

TASK 6 - RDP ACCESS TO WINDOWS HOSTS

CHRISTIAN MILLÁN SORIA

1º DAW TARDE

1. Servidor remoto. ¿Qué es necesario configurar en el host de Windows al que queremos acceder?

Para configurar el acceso remoto en un host de Windows al que deseas acceder, debes seguir los siguientes pasos:

- Verifica la edición de Windows: Asegúrate de que el host de Windows tenga una edición compatible con el acceso remoto. En general, las ediciones profesionales, como Windows 10 Pro o Windows Server, admiten la función de Escritorio remoto, mientras que las ediciones domésticas, como Windows 10 Home, pueden tener limitaciones o requerir soluciones alternativas.
- Habilita la función de Escritorio remoto: Para habilitar el acceso remoto, haz lo siguiente:

Haz clic derecho en el menú "Inicio" y selecciona "Sistema".

En la ventana de Configuración del sistema, selecciona "Configuración avanzada del sistema".

En la pestaña "Remoto", marca la opción "Permitir que los usuarios se conecten de forma remota a este equipo".

Opcionalmente, puedes hacer clic en "Seleccionar usuarios" para especificar qué usuarios o grupos tienen permiso para acceder de forma remota.

- Configura el enrutamiento y acceso remoto (opcional): Si deseas permitir el acceso remoto desde fuera de tu red local, es posible que necesites configurar el enrutamiento y acceso remoto en tu enrutador o firewall para redirigir los puertos necesarios al host de Windows.
- Configura la red y la seguridad: Asegúrate de que el host de Windows esté correctamente conectado a la red y tenga una dirección IP válida. Además, considera configurar las medidas de seguridad apropiadas, como cortafuegos y software antivirus, para proteger el host de accesos no autorizados.

Una vez que hayas completado estos pasos, podrás acceder al host de Windows de forma remota utilizando una herramienta de acceso remoto como el Escritorio remoto de Windows, ingresando la dirección IP o el nombre de host del equipo al que deseas conectarte.

2. Reenvío de puertos del enrutador remoto. ¿Qué es el reenvío de puertos? ¿Qué acciones son necesarias realizar en el enrutador que actúa como puerta de enlace para el host de Windows al que queremos acceder?

El reenvío de puertos, conocido como "port forwarding" en inglés, es un procedimiento esencial para permitir el acceso remoto a un dispositivo o host en una red local desde Internet. Consiste en redirigir el tráfico entrante desde un puerto específico del enrutador hacia un host específico en la red.

A continuación, los pasos necesarios para configurar el reenvío de puertos en el enrutador que actúa como puerta de enlace para el host de Windows al que se desea acceder:

- Accede a la interfaz de administración del enrutador. Para ello, abre un navegador web e ingresa la dirección IP del enrutador en la barra de direcciones. Por lo general, la dirección IP predeterminada es 192.168.1.1 o 192.168.0.1, pero puede variar según el fabricante del enrutador.
- Inicia sesión en la interfaz de administración del enrutador utilizando las credenciales de acceso. Estas credenciales suelen ser proporcionadas por el fabricante o pueden haber sido configuradas previamente.
- Busca la sección de "Reenvío de puertos" o "Port Forwarding" en la configuración del enrutador. La ubicación exacta puede variar según el enrutador y la versión de firmware que estés utilizando.
- Dentro de la sección de reenvío de puertos, deberás agregar una regla de reenvío de puerto para el host de Windows al que deseas acceder. Esto implicará proporcionar la dirección IP local del host y el número de puerto que deseas reenviar.
- Especifica el protocolo de red que deseas reenviar, como TCP o UDP.
- Guarda la configuración y reinicia el enrutador si es necesario para que los cambios surtan efecto.

3. Lado del cliente. Explícame cómo conectar un servidor RDP utilizando un servicio de DDNS gratuito, ya que el sitio del servidor no tiene una IP pública fija.

Si el servidor no tiene una IP pública fija y deseas conectarte a través de RDP utilizando un servicio de DDNS gratuito, puedes seguir los siguientes pasos:

- Obtén una cuenta en un servicio de DDNS gratuito: Existen varios servicios gratuitos de DDNS disponibles, como No-IP, DynDNS y DuckDNS. Crea una cuenta en uno de estos servicios y configura un nombre de host personalizado.
- Configura el DDNS en tu router: Accede a la configuración de tu router y busca la sección de DDNS o Dynamic DNS. Allí deberás ingresar la información de tu cuenta de DDNS, incluyendo el nombre de host, el proveedor de DDNS y las credenciales de inicio de sesión. Guarda la configuración.
- Configura el reenvío de puertos en tu router: Para permitir el acceso RDP desde Internet, debes configurar el reenvío de puertos en tu router. Normalmente, esto se encuentra en la sección de "Reenvío de puertos" o "Virtual Server" de la configuración del router. Debes redirigir el puerto RDP (por defecto es el puerto 3389) al dispositivo que aloja el servidor RDP en tu red local. Asegúrate de guardar la configuración.
- Configura el cliente RDP: En tu PC cliente, abre el cliente RDP (por ejemplo, el "Escritorio remoto de Windows") e introduce el nombre de host que configuraste en el servicio de DDNS. Si el servicio de DDNS está funcionando correctamente, se asociará automáticamente con la dirección IP pública actualizada de tu servidor.
- Conéctate al servidor RDP: Una vez que hayas ingresado el nombre de host del DDNS en el cliente RDP, haz clic en "Conectar" y se establecerá la conexión RDP con el servidor a través de la dirección IP pública actualizada proporcionada por el servicio de DDNS.

4. Windows 10 Pro no permite múltiples conexiones de RDP, pero es posible aplicar un parche para solucionarlo. Lee sobre RDP Wrapper en el enlace adjunto y aplícalo.

En Windows 10 Pro, por defecto, solo se permite una sesión de RDP activa en un momento dado. Sin embargo, si deseas permitir múltiples conexiones RDP simultáneas, es posible aplicar un parche llamado "RDP Wrapper". Este parche permite modificar el archivo de configuración de Windows que controla el número de conexiones RDP simultáneas permitidas.

Para aplicar el parche RDP Wrapper, sigue los siguientes pasos:

- Descarga el archivo de RDP Wrapper desde el sitio web oficial: El archivo está disponible en GitHub en el siguiente enlace: <https://github.com/stascorp/rdpwrap/releases>.

Adicionalmente, adjunto el enlace que aparece en el classroom:

<https://github.com/stascorp/rdpwrap/pull/1160>

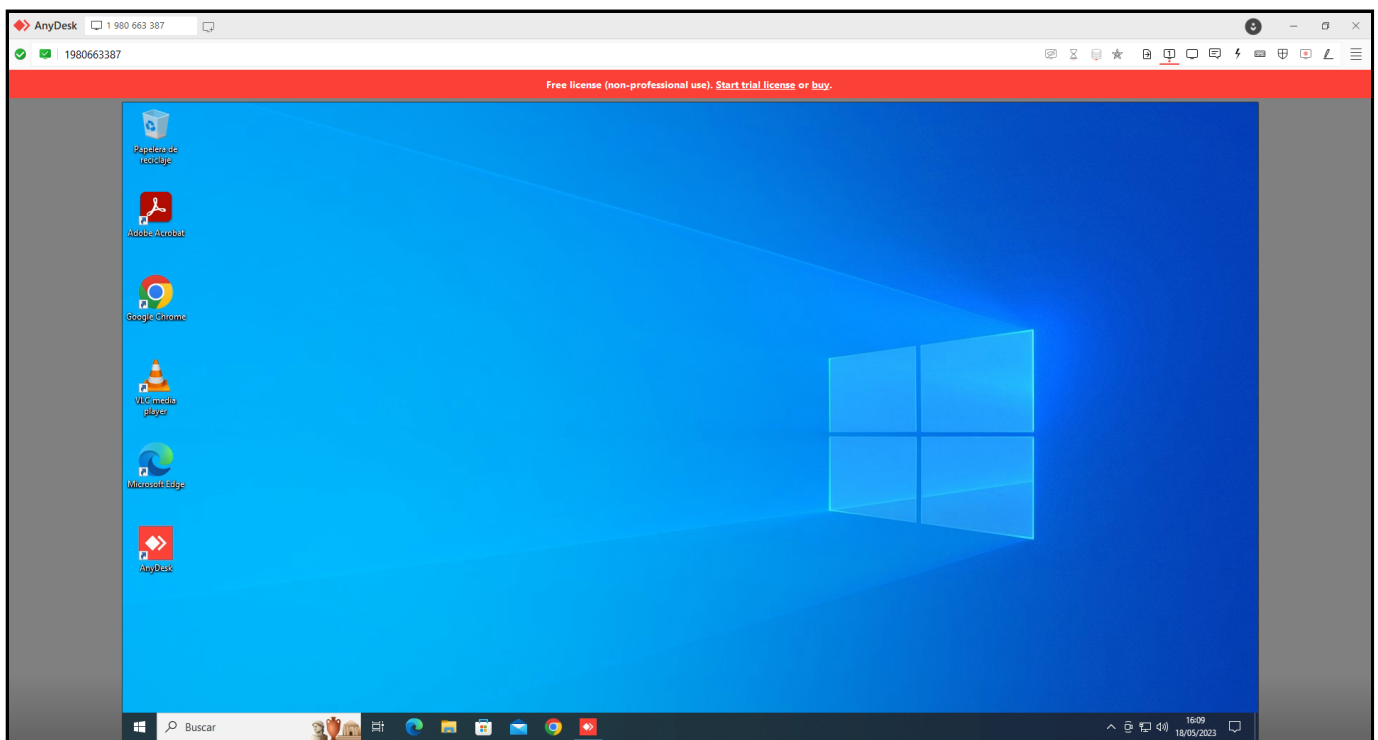
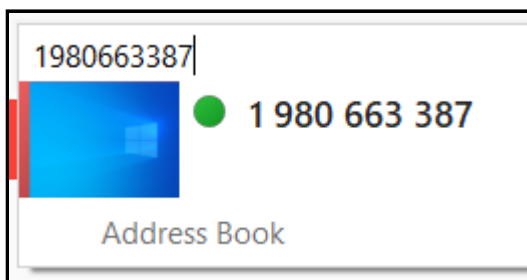
- Descomprime el archivo: Extrae el contenido del archivo ZIP descargado en una carpeta en tu PC.
- Ejecuta el instalador: Navega a la carpeta donde descomprimiste el archivo de RDP Wrapper y ejecuta el archivo "install.bat" con permisos de administrador. Este archivo agregará las entradas necesarias al archivo de configuración de Windows para permitir múltiples conexiones RDP simultáneas.
- Verifica que la instalación se realizó correctamente: Abre el archivo "RDPCheck.exe" en la misma carpeta y verifica que todos los valores muestren "OK". Si hay algún error, sigue las instrucciones que se muestran para solucionar el problema.
- Reinicia el equipo: Después de aplicar el parche, reinicia el equipo para que los cambios surtan efecto.

Una vez que hayas aplicado el parche RDP Wrapper, podrás conectarte a tu PC a través de múltiples sesiones de RDP de forma simultánea. Sin embargo, ten en cuenta que esto puede tener implicaciones de seguridad, ya que permite que múltiples usuarios accedan a la misma PC al mismo tiempo. Asegúrate de tomar las medidas de seguridad necesarias para proteger tu PC y la información que contiene.

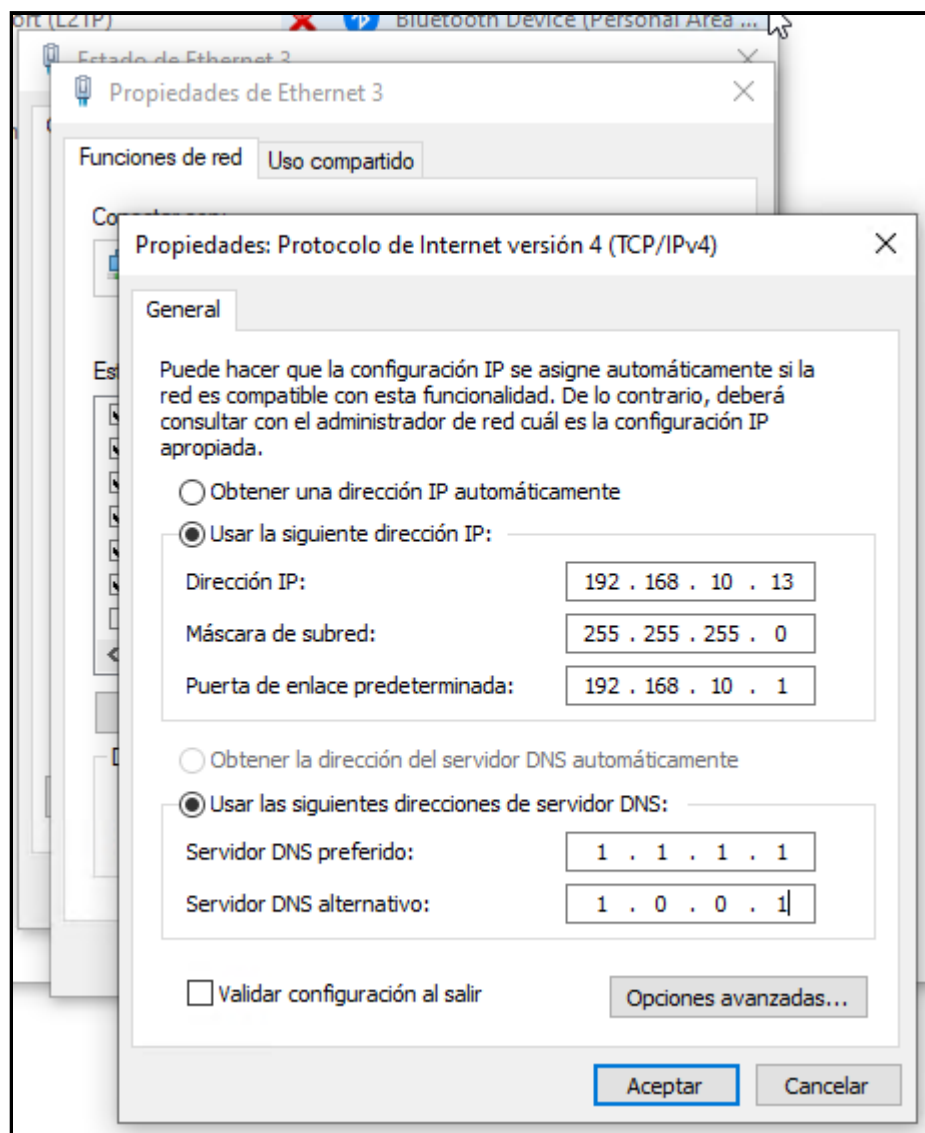
5. Conectar con una máquina externa por RDP (proceso completo).

Tenemos una máquina situada en una red externa a la que tenemos acceso mediante AnyDesk, pero no mediante RDP.

Para empezar, instalo AnyDesk y establezco conexión con dicha máquina.



Lo primero que hago dentro de la máquina es establecer una IP fija, para que no cambie mediante DHCP y la conexión se vea alterada.



Es importante también activar la opción de Escritorio Remoto para que esta conexión se pueda llevar a cabo.

Escritorio remoto

Escritorio remoto te permite conectar y controlar este PC desde un dispositivo remoto mediante un cliente de Escritorio remoto (disponible para Windows, Android, iOS y MacOS). Podrás trabajar desde otro dispositivo como si estuvieras trabajando directamente en este PC.

Habilitar Escritorio remoto

☒ Activado

☒ Mantener mi equipo activo para la conexión cuando está enchufado

[Mostrar configuración](#)


☒ Hacer que mi PC sea reconocible en redes privadas para permitir la conexión automática desde un dispositivo remoto

[Mostrar configuración](#)


Cambio los ajustes del plan de energía para prevenir que el equipo se apague o se ponga en modo suspensión tras un determinado tiempo, ya que este debe estar encendido indefinidamente.

Cambiar la configuración del plan: Equilibrado

Elija la configuración de modo de suspensión y de pantalla para su equipo.

 Apagar la pantalla:

2 horas

 Poner al equipo en estado de suspensión:

Nunca

Una vez realizados estos pasos, me dirijo a la configuración del router, ingresando la dirección 192.168.10.1 en la URL de un navegador. Inicio sesión.



Paso del modo básico de configuración al modo experto para poder acceder a todas las características.



Me dirijo al apartado de Internet.



Entro en el sub-apartado de Redirección de Puertos.

Móvil
Redirección de Puertos
DMZ
Control Parental
DNS & DDNS
UPnP
WoLAN

Lo que tengo que hacer aquí es crear una nueva regla dedicada al equipo servidor al que me quiero conectar.

Establezco que el protocolo que se va a usar es TCP, la IP fija que tiene ahora mi equipo, el puerto público por el que se conectarán los clientes a este servidor y el puerto LAN por el que se pasarán los paquetes de información sobre la conexión que se quiere realizar.

Los paquetes de la conexión entrarán por el puerto 5058 (puede ser cualquier puerto que no esté reservado de forma predeterminada para un protocolo), y una vez dentro de la red buscará el puerto 3389 (dedicado al protocolo RDP), que redirige los paquetes al equipo con IP 192.168.10.13.

Añadir asignación de puertos

Servicio

TCP

▼

Dispositivo

No hay dispositivo

▼

LAN IP

192

.

168

.

10

.

13

Tipo

☒ Puerto

☐ Intervalo de puertos

Puerto público

5058

Puerto LAN

3389

Guardar


Cancelar

TCP	192.168.10.13	TCP	3389	5058		
-----	---------------	-----	------	------	---	---

Por último, creo un nuevo usuario de nombre "remoto" y le establezco una contraseña fuerte, como "XX1269#r".

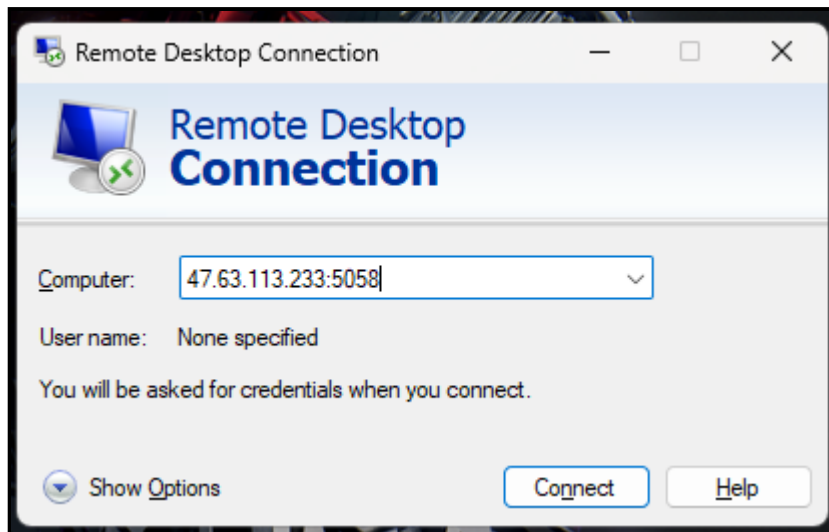
Otros usuarios

Permite que las personas que no forman parte de tu familia inicien sesión con sus propias cuentas. Esto no las agregará a tu familia.

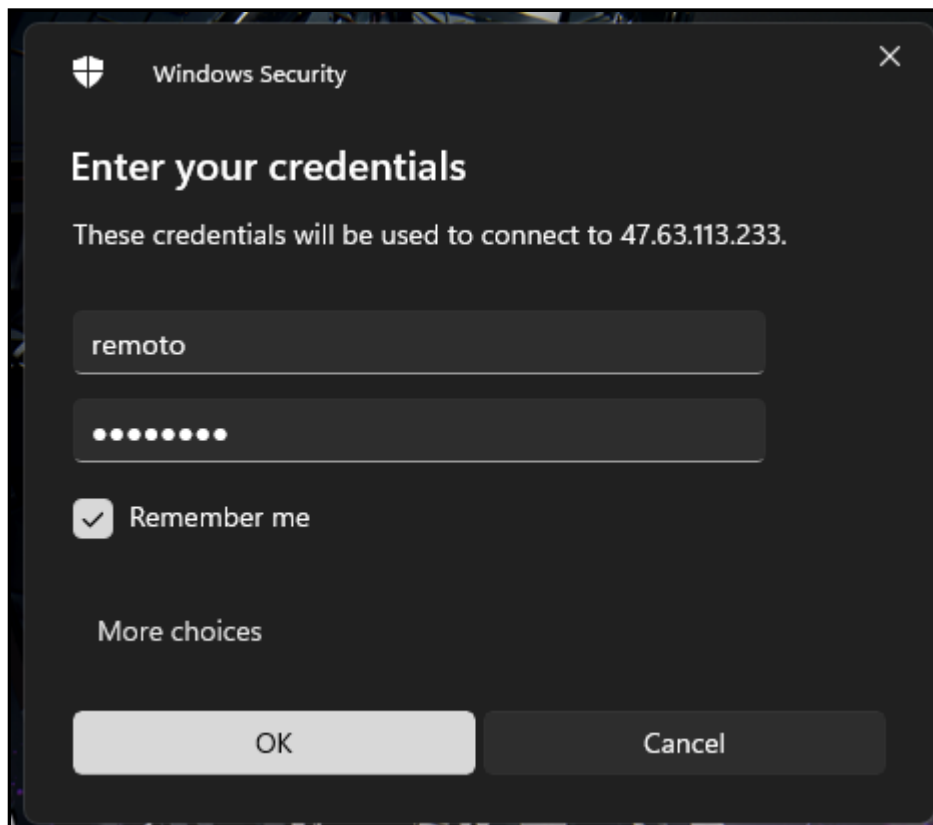


Agregar otra persona a este equipo

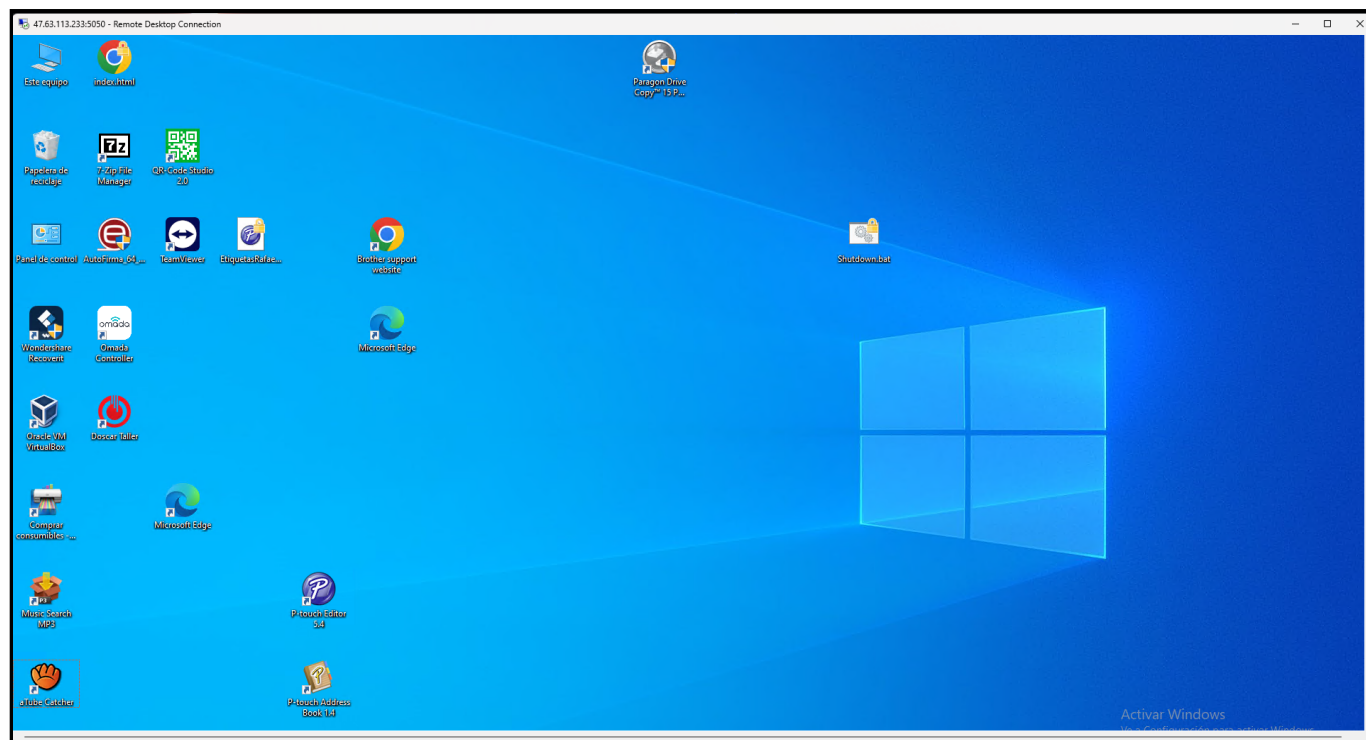
Procedo a, desde el equipo cliente/mi equipo personal, conectarme por Escritorio Remoto, escribiendo la IP pública del equipo servidor y el puerto por el que se enviarán los paquetes.



Escribo las credenciales de inicio de sesión.



Ya puedo acceder al equipo como si estuviera trabajando localmente con él.

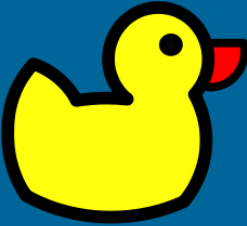


Debido a una medida de pago de Windows, este equipo no podrá mantener varias sesiones con el mismo usuario activas al mismo tiempo. Esto es una característica de pago de la que hablo en el ejercicio 4, con varios enlaces al wrapper, un parche NO OFICIAL que puede permitir que varias personas se conecten con el mismo usuario a la misma máquina sin echar el uno al otro.

Anteriormente vimos como, al establecer conexión por RDP desde la máquina cliente a la máquina servidor, lo hago escribiendo la IP pública de la red en la que se encuentra el equipo servidor.

Esto no es nada recomendable, debido a que cada cierto tiempo, la IP pública puede cambiar si no se ha contratado un servicio que la mantenga fija.

Para solucionar este problema, podemos acudir a Duck DNS, una página que permite crear un dominio con un nombre único en el mundo que suplanta la IP pública de la red para prevenir errores por los cambios de IP mencionados.



Duck DNS

account cmilsor245@g.educaand.es
type free
token 29c3c4b9-5464-4ec5-8219-cdd3407d376d
token generated 5 months ago
created date 28 Nov 2022, 19:49:04

domains 1/5

http://

sub domain

.duckdns.org

add domain

domain	current ip	ipv6	changed
christian1daw	<div>83.60.146.81</div> <div>update ip</div>	<div>ipv6 address</div> <div>update ipv6</div>	<div>6 seconds ago</div> <div>delete domain</div>

This site is protected by reCAPTCHA and the Google [Privacy Policy](#) and [Terms of Service](#) apply.

De esta forma, la conexión se realizaría, en lugar de escribiendo la IP pública de la red a la que nos queremos conectar, escribiendo el nombre del dominio creado en Duck DNS.