Instalación y configuración de los equipos de la red.

Caso práctico

Antonio, el dueño de la academia donde estamos instalando una serie de redes de área local en las aulas, le pregunta a Julia, la técnica superior en Administración de Sistemas Informáticos en red y a Samuel, el técnico en Sistemas Microinformáticos y redes todas las dudas que le surgen:

-Ya he visto que habéis instalado todos los dispositivos necesarios para las conexiones. -Así es, responde Samuel, está hecho todo el cableado y los equipos ya tienen las tarjetas de red instaladas. -Con lo cual, replica Antonio, ya podremos utilizar las redes. -Aún no, ahora que está toda la infraestructura instalada falta configurar los equipos y dispositivos para que puedan comunicarse entre ellos y tengan acceso a Internet, le dice Julia. Además, hay que tener en cuenta los requisitos que nos pediste, sobre que los datos de la administración no puedan ser accesibles desde las aulas. -Pensé que era todo más inmediato. -No Antonio, ahora queda la configuración IP de los equipos y del resto de los dispositivos, apunta Samuel.

Y es en este punto, cuando Samuel se acuerda de todo aquello que estudió en el ciclo a distancia sobre direccionamiento IP.

En este curso has estudiado como se prepara la instalación de una red de área local, con todo el cableado y la instalación de todos los dispositivos físicos necesarios. En la unidad que empiezas, aprenderás a configurar dichos dispositivos para que todo funcione correctamente. Para ello, tendrás que saber configurar una serie de parámetros en cada uno de los equipos que forman parte de la red. Dichos parámetros tendrán que seguir unas normas determinadas para que los equipos se reconozcan entre sí y puedan comunicarse.

Para saber más

En el siguiente enlace dispones de una presentación sobre los contenidos fundamentales que se tratarán a lo largo de todo el tema. Es interesante que veas esta presentación para hacerte una idea de que vas a aprender en la presente unidad:

Resumen de la unidad

INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS EN LA RED

1. CAPA DE RED

- En este apartado verás cuáles son las funciones de la capa de red del modelo OSI.
- Aunque se puede resumir que la principal función de esta capa es la de llevar la información de origen a destino aunque estén en redes diferentes.

1.1- Forma de trabajo de la capa de red

- Puede trabajar con estas dos opciones:
  - Datagramas
  - Circuitos virtuales
- El tipo de servicio puede ser:
  - Servicio orientado a la conexión
  - Servicio no orientado a la conexión

Resumen de la unidad

1.2- Función de direccionamiento

- En este apartado se introduce el concepto de direccionamiento, distinto según en la capa en que trabajes.

	Nivel de enlace	**Nivel de red**	**Nivel de transporte**
Capa del modelo OSI	Capa 2	Capa 3	Capa 4

Direccionamiento	Con la dirección MAC de la tarjeta de red	Con la dirección IP del equipo	Con el puerto de la aplicación correspondiente
Unidad de información	Tramas	Paquetes	Segmento

Resumen de la unidad

2. DIRECCIONES IPV4

- En este apartado verás la diferencia entre una dirección IP y una dirección MAC.
- La dirección IP utiliza 32 bits agrupados en octetos o bytes, separados con un punto en su formato decimal.
- Cada octeto puede tomar valores entre 0 y 255.

2.1- Clases de direcciones IP

- Existen distintas clases de direcciones IP:
  - Clase A
  - Clase B
  - Clase C
  - Clase D
  - Clase E

2.2- Rangos de las clases de direcciones IP:

- Se puede especificar para cada una de las clases:
  - Cuántas redes pueden direccionar.
  - Cuántos equipos pueden direccionar en cada red.
- Aunque existen una serie de direcciones reservadas.

Resumen de la unidad

2.3- Ejemplo de direcciones IP en una red

- Se trata de un ejemplo de primera toma de contacto para ir familiarizándote sobre el uso de las direcciones IP.
- Es un ejemplo muy concreto y en un escenario muy sencillo.

10011101 10001111 11111100 11001111

157.143.252.207

2.4- La máscara de red

- Está constituida por 32 bits.
- Cada clase tiene asociada una máscara por defecto.
- Se pueden modificar para crear subredes dentro de una dirección de red determinada.

2.5- Otra notación para las direcciones IP

- En vez de indicar cuál es la máscara de red utilizada, se puede representar cuántos bits de la dirección IP se utilizan para direccionar la red.
- Su notación será /NºdeBitsdeLaMáscara

Resumen de la unidad

2.6- División en subredes

- Con ayuda de la máscara de red se pueden crear subredes.
- Para ello se "roban" bits dedicados a direccionar equipos para realizar distintas subredes.
- Se reconocen los bits robados gracias a la modificación de la máscara de red.

2.7- Ejemplo de subredes con dirección de clase C

- Ejemplo completísimo de cómo se hacen subredes partiendo de una dirección IP de clase C.
- Es altamente recomendable no seguir avanzando en el tema hasta tener el ejemplo bien entendido.
- Muy importante.

2.8- Ejemplo de subredes con dirección de clase B

- Se trata de un ejemplo parecido al anterior pero con una dirección de clase B.
- Es útil para comprobar cuáles son las diferencias y las similitudes en estos escenarios prácticos con distintas redes según su clase.

Resumen de la unidad

2.9- Protocolo IPV6

- Es un protocolo aún no utilizado para resolver el problema que se plantea con IPV4.
- El problema es que nos quedaremos sin direcciones IP libres para asignar a nuevos equipos.
- Se resolverá con IPV6, que usa 128 en lugar de 32 para direccionar un equipo.

2.10- Protocolo de resolución de direcciones. ARP

- Protocolo ARP. Me proporciona la dirección MAC de un equipo a través de su dirección IP.
- Protocolo RARP. Me proporciona la dirección IP de un equipo a través de una dirección MAC.

Resumen de la unidad

3. CONFIGURACIÓN DE LOS ELEMENTOS DE UNA RED

3.1- Configuración de la tarjeta de red en un sistema propietario.

3.2- Configuración de la tarjeta de red en un sistema libre.

En ambos casos se trata de ver un vídeo explicativo.

Resumen de la unidad

4. DISPOSITIVOS DE INTERCONEXIÓN DE REDES. ROUTERS

- En esta introducción se hace un repaso de:
  - Qué es un encaminador.
  - Qué funciones tiene.
  - En qué capa trabaja.
  - De qué tipos hay.

4.1- Configuración de un encaminador

- Se trata de un ejemplo práctico de cómo se configura un router desde un hyperterminal.
- En función del fabricante del router este proceso puede variar de uno a otro.

4.2- Tabla de rutas

- La tabla de rutas es la información interna que tiene cualquier router en función de la cual determina cuál es el mejor camino que debe seguir la información para ir de un nodo a otro.

Resumen de la unidad

4.3, 4.4, 4.5- Comandos TCP/IP en Windows

- Se muestra una lista de comandos TCP/IP para escribir en la consola de Windows muy importantes para analizar y configurar redes en este sistema.

4.6, 4.7, 4.8, 4.9- Ejemplos de configuración de routers

- En estos cuatro apartados se muestra un par de ejemplos de cómo se tienen que configurar los routers en dos escenarios distintos y cómo han de ser sus tablas de encaminamiento para que la información vaya en la dirección que desea el usuario.

4.10- Enrutamiento dinámico

- Interesante colofón a toda la parte de enrutamiento con un completísimo ejemplo en el que se representan los diagramas físicos y lógicos de una red, así como la distribución de sus direcciones IP.
- Imprescindible.

Resumen de la unidad

4.11- Encaminador inalámbrico

- Versión inalámbrica de un router
- Configuración, seguridad.
- Muy interesantes los vídeos propuestos para entender y

aprender de estos routers.

4.12, 4.13- VLANs

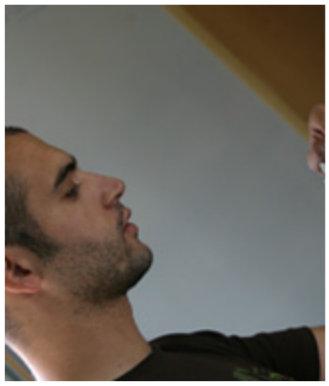
- Se retoma la definición de VLANs y se profundiza en el funcionamiento y configuración del switch para conseguir aislar distintos equipos.
- Muy interesantes los vídeos de PacketTracer donde se ve la configuración y prueba de estas redes.

4.14- PC como routers

- En este apartado se han incluido unos interesantes manuales de cómo configurar nuestro sistema en máquinas virtuales para poder realizar las distintas prácticas.

1.- Capa de red en el modelo OSI.

Caso práctico



Antes de empezar la configuración de cada uno de los equipos de la academia, Julia y Samuel se encuentran conversando sobre este tema:

-Recuerdo que todo el direccionamiento de equipos estaba basado en una de las capas del modelo OSI. -Así es, Samuel, el direccionamiento IP, (Internet protocol) está basado en la capa de red del modelo OSI. Si la red local solo se utilizase con un switch, el direccionamiento es a través de la MAC (Media Access Control) de cada tarjeta de red, que es en la capa de enlace. Pero como pretendemos conectar los equipos a un router, el direccionamiento a utilizar es el de la capa siguiente, que es la capa de red. -Umm, así que existen distintos direccionamientos dependiendo del entorno en el que trabajen los equipos. -Lo has entendido perfectamente, Samuel.

En este tema conocerás en profundidad **la capa de red** del modelo OSI. **La misión fundamental de la capa 3** es conseguir que los datos lleguen desde el origen al destino aunque estos se encuentren en redes diferentes y no tengan conexión directa. Dicho de otro modo, ofrece conexión entre dos equipos y selecciona una ruta entre ellos, aunque los dos equipos se encuentren en redes geográficamente distintas.

Ofrece servicios a la capa de nivel superior, el nivel de transporte, y utiliza los servicios de la capa de nivel inferior, la capa de enlace de datos.

Necesitas saber que para realizar esta comunicación de extremo a extremo la capa 3 utiliza unos procedimientos básicos:

- **Direccionamiento**: la capa de red nos da un método para direccionar los distintos equipos, es decir, poder identificarlos de cierta manera con una dirección única. Al direccionar un dispositivo se le pasa a denominar host. Este término es equivalente a un equipo conectado a una red.
- **Encapsulamiento**: Cuando se quiere enviar un mensaje a través de la red, el mensaje se genera en la capa de aplicación del host origen. Ese mensaje se va transformando a través de las distintas capas hacia abajo añadiéndole

información en cada una de las capas. En concreto, en la capa tres se añaden, entre otras cosas, la dirección del host destino y la dirección del host origen. A este conjunto de información se denomina paquete. Este proceso de encapsulamiento se completa al enviar el paquete a la capa de enlace de datos para que proceda a su preparación para el transporte a través de los medios.

- **Desencapsulamiento**: Cuando el paquete llega al destino hay que procesarlo en la capa 3 del host destino. Se examina la dirección destino para verificar que el paquete fue direccionado a ese dispositivo. Si es correcto, el paquete se desencapsula por la capa de red, es decir, se retira la información añadida en la capa tres del host origen, y el resultado se envía a las capas superiores para que llegue al usuario.

- **Enrutamiento**: La capa de red provee los servicios para dirigir los paquetes a su host destino. Puede que el origen y el destino estén en redes diferentes y que el paquete pueda recorrer muchas redes diferentes. Los routers tienen la función de ir encaminando el paquete para que llegue al destino final.

- **Control de la congestión**: Cuando una red recibe más tráfico del que se puede procesar se puede producir una congestión. El problema de la congestión en un nodo es que tiende a extenderse por toda la red pudiendo llegar a bloquearla por completo. Existen técnicas de gestión y prevención de congestiones que se aplican en la capa 3.

Autoevaluación

¿Cuál es la función principal de la capa de red del modelo OSI?

- ○ Que los datos sean entendidos al llegar al host de destino.
- ○ Que los datos puedan ser enviados a través de los medios físicos.
- ○ Que los datos lleguen al host destino si está dentro de la misma red que el host origen.
- ○ Que los datos lleguen del host origen al destino aunque éstos estén en redes diferentes.

No es correcta.

Incorrecta.

No es la respuesta correcta.

Muy bien. Has captado la idea.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

1.1.- Forma de trabajo de la capa de red.

¿Sabes cómo trabaja la capa de red? ¿Cómo se establecen las rutas? Te interesa conocer que la capa de red puede funcionar de dos formas diferentes:

- Con datagramas: cada paquete de datos se encamina independientemente sin que el origen y el destino tengan que establecer un proceso de comunicación previo.
- Con circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse han de empezar por establecer una conexión. Durante el tiempo que dure esta conexión, los dispositivos de interconexión que haya por el camino elegido reservarán recursos para ese circuito virtual específico.

Acabas de ver que la capa de red tiene dos formas de trabajar internamente, pero independientemente de si trabajamos con datagramas o con circuitos virtuales, se puede dar hacia el nivel de transporte un servicio orientado a conexión o no.

  - **Servicios orientados a la conexión**: solo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que seguirán el resto de los paquetes pertenecientes a esa conexión. Cuando llega un paquete que no es el primero, se identifica a qué conexión pertenece y se envía por el camino adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada nodo.

- **Servicios no orientados a la conexión**: Cada paquete debe llevar la dirección destino y cada uno de los nodos de la red decide el camino de cada paquete, pudiendo ser este camino diferente para dos paquetes de la misma comunicación.

Autoevaluación

Si una comunicación entre dos nodos se realiza sin proceso de comunicación previo y cada paquete puede viajar por un camino diferente, se dice que la comunicación a nivel de red es…

- ○ Con datagramas y servicio orientado a la conexión.
- ○ Con datagramas y servicio no orientado a la conexión.
- ○ Con circuitos virtuales y servicio orientado a la conexión.
- ○ Con circuitos virtuales y servicio no orientado a la conexión.

No está bien.

Efectivamente es correcto.

No es correcta.

No está bien, repasa este capítulo.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

1.2.- Función de direccionamiento.

Caso práctico

Antonio, que acaba de escuchar una conversación entre Samuel y Julia, ha oído que hay dos tipos de direcciones para identificar a un equipo en la red.

-¿Qué diferencia hay entre una dirección IP y una dirección MAC?, pensé que las dos eran lo mismo.

-Pues no, Antonio, le contesta Julia, una dirección MAC identifica a la tarjeta de red que tenemos en el equipo y la dirección IP sirve para identificar al propio equipo en la red.

-Yo podría explicarte en que consiste la diferencia entre las dos, comenta Samuel.

Tú podrás, al final de este tema, al igual que Samuel, explicar la diferencia entre ambas direcciones.

Como puedes imaginar, en una red con varios equipos conectados pueden existir rutas compartidas por varios equipos. La selección del destinatario en estos casos no es tarea sencilla. Los mensajes que atraviesen equipos intermedios deben disponer de algún mecanismo que les permita averiguar cual es el destinatario.

La forma más sencilla de decidir qué equipo es destinatario de una cierta información es a través del direccionamiento. Consiste en asignar una dirección única a cada uno de los equipos de la red e incluirlo en cada mensaje para que así conozca cuál de ellos es el destino.

Has de saber que existen dos tipos de direccionamiento:

- **Direccionamiento a nivel de enlace**: En el direccionamiento a nivel de enlace se utiliza la dirección MAC de la tarjeta de red para buscar al equipo destinatario y sirve para enviar mensajes dentro de la misma red.

- **Direccionamiento a nivel de red**: El direccionamiento a nivel de red utiliza la dirección IP, que ya verás qué es y cómo se utiliza, pero sirve para enviar mensajes entre dos ordenadores aunque no se encuentren en la misma red.

1.3.- Direccionamiento a nivel de enlace.

Si haces memoria, ya has visto en temas anteriores que las redes LAN utilizan un medio compartido para transmitir. Cuando un ordenador perteneciente a una LAN envía un mensaje a través del medio compartido, solo la estación destinataria acepta la trama. Para ello, en el **nivel de enlace**, el equipo destinatario compara la dirección física o MAC del destinatario que aparece en la trama con la suya propia. Si hay coincidencia acepta la trama, en caso contrario, la descarta.

Reflexiona

RECUERDA Las **direcciones MAC** están formadas por dígitos binarios que identifican de forma única una estación de trabajo (a través de la tarjeta de red). En las redes Ethernet hemos visto que están formadas por 48 dígitos agrupados de 8 en 8 bits, representadas en hexadecimal y separadas por puntos.

Las direcciones MAC vienen grabadas en el adaptador de red (tarjeta de red) de forma que no pueden ser modificadas. Para impedir que dos estaciones tengan las mismas direcciones MAC, los fabricantes suelen convenir en los números que asignan a sus dispositivos.

Si utilizas un concentrador o hub en una red LAN, cuando uno de los equipos envía un mensaje, el hub recibe el mensaje y a través de un mensaje de difusión, se lo envía al resto de las estaciones. En la estación se comprueba si la dirección MAC del destinatario es igual a la de la tarjeta de red del equipo y en función de esa comparación se acepta o ignora el mensaje.

Cuando utilizas un conmutador o switch en una red LAN, el switch es capaz de crear dominios de difusión de todos los equipos que tiene conectados, de modo que a través de la dirección MAC del destinatario que aparece en el mensaje, le reenvía al equipo correspondiente sin que el resto de los equipos reciban mensajes que no son para ellos.

Autoevaluación

En el direccionamiento a nivel de enlace…

- Al enviar un mensaje desde un equipo, la reciben siempre todos los equipos restantes.
- Utilizando un hub, la comprobación de la MAC del destinatario se realiza en el propio hub.
- Utilizando un switch, la comprobación de la MAC del destinatario se realiza en el propio switch.
- La comprobación del destino se hace a través de la dirección IP del equipo.

No es correcta.

No es la respuesta correcta.

Efectivamente es correcto.

Incorrecto.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

1.4.- Direccionamiento a nivel de red.

Has de saber que en el direccionamiento a **nivel de red**, para identificar a los equipos ya no utilizarás la dirección MAC de la tarjeta de red, sino que emplearás la dirección IP del equipo. La dirección IP es un número que identifica de manera lógica y jerárquica a cualquier elemento que esté conectado a una red y que utilice el protocolo TCP/IP.

Imagina ahora un conjunto de redes que funcionan con el protocolo TCP/IP cuyas siglas significan Transmisión Control Protocol, Internet Protocol. Estas redes operan como una única red que conecta a muchos ordenadores de cualquier tamaño y forma. Este conjunto de redes pueden ser de distinto tipo (LAN, WAN…) conectadas juntas por dispositivos de interconexión. En el nivel de red el principal protocolo utilizado es el protocolo IPv4, aunque cada vez está tomando más fuerza el protocolo IPv6, del que luego aprenderás más.

El **protocolo IPv4** está basado en datagramas o paquetes sin conexión y es no fiable, con un servicio de “mejor entrega posible”. Se entiende por mejor entrega posible el que IP no hace comprobaciones ni seguimientos. Un ejemplo de servicio de mejor entrega posible sería el servicio postal porque hace lo posible para que las cartas lleguen a su destino, pero si éstas no llegan, será responsabilidad del emisor o el receptor descubrir la pérdida y rectificar el problema.

Es necesario que aprendas que el protocolo IP transporta los datos en paquetes denominados datagramas, cada uno de los cuales es enviado de forma independiente a través de los routers o encaminadotes, que son los dispositivos de interconexión que se utilizan en el nivel de red. Los datagramas pueden viajar a través de routers diferentes y llegar fuera de secuencia o duplicados. IP no hace seguimiento ni ofrece facilidades para ordenar los datagramas una vez recibidos. Es un servicio sin conexión y no crea circuitos virtuales para la entrega.

Podemos resumir diciendo que el direccionamiento a nivel de red se realiza a través de los encaminadores o routers, que son dispositivos de interconexión de nivel tres. Éstos utilizan principalmente el conjunto de protocolos TCP/IP, y más concretamente, que en esta capa se utiliza el protocolo IPv4, que es un protocolo no fiable, no orientado a la conexión y que utiliza datagramas. Para ello, los equipos irán provistos de un identificador único denominado dirección IP.

Autoevaluación

En el direccionamiento a nivel de red…

- ○ Se utiliza el protocolo IP, que es un protocolo orientado a la conexión y utiliza circuitos virtuales.

- Se realiza con dispositivos de interconexión de capa tres, como el hub y el switch.
- Se utiliza la dirección MAC para distinguir al destinatario.
- Se utiliza principalmente el protocolo IP, basado en las direcciones IP.

No es correcta.

No es correcta, debes volver a leer el apartado.

No es correcta, repasa lo leído.

Efectivamente es correcto.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

1.5.- Nivel de transporte.

Recordarás por lo que has aprendido en unidades anteriores que el cuarto nivel del modelo OSI es el nivel de transporte. Este nivel es el encargado de la transferencia de información libre de errores entre emisor y receptor aunque no estén directamente conectados. La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la de destino, independientemente de la red física en la que esté cada máquina.

En el **nivel de transporte** es necesario especificar con qué proceso del receptor se desea comunicar. La diferencia con los niveles de enlace o red es que solo se especifica la dirección del destino, pero en la capa de transporte hay que especificar qué proceso, que se está ejecutando en el receptor, es el que tiene que recibir el mensaje. Las direcciones de transporte se utilizan precisamente para identificar las diferentes aplicaciones de comunicación. Los protocolos que gestionan este direccionamiento son TCP y UDP, abreviatura de User Datagram Protocol. La unidad de datos que se utiliza en esta capa se denomina segmento. Cada origen y destino en TCP se identifica con un número de 16 bits llamado puerto.

Verás en la siguiente tabla una serie de puertos bastante utilizados. Se asocia a cada puerto el protocolo que lo utiliza y el servicio al que está asociado.

Nº puerto	Protocolo	Servicio de Aplicación
21	TCP	FTP
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
53	TCP / UDP	DNS
80	TCP	HTTP
88	TCP	KERBEROS
110	TCP	POP3
6000	TCP	XWINDOW

Autoevaluación

En el direccionamiento a nivel de transporte…

- Se utiliza la dirección IP para el direccionamiento.
- El puerto utilizado para el servicio **http** es el 21.
- Se utilizan dos protocolos: TCP y UDP.
- El puerto es un número de 16 bits que identifica al emisor de un mensaje de red.

No es correcta.

Vuelve a mirar este apartado.

Efectivamente es correcto.

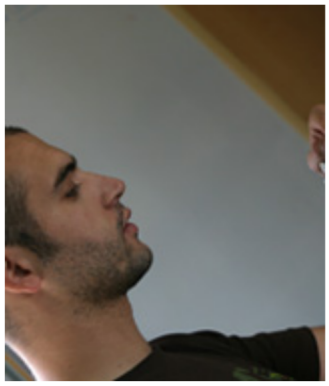
No está bien.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.- Direcciones IPv4.

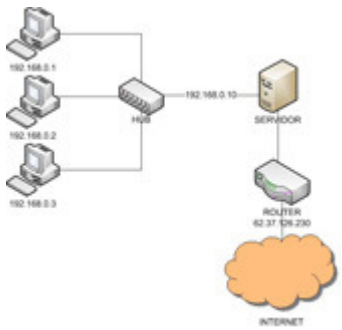
Caso práctico



Samuel está recordado con Julia, los estudios de técnico superior en Administración de Sistemas en red, cuando él estudiaba el módulo de Redes Locales.

-Recuerdo que nuestra profesora siempre insistía en lo importante que era una buena planificación a la hora de asignar direcciones IP en una red -Claro que sí, Samuel, imagínate el volumen de equipos que tenemos en esta academia. Si no tuviéramos planificado cómo se van a asignar las direcciones IP en los equipos, esto podría ser un caos. Por eso es necesario que te explique cómo he ideado la estructuración en subredes y cuáles son las direcciones IP que vamos a asignar. -Estupendo, pues cuéntame como lo vamos a organizar...

Después de este capítulo, verás cómo tú también serás capaz de realizar la distribución de direcciones IP en una red.



Ya viste en el apartado anterior que una dirección IP identifica de manera única a un equipo dentro de una red. No confundir dirección IP, o dirección lógica, con dirección MAC o dirección física. La dirección MAC es un número en hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP puede variar. Cuando se direcciona a nivel de enlace de datos utilizamos las direcciones MAC y cuando se direcciona a nivel de red se utilizan las direcciones IP.

Las **direcciones IPv4** que identifican a los dispositivos y estaciones de la red tienen un tamaño fijo de 32 bits. Estas direcciones se pueden expresar directamente en binario, aunque resulta más cómodo utilizar la notación decimal con puntos. Las direcciones IP se expresan mediante un número binario de 32 bits, con lo que se permite un espacio de direcciones de 232 direcciones posibles. Las direcciones IP se pueden expresar como números en notación decimal: se dividen los 32 bits en cuatro octetos (8 bits). Cada valor decimal de un octeto está comprendido entre 0 y 255. Al expresar las direcciones en decimal, cada octeto se separa con un punto ".". Los ceros iniciales, si los hubiera, se pueden obviar. Ejemplo: 010.128.001.255 sería 10.128.1.255. Cuando la dirección IP se expresa en binario, no se utilizan los puntos para separar los octetos.

Ejercicio resuelto

Vamos a expresar esta dirección IP decimal en su formato binario:

Dirección IP: 192.168.0.15 Dirección IP en binario: 11000000 10101000 00000000 00001111 Su valor en binario se consigue expresando cada una de las cifras separadas por puntos en binario. Si no se utilizan 8 bits en cada número al pasarlo a binario, se rellenan los bits más significativos con ceros.

Vamos a expresar esta dirección IP binaria en su formato decimal:

Dirección IP: 10101010 11000011 00001010 00110011 Dirección IP en decimal: 170.195.10.51

Para saber más

En el siguiente enlace tienes un artículo sobre la dirección IP muy completo. Se habla de las direcciones IP privadas, máscara de subred, creación de subredes y las ventajas y desventajas de la IP dinámica. Además tienes a tu disposición otro segundo enlace donde se ve como se puede cambiar una IP dinámica a estática.

Dirección IP.

Cambiando de dirección IP dinámica a estática.

Autoevaluación

¿Para que sirve el protocolo DHCP?:

- ○ Cambia direcciones IP fijas a variables.
- ○ Sirve para conectar más de un ordenador con la misma dirección IP.
- ○ Sirve para conectar equipos a un servidor.
- ○ Asigna direcciones IP de manera dinámica.

No es correcta.

Incorrecta.

No es correcta, debes repasar.

Efectivamente es correcto.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

2.1.- Clases de direcciones IP.

10011101 10001111 11111100 11001111
157.143.252.207

Acabas de aprender en el apartado anterior que una dirección IP está formada por 32 bits. Esta dirección IP se puede dividir en varios campos:

A. **Identificador**: indica el tipo de dirección.
B. Número de red**.**
C. Número de estación en la red.

A los campos A y B se les llama también bits de red o prefijo de red y al campo C se le llama bits de equipo o de host.

Estas partes son de longitud variable dependiendo de la clase de dirección. Actualmente hay cinco patrones diferentes en uso, cada uno de los cuales define una clase de dirección. Se denominan a estos cinco patrones como clase de dirección A, B, C, D y E.

- La **clase de dirección A** utiliza el primer byte para el identificador de la red y los tres restantes para el identificador de la estación.
- La **clase de dirección B** utiliza los dos primeros bytes para identificar la red y los dos siguientes para identificar la estación.
- La **clase de dirección C** utiliza los tres primeros bytes para identificar la red y el cuarto byte para identificar la estación.

- Las **direcciones de clase D** se reserva para direcciones de multienvío y las **direcciones de clase E** se reservan para uso futuro.

Además, en las direcciones de clase A el primer byte siempre empieza con el bit más significativo a 0. En las direcciones de clase B el primer byte siempre empieza con los dos bits más significativos a 10, en las de clase C el primer byte empieza con los valores 110, en los de clase D con 1110 y los de clase E con 1111. En la siguiente ilustración se ve un resumen de las clases, cuantos bytes utilizan para identificar la red y cuantos para las estaciones.

Mira ahora un ejemplo de cómo se identifica la clase de una dirección IP. Tomando como ejemplo la dirección IP 157.143.252.207, si transformas a notación binaria el primer byte obtenemos: 10011101. En este caso vemos que el primer byte empieza con los bits 10, con lo que se deduce que es una dirección de clase B.

Autoevaluación

Relaciona las siguientes direcciones IP con su clase de dirección IP.

Ejercicio de relacionar

Dirección IP	Relación.	Clase de dirección
4.23.145.90		1. Clase C
227.34.78.7		2. Clase A
246.7.3.8		3. Clase D
129.6.8.4		4. Clase B
198.76.9.23		5. Clase E

Enviar

Cada dirección IP se corresponde con una clase de dirección IP.

2.2.- Rangos de las clases de direcciones IP.

Es necesario que sepas que para cada una de las clases de direcciones, se puede averiguar cuál es el rango de direcciones de dicha clase. Verás cómo se calcula el rango de direcciones con la clase A. Extrapolando esa información al resto de las clases nos darían todos los rangos de todas las clases.

Las direcciones de clase A nos imponen que el bit más significativo del primer byte valga 0, veremos que todas las direcciones de clase A estarán en el rango de estas dos direcciones:

00000000 00000000 00000000 00000000, su equivalente: 0.0.0.0
01111111 11111111 11111111 11111111, su equivalente: 127.255.255.255
Siendo su rango de direcciones todas aquellas que estén comprendidas entre estos dos valores. Si realizamos la misma operación para el resto de las clases, se puede resumir que los rangos de las direcciones IP son los siguientes:

Clase IP	Rango	Nº de redes	Nº de estaciones
A	0.0.0.0 - 127.255.255.255	2^7=128	2^24-2=16777214
B	128.0.0.0 - 191.255.255.255	2^14=16384	2^16-2=65534
C	192.0.0.0 - 223.255.255.255	2^21=2097152	2^8-2=254
D	224.0.0.0 - 239.255.255.255	X	X
E	240.0.0.0 247.255.255.255	X	X

Con esta tabla ahora resultará mucho más sencillo realizar el ejercicio de la anterior autoevaluación.

En esta tabla se representan para cada clase IP el rango posible de direcciones, cuantas subredes se pueden conseguir y cuantas estaciones pueden direccionarse en cada una de las redes. Se observa que en la última columna siempre se resta 2 al número de estaciones posibles, esto es así porque hay dos **direcciones que siempre están reservadas**:

- Cuando los bytes reservados para el nº de estaciones tiene todos los bits a 0: Sirve para identificar toda la red, es decir, es la dirección de red.
- Cuando los bytes reservados para el nº de estaciones tiene todos los bits a 1: Sirve para enviar mensajes a todas las estaciones de la red, es decir, es la dirección de difusión.

Aparte de estas dos direcciones, hay algunas **otras direcciones reservadas** que no se pueden utilizar, que son:

- 127.0.0.1: se reserva para referenciar a direcciones de loopback, es decir, para referirnos a nuestro propio equipo.
- 0.0.0.0: dirección que se utiliza en los equipos al arrancar.

Existen un conjunto de **direcciones que solo son válidas en redes locales**, que no sirven para identificar host en Internet. Estas direcciones son las direcciones privadas, y son las siguientes:

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255
- Clase C: 192.168.0.0 a 192.168.255.255

Ejercicio resuelto

En los siguientes enlaces encontrarás un par de ejemplos de cómo se asignan direcciones IP a todos los equipos que forman parte de la red.

Ejemplo de direcciones de red. (0.03 MB)

Ejemplo de dos redes conectadas con un router. (0.07 MB)

Autoevaluación

¿Cuál de las siguientes direcciones es una dirección válida para un equipo de una red?:

- 192.168.43.255.
- 192.168.43.0.
- 192.168.43.7.
- 127.0.0.1.

No es correcta, es una dirección de difusión.

No es correcta, es una dirección de red.

Efectivamente es correcto.

No es correcta, es una dirección de loopback.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.3.- Ejemplo de direcciones IP en una red.

En este apartado verás un ejemplo práctico de cómo se calculan las direcciones IP disponibles para los equipos en una red. Supón que tienes una red LAN conectada a Internet mediante un router. Propones una dirección IP para numerar las estaciones. Esta dirección será, por ejemplo, de clase C ya que no se prevé que la red se amplíe a más de 200 estaciones. Eliges la IP: 192.118.64.0.

Esta IP es una dirección de red, es decir, indica cuál es el número de nuestra red, ya que el último dígito es 0. A partir de ésta, deberemos numerar las estaciones de red, comenzando por el número 1. Evidentemente, todas ellas tendrán en común la misma dirección de red:

Estación	Nº Dirección IP
1	192.118.64.1
2	192.118.64.2
3	192.118.64.3
4	192.118.64.4
...	...
253	192.118.64.253
254	192.118.64.254

La dirección IP 192.118.64.255 se utiliza para enviar un paquete a todas las estaciones de la red (difusión). Por lo tanto, en nuestra LAN pueden existir 254 estaciones.

Si mi red crece por encima de ese valor, entonces deberé solicitar una nueva IP de clase superior, clase A o clase B, o bien varias de clase C.

2.4.- La máscara de red.

Una vez que has estudiado en profundidad las direcciones IP, ahora es necesario que aprendas otro concepto necesario para la configuración de redes. Este concepto es la máscara de red.

En IPv4, para saber cuantos bits se utilizan para determinar los host y cuantos bits se utilizan para las direcciones de red, se utiliza la máscara de red. Cada dirección de red tiene asociada una máscara de red. La máscara de red está constituida por 32 bits. Si el bit de la máscara de red vale 1 implica que ese mismo bit en la dirección IP se dedica a las direcciones de red. Si el bit de la máscara de red vale 0 implica que ese mismo bit en la dirección IP se dedica a identificar un host.

Las clases de direcciones tienen asociadas unas máscaras de red predeterminadas, que son las siguientes:

- **Clase A**: utiliza el primer byte a identificar la red, con lo que la máscara de red será:
  - 11111111 00000000 00000000 00000000 que es equivalente a: **255.0.0.0**
- **Clase B**: utiliza los dos primeros bytes a identificar la red, con lo que la máscara de red será:
  - 11111111 11111111 00000000 00000000 que es equivalente a **255.255.0.0**
- **Clase C**: utiliza los tres primeros bytes a identificar la red, con lo que la máscara de red será:
  - 11111111 11111111 11111111 00000000 que es equivalente a **255.255.255.0**

Las máscaras de red son útiles para saber cual es la **dirección de red** asociada a una determinada dirección IP. Para poder hacer esto se realiza la operación AND bit a bit entre la dirección IP y la máscara de red. El resultado de esta operación es la dirección de red. Esta operación la realizan los routers cuando les llega un paquete con una determinada IP y una máscara de red, para así saber cuál es la dirección de red de ese paquete y encaminarlo hacia la red adecuada.

Ejemplo de cómo se calcula la dirección de red, dada una dirección IP y su máscara de red:

- Dirección IP: 198.76.9.23, en binario: 11000110 01001100 00001001 00010111
- Máscara de red: 255.255.255.0, en binario: 11111111 11111111 11111111 00000000 (al ser una dirección de clase C)

AND	11000110 01001100 00001001 00010111	Dirección IP
	11111111 11111111 11111111 00000000	Máscara de red
Dirección de red	11000110 01001100 00001001 00000000	Dirección de red: 198.76.9.0

Debes conocer

Recuerda como era la operación AND binaria:

OPERACIÓN	RESULTADO
0 AND 0	0
0 AND 1	0
1 AND 0	0
1 AND 1	1

Autoevaluación

¿Cuál es la dirección de red de esta dirección IP: 125.23.53.124 que tiene asociada la máscara de red 255.0.0.0?:

- 125.0.0.0.
- 125.23.0.0.
- 125.23.53.0.
- 125.23.53.124

Efectivamente es correcto.

No es correcta.

Incorrecta.

No es correcta, debes repasar.

Solución

1. Opción correcta
2. Incorrecto

3. Incorrecto
4. Incorrecto

2.5.- Otra notación para las direcciones IP.

Además de la notación que ya conoces para identificar una dirección IP con la máscara de red asociada, existe otra sintaxis más reducida que sería la siguiente:

- **"/8" = Clase A**
- **"/16" = Clase B**
- **"/24" = Clase C**

Se refiere a que la dirección de red tiene 8, 16 o 24 bits de **prefijo** de red respectivamente. Derivada de esta notación ha aparecido una nueva forma de nombrar las direcciones IP. Consiste en especificar en notación decimal con puntos seguida de una barra inclinada y del número de bits que componen el prefijo. Por ejemplo:

Dirección de estación	Observaciones
118.64.248.86 / 8	Clase A. Se usan 8 bits para el prefijo de red y 24 bits para el número de estación.
129.0.186.63 / 16	Clase B. Se usan 16 bits para el prefijo de red y 16 bits para el número de estación.
221.118.7.19 / 24	Clase C. Se usan 24 bits para el prefijo de red y 8 bits para el número de estación.

Cuando nombramos IP con prefijo: 192.168.1.100/24, no es necesario especificar la máscara, ya que el prefijo nos indica directamente cuántos bits de la dirección corresponden a la identificación de la red y cuáles a la estación de trabajo.

Autoevaluación

Cual es la máscara de red asociada a esta dirección IP: 192.168.9.32/24 :

- ○ 255.0.0.0
- ○ 255.255.0.0
- ○ 255.255.255.0.
- ○ No hay manera de averiguar cual es la máscara de red con esta notación.

No es correcta.

No es correcta, debes repasar.

Efectivamente es correcto.

Incorrecta.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

2.6.- División en subredes.

Cuando te encuentres diseñando una red para un ámbito en concreto, has de barajar la posibilidad de hacer divisiones o grupos entre todos los ordenadores que formen parte de la red para crear parcelas seguras, donde cada ordenador solo puede acceder a su grupo determinado. Este método es lo que se conoce como división en subredes.

La división en subredes es un método para poder crear distintos rangos de redes lógicas. Con esto conseguimos disminuir el tamaño de los dominios de difusión y hacer la red más manejable puesto que su tamaño se dividen en trozos más pequeños.

Para poder utilizar subredes, a la dirección IP que veníamos manejando hasta ahora, se le añade un nuevo campo, de manera que nos queda así:

Identificador de red, Identificador de subred, Nº de host

Esta división se hace dividiendo el campo destinado a la estación de red en dos partes, de forma que desde el exterior los encaminadores creen que se trata de una única red sin subredes.

De esta manera, si el número de equipos de una red es elevado, puedo disponer de una sola dirección de clase B en lugar de varias de clase C. O bien, de una dirección de clase A en lugar de varias de clase B. Lo único que tengo que hacer es dividir la dirección de red en subredes. Desde el exterior todas las subredes se ven como una única red.

En los siguientes apartados estudiarás un ejemplo de como se realiza la división en subredes. El apartado siguiente tienes un ejemplo de subredes con dirección de clase C y en el apartado 2.8 hay otro ejemplo de subredes con dirección de clase B. Comprobarás que no existen muchas diferencias entre ambos ejemplos pero es importante que entiendas bien todo el proceso de cálculo de subredes.

Para saber más

Si el proceso para calcular manualmente subredes se te hace difícil de entender, tienes en el siguiente enlace un documento donde se explica paso por paso las operaciones necesarias para que realices y entiendas un poco mejor estas operaciones.

Cálculo manual de subredes.

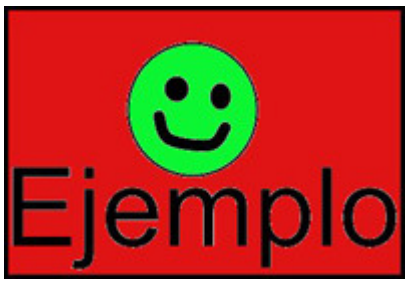
Es muy importante que entiendas bien todo este proceso. Es por ello que además de este manual, tienes a tu disposición una calculadora de subredes online y un enlace para que te puedas descargar otra calculadora. En estas herramientas solo es necesario que conozcas la dirección de red, cuantas subredes tienes que calcular y ellas hacen todos

los cálculos. Te serán útiles para comprobar que los ejercicios te salen bien.

Cálculo de subredes online.

Programa para cálculo de subredes.

2.7.- Ejemplo de subredes con dirección de clase C.



Supón que tienes la dirección de red **221.123.10.0**/24 de clase C. Con las direcciones de clase C se identifican 2^8-2=254 equipos. La máscara de red de esta dirección IP sería 255.255.255.0. Ahora quieres hacer la subdivisión de esta red en 4 subredes distintas.

Primer paso: Definir la máscara de subred: Como necesitas 4 subredes, necesitarás tomar prestado del último byte (parte de host al ser una dirección de clase C) 2 bits que hace posible cuatro combinaciones (2^2=4). El truco para calcular la máscara consiste en poner a 0 todos los bits que se corresponda con la parte de host y el resto a 1.

CÁLCULO DE LA MÁSCARA

	División principal (3 bytes por ser una dirección de Clase C)			Host (En clase C la parte de host tiene 8 bits)	
				División para 4 subredes (2 bits)	División host (6 bits)
IP en binario	11011101	01111011	00001010	ss	hhhhhhhh
IP en decimal	221	123	10	ss	hhhhhhhh
Máscara de subred (binario)	**11111111**	**11111111**	**11111111**	**11**	**000000**
Máscara de subred (decimal)	**255**	**255**	**255**	**192**	

Con estos 2 bits consigues 2^2=4 subredes distintas. Así, las direcciones de subred que quedan son las siguientes:
Segundo paso: Definir las direcciones de cada subred:

Nº de subred	Dirección de subred (en binario). La parte de host se pone a 0 y se pasa a decimal	Dirección de subred (en decimal)

0 (00)	11011101 01111011 00001010 **00** 000000	**221.123.10.0**
1 (01)	11011101 01111011 00001010 **01**000000	**221.123.10.64**
2 (10)	11011101 01111011 00001010 **10**000000	**221.123.10.128**
3 (11)	11011101 01111011 00001010 **00**000000	**221.123.10.192**

Nº de subred	Dirección de difusión o broadcast (en binario). La parte de host se pone a 1 y se pasa a decimal	Dirección de broadcast o difusión (en decimal)
0 (00)	11011101 01111011 00001010 **00**111111	**221.123.10.63**
1 (01)	11011101 01111011 00001010 **01**111111	**221.123.10.127**
2 (10)	11011101 01111011 00001010 **10**111111	**221.123.10.191**
3 (11)	11011101 01111011 00001010 **00**111111	**221.123.10.255**

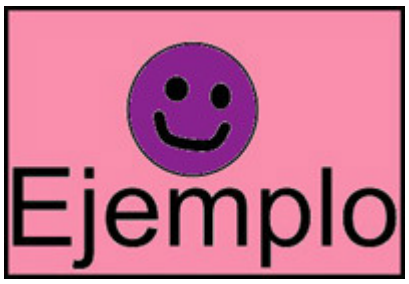
- Nº de equipos por subred: Combinaciones de 6 bits y se elimina la combinación 000000 y la 111111. 2^6-2=62
- Nº de subredes: 4

Nº de subred	Rango de direcciones IP indicando IP primero y último equipo host por subred (en binario)	Rango de direcciones (en decimal)
0 (00)	1ª equipo: 11011101 01111011 00001010 **00**000001 (1) Últ equipo: 11011101 01111011 00001010 **00**111110 (62)	**221.123.10.1** **221.123.10.62**
1 (01)	1ª equipo: 11011101 01111011 00001010 **01**000001 (65) Últ equipo: 11011101 01111011 00001010 **01**111110 (126)	**221.123.10.65** **221.123.10.126**

2 (10)	1ª equipo: 11011101 01111011 00001010 **10**000001 (129) Últ equipo: 11011101 01111011 00001010 **10**111110 (190)	**221.123.10.129** **221.123.10.190**
3 (11)	1ª equipo: 11011101 01111011 00001010 **11**000001 (193) Últ equipo: 11011101 01111011 00001010 **11**111110 (254)	**221.123.10.193** **221.123.10.254**
Para calcular los rangos de direcciones de cada subred no se tiene en cuenta las direcciones con la parte de host con todos los bits a 0 ni con todos los bits a 1		

Con este ejemplo consigues 4 subredes, pero el número total de equipos que se pueden direccionar en total ha descendido, de los 254 que teníamos sin hacer subredes, a 62 X 4= 248 equipos.

2.8.- Ejemplo de subredes con dirección de clase B.



Supón que tienes la dirección de red **138.115.0.0**/16 de clase B. Con las direcciones de clase B se identifican 2^{16}-2=65534 equipos. La máscara de red de esta dirección IP sería 255.255.0.0. Ahora quieres hacer la subdivisión de esta red (igual que en el ejemplo 1) en 4 subredes distintas.

Primer paso: Definir la máscara de subred
Como necesitas 4 subredes, debes tomar 2 bits prestados de los dos últimos bytes (parte de host al ser una dirección de clase B). El truco para calcular la máscara consiste en poner a 0 todos los bits que se corresponda con la parte de host y el resto a 1.

CÁLCULO DE LA MÁSCARA

	División principal (2 bytes por ser una dirección de Clase B)		Host (En clase B la parte de host tiene 16 bits)		
			División para 4 subredes (2 bits)	División host 3º byte (6 bits)	División host 4º byte (8 bits)
IP en binario	10001010	01110011	ss	hhhhhh	hhhhhhhhhh
IP en decimal	138	115	ss	hhhhhh	hhhhhhhhhh
Máscara de subred (binario)	**11111111**	**11111111**	**11000000**		**00000000**
Máscara de subred (decimal	**255**	**255**	**192**		**0**

Con estos 2 bits consigues 2^2=4 subredes distintas. Así, las direcciones de subred que quedan son las siguientes:
Segundo paso: Definir las direcciones de cada subred:

Nº de subred	Dirección de subred (en binario). La parte de host se pone a 0 y se pasa a decimal	Dirección de subred (en decimal)
0 (00)	10001010 01110011 **00** 000000 00000000	**138.115.0.0**
1 (01)	10001010 01110011 **01** 000000 00000000	**138.115.64.0**
2 (10)	10001010 01110011 **10** 000000 00000000	**138.115.128.0**
3 (11)	10001010 01110011 **11** 000000 00000000	**138.115.192.0**

Nº de subred	Dirección de difusión o broadcast (en binario). La parte de host se pone a 1 y se pasa a decimal	Dirección de broadcast o difusión (en decimal)
0 (00)	10001010 01110011 **00** 111111 11111111	**138.115.63.255**
1 (01)	10001010 01110011 **01** 111111 11111111	**138.115.127.255**
2 (10)	10001010 01110011 **10** 111111 11111111	**138.115.191.255**
3 (11)	10001010 01110011 **11** 111111 11111111	**138.115.255.255**

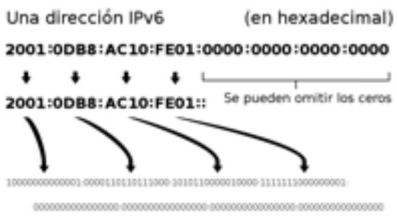
- Nº de equipos por subred: Combinaciones de 14 bits y se elimina la combinación 000000 y la 111111. 2^{14}-2=16382
- Nº de subredes: 4

Nº de subred	Rango de direcciones IP indicando IP primero y último equipo host por subred (en binario)	Rango de direcciones (en decimal)
0 (00)	1ª equipo: 10001010 01110011 **00** 000000 00000001 (0.1) Últ equipo: 10001010 01110011 **00** 111111 11111110 (63.254)	**138.115.0.1** **138.115.63.254**

1 (01)	1ª equipo: 10001010 01110011 **01** 000000 00000001 (64.1) Últ equipo: 10001010 01110011 **01** 111111 11111110 (127.254)	**138.115.64.1** **138.115.127.254**
2 (10)	1ª equipo: 10001010 01110011 **10** 000000 00000001 (128.1) Últ equipo: 10001010 01110011 **10** 111111 11111110 (191.254)	**138.115.128.1** **138.115.191.254**
3 (11)	1ª equipo: 10001010 01110011 **00** 000000 00000001 (192.1) Últ equipo: 10001010 01110011 **00** 111111 11111110 (255.254)	**138.115.192.1** **138.115.255.254**
Para calcular los rangos de direcciones de cada subred no se tiene en cuenta las direcciones con la parte de host con todos los bits a 0 ni con todos los bits a 1		

Con este ejemplo se consiguen 4 subredes pero el número total de equipos que se pueden direccionar en total ha descendido de 65536 que teníamos sin hacer subredes a 16382 X 4= 65528 equipos.

2.9.- Protocolo IPv6.



¿Has oído hablar del protocolo IPv6? Es un protocolo que en el plazo de unos pocos años está llamado a sustituir el protocolo IPv4 que acabas de estudiar. Es interesante que conozcas que el protocolo IPV6 es una versión nueva de IP que tiene como objetivo reemplazar a la versión 4. El principal problema que tenemos con IPv4 es que el número de direcciones de red disponibles para conectar equipos a Internet está agotándose, sobre todo en países superpoblados.

La forma de expresar las direcciones IPv6 es distinta a la versión IPv4. IPv6 está formada por 128 bits en lugar de 32. Y se pueden presentar de tres formas diferentes:

- Por **ocho números en hexadecimal de 16 bits cada uno**, separado por puntos. Ejemplo:
  - 12E:0:0:768F:821:0:2286
- Igual que la anterior, pero **suprimiendo todos los ceros consecutivos** en la dirección y sustituyéndolos por ::. Estos :: solo pueden aparecer una vez en la dirección. Ejemplo:
  - 12E::768F:821:0:2286
- Utilizando **una notación mixta** formada por parte de dirección IPv6 (6 números hexadecimales de 16 bits separado por dos puntos) y otra de IPv4 (4 números decimales de 8 bits). Ejemplo:
  - 65E:0:0:0:0:0:10A:192.168.0.18

En IPv6 también existen las máscaras de red y su función es idéntica a la versión anterior del protocolo. Por su parte, también utilizan los prefijos, pero en este caso su representación es justamente la contraria a IPv4: un prefijo /50, por ejemplo, indica que los últimos bits de la dirección se reservan para numerar las estaciones.

Para saber más

Si quieres aprender más sobre las direcciones IPv6, te propongo que veas estos vídeos. El primero de ellos habla del protocolo IPv6 y el segundo vídeo sobre la transición de IPv4 a IPv6.

Protocolo IPv6.	Transición de IPv4 a IPv6.
http://www.youtube.com/embed/I5b-cXAk0cM	http://www.youtube.com/embed/-4ua2WZSI-c

Autoevaluación

¿Qué ventajas tiene IPv6 sobre IPv4? :

- Es más sencilla su numeración.
- Puede direccionar más equipos en Internet.
- No utiliza máscaras de red.
- No tiene ninguna ventaja sobre IPv4.

No es correcta.

Efectivamente es correcto.

No es correcta, debes repasar.

Es incorrecta.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

2.10.- Protocolo de resolución de direcciones. ARP.

Ya conoces el protocolo IP que se utiliza en la capa 3 del modelo OSI. Es interesante que conozcas otros protocolos que también se utilizan en esta capa como **es el protocolo de resolución de direcciones o ARP**. Es un protocolo que es capaz de encontrar la dirección MAC que corresponde a una dirección IP. El funcionamiento de este protocolo es así:

1. El protocolo ARP consulta la tabla de búsqueda.
2. Si la dirección buscada no se encuentra en la tabla, envía un paquete a la dirección de difusión de la red (una llamada a todos los equipos que forman parte de la red) con la dirección IP por la que se pregunta.
3. El protocolo ARP espera que alguna máquina responda con la dirección MAC que corresponde con dicha IP.
4. El ARP almacenará la dirección en la tabla de búsqueda.

Existe también el protocolo que realiza la operación inversa y se denomina protocolo RARP (siglas de Reverse Address Resolution Protocol).

En la capa de enlace ya hemos visto que se trabaja con la dirección MAC de cada uno de los equipos, y en la capa de red se trabaja con la dirección IP. El protocolo ARP guarda en tablas la correspondencia entre las direcciones físicas (dirección MAC) con su correspondiente dirección IP. Pero en un momento determinado puede no encontrar una entrada en la tabla o esta ha cambiado, bien porque a un equipo se le haya cambiado la tarjeta de red o porque haya cambiado su dirección IP. Es en ese momento cuando el protocolo ARP envía un paquete a través de la dirección de difusión con la dirección IP de la que desea conocer su dirección física. La máquina cuya IP coincide con la que se envió a través de protocolo ARP contestará enviando su dirección MAC.

3.- Configuración de los elementos de una red.

Caso práctico

Antonio observa ahora que Samuel está encendiendo todos los ordenadores de un aula y le pregunta qué está haciendo.

-Samuel, ¿Qué tal llevas el trabajo? ¿Qué haces ahora? -Pues nada Antonio, voy a configurar las tarjetas de red que están instaladas en los equipos con la configuración IP que me ha dado Julia. -¿Y este aparato que tienes aquí con tantas luces que es? -Es el armario de comunicaciones donde tenemos los dispositivos de interconexión central. Estos aparatos son los switch y los routers, los cuales también hay que configurar. -La verdad es que todo el proceso de instalación de redes me está pareciendo de lo más interesante. -Si, responde Samuel, se trata de un campo muy entretenido de la informática.

Una vez que ya has aprendido toda la parte de diseño de las direcciones IP de una red, tendrás que configurar cada uno de los equipos de la red con esas direcciones que les hemos asignado en el diseño de la red. Como has visto en el caso práctico, Samuel se dedica a encender los equipos de una de las aulas de la academia de Antonio para configurar las tarjetas de red que ya tiene instaladas. En este apartado verás como se realiza la configuración de las tarjetas de red de los equipos que forman parte de la red. Y esta configuración lo verás en dos versiones según el sistemaoperativo que esté instalado en los ordenadores.

Por un lado, aprenderás la configuración de la dirección IP y del resto de los parámetros de red en un equipo con un sistema operativo propietario, como es Windows. Después veremos la configuración de la red pero en un equipo con un sistema operativo libre, como es Linux.

3.1.- Configuración de la tarjeta de red en Windows.

En este apartado aprenderás a configurar una tarjeta de red en distintas plataformas de Windows. Para ello es necesario que estés atento a los siguientes vídeos de cómo se realiza la configuración de las tarjetas.

Debes conocer

Te interesará ver los siguientes vídeos de configuración de tarjetas de red en Windows.

Configurar IP estática y dinámica - Windows XP.	Configuración de la dirección IP en Windows Vista.	Configuración de la IP en Windows 7.
http://www.youtube.com/embed/cDTdXjhuKfk	http://www.youtube.com/embed/rTzyTjWADRM	

Para hacer la simulación de configuración de redes lo vas a realizar con máquinas virtuales. En los siguientes enlaces se explica como se configura una red con máquinas virtuales y como poner en red una máquina virtual con otra real con VMware, aunque el proceso es similar si utilizamos virtualBox como herramienta de virtualización. Es conveniente que veas estos enlaces y los practiques porque te resultarán necesarios para la realización de la tarea de esta unidad.

Configuración de red con máquinas virtuales.	Poner en red la máquina virtual y máquina real con VMware. Parte 1.	Poner en red la máquina virtual y máquina real con VMware. Parte 2.
http://www.youtube.com/embed/ZCWLZrka2zw	http://www.youtube.com/embed/rlHGjSo8zO4	http://www.youtube.com/embed/XTcKwEFoJeQ

Autoevaluación

¿Cuál de los siguientes parámetros no es necesario para configurar una tarjeta de red en Windows? :

- ○ Dirección IP.
- ○ Máscara de red.
- ○ Puerta de enlace.
- ○ La dirección de red.

No es correcta.

No es así.

No es correcta, vuelve a ver los vídeos.

Efectivamente es correcto, no es necesario utilizar la dirección de red.

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

3.2.- Configuración de la tarjeta de red en Linux.

Una vez que has aprendido como se configuran las tarjetas de red en Windows, harás lo mismo en una distribución de Linux. En este caso con Ubuntu. Para ello, es necesario que veas los siguientes vídeos de cómo se realiza la configuración de las tarjetas.

Debes conocer

Es necesario que veas los siguientes vídeos de configuración de tarjetas de red en Linux. Aquí se explica como es el proceso de configuración de red en un entorno Linux.

Configuración de red.

http://www.youtube.com/embed/j52TqFMQ-JE

Y ahora te vendría bien ver estos tres métodos para configurar la red en Linux.

Configuración de red. Método 1.	Configuración de red. Método 2.	Configuración de red. Método 3.
http://www.youtube.com/embed/ZIKTcGmNz9k	http://www.youtube.com/embed/m58DwhEXQe8	http://www.youtube.com/embed/GHfzppbCB_Q

Autoevaluación

En uno de estos vídeos nos dice que es la puerta de enlace predeterminada ¿A qué es equivalente este concepto?:

- ○ A la dirección IP.
- ○ A la máscara de red.
- ○ A la dirección del router.
- ○ A la dirección de red.

No es correcta.

No es así.

Efectivamente es correcto, son dos términos equivalentes.

No es correcta, vuelve a ver los vídeos.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

4.- Dispositivos de interconexión de redes. Routers.

Caso práctico

Antonio, el dueño de la academia, está conversando con Julia, acerca de los estudios de técnico superior de Administración de Sistemas en red. Comentan los distintos aparatos que están conectando en la academia.

-Mira Antonio, le dice Julia, esto que tengo aquí es un router, que es el que nos proporciona la conexión a redes externas a nuestra academia. -Vaya Julia, eso se parece bastante a los aparatos que he visto instalados en cada una de las aulas, donde se recoge el cableado de todos los ordenadores. -Eso que has visto instalado en las aulas no son routers, son switches. Sirven para conectar ordenadores si estos se encuentran en la misma red. Pero el router permite la interconexión entre ordenadores aunque estos no se encuentren en la misma red. ¿Entiendes la diferencia? -Creo que si, que he entendido la diferencia.

Un **encaminador** (o un **router en inglés**) es un dispositivo de interconexión de redes que trabaja principalmente en el nivel 3, o nivel de red, del modelo OSI. Mientras que un **conmutador** (o **switch** en inglés) lo hace principalmente en el nivel 2.

Pero cualquier equipo en general también suele trabajar en varios niveles a la vez, por ejemplo, para trabajar en el nivel 3, también hay que trabajar con los niveles inferiores (que encapsularán los paquetes de nivel 3 hasta mandarlos por un interfaz físico), o si se quiere gestionar de forma remota también necesitará todos los niveles superiores al 3 para dar soporte de telnet, ssh o gestión web.

Los encaminadores se utilizan para interconectar redes que operan con la capa de red diferente o igual. Dado que funciona en el nivel de red, los protocolos de comunicación a ambos lados del encaminador deben ser iguales y compatibles con los niveles superiores al de red (transporte y aplicación). Los niveles inferiores son los que pueden diferir sin afectar al encaminamiento.

En una red de área extensa, cualquiera de las estaciones intermedias en la transmisión

de un mensaje, se considera un encaminador debido a que funciona a nivel de red. Su función básica es dirigir los paquetes a su destino. Al recibir un paquete, el encaminador extrae la información del destinatario y decide cuál es la mejor ruta para llegar a él. El direccionamiento que utiliza el nivel de red es con las direcciones IP. El encaminador o router ha de disponer de sus propias direcciones de nivel de red, en general una IP de una subred distinta en cada uno de sus interfaces.

Entre las cuestiones que un router puede tener en cuenta para encaminar, es decir, enviar la información por un enlace u otro, tenemos:

- Número de saltos (nodos) intermedios hasta el destino.
- Velocidad de transmisión máxima de los enlaces.
- Coste de las transmisiones.
- Condiciones de tráfico de los enlaces.
- Decisiones particulares del administrador de la red.

El encaminador o router se utiliza en las siguientes condiciones:

- Proporcionar seguridad a través de sofisticados filtros de paquetes (firewalls o cortafuegos). Siendo esto una función más bien de nivel 4 y/o 7
- Integrar diferentes tecnologías de enlace de datos (nivel 2), tales como Ethernet, Token Ring, FDDI, ATM.
- Permitir la existencia de diferentes rutas alternativas contra congestiones y fallos en las comunicaciones. Ésta es una función principal del nivel 3.
- Necesidad de separar distintas subredes para tener un mejor rendimiento y/o seguridad.
- Necesidad de cambiar, traducir o enmascarar ciertos rangos de direcciones IP privados mediante NAT.

Autoevaluación

¿En que nivel del modelo OSI trabajan los routers principalmente? :

- ○ Nivel de red.
- ○ Nivel de enlace.
- ○ Nivel físico.
- ○ Nivel de transporte.

Efectivamente es correcto.

No es correcta, debes repasar.

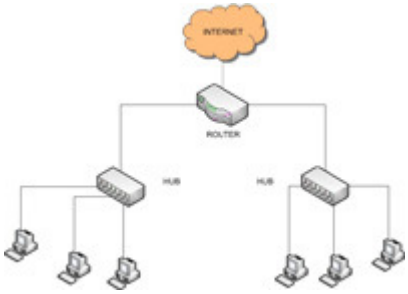
No es correcta.

Es incorrecta.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

4.1.- Introducción a los routers



Las empresas fabricantes de equipos de redes suelen distinguir, a grandes rasgos, **3 segmentos** principales de comercialización:

- **Doméstico** o PYMEs (Pequeñas y medianas empresas) o en inglés **SOHO** (Small Office Home Office)
- **Empresarial** o en inglés **Enterprise**, para empresas de más de 200 empleados o con una gran carga de tráfico digital
- Proveedor de Servicios de Internet o en inglés **ISP** (Internet Service Provider), para empresas que se dedican a dar servicios de Internet como Movistar, Vodafone, Orange, etc. con miles de clientes

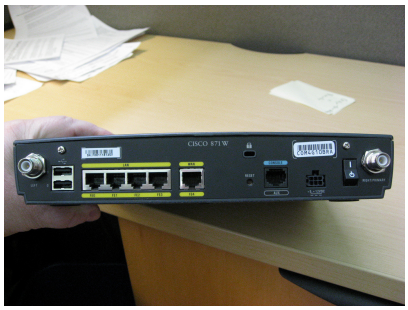
En el ámbito doméstico y PYMEs (cómo clientes de las redes de los ISP), se han usado todo tipo de routers de distintas compañías. Una de las destacadas es **Linksys**, famosa por haber desarrollado uno de los routers con más éxito comercial, el WRT54G, gracias a que tenía un firmware basado en GNU/Linux con un interfaz de gestión web muy potente e intuitivo, pero que por cumplir la licencia GPL se vieron obligados a publicar su código fuente, logrando para su sorpresa convertirse en top ventas. Al hacerse libre su firmware, fue posible para una gran comunidad de entusiastas añadirle nuevas funcionalidades para conseguir hacer cosas sólo disponibles en equipos mucho más caros (empresariales) cómo QoS (para limitar el ancho de banda), VoIP, VPN, firewall, proxy, VLANs, configuraciones avanzadas de WiFi y seguridad, clientes de Emule, Bittorrent, servidores de medios DLNA, FTP, etc.

Existen varios proyectos de desarrollo que proveen versiones mejoradas del firmware para el WRT54G cómo:

- DD-WRT
- OpenWrt
- Tomato

Estos firmwares también se han portado a otros equipos de otras marcas con hardware similar gracias a la facilidad de integrar sus drivers en el núcleo Linux.

Algunas de las compañías produciendo equipos en el segmento doméstico y PYMEs son ASUS, D-Link, TP-Link, Netgear, Belkin o Huawei.



Sin embargo, desde los inicios de Internet, la compañía con más ventas de routers en el **segmento empresarial e ISP** ha sido **Cisco Systems**, que en 2003 adquirió Linksys para intentar entrar en el segmento SOHO y en 2013 lo vendió a Belkin.

Los routers Cisco, tanto los más pequeños cómo los más grandes, siempre han estado corriendo el sistema operativo **IOS** (**Internet Operating System**, no confundir com el sistema operativo del iPhone) y han marcado una especie de

estandar de facto en la industria a la hora de usar los comandos de gestión de los routers.

> Tradicionalmente los routers se han configurado mediante comandos en una consola de texto accediendo a través de un puerto serie (ahora también USB o Universal Serial Bus), o en remoto mediante telnet o ssh. Aún a día de hoy sigue siendo la forma más óptima y útil de acceder a toda la funcionalidad y de poder realizar **scripts** de configuración de múltiples equipos a la vez. Por eso es conveniente conocer estos comandos, incluso aunque últimamente también sea posible gestionarlos mediante interfaz gráfico web en ciertos casos.

Por citar a otras compañías, en el segmento ISP o de grandes empresas, la competencia de Cisco siempre ha sido Juniper y más recientemente Huawei, con equipos muy similares a los de Cisco (con los mismos comandos de IOS, e incluso los mismos bugs, llevándoles a juicio...) pero a precios más competitivos. Cisco perdió mucho mercado de exportaciones tras conocerse el uso de puertas traseras en los equipos de todos los fabricantes americanos para dar acceso a la NSA.

Por otro lado, las funcionalidades de un router siempre se han podido realizar mediante ordenadores personales (PCs) con una o varias tarjetas de red cableadas y/o inalámbricas, normalmente corriendo Unix/Linux por rendimiento, aunque también es posible hacerlo con Windows.

Recomendación

La lista de conceptos, siglas y comandos en el mundo de las redes e informática es muy amplio. Se recomienda usar y personalizar alguna guía cómo esta chuleta usada en un curso de Redes Locales. También puedes usar herramientas de mapas conceptuales.

4.1.1.- Router doméstico o para PYMEs

Te interesará saber que un **encaminador inalámbrico**, o router inalámbrico o router wireless, funciona igual que un router cableado tradicional. La diferencia entre uno y otro es que los routers inalámbricos permiten realizar una interfaz con redes fijas y móviles. Comparten el mismo principio que un enrutador tradicional. La diferencia es que éste permite la conexión de dispositivos inalámbricos a las redes a las que el enrutador está conectado mediante conexiones por cable.

Ésta es una de las características diferenciadoras entre routers domésticos y "profesionales", que en los primeros se trata de integrar en un sólo equipo la mayor funcionalidad posible, mientras que en los routers profesionales se suele dejar por separado los equipos con función de **punto de acceso WiFi**, los **switches** para conectar los clientes de cableado LAN, el **firewall**, el módem ADSL o de fibra (ONT), etc.

Otra característica típica de los routers domésticos o para PYMEs es que vienen preconfigurados con todo lo básico para empezar a enchufarlo y listo:

- IP privada en la LAN, normalmente la 192.168.0.1 /24 o 192.168.1.1 /24
- servidor DHCP para adjudicar direcciones IP privadas a los clientes de la LAN que se conectarán al "swith integrado" en el router que suele ser de 4 puertos
- IP dinámica en el interfaz WAN para recibir una IP pública por parte del ISP
- NAT preconfigurado para traducir las IPs privadas de la LAN a la IP pública de la WAN
- Interfaz de gestión web accesible por defecto desde la LAN, normalmente accediendo a la página http://192.168.0.1 o http://192.168.1.1 y usuario y contraseña "admin" y "admin"
- Firewall preconfigurado para no permitir conexiones entrantes provenientes de Internet, salvo para que los técnicos del ISP se conecten remotamente
- WiFi preconfigurado con contraseña escrita en una pegatina del router
- Interfaz WAN de Ethernet, ADSL o fibra con datos preconfigurados de conexión de enlace
- Ruta estática predeterminada para encaminar todo el tráfico por defecto hacia el interfaz WAN con el ISP

PRÁCTICA: ADMINISTRACIÓN DE UN ROUTER DOMÉSTICO

Conectándote al router de tu casa, de tu centro y/o usando webs con simuladores de interfaces de gestión de routers cómo

- http://ui.linksys.com/
- http://support.dlink.com/FAQView.aspx?f=G4TiCUaI4km213a2MATkCA%3d%3d

Toma capturas y comenta desde dónde se puede realizar las siguientes acciones:

- Cambiar el usuario y/o contraseña de acceso a la web de administración del router
- Realizar una copia de seguridad de la configuración del router (se recomienda que la realices por si tocas algo indebido)
- Cambiar la IP privada en la LAN del router
- Reservar un rango de direcciones IP que no se asignarán en el servidor DHCP a los clientes de la LAN
- Cambiar la configuración de NAT y/o firewall para permitir conexiones entrantes hacia una IP y puerto determinados
- Cambiar la SSID y contraseña de la conexión WiFi
- Redirecciona los puertos NAT para que puedas jugar on-line con tu consola PS4 suponiendo que se le ha asignado (o configurado estáticamente) una dirección IP 192.168.1.125
  - Puedes guiarte por este par de vídeos que muestran cómo hacerlo en un router de Vodafone y un Comtrend de Jazztel

Debes conocer

Vídeos explicativos sobre como configurar un router inalámbrico.

Configurar un router inalámbrico. Parte 1.	Configurar un router inalámbrico. Parte 2.	Configurar un router ADSL inalámbrico.
http://www.youtube.com/embed/RBsLgCrfe2Q	http://www.youtube.com/embed/sgBViMx3EBE	http://www.youtube.com/embed/9DCY8XwButQ

Autoevaluación

¿Cómo se denomina al nombre de una red inalámbrica?

- ○ Wireless Chanel
- ○ SSID.
- ○ WAP
- ○ Ninguna de las anteriores

No es correcto.

Muy bien, estuviste atento a los vídeos.

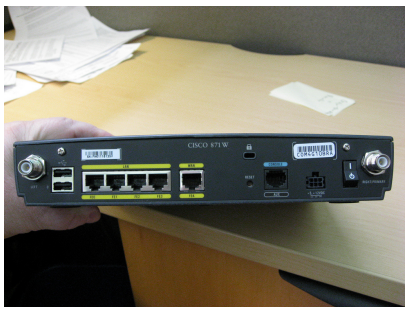
Vuelve a ver los vídeos con atención.

Eso no está bien.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

4.1.2.- Configuración de un router profesional



Dentro de tu vida profesional como técnico o técnica de sistemas microinformáticos y redes, es más que probable que tengas la necesidad de configurar un router en una red. Para funcionar correctamente, un encaminador necesita ajustar un conjunto de parámetros:

- Direcciones de los puertos y redes a las que está conectado.
- Algoritmos de encaminamiento a usar.
- Tablas de encaminamiento estáticas para configurar rutas fijas en la red.

Además, hay otros parámetros relacionados con el filtrado de paquetes, seguridad, etc, que también pueden ser configurados.

PRÁCTICA: CONFIGURACIÓN DE UN ROUTER PROFESIONAL.

Este proceso consta en la configuración más básica de un router explicando los comandos que se emplean aunque éstos pueden variar en función del fabricante del router.

Nos centraremos en la configuración vía consola desde el puerto serie del PC, es decir, conectándonos al router mediante una sesión que abriremos mediante un hyperterminal. Al contrario de los routers domésticos o para PYMEs que vienen preconfigurados con todo lo básico (IPs privada en la LAN, servidor DHCP para los clientes de la LAN, ip dinámica en el interfaz WAN, NAT preconfigurado, etc.), los routers profesionales suelen venir sin ninguna configuración de fábrica para que en caso de que se instalen en una red dónde ya existan otros routers no interfiera con los servidores de DHCP, etc.

Si el router viene con una configuración de fábrica se podría acceder a él vía web conectándose a su LAN. En este caso, se podría reconfigurar siguiendo el proceso que explicaría el manual de usuario o usuaria que el fabricante facilita, pudiendo ser ligeramente diferente según el modelo.

Sin embargo, cómo ya se ha comentado, éste no suele ser el caso en los routers comerciales (cómo los Cisco) que necesitas previamente conectarte a través de una consola en su puerto serie para configurarle las IPs de sus distintos puertos, configurarle opcionalmente el DHCP, NAT, encaminamientos, etc.

Caso práctico

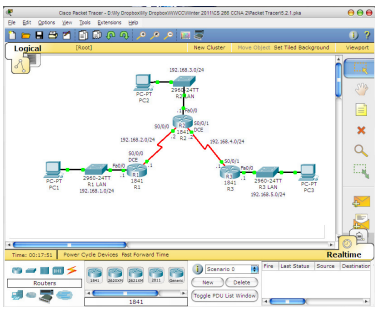
En el siguiente enlace encontraréis toda la práctica explicada de cómo se configura un router profesional desde la consola o puerto serie con el programa hyperterminal que venía de forma predeterminada en ciertas versiones de MS Windows.

Si tu versión de Windows no disponer del programa Hyperterminal, puedes tratar de descargarlo de Microsoft o usar un programa alternativo y más completo como Putty o SecureCRT.

Si no dispones en tu centro de un router Cisco para hacer la práctica, puedes recurrir al uso de simuladores didácticos como Packet Tracer o emuladores (más reales aunque más complicados) como GNS3.

Configuración de un router. (0.92 MB)

4.1.3.- PCs como emuladores y simuladores de routers



Existen programas para PC que permiten "simular" varias redes interconectadas con varios equipos (PCs, switches, puntos de acceso WiFi, routers, firewalls, etc.) en un escenario que permite jugar a configurarlos simulando un interfaz real de comandos de configuración y probar la conectividad de los distintos elementos, incluso analizando cómo se envían las diferentes unidades de datos en cada uno de los niveles OSI.

Uno de los programas simuladores de redes más usado en entornos educativos es el **Cisco Packet Tracer** disponible para descargar para Windows y Linux (la versión 5 funciona con WINE) a través de la Cisco Networking Academy. Existe un paquete para traducirlo al español. Incluso existe una app para Android y iPhone.

Por otro lado, existen "emuladores" de routers comerciales como GNS3, que permite por un lado disponer de toda la funcionalidad de routers de varios fabricantes como Cisco o Juniper usando directamente sus firmware y emulando su hardware. Permite tener varios routers, switches y equipos interconectados de una forma más real, llegando incluso a poder interconectar a una red real física. GNS3 es un software muy avanzado y no es simple de instalar/configurar, por eso se recomienda usar soluciones todo-en-uno que implementan varios emuladores de diferentes equipos preparados para funcionar como GNS3 Workbench o Live Raizo. Otro problema de los "emuladores" es que necesitan más recursos de RAM y CPU para poder emular varios equipos a la vez, mientras que un simulador no necesita tantos recursos, aunque no sea tan real y por tanto puede carecer de algunas funcionalidades.

Por último existen implementaciones de funcionalidades de routers nativas en los sistemas operativos de PCs, y también implementaciones de encaminamientos dinámicos avanzados para Linux como el proyecto libre que empezó siendo Zebra, continuó como Quagga y a día de hoy sigue evolucionando como Free Range Routing (FRR).

Para saber más

Aunque en los ejemplos de encaminamiento se trabajará con el simulador Packet Tracer, existen multitud de emuladores y simuladores desde los más básicos a los más completos. Para una larga lista con un breve análisis de cada uno de ellos puedes consultar ésta web que se va actualizando y en los comentarios se recomiendan algunos para usos concretos

4.2.- PCs como estaciones finales y como routers.

Tienes que saber que se puede utilizar un PC para realizar las funciones de encaminamiento entre distintos segmentos de red, como si de un router se tratara. En redes con distintos segmentos de red se utilizan routers específicos para hacer de encaminadores entre dos segmentos de red, pero también se pueden utilizar varios PC con distintos sistemas operativos tanto de la familia de Windows como de Linux para hacer de enrutador entre esos segmentos de red.

Verás en el siguiente enlace como configurar un pc como router.

Debes conocer

Te interesará ver el siguiente vídeo sobre la configuración del PC como router.

Configurar un PC como router

https://www.youtube.com/embed/XDrhw-n2TZE

Además de visitar este enlace, es necesario que aprendas a utilizar un PC como router en máquinas virtuales. Para ello tienes a tu disposición los siguientes documentos para realizar estas operaciones con el software de simulación VMware. El procedimiento es análogo si prefieres utilizar VirtualBox.

Máquinas virtuales. Parte I. (0.58 MB)

Máquinas virtuales. Parte II. (0.35 MB)

Máquina virtual con Ubuntu. (0.08 MB)

Para saber más

Si te apetece seguir ampliando conocimientos sobre estos temas de

enrutamiento utilizando PC, te recomiendo que visites los siguientes vídeotutoriales.

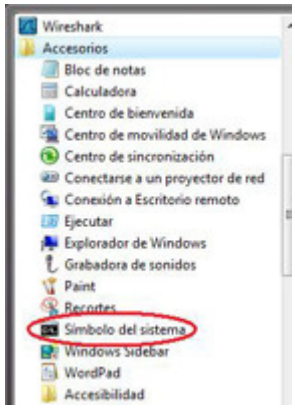
Manual de enrutamiento con Windows 2003 Server.	Enrutamiento con Ubuntu.	Configurar un PC como NAT.
http://www.youtube.com/embed/-6Gnezvz5_w	http://www.youtube.com/embed/CXzCaG4nSSs	http://www.youtube.com/embed/rRiFaEYu-1w

4.2.1.- Comandos TCP/IP para Windows de información.

A lo largo de tu vida profesional te darás cuenta que es necesario conocer una serie de comandos TCP/IP que te permitirán analizar e incluso configurar distintos aspectos de tu red en Windows. Todos los comandos que aprenderás en este apartado son para ejecutarlos en la ventana del sistema, en cualquier sistema Windows.

Para abrir la ventana del sistema puedes hacerlo de **dos modos**:

1. Inicio, todos los programas, accesorios, Símbolo del sistema.
2. Inicio, Ejecutar, escribes el comando **cmd** y aceptar.



Una vez en la ventana del sistema, existen una serie de comandos que te serán útiles cuando trabajes con redes Windows. A continuación tienes un listado de **comandos** con sus opciones (escríbelos en minúsculas):

- **Ping** [IP o host]: diagnostica la conexión entre la red y una dirección IP remota.
  - **-t**: permite hacer pings de manera continua, para detenerlo ctrl-c
  - **-l**: genera una carga de red, especificando el tamaño del paquete.

- **Tracert** [@IP o nombre del host]: muestra todas las direcciones IP intermedias por las que pasa un paquete entre el equipo local y la dirección IP especificada.

- **Ipconfig** /all [/release [tarjeta]] [/renew [tarjeta]] /flushdns /displaydns /registerdns [-a] [-a] [-a]: Sin opciones, este comando muestra la dirección IP activa, la máscara de red, así como, la puerta de enlace predeterminada al nivel de las interfaces de red conocidas en el equipo local:
  - /**all**: Muestra toda la configuración de la red, incluyendo los servidores DNS, WINS, DHCP, etc ...
  - /**renew [tarjeta]**: Renueva la configuración DHCP de todas las tarjetas (si ninguna tarjeta es especificada) o de una tarjeta específica si utiliza el parámetro tarjeta. El nombre de la tarjeta, es el que aparece con ipconfig sin parámetros.
  - /**release [tarjeta]**: Envía un mensaje DHCPRELEASE al servidor DHCP para liberar la configuración DHCP actual y anular la configuración IP de todas las tarjetas (si ninguna tarjeta es especificada), o de sólo una tarjeta específica si utiliza el parámetro tarjeta. Este parámetro desactiva el TCP/IP de las tarjetas configuradas a fin de obtener automáticamente una dirección IP.
  - /**flushdns**: Vacía y reinicializa el caché de resolución del cliente DNS. Esta opción es útil para excluir las entradas de caché negativas así como todas las otras entradas agregadas de manera dinámica.
  - /**displaydns**: Muestra el caché de resolución del cliente DNS, que incluye las entradas precargadas desde el archivo de host local así como todos los registros de recursos recientemente obtenidos por las peticiones de nombres resueltas por el ordenador. El servicio Cliente DNS utiliza esta información para resolver rápidamente los nombres frecuentemente solicitados, antes de

interrogar a sus servidores DNS configurados.
    - /**registerdns**: Actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.

- **Netstat** [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]: Muestra el estado de la pila TCP/IP en el equipo local.
    - **-a** Muestra todas las conexiones y puertos de escucha. (Normalmente las conexiones del lado del servidor no se muestran).
    - **-e** Muestra estadísticas Ethernet. Se puede combinar con la opción –s.
    - **-n** Muestra direcciones y números de puerto en formato numérico.
    - **-p** proto Muestra las conexiones del protocolo especificado por proto; proto puede ser tcp o udp. Utilizada con la opción –s para mostrar estadísticas por protocolo, proto puede ser tcp, udp, o ip. -r Muestra el contenido de la tabla de rutas.
    - **-s** Muestra estadísticas por protocolo. Por defecto, se muestran las estadísticas para TCP, UDP e IP; la opción –p puede ser utilizada para especificar un subconjunto de los valores por defecto.
    - **intervalo** Vuelve a mostrar las estadísticas seleccionadas, con una pausa de “intervalo” segundos entre cada muestra. Con ctrl-c se detiene la presentación de las estadísticas.

4.2.2.- Comandos TCP/IP para Windows de enrutamiento.

En este apartado puedes ver el resto del listado de comandos TCP/IP para Windows. Te serán muy útiles para analizar y configurar redes Windows.

- **Route** [-f] [comando [destino] [MASK máscara de red] [puerto de enlace]: Muestra o modifica la tabla de enrutamiento.
  - o -f Borra, de las tablas de enrutamiento, todas las entradas de las puertas de enlace. Utilizada conjuntamente con otro comando, las tablas son borradas antes de la ejecución del comando.
  - -p Vuelve persistente la entrada en la tabla después de reiniciar el equipo.
  - comando: Especifica uno de los cuatro comandos siguientes:
    - DELETE: borra una ruta.
    - PRINT: Muestra una ruta.
    - ADD: Agrega una ruta.
    - CHANGE: Modifica una ruta existente.
  - destino: Especifica el host.
  - MASK: Si la clave MASK está presente, el parámetro que sigue es interpretado como el parámetro de la máscara de red.
  - máscara de red: Si se proporciona, especifica el valor de máscara de subred asociado con esta ruta. Si no es así, éste toma el valor por defecto de 255.255.255.255.
  - puerta de enlace: Especifica la puerta de enlace.
  - METRIC: Especifica el coste métrico para el destino.

- **ARP**: Resolución de direcciones IP en direcciones MAC. Muestra y modifica las tablas de traducción de direcciones IP a direcciones Físicas utilizadas por el protocolo de resolución de dirección (ARP).
  - ARP -s adr_inet adr_eth [adr_if]
  - ARP -d adr_inet [adr_if]
  - ARP -a [adr_inet] [-N adr_if]
  - -a Muestra las entradas ARP activas interrogando al protocolo de datos activos. Si adr_inet es precisado, únicamente las direcciones IP y Físicas del ordenador especificado son mostrados. Si más de una interfaz de red utiliza ARP, las entradas de cada tabla ARP son mostradas.
  - -g Idéntico a –a.
  - adr_inet Especifica una dirección Internet.
  - -N adr_if Muestra las entradas ARP para la interfaz de red especificada por adr_if.
  - -d Borra al host especificado por adr_inet.
  - -s Agrega al host y relaciona la dirección Internet adr_inet a la Física adr_eth. La dirección física está dada bajo la forma de 6 bytes en hexadecimal separados por guiones. La entrada es permanente.
  - adr_eth Especifica una dirección física.

- adr_if Precisado, especifica la dirección Internet de la interfaz cuya tabla de traducción de direcciones debería ser modificada. No precisada, la primera interfaz aplicable será utilizada.

- **Nbtstat**: Actualización del caché del archivo Lmhosts. Muestra estadísticas del protocolo y las conexiones TCP/IP actuales utilizando NBT (NetBIOS en TCP/IP).
  - NBTSTAT [-a Nom Remoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-s] [S] [intervalo]
  - -a (estado de la tarjeta) Lista la tabla de nombres del equipo remoto (nombre conocido).
  - -A (estado de la tarjeta) Lista la tabla de nombres del equipo remoto (dirección IP)
  - -c (caché) Lista el caché de nombres remotos incluyendo las direcciones IP.
  - -n (nombres) Lista los nombres NetBIOS locales.
  - -r (resueltos) Lista de nombres resueltos por difusión y vía WINS.
  - -R (recarga) Purga y recarga la tabla del caché de nombres remotos.
  - -S (sesión) Lista la tabla de sesiones con las direcciones de destino IP.
  - -s (sesión) Lista la tabla de sesiones establecidas convirtiendo las direcciones de destino IP en nombres de host a través del archivo host.

4.2.3.- Comandos TCP/IP para Windows de conexión.

Este ya es la última parte de la lista de comandos para TCP/IP para Windows.

- **Telnet**: El comando telnet permite acceder en modo Terminal (Pantalla pasiva) a un host remoto. Este también permite ver si un cualquier servicio TCP funciona en un servidor remoto especificando después de la dirección IP el número de puerto TCP.
  - telnet < IP o host >
  - telnet < IP o host > < port TCP >

De este modo podemos verificar si el servicio SMTP, por ejemplo, funciona en un servidor Microsoft Exchange, utilizando la dirección IP del conector SMTP y luego 25 como número de puerto. Los puertos más comunes son:

- ftp (21),
- telnet (23),
- smtp (25),
- www (80),
- kerberos (88),
- pop3 (110),
- nntp (119) ,
- et nbt (137-139).

- **Hostname**: Muestra el nombre del equipo.
- **Ftp**: Cliente de descarga de archivos.
  - ftp –s:< file>
  - -s: esta opción permite ejecutar un FTP en modo batch: especifica un archivo textual conteniendo los comandos FTP.

Autoevaluación

¿Qué comando se utiliza si quieres comprobar la conexión de tu equipo con una dirección remota?:

- ○ Telnet.
- ○ Arp.
- ○ Ping.
- ○ Tracert.

Repasa el listado.

Vuelve a repasar.

Efectivamente es correcto.

No es correcta.

Solución

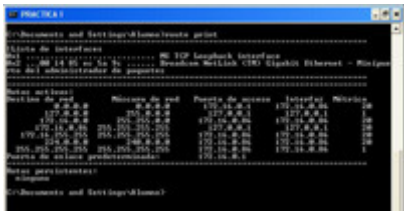
1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

4.3.- Tabla de rutas y encaminamiento

Para saber como funciona un encaminador o router necesitas saber que estos disponen de una tabla de rutas con las que deciden por qué camino deben enviar los mensajes para que lleguen a su destino. Estas tablas de rutas, o tablas de encaminamiento, tienen en cada fila:

1. La dirección de red a las que se puede llegar desde este router.
2. La dirección IP del router por el que debe salir el mensaje.
3. Máscara de red utilizada en cada red.
4. Un parámetro que indica el coste de ir por ese camino.

En la siguiente imagen aparece una tabla de un router donde se ven los campos por los que está formada una tabla de encaminamiento.



Un router funciona básicamente de la siguiente manera:

1. El router **recibe** un mensaje con una dirección IP del origen y una dirección IP del destino donde debe llegar ese mensaje.
2. Con la máscara de red que tiene guardada en su tabla de encaminamiento, es capaz de **averiguar** cual es la dirección de red a la que va dirigido ese mensaje.
3. **Consulta** en su tabla la dirección de red (primera columna de la tabla, que corresponde con la dirección de red de destino) y mira la dirección IP del router por el que debe salir el mensaje (columna de interfaz).
4. Entonces **envía** ese mensaje por la dirección correspondiente.
5. En la columna métrica se **especifica el coste** que tiene para ese mensaje continuar por ese camino. (Si hubiera dos posibles rutas por dos routers diferentes, podría elegir el que menos coste tenga).

Debes conocer

Te vendrá bien ver en este ejemplo un router que tiene conectadas dos redes y una salida a Internet. La tabla de enrutamiento del router sería la siguiente:

En las tablas de encaminamiento no aparecen direcciones de estaciones destinatarias, sino solamente de redes destinatarias. De este modo se simplifican el número de entradas de la tabla de encaminamiento.

¿Cómo crees que averigua el router la dirección IP de una estación concreta?

Cuando el router recibe un paquete:

- toma la dirección IP de la estación de destino.
- Pone a 0 los bits de número de estación y la compara con las entradas disponibles en su tabla.

¿Y cómo pone a 0 los bits de número de estación?

- Usando la máscara de red. Realiza la operación AND de la IP de destino con la máscara de red.

4.3.1.- Enrutamiento estático.

Es necesario que sepas que el enrutamiento es el relevo de tráfico de una red a otra, paquete por paquete. Consiste en pasar la responsabilidad de un enrutador a otro, es decir, un enrutador decide cómo enviar un paquete y se desentiende de lo que le pueda pasar al mismo de ahí para adelante, eso en inglés se llama **relay**, en español se llama *relevo*. Otra forma de decirlo, más técnicamente, **es la conmutación de paquetes de una red a otra**. La idea del enrutamiento está estrechamente ligada a las redes/subredes (IP, IPX, etc.) y al hecho de que los enrutadores son los separadores de esas redes/subredes. El enrutador es un dispositivo que conoce *hacia dónde* quedan las redes que él conoce. Este "*hacia dónde*" *indica* de cuál de sus interfaces, o **a través de qué enrutador vecino, se puede llegar más *cerca* a las redes destino** en cuestión.

La **base de todas estas decisiones es la tabla de enrutamiento**, una especie de base de datos sobre las rutas que dice justamente esa información: **por dónde se está más *cerca* de una red en particular**. La tabla de enrutamiento es la información que usa el enrutador. Es decir, aún si están configuradas ciertas rutas, eso no significa que tengan que aparecer en la tabla de enrutamiento, y por ende, no implica que se vayan a enrutar. Pero si éstas están en la tabla de enrutamiento, eso sí va a influir en la forma en que se enrutan los paquetes destinados a una red de las que están presentes en la tabla.

¿Entonces qué le pasa a un paquete IP cuando llega al enrutador? Simple, si el paquete tiene una dirección IP que no pertenece a alguna interfaz del enrutador (es decir **que no sea para el enrutador mismo**, como un telnet por ejemplo), **se le busca un destino en la tabla de enrutamiento** y ese destino se debe resolver en una interfaz de salida o una IP de siguiente salto (**un vecino al que se asocia mayor *cercanía* a la red destino**). **El paquete entonces es encapsulado** con encabezados de **capa dos** apropiados para la interfaz de salida. Una vez que el paquete es encapsulado en la tecnología de la interfaz de salida, la responsabilidad de éste enrutador termina. **El siguiente enrutador deberá repetir el proceso, y nosotros debemos esperar que el resultado sea que el paquete estará efectivamente más cerca de la red destino**. El proceso que acabo de describir sucede, en teoría, **para cada paquete** y de este modo, el flujo de datos entre dos nodos de la red (dos PCs o dos dispositivos de red) llega a su destino.

Es importante notar que nunca hemos dicho red origen y eso se debe a que **el paradigma del enrutamiento sólo considera hacia dónde se dirige el tráfico**, el tráfico de vuelta se considera también un destino pero en dirección opuesta. Es decir, el enrutamiento se debe analizar en una dirección y luego se debe analizar en la dirección inversa, para poder garantizar que existe la información necesaria en las tablas de enrutamiento para que el tráfico pueda regresar. **¡El hecho de que el tráfico llegue al destino original no garantiza que el tráfico pueda regresar!**

Lo único que parece faltar de la introducción anterior es aclarar qué es exactamente **una ruta**. Bien, una ruta es una red destino con unos parámetros asociados, como son la interfaz de salida y la métrica o costo asociado al camino para llegar hasta la red destino, entre otras cosas. Es importante reconocer que el elemento clave de una ruta es la red destino. Consecuencia de lo anterior es que una tabla de enrutamiento debe tener todas las rutas que existan en un dominio de enrutamiento.

¿Cómo se configura el enrutamiento?: En resumen, el enrutamiento es llenar la tabla de rutas con información de cómo se envían los paquetes. Además, todos los enrutadores de la red tendrán esa misma información. Esta información le llega al enrutador, bien sea porque la conoce directamente al configurarla manualmente, o porque se le informa a través de un protocolo de enrutamiento en particular.

Debes conocer

En el siguiente enlace encontrarás un documento en el que se explica detalladamente en que consiste el enrutamiento estático, que función concreta tienen las tablas de enrutamiento o tablas de encaminamiento así como un ejemplo completo realizado en Packet Tracer. También se incluyen diagramas físicos y lógicos de una red. Este documento es muy importante ya que te ayudará a tener una visión de conjunto de todo lo aprendido hasta ahora.

Enrutamiento estático. (0.17 MB)

4.3.2.- Encaminamiento entre tres redes y dos routers.

Antes de continuar avanzando en la teoría sería interesante que vieras algún ejemplo de cómo se realiza el encaminamiento en un escenario concreto. El ejemplo elegido ha sido el encaminamiento entre tres redes utilizando dos routers.

Imagínate que estás trabajando para una empresa que tiene tres redes de área local independientes entre ellas. La dirección de red de cada una de estas redes son las siguientes:

- **Red 1**: Dirección de red: 192.168.1.0
- **Red 2**: Dirección de red: 192.168.2.0
- **Red 3**: Dirección de red: 192.168.3.0

El objetivo principal es que tres redes con direcciones IP independientes y aisladas puedan comunicarse entre sí. Para ello, tendrás que colocar un router entre la red 1 y la red 2 y otro router entre la red 2 y la red 3. Cada uno de los routers tendrá dos direcciones IP asignadas, una por cada una de las redes a las que está conectado. Y esas direcciones que se asignan a los router serán las puertas de enlace de cada una de estas redes. Lo verás mejor con el ejemplo.

- **Router 1**: Conectado a la Red 1 y a la Red 2. Se le asigna a la conexión de la Red 1 la dirección 192.168.1.1 y a la conexión de la Red 2 la dirección 192.168.2.1. Estas direcciones serán a su vez las puertas de enlace de las respectivas redes.
- **Router 2**: Conectado a la Red 2 y a la Red 3. Se le asigna a la conexión de la Red 3 la dirección 192.168.3.1 y a la conexión de la Red 2 la dirección 192.168.2.2 (ya que la dirección 192.168.2.1 está ocupada por el otro router). Estas direcciones serán a su vez las puertas de enlace de las respectivas redes.

Tal y como está configurado, la Red 1 se puede comunicar con la Red 2, la Red 2 se comunica con la Red 3, pero no se pueden conectar la Red 1 con la Red 3 hasta que no configuremos adecuadamente los routers.

En el Router 1 hay que decirle que para llegar desde la Red 1 a cualquier dirección de la Red 3 tiene que dar un salto y dirigirse a la dirección 192.168.2.2

En el Router 2 hay que decirle que para llegar desde la Red 3 a cualquier dirección de la Red 1 tiene que dar un salto y dirigirse a la dirección 192.168.2.1

Esta información sobre los saltos, para indicar a los routers qué caminos tienen que seguir, se guardará en cada uno de los routers en forma de tabla. Dicha tabla se denomina **Tabla de rutas, tabla de enrutamiento o tabla de encaminamiento** y la analizarás con más detalle a lo largo de este tema.

En la siguiente imagen se ve un esquema completo del ejemplo que acabas de ver.

Debes conocer

Te propongo que veas estos vídeos sobre encaminamiento entre redes. El primero de los enlaces es el caso que acabas de estudiar y los otros dos vídeos se ve un ejemplo de conexión entre dos redes con el programa Packet Tracer.

Encaminamiento entre tres redes con dos routers	Interconexión de redes. 2 Redes conectadas por un router. Parte 1.	Interconexión de redes. 2 Redes conectadas por un router. Parte 2.
http://www.youtube.com/embed/DrRgqcmJeMI	http://www.youtube.com/embed/fuc3LIpUD1M	http://www.youtube.com/embed/IBYZgImj2O4

4.3.3.- Enrutamiento estático con nodos en anillo. Diseño de la red.

Otro caso de estudio referente al enrutamiento estático puede encontrarlo al intentar conectar tres redes de área local que están aisladas y que son independientes, en forma de anillo. Para ello necesitas tres routers colocados de la siguiente manera:

Si la Red 1 necesita comunicarse con algún equipo externo a su red, sale a través de la puerta de enlace del Router 1. Lo mismo sucede con la Red 2 y el Router 2 y la Red 3 con la puerta de enlace del Router 3.

Si quieres conseguir que la comunicación a través de las redes sea en forma de anillo hay que configurar los routers de manera que del Router 1 la información vaya al Router 2, del Router 2 al Router 3 y del Router 3 al Router 1. Dicho de otro modo, habrá que configurar las tablas de enrutamiento de forma adecuada en cada uno de ellos.

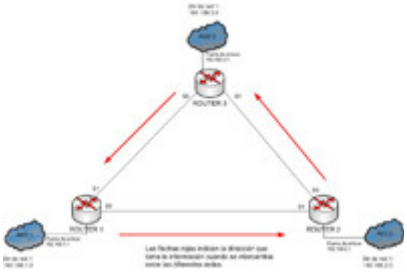
Partimos como ejemplo que las direcciones de las distintas redes son las siguientes:

- Red 1: 192.168.1.0
- Red 2: 192.168.2.0
- Red 3: 192.168.3.0

Las direcciones utilizadas como puertas de enlace son las siguientes:

- Puerta de enlace de la red 1: 192.168.1.1
- Puerta de enlace de la red 2: 192.168.2.1
- Puerta de enlace de la red 3: 192.168.3.1

Después de conocidos los datos iniciales, verás ahora como se conectan los routers entre sí. Cada uno de ellos tiene dos puertos seriales, que son los puertos a través de los cuales se puede conectar a otros routers. Cada router utiliza uno de los puertos como puerto origen de la comunicación y otro puerto como destino. Se dará el nombre S0 a los puertos de origen y S1 a los puertos destino. Se utiliza como nombre de los puertos origen S0 y los puertos destino S1. Así queda establecido cuál es el origen y el destino de cada una de las conexiones. Con esto consigues que la información vaya del Router 1 al Router 2, del Router 2 al Router 3 y del Router 3 al Router 1, como ves en este esquema:



Autoevaluación

¿Qué es un puerto serial de un router?:

- ○ El puerto que se utiliza para conectar un router con otros routers.
- ○ Es el equivalente a una puerta de enlace.
- ○ El puerto que comunica directamente a dos redes independientes.
- ○ Ninguna de las anteriores.

Efectivamente, es correcto.

Repasa el apartado.

Vuelve a repasar.

No es correcta.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

4.3.4.- Enrutamiento estático con nodos en anillo. Puertos seriales.

En este apartado continuamos con el ejemplo del apartado anterior. El siguiente paso será establecer las direcciones de los puertos seriales de cada uno de los routers. Estas direcciones tienen que ser del mismo rango de red para cada par de enlaces directos entre dos routers. En el ejemplo se utilizan las siguientes direcciones IP:

- Router 1, puerto S0: 200.100.5.1
- Router 2, puerto S1: 200.100.5.2
- Router 2, puerto S0: 200.100.10.1
- Router 3, puerto S1: 200.100.10.2
- Router 3, puerto S0: 200.100.15.1
- Router 3, puerto S1: 200.100.15.2

En el siguiente diagrama verás cual es la situación de partida para poder configurar las tablas de rutas de los routers. Se toman como datos las direcciones de red propuestas en el apartado anterior:

En base a estos datos, puedes obtener la información para configurar adecuadamente la tabla de rutas de cada uno de los routers.

Si la configuración que se pretende es en forma de anillo, la información viajará desde el router 1 al router 2, del router 2 al router 3 y del router 3 al router 1. Verás ahora con detalle como se configuran las tablas de encaminamiento.

4.3.5.- Enrutamiento estático con nodos en anillo. Configuración de los routers.

Se empieza ahora la configuración de cada uno de los routers. Para el router 1: si un ordenador de la red 1 quiere comunicarse con otro de la red 2, la información ha de pasar por el puerto s1 del router 2. Si un ordenador de la red 1 quiere comunicarse con otro de la red 3, la información ha de pasar por el mismo puerto s1 del router 2. No se puede utilizar el enlace directo entre el router 1 y el router 3 porque entonces la información no haría un recorrido en forma de anillo. Dicho esto, se puede concluir que en la tabla de enrutamiento del **router 1** se tendrá la siguiente información:

- Dirección de destino: 192.168.2.0 tiene que pasar por 200.100.5.2
- Dirección de destino: 192.168.3.1 tiene que pasar por 200.100.5.2

Si un equipo de la red 2 quiere comunicarse con un equipo de la red 2, la información tiene que pasar a través del puerto s1 del router 3. Y si de la red 2 hubiera algún equipo que quisiera conectarse con otro equipo de la red 1, también lo haría a través del mismo puerto. Con lo que la tabla de rutas del **router 2** sería así:

- Dirección de destino: 192.168.3.0 tiene que pasar por 200.100.10.2
- Dirección de destino: 192.168.1.0 tiene que pasar por 200.100.10.2

Y siguiendo un razonamiento análogo para el **router 3** obtendrías la siguiente información sobre la tabla de rutas del router 3:

- Dirección de destino: 192.168.1.0 tiene que pasar por 200.100.15.2
- Dirección de destino: 192.168.2.0 tiene que pasar por 200.100.15.2

Esta configuración de las tablas de enrutamiento tiene que ser así, si lo que se pretende conseguir es que la comunicación entre los routers sea en forma de anillo.

Debes conocer

En los siguientes enlaces encontrarás una serie de vídeos que te servirán para dejar completamente fijado este ejemplo de enrutamiento estático con nodos en anillo. La simulación se realiza con el programa Packet Tracer.

Enrutamiento estático con nodos en anillo. Simulación Práctica 1. Parte 1.

Enrutamiento estático con nodos en anillo. Simulación Práctica 1. Parte 2

http://www.youtube.com/embed/b6q-wgz2tFg

http://www.youtube.com/embed/FszCltZqCXo

Enrutamiento estático con nodos en anillo. Simulación práctica 2. Parte 1.

http://www.youtube.com/embed/f5s6LCINHAY

Enrutamiento estático con nodos en anillo.Simulación práctica 2. Parte 2.

http://www.youtube.com/embed/VHV66OoaniM

Enrutamiento estático con nodos en anillo.Simulación práctica 2. Parte 3.

http://www.youtube.com/embed/2qtK3ZaC3Ec

Para saber más

En los siguientes enlaces encontrarás una serie de enlaces a vídeos sobre enrutamiento dinámico.

Dos redes con dos routers mediante encaminamiento dinámico. Parte 1.

http://www.youtube.com/embed/I5uyWntfe10

Dos redes con dos routers mediante encaminamiento dinámico. Parte 2

http://www.youtube.com/embed/FwS-DlKMddI

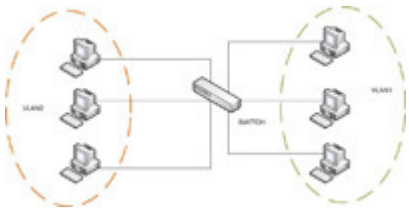
Enrutamiento dinámico. Ejemplo con Packet Tracer.

http://www.youtube.com/embed/5p-hPTA-q8s

Enrutamiento de redes utilizando RIP.

http://www.youtube.com/embed/VHV66OoaniM

4.3.6.- Enrutamientos entre VLAN. Ejemplo básico.



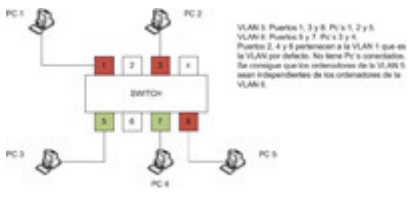
Recuerda que en la unidad anterior (que) ya aprendiste lo que era una VLAN, siglas de Virtual Local Area Network, y las ventajas que tenían. Hacemos un breve recordatorio de que era una VLAN:

- Una VLAN es una red LAN independiente.
- Una VLAN permite que los ordenadores de las distintas subredes estén separadas, aunque comparten el mismo cableado, switches, etc… es decir, que comparten la misma infraestructura.
- Se le puede otorgar un nombre a la VLAN para facilitar su identificación.

Una red VLAN consiste en una red en la que los ordenadores están todos conectados a un switch, pero dicho switch puede configurarse en distintas subredes VLAN a través de sus puertos. Para poder realizar una VLAN en lo primero que te tienes que fijar es en el tipo de switch que vas a utilizar. No todos los switch soportan VLAN. ¿Qué tienes que tener en cuenta a la hora de comprar un switch?

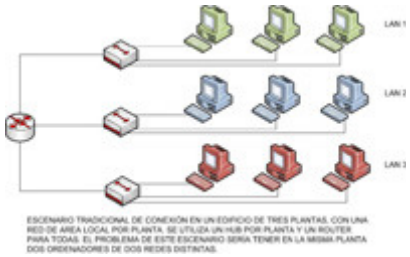
- Velocidad del switch: puede ser 10/100/1000
- Si es gestionable: que tiene direcciones IP y se puede configurar. Los switch no gestionables son más baratos.
- Que soporte VLAN.

Para que entiendas las VLAN haremos un ejemplo. Imagínate un switch con 8 puertos al que tenemos conectados 5 equipos en los puertos 1, 3, 5, 7 y 8. Si configuramos distintas VLAN, aunque los cinco equipos estén en el mismo switch, se pueden aislar de forma independiente entre sí de modo que los equipos de una VLAN no pueden ver a los equipos de otra VLAN distinta. Para ello, asignamos distintos puertos del switch a distintas VLAN. Los puertos que no se asignan a una VLAN en concreto, por defecto pertenecen a la VLAN 1. En este esquema vemos un ejemplo completo de switch de tres puertos.



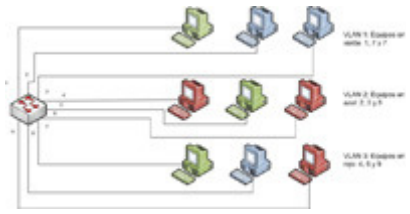
4.3.7.- Enrutamientos entre VLAN. Ejemplo avanzado.

En este apartado verás otro ejemplo de porqué son tan útiles las redes VLAN para aislar unos equipos de otros. Se parte del siguiente escenario. Imagínate una empresa que tiene sus equipos en tres plantas de un edificio. En cada una de las plantas tenemos una red de área local diferente. Estos equipos están conectados entre sí por medio de tres hub y un router de la siguiente manera:



ESCENARIO TRADICIONAL DE CONEXIÓN EN UN EDIFICIO DE TRES PLANTAS, CON UNA RED DE ÁREA LOCAL POR PLANTA. SE UTILIZA UN HUB POR PLANTA Y UN ROUTER PARA TODAS. EL PROBLEMA DE ESTE ESCENARIO SERÍA TENER EN LA MISMA PLANTA DOS ORDENADORES DE DOS REDES DISTINTAS.

¿Qué solución te puede aportar una red VLAN y qué mejoras tiene? Con distintas redes VLAN se conectarían todos los equipos directamente a un switch. Al configurar los puertos del switch agrupados en distintas VLAN se consiguen también aislar y mantener independientes dos distintos equipos, con la ventaja de que dichos equipos no tienen por qué estar situados en la misma planta o en la misma habitación del edificio. En la siguiente imagen verás un ejemplo de agrupación con VLAN en la misma empresa del ejercicio anterior:



De este modo, es mucho más fácil el tener distintas redes de área local en distintas ubicaciones de un edificio configurando adecuadamente un switch.

Debes conocer

Vídeos explicativos sobre las LANs virtuales. Se trata de un ejemplo de redes VLAN en Packet Tracer:

Ejemplo de VLAN. Parte I.

Ejemplo de VLAN. Parte II.

Para saber más

Si te interesa seguir ampliando tus conocimientos sobre VLAN, te recomiendo que no te pierdas los siguientes enlaces que puedes encontrar en Internet.

Interconexión de switch mediante Trunk. Parte I.

http://www.youtube.com/embed/KpdZm35TXiU

Interconexión de switch mediante Trunk. Parte II.

http://www.youtube.com/embed/I-QVIChxvBc

Interconexión de VLAN de switch independientes.

http://www.youtube.com/embed/vwATsyXKCrU

Enrutamiento inter-VLAN.

http://www.youtube.com/embed/S8AmyVTtW1I

Autoevaluación

¿Cuál es la ventaja que me ofrece el poder utilizar VLAN con switch?

- ○ Aislar ordenadores dentro de la misma red.
- ○ Aumenta la velocidad de la red.
- ○ Disminuye el tiempo de espera en las comunicaciones.
- ○ Ninguna de las anteriores.

Muy bien, has estado muy atento a los vídeos.

Vuelve a visionar los vídeos.

No es correcta.

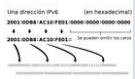
Vuelve a ver los vídeos.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurs
	Autoría: LordT. Licencia: Creative Commons 2.5 . Procedencia: http://es.wikipedia.org /wiki/Archivo:Pila-osi-es-2.svg		Autoría: Sten Porse. Licencia: Creative Commons 3 Procedencia: http://commons. /wiki/File:Middle_Age-road.JP
	Autoría: Indeterminada. Licencia: Dominio público. Procedencia: http://commons.wikimedia.org /wiki/File:Ipv6_address.svg		Autoría: Indeterminada. Licencia: Dominio público. Procedencia: http://commons. /wiki/File:Ipv6_address.svg
	Autoría: Zymos. Licencia: Dominio público. Procedencia: http://commons.wikimedia.org /wiki/File:Icon-windows_os.svg		Autoría: Larry Ewing. Licencia: Redistribution, deriva commercial use, and all other Procedencia: http://commons. /wiki/File:NewTux.svg
	Autoría: Hellisp. Licencia: C.C. 3.0. Procedencia: http://commons.wikimedia.org /wiki/File:Dlink_wireless_router.jpg		Autoría: Kamo64. Licencia: Dominio público. Procedencia: http://es.wikiped /wiki/Archivo:Tabla_de_enruta
	Autoría: Patrick.charpiat. Licencia: CC 2.5. Procedencia: http://commons.wikimedia.org /wiki/File:Route-aubisque.JPG		Autoría: Vanessaezekowitz. Licencia: CC 3.0. Procedencia: http://it.wikipedia /wiki/File:Basic_desktop_comp
	Autoría: Ojota. Licencia: CC 3.0. Procedencia: http://wikimania2009.wikimedia.org /wiki/File:Subtes-2008.svg		Autoría: lamlatin. Licencia: CC 3.0. Procedencia: http://commons. /wiki/File:Ruta_5_amambay_p
	Autoría: Weihao Chiu. Licencia: C.C. 3.0. Procedencia: http://commons.wikimedia.org /wiki/File:D-Link_DI-524.jpg		Autoría: Msgj. Licencia: Dominio publico. Procedencia: http://commons. /wiki/File:Computer-aj_aj_asht

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

Junta de Andalucía

Antes de cualquier uso leer detenidamente el siguente Aviso legal

Historial de actualizaciones

Versión: 01.01.01	Fecha de actualización: 13/05/21
Actualización de materiales y correcciones menores.	

Versión: 01.01.00	Fecha de actualización: 30/05/17	Autoría: Jesús Manuel Marín Navarro

Ubicación: todo el documento
Mejora (tipo 1): Faltaba la numeración de las secciones de contenido.
Añadida licencia
Marcadas palabras en otro idioma
Corregidos los enlaces a Glosario.
Orientaciones del alumnado , orientaciones de tutoría y mapa conceptual actualizado con nuevo índice y contenidos.
Repaso general.
Ubicación: Todo el apartado 4
Mejora (tipo 1): Se ha reordenado toda la estructura del apartado 4, para separar más claramente los PCs de los routers. También se han separado los routers domésticos de los profesionales de entorno empresarial. Se han añadido contenidos explicando ésto, hablando de los routers comerciales como los Cisco, de los simuladores y emuladores como Cisco Packet Tracer y GNS3 entre otros. En 4.1.1 se ha creado una práctica con routers domésticos
Ubicación: Configuración de un encaminador.
Mejora (tipo 2): Actualizar la práctica en la que un router se configura a través de hyperterminal.
Se debería realizar la práctica de configuración básica de un router doméstico ADSL.

Versión: 01.00.00	Fecha de actualización: 25/10/14

Versión inicial de los materiales.