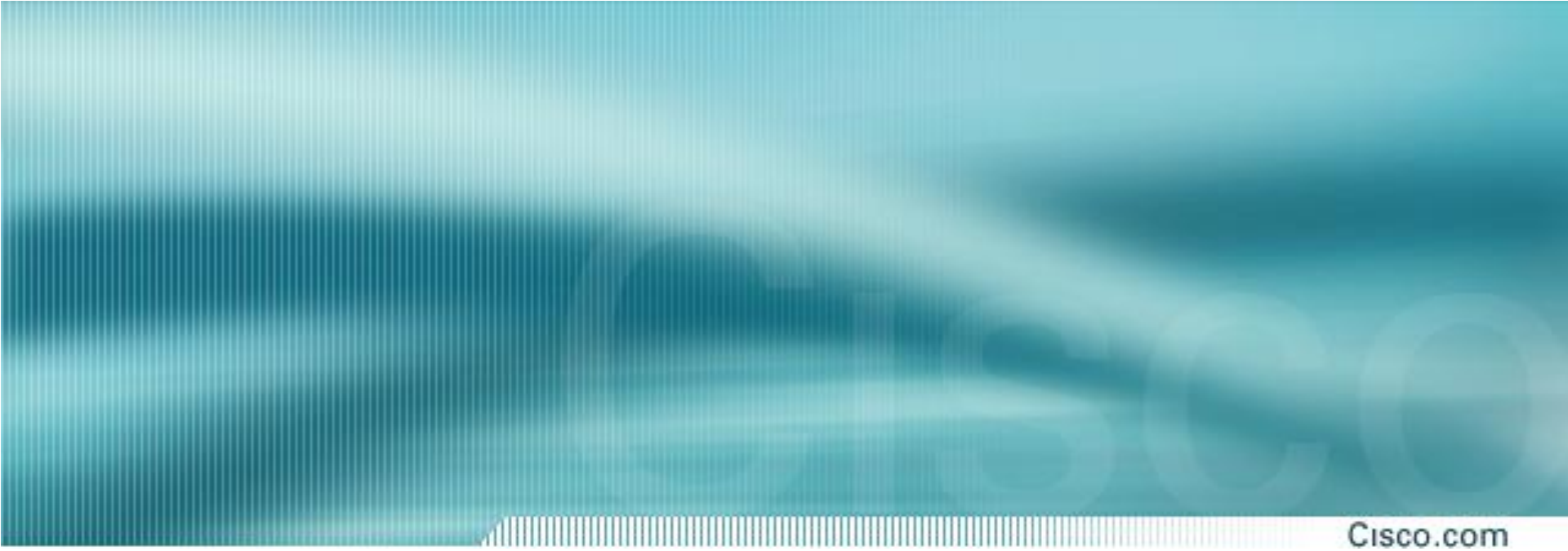


CCNA 1 v3.0 Módulo 10 Principios básicos de enrutamiento y subredes

Docente: Mg. Robert Romero Flores

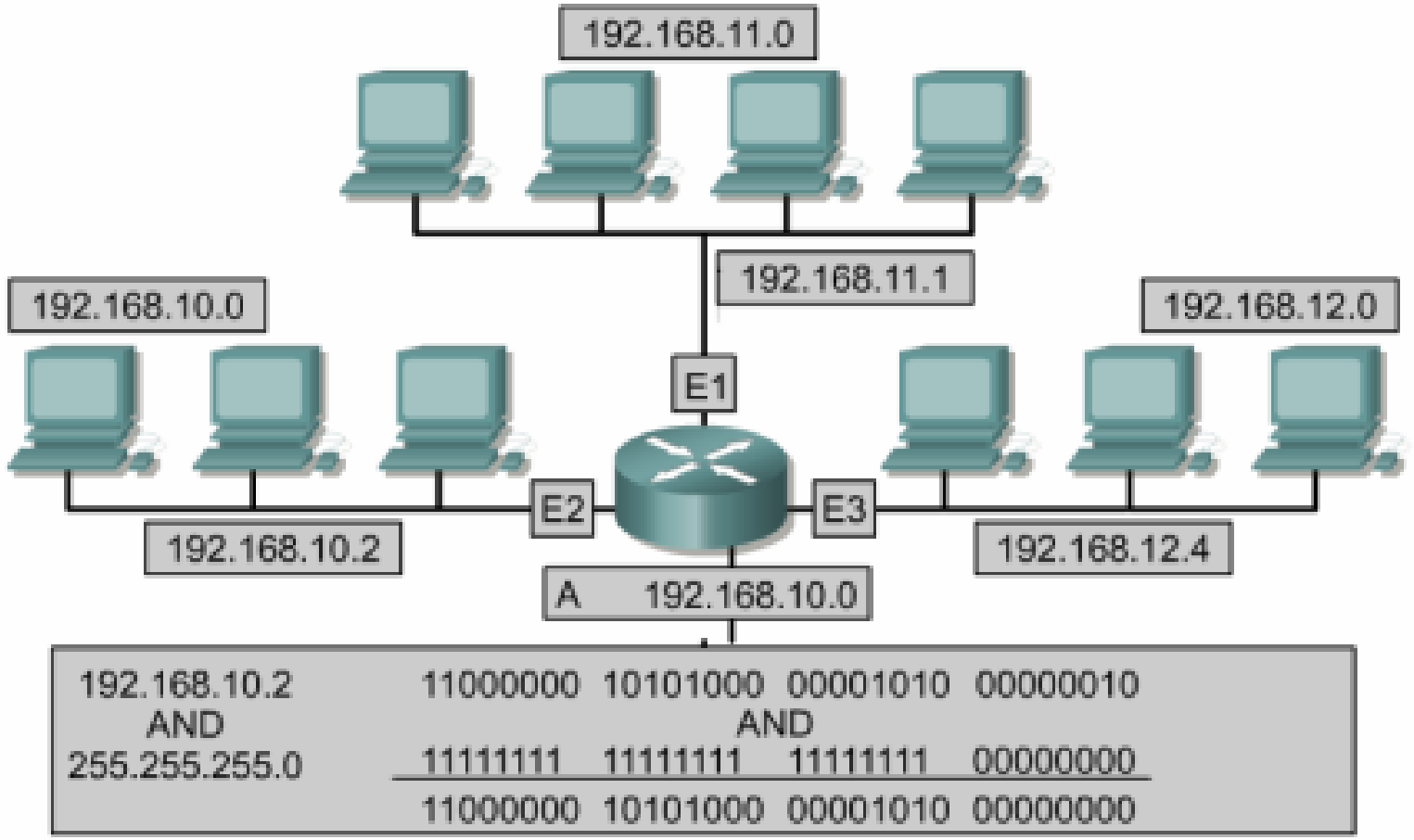
Objetivos

- **Los estudiantes que completen este módulo deberán poder:**
- **Describir los protocolos enrutados (enrutables)**
- **Enumerar los pasos del encapsulamiento de datos en una internetwork a medida que los datos se enrutan a uno o más dispositivos de Capa 3.**
- **Describir la entrega no orientada a conexión y orientada a conexión.**
- **Nombrar los campos de los paquetes IP.**
- **Describir el proceso de enrutamiento.**
- **Comparar y contrastar los diferentes tipos de protocolos de enrutamiento.**
- **Enumerar y describir las distintas métricas utilizadas por los protocolos de enrutamiento.**
- **Enumerar varios usos de la división en subredes.**
- **Determinar las máscaras de subred para una situación determinada.**
- **Utilizar máscaras de subred para determinar el ID de subred.**

Protocolo enrutado

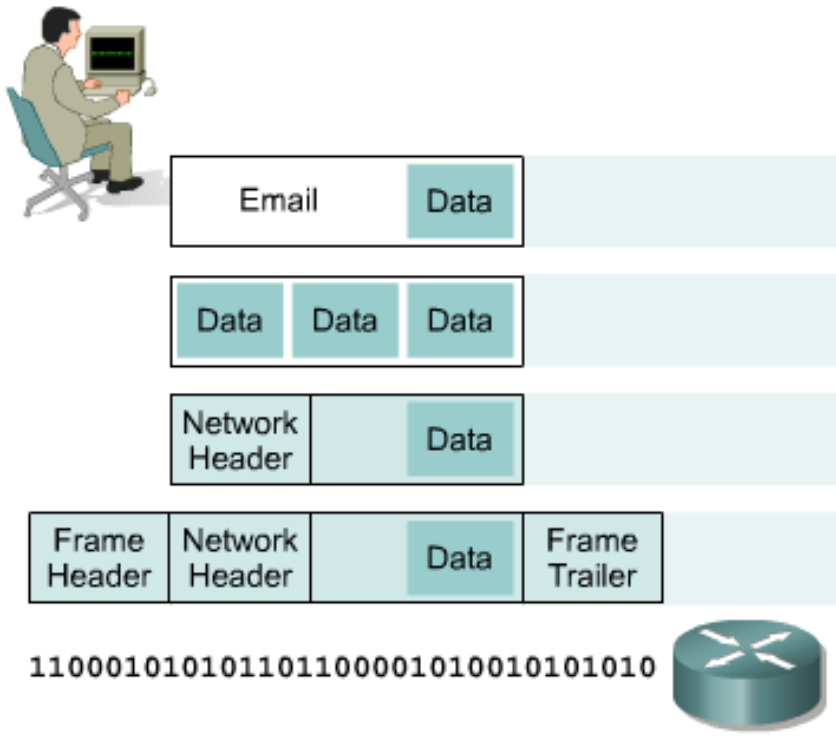
Protocolos enrutables y enrutados

- **Un protocolo es un conjunto de reglas que determina cómo se comunican los computadores entre sí a través de las redes. Los computadores se comunican intercambiando mensajes de datos. Para aceptar y actuar sobre estos mensajes, los computadores deben contar con definiciones de cómo interpretar el mensaje. Los ejemplos de mensajes incluyen aquellos que establecen una conexión a una máquina remota, mensajes de correo electrónico y archivos que se transmiten en la red.**
- **Un protocolo describe lo siguiente:**
- **El formato al cual el mensaje se debe conformar**
- **La manera en que los computadores intercambian un mensaje dentro del contexto de una actividad en particular Un protocolo enrutado permite que un Router envíe datos entre nodos de diferentes redes. Para que un protocolo sea enrutable, debe admitir la capacidad de asignar a cada dispositivo individual un número de red y uno de Host. Algunos protocolos como los IPX, requieren sólo de un número de red porque estos protocolos utilizan la dirección MAC del Host como número de Host. Otros protocolos, como el IP, requieren una dirección completa que especifique la porción de red y la porción de Host. Estos protocolos también necesitan una máscara de red para diferenciar estos dos números. La dirección de red se obtiene al realizar la operación "AND" con la dirección y la máscara de red.**

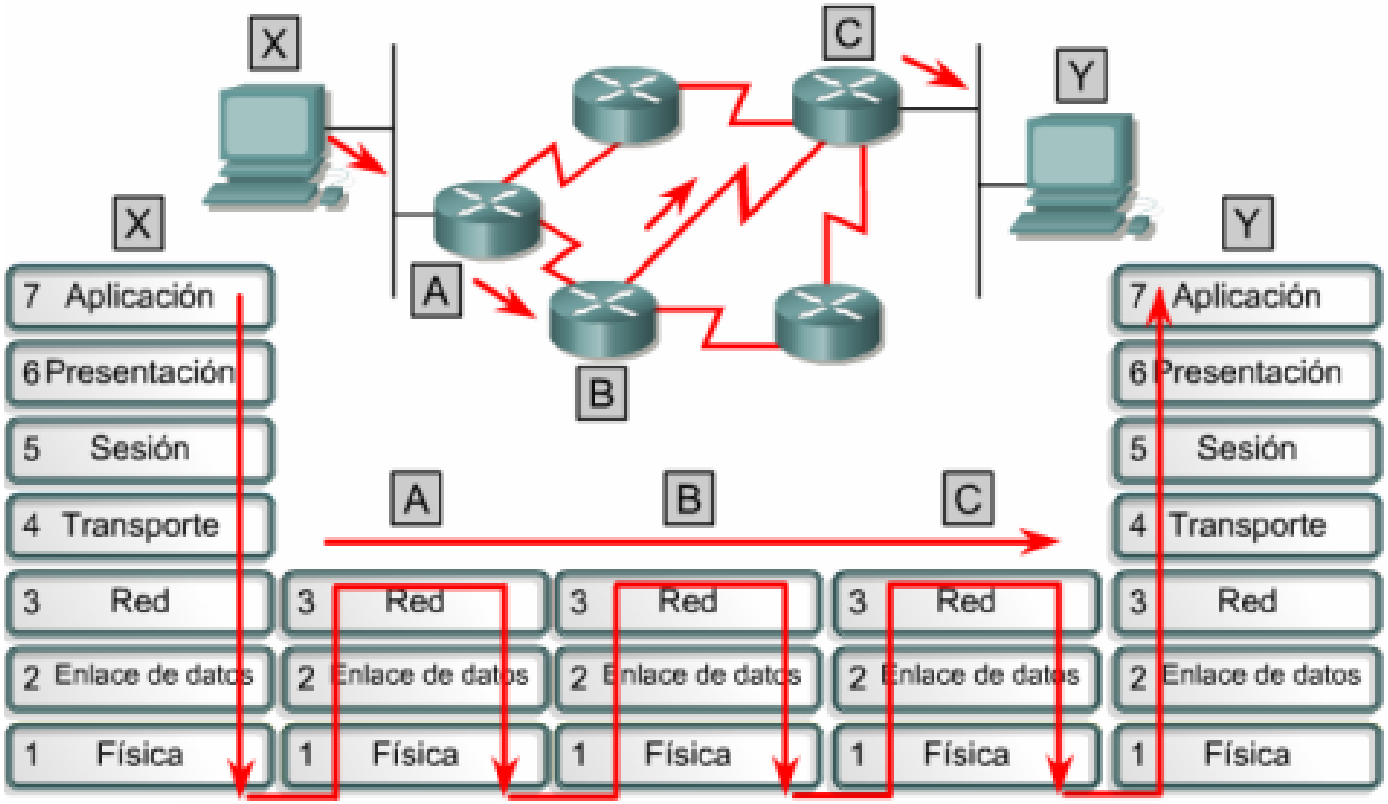


IP como protocolo enrutado

- **El Protocolo Internet (IP) es la implementación más popular de un esquema de direccionamiento de red jerárquico. IP es un protocolo de entrega no orientado a la conexión, poco confiable y de máximo esfuerzo. El término no orientado a la conexión significa que no se establece ningún circuito de conexión dedicado antes de la transmisión, como sí lo hay cuando se establece una comunicación telefónica. IP determina la ruta más eficiente para los datos basándose en el protocolo de enrutamiento. Los términos poco confiables y de máximo esfuerzo no implican que el sistema no sea confiable y que no funcione bien; más bien significan que IP no verifica que los datos lleguen a su destino. La verificación de la entrega no siempre se lleva a cabo**



Propagación y conmutación de los paquetes dentro del Router



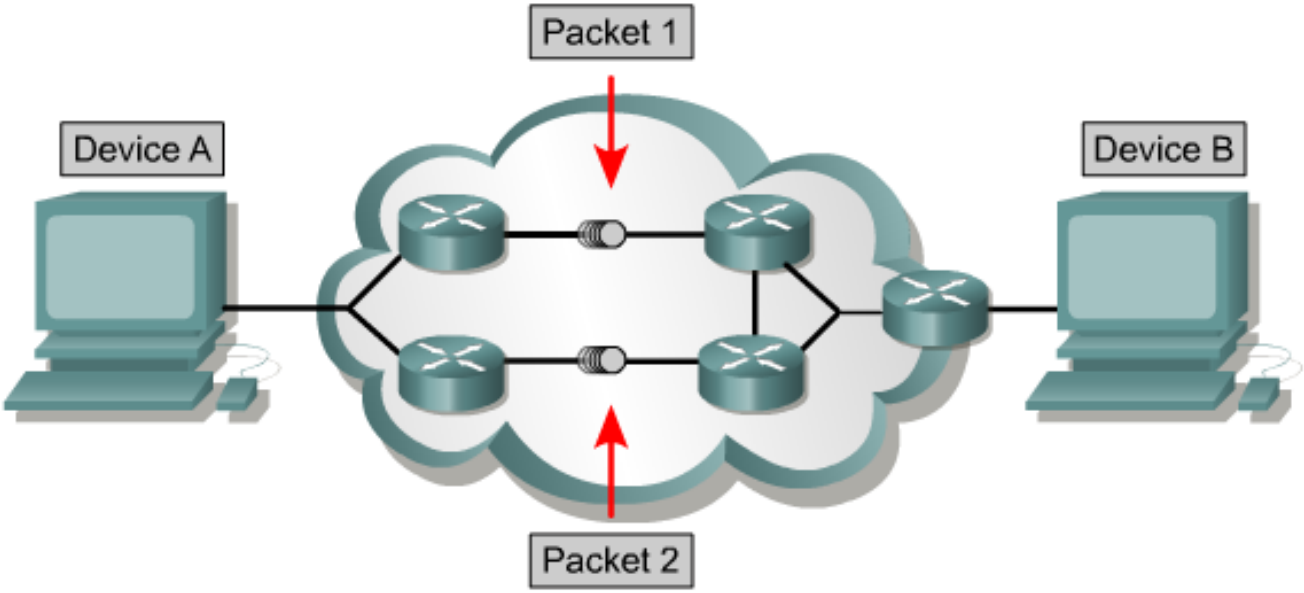
Cada router ofrece sus servicios para admitir las funciones de las capas superiores.

Propagación y conmutación de los paquetes dentro del Router

- **Las tramas de Ethernet de Capa 2 están diseñadas para operar dentro de un dominio de broadcast utilizando la dirección MAC que está grabada en del dispositivo físico. Otros tipos de tramas de Capa 2 incluyen los enlaces seriales del protocolo punto a punto (PPP) y las conexiones de Frame Relay, que utilizan esquemas de direccionamiento de Capa 2 diferentes. No obstante el tipo de direccionamiento de Capa 2 utilizado, las tramas están diseñadas para operar dentro del dominio de broadcast de Capa 2, y cuando los datos atraviesan un dispositivo de Capa 3, la información de Capa 2 cambia.**
- **En el momento en que se recibe una trama en la interfaz del Router, se extrae la dirección MAC destino. Se revisa la dirección para ver si la trama se dirige directamente a la interfaz del Router, o si es un broadcast. En cualquiera de los dos casos se acepta la trama. De lo contrario, se descarta la trama ya que está destinada a otro dispositivo en el dominio de colisión. Se extrae la información de verificación por redundancia cíclica (CRC) de la información final de la trama aceptada, y la CRC se calcula para verificar**
- **que los datos de la trama no tengan errores. La trama se descarta si está dañada. Si la verificación es válida, el encabezado de la trama y la información final se descartan y el paquete pasa hacia arriba a la Capa 3. Allí se verifica el paquete para asegurar que esté realmente destinado al Router, o si tiene que ser enrutado a otro dispositivo en la internetwork. Si la dirección IP destino concuerda con uno de los puertos del Router, se elimina el encabezado de Capa 3 y los datos pasan a la Capa 4. Si es necesario enrutar el paquete, se comparará la dirección IP destino con la tabla de enrutamiento. Si se encuentra una concordancia o si hay una ruta por defecto, el paquete se enviará a la interfaz especificada en la sentencia de concordancia de la tabla de enrutamiento. Cuando el paquete se conmuta a la interfaz de salida, se agrega un nuevo valor de verificación CRC como información final de la trama, y se agrega el encabezado de trama apropiado al paquete. Entonces la trama se transmite al siguiente dominio de broadcast en su viaje hacia el destino final.**

Protocolo Internet (IP)

- **Existen dos tipos de servicios de envío: los no orientados a conexión y los orientados a conexión. Estos dos servicios son los que realmente permiten el envío de datos de extremo a extremo en una internetwork.**
- **La mayoría de los servicios utilizan sistemas de entrega no orientados a conexión. Es posible que los diferentes paquetes tomen distintas rutas para transitar por la red, pero se reensamblan al llegar a su destino. En un sistema no orientado a conexión, no se comunica con el destino antes de enviar un paquete Una buena comparación para un sistema no orientado a conexión es el sistema postal. No se comunica con el destinatario para ver si aceptará la carta antes de enviarla. Además, el remitente nunca sabe si la carta llegó a su destino.**

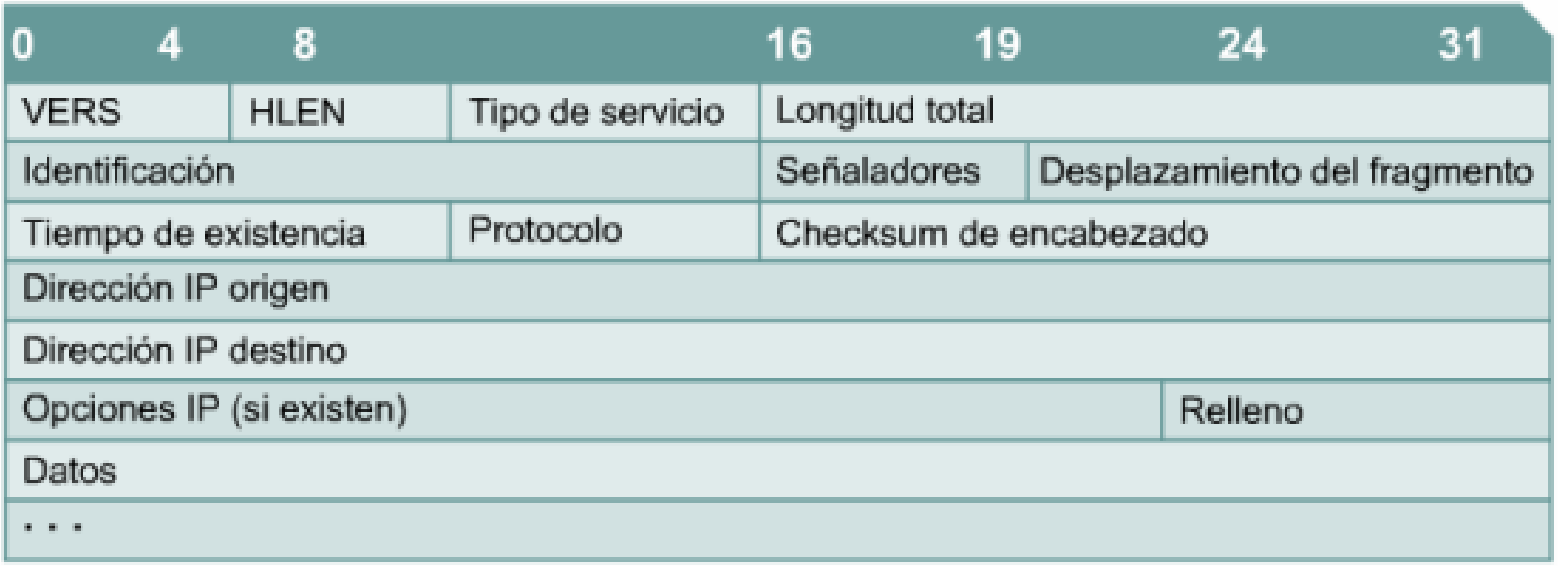


Anatomía de un paquete IP

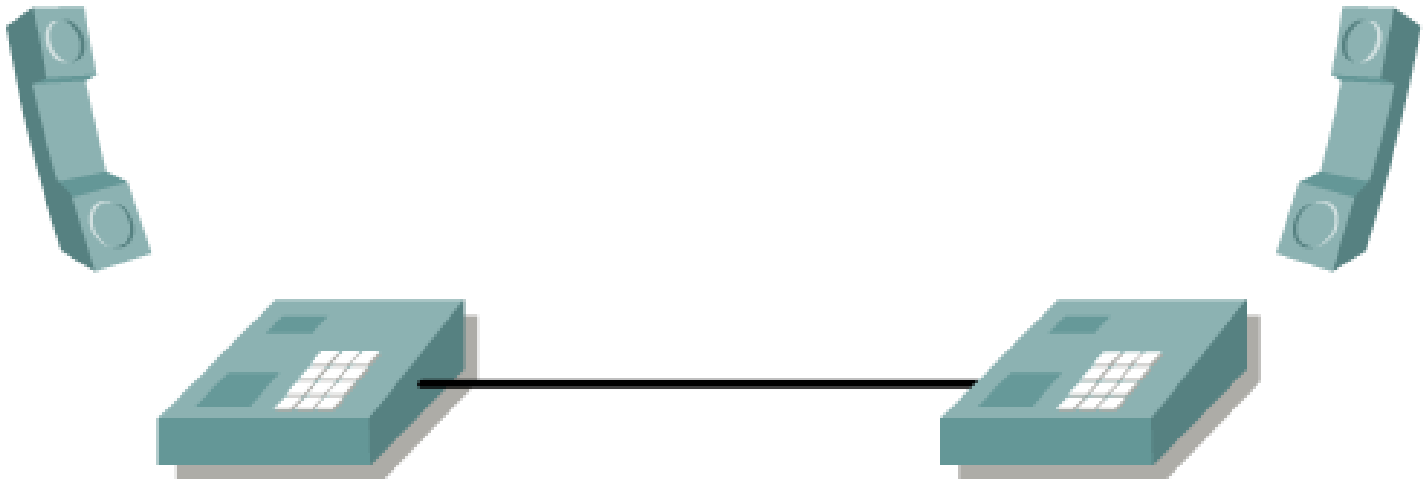
- **Versión: Especifica el formato del encabezado de IP. Este campo de cuatro bits contiene el número 4 si el encabezado es IPv4 o el número 6 si el encabezado es IPV6. Sin embargo este campo no se usa para distinguir entre ambas versiones, para esto se usa el campo de tipo que se encuentra en el encabezado de la trama de capa 2.**
- **Longitud del encabezado IP (HLEN): Indica la longitud del encabezado del datagrama en palabras de 32 bits. Este número representa la longitud total de toda la información del encabezado, e incluye los dos campos de encabezados de longitud variable.**
- **Tipo de servicio (TOS): Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular, 8 bits.**
- **Longitud total: Especifica la longitud total de todo el paquete en bytes, incluyendo los datos y el encabezado, 16 bits. Para calcular la longitud de la carga de datos reste HLEN a la longitud total.**
- **Identificación: Contiene un número entero que identifica el datagrama actual, 16 bits. Este es el número de secuencia.**
- **Señaladores: Un campo de tres bits en el que los dos bits de menor peso controlan la fragmentación. Un bit especifica si el paquete puede fragmentarse, y el otro especifica si el paquete es el último fragmento en una serie de paquetes fragmentados.**

Anatomía de un paquete IP

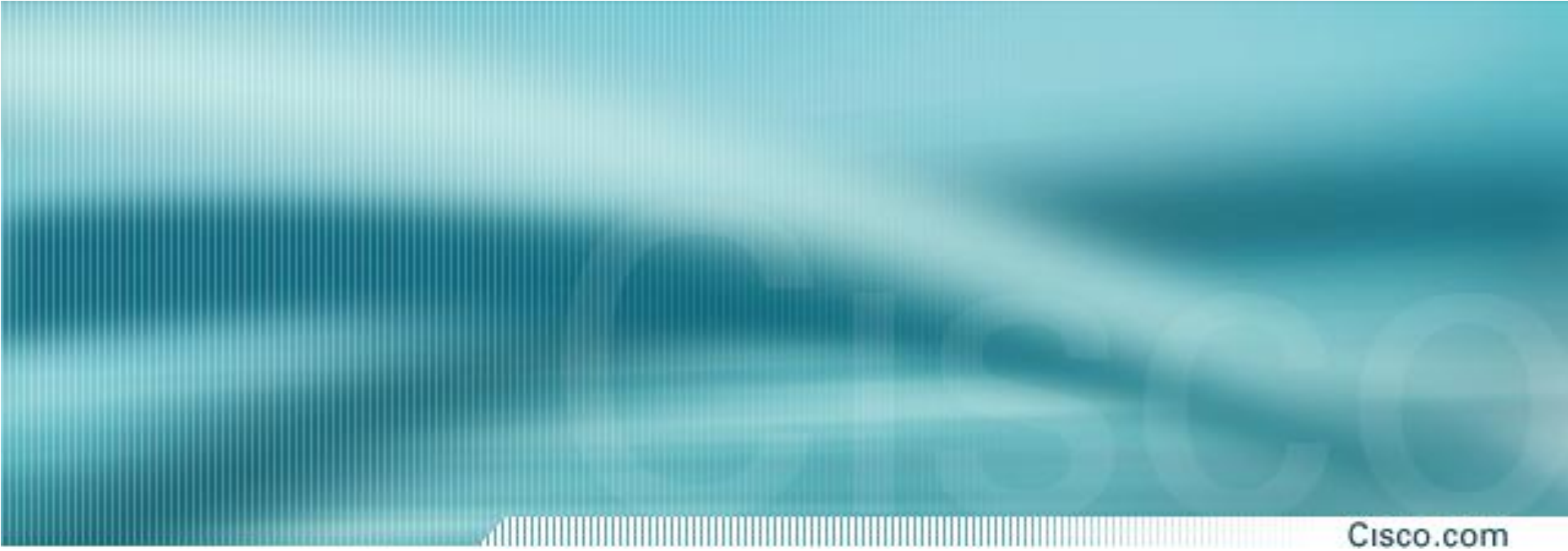
- **Desplazamiento de fragmentos: usado para ensamblar los fragmentos de datagramas, 13 bits.**
- **Este campo permite que el campo anterior termine en un límite de 16 bits.**
- **Tiempo de existencia (TTL): campo que especifica el número de saltos que un paquete puede**
- **recorrer. Este número disminuye por uno cuando el paquete pasa por un Router. Cuando el contador llega a cero el paquete se elimina. Esto evita que los paquetes entren en un loop (bucle) interminable.**
- **Protocolo: indica cuál es el protocolo de capa superior, por ejemplo, TCP o UDP, que recibe el paquete entrante luego de que se ha completado el procesamiento IP, ocho bits.**
- **Checksum del encabezado: ayuda a garantizar la integridad del encabezado IP, 16 bits.**
- **Dirección de origen: especifica la dirección IP del nodo emisor, 32 bits.**
- **Dirección de destino: especifica la dirección IP del nodo receptor, 32 bits.**
- **Opciones: permite que IP admita varias opciones, como seguridad, longitud variable.**
- **Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits**
- **Datos: contiene información de capa superior, longitud variable hasta un de máximo 64 Kb.**



Llamadas telefónicas: Orientadas a la Conexión



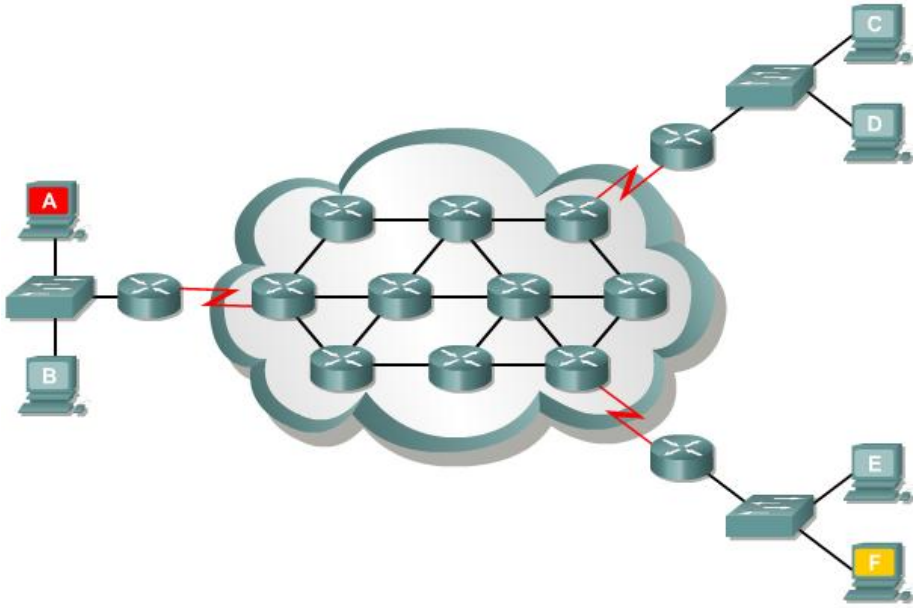
Se establece una conexión entre el emisor y receptor antes que se transfieran los datos.



Protocolos de enrutarniento IP

Descripción del enrutamiento

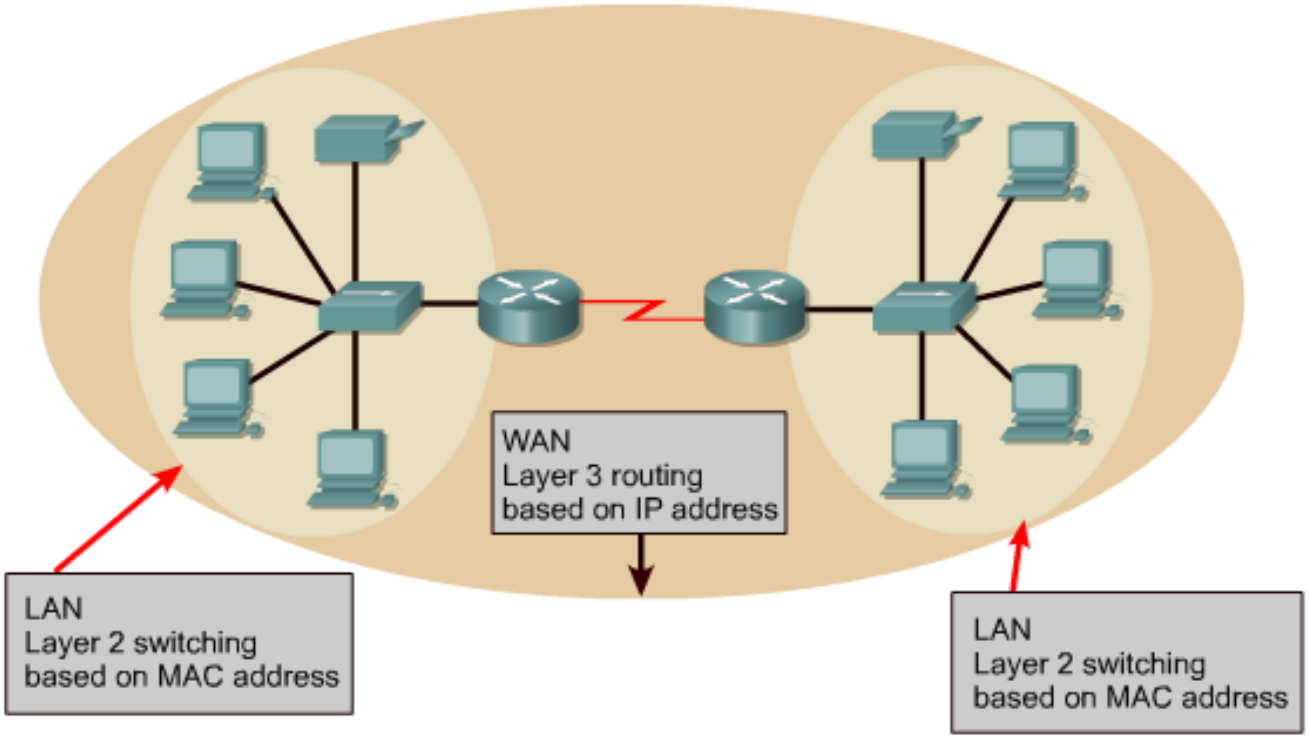
- **La función de enrutamiento es una función de la Capa 3 del modelo OSI. El enrutamiento es un esquema de organización jerárquico que permite que se agrupen direcciones individuales. Estas direcciones individuales son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos. El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro.**
- **El dispositivo primario que realiza el proceso de enrutamiento es el Router.**



- **Las siguientes son las dos funciones principales de un Router:**
- **Los Routers deben mantener tablas de enrutamiento y asegurarse de que otros Routers conozcan las modificaciones a la topología de la red. Esta función se lleva a cabo utilizando un protocolo de enrutamiento para comunicar la información de la red a otros Routers.**
- **Cuando los paquetes llegan a una interfaz, el Router debe utilizar la tabla de enrutamietno para establecer el destino. El Router envía los paquetes a la interfaz apropiada, agrega la información de entramado necesaria para esa interfaz, y luego transmite la trama.**
- **Un Router es un dispositivo de la capa de red que usa una o más métricas de enrutamiento para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Las métricas de enrutamiento son valores que se utilizan para determinar las ventajas de una ruta sobre otra. Los protocolos de enrutamiento utilizan varias combinaciones de métricas para determinar la mejor ruta para los datos.**

El enrutamiento en comparación con la conmutación

- **A menudo, se compara el enrutamiento con la conmutación. Un observador inexperto puede pensar que el enrutamiento y la conmutación cumplen la misma función. La diferencia básica es que la conmutación tiene lugar en la Capa 2, o sea, la capa de enlace de los datos, en el modelo OSI y el enrutamiento en la Capa 3. Esta diferencia significa que el enrutamiento y la conmutación usan información diferente en el proceso de desplazar los datos desde el origen al destino.**

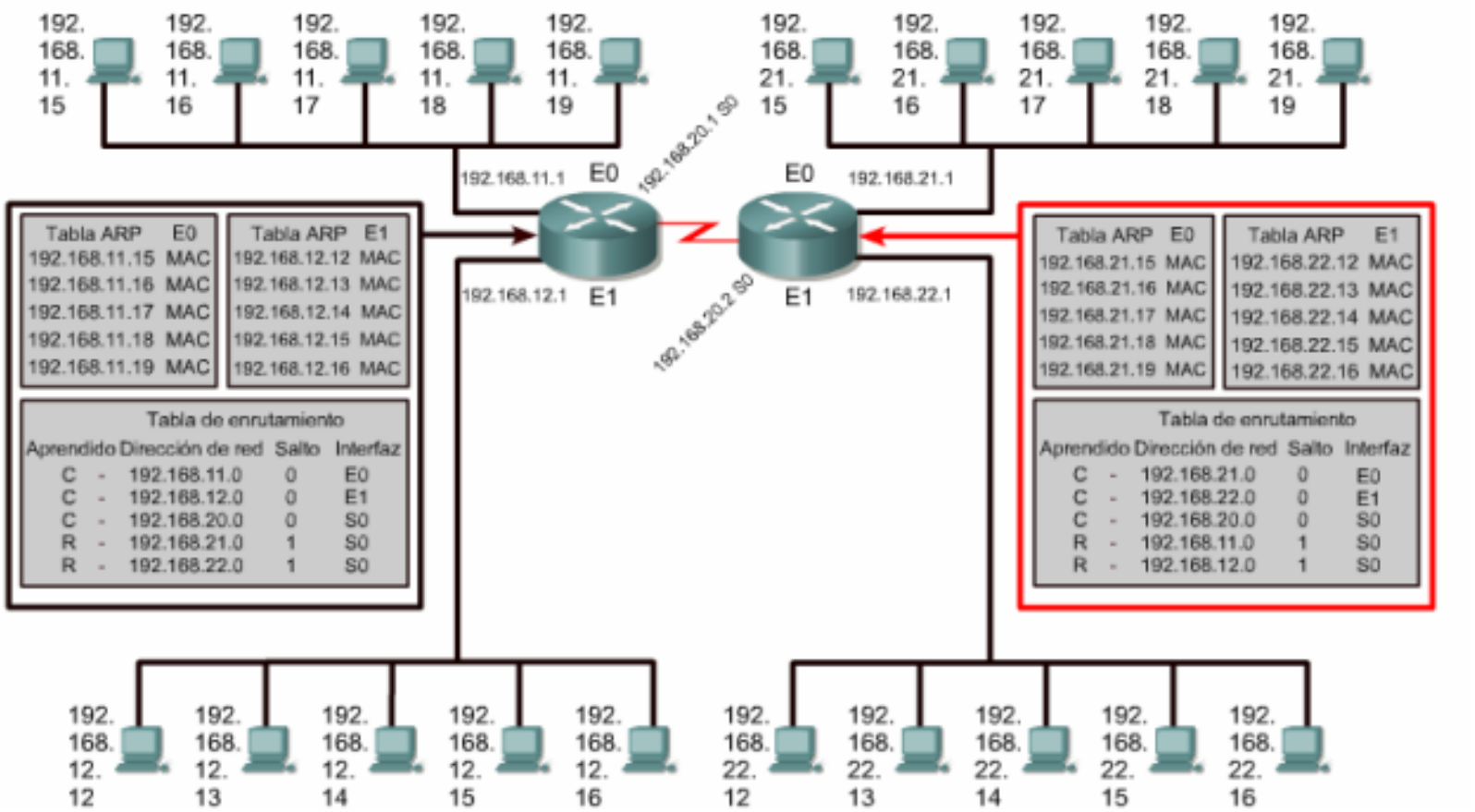


El enrutamiento en comparación con la conmutación

Cisco.com

Features	Router	Switch
Speed	Slower	Faster
OSI Layer	Layer 3	Layer 2
Addressing used	IP	MAC
Broadcasts	Blocks	Forwards
Security	Higher	Lower

La relación entre la conmutación y el enrutamiento es comparable con la relación entre las comunicaciones telefónicas locales y de larga distancia. Cuando se realiza una comunicación telefónica a un número dentro de un mismo código de área, un Switch local administra la llamada. Sin embargo, el Switch local sólo puede llevar registro de sus propios números locales. El Switch local no puede administrar todos los números telefónicos del mundo. Cuando el Switch recibe un pedido de llamada fuera de su código de área, transfiere la llamada a un Switch de nivel superior que reconoce los códigos de área. El Switch de nivel superior entonces transfiere la llamada de modo que finalmente llegue al Switch local del código de área marcado. El Router tiene una función parecida a la del Switch de nivel superior en el ejemplo del teléfono. La figura muestra las tablas ARP de las direcciones MAC de Capa 2 y las tablas de enrutamiento de las direcciones IP de Capa 3. Cada interfaz de computador y de Router mantiene una tabla ARP para comunicaciones de Capa 2. La tabla ARP funciona sólo para el dominio de broadcast al cual está conectada.. El Router también mantiene una tabla de enrutamiento que le permite enrutar los datos fuera del dominio de broadcast. Cada componente de la tabla ARP contiene un par de direcciones IP-MAC (en el gráfico las direcciones MAC están representadas por la sigla MAC, debido a que las direcciones verdaderas son demasiado largas y no caben en el gráfico).



Enrutado comparado con enrutamiento

- **Protocolo Enrutado:**

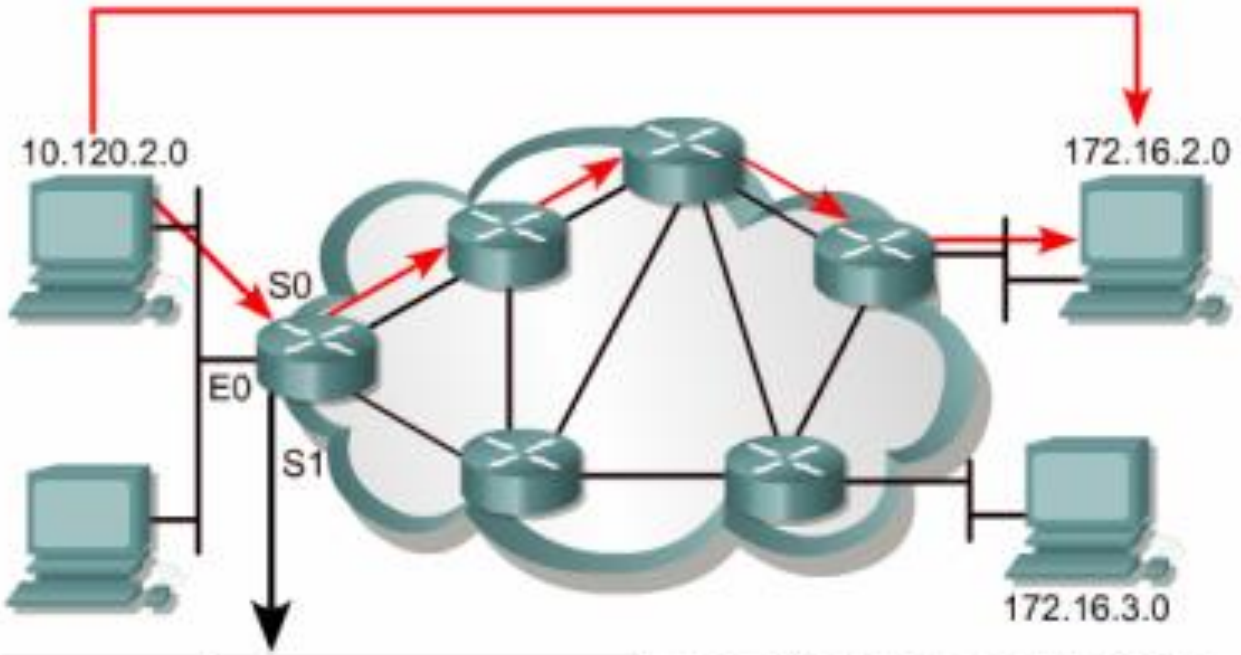
  Incluye cualquier protocolo de red que provee suficiente información en su capa de red para permitir a un ruteador encontrar el siguiente dispositivo y por último su destino.

  Define el formato y uso de lso campos dentro de un paquete.

- **Protocolo de Ruteo:**

  Provee procesos para compartir informaciòn de ruteo.

  Permite a los ruteadores comunicarse con otros ruteadores para actualizar y mantener las tablas de ruteo.



Protocolo de red	Red destino	Interfaz de salida
Conectado	10.120.2.0	E0
RIP	172.16.2.0	S0
IGRP	172.16.3.0	S1

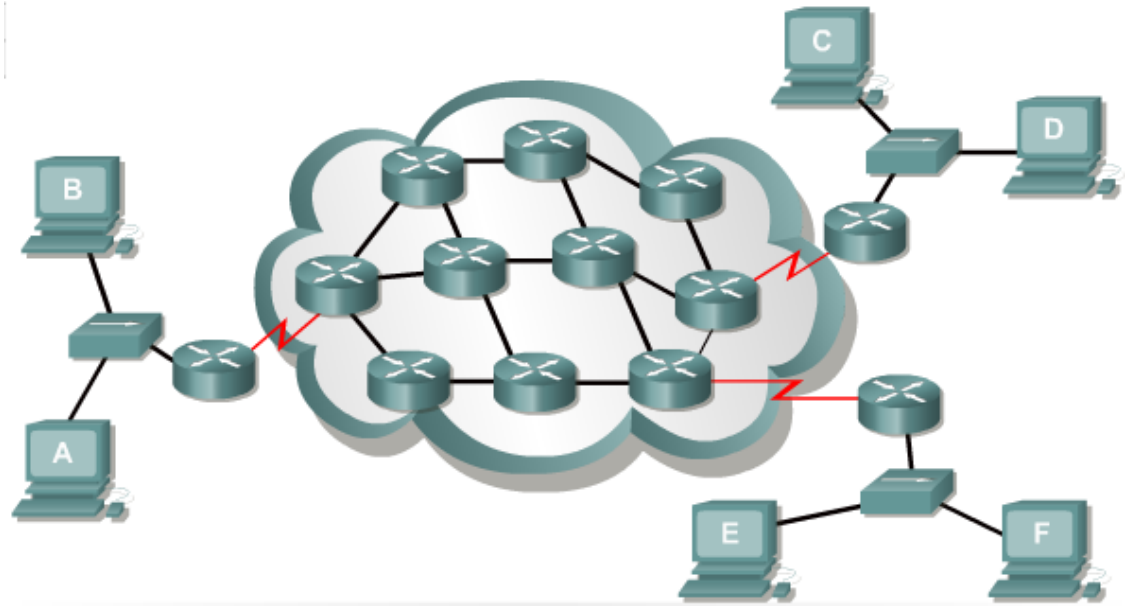
Protocolo de

Los protocolos de enrutamiento se utilizan entre routers para determinar rutas y mantener tablas de enrutamiento

Después de que se determina la ruta un router puede enrutar un protocolo enrutado

Determinación de la ruta

- **La determinación de la ruta ocurre a nivel de la capa de red. La determinación de la ruta permite que un Router compare la dirección destino con las rutas disponibles en la tabla de enrutamiento, y seleccione la mejor ruta. Los Routers conocen las rutas disponibles por medio del enrutamiento estático o dinámico. Las rutas configuradas de forma manual por el administrador de la red son las rutas estáticas. Las rutas aprendidas por medio de otros Routers usando un protocolo de enrutamiento son las rutas dinámicas.**



If computer A was sending data to computer F, what path would the data take? That is determined by the information in the routing table.

Tablas de enrutamiento

- **Los Routers utilizan protocolos de enrutamiento para crear y guardar tablas de enrutamiento que contienen información sobre las rutas. Esto ayuda al proceso de determinación de la ruta. Los protocolos de enrutamiento llenan las tablas de enrutamiento con una amplia variedad de información. Esta información varía según el protocolo de enrutamiento utilizado. Las tablas de enrutamiento contienen la información necesaria para enviar paquetes de datos a través de redes conectadas. Los dispositivos de Capa 3 interconectan dominios de broadcast o LAN. Se requiere un esquema de direccionamiento jerárquico para poder transferir los datos**

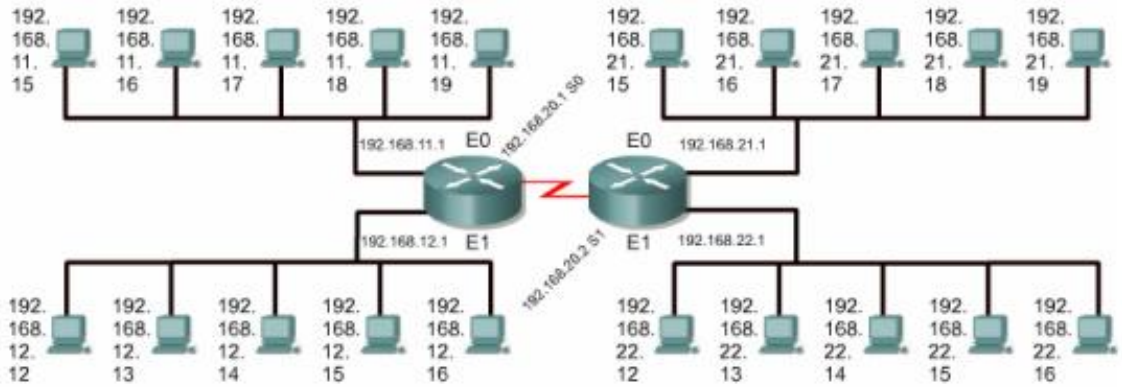


Tabla de enrutamiento

Aprendido	Dirección de red	Salto	Interfaz
C -	192.168.11.0	0	E0
C -	192.168.12.0	0	E1
C -	192.168.20.0	0	S0
R -	192.168.21.0	1	S0
R -	192.168.22.0	1	S0

Tabla de enrutamiento

Aprendido	Dirección de red	Salto	Interfaz
C -	192.168.21.0	0	E0
C -	192.168.22.0	0	E1
C -	192.168.20.0	0	S1
R -	192.168.11.0	1	S1
R -	192.168.12.0	1	S1

Algoritmos de enrutamiento y métricas

Los protocolos de enrutamiento con frecuencia tienen uno o más de los siguientes objetivos de diseño:

- **Optimización: la optimización describe la capacidad del algoritmo de enrutamiento de seleccionar la mejor ruta. La mejor ruta depende de las métricas y el peso de las métricas que se usan para hacer el cálculo. Por ejemplo, un algoritmo puede utilizar tanto las métricas del número de saltos como la del retardo, pero puede considerar las métricas de retardo como de mayor peso en el cálculo.**
- **Simplicidad y bajo gasto: cuanto más simple sea el algoritmo, más eficientemente será procesado por la CPU y la memoria del Router. Esto es importante ya que la red puede aumentar en grandes proporciones, como la Internet.**
- **Solidez y estabilidad: un algoritmo debe funcionar de manera correcta cuando se enfrenta con una situación inusual o desconocida; por ejemplo, fallas en el hardware, condiciones de carga elevada y errores en la implementación.**
- **Flexibilidad: un algoritmo de enrutamiento debe adaptarse rápidamente a una gran variedad de cambios en la red. Estos cambios incluyen la disponibilidad y memoria del Router, cambios en el ancho de banda y retardo en la red.**
- **Convergencia rápida: la convergencia es el proceso en el cual todos los Routers llegan a un acuerdo con respecto a las rutas disponibles. Cuando un evento en la red provoca cambios en la disponibilidad de los Routers, se necesitan actualizaciones para restablecer la conectividad en la red. Los algoritmos de enrutamiento que convergen lentamente pueden hacer que los datos no puedan enviarse.**

Protocol	Metric	Maximum number of routers	Origins
RIP	Hop count	15	Xerox
IGRP	• Bandwidth • Load • Delay • Reliability	255	Cisco

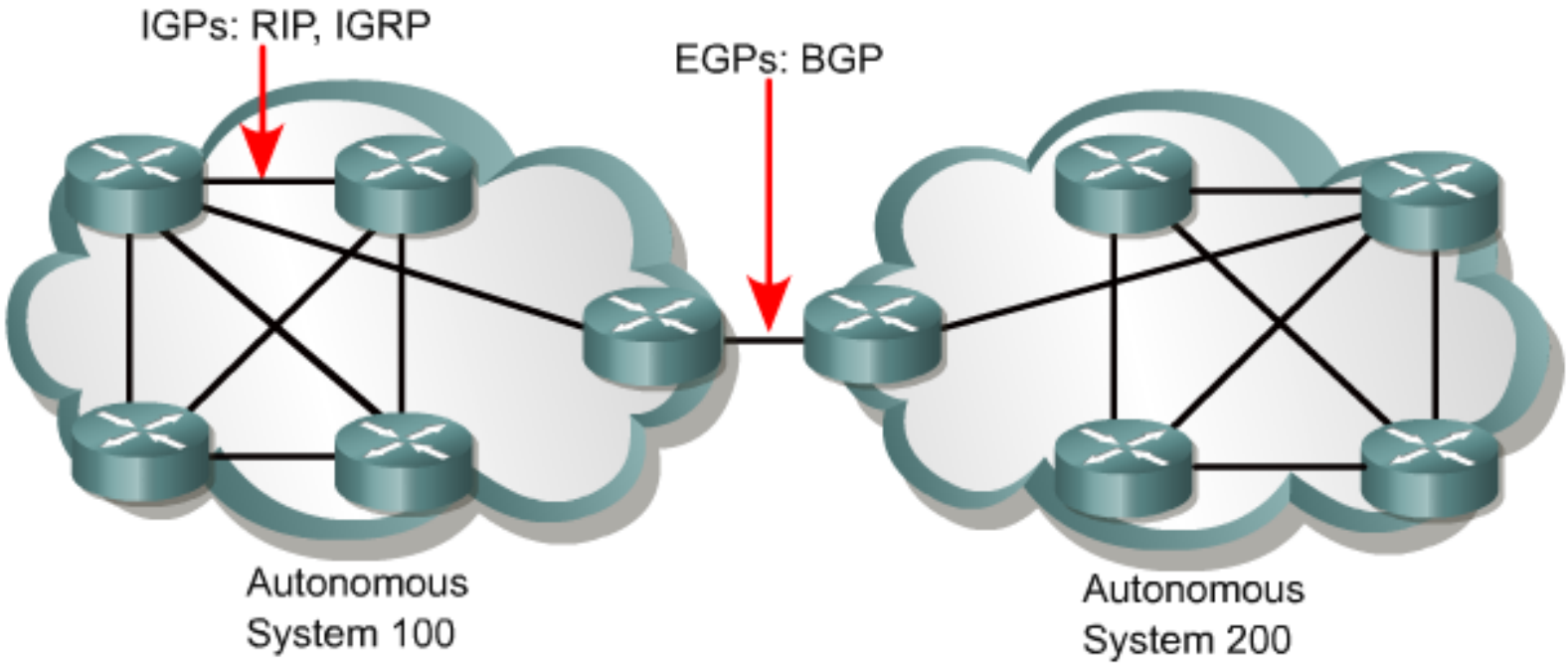
IGP y EGP

- **IGPs rutea datos dentro de sistemas autónomos**

  RIP, RIPv2, IGRP, EIGRP, OSPF, IS-IS

- **EGPs rutea datos entre sistemas autónomos**

  Border Gateway Protocol (BGP)



Los IGP enrutan datos dentro de un sistema autónomo.

- **Protocolo de información de enrutamiento (RIP) y (RIPv2).**
- **Protocolo de enrutamiento de Gateway interior (IGRP) .**
- **Protocolo de enrutamiento de Gateway interior mejorado (EIGRP) .**
- **Primero la ruta libre más corta (OSPF)**
- **Protocolo de sistema intermedio-sistema intermedio (IS-IS).**
- **Los EGP enrutan datos entre sistemas autónomos. Un ejemplo de EGP es el protocolo de Gateway fronterizo (BGP).**

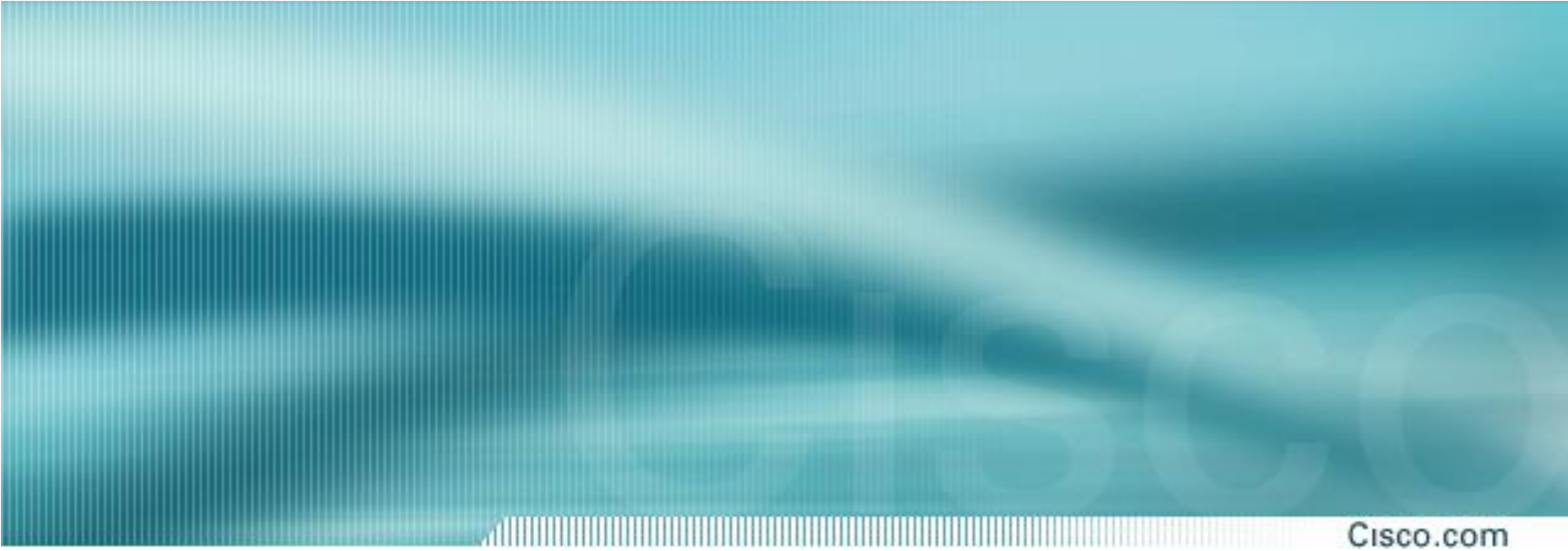
Estado de Enlace y Vector de Distancia

- **Los ejemplos de los protocolos por vector-distancia incluyen los siguientes:**
- **Protocolo de información de enrutamiento(RIP): es el IGP más común de la red. RIP utiliza números de saltos como su única métrica de enrutamiento.**
- **Protocolo de enrutamiento de Gateway interior (IGRP): es un IGP desarrollado por Cisco para resolver problemas relacionados con el enrutamiento en redes extensas y heterogéneas.**
- **IGRP mejorada (EIGRP): esta IGP propiedad de Cisco incluye varias de las características de un protocolo de enrutamiento de estado de enlace. Es por esto que se ha conocido como protocolo híbrido balanceado, pero en realidad es un protocolo de enrutamiento vector-distancia avanzado.**

Protocolos de enrutamiento

- RIP
- RIP v2
- IGRP
- EIGRP
- OSPF
- IS-IS
- BGP

- **RIP es un protocolo de enrutamiento vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier enlace en internetwork. Si existen varias rutas hasta un destino, RIP elige la ruta con el menor número de saltos. Sin embargo, debido a que el número de saltos es la única métrica de enrutamiento que RIP utiliza, no siempre elige el camino más rápido hacia el destino.**
- **Además, RIP no puede enrutar un paquete más allá de los 15 saltos. RIP Versión 1 (RIPv1) necesita que todos los dispositivos de la red utilicen la misma máscara de subred, debido a que no incluye la información de la máscara en sus actualizaciones de enrutamiento. Esto también se conoce como enrutamiento con clase.**
- **RIP Versión 2 (RIPv2) ofrece un prefijo de enrutamiento y envía información de la máscara de subred en sus actualizaciones. Esto también se conoce como enrutamiento sin clase. En los protocolos sin clase, las distintas subredes dentro de la misma red pueden tener varias máscaras de subred. El uso de diferentes máscaras de subred dentro de la misma red se denomina máscara de subred de longitud variable (VLSM).**
- **IGRP es un protocolo de enrutamiento por vector-distancia desarrollado por Cisco. El IGRP se desarrolló específicamente para ocuparse de los problemas relacionados con el enrutamiento de grandes redes que no se podían administrar con protocolos como, por ejemplo, RIP. IGRP puede elegir la ruta disponible más rápida basándose en el retardo, el ancho de banda, la carga y la confiabilidad. IGRP también posee un límite máximo de número de saltos mucho mayor que RIP. IGRP utiliza sólo enrutamiento con clase.**
- **OSPF es un protocolo de enrutamiento de estado de enlace desarrollado por la Fuerza de tareas de ingeniería de Internet (IETF) en 1988. El OSPF se elaboró para cubrir las necesidades de las grandes internetworks escalables que RIP no podía cubrir.**



Mecanismos de la división en subredes

Clases de direcciones IP de red

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

Introduction to Subnetting

- **Host bits must are reassigned (or "borrowed") as network bits.**
- **The starting point is always the leftmost host bit.**

Class C network address 192.168.10.0

11000000.10101000.00001010.00000000
N . N . N . H

11000000.10101000.00001010.00000000
N . N . N . sN H
In this example three bits have been assigned to designate the subnet.

3 bits borrowed allows 2^3-2 or 6 subnets

Class B network address 147.10.0.0

10010011.00001010.00000000.00000000
N . N . H . H

10010011.00001010.00000000.00000000
N . N . sN H. H
In this example five bits have been assigned to designate the subnet.

5 bits borrowed allows 2^5-2 or 30 subnets

Class A network adress 28.0.0.0

00011100.00000000.00000000.00000000
N . H . H . H

00011100.00000000.00000000.00000000
N . sN . sN H . H
In this example twelve bits have been assigned to designate the subnet.

12 bits borrowed allows 2^{12}-2 or 4094 subnets

Introducción y razones para realizar subredes

- **Para crear la estructura de subred, los bits de host se deben reasignar como bits de subred. Este proceso es a veces denominado "pedir bits prestados". Sin embargo, un término más preciso sería "prestar" bits. El punto de inicio de este proceso se encuentra siempre en el bit del Host del extremo izquierdo, aquel que se encuentra más cerca del octeto de red anterior.**
- **Las direcciones de subred incluyen la porción de red Clase A, Clase B o Clase C además de un campo de subred y un campo de Host. El campo de subred y el campo de Host se crean a partir de la porción de Host original de la dirección IP entera. Esto se hace mediante la reasignación de bits de la parte de host a la parte original de red de la dirección. La capacidad de dividir la porción de Host original de la dirección en nuevas subredes y campos de Host ofrece flexibilidad de direccionamiento al administrador de la red.**

Cómo establecer la dirección de la máscara de subred

- **Además de la necesidad de contar con 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 ofrece algo de seguridad ya que el acceso a las otras subredes está disponible solamente a través de los servicios de un Router. Además, el uso de listas de acceso puede ofrecer seguridad en el acceso. Estas listas pueden permitir o negar el acceso a la subred, tomando en cuenta varios criterios, de esta manera brindan mayor seguridad. Más tarde se estudiarán las listas de acceso. Algunos propietarios de redes Clases A y B han descubierto que la división en subredes crea una fuente de ingresos para la organización a través del alquiler o venta de direcciones IP que anteriormente no se utilizaban.**

Cómo establecer la dirección de la máscara de subred

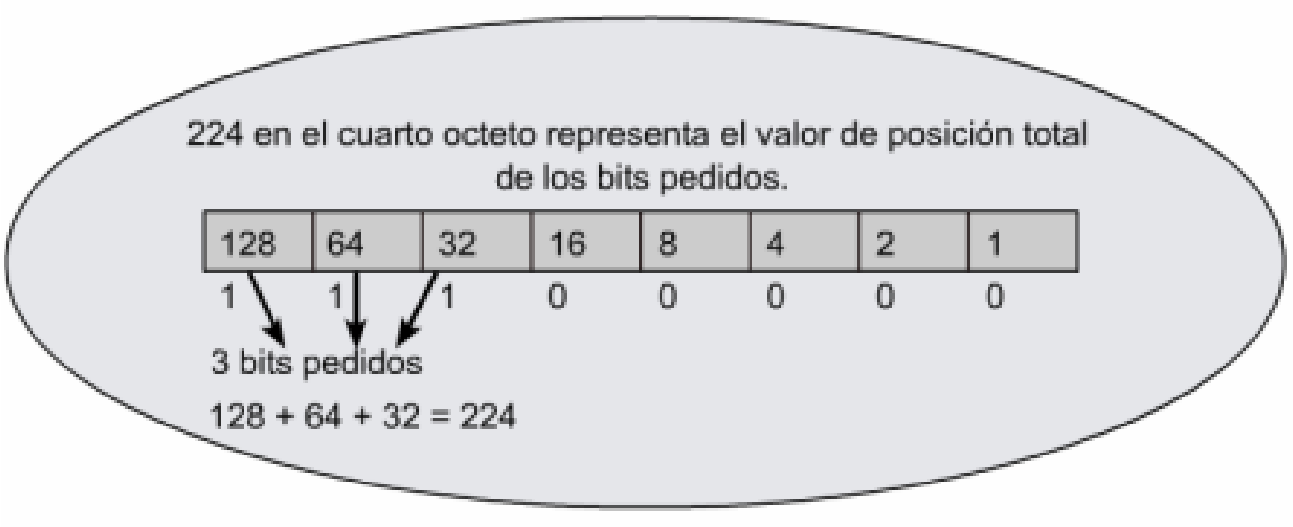
- **La selección del número de bits a utilizar en el proceso de división en subredes dependerá del número máximo de Hosts que se requiere por subred. Es necesario tener una buena comprensión de la matemática binaria básica y del valor de posición de los bits en cada octeto para calcular el número de subredes y Hosts creados cuando se pide bits prestados.**

Bits pedidos	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1

Cómo establecer la dirección de la máscara de subred

Es posible que los últimos dos bits del último octeto nunca se asignen a la subred, sea cual sea la clase de dirección IP. Estos bits se denominan los dos últimos bits significativos. El uso de todos los bits disponibles para crear subredes, excepto los dos últimos, dará como resultado subredes con sólo dos Hosts utilizables.
Este es un método práctico de conservación de direcciones para el direccionamiento de enlace serial de Routers. Sin embargo, para una LAN que está en funcionamiento, puede que esto origine gastos prohibitivos en equipos.

Formato de barra diagonal	/25	/26	/27	/28	/29	/30	N/A	N/A
Máscara	128	192	224	240	248	252	254	255
Bits pedidos	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1



Aplicación de la máscara de subred

- **Una vez que la máscara está establecida, puede utilizarse para crear el esquema de subred. La tabla de la Figura es un ejemplo de subredes y direcciones que se crean al asignar tres bits al campo de la subred.**
- **Esto creará ocho subredes con 32 Hosts por subred. Comience desde cero (0) al asignar números a las subredes. La primera subred es siempre llamada subred cero.**
- **Al llenar la tabla de subred, tres de los campos son automáticos, otros requieren de cálculos. El ID de subred de la subred 0 equivale al número principal de la red, en este caso 192.168.10.0. El ID de broadcast de toda la red es el máximo número posible, en este caso 192.168.10.255. El tercer número representa el ID de subred para la subred número siete. Este número consiste en los tres octetos de red con el número de máscara de subred insertado en la posición del cuarto octeto. Se asignaron tres bits al campo de subred con un valor acumulativo de 224. El ID de la subred siete es 192.168.10.224. Al insertar estos números, se establecen puntos de referencia que verificarán la exactitud cuando se complete la tabla.**

Subred N	ID de subred	Rango de hos	ID de broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

Formato de barra diagonal	/25	/26	/27	/28	/29	/30	No es aplicable	No es aplicable
Máscara	128	192	224	240	248	252	254	255
Bits pedidos	1	2	3	4	5	6	7	8
Valor	128	64	32	16	8	4	2	1
Subredes totales		4	8	16	32	64		
Subredes que se pueden utilizar		2	6	14	30	62		
Hosts totales		64	32	16	8	4		
Hosts que se pueden utilizar		62	30	14	6	2		

Cómo dividir las redes de Clase A y B en subredes

- **El procedimiento de dividir las redes de Clase A y B en subredes es idéntico al proceso utilizado para la Clase C, excepto que puede haber muchos más bits involucrados. Hay 22 bits disponibles para asignación a los campos de subred en una dirección de Clase A, y 14 bits en la de B.**

Class B network address 147.10.0.0 (14 bits available)
11001011.00001010.00000000.00000000 N . N . H . H
10010011.00001010.00000000.00000000 N . N . sN . sN H In this example 12 bits have been assigned to designate the subnet.

Class A network adress 28.0.0.0 (22 bits available)
00011100.00000000.00000000.00000000 N . H . H . H
00011100.00000000.00000000.00000000 N . sN . sN . sN H In this example 20 bits have been assigned to designate the subnet.

Cálculo de la subred de residencia utilizando la operación "AND"

- Los Routers utilizan máscaras de subred para establecer las subredes de origen para nodos individuales.
- Este proceso se denomina operación "AND" lógico. La operación "AND" es un proceso binario por medio del cual un Router calcula el ID de la subred para un paquete entrante. La operación "AND" es parecida a la multiplicación.
- Este proceso se administra a un nivel binario. Por lo tanto, es necesario ver la dirección IP y la máscara de forma binaria. Se realiza la operación "AND"con la dirección IP y la dirección de subred y el resultado es el ID de subred. El Router entonces utiliza esa información para enviar el paquete por la interfaz correcta.

Packet Address	192.168.10.65	11000000.10101000.00001010.010	00001
Subnet Mask	255.255.255.224	11111111.11111111.11111111.111	00000
Subnetwork Address	192.168.10.64	11000000.10101000.00001010.010	00000