Administración de redes Windows.

Caso práctico

Juan, empleado de la empresa BK Programación, está trabajando con su Windows 10 recién instalado, y mientras espera a que se actualice automáticamente desde Internet, está reflexionando sobre lo fácil que ha sido hacer la instalación y sobre todo que el equipo esta conectado a una red y él no ha tenido que configurar prácticamente nada. Sin embargo, han debido de establecerse una serie de configuraciones internas que a él le gustaría conocer por si necesita manejarlas en un futuro.

En esta unidad se va a configurar la red en Windows, para ello se configura una red con 2 máquinas virtuales y se compartirán recursos. En la segunda parte de la unidad se profundizará en los distintos servicios de redes, para instalar algunos de ellos en Windows.

En los sistemas operativos Windows hay dos formas principales de trabajar en red en una empresa: grupo de trabajo y dominio.

En los sistemas cliente Windows 7, Windows 8 y Windows 10, estaba también grupo de hogar, que ha desaparecido en la actualización 1803 de Windows 10 (marzo del 2018). Grupo de hogar como dice su nombre está orientado a hogares domésticos, y por ese motivo no se va a tratar en esta unidad.

1.- Configuración de red en Microsoft Windows.

Caso práctico

Juan se plantea cómo se ha configurado el ordenador de forma automática, y que apenas ha tenido que intervenir en la configuración de la red. Está pensando que debería conocer más sobre la configuración de redes en Windows, ya que puede serle útil en algún momento y además, en algunos casos, puede necesitar no sólo quedarse con la configuración por defecto, si no ir más allá. Por eso va a repasar la administración de la red dentro del sistema operativo.

Administrar una red consiste en aplicar una serie de técnicas que la mantengan siempre operativa, de forma óptima y segura, para gestionar el uso eficiente de sus recursos y garantizar la calidad de los servicios que ofrece.

1.1.- Introducción.

Grupo de trabajo y dominio.

Se explica la diferencia de trabajar en grupo de trabajo o en un dominio.

Grupo de trabajo *(*Workgroups*)*.
Por defecto, los ordenadores que forman parte del mismo grupo aparecen juntos cuando se exploran en “Mis sitios de Red” o en “Red” en el explorador de Windows. La administración de cada ordenador es local e independiente. Un ordenador, exporta o comparte recursos concretos, y el usuario remoto tiene que disponer de una cuenta y permisos suficientes. Esta es la forma que se va a trabajar en esta unidad. Vamos a tener 2 equipos, cada uno con sus usuarios y password. También recibe tradicionalmente el nombre de red punto a punto (peer to peer) en la que cada usuario, para conectarse a cualquier equipo tiene que tener una cuenta de ese equipo.

Imaginemos, una empresa con 10 ordenadores y sus trabajadores, si queremos que un trabajador, se pueda poner en cualquier puesto, tendremos que crear una cuenta para ese trabajador en cada equipo. Esta organización, según se hace la empresa grande se hace complicada.

Dominio. Es la forma habitual de trabajar en una empresa grande, hay 1 ordenador principal con sistema operativo Windows Server, en el que se instala un controlador de dominio. Después, se introduce al resto de los equipos en ese dominio. Las cuentas de usuarios que se creen en el controlador, sirven para iniciar sesión en cualquier equipo del dominio.
En el ejemplo anterior, el trabajador podrá iniciar sesión en cualquier equipo, solo con tener una cuenta creada en el equipo controlador de dominio.

En el **controlador de dominio** se centraliza las cuentas de usuarios, grupos, equipos, directivas de seguridad, recursos compartidos.

No es necesario que los ordenadores que forman un dominio se encuentren físicamente cercanos, pueden estar en distintas sedes geográficas. Para crear un dominio, es necesario que al menos uno de los servidores Windows Server de la red se convierta en un DC. Para ello, se debe ejecutar un asistente denominado **dcpromo**.
Los contenidos de dominios no forman parte de la asignatura de Sistemas Informáticos, por lo que en esta unidad sólo se va a trabajar en grupo de trabajo.

Para saber más

Página de Microsoft que explica las diferentes formas de organizar equipos en las redes con Windows 10.

¿Diferencias entre un dominio, un grupo de trabajo y un grupo en el hogar?

1.2.- Ejercicio configuración Red. Instalación de 2 máquinas Windows en Red en grupo de trabajo.

Lo primero que se va a realizar es configurar 2 máquinas virtuales Microsoft Windows en la misma red. Este será el primer ejercicio de la tarea de la unidad.

Paso 1. Clonar una máquina Windows

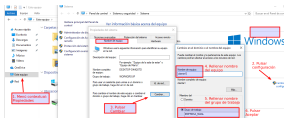
- Clonar con VirtualBox la máquina virtual Windows10Sistemas utilizada en las unidades anteriores.
- Al clonar, tener especial cuidado en marcar “Reiniciar MAC”, sino lo hacemos las 2 tarjetas de red tendrían la misma dirección física, y tal como se dijo en la unidad 8, toda tarjeta de red tiene una dirección única en el mundo, por lo que no podrá funcionar la red.

Paso 2. Configurar nombres de las máquinas y grupo de trabajo

Las 2 máquinas se van a introducir en el mismo grupo de trabajo.
Para ello, seguir los pasos siguientes (según imagen):

- Ir al Menú contextual de Equipo y pulsar Propiedades.
- Pulsar en “Cambiar configuración” y seleccionar Solapa “Nombre de equipo”
- Pulsar el botón “Cambiar”.
- En esta última ventana que aparece, se configura Nombre de Equipo y Nombre del Grupo de Trabajo.
- Poner a las dos máquinas el nombre: cliente1 y cliente2
- Introducir a ambas máquinas en el mismo grupo de trabajo: “Empresa_InicialesApellidoNombreAlumno”

Una vez rellenos los datos, pulsar Aceptar. Al pulsar Aceptar, hay que reiniciar la máquina para que los cambios tengan efecto.



Miguel Angel García Lara (CC BY-NC-SA)

Paso 3. Crear 2 usuarios, uno administrador y otro normal en cada máquina.

Crear en cada máquina dos usuarios, uno administrador y otro perteneciente al grupo usuario. Utilizar los nombres y password especificados en las tablas:

Usuarios en cliente1

Nombre usuario	Password	Único grupo al que pertenecen
Supervisor	Administradores	empleado1
super1	Empleado	Usuarios

Usuarios en cliente2

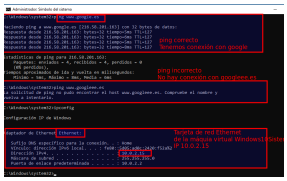
Nombre usuario	Password	Único grupo al que pertenecen
Supervisor	Administradores	empleado2
super2	Empleado	Usuarios

Paso 4. Configuración de la red por defecto en VirtualBox

Por defecto, VirtualBox tiene configuradas las máquinas en NAT, de esta forma salen a Internet, pues la máquina anfitrión realiza puente con la huésped. Para comprobarlo y entenderlo se realizan los pasos siguientes:

- Comprobar que ambas máquinas tienen Internet. Para ello, ejecutar en terminal: ping www.elpais.es
  Se envían paquetes a la página de El Pais y se devuelve el tiempo de respuesta.
- Comprobar que ambas máquinas tienen la misma dirección IP en la tarjeta de red Ethernet. Para ello, ejecutar **ipconfig**. Sin embargo, se conectan a Internet sin problemas estando las dos máquinas encendidas (lo que demuestra que no están en la misma red, porque dentro de la misma red dos máquinas no pueden tener la misma IP)

En la imagen siguiente se muestra la ejecución de ambos comandos.



Paso 5. Configuración de los 2 equipos en red interna en VirtualBox.

Apagar las 2 máquinas y en VirtualBox, en Configuración / Red cambiar “NAT” a “Red interna”.
Esto equivale a conectar las 2 máquinas físicamente en el mismo switch. De esta forma, ambas máquinas están en la misma red física, pero falta el direccionamiento IP para que se puedan conectar entre ellas.

Paso 6. Comprobar que ahora no hay conexión a Internet.

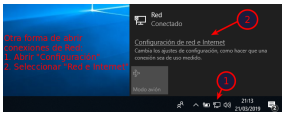
Ahora las máquinas ya no salen a Internet, ni siquiera tienen red local pues no tienen asignada IP. Al ejecutar los mismos comandos que en paso 4 se observan las diferencias siguientes: el ping no responde (los paquetes se pierden) y en ipconfig, se ve la conexión de red desactivada (sin dirección IP)

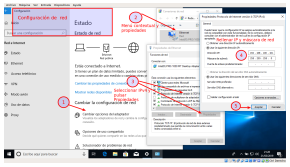
Paso 7. Configurar la red local, asignando dirección IP estática a ambas máquinas.

En este paso se configuran las direcciones IP en ambas máquinas. Las direcciones a configurar son las de la tabla. Para la configuración, seguir las capturas.

Direcciones de red

Nombre máquina	IP	Máscara de red
cliente1	192.168.100.101	255.255.255.0
cliente2	192.168.100.102	255.255.255.0





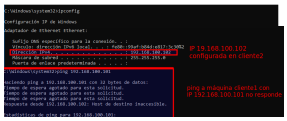
Según direccionamiento IP estudiado en la unidad 8, estamos configurando ambas máquinas en la misma red con dirección 192.168.100.0/24 (red de clase C con máscara de 24 bits)

No configuramos puerta de enlace ni DNS. Vamos a tener las 2 máquinas en la misma red local, pero no van a salir a Internet. Para salir a Internet, tendríamos que tener un router que conecte nuestra red con Internet. La dirección interna del router sería la puerta de enlace. El servidor DNS es un equipo de Internet que se utiliza para la resolución de nombres (direcciones web) en IP, como de momento no salimos a Internet no nos hace falta.

Paso 8. Ejecutar ipconfig para comprobar IP asignadas.

Vamos a comprobar la conexión a la otra máquina con ping.
Para ello, en cliente 1 ejecutamos ping 192.168.100.102 y en cliente 2 ejecutamos ping 192.168.100.101.
Resulta que no responden los ping, pues por defecto, el firewall de Windows no admite ping. Hay que bloquear el firewall en las máquinas o crear una regla de exclusión.

En la imagen, se ejecuta en la máquina cliente2 el comando ipconfig, donde se ve la IP bien configurada, pero sin embargo no responde el ping a la máquina cliente1.



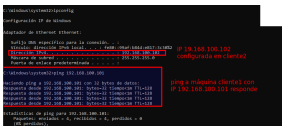
Crear reglas de exclusión en el firewall para permitir ping en las máquinas

Pasos:

En máquina cliente1, abrir “Windows Defender Firewall de Windows con seguridad avanzada:

- Seleccionar “Reglas de entrada” y a la derecha en “Nueva Regla”
- Seleccionar “Personalizada” y pulsar Siguiente.
- Seleccionar “Todos los programas” y pulsar Siguiente.
- Seleccionar “Tipo de protocolo ICMPv4” y pulsar en Configuración de ICMP “Personalizada”
- Pulsar en “Tipos de ICMP específicos” y activar “Petición de eco”. Pulsar en Aceptar y Siguiente varias veces, hasta que se solicita el nombre de la regla. Rellenar como nombre “Permitir ping”

Una vez añadida la regla en la máquina “cliente1”, cliente2 ejecuta ping 192.168.100.101 con respuesta satisfactoria.



Por último, crear la regla en la máquina cliente2 y comprobar ping contrario.

2.- Compartir recursos en la Red.

Caso práctico

Un tema que le preocupa a Juan es cómo compartir a través de la red los recursos de equipos conectados.

Porque poner todo a disposición de todos, que sería lo más fácil, puede suponer problemas de seguridad en la red y una mala gestión de los recursos. Así que será necesario, establecer una política de gestión de permisos en torno a los recursos compartidos.

En cuanto a la configuración que Windows hace en el equipo para acceder a la red, se pregunta:

¿Cuánta libertad tienen los otros usuarios en otros equipos de la red para llegar a mi ordenador y tomar lo que necesiten?

¿Qué se ha quedado a la vista de los demás para que puedan utilizarlo?

¿Qué puedo yo utilizar de los equipos de los demás?

Cuando hablamos de recursos compartidos en red estamos tratando de carpetas, de ficheros y de dispositivos que se hayan en un equipo, pero que de alguna manera, se ponen a disposición de todos aquellos que se conectan a él a través de una red, o sólo a disposición de algunos de ellos dependiendo de la forma de compartirlos. Y todo ello haciéndose extensivo a cada uno de los equipos que forman parte de dicha red.

Para hacer que un recurso sea compartido hay que ponerlo accesible a través la red, y una vez que esta compartido, los usuarios, con los permisos adecuados, podrán acceder a su contenido ya sean aplicaciones o datos, o utilizarlo remotamente si se trata de un dispositivo, tal como una impresora.

En un entorno de red es preciso definir permisos de acceso y privilegios de uso sobre los recursos que se comparten, para mantener cierto nivel de seguridad y asegurar que lo compartido sólo pueda ser utilizado por quien tenga derecho, y bajo las condiciones de uso fijadas sobre el recurso, mientras que se bloquea el acceso a usuarios no autorizados.

2.1.- Solapa Compartir.

Si pulsamos menú contextual en una carpeta y propiedades, tenemos las solapas Compartir y Seguridad. En la unidad 4, vimos la **solapa "Seguridad"** donde se dijo que representaba la seguridad local en el equipo, conocidos como **permisos NTFS.**
En este libro se estudia la **solapa "Compartir"**, que sirve para configurar los permisos cuando acedemos a un equipo **desde la red**.

Se comienza con varias particularidades cuando se comparte:

- Se pueden compartir carpetas e impresoras. No se pueden compartir archivos de forma individual. Se llama recurso a la carpeta o impresora compartida.
- Cuando se comparte un recurso, se le pone un nombre que puede ser distinto al nombre de la carpeta o impresora.
- Una carpeta compartida se suele distinguir en el Explorador de Windows por un icono de una mano que sostiene una carpeta.
- Cuando se comparte una carpeta, se concede un permiso de lectura al grupo Todos de forma predeterminada. Se pueden cambiar los permisos por defecto y agregar o eliminar a usuarios y grupos.
- Una carpeta compartida, no se puede mover, si se mueve deja de ser compartido el recurso.
- Un recurso tiene una ruta UNC, esta ruta está formada por \\NombreEquipo\NombreRecurso
- Esta ruta UNC es una forma rápida de acceder al recurso, pues se puede escribir directamente en el explorador de Windows o en Ejecutar.
- Se puede ocultar un recurso, para ello se añade un signo de dólar ($) al final del nombre del recurso. De esta forma no se ve en el explorador de Windows cuando se explora la red, aunque si se tiene acceso a través de su ruta UNC \\NombreEquipo\NombreRecurso$
- Límite de usuarios: Indica el número de usuarios que pueden conectarse simultáneamente a la carpeta compartida. Por defecto son 20, que es el máximo permitido en Windows 10.

Tipos de permisos al compartir

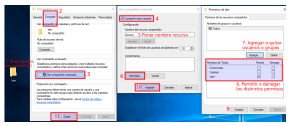
Cuando se comparte un recurso, se puede compartir a usuarios o grupos y existen 3 tipos de permisos:
Lectura, cambio y control total

- El permiso de lectura permite:
  - Ver los nombres de archivos y de subcarpetas
  - Recorrer las subcarpetas
  - Ver los datos de los archivos
  - Ejecutar archivos de programa
- El permiso de cambio proporciona todos los permisos de lectura, así como:
  - Agregar archivos y subcarpetas
  - Cambiar datos en archivos
  - Eliminar subcarpetas y archivos
- El permiso de control total proporciona todos los permisos de lectura y de cambio, así como:
  - Cambiar permisos
  - Tomar posesión

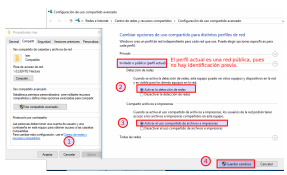
¿Cómo compartir un recurso?

La forma más habitual de compartir un recurso es mediante el Explorador de Windows, pulsando en menú contextual en propiedades / Solapa Compartir / Uso compartido avanzado.
La solapa Compartir funciona de una forma muy similar a la solapa Seguridad.

En la imagen se muestra como se comparte una carpeta llamada "Leer" con el nombre de recurso "Lectura" y a "Todos" los usuarios con el permiso Lectura.



La primera vez que se comparten recursos, es necesario "Activar detección de redes y uso compartido de archivos". Si no se activa esta opción, no se podrá acceder a los equipos en la red, aunque se hayan compartido recursos.

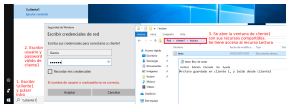


Como acceder a las carpetas compartidas en otro equipo

Desde un ordenador de la red, se puede aceder a un recurso de otro ordenador de las formas siguientes:

- Ejecutando directamente la ruta UNC: \\nombreEquipo\nombreRecurso
- A través del explorador de Windows, pulsando en Red.

Se muestra una captura utilizando ruta UNC con acceso desde cliente2 a cliente1. En cliente2 se ha iniciado sesión con supervisor, al acceder a \\cliente1 y cliente1, pregunta una identificación válida. Para realizar la conexión, hay que utilizar los datos de un usuario y password de cliente1.
Es importante observar que si supervisor tuviera el mismo password en los 2 equipos, se habría accedido directamente. Por ese motivo, se han configurado distintas password para cada máquina, para mayor comprensión didáctica de los ejemplos.



Calcular los permisos al compartir

El algoritmo es igual, que el visto en la unidad 4 en la solapa Seguridad, basado en las dos normas siguientes:

- Los permisos compartidos son acumulativos.
- Denegar prevalece sobre otros permisos.

Ejemplos:

1. Un usuario tiene permiso de lectura en una carpeta compartida, y el usuario pertenece a un grupo que tiene control total.
   Respuesta.- El usuario se conectará con control Total
2. Un usuario pertenece a 3 grupos: uno de ellos no tiene permiso explícito, otro tiene permiso lectura y otro tiene permiso Cambiar.
   Respuesta.- El usuario se conecta con Cambio
3. Un usuario pertenece a 3 grupos: uno de ellos tiene lectura denegada, otro tiene permiso lectura y otro tiene permiso Cambiar.
   Respuesta.- El usuario no tiene ningún permiso.

Observaciones:

Al igual que en la configuración de los permisos locales, debemos **denegar permisos de forma cuidadosa** al compartir.

Combinación de permisos en las solapas Compartir y Seguridad

Una de las primeras preguntas que nos debemos hacer, es cómo se combinan los permisos de compartir en Red y la seguridad local NTFS.
En un recurso compartido, el usuario tendrá permisos de lectura, cambio, control total o ningún permiso. El usuario se conecta desde la red, y obtendrá dicho permiso.
Pero, ¿qué ocurre con la seguridad local?

- Si la partición es FAT 32, los permisos obtenidos al conectar al recurso son los mismos en todas las subcarpetas y ficheros del recurso. (Pues FAT 32, no tiene seguridad local)
- Si la partición es NTFS, los permisos obtenidos al conectar al recurso se ven afectados por los permisos NTFS LOCALES. De esa forma, es posible que en algunas subcarpetas podamos realizar cambios y en otras no.

Se puede resumir que cuando un usuario conecta desde la red, los permisos que tiene son los más restrictivos de las solapas Compartir y Seguridad (es decir la intersección)

Ejemplo: Un usuario tiene en un recurso el permiso de cambio, y de forma local tiene el permiso lectura. ¿Qué permiso tiene el usuario cuando acceda desde la red?
Respuesta: El usuario solo tendrá lectura.

Recomendación final sobre seguridad local y compartir recursos.

Se han visto dos formas de poner permisos, una de forma local y otra en la red. Hay que ser muy ordenado en la administración de permisos, pues se ha visto que cuando se accede desde la red, se tienen en cuenta ambos.
Por este motivo se dan 2 recomendaciones conjuntas para facilitar la administración, y evitar conflictos:

1. Administrar toda la seguridad con los permisos NTFS.
2. Compartir el recurso a Todos los usuarios y con control total.

Este punto de vista se explica de la siguiente forma, si configuramos muy bien el equipo desde la seguridad local, ya no nos importa compartir con control total a Todos, pues la seguridad local se impondrá por ser más restrictiva.

Información de Microsoft sobre cómo compartir en Windows.

3.- Servicios de redes.

Caso práctico

María se dispone a montar una plataforma web para unos clientes de BK Programación. Sabe que a **Carlos** le interesa el tema de los servicios de Internet, por lo que le incorpora al proyecto para trabajar conjuntamente y que aprenda sobre ello. Durante las primeras reuniones para coordinar las tareas a **Carlos** le surgen ciertas dudas:

—¿En qué consiste la arquitectura cliente-servidor?—Si hay varios servicios funcionando o recursos a compartir en un equipo, ¿cómo podemos hacerlos accesibles a otros ordenadores?—¿La información de cada servicio viaja por canales independientes? ¿Qué tipos de servidores existen? ¿Qué diferencia hay entre un servidor de aplicaciones y un servidor web? ¿Y entre un servidor de ficheros y un servidor FTP?

María decide explicarle detenidamente cada una de sus preguntas. **Carlos** escucha con atención y toma nota de los conceptos clave.

Los servicios en red son importantes en toda infraestructura de red, ya que gracias a ellos los diferentes ordenadores puedes comunicarse, y el sistema informático es más potente.

Dentro de los servicios de red verás cómo gestionarlos y qué puertos están relacionados con los mismos. Posteriormente estudiaras la configuración y gestión básica de algunos servidores importantes, tales como los servidores de archivos, de impresión y de aplicaciones. Para finalmente mostrarte cómo controlar estos servicios.

3.1.- Arquitectura cliente-servidor.

Los servicios son procesos, programas en ejecución, que suelen ejecutarse de forma transparente al usuario. Muchos se activan de forma automática al inicio del sistema operativo, o tras una petición del usuario, en función del rendimiento del equipo, del tráfico de la red, etc.

El estudio se va a centrar en los servicios de red.
La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los proveedores de recursos o servicios, conocidos como servidores, y los solicitantes de estos, que son los clientes. Un cliente realiza peticiones a otro programa, el servidor, que atiende dichas peticiones dando respuesta.
La separación entre cliente y servidor es una separación de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina, ni es necesariamente un sólo programa.
Se ha visto en anterior unidad, que todos los equipos conectados a una red tienen una dirección IP que los identifica, ya sean ordenadores cliente o servidores.

Puertos

Cada sistema operativo posee unos puertos virtuales o lógicos. Esto significa que, al contrario que los puertos físicos (USB, Firewire, DVI, HDMI, etc.) sólo existen virtualmente para el ordenador. Los sistemas operativos cuentan con más de 65.000 puertos virtuales disponibles para abrir conexiones, y se las ceden a los programas para que vuelquen sus datos en la red. Los programas los solicitan y el sistema operativo los gestiona para poder utilizarlos y establecer una conexión lógica. Esto permite que puedan comunicarse con otro ordenador "punto a punto". Finalmente, toda comunicación entre dos dispositivos en Internet se traduce en un flujo de datos entre dos puertos virtuales abiertos por alguna aplicación, entre una parte cliente y una servidora.

Los programas que comienzan la comunicación en un puerto se llaman clientes y los programas que están siempre usando un puerto esperando que los clientes se conecten a él, se llaman servidores, se dice que los servidores están escuchando.
Por ejemplo, un servidor web, está siempre esperando que un cliente (el navegador) se conecte para mostrarle el contenido de la página web. El servidor web suele utilizar permanentemente el puerto 80 para esperar conexiones entrantes y los navegadores suelen usar un puerto cualquiera de los 65.000 para establecer el flujo de comunicación. El hecho de que se utilice el puerto 80 para ofrecer páginas web es una convención histórica, pero en realidad podría utilizarse cualquier otro. Para enviar y recibir correo, por ejemplo, se utiliza el 25.

El número de puertos se codifica con 16 bits, lo que significa que hay 216 = 65536 posibles puertos.

Los puertos del 0 al 1023 son los "puertos conocidos" o reservados. Están reservados para los servidores. Sin embargo, un administrador de red puede conectar servicios con puertos de su elección.
Los puertos del 1024 al 49151 son los "puertos registrados". Los programadores, cuando programan un servicio suelen utilizar los puertos registrados.
Los puertos del 49152 al 65535 son los "puertos dinámicos y/o privados". Se utilizan para comunicaciones muy cortas, de ahí el nombre de dinámico.
Del lado del cliente, el sistema operativo elige el puerto entre los disponibles de forma aleatoria, nunca entre los puertos 0 y 1023 por ser los reservados para los servidores.
Se refleja a continuación una lista de los puertos reservados para los servicios más importantes:

A continuación, se indican algunos de los puertos conocidos más utilizados:

Puertos conocidos asociados a servicios o aplicaciones

Puerto	Servicio o aplicación
21 (control), 20 (datos)	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
143	IMAP
119	NNTP

Monitorización de red.

En ocasiones, la velocidad de la red decrece, siendo necesario averiguar el motivo: ¿hay algún usuario ajeno a la red que está aprovechándose del ancho de banda? ¿Se está siendo víctimas de otro tipo de ataque: sniffing, spoofin IP, DoS?

La solución es incrementar el control sobre la red utilizando herramientas de análisis de red. Estas herramientas realizan un estudio detallado y pormenorizado del tráfico que circula por la red.

La monitorización se considera, también, una tarea de mantenimiento preventivo, tanto a nivel de seguridad como de dimensionamiento de red: puede ocurrir que el ancho de banda sea insuficiente o por el contrario esté sobredimensionado.

Algunas de las herramientas de monitorización de redes más conocidas:

Wireshark
Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones. Tiene una interfaz gráfica, y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo.
Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP. Wireshark es software libre y se ejecuta sobre la mayoría de sistemas operativos Unix, Linux, Mac OS X y Microsoft Windows.
Nmap
Es un programa de código abierto que sirve para efectuar rastreo de puertos. Nmap es difícilmente detectable, ha sido creado para evadir los Sistema de detección de intrusos (IDS) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.
Nagios
Software libre para Linux, permite monitorizar la red, permitiendo al administrador configurar advertencias.

Estas herramientas de monitorización darán información sobre:

- Número de equipos conectados y sus direcciones IP.
- Tipo de tráfico predominante.
- Qué puertos están abiertos.
- Qué conexiones establecidas hay.
- Algunos programas permiten la realización de inventarios de los equipos de la red (puntos de red, segmentos, cableado, switches, routers, PC, etc.)

En el capítulo 4 se estudian los comandos TCP/IP que sirven para resolver problemas de red y monitorizar redes.

Para saber más

Conoce más puertos asignados a otros conocidos servicios de red.

Servicios y sus números de puertos.

Autoevaluación

¿A qué puerto está asociado el servicio de IMAP?

- ○ 119
- ○ 110
- ○ 143
- ○ 234

No, 119 es incorrecto.

No, 110 es incorrecto.

Sí, efectivamente.

No, 234 es incorrecto.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

3.2.- Servicios de infraestructura de red.

Existen muchos servicios, algunos de ellos necesarios para crear una infraestructura de red. Entre ellos:

- **Encaminamiento:** permite a un servidor actuar como router para permitir la comunicación entre dos o más redes. En el libro 9.A.1. hemos configurado las IP, de los equipos cliente1 y cliente2, pero no se ha puesto puerta de enlace. La puerta de enlace será normalmente la dirección del router, por el que saldremos a Internet.
- **Servidor DHCP**. Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando conectamos un ordenador en casa, no es necesario configurar la dirección IP como se ha hecho en el libro A.1. Ello se debe, a que los routers de las compañías telefónicas suelen tener instalado el servidor DHCP, de forma que cuando se conecta un ordenador a dicha red, el servidor DHCP facilita una IP al ordenador.
- **Servidor DNS**. Un servidor DNS es un equipo en Internet que facilita la navegación web, pues traduce las direcciones web, que se utilizan en los navegadores web a las direcciones IP correspondientes. Son como un diccionario con 2 columnas: direcciones web y direcciones IP. En los ordenadores de los domicilios particulares, no suele ser necesario especificar la dirección IP del servidor DNS, pues suele estar indicado en los routers.

Se profundizó el enrutamiento en la unidad 8, ahora se va a profundizar en los servicios DHCP y DNS.

1. Servicio DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración de equipo dinámica)

El mantenimiento y la configuración de la red de los equipos de una red pequeña es relativamente fácil. Sin embargo, si la red es grande, cualquier cambio en la configuración de red: dirección IP, puerta de enlace, DNS conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, utilizar IP estáticas (IP fijas) puede obtener un mal aprovechamiento de las direcciones IP de la red. Por ejemplo, en una clase C solo se pueden tener 254 equipos. De forma estática solo se pueden tener esos equipos, pero si se configuran de forma dinámica, se pueden reutilizar las direcciones IP en otros equipos. Podemos tener en una empresa con bastantes ordenadores portátiles, más de 254, que cuando se enciendan, el servidor DHCP les asigna una dirección IP y al apagar el equipo, se queda libre para otro ordenador.

Los datos mínimos que un servidor de DHCP proporciona a un cliente son:

- Dirección IP.
- Máscara de red.
- Puerta de enlace o gateway.
- Dirección IP del servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

Asignación dinámica. Asigna direcciones IPs libres de un rango de direcciones establecido por el administrador.
Reserva por dirección IP. Consiste en asignar siempre la misma IP a un equipo concreto. Para ello se utiliza la dirección MAC. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP deberemos configurar nuevamente la impresora en todos los equipos clientes que la utilicen.

Más información en el siguiente enlace.

2. Servicio DNS (Domain Name System, Sistema de nombres de dominio)

Si ejecutamos ping a www.educa.madrid.org vemos que responde el equipo 213.229.137.36, que es su dirección IP correspondiente.

Para navegar es más fácil memorizar la página www.educa.madrid.org que su IP, además ofrece más flexibilidad; pues si cambia el alojamiento de la página web, cambia la dirección IP, pero los clientes no notan ningún cambio, pues se sigue navegando en la página web con la dirección web.

Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba en los propios ordenadores a través de un fichero (\winnt\system32\driver\etc\hosts en Windows o /etc/hosts en Linux). Esta opción presentaba el problema que cualquier cambio, significaba cambiar el fichero en todos los ordenadores de la red.

De ahí se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se dispone de uno o más servidores encargados de resolver los nombres de los equipos pertenecientes a su ámbito, consiguiendo la centralización necesaria para la correcta sincronización de los equipos y un sistema jerárquico que permite una administración focalizada y descentralizada.

2.1. Espacio de nombres de dominio

Al igual que los ficheros de los sistemas operativos se organizan en árboles jerárquicos, el sistema de nombres de dominios también se estructura con un árbol jerárquico en el que las distintas ramas que encontramos reciben el nombre de dominio y el nombre completo de un equipo (el equivalente al nombre de un fichero) o FQDN (path absoluto) es el nombre resultante de recorrer todos los dominios por los que pasamos, desde las hojas hasta la raíz del árbol utilizando, en este caso, el carácter '.' (punto) como separador.
En la imagen se muestra un ejemplo de jerarquía de los dominios de Internet.

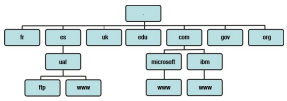


Imagen de los materiales originales de FP a Distancia (CC BY-NC-SA)

Dependiendo de la profundidad del árbol, se hablará de dominios de primer, segundo o tercer nivel.
Como ejemplo en la imagen se obtiene el dominio de tercer nivel www.microsoft.com

En el primer nivel del árbol encontramos que los nombres de los nodos ya están establecidos de antemano, existiendo dos tipos de divisiones: geográfica y organizativa.

División geográfica: se distingue una rama -dominio- por país:
- Para España .es
- Para Gran Bretaña, .uk
- Para Alemania, .de.

División organizativa:
- Para empresas .com, independientemente del país en el que se encuentren.
- Para organizaciones establecidas mediante tratados internacionales .int
- Para organizaciones no gubernamentales .org
- Organizaciones educativas .edu, del gobierno .gov y del ejército de EE.UU. .mil

Posteriormente, se han introducido nuevos dominios de primer nivel como .name para nombres de personas; .info para proveedores de servicios de información; .web para empresas relativas a servicios web; etcétera.

Cada rama del árbol jerárquico recibe el nombre de dominio y la asignación de nombres se delega en un responsable. Para España, la rama .es la mantiene la empresa pública REDES, que a su vez podrá delegar la resolución de nombres de las distintas ramas en las que se divide, en otras corporaciones.

Una característica crucial es la máxima disponibilidad del servicio DNS. Para ello, existen varios servidores capaces de realizar el mismo servicio aunque la autoridad de resolución de nombres de zona siga recayendo en un servidor principal. Estos servidores con autoridad reciben el nombre de servidores primarios y el resto servidores secundarios.
Para que no existan problemas de sincronización cada vez que se modifique un dato del servidor primario debe transmitirse a todos los secundarios para el correcto funcionamiento del sistema.

2.2. Registrar un dominio

Cualquier persona física con residencia en España, así como empresas constituidas según la legislación española, puede solicitar el registro de dominios a través de la página estatal nic.es o bien, por medio de los agentes registradores acreditados. Los nombres de dominio se deben, según la reglamentación española, corresponder con:

- Nombre (o abreviatura) de una empresa que la identifique de forma inequívoca.
- Nombres comerciales o de marcas.
- Nombre de personas tal y como aparecen en su DNI, con un máximo de 60 caracteres.
- Nombres de profesiones y el apellido o nombre del profesional que se dedica a dicha labor o del nombre del establecimiento.

Para saber más

Puedes investigar más sobre las denominaciones de origen, en cuyo caso debe solicitarlo el órgano regulador de dicha denominación.

Información adicional sobre el servidor DNS.

3.3.- Servicio FTP (File Transfer Protocol, Protocolos de transferencia de ficheros.

Las redes de ordenadores se idearon para el intercambio de información y la compartición de ficheros. Tenemos dos opciones, a través de un servidor de archivos, o mediante el uso de un servidor FTP.
Un servidor de archivos o ficheros nos permite compartir recursos, dentro de una misma red local como se ha visto en el libro B al compartir recursos en Windows. O como se estudiará en la unidad 10 en Linux, al utilizar los servicios NFS y Samba.
Por otro lado, el servicio FTP permite conectarse a un equipo (el servidor FTP) y transferir ficheros desde éste hacia el equipo del cliente (cliente FTP) y en sentido inverso.

El protocolo FTP establece una doble conexión TCP entre el cliente y el servidor:

- **Conexión de control:** suele emplearse el puerto 21 del servidor y sirve para indicarle a éste las operaciones que se quieren llevar a cabo.
- **Conexión de datos:** se usa normalmente el puerto 20 del servidor y es la que se sirve para la transferencia de ficheros hacia o desde el servidor.

Cuando un cliente FTP se quiere conectar al servidor FTP, existen dos tipos de autentificación:

- **Anónimo.** La comunicación se realiza sin ningún tipo de identificación y, por lo tanto el usuario tendrá muy pocos privilegios en el servidor. En este caso, el usuario estará confinado en un directorio público donde puede descargar los archivos allí ubicados pero sin posibilidad de escribir o modificar ningún fichero. El directorio público suele llamarse pub.
- **Acceso autorizado.** El usuario establece la comunicación con una cuenta de usuario. Tras identificarse, se confina al usuario a su directorio predeterminado desde donde puede descargar ficheros y, si la política implantada lo permite, también escribir. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.

Estos parámetros **(el tipo de autenticación y los permisos) se establecerán en la configuración del sitio FTP en el equipo servidor.**

Como ejemplo, el servidor (nombre del dominio) ftp de Educamadrid se llama ftp.educa.madrid.org, que permite el acceso anónimo. Para ello, abrimos el navegador web y escribimos ftp://ftp.educa.madrid.org. Al pulsar intro en el navegador, entramos como usuario anónimo al servidor ftp de Educamadrid (ver imagen)

Cuando en el navegador web se escribe ftp:// significa que la comunicación se realiza con el protocolo ftp, a diferencia de cuando se escribe htpp:// que la comunicación se realiza con el protocolo http.

Miguel Ángel García Lara (CC BY-NC)

Servidores FTP

Los servidores FTP más utilizados son IIS (Internet Information Server) en los equipos Windows, Filezilla Server (para Windows y Linux) y vsftpd (para servidores Linux)

Clientes FTP
Los clientes FTP son el software que utilizamos para conectar al servidor FTP.
Los clientes FTP más utilizados son Filezilla, cuteftp, vsftp y los propios navegadores web.
Las propias terminales de comandos, tanto de Windows como GNU-Linux incluyen un cliente ftp. Para conectarnos se escribe ftp nombre_servidor.
Para explorar el servidor y realizar la transferencia de ficheros se utilizan los comandos ftp.

Archivo anexo a la unidad en el capítulo 4.

3.4.- Servicio Web. Protocolo HTTP (Hipertext Transfer Protocol, Protocolo de transferencia de hipertexto).

Conocido con sus siglas www (World Wide Web) que aparecen en el nombre de prácticamente todos los servidores web, el servicio web es el servicio más utilizado de los que se ofrecen en Internet.
Un servidor web se encarga de alojar y proporcionar las páginas web solicitadas por los clientes desde sus navegadores. Un servidor web maneja el protocolo HTTP. Cuando el servidor web recibe una petición HTTP, este responde con una respuesta HTTP, normalmente una página HTML. El servidor Web puede responder con una página HTML estática, una imagen, enviando una redirección, o delegando la generación dinámica de la respuesta a algún otro programa, como por ejemplo algún script CGI, JSP (JavaServer Pages), Servlets, ASP (ActiveServer Pages), PHP, este tipo de programas del lado del servidor se dice que generan una página dinámica del lado servidor, enviando la página resultante en HTML, para que pueda ser vista en el navegador web del usuario.

La variante segura de HTTP es el protocolo HTTPS donde la S significa Secure. El protocolo HTTPS protege la integridad y confidencialidad de los datos entre el cliente y servidor.
La integridad se refiere a que la página recibida en el cliente sea la realente enviada por el servidor.
La confidencialidad a que los datos enviados en la comunicación no puedan ser interceptados por viajar cifrados.

Servidor web

Los servidores web más conocidos son:

- Apache: software libre multiplataforma para Windows, Linux y MacOS. Página oficial:
- Nginx, también software libre multiplataforma. Página oficial:
- IIS - Internet Information Server, servicio de Microsoft para los sistemas operativos Windows.

En la actualidad crece el número de servidores que utilizan IIS, siendo en la actualidad del 40%, parecidos a los que suman Apache y Nginx. Pero si se mira las visitas realizadas a los servidores, Apache y Nginx suman un 60% mientras que IIS son un 10%. Vínculo de cuota de servidores en diciembre 2018:

Cliente web

Los clientes son los navegadores web como Mozilla Firefox, Google Chrome, Internet Explorer, Safari, etcétera.
Las principales diferencias entre los clientes web residen en el número e importancia de vulnerabilidades que presentan así como en diferentes matizaciones que existen en cuanto a la interpretación del código HTML y que puede impedir la correcta visualización de algunas páginas en determinados clientes. También incluyen la interpretación de scripts del lado cliente como Javascript.

3.5.- Servicio de correo electrónico.

El sistema de correo electrónico es junto al servicio web, los servicios de Internet más utilizados a nivel de usuarios.
Este servicio **es un sistema para la transferencia de mensajes**, rápido y eficiente, ideado bajo la arquitectura cliente-servidor típica de Internet.

Servidor de correo

El servidor tiene los siguientes componentes, trabajando con varios protocolos:

Servidor de correo saliente El cliente envía el email al servidor, y a su vez el servidor envía el correo al servidor del destinatario. Utiliza el protocolo SMTP.

Servidor de correo entrante Almacena los correos electrónicos recibidos en los buzones de los usuarios. Cuando el cliente se conecta, se le envían los correos electrónicos que ha recibido. Utiliza los protocolos POP e IMAP.

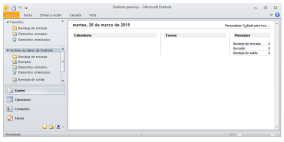
Clientes de correo

En la actualidad se utiliza el correo web de forma masiva, pero en las empresas el correo electrónico se suele utilizar con clienes de correo.

Cuando se envía un mensaje, este mensaje se envía al servidor. Después, según el tipo de correo que se utilice, el servidor envía al destinatario el mensaje, o lo solicita el destinatario al servidor.
Esto da lugar a 2 tipos de software de correo:

Correo web: el más utilizado en la actualidad a nivel particular. El usuario se conecta al servidor de correo con un navegador web. El usuario tiene acceso a todo su correo y administración: puede crear mensajes, borrar, organizar en bandejas y administrar los contactos. La información siempre está en el servidor, por lo que el usuario se puede conectar desde cualquier ordenador con Internet.

Clientes de correo: se instala software de correo en el ordenador, y el cliente conecta al servidor, descargándose todos los correos en el propio equipo. La bandeja de entrada, salida, contactos, las tiene el usuario en el propio equipo.
Entre los clientes de correo más conocidos se encuentran Evolution, Microsoft Outlook y Mozilla Thunderbird.
Esta es la forma más habitual en la conexión en las empresas. El usuario tiene en su equipo todos los mensajes y contactos anteriores, sin necesidad de conectarse a Internet.
Todos ellos presentan funciones similares: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.
Se incluye una imagen del cliente Microsoft Outlook:



3.6.- Acceso remoto.

Los servicios de acceso remoto, permiten controlar y administrar otro ordenador a través de la red. Así por ejemplo, desde un equipo en casa se puede conectar al equipo del trabajo, y se pueden usar todos sus programas, archivos y recursos de red como si se estuviese físicamente en el equipo de la oficina.
Para realizar la conexión, en las distintas aplicaciones, es necesario instalar el software servidor en el equipo que se quiere controlar, y el programa llamado cliente en la máquina desde la que se va a llevar el control.

Se especifican varios servicios de acceso remoto clasificados por su interfaz de texto o interfaz gráfica:

Acceso remoto en modo terminal.

En modo terminal, se utilizan como accesos remotos los servicios Telnet y SSH.
Telnet es una aplicación TCP/IP y se utiliza tanto en Windows como Linux, incluida en las terminales de Windows y GNU-Linux. Pero en la actualidad se utiliza muy poco por ser inseguro, pues el envío de la información se realiza en texto plano sin cofificar.

SSH tiene la misma funcionalidad que Telnet, e igualmente es el nombre de un protocolo y de un programa, pero se le han añadido: el cifrado de las conexiones para evitar que los datos sean interceptados. Además emplea mecanismos de autenticación más seguros para los usuarios que se conectan. El servicio ssh es software libre y utilizado incialmente en GNU-Linux, se ha extendido su uso a Windows.
En la unidad 10 se utilizará el servicio de acceso remoto ssh.

La ventaja de los accesos remotos por terminal, es la fluidez en la comunicación, pues necesitan poco ancho de banda al incorporar solo texto en la comunicación.

Acceso remoto en modo gráfico.
En modo gráfico las aplicaciones más conocidas son:

- Escritorio remoto y Terminal Server aplicaciones incluidas en las versiones más completas de Microsoft Windows.
- VNC (Visual Network Control), software libre utilizado en máquinas Windows y Linux.
- Teamviewer, aplicación externa de Windows, que suelen utilizar los servicios técnicos telefónicos para la solución de problemas.

3.7.- Ejemplo. Instalación y configuración de un servidor FTP en “Internet Information Service” en Windows 10.

En este tutorial se va a instalar y configurar el servidor FTP que viene con Windows 10.
Este tutorial corresponde a un ejercicio de la tarea.
Se creará un servidor FTP con nombre ‘ftp.empresa_inicialesAlumno.es’ que exija autenticación a los usuarios y donde estos tengan permisos para bajar y subir archivos. Además, se verá cómo se conecta un cliente al servicio FTP.
El servicio IIS (Internet Information Service) incluido en los sistemas operativos Windows, incluye el servidor web y el servidor FTP de Microsoft. Microsoft denomina a los servidores web y ftp, como mis “sitios web” y “sitios ftp”.

Paso 1. Instalar IIS con el servidor FTP.

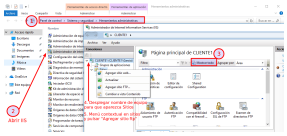
Instalar IIS y el servidor FTP de Windows. Para ello, ir a Panel de control / Programas / Añadir características de Windows /
Marcamos las opciones de añadir “Internet Information Services” y “Servicio FTP”, tal como se ve en la captura.

Cuando se pulsa Aceptar, se instala el servidor.

Paso 2. Crear nuevo servidor FTP

Para configurar el servicio FTP regresamos de nuevo al Panel de control – Sistema y seguridad - Herramientas Administrativas y hacemos clic sobre “Administrador de Internet Information Service (IIS)”.

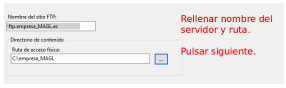
Seguimos los pasos de la imagen para añadir el sitio FTP: Pulsar mostrar todo. Menú contextual en nombre de equipo para que aparezca “Mis sitios” y menú contextual para seleccionar “Agregar sitio FTP”.



Paso 3. Rellenar nombre del nuevo sitio FTP y ruta

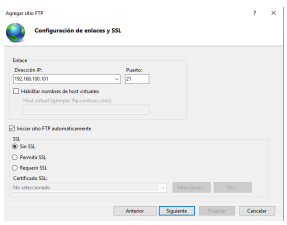
Se escribe los campos en la ventana que aparece (ver captura):

Nombre del sitio FTP: Rellenar con ftp.empresa_InicialesAlumno.es
Ruta de acceso física: se introduce la ruta de la carpeta donde se van a alojar los ficheros del sitio FTP. Crear la carpeta empresa_InicialesAlumno en C, y rellenar “C:/empresa_InicialesAlumno”.



Paso 4. Ventana “Configuración de enlaces y SSL”

Se abre esta ventana, rellenamos con los datos de la captura.

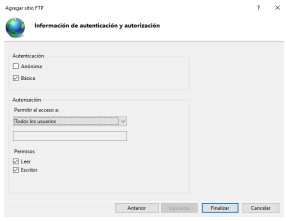


Explicación de cada opción:

- Enlace - Dirección IP: en este campo se puede indicar qué dirección IP se le asignará a este sitio FTP, ya que el equipo puede tener varias direcciones IP (varias interfaces de red). Por defecto queda seleccionado “Todas las no asignadas”. Si tenemos varios sitios FTP y queremos que sean accesibles desde fuera del equipo, podremos indicar qué dirección IP se le asignará a cada sitio FTP.
- Habilitar nombres de host virtuales: si queremos tener varios sitios FTP en un equipo con una sola dirección IP y queremos que sean accesibles desde fuera del equipo (LAN o Internet) podremos marcar esta opción de “Habilitar nombres de host virtuales” e indicar el nombre del sitio ftp que queramos establecer. Es decir, se pueden tener 2 servidores virtuales (de ahí su nombre) en un único servidor, utilizando nombres distintos: ftp.empresa1.es y ftp.empresa2.es
- Iniciar sitio FTP automáticamente: dejando marcada la opción el servicio del sitio FTP se inicia automáticamente al arrancar el equipo.
- SSL, permite 3 opciones:
  Sin SSL: seleccionando esta opción de Secure Sockets Layer (Protocolo de Capa de Conexión Segura) se desactiva este protocolo.
  Permitir: con esta opción el usuario se puede conectar con SSL y sin SSL.
  Requerir SSL: el usuario solo se puede conectar usando SSL.
  En nuestro caso, al no tener instalado ningún certificado de seguridad, hay que marcar “Sin SSL”

Paso 5. Ventana “Información de autentificación y autorización”

Se abre esta ventana y rellenamos con los datos de la captura. Al pulsar “Finalizar”, ha quedado creado el sitio web.

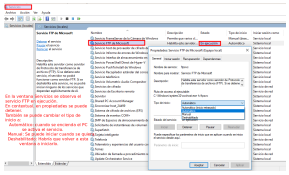


Explicación de las distintas opciones:
En esta ventana se configura si se permite el acceso anónimo o basado en “autenticación básica” donde los usuarios tienen que proporcionar un nombre de usuario y contraseña válidos de Windows. Es importante saber que la autenticación básica transmite contraseñas no cifradas por la red, de ahí, que en un entorno profesional es obligatorio utilizar SSL.

Marcada la autorización básica, se puede seleccionar a “Todos los usuarios” o a usuarios o grupos concretos.

Paso 6. Ventana servicios en Windows.

Se comprueba que el servicio Ftp está activo en Windows, para ello, se abre la ventana servicios y se comprueba que el “Servicio FTP” se encuentra en ejecución, tal como se muestra en la captura. En esta ventana de Windows se inician o detienen todos los servicios. Asimismo, pulsando en propiedades en el nombre de cada servicio tenemos las opciones de seleccionar en “Tipo de inicio“:
- Automático: siempre que se inicie el ordenador, se inicia el servicio.
- Manual: hay que iniciar el servicio manualmente.
- Deshabilitado: no se puede iniciar el servicio.

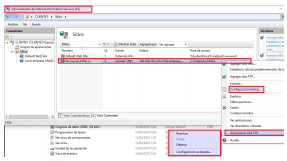


Paso 7. Configuración y control del sitio FTP.

En Servicios se puede detener o iniciar el servicio FTP, pero hemos visto que se pueden configurar varios “sitios FTP”. Si se quieren tener unos activos y otros detenidos, se configura en la consola de “Internet Information Services”

Al pulsar menú contextual en el sitio, se puede Iniciar y Detener. Y también configurar en “Configuración básica” y “Configuración avanzada”.

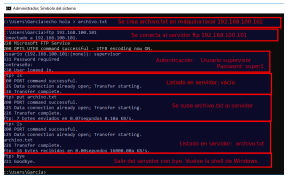
Incluso, vemos las opciones para agregar un nuevo “sitio ftp” y un “sitio web”



Conexión de clientes al servicio FTP.

En este ejemplo se va a realizar la conexión con la terminal de Windows. En el equipo cliente2 se abre la terminal y se escribe:
ftp 192.168.100.101
Nos pide usuario y contraseña. Una vez dentro, se pueden utilizar los comandos de ftp. (Anexo de la unidad)

En la captura, se realiza una conexión desde cliente2 al servidor ftp y se sube un fichero desde cliuente2 a cliente1.



Observación final:
La conexión con nombre del dominio se realizaría escribiendo:
ftp ftp.empresa_MAGL.es
En el ejemplo visto aquí, no funciona si escribimos esta dirección. ¿Por qué?, porque no tenemos un servidor DNS que diga que ftp.empresa_MAGL.es corresponde a la IP 192.168.100.101

4.- Comandos de red.

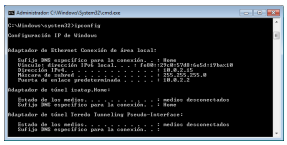
Caso práctico

Juan se plantea distintas utilidades para monitorizar la red. Por eso va a repasar los principales comandosTCP/IP en Windows.

4.1.- Comandos TCP/IP en Windows.

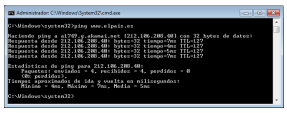
El protocolo TCP/IP, facilita distintas utilidades para monitorizar la red, por lo que estos comandos los tenemos tanto en Windows como en Linux, con pequeñas diferencias en sus nombres o ejecución.
Se muestran a continuación los de Windows con ejemplos de ejecución.

Comando ipconfig
Devuelve la configuración de las distintas tarjetas de red, con su dirección IP, máscara y puerta de enlace.
Con la opción /all devuelve una información más completa, entre ella, la dirección física (MAC) de las distintas conexiones.



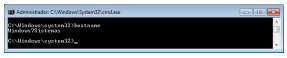
Miguel Ángel García Lara (CC BY-NC-SA)

Comando ping
Sirve para ver si tenemos conexión con cualquier equipo, podemos utilizar tanto la dirección web, como su IP. En el ejemplo se realiza ping con éxito a www.elpais.es



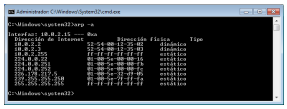
Miguel Ángel García Lara (CC BY-NC-SA)

Comando hostname
Devuelve el nombre del equipo



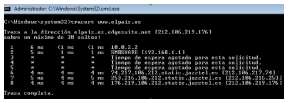
Miguel Ángel García Lara (CC BY-NC-SA)

Comando arp
En la unidad anterior se estudió que los protocolos arp y rarp traducen IP en direcciones físicas y viceversa. El comando arp –a muestra las relaciones IP y MAC conocidas en este momento.
Con otras opciones, se pueden añadur datos.



Miguel Ángel García Lara (CC BY-NC-SA)

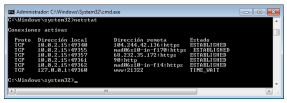
Comando tracert
El comando tracert (viene de traceroute) devuelve por todos los equipos que pasan las tramas para llegar del PC actual a un PC destino. Algunos datos no se muestran, porque los router bloquean estas peticiones (también pasa muchas veces con el comando ping)



Miguel Ángel García Lara (CC BY-NC-SA)

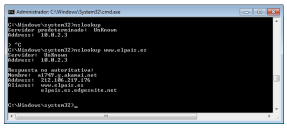
Comando netstat
Netstat muestra todas las conexiones activas en nuestro equipo y con qué dirección remota están establecidas.
Con la opción –a, además de las conexiones establecidas, nos daría todos los puertos que están abiertos, escuchando (todas las puertas abiertas a nuestro equipo), esperando peticiones remotas.

Recordar que cuando por ejemplo en el navegador ponemos http://www.elpais.es estamos utilizando el protocolo http que utiliza por defecto el puerto 80. Lo que quiere decir que nos conectamos al ordenador www.elpais.es por el puerto 80. De hecho, podíamos haber escrito en el navegador: http://www.elpais.es:80

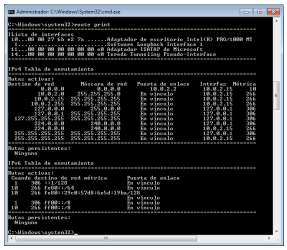


Miguel Ángel García Lara (CC BY-NC-SA)

Comando nslookup
El comando nslookup sin ninguna opción, nos devuelve la dirección IP de nuestro servidor DNS. También podemos averiguar la dirección IP de cualquier página web. (ver captura).



Comando route
El comando route con la opción print, muestra la tabla de enrutamiento actual.
Con otras opciones, sirve para configurar rutas.



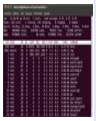
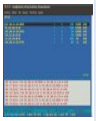
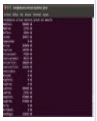
Para saber más

Para ver más información de las opciones de estos comandos, ver el vínculo siguiente:

Comandos de red

Anexo.- Licencias de recursos.

Licencias de recursos utilizados en la Unidad de Trabajo.

Recurso (1)	Datos del recurso (1)	Recurso (2)	Datos del recurso (2)
	Autoría: warszawianka. Licencia: GPL. Procedencia: http://openclipart.org/detail/35347/tango-system-users-by-warszawianka		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla donde se muestra el terminal del sistema.
	Autoría: Andrew Fitzsimon / Anonymous. Licencia: GPL. Procedencia: http://openclipart.org/detail/25528/text-page-icon-by-anonymous-25528		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla de Ubuntu, propiedad de Ubuntu.
	Autoría: Webmin. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la interfaz web Webmin propiedad de Webmin.		Autoría: Mfield, Matthew Field. Licencia: Uso Educativo no comercial. Procedencia: http://es.wikipedia.org/wiki/Archivo:Hard_disk_platters_and_head.jpg
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del administrador de volúmenes propiedad de Ubuntu.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del administrador de volúmenes propiedad de Ubuntu.
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del comando fdisk propiedad de Ubuntu.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal de Ubuntu, propiedad de Ubuntu.
	Autoría: Super GRUB Disk. Licencia: GNU/GPL. Procedencia: Captura de pantalla de http://www.supergrubdisk.org/		Autoría: Sysv-rc-config. Licencia: GNU/GPL. Procedencia: Captura de pantalla de la herramine sysv-rf-config, de Ubuntu.
	Autoría: chkconfig. Licencia: GNU/GPL. Procedencia: Captura de pantalla de chkconfig, propiedad de Ubuntu.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal de Ubuntu, propiedad de Ubuntu.
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del comando top, propiedad de Ubuntu.		Autoría: unknown - public domain. Licencia: GNU/GPL. Procedencia: http://cliparts101.com/free_clipart/14885/analog_clock.aspx
	Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del escritorio, propiedad de Ubuntu.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal de Ubuntu, propiedad de Ubuntu.
	Autoría: iptraf y Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla de iptraf.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal de Ubuntu mostrando el fichero meminfo, propiedad de Ubuntu.
	Autoría: Webmin. Licencia: GNU/GPL. Procedencia: Captura de pantalla de Webmin, propiedad de www.webmin.com.		Autoría: Austinmurphy at en.wikipedia. Licencia: GNU Free Documentation License. Procedencia: http://es.wikipedia.org/wiki/Archivo:LTO2-cart-purple.jpg

	Autoría: putty. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal mostrando el comando tar, propiedad de Ubuntu.		Autoría: Ubuntu. Licencia: GNU/GPL. Procedencia: Captura de pantalla del terminal mostrando fdisk –l, propiedad de Ubuntu.
	Autoría: http://rsync.samba.org/. Licencia: GNU/GPL. Procedencia: http://rsync.samba.org/		Autoría: YO Pictureve. Licencia: Creative commons. Procedencia: http://es.wikipedia.org/wiki/Archivo:CD_VIRGEN_PARA_QUEMAR_O_GRABAR_ARCHIVOS.jpg
	Autoría: Déjà Dup. Licencia: GNU/GPL. Procedencia: Captura de pantalla de Deja Dup, propiedad de Deja Dup.		Autoría: Brasero. Licencia: GNU/GPL. Procedencia: Captura de pantalla de Brasero, propiedad de Brasero.
	Autoría: Clonezilla. Licencia: GNU/GPL. Procedencia: Captura de pantalla de Clonezilla, propiedad de Clonezilla.		