6.1.- Servicio de enrutamiento y acceso remoto

6.1.1. Qué es un enrutador

Los *enrutadores* son un sistema intermedio de la capa de red que se utiliza para conectar redes mediante un protocolo de capa de red común. Los sistemas intermedios son dispositivos de red que tienen la capacidad de reenviar paquetes entre distintas partes de una red.

Los enrutadores permiten ampliar la red y mantener el ancho de banda al segmentar el tráfico de red. Por ejemplo, los equipos de pruebas de una organización pueden estar en un segmento de la red, mientras que los equipos de producción están en un segmento de red independiente. Un enrutador conecta estos dos segmentos independientes.

Los dos tipos de enrutadores que se utilizan en un entorno de red son:

- *Enrutador de hardware*. Dispositivo de hardware dedicado que ejecuta software especializado con el propósito exclusivo de realizar el enrutamiento.
- *Enrutador de software*. Enrutador que efectúa el enrutamiento como uno de los múltiples procesos que se ejecutan en el equipo enrutador. El servicio de enrutamiento y el de acceso remoto de Microsoft Windows Server es un servicio que efectúa el enrutamiento además de otros procesos. Cuando se habilita como enrutador de red, Microsoft Windows Server admite el enrutamiento estático y el dinámico. En el enrutamiento estático, el administrador actualiza manualmente la tabla de enrutamiento. En el enrutamiento dinámico, son los protocolos de enrutamiento los que actualizan dicha tabla.

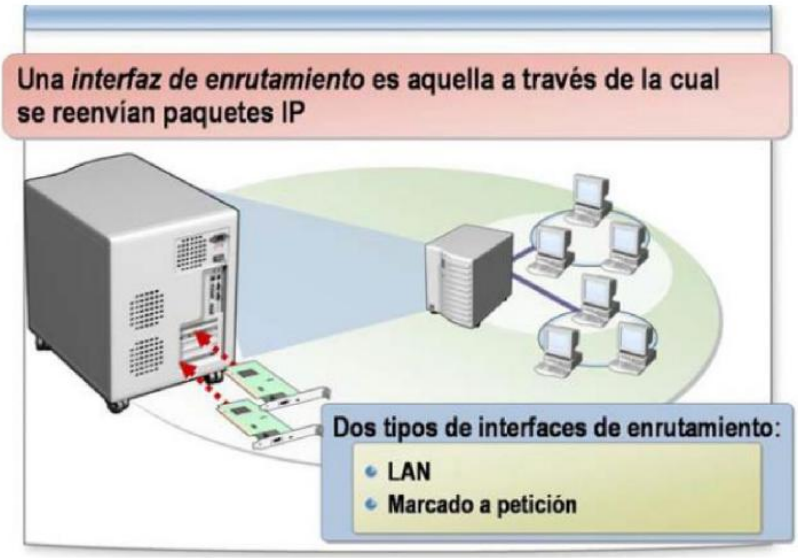
Los componentes principales de una solución de enrutamiento son:

- *Interfaz de enrutamiento*. Interfaz física o lógica a través de la que se reenvían paquetes.
- *Protocolo de enrutamiento*. Conjunto de mensajes que los enrutadores utilizan para compartir tablas de enrutamiento de modo que pueda determinar la ruta de acceso apropiada para reenviar datos.
- *Tabla de enrutamiento*. Conjunto de entradas llamadas rutas que contienen información acerca de la ubicación de los identificadores de red en la interconexión de redes.

6.1.2. Qué es una interfaz de enrutamiento

Una *interfaz de enrutamiento* es una interfaz física o lógica a través de la que se reenvían paquetes de Protocolo Internet (IP). El enrutador basado en Microsoft Windows Server utiliza una interfaz de enrutamiento para reenviar paquetes IP. Los tipos de interfaces de enrutamiento que podemos utilizar en Windows Server son:

Interfaces de red de área local (LAN). Estas interfaces suelen representar un adaptador de red instalado, aunque también puede utilizarse un adaptador de red de área extensa (WAN, *Wide Area Network*) como interfaz. Normalmente, las interfaces LAN no requieren un proceso de autenticación para activarse.



Interfaces de marcado a petición. Estas interfaces representan una conexión punto a punto que requiere autenticación para completar la conexión. Dos ejemplos son una red privada virtual (VPN, *Virtual Private Network*) de enrutador a enrutador y una línea telefónica conectada mediante módems. Una red VPN es la extensión de una red privada a través de redes compartidas o públicas. Las conexiones de marcado a petición pueden ser a petición (sólo se establecen cuando es necesario) o persistentes (una vez establecida, la conexión se mantiene).

6.1.3. Qué es un protocolo de enrutamiento

Un *protocolo de enrutamiento* es un conjunto de mensajes que los enrutadores utilizan con el fin de determinar la ruta apropiada para reenviar datos. Los protocolos de enrutamiento administran automáticamente los cambios de la tabla de enrutamiento que puedan producirse debido a cambios en la red.

Un servidor con Enrutamiento y acceso remoto de Microsoft Windows Server que no tenga configurado un protocolo de enrutamiento sólo puede enrutar entre:

- Las redes a las que está conectado físicamente el servidor de Enrutamiento y acceso remoto.
- Las redes para las que el servidor de Enrutamiento y acceso remoto tenga configuradas rutas estáticas (especificadas manualmente por un administrador).

Sin embargo, cuando se agrega un protocolo de enrutamiento, el servidor puede comunicarse con todos lo demás enrutadores de la red que estén configurados con el mismo protocolo de enrutamiento. La tabla de enrutamiento del enrutador de Microsoft Windows Server se actualiza automáticamente con las rutas de los demás enrutadores.

Enrutamiento y acceso remoto de Microsoft Windows Server admite dos tipos de protocolos de enrutamiento:

- *Protocolo de información de enrutamiento (RIP)*. Diseñado para intercambiar información de enrutamiento en una red de tamaño pequeño a mediano.
- *Abrir primero la ruta de acceso más corta (OSPF)*. Diseñado para intercambiar información de enrutamiento en una red de tamaño grande o muy grande.

Cómo funciona RIP

El proceso de RIP evita que la administración de las tablas de enrutamiento se convierta en una carga.

1. RIP crea dinámicamente tablas de enrutamiento mediante el envío de anuncios del contenido de su propia tabla de enrutamiento a sus interfaces configuradas.

2. Los enrutadores conectados a esas interfaces reciben los anuncios y los utilizan para crear las tablas de enrutamiento apropiadas.

3. Los enrutadores que reciben los anuncios compilan su propia tabla de enrutamiento, que a continuación se transmite a otros enrutadores. Este proceso continúa hasta que cada uno de los enrutadores configurados haya recibido las rutas de todos los demás.

Cómo funciona OSPF

En lugar de intercambiar entradas de las tablas de enrutamiento como hacen los enrutadores RIP, los enrutadores OSPF mantienen un mapa de la red que se actualiza después de cualquier cambio en la topología. Este mapa se denomina base de datos de estado de vínculos.

1. OSPF permite que un enrutador calcule la ruta de acceso más corta para enviar paquetes a cada nodo.

2. El enrutador envía información (denominada anuncios de estado de vínculos) acerca de los nodos a los que está vinculado a todos los demás enrutadores de la red. El enrutador recopila información de los demás enrutadores, que utiliza para conocer el estado de los vínculos y efectuar cálculos.

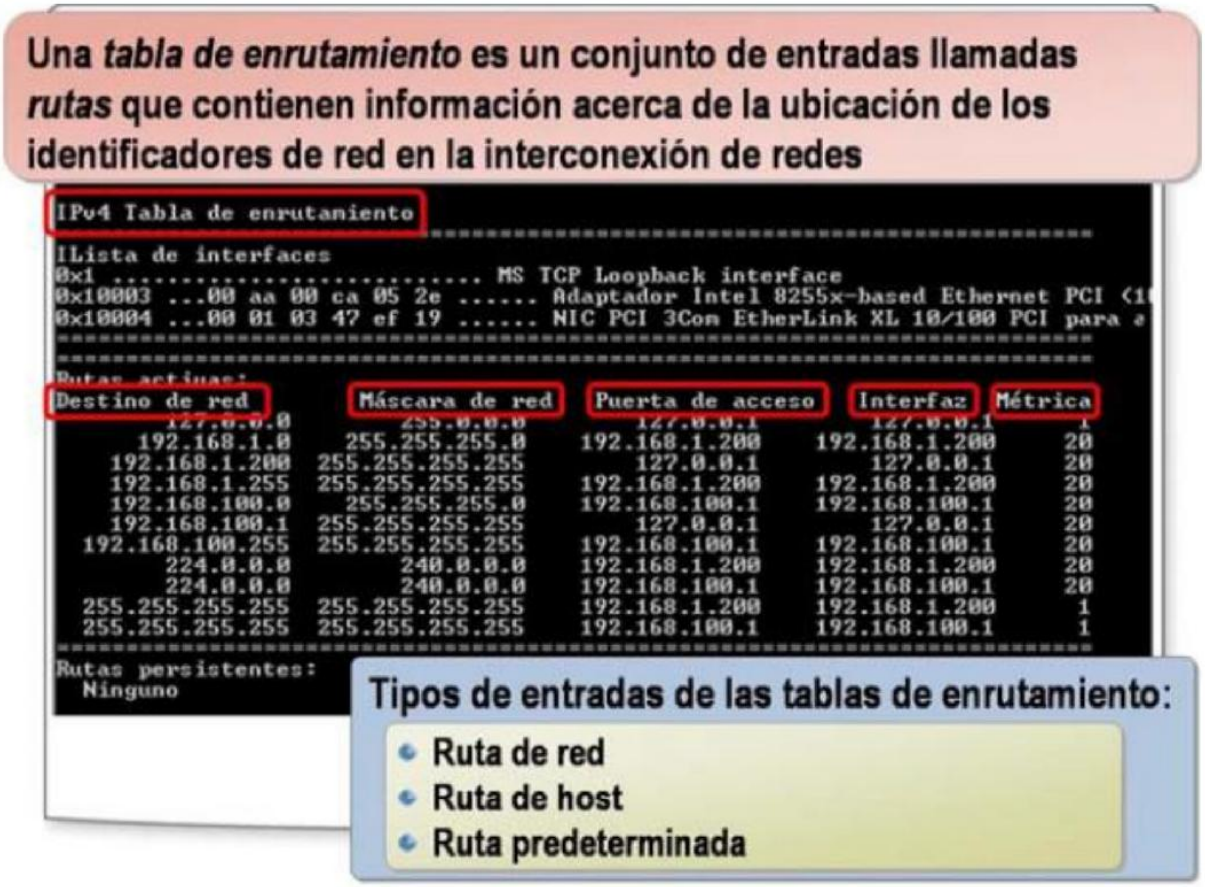
Comparación de RIP y OSPF

RIP es sencillo de configurar e implementar. Sin embargo, a medida que la red crece los anuncios periódicos que envía cada enrutador RIP pueden producir un tráfico excesivo en la red. (RIP suele utilizarse en redes de hasta 50 servidores.)

OSPF funciona de forma eficaz en redes grandes porque calcula la mejor ruta que puede utilizarse y requiere menos mensajes de estado. A diferencia de RIP, OSPF no anuncia todas las rutas conocidas a los demás enrutadores, sino únicamente los cambios realizados en sus rutas.

El inconveniente de OSPF es su complejidad: es más difícil de configurar y requiere más administración que RIP. Nosotros nos vamos a limitar a ver cómo se configura RIP.

6.1.4. Qué es una tabla de enrutamiento



Tal y como hemos visto en unidades anteriores una *tabla de enrutamiento* es un conjunto de entradas llamadas *rutas* que contienen información acerca de la ubicación de los identificadores de red en la interconexión de redes.

La información de una tabla de enrutamiento ayuda a determinar la ruta óptima en una interconexión de redes. La tabla de enrutamiento no es exclusiva de un enrutador. Los hosts (no enrutadores) pueden tener también una tabla de enrutamiento que utilizan para determinar la ruta óptima.

Tipos de entradas de las tablas de enrutamiento

Como ya vimos en unidades anteriores, hay tres tipos de entradas en las tablas de enrutamiento:

- *Ruta de red*. Ruta de acceso a un identificador de red específico en la interconexión de redes. En una ruta de red la máscara contiene unos y ceros.
- *Ruta de host*. Ruta de acceso a una dirección de la interconexión de redes (identificador de red y de nodo). Las rutas de host suelen utilizarse para crear rutas personalizadas a hosts específicos a fin de controlar u optimizar el tráfico de red. En una ruta de host la máscara es la 255.255.255.255 (todo unos porque tienen que coincidir todos los bits)
- *Ruta predeterminada*. Se utiliza cuando no se encuentran otras rutas en la tabla de enrutamiento. En una ruta predeterminada la máscara es la 0.0.0.0 (todo ceros porque cualquier destino puede utilizar esta ruta)

Por ejemplo, si un host o un enrutador no puede encontrar una ruta de red o de host hasta el destino, se utiliza la ruta predeterminada. La ruta predeterminada simplifica la configuración de hosts. Es lo que conocemos como puerta de enlace predeterminada (normalmente conocida en los equipos como la IP del router)

En lugar de configurar hosts con rutas para todos los identificadores de red de la interconexión de redes, se emplea una única ruta predeterminada para reenviar todos los paquetes cuya dirección de red o de interconexión de redesde destino no se encuentre en la tabla de enrutamiento.

Estructura de la tabla de enrutamiento

Cada entrada de la tabla de enrutamiento consta de los campos de información siguientes:

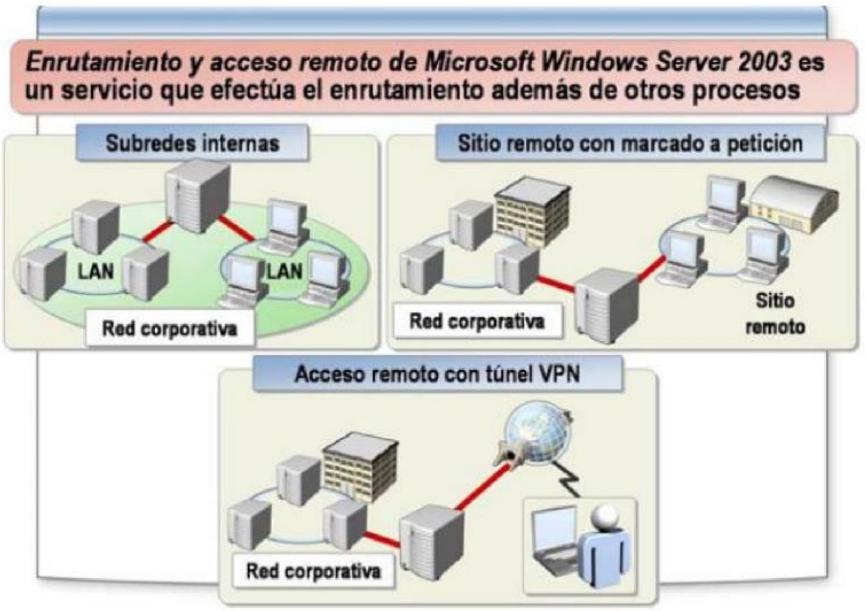
- *Destino de red*. Especifica el destino de red de la ruta. El destino puede ser una dirección IP (donde los bits de host de la dirección de red se establecen en 0), una dirección IP correspondiente a una ruta de host o 0.0.0.0, en el caso de la ruta predeterminada.
- *Máscara de red*. Especifica la máscara de subred asociada con el destino de red. Su valor puede ser la máscara de subred apropiada correspondiente a una dirección de red IP, 255.255.255.255 en el caso de una ruta de host o 0.0.0.0 en el caso de la ruta predeterminada.
- *Puerta de acceso*. Especifica la dirección IP de reenvío o siguiente salto a través de la cual puede llegarse al conjunto de direcciones definidas por el destino de red y la máscara de subred.
- *Interfaz*. Especifica el número de interfaz de red para la ruta especificada. Se trata de un número de puerto u otro tipo de identificador lógico.
- *Métrica*. Especifica la medida de costo de una ruta en números enteros. Normalmente, la métrica más baja es la ruta preferida. Si hay varias rutas a una red de destino dada, se utiliza la que tenga la menor métrica.

Recordemos que el comando **route print** en el símbolo del sistema muestra todo el contenido de una tabla de enrutamiento.

6.2.- Servicios de enrutamiento y acceso remoto de Microsoft Windows Server

6.2.1. Introducción

Enrutamiento y acceso remoto de Microsoft Windows Server es un servicio que efectúa el enrutamiento además de otros procesos. Un servidor con enrutamiento y acceso remoto de Microsoft Windows Server puede utilizarse para:



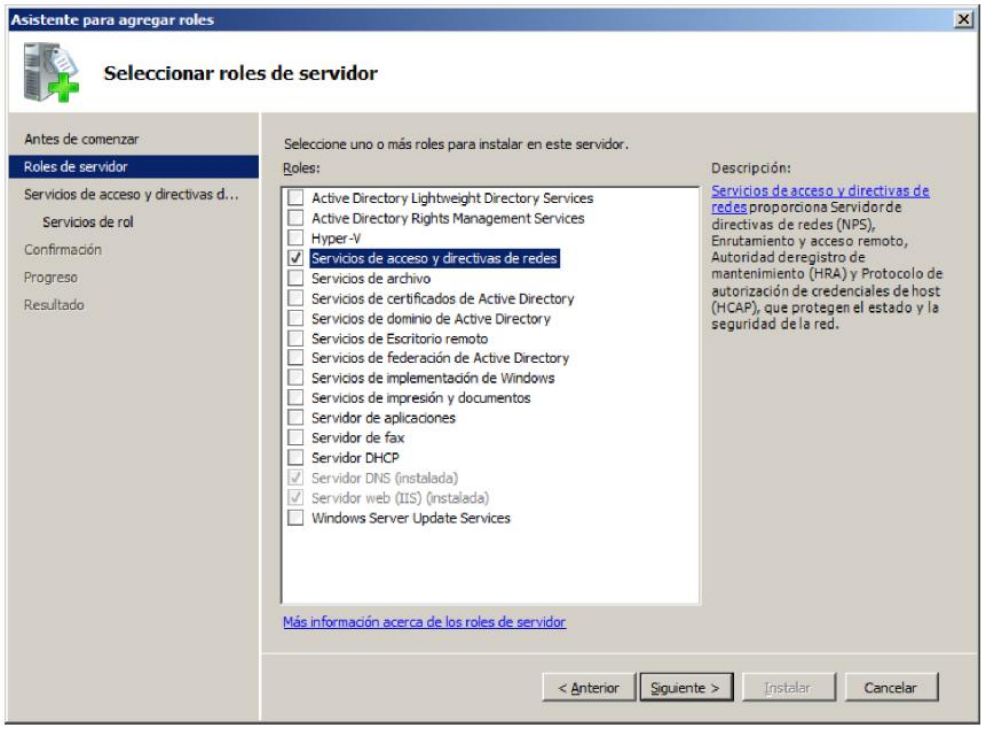
- Conectar segmentos de LAN (subredes) en una red corporativa.
- Conectar sucursales a intranets corporativas y compartir recursos como si todos los equipos estuvieran conectados a la misma LAN.
- Proporcionar a los equipos remotos acceso a recursos de la red corporativa.

Los administradores de sistemas pueden ver y utilizar Enrutamiento y acceso remoto para ver y administrar los servidores de enrutamiento que ejecuten Microsoft Windows Server y los servidores de acceso remoto de una red.

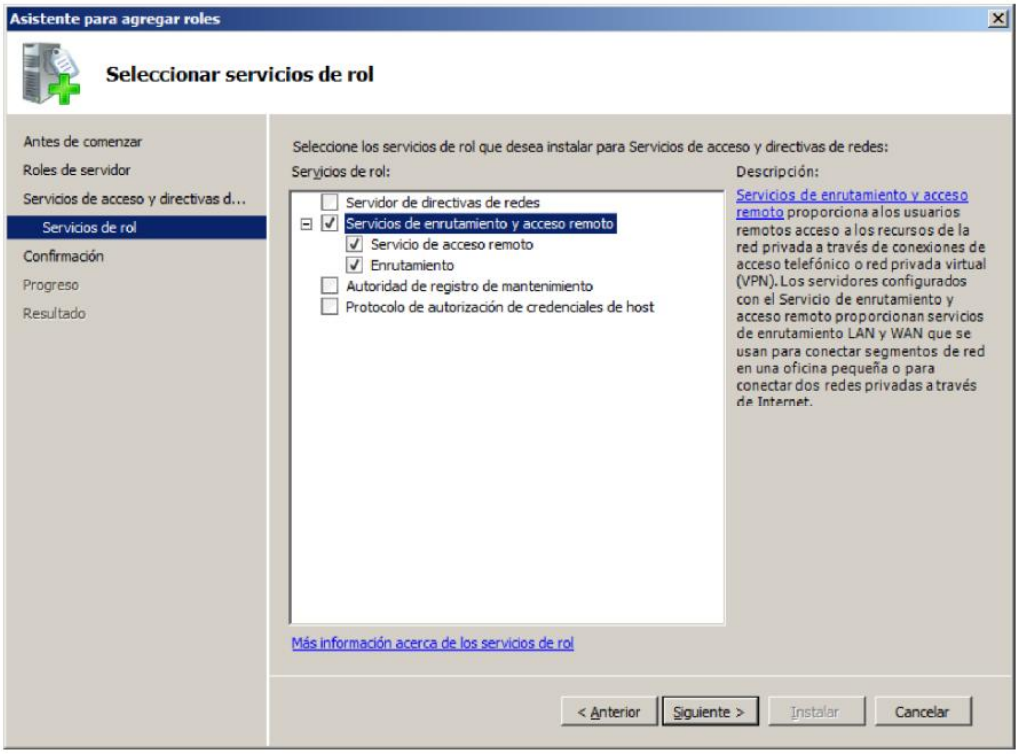
Este servicio permite a los administradores configurar servidores VPN, enrutamiento LAN, o enrutamiento NAT.

6.2.2. Cómo habilitar el servicio de enrutamiento y acceso remoto para enrutamiento LAN

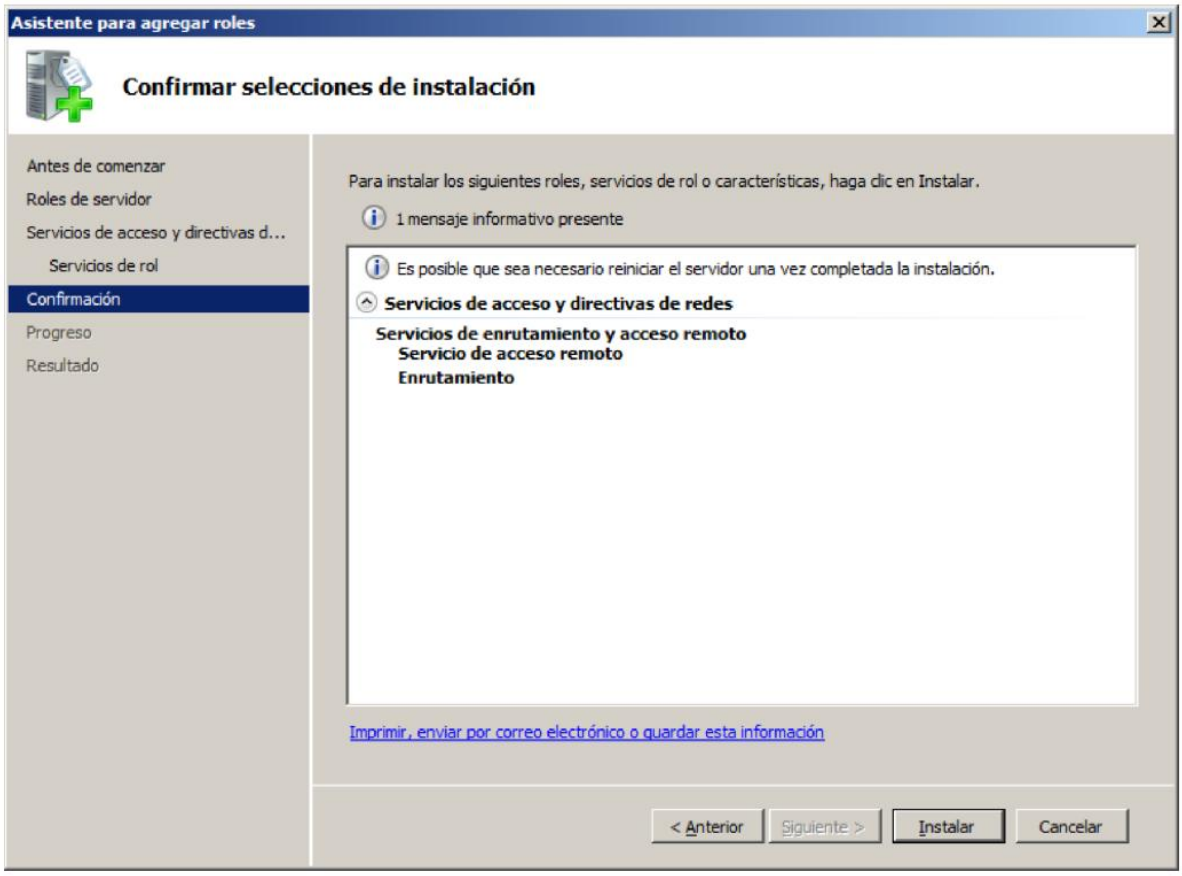
Para habilitar el servicio de enrutamiento y acceso remoto lo primero que debemos hacer es asegurarnos de que toda la configuración de red y de equipo es correcta en el servidor. Una vez que tenemos todo preparado agregamos el rol "Servicios de acceso y directivas de redes":



Seleccionamos los servicios de rol: "Servicios de enrutamiento y acceso remoto" que es conocido en Windows como RRAS (Routing and remote access services)

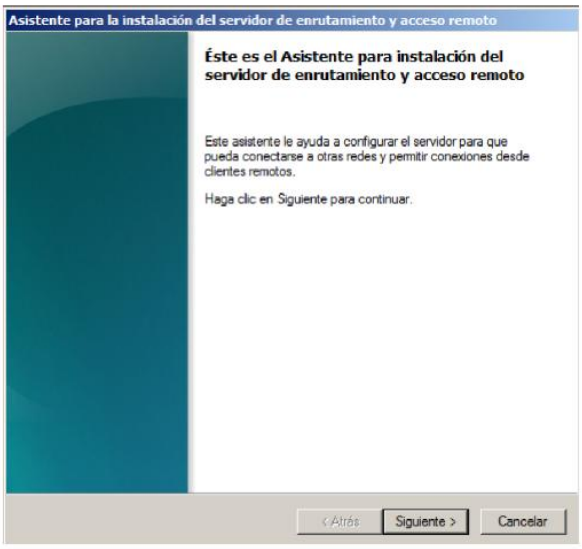


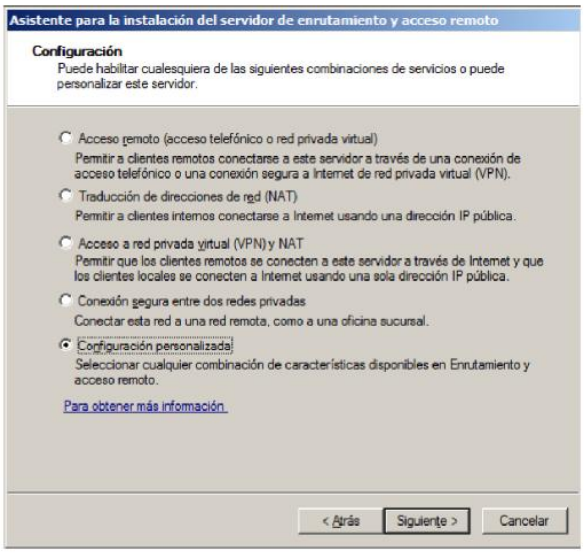
Confirmamos que lo que nos muestra es lo que queremos instalar e instalamos:



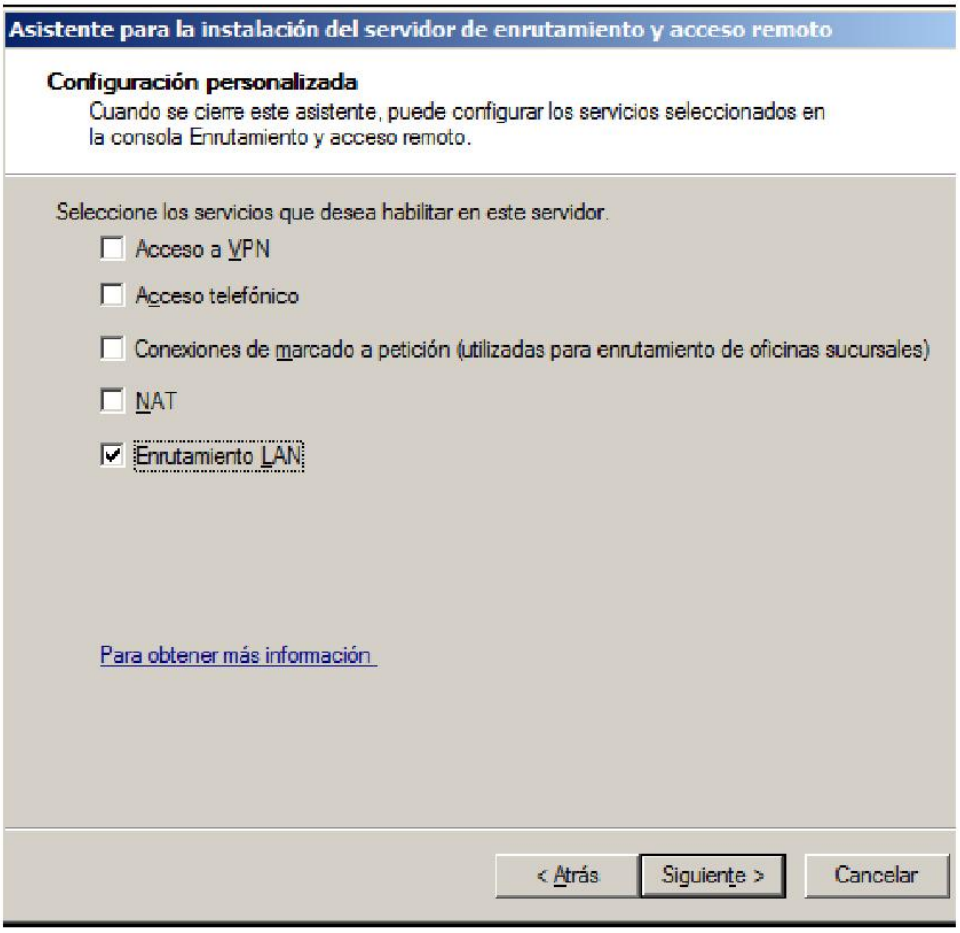
Ya tenemos instalado el servicio de enrutamiento. Este servicio por defecto no está habilitado. Es necesario configurarlo y habilitarlo para que se pueda utilizar. Supongamos por ejemplo que queremos comunicar dos redes locales. Arrancamos la herramienta administrativa "Enrutamiento y acceso remoto":

Botón derecho sobre el servidor y elegimos la opción "Configurar y habilitar el servicio de escritorio remoto". Cuando nos pregunta la configuración que queremos habilitar seleccionamos "Configuración personalizada"

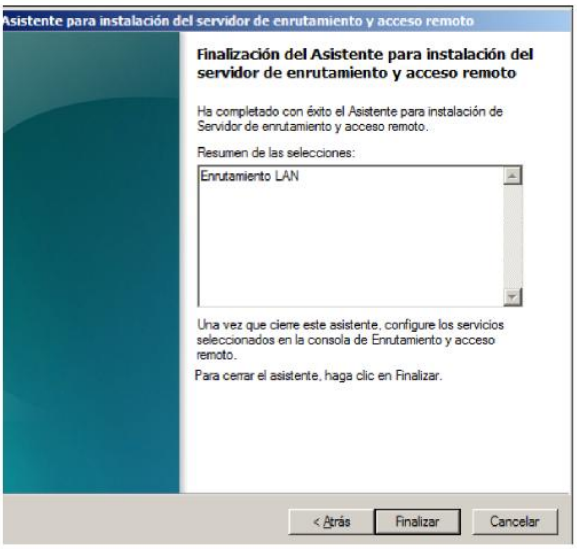


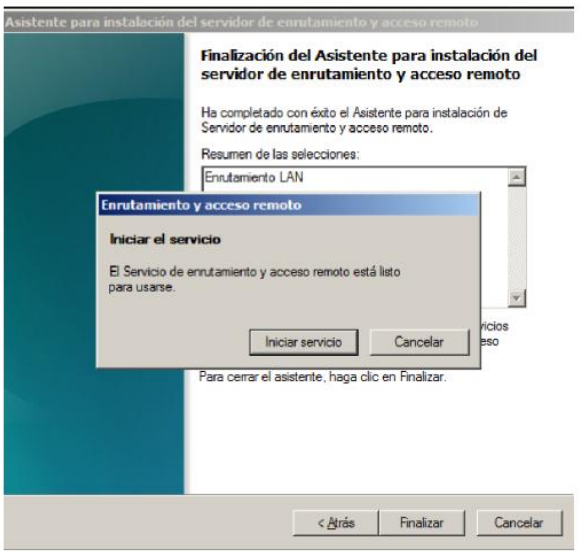


Elegimos el servicio de "Enrutamiento LAN" para habilitar el enrutamiento entre redes locales:

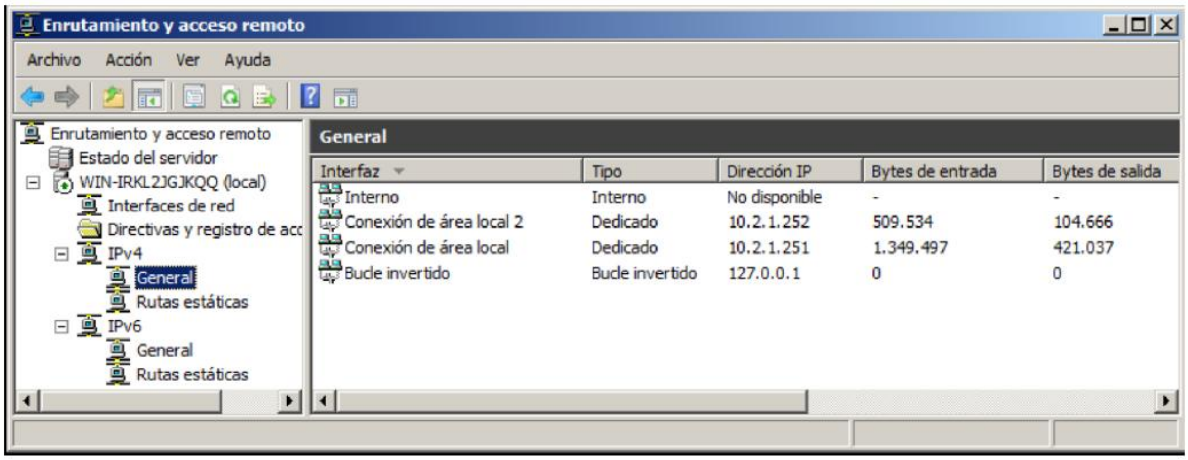


Continuamos con el asistente y le podemos dar a iniciar servicio:





Si seleccionamos el servidor dentro de la herramienta y seleccionamos Ipv4 / general nos aparece la información de las dos tarjetas de red que tiene nuestro servidor y que van a ser enrutadas (conexión de área local y conexión de área local 2). Las dos otras interfaces las crea el RRAS y nos desentendemos de ellas. No hay que hacer ninguna operación adicional si lo único que queremos es que todas las tarjetas que tiene el servidor se comuniquen.



Hay que tener en cuenta que si añadimos las tarjetas de red después de habilitar el enrutamiento LAN los adaptadores de red puede que no sean detectados. Es más que recomendable que toda la configuración de red de los adaptadores de red del servidor de enrutamiento esté debidamente configurada antes de habilitarlo.

De tener que modificar algo posteriormente es recomendable deshabilitarlo, cambiar las configuraciones y volverlo a configurar y habilitar desde 0.

6.3.- Configurar filtros de paquetes

6.3.1. Qué es el filtrado de paquetes

El tráfico IP dirigido a un equipo host o proveniente de él puede administrarse con el filtrado de TCP/IP.Sin embargo, al configurar el filtrado de paquetes en un enrutador, puede controlarse todo el tráfico IP de la red que pase por ese enrutador.

El *filtrado de paquetes* impide que determinados tipos de paquetes de red se envíen o reciban a través de un enrutador.

Un *filtro de paquetes* es una opción de configuración TCP/IP diseñada para permitir o denegar la entrada o salida de los paquetes.

Enrutamiento y acceso remoto de Microsoft Windows Server admite el filtrado de paquetes IP. Mediante Enrutamiento y acceso remoto es posible especificar filtros de paquetes por cada interfaz y, a continuación, configurarlos para realizar una de las acciones siguientes:

- Dejar pasar todo el tráfico excepto los paquetes que el filtro prohíba.
- Descartar todo el tráfico excepto los paquetes que el filtro permita.

Al configurar un filtro de paquetes, debe especificarse en primer lugar si se trata de un filtro de entrada o de salida. Después, se selecciona una acción de filtrado, ya sea para aceptar o para descartar todos los paquetes especificados en el filtro.

El filtrado de paquetes se utiliza para:

- Impedir el acceso de usuarios no autorizados.
- Impedir el acceso a recursos.
- Mejorar el rendimiento al impedir que los paquetes no necesarios se transmitan a través de una conexión lenta.

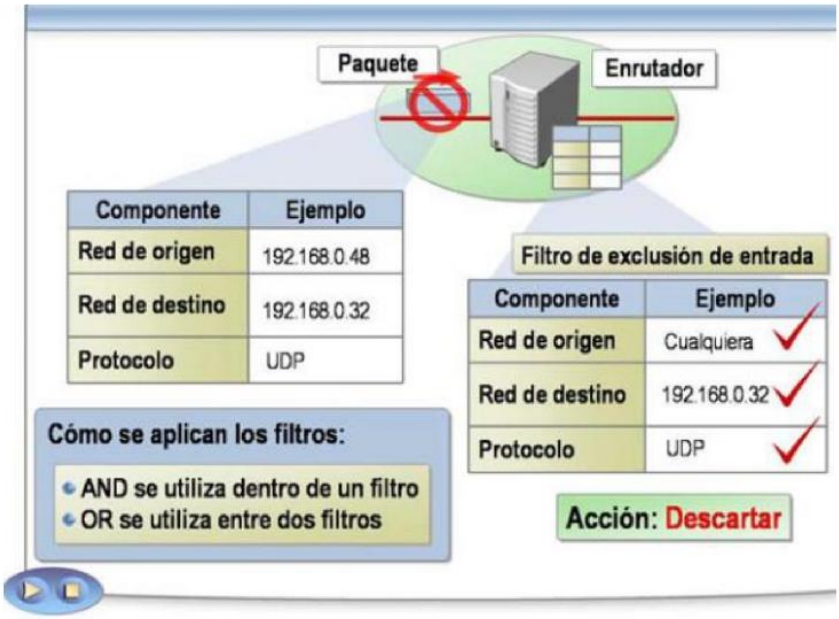
Por ejemplo, si se desea permitir que los usuarios de Internet se conecten a un servidor Web de la red interna a través de un servidor de Enrutamiento y acceso remoto, se puede configurar un filtro

de entrada que sólo permita los paquetes del puerto TCP 80 y la dirección IP del servidor Web. No se admitirían otros paquetes provenientes de Internet.

Si se desea restringir la red interna para permitir el acceso sólo a los sitios Web de Internet que utilizan el puerto 80, se puede crear un filtro de salida que sólo permita los paquetes dirigidos al puerto TCP 80. Los demás paquetes no podrían atravesar el servidor de Enrutamiento y acceso remoto.

6.3.2. Cómo aplicar filtros de paquetes

En un único filtro pueden establecerse varios parámetros. Asimismo, es posible crear un conjunto de filtros que indiquen al enrutador el tipo de tráfico que se permite o se prohíbe en cada interfaz configurada. Estos filtros pueden establecerse para el tráfico entrante y saliente.



Si se configuran varios parámetros en un filtro, esos parámetros se comparan mediante un operador lógico AND al aplicar el filtro a un paquete.

Por ejemplo, los campos del paquete deben coincidir con todos los parámetros configurados del filtro. Si el paquete cumple con todos los parámetros, la acción del filtro se aplica para recibirlo o descartarlo.

Como para cada interfaz pueden definirse tanto filtros de entrada como de salida, es posible crear filtros contradictorios. Cuando hay varios filtros configurados, los filtros independientes aplicados al paquete de entrada o de salida se comparan mediante un operador lógico OR.

Por ejemplo, el filtro de entrada de una interfaz permite el tráfico entrante, pero el filtro de salida de la otra interfaz no permite el tráfico saliente. El resultado es que el tráfico se descarta y no atraviesa el enrutador. (Si el paquete coincide al menos con uno de los filtros configurados, se recibe o se descarta dependiendo de la acción establecida en el filtro.)

Los filtros de paquetes se aplican según las reglas siguientes:

1. Los paquetes entrantes y salientes se comparan con el filtro de paquetes de un enrutador.

2. Si el paquete cumple con todos los parámetros del primer filtro, la acción del filtro se aplica para recibirlo o descartarlo.

3. Si el paquete no cumple con todos los parámetros del primer filtro, se compara con el siguiente filtro de paquetes en el enrutador.

4. Si no se aplica ninguno de los filtros de paquetes y el enrutador está configurado con un filtro de exclusión, el paquete atraviesa el enrutador.

Si el enrutador está configurado con un filtro de inclusión, el paquete se descarta y no atraviesa el enrutador.