**Unidad Didáctica 6. Compartición de recursos en red mediante el protocolo**

**CIFS/SAMBA**

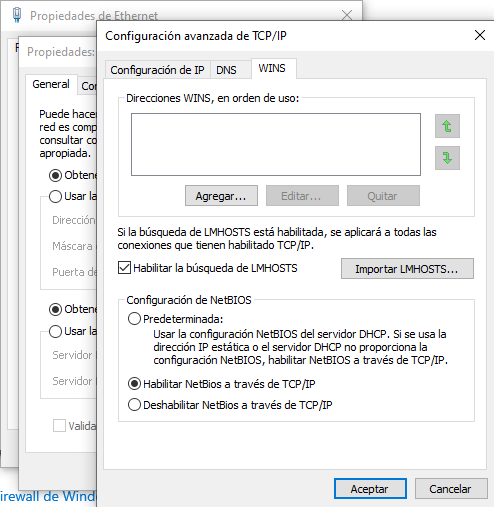
**Ejercicio 1. Investiga y amplía la información comentada sobre NetBIOS. ¿Para qué sirve el comando nbtstat? Prueba y estudia sus diversas opciones.**

NetBIOS permite que las computadoras se encuentren y se comuniquen entre sí en la misma red utilizando identificadores únicos llamados nombres NetBIOS. Este protocolo opera en la capa de sesión (capa 5) del modelo OSI y utiliza puertos UDP 137, 138 y el puerto TCP 139 para proporcionar sus servicios.

1. **Resolución de Nombres:** NetBIOS permite que las computadoras resuelven nombres NetBIOS en direcciones IP utilizando varios métodos, como caché local, servidores WINS o difusiones.
2. **Establecimiento de Sesiones**: Después de resolver un nombre NetBIOS, se puede establecer una sesión entre dos computadoras. Esta sesión permite que las computadoras intercambian mensajes, datos y comandos.
3. **Distribución de Datagramas**: NetBIOS admite la comunicación sin conexión a través de la distribución de datagramas. Permite que las computadoras envíen paquetes, conocidos como datagramas NetBIOS, a otras computadoras sin establecer una sesión.

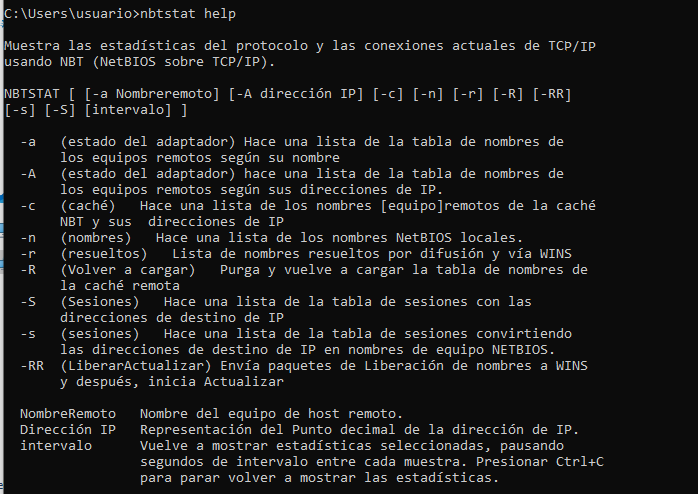
Para activar NetBios en Windows debemos seguir los siguientes pasos: Ve a las propiedades de la conexión de red → En Protocolo de Internet (TCP/IPv4), haz clic en Propiedades → Ve a Opciones avanzadas > WINS y Habilitar NetBIOS sobre TCP/IP

**Esta configuración será aplicado a las dos máquinas Windows**



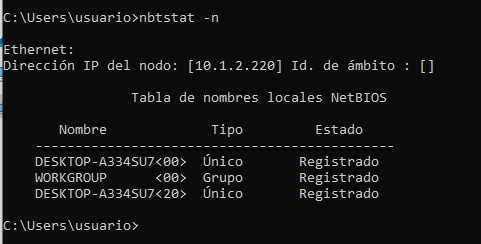
**Comando nbtstat**

El comando nbtstat se utiliza para diagnosticar y resolver problemas relacionados con NetBIOS sobre TCP/IP (NBT). Proporciona información sobre las conexiones y la tabla de nombres NetBIOS que está usando un dispositivo, lo que es útil para administrar redes y solucionar problemas de comunicación entre equipos en una red local o remota



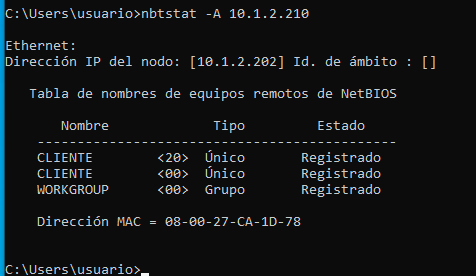
Como podemos ver, tenemos diferentes opciones de uso para este comando, las más comunes de usar son: -a, -A, -n, -s

1. **Mostrar la tabla de nombres NetBIOS registrados localmente**



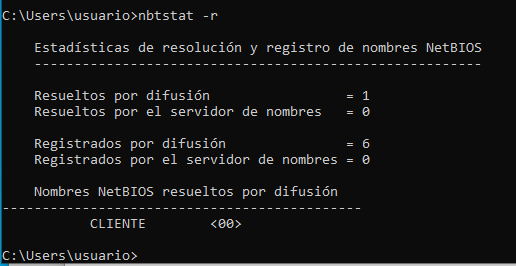
Muestra los nombres NetBIOS registrados localmente y su estado, incluyendo nombres únicos y de grupo.

1. **Listar la tabla de nombres NetBIOS de un equipo remoto**



Devuelve la lista de nombres NetBIOS asociados con la dirección IP indicada, incluyendo los roles de los dispositivos.

1. **Ver conexiones y estadísticas NetBIOS actuales**



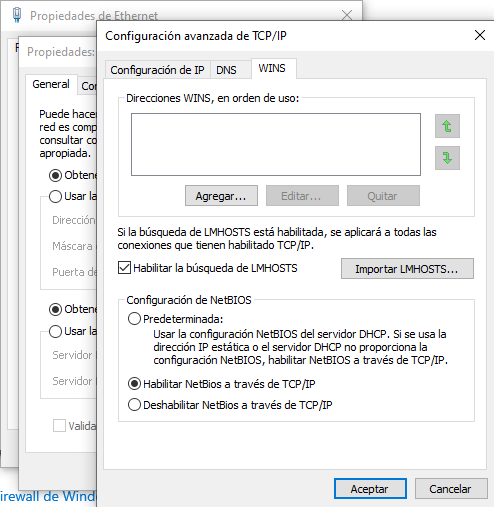
Muestra información sobre las sesiones actuales, como las direcciones IP y los nombres NetBIOS involucrados en la comunicación.

En este caso muestra el nombre de la máquina llamada “Cliente” de la red.

**Ejercicio 2. Muestra y comenta cómo activar “NetBIOS a través de TCP/IP”. Además de lo anterior, detalla cómo configurar las opciones de uso compartido avanzadas, características de Windows “SMB 1.0/CIFS” y servicios relacionados con la activación de la detección de redes.**

***Activar NetBIOS***

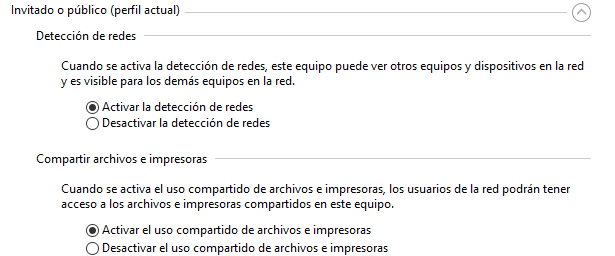
Para activar NetBios en Windows debemos seguir los siguientes pasos: Ve a las propiedades de la conexión de red → En Protocolo de Internet (TCP/IPv4), haz clic en Propiedades → Ve a Opciones avanzadas → WINS y Habilitar NetBIOS sobre TCP/IP

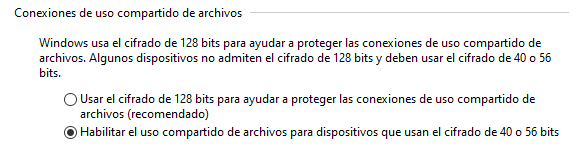


***Opciones de uso compartido avanzadas***

Para configurar las opciones de uso compartido en Windows seguiremos los siguientes pasos: Ve a Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Haz clic en Cambiar configuración de uso compartido avanzado

Una vez aquí activaremos: Detección de redes y uso compartido de archivos e impresoras

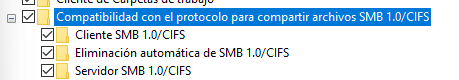




***Habilitar características de Windows “SMB 1.0/CIFS”***

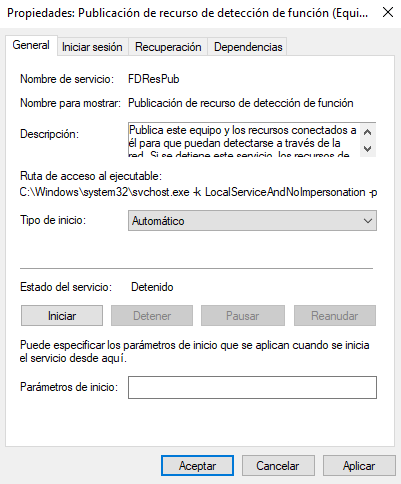
Para habilitar estas características seguiremos los siguientes pasos: Ve al Panel de control → Programas → Activar o desactivar las características de Windows.

Una vez aquí, activa la característica de SMB 1.0. Al activar esta característica sería necesaria el reinicio del sistema



***Servicios relacionados con la detección de redes***

Para configurar esta característica entraremos en Servicios → Busca Publicación de recursos de detección de funciones → Establece el tipo de inicio en Automático y haz clic en Iniciar



A continuación, haremos lo mismo para Host del proveedor de detección de funciones.

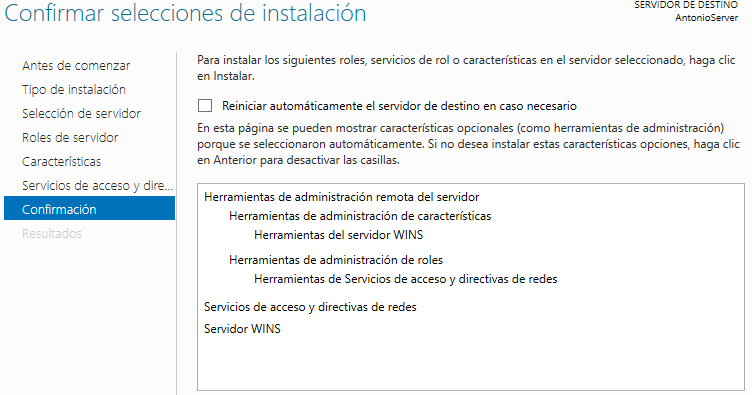
**Ejercicio 3. Teniendo en cuenta lo comentado en clase, comprueba la importancia del orden durante el arranque de las máquinas con sistemas Windows 10. ¿Qué conclusiones has sacado en relación con el protocolo NetBIOS?**

El orden de arranque de las máquinas en una red es crucial cuando se utiliza el protocolo NetBIOS, especialmente en redes donde no hay un servidor WINS configurado, las máquinas dependen de la resolución de nombres a través de transmisiones (broadcasts).

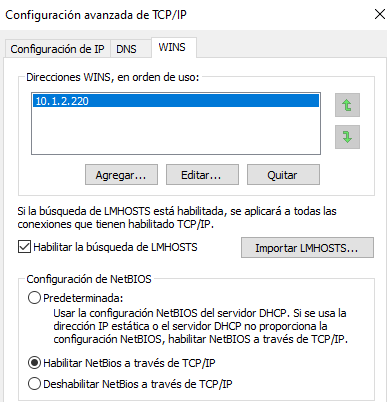
La secuencia de inicio también afecta a los servicios esenciales, como la detección de redes y el registro de nombres NetBIOS. Si estos servicios no están activos cuando se inician los clientes, las peticiones de red pueden fallar. En redes modernas, aunque NetBIOS sigue siendo compatible, la mayoría de las redes usan DNS y otros protocolos más eficientes para la resolución de nombres.

**Ejercicio 4. Instala y configura un servidor WINS en Windows Server. Configura las máquinas Windows 10 para que sean clientes de WINS. ¿Has notado algún cambio con respecto a lo observado en el ejercicio anterior?**

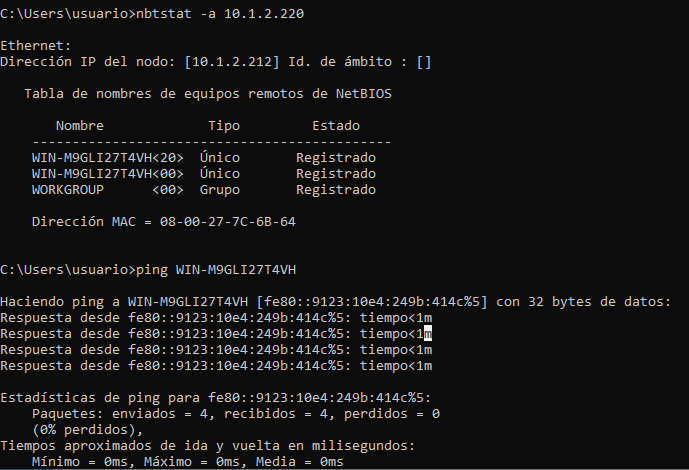
Instala en el servidor la característica de servicios en red y añade la característica de Servidor WINS



Una vez instalado, entramos en la máquina de Windows 10, aquí cambiaremos las propiedades de Internet y aplicamos la dirección del servidor donde hemos instalado WINS

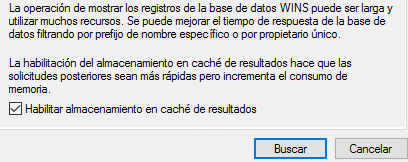


Para comprobar la conexión, desde la propia máquina cliente (Windows 10) usaremos el comando:

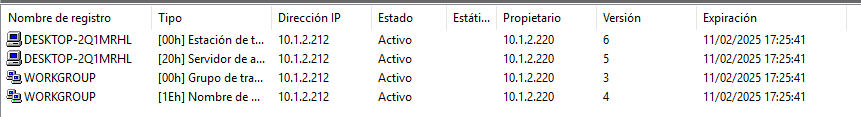


Con este comando podemos ver las entradas en la caché de nombres NetBIOS.

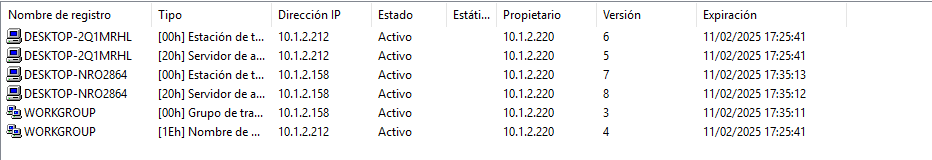
Por último entraremos en el servidor a la herramienta WINS, para ello aplicamos el siguiente filtro de búsqueda



Una vez activado podremos ver la conexión con el cliente



Si conectamos otro cliente al servicio con el mismo método veremos las nuevas conexiones



**Ejercicio 5. En un entorno donde no existe un servidor WINS, descarga la herramienta “Advanced port scanner” (https://www.advanced-port-scanner.com/es/). ¿Qué beneficios podríamos obtener a partir de su uso?**

Advanced Port Scanner es una herramienta útil que permite analizar una red local o remota para obtener información sobre los dispositivos conectados. En redes donde no existe un servidor WINS, esta herramienta ayuda a:

1. **Detectar dispositivos**: Encuentra todos los dispositivos conectados a la red, incluso si no tienen un nombre asociado.
2. **Escanear puertos**: Muestra qué puertos están abiertos en los dispositivos, lo que ayuda a identificar posibles riesgos de seguridad.
3. **Ver servicios activos**: Te dice qué servicios están funcionando en los puertos abiertos, lo que te permite conocer qué aplicaciones están corriendo.
4. **Evaluar seguridad**: Al detectar puertos abiertos y servicios activos, puedes identificar vulnerabilidades que podrían poner en riesgo la red.
5. **Obtener detalles**: Proporciona información sobre direcciones IP, sistemas operativos y versiones de software, facilitando la gestión de la red.