La red del Data Center

Guillermo Pérez Trabado *©2016-2022*

Diseño de Infraestructuras de Redes

Depto. de Arquitectura de Computadores - Universidad de Málaga

Introducción

En esta etapa ya se ha configurado en enrutamiento entre todas las LANs de los departamentos de la empresa, pero no hemos organizado los servidores del Data Center. De hecho, los servidores han quedado en la VLAN 1, que es la VLAN por defecto de los switches, y dicha VLAN es inaccesible por parte del router ya que no hemos creado ningún subinterfaz para la misma.

En la realidad de una empresa, para no hacer los cambios de forma traumática hubiéramos configurado un interfaz para la VLAN1 de forma que los departamentos podrían seguir accediendo a los servidores a través del router para mantener la compatibilidad con el diseño anterior mientras hacemos la transición.

El paso actual consiste en mejorar la seguridad de nuestro data center separando:

- Cada **stack de aplicación** en su propia subred, dividida a su vez en tres tiers con sus correspondientes LANs internas aisladas (sin router).
- Los **servicios de soporte** (como DNS) que el data center presta a los departamentos, también estarán en LANs separadas.

En este paso no vamos a controlar el acceso de cada departamento a las aplicaciones del data center, pero en el futuro, el hecho de tener cada aplicación en una red independiente nos va a facilitar la escritura de reglas de ACL (Access Control List) que son las reglas que los cortafuegos usan para restringir el acceso a las aplicaciones.

1. Diseño lógico

El primer paso es elaborar el diseño lógico que detalla cómo dividir todos los servidores del Data Center en subredes aisladas entre sí para aumentar la seguridad.

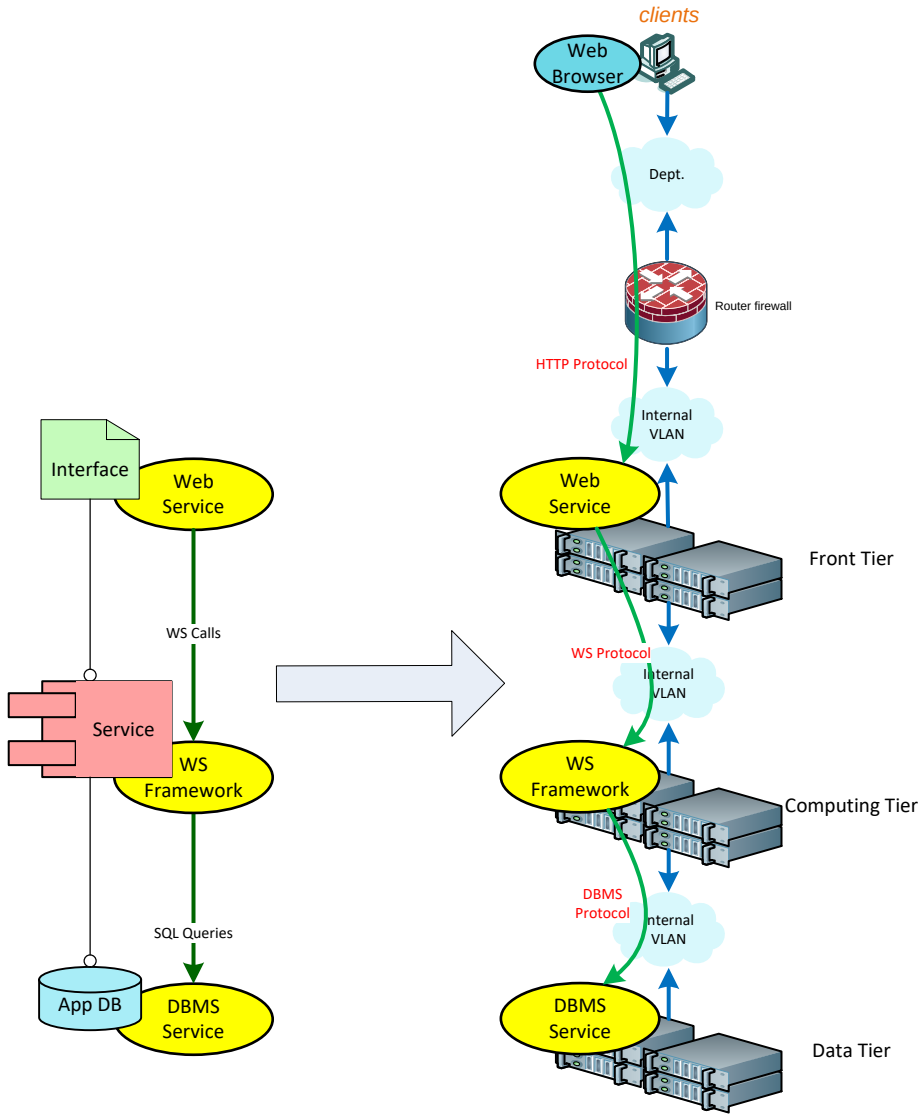
Modelo de 3 layer y 3 tiers

En la introducción de la asignatura explicamos cómo las aplicaciones se implementan con tres capas de software (interface layer, business logic layer y data layer) que se ejecutan en tres capas de servicios. Los servicios deben ejecutarse en una **infraestructura** formada por hosts (tiers) separados, lo que resulta en que una aplicación requiere usar al menos tres hosts. En la realidad de la empresa, las necesidades de **alta disponibilidad** (tolerancia a fallos) y **load balance** (aumento de la capacidad de procesamiento) requieren que cada tier sea en realidad un cluster formado por dos o más servidores.

Además, la seguridad de la infraestructura requiere que no haya conexión directa de red entre hosts que no tengan obligatoriamente que comunicarse entre sí. Esto da lugar a una arquitectura de red en forma de torre (stack) de hosts separados con LANs aisladas que solo

sirven para interconectar entre sí los hosts de un tier con los del siguiente. Este tipo de diseño ha empezado a recibir el nombre de **network micro-segmentation**, que consiste en crear multiples LANs específicas para interconectar algunos componentes del Data Center y que no tienen conexión a ningún router. Este diseño se ha popularizado dato que las LANs intermedias en realidad son VLANs definidas por software con un coste muy reducido ya que no son equipos reales. El objetivo de la micro-segmentación es **reducir la superficie de ataque** de cada componente haciendo que solo pueda ser accedido por aquellos otros que realmente necesitan dicho acceso.

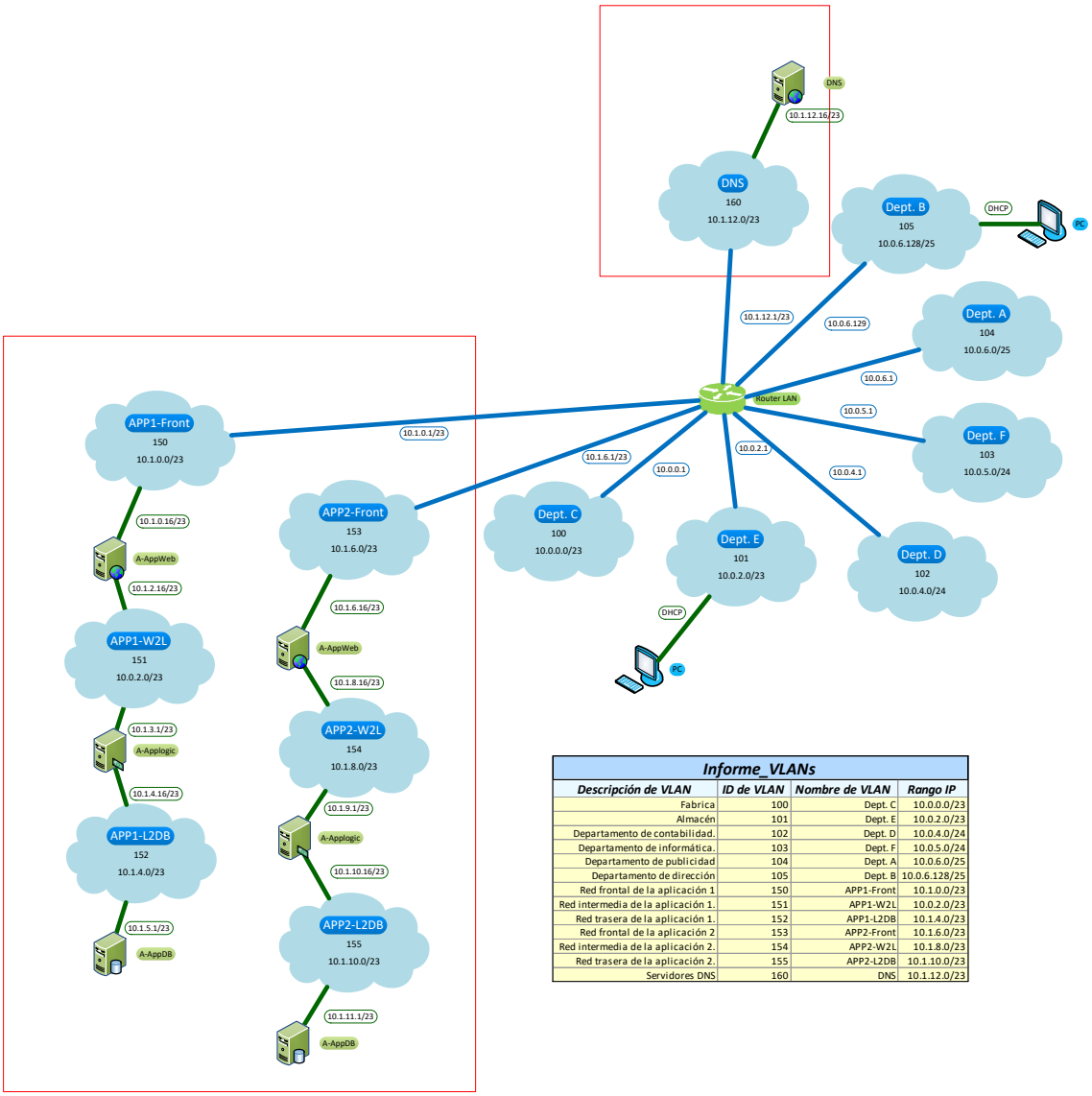
En la figura siguiente puede observarse la arquitectura de layers (a la izquierda) y el stack de hosts de la infraestructura usando network micro-segmentation (a la derecha). Observa que la red del front-tier (servicio web) debe ofrecer acceso a los departamentos a través del router. Sin embargo, el router nos permitirá especificar reglas de acceso para restringir al máximo la superficie de ataque de este primer tier, por lo que realmente tendremos un firewall.



Estructura lógica del data center

Dada la cantidad de nuevas LANs y la complejidad de la conexión de los hosts, hemos de añadir la estructura del data center a nuestro esquema lógico para facilitar el diseño y su posterior

implementación. En la figura siguiente puedes ver que al diseño ya existente se han añadido los stacks de las dos aplicaciones existentes y otra VLAN adicional para el servidor de DNS.



Informe_VLANs			
Descripción de VLAN	***ID de VLAN***	***Nombre de VLAN***	***Rango IP***
Fabrica	100	Dept. C	10.0.0.0/23
Almacén	101	Dept. E	10.0.2.0/23
Departamento de contabilidad.	102	Dept. D	10.0.4.0/24
Departamento de informática.	103	Dept. F	10.0.5.0/24
Departamento de publicidad	104	Dept. A	10.0.6.0/25
Departamento de dirección	105	Dept. B	10.0.6.128/25
Red frontal de la aplicación 1	150	APP1-Front	10.1.0.0/23
Red intermedia de la aplicación 1.	151	APP1-W2L	10.0.2.0/23
Red trasera de la aplicación 1.	152	APP1-L2DB	10.1.4.0/23
Red frontal de la aplicación 2	153	APP2-Front	10.1.6.0/23
Red intermedia de la aplicación 2.	154	APP2-W2L	10.1.8.0/23
Red trasera de la aplicación 2.	155	APP2-L2DB	10.1.10.0/23
Servidores DNS	160	DNS	10.1.12.0/23

Varios detalles y dudas a aclarar sobre la estructura del data center:

- **Uso de LANs entre servidores**: Podría pensarse en la posibilidad de unir los servidores de una aplicación mediante enlaces punto a punto (un cable). Sin embargo, hemos mencionado que normalmente un tier está formado como mínimo por dos hosts configurados como un cluster. Si cada host del cluster de un tier se comunica con todos los hosts del cluster del tier siguiente, evidentemente necesitamos una VLAN en lugar de un cable para poder implementar las comunicaciones y garantizar el crecimiento futuro. Incluso si solo tenemos una máquina (host) en cada tier, en el futuro podemos evolucionar hacia un cluster, por lo que es mejor hacer una configuración escalable.
- **Plan de numeración IP del data center**: Por las mismas razones anteriores (la escalabilidad) debemos asignar un rango IP a cada LAN con suficientes direcciones como para soportar los interfaces de los servidores que forman los dos clústeres que se encuentran en una VLAN.

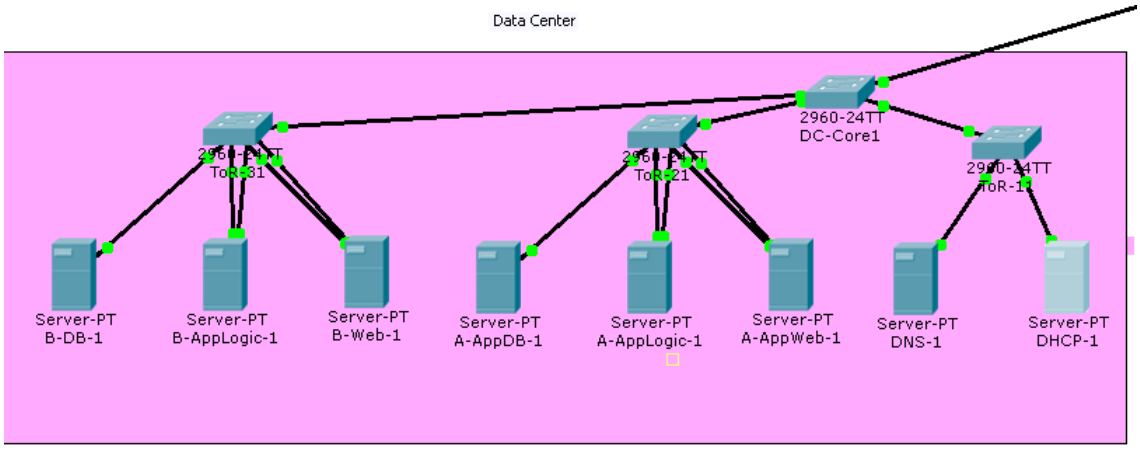
Respecto a cómo numerar dichos rangos, tenemos que hacer que la numeración sea compatible con la de los departamentos. Es decir, usar parte de la subred 10.x.x.x/8 que no esté asignada a los departamentos. Como el número de departamentos puede crecer en el futuro, es recomendable no empezar a asignar justo detrás del último departamento, sino dejar un hueco libre para poder ampliar el intranet de departamento sin colisionar con el data center. Por ejemplo, en lugar de comenzar a numerar en 10.0.7.0 en nuestro ejemplo, podemos saltar a 10.0.128.0 o bien 10.1.0.0 para dejar más o menos hueco a los departamentos y otras oficinas.

- **Aislamiento de las LANs del data center:** Una duda que a veces se plantea es si el hecho de que un host esté conectado a dos LANs a la vez implica que el tráfico IP puede atravesar de una LAN a otra a través de dicho host. La respuesta es **no**. El sistema operativo de un host no tiene activada la función de **forwarding** como sí la tiene un router. Si un origen trata de enviar paquetes IP a un host para que los reenvíe por otro de sus interfaces, el comportamiento del host será descartar (**drop**) los paquetes recibidos.

2. Diseño físico del data center en Packet Tracer

Para implementar en Packet Tracer la estructura lógica del data center necesitamos:

- Crear las VLANs necesarias para interconectar los servidores en los switches del data center. Esto es fácil de realizar ya que tan solo tenemos que dar de alta las nuevas VLANs en el switch máster de VTP de nuestra red.
- Disponer de dos interfaces de red en cada servidor del tier de lógica de negocio y en el de interfaz de usuario. En un escenario real esto se puede realizar poniendo los enlaces de los servidores en modo trunk y creando subinterfaces para cada VLAN en el interfaz del host. Sin embargo, Packet Tracer no es capaz de simular el trunking en los servidores, por lo que es necesario añadir una segunda tarjeta de red a cada servidor de los dos tiers mencionados, tal como se muestra en la figura siguiente.



Como se observa en el esquema lógico, no hay que conectar el router LAN a las VLANs internas del data center con excepción de la más frontal de cada aplicación. Por otro lado, al no haber router, tampoco hay servidor DHCP en cada VLAN del data center por lo que las direcciones IP de cada servidor **se asignan de forma estática**.

3. Actualizar la documentación del plan de numeración

En el diseño lógico se han añadido nuevas LANs al diseño con sus respectivos rangos IP. La hoja de cálculo en Excel que hemos elaborado previamente debe actualizarse con las nuevas VLANs y sus respectivos rangos IP.

Algunas de estas VLANs están conectadas al router y otras no. En el caso de aquellas que están aisladas simplemente tenemos que dejar en blanco la celda que designa el router de la VLAN.