Routing Inter-site

Guillermo Pérez Trabado *©2016-2024*

Diseño de Infraestructuras de Redes

Depto. de Arquitectura de Computadores - Universidad de Málaga

Introducción al escenario

Una situación probable en una empresa es el crecimiento de la misma con la necesidad de tener presencia en otros lugares alejados de la sede principal de la empresa. El crecimiento puede tener lugar de diversas formas, pero las más comunes son:

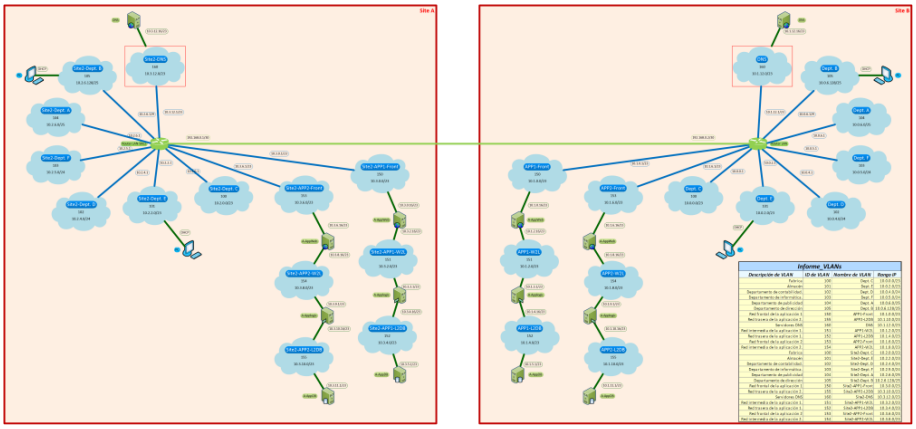
- Crear desde cero una nueva ubicación (site) en otra ciudad incluso de otro continente.
- La fusión con o absorción de otra empresa ya existente y que ya posee sites en otras ubicaciones.

En cualquiera de los dos casos podemos generalizar y extraer las siguientes conclusiones:

- La red de todos los sites tendrá una estructura similar a la que ya hemos aplicado a nuestro diseño hasta ahora: Cableado estructurado, un árbol de switches a dos niveles, VLANs para departamentos, un router LAN central, un data center con ToR switches y Core Switches, servidores de aplicaciones, etc.
- Las redes de todos los sites deben poder **interoperar** como una empresa más grande de forma transparente. Es decir, un departamento de cualquier site debe poder acceder a las aplicaciones de la empresa a las que tenga autorización (esté en el site que esté). Es decir, que la red debe permitir el acceso universal de cualquier terminal a cualquier servidor.
- Sin embargo, más tarde tendremos que crear una política de seguridad global de la empresa que tenga en cuenta todos los departamentos y aplicaciones como si no estuvieran divididos en sites. De nuevo, todo aquello que no esté definido está prohibido por defecto, pero la política **no tendrá en cuenta dónde está el usuario,** pero sí **a qué departamento pertenece el usuario y qué debe poder hacer**.

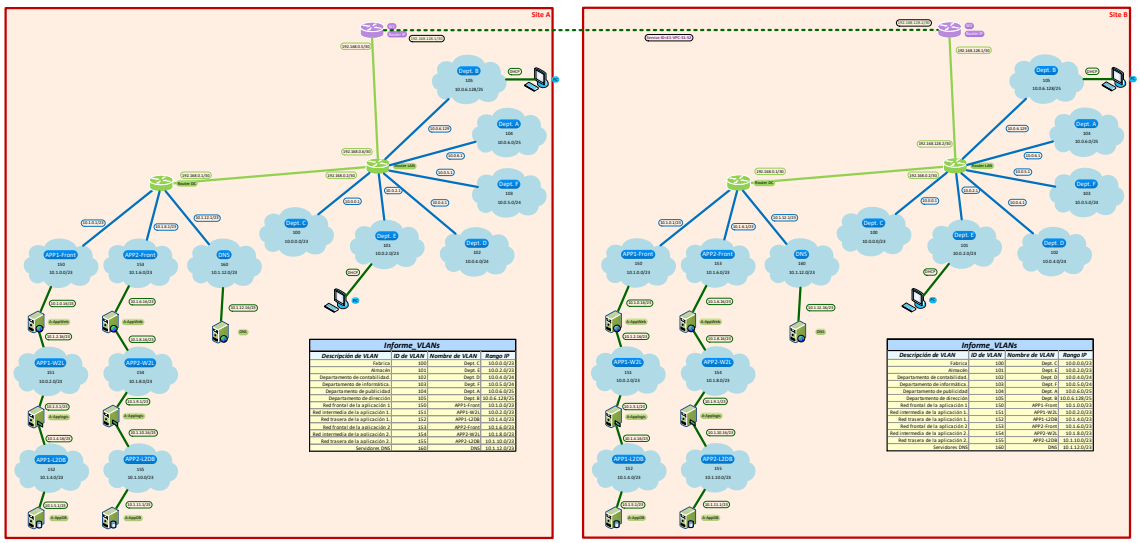
1. Esquema lógico de la fusión de empresas

El esquema lógico es muy sencillo porque se trata simplemente de unir los dos sites sin alterar su estructura. Ya que la estructura lógica de cada site es un árbol con el router LAN en la raíz, la forma más simple de unirlos es conectar los routers entre sí mediante un **enlace WAN punto a punto**. El esquema lógico mantiene independiente el árbol de LANs de cada site.

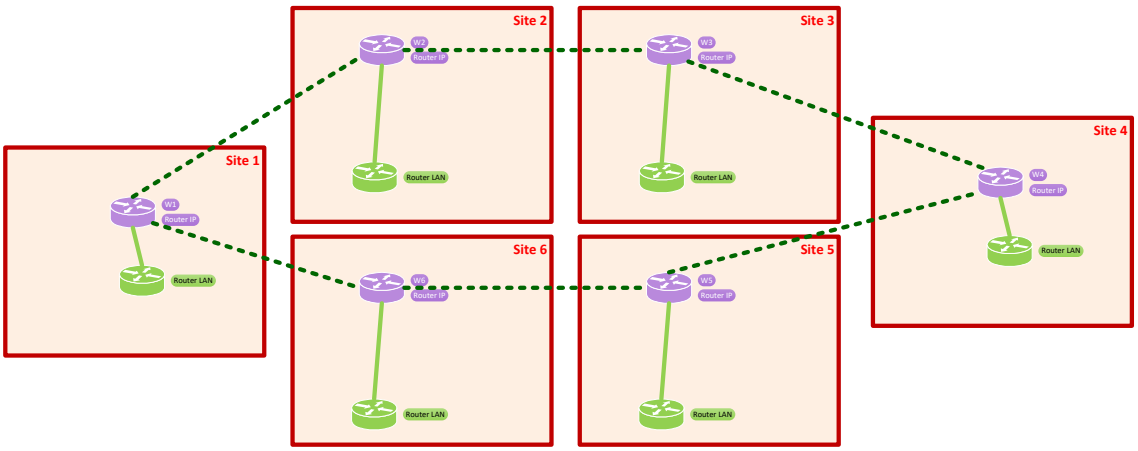


Aunque podemos poner el enlace entre los routers LAN que son de nuestra propiedad, este enlace es proporcionado por un operador de telecomunicaciones. En muchas ocasiones, los routers que están conectados al enlace son proporcionados por el propio operador (routers WAN). Dichos routers están especializados en gestionar dicho enlace y a veces tienen interfaces y software con tecnologías específicas para gestionar dicho enlace. Por esta razón, en lugar de conectar nuestros routers LAN directamente, conectamos dichos routers a los routers WAN que terminan el enlace. Es decir, el **punto de presencia** (**PoP**) del operador en nuestro site es el interfaz Ethernet del router WAN donde nuestro router LAN se conecta.

Además, esto permite separar funciones. Los routers WAN pueden tener uno o más enlaces con distintos sites estableciendo un grafo de conexiones que constituye la red troncal entre sites (**backbone network**). Por tanto, pueden especializarse en gestionar dicha red, mientras que los routers LAN se especializan en el Routing intra-site. El esquema lógico tiene que reflejar la existencia de dichos routers y la configuración de los enlaces punto a punto como en la siguiente figura.

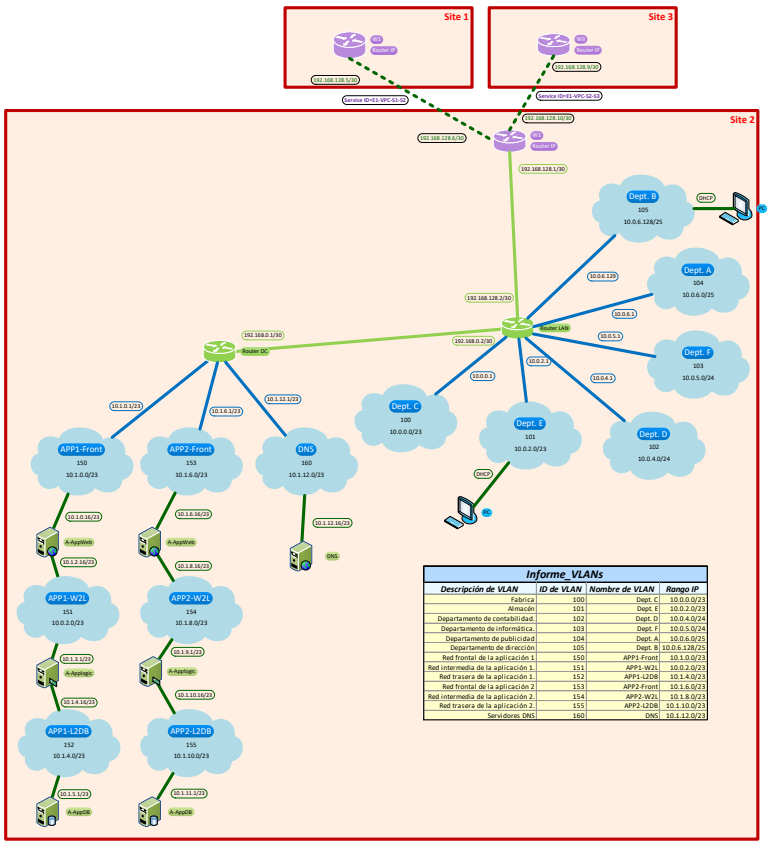


Como la empresa está formada por un cierto número de sites, una forma económica de tener redundancia y minimizar el número de enlaces necesarios es usar un anillo. La siguiente figura da una idea de la estructura circular del **backbone network** formado por los routers WAN de la empresa. Cada site está conectado a dos vecinos de forma que hay dos caminos posibles para llegar a cualquier otro site. En caso de fallo de un camino, se usará el otro aunque no sea óptimo.



Esquema lógico de cada site

Como el administrador de cada site debe trabajar de forma independiente, no tiene sentido que en su esquema lógico refleje los detalles de los sites vecinos. Por tanto, lo único que tiene que añadir a su esquema lógico es la información necesaria para administrar su lado del enlace punto a punto con cada site vecino. Es decir, su router WAN y las direcciones IP del mismo en cada uno de los enlaces WAN. El esquema lógico quedará como se muestra en la siguiente figura. (Este es el esquema lógico que se te pide entregar en esta etapa.)



Plan global de numeración IP

Un detalle importante de la fusión de varias empresas en una sola es la organización del plan **global** de numeración IP de la empresa. Si ambos sites usan rangos de direcciones IP comunes, es imposible para las máquinas de un rango replicado hablar con cualquier dirección del otro site. La razón es sencilla. Si un router LAN conoce otra subred local con el mismo rango IP, nunca mandará un paquete a una subred remota en otro site con dicho rango ya que ***conoce otra ruta con menos distancia a dicho rango*** que es la LAN local. No debe haber direcciones repetidas en distintos sites. Por tanto:

- Es necesario hacer una reunión entre administradores y acordar los rangos IP a usar en cada site, tanto para los departamentos como para las aplicaciones del data center.
- Incluso si de momento no hay cortafuegos, es conveniente asignar prefijos que contengan **todas las VLANs de cada site** que hagan sencillo definir reglas de acceso (ACLs) para poder filtrar el tráfico de un site a otro con una sola regla en lugar de una larga lista de reglas. **Recuerda que un cortafuegos es más eficiente cuantas menos reglas tenga que aplicar a un paquete para decidir si es válido o no.**
    - Por ejemplo, el site 1 usa 10.0-15.x.x, el 2 10.16-31.x.x, etc. El administrador de cada site distribuirá sus direcciones entre departamento y data center según sus propios criterios.
    - Recuerda que cada site también debería disponer de direcciones para numerar de forma autónoma sus enlaces punto a punto. No se recomienda usar una subred del bloque 10.x.x.x ni de 172.16.x.x para los enlaces punto a punto ya que con la fragmentación perderemos demasiadas direcciones. Por eso es mejor usar una subred de 256 direcciones cualquiera del bloque 192.168.x.x. Por ejemplo 192.168.5.0/24.
- Las conclusiones del reparto de direcciones entre sites deben ser publicadas para todos los administradores en forma de una tabla que indique claramente las direcciones que puede usar cada site. **Esta tabla debe ser publicada en el foro privado de cada grupo** para que todos los administradores puedan consultarla. Puedes encontrar el foro privado en la pestaña para esta etapa de la práctica.
- Además, la tabla anterior debe ser incluida en la documentación de la red de cada estudiante.
-

Otro aspecto a tener en cuenta es que tenemos que los administradores deben numerar de forma global todos los enlaces punto a punto entre sites. Para ello también es necesario acordar el uso de un rango de direcciones global a toda la empresa reservado para enlaces del **backbone network**. Dicha numeración también debe estar publicada para todos y también incluirse en la documentación de cada site. Igualmente es preferible asignar subredes del bloque 192.168.0.0/16 para este fin, evitando fragmentar los preciados bloques *10.0.0.0/8* y *172.16.0.0/20*.

Por ejemplo, la tabla siguiente muestra los enlaces que unen los 4 sites de una empresa y se detalla las direcciones y los nombres de los routers de cada extremo.

Enlace	Router1	Router2	Base	IP1	IP2
E1-VPC-S1-S2	S1-WAN	S2-WAN	192.168.1.0/30	192.168.1.1	192.168.1.2
E1-VPC-S2-S3	S2-WAN	S3-WAN	192.168.1.4/30	192.168.1.5	192.168.1.6
E1-VPC-S3-S4	S3-WAN	S4-WAN	192.168.1.8/30	192.168.1.9	192.168.1.10
E1-VPC-S4-S1	S4-WAN	S1-WAN	192.168.1.12/30	192.168.1.13	192.168.1.14

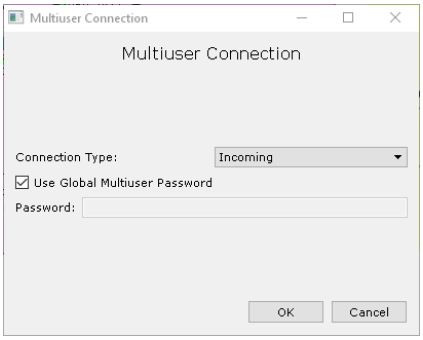
2. Implementación de la fusión

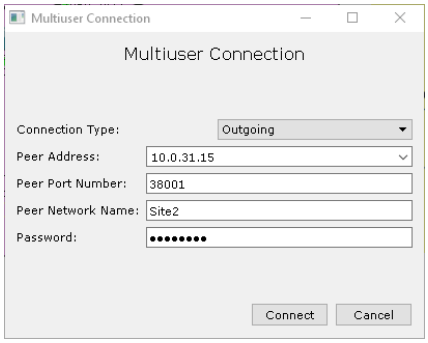
En una empresa real no es posible instalar nuestro propio medio (una fibra óptica) de cientos o miles de kilómetros porque los costes son elevadísimos (obras, permisos, compra de terrenos, etc.). Por tanto, vamos a alquilar el medio a un operador de telecomunicaciones que nos proporciona un extremo en cada site sin que nos importe lo que hay por en medio. El operador de telecomunicaciones va a ser simulador en varios Packet Tracers que van a estar corriendo siempre en un servidor ubicado en una red VPN dentro de la UMA. Precisamente necesitamos tener activada la VPN para poder conectar con el servidor.

Comunicación entre dos archivos de Packet Tracer

Para conectar nuestro Packet Tracer al servidor, necesitamos un componente llamado Multiuser Connection, que permite conectar un cable desde un puerto de un equipo de nuestro diseño a otro puerto de otro equipo en el Packet Tracer remoto.

Para aprender a usarla, añade una conexión multiuser a tu diseño (está en su propia sección de la paleta, con el icono de una nube). Si haces click en la nube aparece un panel de configuración. Por defecto está en **modo servidor** (*incoming*), pero se puede cambiar a modo cliente (*outgoing*). Evidentemente, para conectar dos esquemas de Packet Tracer, uno de ellos tiene que tener una conexión Multiuser en modo servidor y el otro en modo cliente:





En la configuración de la conexión en modo cliente se deben especificar los parámetros para encontrar el otro programa, que puede estar corriendo en el mismo o en otro ordenador: IP, el puerto TCP, el nombre de la conexión en el otro Packet Tracer y el password. Cuando pulsamos **Connect en el cliente** la nube del cliente debe ponerse de color azul si todo va bien.

Los parámetros para conectar al servidor de circuitos WAN en esta práctica son:

- **Servidor**: ptracer.ho.ac.uma.es (conéctate a la VPN antes).
- **Puerto**: 38002
- **Network name**: Es una cadena con el formato **Ex-VPC-Sy-Sz-t**, donde ***x*** es el número de empresa (1 a 5), ***y*** y ***z*** son el número de los sites a conectar (de 1 a 6) y ***t*** es el extremo del enlace (la letra A o B). Tu profesor te asignará en clase un número de empresa y site.

Por ejemplo, para conectar el site 3 de la empresa 4 con sus vecinos, se conectará a *E4-VPC-S2-S3-B* y a *E4-VPC-S3-S4-A*, mientras que su vecino del site 2 se conectará a *E4-VPC-S1-S2-B* y a *E4-VPC-S2-S3-A*.

- **Password**: Es siempre *vc0910$$*.

El vecino anterior al site 1 es el 6, y el siguiente al 6 es el 1, para poder formar un anillo de sites.

Una vez establecida la conexión (la nube se pone en color azul al pasar el ratón por encima y podemos ver los datos de la conexión) podemos conectar los cables entre puertos de cualquier equipo local y el puerto remoto que aparezca en la nube. Al pinchar en una nube ya conectada para conectar un cable, nos listará el puerto disponible para conectar.

No pongas los cables antes de conectar las nubes y nunca elijas la opción create new link. No sirve de nada ya que conecta el cable a la nube remota pero sin un puerto. Tu cable quedará desconectado para siempre ya que no hay nadie en el servidor que lo conecte. Sin embargo, cuando conectas un cable después de conectar la nube te da a elegir los puertos que han sido ya conectados remotamente.
Si conectas correctamente un cable a una nube remota y guardas el diseño, las conexiones realizadas se conservan aunque cierres Packet Tracer o la conexión a la nube remota.

Configuración del enlace punto a punto entre routers WAN

Para conectar ambas empresas necesitamos primero conectar ambos routers. Los pasos para cablear son los siguientes:

- Como router WAN de tu site añade un router genérico vacío y ponle un puerto Ethernet a 1 Gbps en cobre y dos puerto Ethernet a 1 Gbps en fibra.
- Crea una conexión Multiuser en el Packet Trace. Conecta con el extremo A o B del circuito privado virtual que debes usar para conectar al otro site. (El nombre del circuito está descrito más arriba).
- Cuando la nube esté de color en azul hay que conectar el router a la nube con una **fibra óptica** usando un puerto Ethernet óptico de 1Gbps del router WAN. En el lado de la nube elige el puerto óptico remoto.
- Activa el interfaz óptico (**no shutdown**). Si el cable está conectado correctamente, el diodo del interfaz debe pasar a color verde y aparecerán mensajes en la consola indicando que el interfaz está activo.

El estado del enlace solo indica que el puerto del router ha negociado bien con el puerto del switch de la red del operador. Pero si el router WAN del otro site no está bien conectado, no habrá nadie a quien entregar los paquetes Ethernet que atraviesan la red del operador.
Antes de seguir verifica que ambos routers WAN tengan sus enlaces operativos.

- El siguiente paso es configurar la dirección IP de cada extremo del enlace. Un enlace punto a punto **es una subred de 4 direcciones IP**. Como la primera y la última no se pueden usar, necesitamos usar las dos intermedias. La máscara a usar es /30 (255.255.255.252). Recuerda que la subred no puede comenzar en cualquier dirección, sino que su inicio debe ser múltiplo de su tamaño.
  Es decir, que un enlace no puede comenzar por ejemplo en 192.168.0.2/30 ya que esta dirección con esa máscara **pertenece obligatoriamente al bloque** de 4 IPs que comienza en 192.168.0.0 y llega hasta 192.168.0.3.

- Recuerda documentar siempre los enlaces punto a punto antes de configurarlos.
- Una vez puestas ambas direcciones, prueba a hacer ping desde la consola de uno de los dos routers al otro para verificar que hay conectividad IP.

Una vez terminada la configuración de todos los enlaces WAN de tu site, recuerda conectar tu router punto a punto con el router LAN:

- Pon un cable ethernet cruzado (cross-over) entre los puertos Ethernet libres de ambos routers.
- Elige un par de direcciones para el enlace punto a punto del rango que te ha sido asignado para tu site y añade una tabla adicional para los enlaces punto a punto locales a tu site (**distinta de la tabla de enlaces punto a punto de la empresa**). En el ejemplo siguiente hay varios routers en un site y se documentan todos los enlaces punto a punto existentes (R1, R2 y W1).

Enlace	Router1	Router2	Base	IP1	IP2	Notas
Link-R1-R2	Site1-R1	Site2-R2	192.168.0.0/30	192.168.0.1	192.168.0.2	
Link-R1-W1	Site1-R1	Site1-W1	192.168.0.4/30	192.168.0.5	192.168.0.6	

- Activa los interfaces físicos de ambos routers y configura las direcciones IP.
- Prueba el nuevo enlace haciendo ping desde un router al otro.

3. Adaptación de los sites para poder comunicarse

Uno de los mayores problemas que nos vamos a encontrar en una fusión es que, como las redes fueron diseñadas sin prever que se fusionarían, ambas están usando los mismos rangos de direcciones IP para distintas VLANs. Como las direcciones están duplicadas en ambas empresas, es imposible que nada pueda funcionar globalmente.

Para resolverlo tenemos que renumerar las empresas con el plan de numeración IP global a todos los sites que se ha negociado entre todos los administradores. Tendremos que reconfigurar posiblemente todas nuestras VLANs.

La parte más tediosa no es cambiar la documentación sino cambiar la configuración. Por suerte, una gran parte de los cambios va a ser muy rápidos porque una gran parte de la configuración está centralizada en el router LAN del site.

Reconfigurar VLANs de departamentos

Ve al router LAN y salva su configuración en un fichero. Con un editor de texto reemplaza las direcciones de:

- Los pools de DHCP de las VLANs de departamentos en el router.
- Las direcciones IP de los interfaces del router en cada VLAN.

Edita siempre tu documentación primero y luego síguela para hacer los cambios de configuración sistemáticamente.

Reconfigurar VLANs del Data Center

En el Data Center no hay servidores DHCP. Los servidores de las aplicaciones tienen direcciones IP estáticas, por lo que deberías de cambiarlas entrando en cada servidor uno a uno, de nuevo usando la documentación.

4. Configurando el Routing dinámico entre sites

Hasta el momento solo hemos conseguido que los routers LAN puedan verse entre sí, pero no pueden enrutar tráfico de sus VLANs hacia el otro site porque no conocer qué subredes existen detrás de su router vecino.

En lugar de configurar manualmente la lista de rutas de la empresa en cada router vamos a configurar un algoritmo de Routing dinámico para que los routers actualicen de forma automática dicha información de forma que cualquier cambio futuro se propagará inmediatamente.

Existen diferentes algoritmos de Routing dinámico. Los más usados dentro de una empresa son RIPv2, EIGRP y OSPF. La configuración de todos ellos es prácticamente idéntica.

Configuración del algoritmo de routing en cada router

1. En la consola de comandos de **todos y cada uno de los routers LAN** configuramos EIGRP con los siguientes comandos después de haber entrado en el modo de configuración. Los diversos subcomandos cambian aspectos importantes del funcionamiento:
    - El comando **router eigrp** indica el identificador del **Autonomous System** (AS) que usarán todos los routers del grupo que quieran compartir rutas. Un router puede estar en varios AS a la vez, por lo que hay que elegir un AS para los routers de toda la empresa que necesiten compartir rutas de forma dinámica.
    - El comando **auto-summary** indica que no se deben agregar todas las subredes en una sola **super-red** que contenga todas las direcciones, sino que se deben enviar las subredes de forma independiente.
    - El comando **`network`** tiene dos funciones:
        i. Indica por qué interfaces se puede intercambiar información con otros routers. Solo se puede dialogar por un interfaz **cuya dirección IP esté incluida en el patrón especificado por algún comando network**.
        ii. También indica qué subredes IP pueden incluirse en la información enviada a otros routers. Por tanto, una subred solo se envía a un router vecino si el rango IP **está incluido en el patrón especificado por algún comando network**.
        iii. El comando network incluye un wildcard que permite restringir el rango definido a un patrón mucho más pequeño que la clase por defecto.

    Así, en el ejemplo siguiente, el patrón 192.168.0.0 0.0.0.7 indica que si el router puede negociatr por cualquier interfaz que tenga una dirección dentro del rango 192.168.0.0/28 y el patrón 10.0.0.0 0.0.255.255 indica que se puede enviar información de todas las VLANs conocidas con el prefijo 10.0.x.x.

```
# Este router forma parte del AS 400
router eigrp 400
 no auto-summary
 # Este patrón solo se aplica al rango 192.168.0.0/28
 network 192.168.0.0 0.0.0.7
```

```
 # Este comando solo se aplica a 10.0.0.0/16
 network 10.0.0.0 0.0.255.255
```

2. Si, como ejemplo, usamos el comando **`sh ip protocols`** en un router podremos ver el estado del protocolo de routing dinámico. Por ejemplo la lista de routers de los que se recibe información:

```
Router-WAN0#sh ip protocols

Routing Protocol is "eigrp  400 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
Redistributing: eigrp 400
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
     192.168.0.0/28
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.0.5     90            167008
  Distance: internal 90 external 170
```

3. Usando el comando **`sh ip route`** en cualquier router podremos ver las tablas de rutas incluyendo tanto rutas estáticas como las aprendidas dinámicamente. La letra que precede a cada entrada indica la fuente de la que se ha obtenido la ruta. Por ejemplo las obtenidas por EIGRP tienen una **D** delante:

```
Router-WAN0#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 4 masks
D       10.0.0.0/23 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.0.2.0/23 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.0.4.0/24 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.0.5.0/24 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.0.6.0/25 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.0.6.128/26 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.1.0.0/23 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.1.6.0/23 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
D       10.1.12.0/24 [90/30720] via 192.168.0.5, 00:01:17, GigabitEthernet9/0
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.4 is directly connected, GigabitEthernet9/0
```

Prueba final de la conectividad

Para verificar que el Routing dinámico está funcionando correctamente:

- Primero verifica que en cada router LAN aparecen las rutas de **todas las VLANs de departamentos de los sites remotos**. Si solo aparecen las VLANs locales, repasa la configuración.
- Después verifica que un PC de un departamento de un site puede hacer ping a algún interfaz del router LAN del otro site. Preferiblemente una VLAN del data center del otro site.

- Si eso funciona prueba ahora a hacer ping o incluso acceder a la web de un servidor web de un site distinto (con ping y con el navegador http).
- También puedes verificar que los PCs de departamentos de distinto site pueden hacer ping entre ellos, aunque esto no es de mucha utilidad en la realidad.

Para verificar las rutas, además de usar la consola de cada router, puedes usar la herramienta con la lupa y abrir una ventana con la tabla de rutas de cada router.

Nota importante:

Las comunicaciones a través del enlace WAN pasan a través de otro Packet Tracer que está simulando una red Ethernet muy realista. Dependiendo de la concurrencia y debido al coste de la simulación y las comunicaciones entre Packet Tracers, es posible que el algoritmo de routing sufra timeouts que hagan que las rutas aparezcan y desaparezcan de tus routers cada pocos segundos.

Si las rutas no se quedan de forma estable, será difícil que puedas hacer operaciones de más alto nivel tales como usar el navegador web. Si esto pasa continuamente y no eres capaz de completar ninguna prueba, avisa a través del foro de la asignatura.