**LoopBack**

La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento.

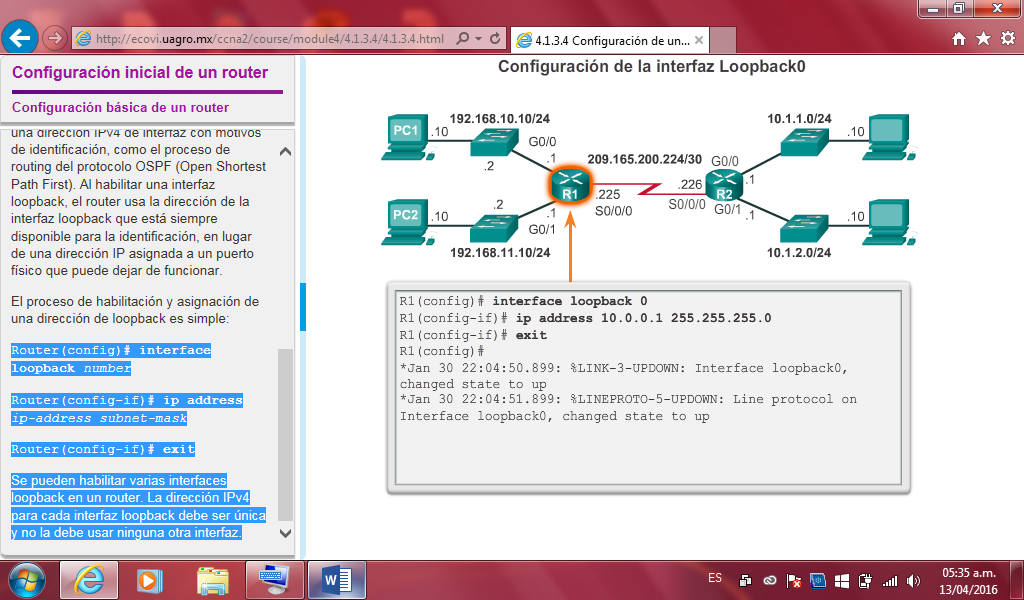
La interfaz loopback es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.

Además, la dirección IPv4 asignada a la interfaz loopback puede ser importante para los procesos en el router que usan una dirección IPv4 de interfaz con motivos de identificación, como el proceso de routing del protocolo OSPF (Open Shortest Path First). Al habilitar una interfaz loopback, el router usa la dirección de la interfaz loopback que está siempre disponible para la identificación, en lugar de una dirección IP asignada a un puerto físico que puede dejar de funcionar.

El proceso de habilitación y asignación de una dirección de loopback es simple:

* Router(config)# interface loopback number
* Router(config-if)# ip address ip-address subnet-mask
* Router(config-if)# exit

Se pueden habilitar varias interfaces loopback en un router. La dirección IPv4 para cada interfaz loopback debe ser única y no la debe usar ninguna otra interfaz.



**Poison Revers**

Envenenamiento en Reverso (Poison Reverse) es cuando un enlace se cae, el enrutador inmediatamente envia un mensaje con la ruta y una distancia de infinito.Es una tecnica que complementa al split – horizon ya que el alcance de poison – reverse es mayor para evitar los loops de enrrutamiento, se trata de crear una entrada en la tabla de enrutamiento en la que se guarda la información respecto de una ruta que esta fuera de servicio “ruta envenenada” esperando que el resto de la red converja en la misma información en esa entrada la red de destino es marcada como inalcanzable “RIP Metrica =16 infinito” y esa información se publica con las actualizaciones del protocolo hacia los dispositivos vecinos, de este modo se evita que el dispositivo pueda aceptar información incoherente.

**Auto Sumary**

La sumarización de redes es una técnica que nos sirve para optimizar los recursos de los routers, además de que nos permite mantener una red menos compleja y más estable.

•La Sumarización es por defecto a clases principales: máscaras /8, /16 o /24.

•Pero RIP v2 o EIGRP realizan un auto- summarization únicamente cada vez que se cruza una frontera entre dos clases principales difererentes.

•En esta figura, debido a que RTC y RTD tienen ambos redes de clase general (1.0.0.0/8 y 2.0.0.0/8) y los paquetes son enviados a través de ellas, entonces se sumarizará por defecto.

Cuando trabajamos con protocolos de enrutamiento dinámicos como Rip o Eigrp, nos aconsejan siempre desactivar la sumarización automática, a pesar de que al mismo tiempo nos dicen "Sumarizar es bueno". Esto genera una confusión al momento de estudiar cómo funciona esto, y porque nos aconsejan siempre realizar una sumarización manual de las rutas.

Rip y Eigrp realizan sumarización automática en los router que poseen "Dos redes distintas", quizás suena obvio, ya que normalmente todos los routers poseen más de una red conectada. Sin embargo esto es lo que produce la confusión, ya que un router cuando posee dos SUBREDES que pertenecen a la misma RED no sumariza automáticamente, por lo tanto no es tomado como "Router Borde".

Esto sucede para todo el tráfico que viaja entre las LAN, esto podría generar un loop o un enrutamiento suboptimo, por lo tanto se aconseja en estos casos desactivar la sumarización automática., con el comando **no auto-summary** en la configuración de RIP.