255.255.255.0

Dirección IP de la 1º subred: 192.168.1.16 255.255.255.240
Dirección IP de la 2º subred: 192.168.1.32 255.255.255.240
Dirección IP de la 3º subred: 192.168.1.48 255.255.255.240
Dirección IP de la 4º subred: 192.168.1.64 255.255.255.240
.....

Dirección IP de la 13º subred: 192.168.1.208 255.255.255.240
Dirección IP de la 14º subred: 192.168.1.224 255.255.255.240

Otra forma de identificar las máscaras es sumar los bits en uno y colocarlos detrás de la dirección IP separados por una barra:

Dirección IP de la red original: 192.168.1.0/24
Dirección IP de la 1º subred: 192.168.1.16/28
Dirección IP de la 2º subred: 192.168.1.32/28
Dirección IP de la 3º subred: 192.168.1.48/28
Dirección IP de la 4º subred: 192.168.1.64/28
.....

Dirección IP de la 13º subred: 192.168.1.208/28
Dirección IP de la 14º subred: 192.168.1.224/28

RECUERDE:

La dirección de subred 0 no se utiliza por ser el ID de la red, y la última, en este caso 240, tampoco por ser la dirección de broadcast. Si bien los routers permiten la utilización de la subred 0 por medio de comandos por el momento descartaremos la primera y la última.

Paso 5- Identifique el rango de Host que integran las subredes.
Hasta ahora hemos trabajado con los bits del rango de red, es decir de izquierda a derecha en el octeto correspondiente, ahora lo haremos con los bits restantes del rango de host, es decir de derecha a izquierda.

Tomemos como ejemplo la subred 196.168.1.16/28 y apliquemos la fórmula $\mathbf{2^N-2}$, nos han quedado 4 bits libres por lo tanto: $\mathbf{2^4-2=16-2=14}$. Estas subredes tendrán 14 host validos utilizables cada una.

NÚMERO DE HOST	VALOR DEL OCTETO	VALOR DECIMAL
	00010000	SUBRED
1	00010001	17
2	00010010	18
3	00010011	19
4	00010100	20
5	00010101	21
6	00010110	22
7	00010111	23
8	00011000	24
9	00011001	25
10	00011010	26
11	00011011	27
12	00011100	28
13	00011101	29
14	00011110	30
15	00011111	BROADCAST

El Rango de Host válido para la subred 192.168.1.16/28 será:

192.168.1.17
al
192.168.1.30

El mismo procedimiento se lleva a cabo con el resto de las subredes:

Nº DE SUBRED	RANGO DE HOST VÁLIDOS	BROADCAST
192.168.1.16	17 AL 30	31
192.168.1.32	31 AL 62	63
192.168.1.64	65 AL 78	79
192.168.1.80	81 AL 94	95
192.168.1.96	97 AL 110	111
.....	.....	.....
192.169.1.224	225 AL 238	239

RECUERDE:

La dirección de broadcast de una subred será la inmediatamente inferior a la subred siguiente.

RECUERDE:

Paso 1

Piense en binarios.

Paso 2

Encuentre la máscara contando de izquierda a derecha los bits que tomará prestados del rango de host. Cada uno tendrá dos estados, un bit dos subredes, dos bits cuatro subredes, tres bits ocho subredes....

Paso 3

Reste a 256 la suma de los bit que ha tomado en el paso anterior para obtener la primer subred válida que a su vez será el incremento.

Paso 4

Obtenga las direcciones IP de las subredes siguientes sumando a la primera subred el incremento para obtener la segunda, luego a la segunda más el incremento para obtener la tercera y así hasta la última.

Paso 5

Identifique el rango de host y la correspondiente dirección de broadcast de cada subred.

RECUERDE:

Clase A:

RED	MÁSCARA DE RED			
10	255	0	0	0

Clase B:

RED		MÁSCARA DE RED			
172	16	255	255	0	0

Clase C:

RED			MÁSCARA DE RED			
192	168	0	255	255	255	0

RECUERDE:

Las diferentes clases de redes se pueden identificar fácilmente en números binarios observando el comienzo del primer octeto, puesto que:

*Las clases **A** comienzan con **00**xxxxxx*
*Las clases **B** comienzan con **10**xxxxxx*
*Las clases **C** comienzan con **11**xxxxxx*
*Las clases **D** comienzan con **111**xxxxx*
*Las clases **E** comienzan con **1111**xxxx*