



9. Administración de redes Windows

Autor	ⓧ Xerach Casanova
Clase	Sistemas Informáticos
Fecha	@Mar 16, 2021 7:51 AM

1. Configuración de red en Microsoft Windows

1.1. Introducción

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

2. Compartir recursos en la red

2.1. Solapa compartir

3. Servicios de redes

3.1. Arquitectura cliente - servidor

3.2. Servicios de infraestructura de red

3.3. Servicio FTP (File Transfer Protocol, protocolos de transferencia de ficheros)

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

3.5. Servicio de correo electrónico

3.6. Acceso remoto

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

4. Comandos TCP/OP en Windows

Mapa conceptual

1. Configuración de red en Microsoft Windows

Administrar una red consiste en aplicar una serie de técnicas que la mantengan operativa de forma óptima y segura, gestionando el uso eficiente de los recursos y garantizando la calidad de los servicios ofrecidos.

1.1. Introducción

Grupo de trabajo (Workgroups).

Por defecto, todos los ordenadores que forman parte del mismo grupo aparecen juntos cuando se exploran en "mis sitios de red" o en "red".

La administración de cada ordenador es local e independiente y exporta y comparte recursos concretos. El usuario remoto debe disponer de una cuenta y permisos suficientes.

Este tipo de red tradicionalmente recibe el nombre de red peer to peer.

Dominio

Es la forma habitual de trabajar en una empresa grande. Hay un ordenador principal con Windows Server y en él se instala un controlador de dominio en el cual se introducen todos los equipos de ese dominio. Las cuentas que se creen en el ordenador sirven para inicial sesión en cualquier equipo del dominio. De manera que todos los usuarios podrían iniciar sesión en cualquier equipo controlador de dominio.

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

Para crear un dominio es necesario que al menos un servidor Windows Server se convierta en DC, para ello se ejecuta un asistente llamado dcpromo.

1.2. Ejercicio configuración Red. Instalación de 2 máquinas 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 ", 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.

MAC

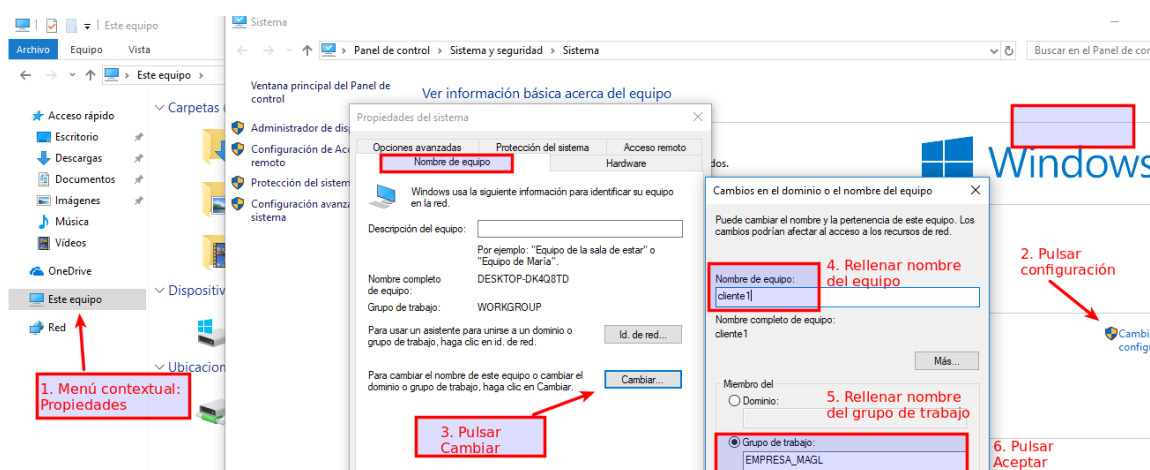
Paso 2. Configurar nombres de las máquinas y grupo de trabajo

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.



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 País y se devuelve el tiempo de respuesta.
- Comprobar que ambas máquinas tienen la misma dirección 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.

```
Administrador: Símbolo del sistema
C:\Windows\system32>ping www.google.es

Haciendo ping a www.google.es [216.58.201.163] con 32 bytes de datos:
Respuesta desde 216.58.201.163: bytes=32 tiempo=5ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=6ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=5ms TTL=127
Respuesta desde 216.58.201.163: bytes=32 tiempo=8ms TTL=127

Estadísticas de ping para 216.58.201.163:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 5ms, Máximo = 8ms, Media = 6ms

C:\Windows\system32>ping www.googleee.es
La solicitud de ping no pudo encontrar el host www.googleee.es. Compruebe el nombre y
vuelva a intentarlo.

C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:
    Sufijo DNS específico para la conexión. . . : Home
    Vínculo: dirección IPv6 local. . . . : fe80::5d05:ad0c:2420:f52a%2
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . : 10.0.2.2
```

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.

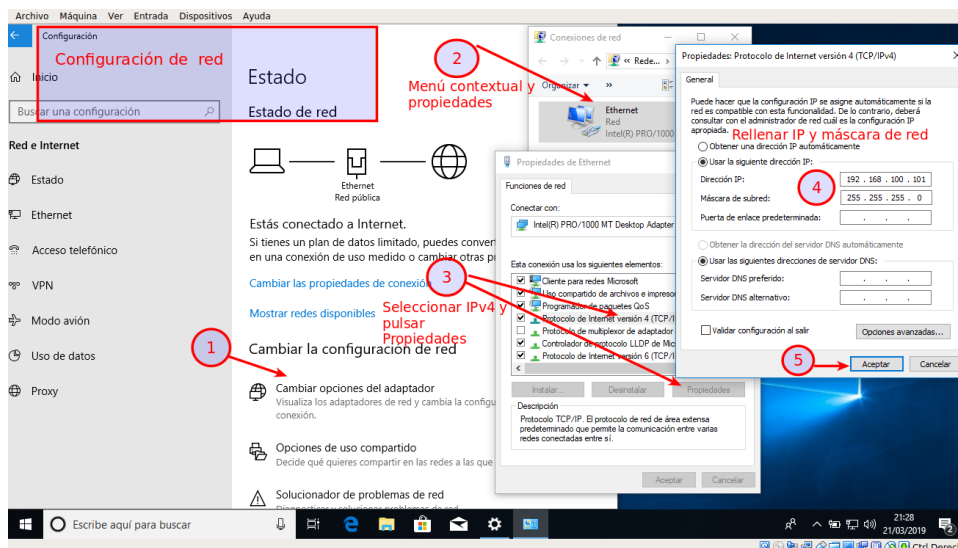
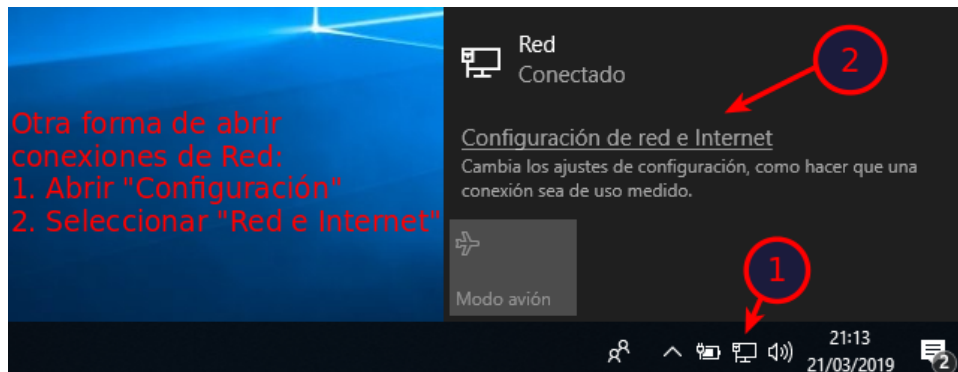
Paso 6. Comprobar que ahora no hay conexión a Internet.

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.

```
C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . : fe80::99af:b84d:e817:3c30%2
    Dirección IPv4. . . . . : 192.168.100.102
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

C:\Windows\system32>ping 192.168.100.101

Haciendo ping a 192.168.100.101 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.100.102: Host de destino inaccesible.

Estadísticas de ping para 192.168.100.101:
```

IP 19.168.100.102 configurada en cliente2

ping a máquina cliente1 con IP 192.168.100.101 no responde

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 "Personalizada"

ICMP

- 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.

```
C:\Windows\system32>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::99af:b84d:e817:3c30%2
    Dirección IPv4. . . . . : 192.168.100.102
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

C:\Windows\system32>ping 192.168.100.101

Haciendo ping a 192.168.100.101 con 32 bytes de datos:
Respuesta desde 192.168.100.101: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.101: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.101: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.100.101: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.100.101:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
```

IP 192.168.100.102 configurada en cliente2

ping a máquina cliente1 con IP 192.168.100.101 responde

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

2. Compartir recursos en la red

Hablar de recursos compartidos en red es hablar de ficheros, carpetas y dispositivos en un equipo a disposición de todo el que se conecta a través de la red, o solo de algunos de ellos.

para hacer que un recurso sea compartido hay que ponerlo accesible a través de la red. Los usuarios con permisos adecuados podrán acceder a su contenido, o utilizarse remotamente en caso de los dispositivos.

En un entorno de red es preciso definir permisos de acceso y privilegios sobre los recursos compartidos. Solo puede ser utilizado por quien tenga derecho y bajo condiciones fijadas.

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.

Estudiaremos la **solapa “Compartir”**, que sirve para configurar los permisos cuando accedemos 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 , esta ruta está formada por
\\NombreEquipo\NombreRecurso
UNC
- 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

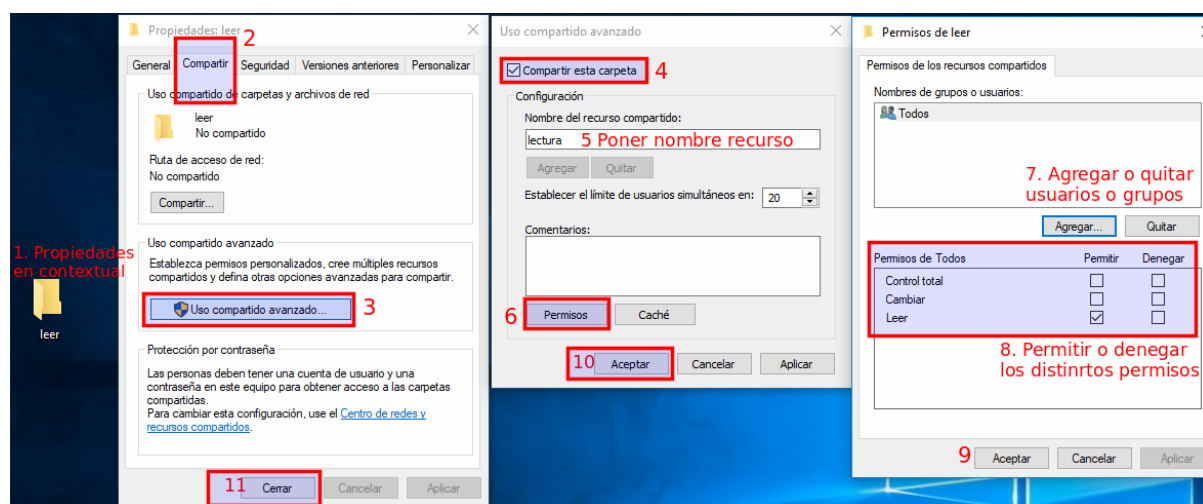
- El permiso de lectura permite:
 - Ver los nombres de archivos y de subcarpetas
 - Recorrer las subcarpetas
 - Ver los datos de los archivos

- 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

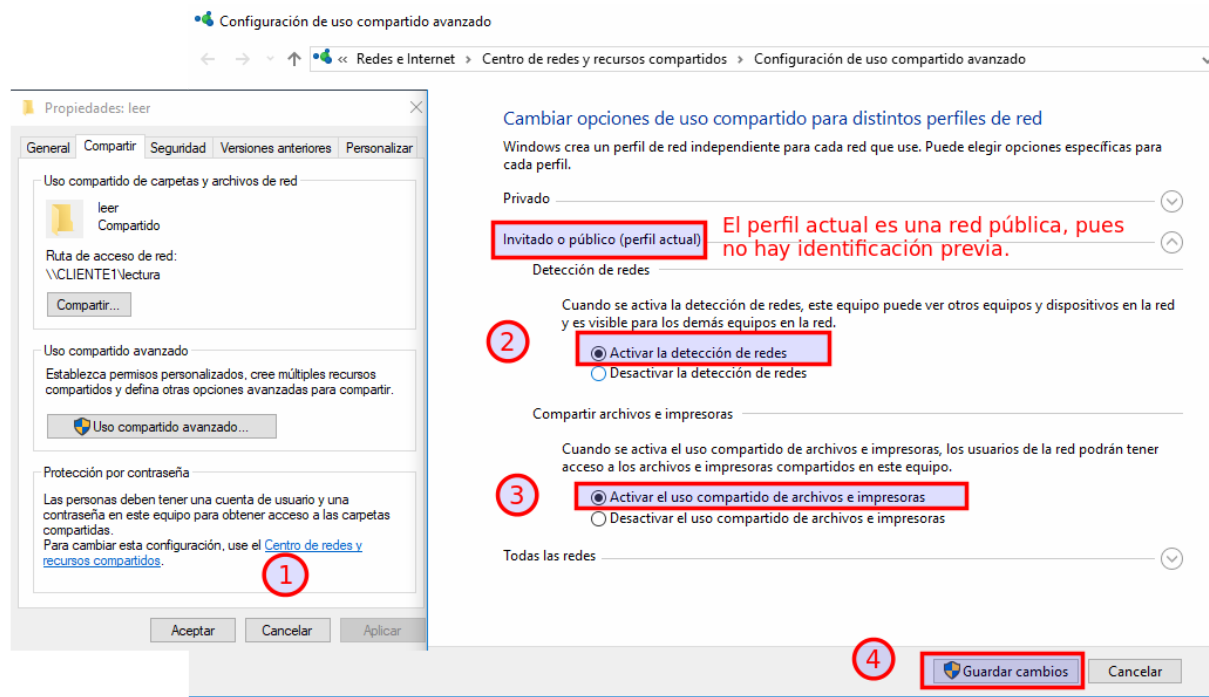
¿Cómo compartir un recurso?

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.

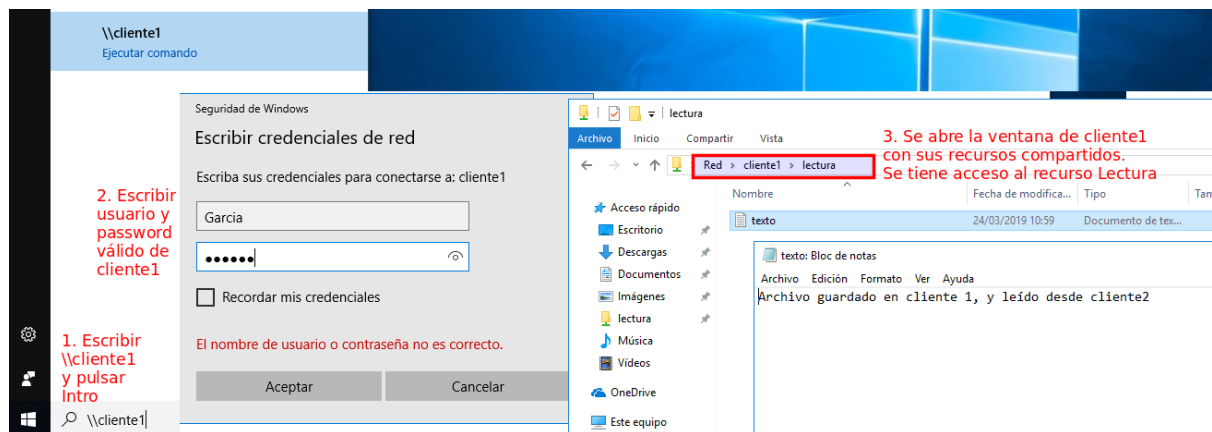


Como acceder a las carpetas compartidas en otro equipo

Desde un ordenador de la red, se puede acceder 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.

3. Servicios de redes

Los servicios de red son importantes en toda infraestructura de red, gracias a ellos los diferentes ordenadores se comunican.

Dentro de los servicios de red podemos gestionarlos y también sus puertos.

3.1. Arquitectura cliente - servidor

Los servicios son procesos, programas en ejecución de forma transparente para el usuario, muchos se activan de forma automática y otros a petición del usuario en función del rendimiento del equipo, tráfico 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 (servidores) y los solicitantes de estos (clientes).

La separación entre cliente y servidor es de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina o un solo programa.

Puertos

Cada sistema operativo ofrece puertos virtuales o lógicos, solo existen de manera virtual para el ordenador. Los S.O. cuentan con más de 65000 puertos para abrir conexiones y se las ceden a los programas para volcar datos en la red.

Los programas solicitan y el S.O. los gestiona para poder utilizarlos y establecer una conexión lógica. Esto permite que se puedan comunicar con otro ordenador peer to peer.

La comunicación entre distintos dispositivos se traduce en un flujo de datos entre dos puertos virtuales abiertos por alguna aplicación.

Los programas que comienzan comunicación en un puerto se llaman clientes y los programas que usan el puerto esperando a que los clientes conecten a él son servidores (a la escucha).

Un ejemplo es un servidor web a la espera de que el cliente (navegador) se conecte para mostrar contenido web, a través del puerto 80.

El número de puertos se codifica con 16 bits, lo que significa que hay $2^{16} = 65536$ posibles puertos.

Los puertos del 0 al 1023 son puertos conocidos o reservados para servidores. Un administrador de red puede conectar servicios con puertos a su elección.

Del 1024 al 49151 son puertos registrados. Los programadores cuando programan algún servicio utilizan puertos registrados.

Los puertos del 49152 al 65535 son dinámicos y/o privados.

Del lado del cliente el S.O. el elige el puerto entre los disponibles de manera aleatoria, nunca entre el 0 y el 1023, reservado para servidores.

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 y hay que averiguar el motivo por si hay alguien ajeno aprovechándose del ancho de banda o si se está siendo víctima de ataques como sniffing, spoofing IP DoS

Se deben utilizar herramientas de análisis de red, las cuales realizan un estudio detallado del tráfico que circula por la red.

La monitorización sirve también para mantenimiento preventivo como dimensionamiento de red: puede ocurrir que el ancho de banda insuficiente o si está sobredimensionado.

Algunas herramientas conocidas:

Wireshark

Analizador de protocolos para solucionar problemas de redes y telecomunicaciones. Tiene interfaz gráfica y opciones de organización y filtrado. También permite ver todo el tráfico de red.

Incluye un completo lenguaje para filtrar lo que queremos ver y habilidad de mostrar el flujo reconstruido de una sesión TCP. Es software libre y se ejecuta en la mayoría de S.O.

Nmap

Programa de código abierto para efectuar rastreo de puertos. Difícilmente detectable y creado para evadir Sistemas de detección de intrusos. Interfiere lo menos posible con operaciones normales.

Nagios

Software libre para linux, permite monitorizar la red y configurar advertencias.

Estas herramientas de monitorización dan info 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.)

3.2. Servicios de infraestructura de red

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

- **Encaminamiento.** Permite al servidor actuar como router y permite la comunicación entre dos o más redes. La puerta de enlace es normalmente la dirección del router por la que salimos a internet.
- **Servidor DHCP.** Asigna automáticamente la configuración IP de los equipos clientes en la red. Los router de las compañías suelen tener instalado este servidor, de manera que cuando se conecta un ordenador a dicha red, el servidor DHCP asigna una IP al ordenador.
- **Servidor DNI,** es un equipo en internet que facilita la navegación web, traduce las direcciones web a las direcciones IP. En los domicilios particulares no es necesario especificar la IP del servidor DNS, ya que suele estar indicado en el router.

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

El mantenimiento en una red grande conlleva un trabajo complicado cuando se hace algún cambio en la configuración de red. Por otra parte, utilizar IP estáticas conlleva obtener un mal aprovechamiento de las direcciones IP de la red. Por ejemplo utilizando IP dinámicas podemos asignar una dirección IP que cuando se apaga 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 IP:

Asignación dinámica, asigna IP's libres en un rango de direcciones establecidos por el administrador.

Reserva por dirección IP. Consiste en asignar la misma IP a un equipo concreto, para ello utiliza la dirección MAC. Útil sobre todo para dispositivos como impresoras.

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

Si ejecutamos ping a www.educa.madrid.org vemos que el equipo responde 213.229.136.36, su dirección correspondiente.

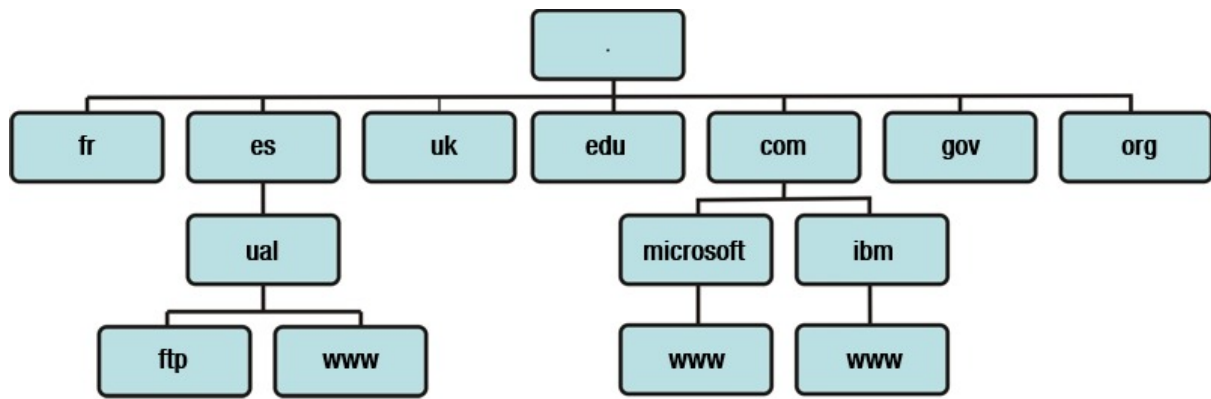
Para navegar es más fácil memorizar el nombre de la página que su IP y ofrece mayor flexibilidad, pues si cambia el alojamiento, cambia la IP pero no el nombre.

Inicialmente la asociación la realizaban los ordenadores a través de un fichero, esa opción presentaba el problema que cualquier cambio significaba cambiar el fichero en todos los ordenadores.

El sistema de resolución de nombres DNS basado en dominios surge para resolver ese problema. Se dispone de uno o más servidores encargados de resolver los nombres de los equipos de su ámbito.

Espacio de nombres de dominio

Al igual que los ficheros de los S.O. se organizan en árboles jerárquicos, también lo hace el sistema de nombres de dominio, en el que las distintas ramas 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 los dominios por los que pasamos, desde las hojas hasta la raíz del árbol, usando punto como separador.



Dependiendo de la profundidad del árbol se habla de dominios de primer, segundo o tercer nivel.

En el primer nivel nos encontramos que los nombres de los nodos ya están establecidos de antemano. Existen dos tipos de divisiones, geográfica (.es, .uk...) y organizativa: (.com, .int, .org, .edu...)

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

Cada rama recibe el nombre del dominio y la asignación de redes delega en un responsable, para España es la empresa pública REDES que a su vez delega la resolución de nombres de las distintas ramas en otras corporaciones.

Una característica crucial es la máxima disponibilidad del servicio DNS, existen varios servidores capaces de realizar el mismo servicio, aunque la autoridad de resolución de nombres recaiga en un servidor principal. Estos servidores con autoridad reciben el nombre de servidores primarios y el resto son secundarios.

Cada vez que se modifica un dato en el servidor primario se transmite a los secundarios para que no haya problemas de sincronización.

Registrar un dominio

Cualquier persona física con residencia en España, o empresas constituidas pueden solicitar registros de dominio a través de nic.es o por medio de agentes registradores. Los nombres deben corresponder con:

- Nombre o abreviatura de una empresa que la identifique de manera inequívoca.
- Nombres comerciales o de marcas

- Nombres de personas tal y como aparecen en el dni con un máximo de 60 caracteres
- Nombres de profesiones y el apellido o nombre del profesional.

3.3. Servicio FTP (File Transfer Protocol, protocolos de transferencia de ficheros)

Para transferir ficheros por internet, tenemos dos opciones. Uno es mediante el uso de un servidor FTP, un servidor de archivos o ficheros que permite compartir recursos, dentro de una red local, o el servicio FTP que permite conectarse a un equipo y transferir desde éste hacia el cliente o en sentido inverso.

El protocolo FTP establece doble conexión TCP entre cliente y servidor.

- **Conexión de control.** Suele emplearse el puerto 21 del servidor e indica a éste las operaciones que se deben llevar a cabo.
- **Conexión de datos.** Se usa normalmente el puerto 20 del servidor y sirve para transferir ficheros desde o hasta el servidor.

Existen dos tipos de autenticación.

- **Anónimo.** La comunicación se realiza sin identificación, el usuario tiene pocos privilegios en el servidor, solo puede descargar archivos pero no puede escribir o modificar. El directorio público se suele llamar pub.
- **Acceso autorizado.** Establece comunicación con una cuenta de usuario. Tras identificarse se confina al usuario a su directorio predeterminado, en el cual puede descargar ficheros e incluso, si la política implantada lo permite, puede escribir.

Los parámetros de autenticación y permisos se establecen en la configuración del sitio FTP en el equipo servidor.

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

El servicio web es el más utilizado de los que se ofrecen en internet. Un servidor web aloja y proporciona páginas web solicitadas por clientes desde navegador. Un servidor web maneja el protocolo HTTP y cuando recibe una petición responde con una respuesta HTTP, normalmente una página HTML

estática, una imagen, redireccionando o delegando en generación dinámica como FGI, JSP, ASP, PHP, etc... las cuales generan una página dinámica del lado servidor y envían la página resultante en HTML al cliente.

La variante es HTTPS (secure), la cual protege la integridad y confidencialidad de datos entre cliente y servidor.

Servidor web

Los más conocidos son:

- Apache, software libre multiplataforma para Windows, Linux y MacOS
- Nginx, software libre multiplataforma.
- IIS. Internet Information Server, de Microsoft para Windows.

Clientes web

Son los navegadores web: firefox, chrome, Internet Explorer, etc...

Sus diferencias son las vulnerabilidades que presentan y matizaciones de representación de código HTML. También incluyen interpretación de scripts en cliente como JavaScript.

3.5. Servicio de correo electrónico

Es junto al servicio web, el más utilizado a nivel de usuarios.

Es un servicio de transferencia de mensajes, rápido y eficiente, bajo arquitectura cliente servidor.

Servidor de correo

Tiene los siguientes componentes y trabaja con varios protocolos:

Servidor de correo saliente. El cliente envía un email al servidor y el servidor envía el correo al destinatario. Protocolo SMTP.

Servidor de correo entrante. Almacena los correos en buzones de usuarios y cuando el cliente conecta se le envían los correos recibidos. Utiliza POP e IMAP.

Clientes de correo

En la actualidad se utiliza el correo web de forma masiva, pero las empresas suelen utilizar clientes de correo.

Cuando se envía un mensaje, se envía al servidor, después según el tipo de correo, el servidor envía al destinatario el mensaje o lo solicita el destinatario al

servidor.

Correo web. El más utilizado a nivel particular, se conecta al servidor con un navegador web, accede y administra a su correo. La información siempre está en el servidor.

Clientes de correo. Se instala el software de correo en el ordenador y el cliente se conecta al servidor descargándose en su propio equipo.

Los más conocidos son: Evolution, Microsoft Outlook y Mozilla Thunderbird.

Es el sistema más habitual en empresas.

3.6. Acceso remoto

Permiten controlar y administrar otro ordenador a través de la red. Para realizar esta conexión se usan distintas aplicaciones, con el software servidor en el equipo a controlar y el software cliente en el equipo que va a llevar el control.

Acceso remoto en modo terminal

Se usan los servicios Telnet y SSH.

Telnet es una app TCP/IP y se utiliza en Linux y Windows, se usa muy poco por ser inseguro.

SSH tiene la misma funcionalidad e igualmente es el nombre de un protocolo y de un programa, pero se le ha añadido el cifrado de las conexiones para evitar que los datos sean interceptados. También maneja mecanismos de autenticación más seguros. SSH es software libre.

La ventaja del acceso remoto por terminal es la fluidez de la comunicación.

Acceso remoto en modo gráfico

Las más conocidas son:

- Escritorio remoto y Terminal Server incluidas en las versiones más completas de Windows.
- VNC, software libre para Windows y Linux.
- Teamviewer, aplicación externa de Windows.

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

En este tutorial se va a instalar y configurar el servidor FTP que viene con Windows 10.

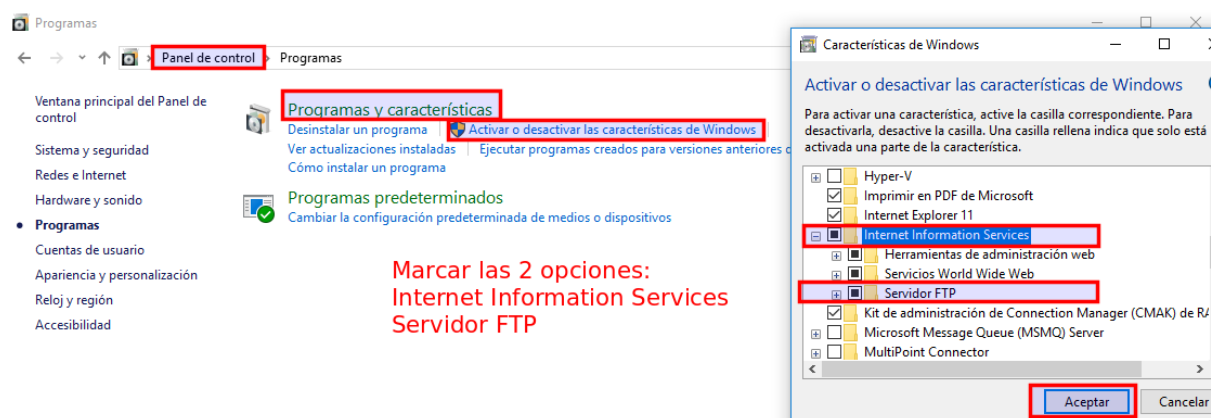
Este tutorial corresponde a un ejercicio de la tarea.

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.

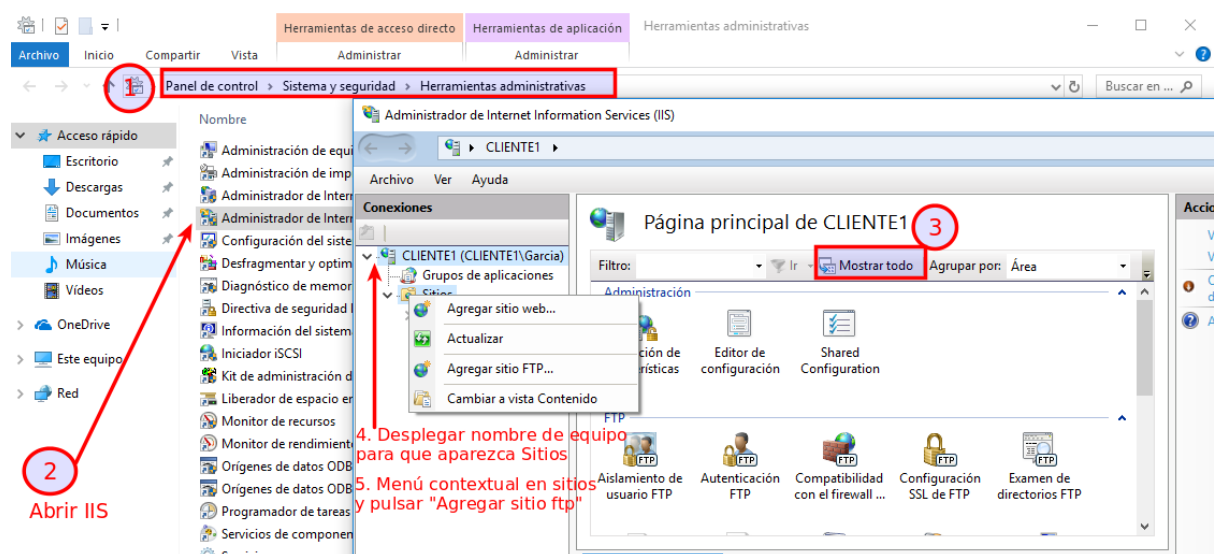


Cuando se pulsa Aceptar, se instala el servidor.

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".

Nombre del sitio FTP:
ftp.empresa_MAGL.es

Directorio de contenido
Ruta de acceso física:
C:\empresa_MAGL

Rellenar nombre del servidor y ruta.

Pulsar siguiente.

Paso 4. Ventana "Configuración de enlaces y SSL"

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

**Configuración de enlaces y SSL**

Enlace

Dirección IP: Puerto:

☐ Habilitar nombres de host virtuales:

Host virtual (ejemplo: ftp.contoso.com):

☒ Iniciar sitio FTP automáticamente

SSL

☒ Sin SSL

☐ Permitir SSL

☐ Requerir SSL

Certificado SSL:

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 autenticación y autorización"

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

Agregar sitio FTP ? X



Información de autenticación y autorización

Autenticación

☐ Anónima

☒ Básica

Autorización

Permitir el acceso a:

v

Permisos

☒ Leer

☒ Escribir

Anterior
Siguiente
Finalizar
Cancelar

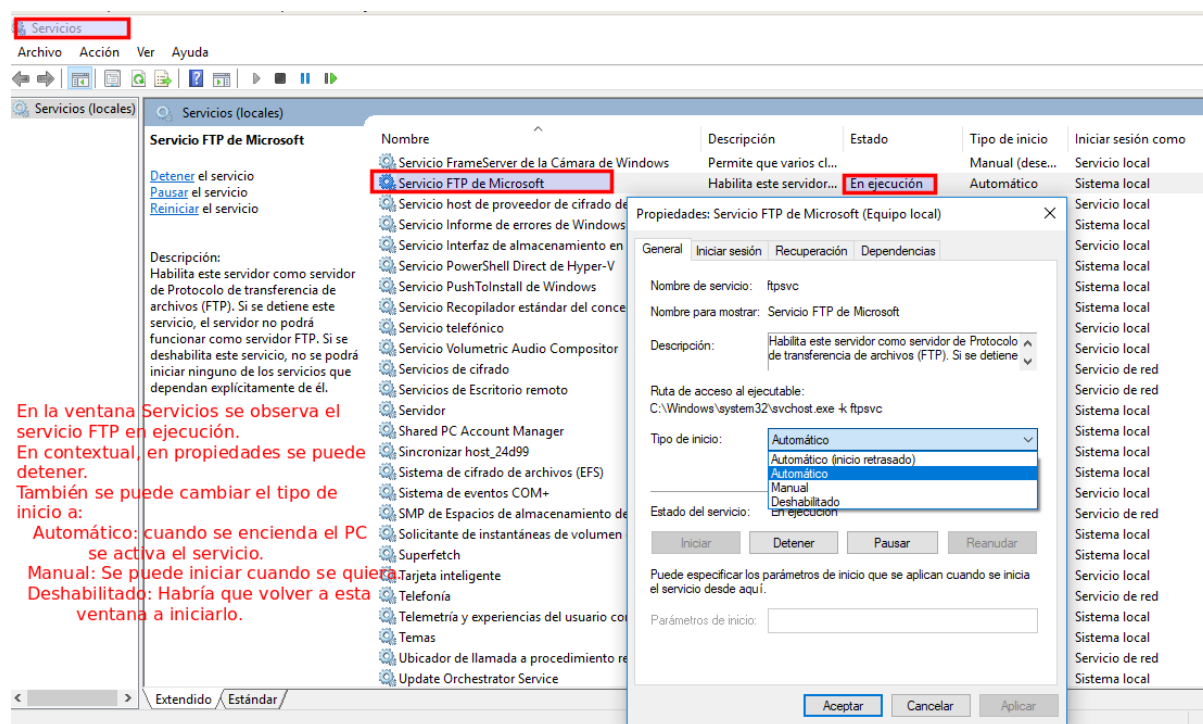
Explicación de las distintas opciones:

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.

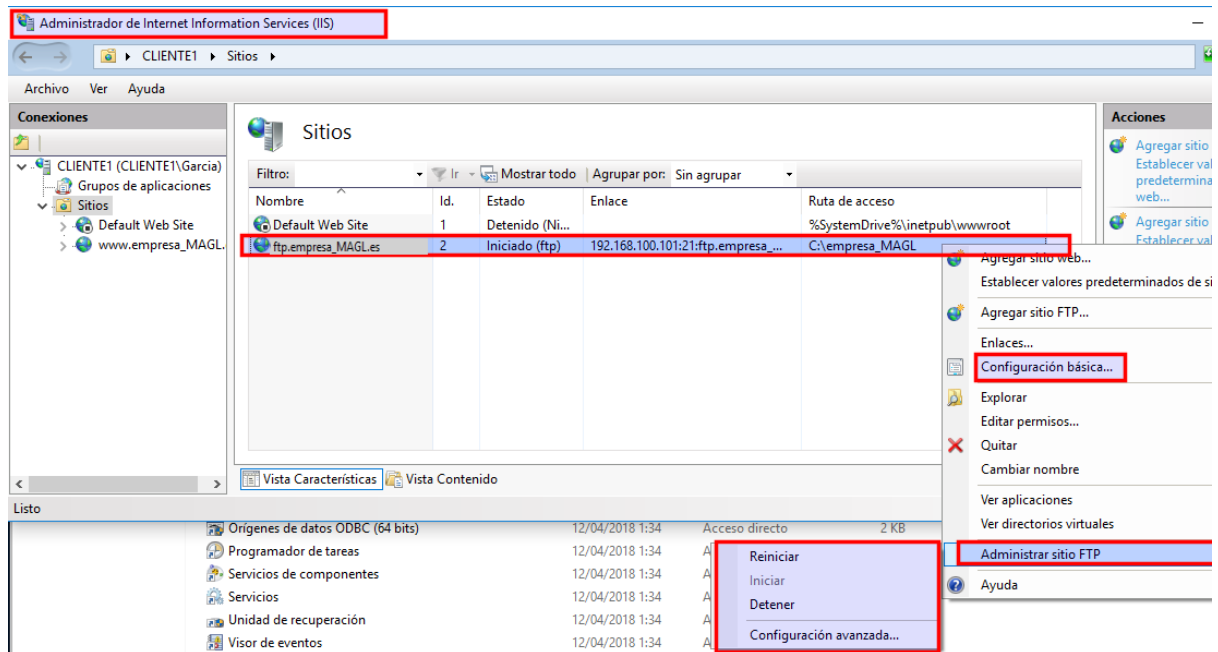


Paso 7. Configuración y control del sitio FTP.

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.

```
Administrador: Símbolo del sistema

c:\Users\Garcia>echo hola > archivo.txt Se crea archivo.txt en máquina local 192.168.100.102

c:\Users\Garcia>ftp 192.168.100.101 Se conecta al servidor ftp 192.168.100.101
Conectado a 192.168.100.101.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Usuario (192.168.100.101:(none)): supervisor
331 Password required
Contraseña:
230 User logged in. Autenticación: Usuario supervisor
Password: super1

ftp> ls
200 PORT command successful. Listado en servidor: vacío
125 Data connection already open; Transfer starting.
226 Transfer complete.

ftp> put archivo.txt
200 PORT command successful. Se sube archivo.txt al servidor
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp: 7 bytes enviados en 0.07segundos 0.10a KB/s.

ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
archivo.txt
226 Transfer complete. Listado en servidor: archivo.txt
ftp: 16 bytes recibidos en 0.00segundos 16000.00a KB/s.

ftp> bye
221 Goodbye. Salir del servidor con bye. Vuelve la shell de Windows.

c:\Users\Garcia>
```

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 TCP/OP 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.

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

Comando hostname

Devuelve el nombre del equipo

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 añadir datos.

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)

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>

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.

Mapa conceptual

