Conceptos Previos (V1.1)

Infraestructuras de Redes

Escuela Técnica Superior de Ingeniería Informática

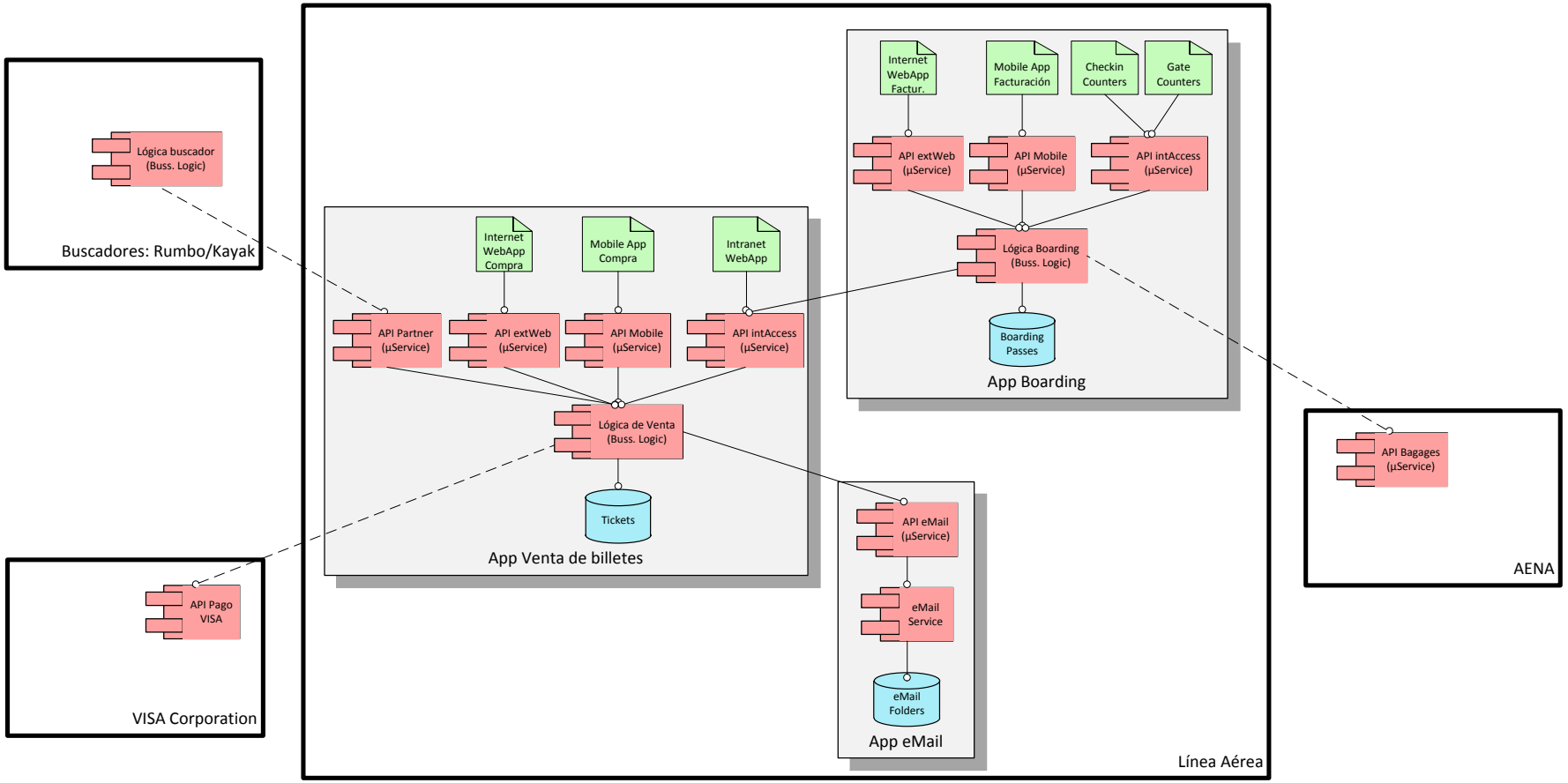
Depto. de Arquitectura de Computadores
Universidad de Málaga

Aplicación

- Aplicación: Herramienta que apoya en el desarrollo de una **función** de la empresa.
  - La aplicación suele incluir una Base de Datos, Algoritmos (lógica de negocio) y UI (interfaces).
  - Una WebApp y una MobileApp no son aplicaciones. Son solo UIs de una aplicación.
  - Por ejemplo: vender billetes de avión. Podemos tener una App, una página Web en Internet, y otro UI Web para los trabajadores internos.

- Las aplicaciones de la empresa se **aíslan** totalmente entre sí para facilitar el diseño, mantenimiento, despliegue, infraestructuras, etc.
  - La venta de billetes de unas líneas aéreas y la facturación en los aeropuertos son aplicaciones distintas.
    - Por ejemplo, el asiento concreto se asigna en la tarjeta de embarque, no en el billete. Pero el billete indica qué tipo de asiento hemos pagado.
  - La aplicación de facturación requiere consultar datos de la aplicación de billetes para aceptar la generación de la tarjeta de embarque. La única relación entre ambas es una API para que una pueda consultar esos datos de la otra.
  - Ambas aplicaciones necesitan usar una API con la aplicación de eMail para enviar confirmaciones.
  - Ambas aplicaciones se comunican con las de otras empresas.

Ejemplo: Línea aérea



FT, HA y DR

- Fallos a gran escala:
  - **Desastre**: Incidente que genera fallos múltiples o críticos, y posiblemente permanentes: Corte de energía, incendio, inundación, robo de equipos, hacking, …
  - **Disponibilidad**: Tiempo que está disponible una aplicación (normalmente se mide en % sobre un año completo).
- Capacidades de una aplicación frente a fallos:
  - **FT (Fault Tolerance)**: Capacidad de seguir funcionando sin errores a pesar de existir algunos fallos.
  - **HA (High Availability)**: Alta Disponibilidad. Capacidad de no parar los servicios nunca (que estén siempre disponibles), incluso con una gran acumulación de fallos.
  - **DR (Disaster Recovery)**: Capacidad combinada FT y HA incluso para desastres a gran escala. Implica mantener el servicio y no perder datos.

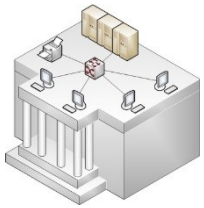
Service Level Agreement

- Es un acuerdo escrito que especifica los niveles mínimos de «servicio» que una infraestructura IT debe ofrecer.
- Incluyen diversos aspectos divididos en dos campos:
  - Availability: Especifican el nivel de Availability ofrecido, detallando a qué tipo de fallos es tolerante (averías de equipos concretos como routers, switches, etc.) y a cuáles no lo es. También se especifica si debe ser tolerante a desastres.
  - Rendimiento: Especifica el comportamiento esperado de la infraestructura de red, especificando mínimos garantizados en parámetros como:
    - **Latencia** máxima: retardo de los paquetes al cruzar la red. Está fuertemente ligado al RTT (Round Trip Time).
    - **Throughput** mínimo: volumen de **tráfico sostenido** que puede atravesar la red medido en (K/M/G)bits/s.
    - **Tasa de error** máxima: probabilidad de 1 bit erróneo. La tasa de error actual es tan baja que es equivalente a cero.
    - **Tasa de drop** máxima: probabilidad de perder un paquete por congestión en la red. La congestión es la fuente principal de pérdida de paquetes.
    - **Jittering** máximo: Desviación estándar de la latencia. Es la variabilidad en el retardo. No basta que la transmisión sea rápida, sino que tiene que ser predecible.
- El SLA forma parte del contrato entre el Operador de Telecomunicaciones y la Empresa que usa los servicios.

Ubicación de las Infraestructuras

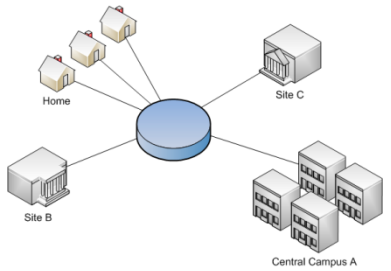
- Data Center: Concentración de sistemas en una sala o varias salas en el mismo edificio.
  - Un Data Center está expuesto a sufrir una **destrucción completa** en caso de **desastre**.
- Site: Data Center de la misma empresa suficientemente separado de otro como para que no sean afectados por el mismo desastres.
  - ¿En el mismo edificio? -> No es un site.
  - ¿En el mismo campus? -> No es un site.
  - ¿En la misma ciudad? -> Se considera site, aunque hay desastres que los afectan conjuntamente: inundaciones, huracanes, terremotos,…
  - ¿En la misma región? -> Site

Edificio

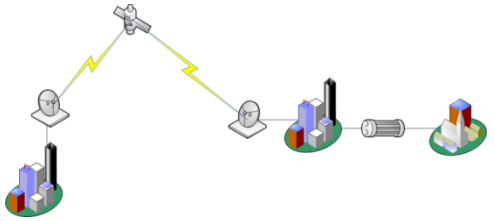


Campus

Ciudad

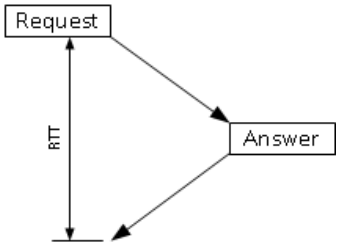


Región
Pais



Latencia

- El principal enemigo de la distribución geográfica es el RTT (Round Trip Time).
- El RTT determina la **latencia mínima** de un servicio web (WS) independientemente de su implementación.
- El **rate** de un servicio (calls/s) en un programa secuencial está limitado por el RTT.
  - LAN Ethernet: : RTT_{aprox}<1ms ➔ >1000 calls/s
  - Málaga-Madrid: RTT_{aprox}~ 10-20ms ➔ 100-50 calls/s
  - Málaga-Berlín: RTT_{aprox}~ 53ms ➔ 33 calls/s
  - Málaga-Oslo: RTT_{aprox}~ 81ms ➔ 12 calls/s
  - Málaga-Atlanta, GA: RTT_{aprox}~ 109ms ➔ 9,1calls/s
  - Málaga-Vancouver: RTT_{aprox}~ 177ms ➔ 5,6 calls/s
  - Málaga-Japón: RTT_{aprox}~ 245ms ➔ 4 calls/s



On premises, Cloud, Hybrid

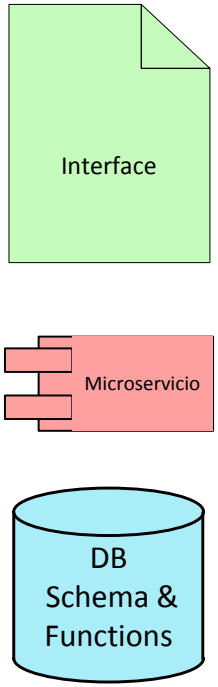
- On-premises Data Center:
  - Los sistemas propiedad de la empresa están ubicados en los locales de la propia empresa.
- Colocation Data Center:
  - Los sistemas propiedad de la empresa están en espacio alquilado Data Center gestionado por otra empresa. El alquiler incluye todos los servicios adicionales: seguridad, refrigeración, extinción de incendios, electricidad.
  - https://www.movistar.es/grandes-empresas/soluciones/centro-datos-gestionado/
  - https://ww2.movistar.cl/empresas/productos-y-servicios/servicios-digitales/housing-data-center/
  - https://phoenixnap.com/blog/data-center-colocation
- Virtual Data Center (Cloud):
  - Los sistemas son alquilados a otra empresa que los gestiona en su propio Data Center. Pueden ser sistemas físicos o virtuales.
  - Amazon Web Services, OVH, Digital Ocean, …
  - https://www.movistar.es/grandes-empresas/soluciones/fichas/virtual-data-center/#
- Hybrid Data Center:
  - Los sistemas están repartidos entre los tipos anteriores.
  - Las leyes de protección de datos prohíben que ciertos datos estén físicamente fuera de la empresa, por lo que puede ser imprescindible un Data Center On-premises (ejemplo: las administraciones públicas).

Clusters y Sites

- **Cluster**: Grupo de servidores que trabajan conjuntamente prestando el mismo servicio.
  - Al trabajar cooperando estrechamente, deben estar muy cerca (limitación de rate por RTT). Como mucho deberían estar a menos de 10 Km.
  - El riesgo de corte de comunicaciones entre Sites complica mucho la implementación.
  - **Por tanto, un cluster siempre está en un solo Site.**
    - Para replicar datos entre Sites se usan estrategias **entre clusters**.
- Ubicación de los sites:
  - Los Sites deben estar suficientemente alejados para reducir el riesgo de desastres comunes.
  - Los Sites deben estar cerca de los clientes de cada región en la que operamos para reducir el RTT.
  - Preguntas:
    - ¿Es realmente un servicio Cloud totalmente transparente?
      - No. Debemos saber explícitamente en qué sites vamos a contratar en función de las regiones de nuestros clientes.
    - En Manassas,VA, Amazon tiene dos Data Centers distintos a ambos lados de una misma calle. ¿Es eso tolerante a desastres?
      - Depende del desastre.

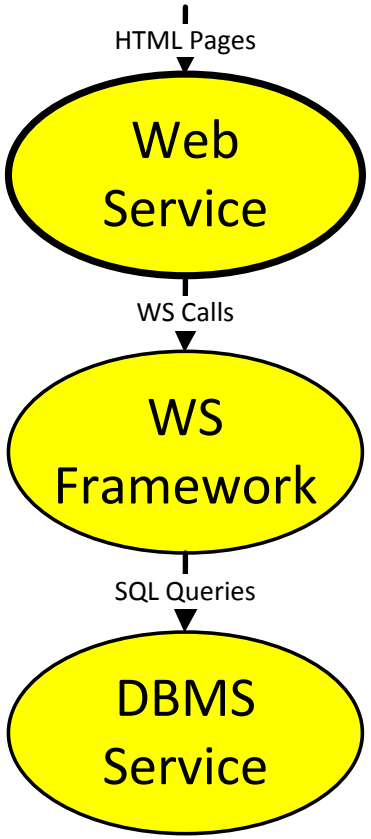
Módulos Software de la Aplicación

- Nos referimos al código que los programadores escriben para implementar la aplicación.
  - Interfaces HTML:
  - Funciones del negocio (microservicios SOAP,REST):
  - Esquema de BD y código dentro de la BD.



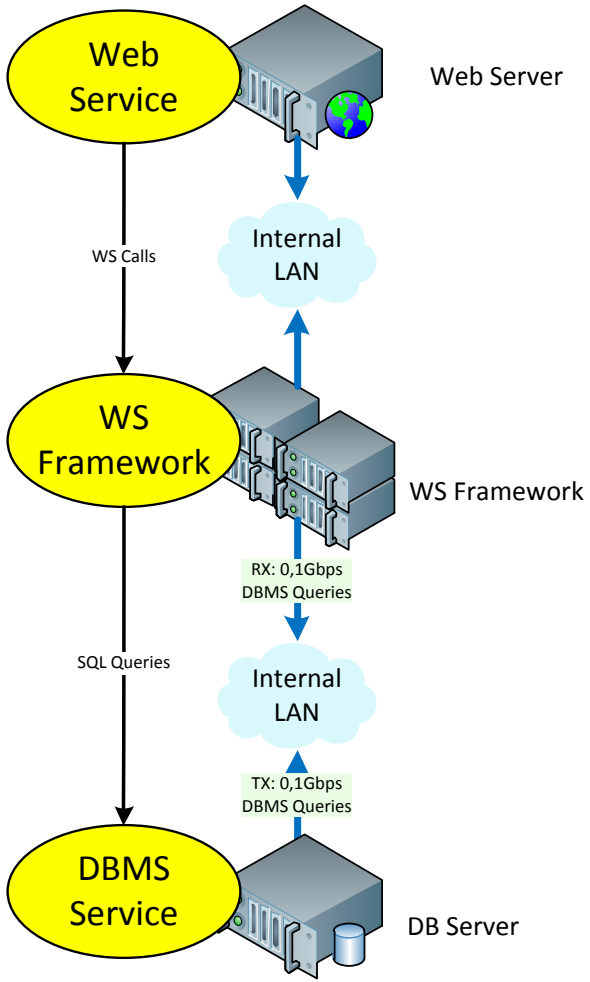
Servicios

- Los servicios son procesos que se ejecutan permanentemente en una máquina (SO).
  - Servicios de UI: Apache, MS IIS, NGINX, SSH, …
  - Frameworks para ejecutar microservicios: Tomcat, JavaEE (Glassfish, JBOSS, Oracle WL, IBM Websphere), Apache,…
  - Servicios de BD y NAS: Oracle, MySQL, Postgres, SQLServer, NFS, SMB, …



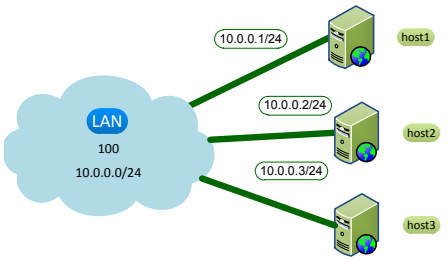
Hosts (~~Servidores~~)

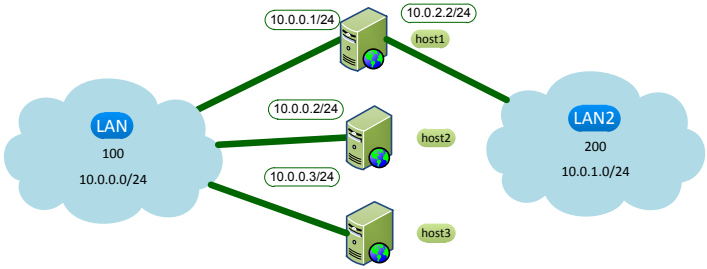
- Los **hosts** son máquinas que ejecutan un Sistema Operativo y que pueden ejecutar uno o más servicios.
  - Un **host** puede ejecutar a la vez los **servicios** Apache y Oracle. ¿Pero debe hacerlo?
- Es preferible evitar el término **servidor** ya que es muy ambiguo (puede ser una máquina o un servicio).
  - El «*servidor web*», ¿es la ***máquina*** que ejecuta el servicio web o es el ***proceso*** del servicio web?
  - Nota: Tradicionalmente se refiere a la máquina, pero es preferible decir «**el host que ejecuta el servicio web**». Si dicha máquina también ejecuta un DBMS, al decir «*el servidor de BD*», estamos hablando del mismo host.

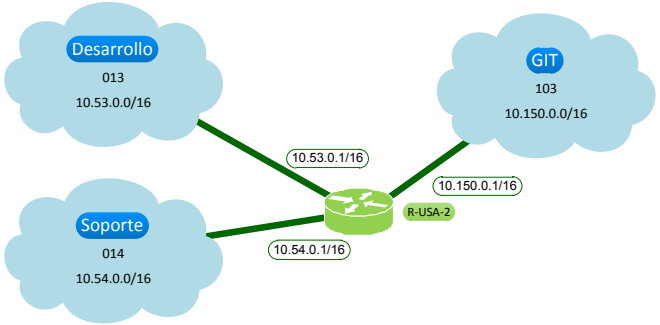


LAN

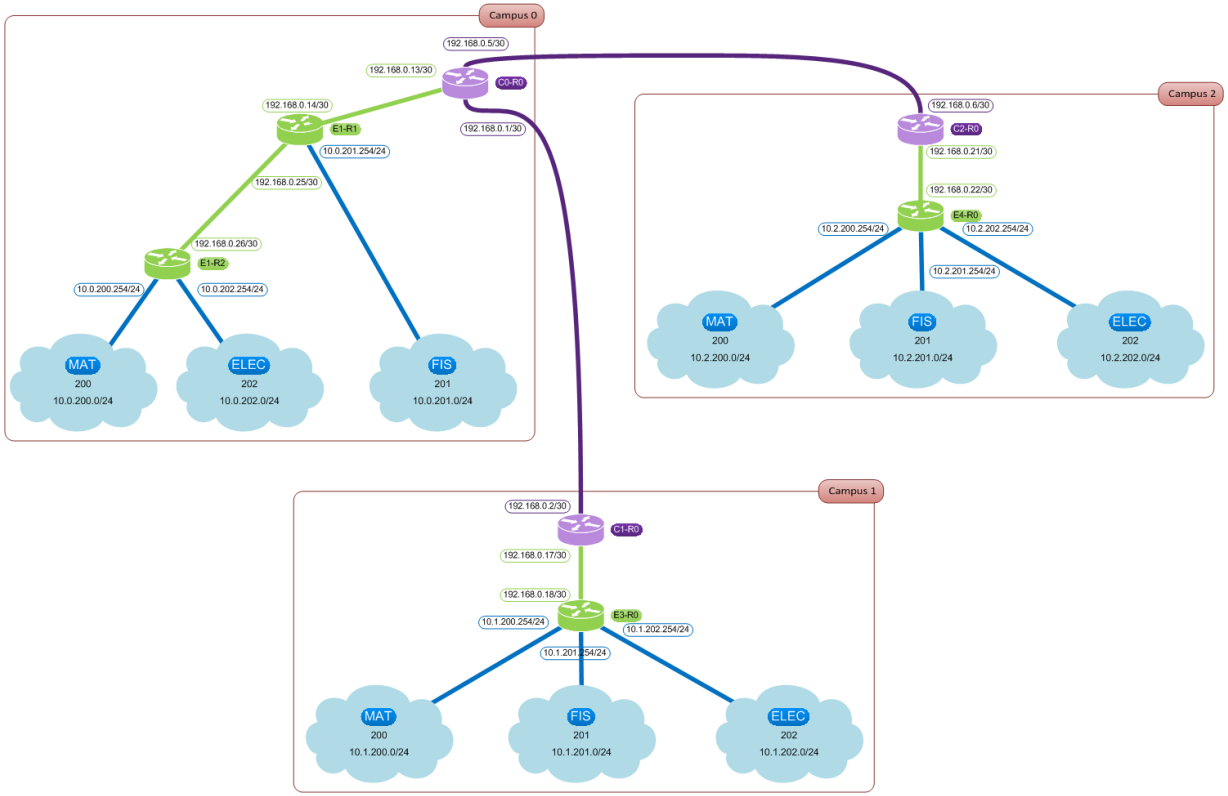
- Una LAN es una red de nivel 2 con tecnología IEEE 802.x (Ethernet, Wifi, etc) en la que todos los hosts pueden comunicarse entre ellos sin pasar por un router IP.
  - Una LAN tiene asociado un rango IP único (IP base+mascara).
- Un host puede estar conectado a varias LANs.
  - Cada interfaz (NIC) tendrá una IP en el rango de cada VLAN.
- Dos o más LANs se interconectan a través de un router.
  - Cada interfaz del router tendrá una IP en el rango de cada VLAN.







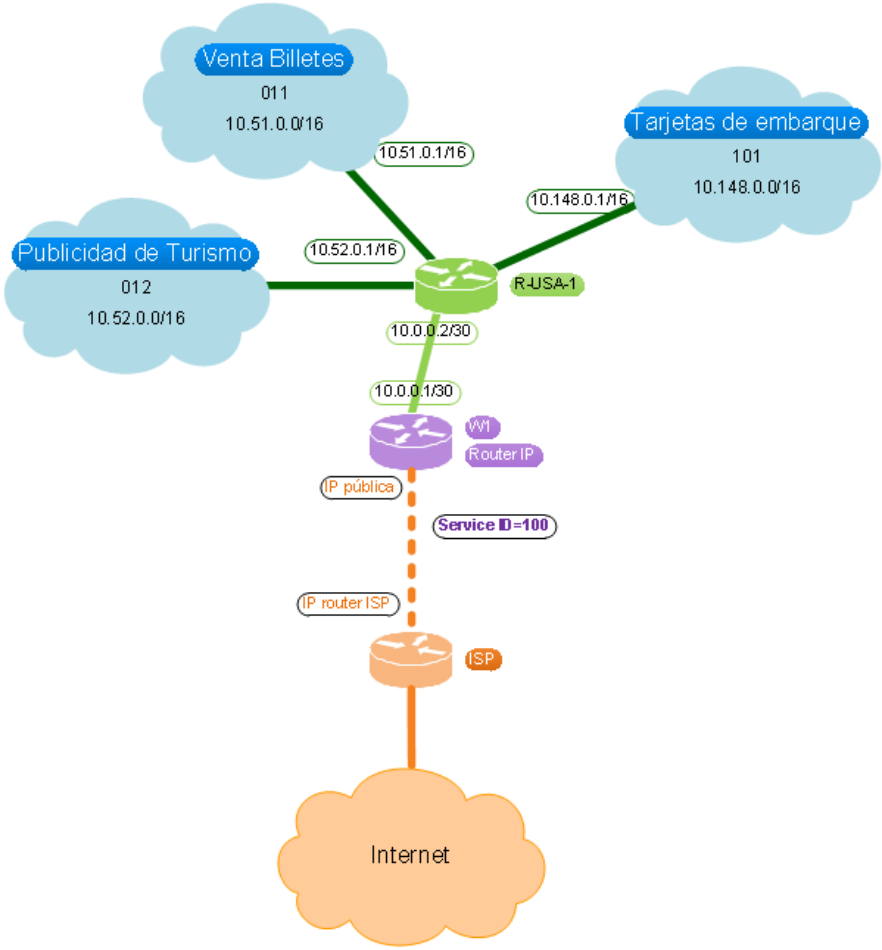
WAN



- Un enlace WAN es una Interconexión **privada** a gran distancia entre dos **sites**.
  - Por cuestiones de coste, no es propiedad de la empresa.
  - Se **alquila** como servicio a un **Operador de Telecomunicaciones**.
- Los enlaces WAN incluyen un **router WAN en cada extremo** (en morado) que hace de interfaz entre el Router LAN y la red del operador.
  - El enlace a través de la red WAN (en morado) funciona como una conexión transparente punto a punto (no se ven los equipos del operador).
  - Aunque pasa por un operador, no tiene nada que ver con **Internet**.

Internet

- El acceso a Internet es un servicio de un ISP (Internet Service Provider) que consiste en enrutar tráfico al conjunto de Internet.
- Consta de dos servicios:
  - Una conexión WAN hasta el router del ISP (enlace punteado).
  - El propio servicio de enrutamiento en el ISP (router naranja).
- Si la empresa tiene varias aplicaciones:
  - Pueden compartir el acceso mediante un router.
  - Cada aplicación puede tener un acceso separado para evitar interferencias.



Servicios WAN y servicio de Internet

- Los operadores de telecomunicaciones ofrecen distintos tipos de servicios.
  - Conexiones WAN privadas punto a punto (Transporte de datos).
  - Servicio de acceso a Internet (ISP).
- Las conexiones WAN son privadas por su implementación tecnológica.
  - Son servicios de nivel 2 (links).
  - No «pasan» por internet. Los implementa la red de transporte privada del operador (fibra+switches).
- El servicio de Internet requiere dos servicios:
  - El enlace WAN hasta el ISP.
  - En servicio de tránsito (enrutamiento) en el ISP.
  - Cada uno puede ser un cuello de botella. Ejemplo:
    - La fibra doméstica usa un enlace óptico GPON a 2Gbps. El contrato del usuario define el rate permitido por el router: 100Mbps, 300Mbps, 1Gbps.
    - La fibra de empresa puede usar una fibra GPON (2Gbps) o una fibra Ethernet a 10, 25, 40 o 100Gbps. El contrato de empresa puede ir de 100Mbps hasta 100Gbps de routing a Internet.

Intranet, DMZ

- Intranet
  - No es un concepto tecnológico, sino de seguridad.
  - En general, es la parte de la red de la empresa que no tiene conexión con Internet.
    - Una **intranet** es la **red interna (sin conexión con internet)** de todos los sites de la empresa.
  - Dependiendo de la forma de interconexión entre sites:
    - Si la interconexión no pasa por internet ni está limitada por firewalls, podemos considerar que la **intranet** está formada por la **red interna completa** de todos los sites de la empresa.
    - Si la interconexión está limitada por cortafuegos, o pasa por internet, podemos considerar que cada site tiene su propia **intranet** a pesar de estar interconectadas.
- DMZ
  - Es la parte de la red de la empresa que tiene conexión a Internet: **Hacia** Internet o **desde** Internet.
  - Se considera **insegura** por principio. Expuesta a ataques de hackers.
  - Las **LANs con hosts que ejecutan servicios de aplicaciones** que dan servicio en Internet se consideran DMZ.
- Transitividad de la exposición al riesgo
  - Si un host en la **Intranet** puede conectar con una máquina en Internet, se considera que pertenece a **DMZ**, y por tanto su **LAN** no se puede considerar **Intranet**.
  - Si la LAN se conecta por un router **sin Firewall** a otras LANs, dichas LANs deben ser consideradas DMZ.

Objetivos del Diseño de Redes

- Diseñar una Infraestructura de Redes para dar servicio a las aplicaciones de una empresa.
- Entrada:
  - Diseño de las aplicaciones.
  - Distribución geográfica de la empresa.
  - Estructura organizativa y políticas de seguridad de la empresa.
  - SLA (Requisitos de HA, DR, FT, y rendimiento esperado).
- Salida:
  - **Diseño del hardware** a comprar o **servicios de telecomunicaciones** a contratar.
  - **Proyecto de instalación** de la infraestructura: Incluye instalación del software de los servicios.
  - Descripción de las tareas de **despliegue inicial,** puesta al día periódica.
  - **Plan de Continuidad de Negocio**: Incluye tareas periódicas de monitorización, mantenimiento y tareas extraordinarias de recuperación en caso de desastres.

Etapas de diseño

- Diseñaremos diversas arquitecturas iterativamente a partir de la arquitectura de la aplicación.
  - Estructura de la seguridad.
  - Diseño de la red lógica.
  - Adaptación de la estructura lógica a los sites.
  - Diseño de la red física de cada site.
  - Mapeo de la estructura lógica sobre la red física.