Sistemas Telemáticos

resumido por Alexandru Theodor Muntenas²

Capítulo 3
Servicios Transversales

Sobre el recurso

- Este resumen es una herramienta de estudio.
- Incluirá los conceptos claves de cada apartado.
- Si fuese necesario, se añadirán esquemas o gráficos para mejorar las explicaciones.
- Este recurso no tiene intencionalidad de ser una presentación de diapositivas. Se usa el formato para mejorar la maquetación.
- Toda la información proviene de la obra de *Sistemas Telemáticos (3ª edición)* de *Maciá et all*.

Introducción

- Los *servicios transverales* son servicios que, de forma independiente, no tienen funcionalidad suficiente para ser útiles para el usuario final. Son sencillos, realizan una función específica, y la combinación de estos, permite la creación de servicios más complejos.
- De todos los servicios transversales que se han desarrollado en la red destacaremos:
  - Los servicios de directorio.
  - El servicio de nombres de dominio (DNS).
  - Los servicios de seguridad.
  - El servicio de sincronización de reloj (NTP).
- Estudiaremos los primeros tres.

El servicio de directorio X.500

- Muchas veces necesitamos una serie de datos sobre los equipos, infra. y usuarios de la red para facilitar los servicios que se pretenden.
- Por ejemplo, un servicio que almacena las credenciales de acceso de los usuarios a diferentes máquinas conectadas en red.
- Por ejemplo 2, un servicio que nos informa de los diferentes nodos que componen una red y los servicios que ofrecen.
- Este tipo de servicios son ofrecidos por los *servicios de directorio*, que son como bases de datos pero con determinadas características que las hacen especiales:
  - La información se puede distribuir entre varios nodos interconectados para repartir la carga de solicitudes de servicio, aunque con el coste de aumentar la complejidad de la gestión del servicio.
  - Como la información está distribuida, disponen de mecanismos para poder encontrar la información solicitada de forma eficiente.
  - Tienen una estructura estandarizada específica que está bien documentada para organizar la información y facilitar el acceso de las aplicaciones al mismo.

El servicio de directorio X.500

- *El directorio X.500* es un estándar de servicio de directorio.
- X.500 puede tener info relacionadas con las comunicaciones, como usuarios, terminales, servidores, etc.
- X.500 es un servicio distribuido (la info está repartida en varios nodos) y accesible globalmente (puedo acceder a toda la información del directorio desde cualquier nodo).
- X.500 dispone de mecanismos de seguridad para garantizar el acceso seguro a la info.

El servicio de directorio X.500

Arquitectura del servicio

- El servicio X.500 está compuesto por diferentes nodos con funciones específicas:
  - El usuario, el que solicita la información que hay en el directorio.
  - "Directory User Agent" o DUA, que traduce las órdenes del usuario al protocolo para la comunicación con el servidor.
  - "Directory System Agent" o DSA, que toma las órdenes del DUA, las procesa y devuelve una respuesta.
- El DUA y DSA se comunican usando el protocolo "Directory Access Protocol" o DAP.
- El DSA puede comunicarse con otros DSA de la red usando el protocolo "Directory System Protocol" o DSP.
- Los protocolos DAP y DSP se transmiten sobre TCP sobre el puerto 389 (by default).

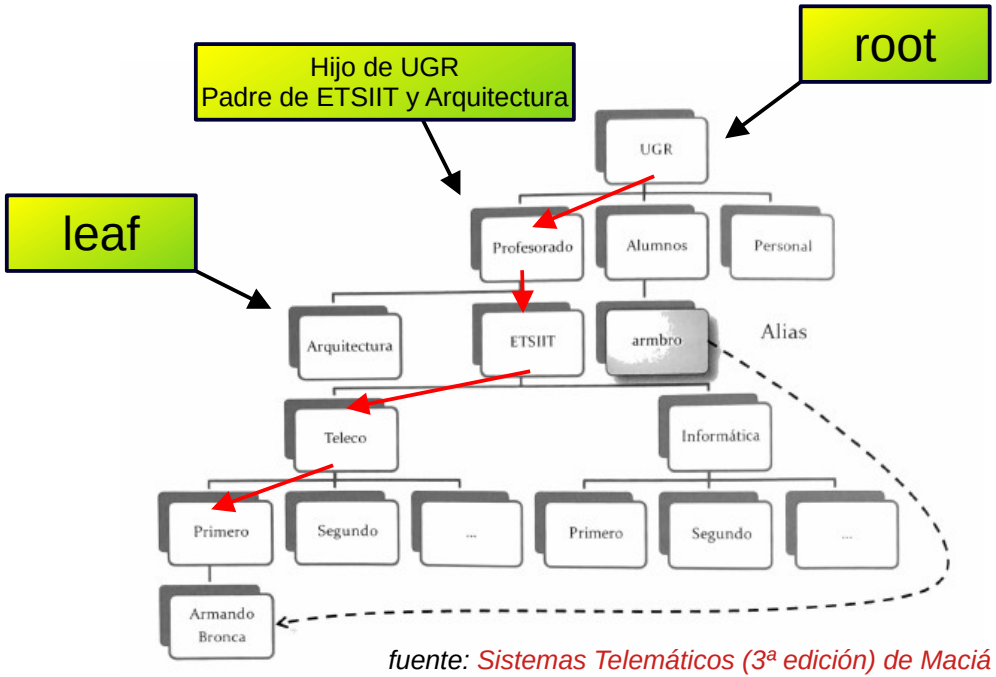
El servicio de directorio X.500

Organización de la información

- La información se organiza en forma de árbol invertido, que recibe el nombre de “Directory Information Tree” o DIT.
- A cada componente del árbol se le denomina entrada o nodo.
- El primer nodo del árbol recibe el nombre de “root” (raíz).
- De los nodos (“padres”) pueden colgar más nodos (“hijos”).
- Si un nodo no tiene hijos, es decir, no cuelga ningún otro nodo, recibirá el nombre de “leaf” (hoja).
- Cada nodo del árbol está identificado por un “Relative Distinguished Name” o RDN. No puede haber dos nodos padres o hijos con el mismo RDN al estar a la misma altura, pero si se encuetran a diferentes niveles, sí.
- Para identificar de forma única cada nodo en el árbol completo, usamos los “Distinguished Name” o DN.

El servicio de directorio X.500

Organización de la información



fuente: Sistemas Telemáticos (3ª edición) de Maciá et all.

- El DN está formado por la concatenación de los diferentes RDN de los nodos que se atraviesan hasta llegar al nodo en cuestión.

  El nodo con RDN “Primero” (que es hijo de Teleco), tendría el siguiente DN:

  DN = {UGR; Profesorado; ETSIIT; Teleco; Primero}

El servicio de directorio X.500

Organización de la información

- Existen varias categorías de nodos:
  - Objeto, representa objetos en los que se almacena información (ej. ordenadores, ficheros, etc.). Tienen atributos (ej. Numérico, texto) del objeto al que representan.
  - Alias, son nodos que proporcionan nombres alternativos a los objetos de un árbol (ej. abreviar un DN largo o situar un objeto en varias partes del árbol). Solo tiene un atributo que contiene el DN del objeto al que apuntan.
  - Subentradas, nodos que almacenan información relevante para los administradores del directorio, no visible para los usuarios, como número de accesos a un objeto, intentos fallidos de acceso al directorio, el tipo de entrada más consultada...

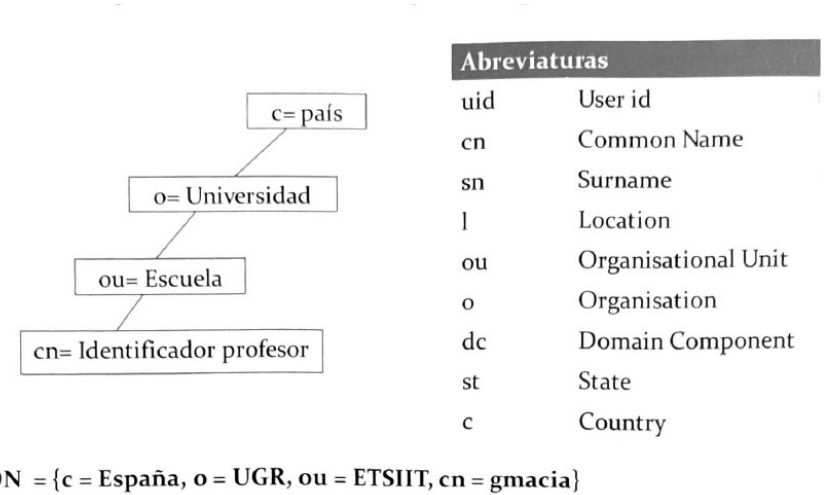
El servicio de directorio X.500

Organización de la información

- Destacamos los siguientes tipos de atributo en los servicios de directorio:
  - Atributos de “usuario”, son características introducidas, consultadas y modificadas por los usuarios del directorio (ej. el email de un usuario de un sistema)
  - Atributos “operacionales”, no son visibles para el usuario, pero sirven para monitorizar el directorio y su funcionamiento, como el número de veces que se ha accedido a la información contenido en un objeto.
  - Atributos “colectivos”, son atributos que tienen información que se aplica a un conjunto de nodos y el listado de esos nodos, como el número de accesos que se han producido a una lista de nodos en un determinado subnivel.

El servicio de directorio X.500

Organización de la información



Abreviaturas	
uid	User id
cn	Common Name
sn	Surname
l	Location
ou	Organisational Unit
o	Organisation
dc	Domain Component
st	State
c	Country

DN = {c = España, o = UGR, ou = ETSIIT, cn = gmacia}

Figura 3.4. *Estructura lógica de un árbol de directorio X.500. Abreviaturas comunes utilizadas para los objetos.*

fuente: Sistemas Telemáticos (3ª edición) de Maciá et all.

- Podemos distinguir distintos nodos de tipo objeto, las más comunes son las que salen en la tabla con sus respectivas abreviaturas.

El servicio de directorio X.500

Servicios ofrecidos por el directorio

- Leer un DN (leer los atributos de un nodo).
- Comparar un atributo de un DN con un valor concreto.
- Ver los hijos que tiene un nodo.
- Buscar un DN siguiendo unos criterios determinados fijados por el valor de uno o varios atributos.
- Añadir, modificar y borrar nodos (con sus atributos) de un árbol.
- Modificar el RDN de un nodo.

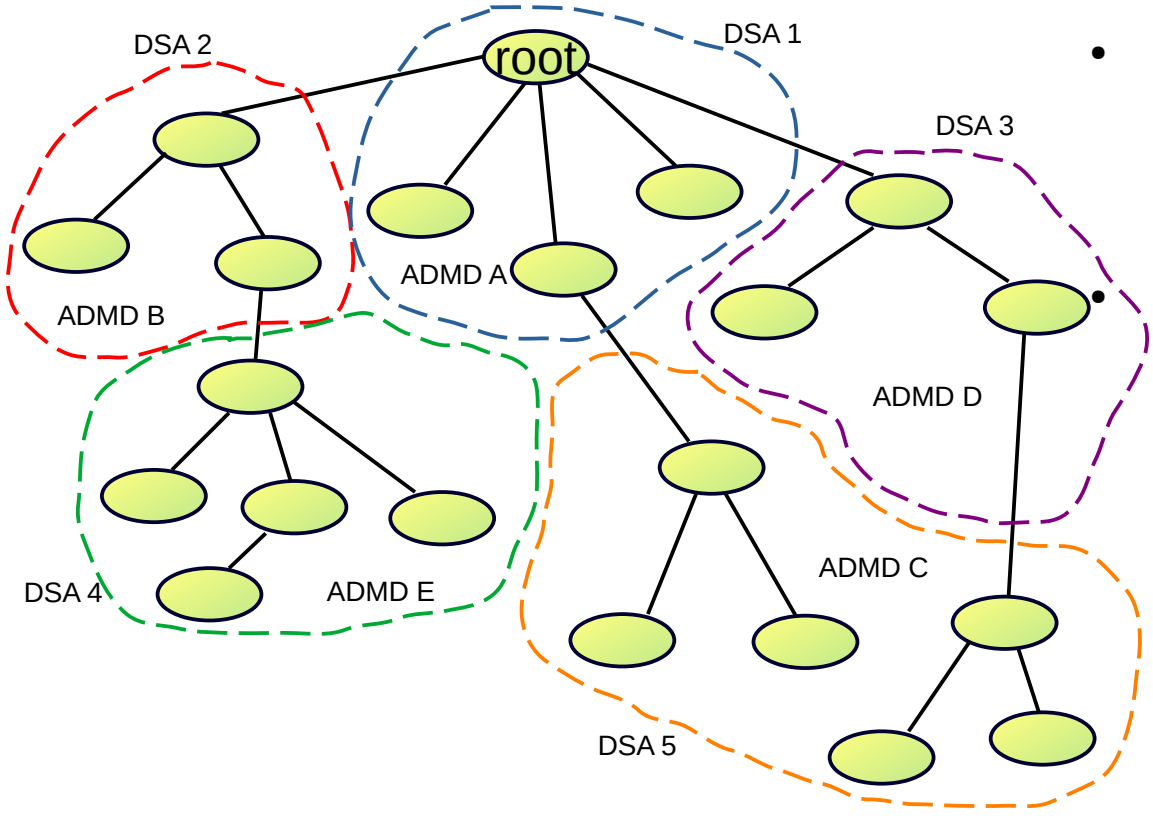
El servicio de directorio X.500

Distribución de la información

- La información contenida en el árbol del directoria se encuentra distribuida entre todos los agentes DSA del servicio.
- Podemos dividir el árbol en subárboles (contexto de nombramiento), con nodos y un conjunto de entradas subordinadas.
- Un DSA puede tener uno o varios contextos de nombramientos.
- El conjunto de contextos de nombramientos gestionado por un DSA se llama "Administrative Management Domain" o ADMD.
- El DN de la entrada raíz de un contexto de nombramiento será el prefijo de contexto, todas las entradas correspondientes a dicho contexto empiezan con ese prefijo.

El servicio de directorio X.500

Organización de la información



- Podemos distinguir distintos nodos de tipo objeto, las más comunes son las que salen en la tabla con sus respectivas abreviaturas.
- El ADMD A es el superior, los demás son contextos subordinados (ADMD B, ADMD C, ADMD D) y estos son superiores a otros contextos (ADMD E).

El servicio de directorio X.500

Acceso a la información distribuida

- Cada DSA tendrá información sobre los DSAs que contienen contextos subordinados y/o superiores.
- Las DSA tendrá una referencia subordinada inmediata para tal contexto, un atributo que relaciona un prefijo de contexto con el DSA que contiene a dicho contexto. [$DSA_{DESTINO}$, prefijo contexto].
- Las DSA también tendrán una referencia superior en las que se indica el DN del DSA que contiene información sobre contextos superiores a los administrados por el DSA subordinado.
- Cuando se hace una consulta a través de DAP, el DSA Comprueba si es responsable del contexto. Si no lo es, comprueba si es un contexto subordinado y deriva la petición al DSA subordinado, y en caso de que no, redireccionará la petición a un DSA superior.

El servicio de directorio X.500

Implementaciones del servicio X.500

- Hay varias implementaciones como CA Directory, Nexor Directory, entre otros, pero destaca una que incorpora un subconjunto de las funcionalidades DAP, llamado “Lightweight Directory Access Protocol” o LDAP.
- LDAP ha tenido bastante aceptación, aunque tenga una funcionalidad reducida del protocolo DAP, llegando a considerarse como una implementación de X.500.
- Los softwares que implementan LDAP son OpenLDAP, Active Directory, OpenDS, etc.

El servicio de nombres de dominio (DNS)

- Los sistemas que componen Internet usan el protocolo de nivel de red IP para comunicarse entre sí.
- Las direcciones IP identifican las interfaces de red conectadas en Internet.
- Una dirección IP es un número de 32 bits, habitualmente representado con 4 dígitos, cada uno de 8 bits (0-255) separados por un punto. (Ej: 192.168.159.24)
- Para no tener que acordarnos de las direcciones IP, usamos un “servicio de nombres de dominio” o DNS, que relaciona un nombre (dominio) con una dirección IP.

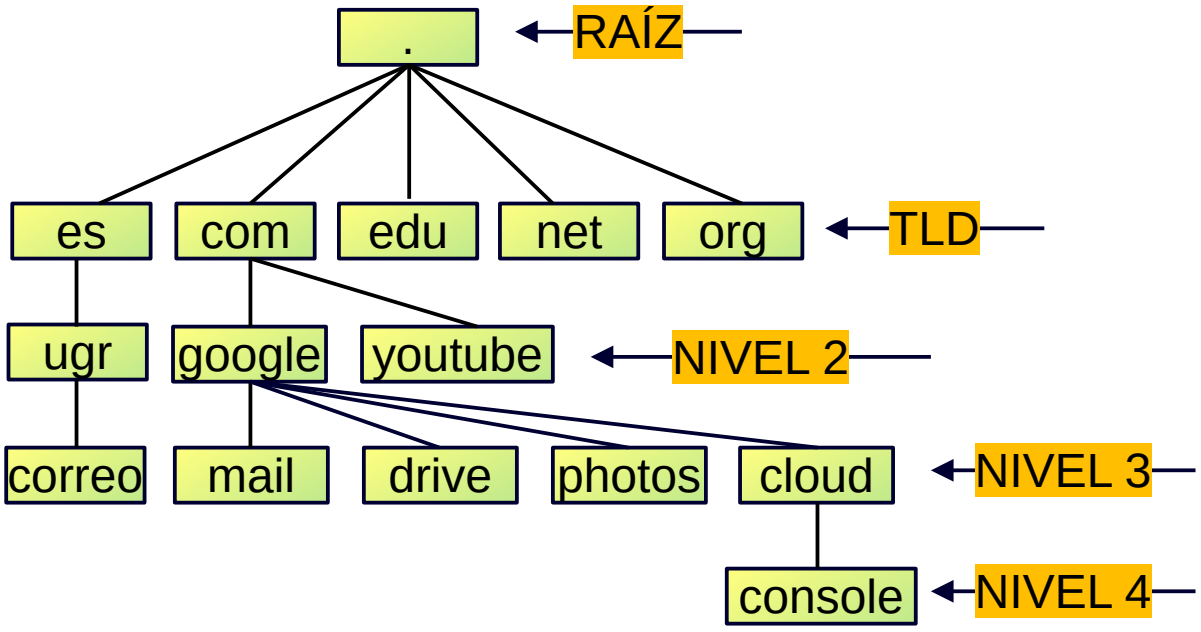
El servicio de nombres de dominio (DNS)

Los nombres de dominio

- Cada nombre de dominio debe ser único en todo Internet.
- Para evitar duplicados, tenemos una autoridad centralizada que controla la entrada de cualquier sistema en la red (asignando su dirección IP y un nombre de dominio), la "Internet Corporation for Assigned Names and Number" o ICANN a través de la "Internet Assigned Numbers Authority" o IANA.
- La gestión se reparte entre los "Network Information Center" o NIC, que son entidades autorizadas que se dedican a gestionar una parte de las numeraciones y los nombres de Internet.
- Para que se pueda hacer el reparto, los nombres de dominio se gestionan con una estructura jerárquica.
- Es como un árbol del servicio de directorio, de la raíz (.) descuelgan los "Top Level Domain" o TLD (es, com, edu, net, org...), y en los subniveles los subdominios.
- En España, el NIC gestiona el dominio ".es".

El servicio de nombres de dominio (DNS)

Los nombres de dominio



- Para referirnos a un nodo hoja, tendremos que concatenar todos los nodos por los que hay que pasar para llegar a él.

  Por ejemplo, para referirnos a la consola de la nube de Google, lo hacemos como:

  ”console.cloud.google.com.”

  El punto al final es el nodo raíz común para todos los dominios. Se asume su existencia aunque no se indique expresamente.

  En el navegador web introduciremos “console.cloud.google.com” y el punto lo añadirá automáticamente, aunque no se mostrará en la interfaz.

El servicio de nombres de dominio (DNS)

Componentes de servicio

- La gestión al ser descentralizada, cada servidor DNS almacena la información de los dominios que gestiona o “tiene autoridad”.
- Llamamos “zona DNS” a la parte delegada del espacio de nombres de dominios de Internet, gestionada por una entidad específica, que contiene la información técnica de un dominio (subdominios, dominios y sus IPs, etc).
- Habitualmente, cada zona DNS tiene un servidor autoridad primario (con una copia principal de los datos de la zona) y uno secundario (con una copia periódica del primario), por tanto, si cae el principal, siempre hay un “backup”.
- Los servidores DNS más importante son la de las TLD, que reciben el nombre de “servidores raíz”, y son identificados con una letra en el rango A-M y su denominación real es “LETRA.root-servers.net.
- Como hay muchos servidores DNS, se hace uso de la técnica de encaminamiento *anycast* que envía los mensajes DNS al destino más cercano al emisor del mismo.
- Existen 13 servidores raíz (privadas y públicas), con numerosas máquinas distribuidas geográficamente para garantizar la estabilidad y repartir la carga de tráfico.

El servicio de nombres de dominio (DNS)

Procedimiento de resolución

- Un programa de usuario necesita resolver la dirección IP de un dominio, por tanto, pide al sistema que lo haga.
- El sistema genera un mensaje de consulta, que envía al "resolutor local", un servidor DNS que se ejecuta en la propia máquina del usuario que revisa si puede resolver la dirección IP sin recurrir a otro servidor. Para ello, revisa si:
  - Tiene información local de DNS (en archivos de configuración, que contienen información sobre el dominio en cuestión).
  - Tiene información en caché (si la consulta se hizo recientemente, el resolutor guarda temporalmente la respuesta para no tener que estar solicitando continuamente la información a otros resolutores).
- Si no encuentra la información de forma local, para responder a la petición del programa, tendrá que recurrir al "servidor DNS primario" o "servidor DNS secundario" configurado en el sistema operativo (se puede personalizar), y el resolutor local pide resolver al *servidor DNS primario* (o secundario si el primero no está operativo) la dirección IP del dominio solicitado.
- El servidor DNS recibe la petición, comprueba si tiene autoridad sobre dicho dominio:
  - Si la tiene, envía la respuesta al resolutor local.
  - Si no, se deberá buscar al servidor con autoridad para dicho dominio para continuar el proceso de resolución.
- Para encontrar al servidor DNS con autoridad se pregunta a los servidores raíz, sobre el prefijo TLD del dominio solicitado.

El servicio de nombres de dominio (DNS)

Procedimiento de resolución

- La búsqueda de un servidor con autoridad para resolver la consulta se puede realizar de dos formas:
  - El servidor DNS primario se “busca la vida” para encontrar el servidor DNS que tiene autoridad, le pregunta y el propio servidor DNS primario responde al resolutor local con la respuesta del servidor con autoridad. (búsqueda recursiva)
  - El servidor DNS primario se “desentiente” y le “dice al resolutor local dónde se encuentra el servidor DNS al que tiene que preguntar” y el resolutor local luego le pregunta al servidor DNS indicado. (búsqueda iterativa)
- Ejemplo: Encontrar la IP del dominio nube.micd.es
  1) Se consulta al servidor raíz cuál es el servidor con autoridad sobre los dominios “.es”.
  2) Se consulta a ese servidor cuál es el servidor sobre los dominios “.micd.es”.
  3) Este proceso se repite de forma sucesiva hasta encontrar el servidor con autoridad sobre el dominio, que devolvería la respuesta, la dirección IP del dominio “nube.micd.es”.

El servicio de nombres de dominio (DNS)

Procedimiento de resolución

- Habitualmente las consultas DNS son almacenadas temporalmente en caché por casi todos los servidores, de esta forma, se responde con mayor velocidad a las consultas sucesivas.
- Los mensajes del protocolo DNS se transmiten a través del protocolo TCP (>512 bytes) o UDP (<512 bytes) a través del puerto 53.

El servicio de nombres de dominio (DNS)

Los registros DNS

- Los registros DNS se encuentran almacenados en las base de datos de los servidores DNS, y contienen la relación entre nombres y direcciones IP.
- Existen varios tipos de registros, pero todos poseen seis campos compunes:
  - Nombre del dominio (indica el nombre de dominio para el que se almacena info en el registro).
  - Tiempo de vida (el tiempo que se puede guardar un registro en caché, menos tiempo = más peticiones = si hay cambios, son instantáneos; más tiempo = menos peticiones = si hay cambios, tarda más).
  - Clase (indica el protocolo asociado al dominio, lo habitual es IN, de INternet protocol).
  - Longitud de la información (en 2 bytes indica el tamaño de la info que viaja en el campo de info).
  - Tipo de registro (define la función del registro):
    - A (Address), contiene la IP asociada al dominio.
    - NS (Name Server), contiene el nombre del servidor con autoridad sobre dicho dominio.
    - CNAME (Canonical Name), son alias del dominio al que apuntan.
    - SOA (Start of Authority), información sobre la zona sobre la que el servidor DNS tiene autoridad.
    - PTR (Pointer), es lo contrario del registro A, contiene el dominio asociado a la IP.
    - SRV (Service), registros que ayudan a localizar servicios en Internet. El nombre de dominio solo refiere a un servicio, pero el SRV nos permite indicar el puerto donde se encuentran otros servicios para la IP.
    - MX (Mail Exchange), indican la IP del servidor de correo que corresponde a dicho dominio.

El servicio de nombres de dominio (DNS)

Reparto de carga entre máquinas o servidores DNS

- Con el DNS podemos balancear la cantidad de tráfico que se dirige a una red, por ejemplo, un nombre de dominio puede tener asociadas varias direcciones IPs y por tanto, cuando el host consulta el dominio elegirá aleatoriamente la dirección IP al que enviará el tráfico.
- Con registros tipo NS podemos hacer un reparto de carga entre varios servidores DNS también.

El servicio de nombres de dominio (DNS)

Estructura de los mensajes

- Los mensajes que se transmiten en las consultas y respuestas en el protocolo DNS están definidos por la RFC1035.
- Los mensajes tienen una cabecera de longitud fija de 12 bytes que incluyen:
  - ID de consulta (valor aleatorio, con el que luego se asociará una respuesta).
  - Parámetros de consulta:
    - Tipo de mensaje (si es consulta o respuesta).
    - Respuesta con/sin autoridad (indica si el servidor que responde tiene autoridad, si la info proviene de la caché del servidor DNS puede que sea respuesta sin autoridad).
    - Recursividad deseada (si el servidor consultado debe usar búsqueda recursiva).
    - Código de respuesta (el servidor incluye información sobre la respuesta, si hay error, si el tipo de consulta no está soportada, si el dominio no existe...).
  - Número de solicitudes / respuestas / registros en la sección de autoridad / registros en la sección de registros adicionales.
  - Cuerpo de mensaje (tamaño variable), con algunos de los siguientes campos:
    - Solicitudes (indican las solicitudes incluídas en la consulta, compuesta por el nombre de dominio, clase y tipo de registro solicitado para dicho nombre).
    - Respuesta (donde el servidor incluye las respuestas de todos los registros solicitados).
    - Sección de autoridad (listado de registros NS en el que se indican todos los servidores con autoridad sobre el dominio consultado).
    - Registros adicionales (información adicional, como direcciones tipo A para los nombres de los servidores DNS indicados en los registros NS de la sección de autoridad).

El servicio de nombres de dominio (DNS)

Ejemplo de configuración de un servidor.

```
labredes.pri. 94400 IN SOA eihal.labredes.pri.   admin.labredes.pri.(
                       2008042401      ; Serial
                       28800           ; Refresh (seconds)
                       14400           ; Retry (seconds)
                       360000          ; Expire (seconds)
                       86400 )         ; Minimum TTL(seconds)

labredes.pri.             IN NS    eihal.labredes.pri.
labredes.pri.             IN MX    10 mailserver.labredes.pri.
_sip._udp.labredes.pri.   IN SRV   10 1 5056 voipserver.labredes.pri.
controler.labredes.pri.   IN CNAME eihal.labredes.pri.

eihal.labredes.pri.       IN A     172.18.140.21
ei140146.labredes.pri.    IN A     172.18.140.146
mailserver.labredes.pri.  IN A     172.18.140.148
voipserver.labredes.pri.  IN A     172.18.140.149
```

fuente: Sistemas Telemáticos (3ª edición) de Maciá et all.

- Ejemplo de configuración de un servidor DNS implementado con BIND.
- Tenemos un registro SOA que indica que:
  - este servidor tiene autoridad sobre la zona “labredes.pri.”,
  - el tiempo de vida es 94400 por defecto para este registro,
  - que el protocolo asociado al dominio es de tipo IN,
  - que el servidor DNS primario de esta zona es “eihal.labredes.pri.”,
  - que el correo electrónico del administrador es “admin.labredes.pri.” o “admin@labredes.pri”,
  - el *serial* es un identificador que ayuda a los servidores secundarios saber si han cambiado los datos (última fecha de modificación “2008-04-24” y el número de revisión “01” que va incrementando),
  - *refresh* indica el tiempo que tienen que esperar los servidores secundarios antes de verificar si hay cambios en el principal,
  - *retry* indica al secundario cuanto tiempo debe de esperar para reintentar conectarse al principal si este no responde,
  - *expire* indica al secundario cuando debe dejar de responder si no puede contactar al principal,
  - y *minimum TTL* indica el tiempo durante el cual se pueden almacenar en caché los registros de esta zona.

El servicio de nombres de dominio (DNS)

Ejemplo de configuración de un servidor.

```
labredes.pri. 94400 IN SOA eihal.labredes.pri.   admin.labredes.pri.(
                        2008042401      ; Serial
                        28800           ; Refresh (seconds)
                        14400           ; Retry (seconds)
                        360000          ; Expire (seconds)
                        86400 )         ; Minimum TTL(seconds)

labredes.pri.             IN NS    eihal.labredes.pri.
labredes.pri.             IN MX    10 mailserver.labredes.pri.
_sip._udp.labredes.pri.   IN SRV   10 1 5056 voipserver.labredes.pri.
controler.labredes.pri.   IN CNAME eihal.labredes.pri.

eihal.labredes.pri.       IN A     172.18.140.21
ei140146.labredes.pri.    IN A     172.18.140.146
mailserver.labredes.pri.  IN A     172.18.140.148
voipserver.labredes.pri.  IN A     172.18.140.149
```

fuente: Sistemas Telemáticos (3ª edición) de Maciá et all.

- Después del registro SOA encontramos uno de tipo NS, que indica que el dominio labredes.pri tiene como servidor con autoridad "eihal.labredes.pri.".
- Luego aparece un registro de tipo MX que indica que el servidor de correo para todas las direcciones con formato xxx@labredes.pri es "mailserver.labredes.pri.".
  - El número 10 indica prioridad del registro. Si hay varios registros MX, se tonaría el de mayor prioridad, menor valor), si todos tienen la misma prioridad, se haría un reparto de carga.
- Luego encontramos un registro de tipo SRV que indica que el servicio (de tipo SIP) apuntado por el nombre "_sip.udp.labredes.pri" se encuentra en el servidor "voipserver.labredes.pri." en el puerto 5056, el número 10 representa la prioridad y el 1 representa la probabilidad (valor de 0 a 65535) de que se tome esa entrada en caso de haber más registros con la misma prioridad.
- El registro CNAME indica que el servidor "eihal.labredes.pri." tiene de alias "controler.labredes.pri.".
- Luego encontramos los registros de tipo A en las que se encuentran las direcciones IP asociadas a los diferentes máquinas declaradas dentro del dominio.

  Ej: ei140146.labredes.pri. tiene IP 172.18.140.146.

Soluciones para la seguridad

Servicios de seguridad + Amenazas y ataques a la seguridad

- Necesitamos garantizar la seguridad de las comunicaciones (ej: métodos fiables para autentificar a los usuarios en una red, evitar que alguien pueda suplantar o sustituir información en las comunicaciones, garantizar la integridad de los datos transmitidos, etc.).
- Los distintos acontecimientos (eventos) que se producen en una red, pueden ser *normales* (si responden al patrón de comportamiento normal del tráfico en dicha red o de la acción con respecto al servicio considerado) o *anómalos* (todo lo contrario).
- Los eventos anómalos son los que nos interesan mitigar, son las amenazas a la seguridad de la red.
- Pero una amenaza de seguridad es distinto de un ataque a la seguridad.
- Consideramos ataque a la seguridad a la red cuando este evento altera el funcionamiento normal del servicio o la red.

Soluciones para la seguridad

Servicios de seguridad + Amenazas y ataques a la seguridad

- Podemos distinguir varios tipos de ataque, en función de cómo actúa sobre el flujo de la información:
  - DoS (Denial of Service) (interrupción del flujo de información, un atacante puede reventar un servidor a peticiones para sobrecargarlo y evitando ofrecer servicio a los clientes).
  - Sniffing (intercepción de las comunicaciones)
  - MitM (modificación de la información intercambiada entre origen y destino, el atacante recibe la info del origen, la modifica y las envía al destino simulando ser el origen).
  - Replay Attack (creación de mensajes falsos dirigidos al destino, ej: atacante ve una orden de transferencia de 10€ a un banco, recrea la orden y la envía varias veces para arruinar a la víctima).

Soluciones para la seguridad

Servicios básicos de seguridad

- Son los servicios que hay en una red de comunicación que ofrecen seguridad a las comunicaciones.
- Resaltamos los servicios de:
  - Autenticación (identificar y verificar a cada uno de los participantes).
  - Confidencialidad (si alguien “pincha” la comunicación “no se entera de ná’”).
  - No repudio (garantiza que el emisor no pueda decir que no ha enviado cierta información).
  - Disponibilidad (garantiza que un servicio estará accesible y plenamente funcional de la forma prevista).
  - Integridad (garantiza que el receptor pueda verificar si el mensaje recibido es exactamente igual al enviado por el emisor).
  - Privacidad (garantiza que los datos relacionados con los intervinientes en una comunicación no puede ser obtenidos por terceras partes).

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Implementar arquitecturas de seguridad.
    - Mecanismos que se introducen en la propia arquitectura de la red.
    - Algunos son:
      - "Intrusion Detection System" o IDS. Consiste en situar elementos en la red para monitorizar el comportamiento de sus componentes para detectar si se están produciendo actividades maliciosas o no. Destacan los antivirus (monitorizan la actividad de los *hosts*, para detectar la presencia de *malware*), software que detectan tráfico de red malicioso, actividades sospechosas de programas... Funcionan de dos formas:
        - El sistema conoce los patrones de ataque de antemano, los detecta y revienta el ataque. (IDS basado en firmas). Útil si los ataques son conocidos, inútil en casos de ataques no reportados "zero-day attacks".
        - El sistema sabe cómo funciona el sistema con normalidad y cualquier cosa fuera de lo común lo revienta. (IDS basado en anomalías). Útil en detectar ataques no conocidos, al precio de *falsos positivos* de vez en cuando.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Implementar arquitecturas de seguridad.
    - Algunos son:
      - Sistemas de control de acceso, diseñado para restringir el acceso a determinados recursos de una red en función de unas políticas de seguridad previamente establecidas. Se decide lo que se quiere proteger, las amenazas que pueden sufrir, y los mínimos accesos necesarios para poder prestar los servicios que la red ofrece. Luego se implementa una política de acceso con determinadas herramientas.
        - Destacan los cortafuegos, equipos de control de tráfico entrante y saliente, una "aduana para las comunicaciones", siguiendo unos criterios establecidos en base a: IP origen/destino, puertos origen/destino, tipo de mensaje, etc.
          - Un caso especial, el proxy, que analiza el contenido de los mensajes a nivel de aplicación para permitir o restringir su paso.
      - Sistemas de autenticación, identifican y verifican a usuarios. Muchas veces necesario para implantar sistemas de control de acceso para determinar cuales son los usuarios que están tratando de acceder a los recursos de la red.

        Los mecanismos de autenticación puede ser mediante códigos, certificados digitales, biometría, etc.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Para prestar servicios de seguridad, se han desarrollado tecnologías fundamentalmente basadas en la criptografía.
    - La criptografía comprende las técnicas que permiten cifrar y proteger los mensajes transmitidos de la intercepción por parte de intrusos.
    - Existen varias técnicas, pero los más relevantes en el sector son:
      - Cifrado simétrico, se utiliza una única clave tanto para cifrar como para descifrar la información (la clave ha sido previamente compartida entre el emisor y el receptor a través de un canal seguro).
      - Cifrado asimétrico, el cifrado se hace con una clave y el descifrado con una clave diferente.
        - Destaca la criptografía de clave pública y privada: cada interlocutor tiene una pareja de claves (una privada, que solo la conocerá el interlocutor, y otra pública, que podrán conocer el resto de posibles interlocutores).
        - Un mensaje cifrado con clave pública solo puede ser descifrado por su clave privada asociada.
        - Un mensaje cifrado con una clave privada solo puede ser descifrado por la clave pública asociada.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Usar el sistema de cifrado asimétrico conlleva necesitar más capacidad de cómputo, por tanto, este sistema se suele usar en los escenarios donde es estrictamente necesario. El resto de casos, se usa el cifrado simétrico, permitiendo reducir la latencia en las comunicaciones y el gasto de energía.
    - Algunas aplicaciones de la criptografía son:
      - Cifrado de la información, suele ser el principal objetivo de las aplicaciones criptográficas.

        Se puede usar primero una técnica de cifrado simétrico, con algoritmos como el de "*Diffie-Hellman*" podemos intercambiar de forma segura la clave única de cifrado a traves de un canal inseguro, entre dos partes que no han tenido contacto previo.

        También se puede realizar el cifrado mediante técnicas de cifrado asimétrico, el emisor poseera la clave pública del receptor, que usará para cifrar la información, y solo el receptor podrá descifrarla, puesto que es el único que posee su clave cifrada.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Algunas aplicaciones de la criptografía son:
      - Firma digital, mecanismo con el que el receptor puede estar seguro de que: el emisor es quien dice ser (autenticación y no repudio) y ningún intruso haya podido modificar los datos (integridad).

        Para generar una firma digital:

        1) Se genera un código resumen o *hash* para los datos, son códigos que toman de entrada un conjunto de elementos de longitud variable y da un conjunto finito de resultados (normalmente cadenas de tamaño fijo), los algoritmos más utilizados son MD5 y SHA.
        2) Se cifra el código hash con la clave privada del emisor, se crea la firma digital.
        3) Se adjunta la firma digital a los datos y también un certificado digital (lo vemos más adelante) conteniendo la clave pública del emisor.
        4) Se envía toda esta información al destino.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Algunas aplicaciones de la criptografía son:
      - Firma digital

        Para verificar la firma digital:

        1) Se separan los datos recibidos de la firma digital y el certificado.
        2) A los datos se les calcula el *hash*, obteniendo el código que supuestamente firmó el emisor.
        3) Con la clave pública del emisor contenida en el certificado se descifra la firma digital, obteniendo el *hash* calculado por el emisor.
        4) Si coinciden ambos *hashes*, la firma es correcta.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Algunas aplicaciones de la criptografía son:
      - Certificados digitales, son documentos digitales que contiene claves correspondientes a un individuo o una entidad, estas claves pueden ser la clave privada, pública o ambas.

        En el proceso de firma digital, el receptor utiliza la clave pública contenida en el certificado digital adjuntado. Pero, solo podrá comprobar si ese certificado es auténtico si el certificado ha sido emitido por una *autoridad de certificación*, que tiene la finalidad de garantizar que dicho individuo es realmente el poseedor de las claves contenidas en el certificado.

        El certificado digital tendrá también la clave pública de la autoridad certificadora, que usará para verificar que la clave pública del individuo no ha sido alterado.

        Pero para garantizar que la clave pública de la autoridad certificadora es genuina, tendremos que recurrir al uso de la clave pública de una autoridad certificadora superior que nos garantice que la autoridad certificadora es real.

        Y de esta forma, damos con la cadena de certificación hasta llegar a los certificados raíz, los cuales no estarán firmados.

Soluciones para la seguridad

Soluciones para la seguridad + Arquitecturas de seguridad + Tecnologías de seguridad

- Para implementar servicios de seguridad, dos estrategias:
  - Tecnologías de seguridad
    - Algunas aplicaciones de la criptografía son:
      - Certificados digitales

        El estándar más extendido es el X.509, que define la información contenida en los certificados y los métodos de verificación de la validez.

        Un certificado X.509 contiene habitualmente
        - la versión del certificado, el número de serie,
        - el algoritmo con el que se ha firmado el certificado por parte de la autoridad certificadora,
        - los datos de la autoridad certificadora (issuer),
        - fechas de validez del certificado (no antes de / no después de),
        - datos del sujeto,
        - la clave pública del sujeto,
        - y opcionalmente, la clave privada del sujeto (suelen tener una extensión .pfx o .p12 y habitualmente protegida por contraseña) y una firma generada por la autoridad emisora del certificado.

Sistemas Telemáticos

resumido por Alexandru Theodor Muntenas²

Capítulo 3
Servicios Transversales