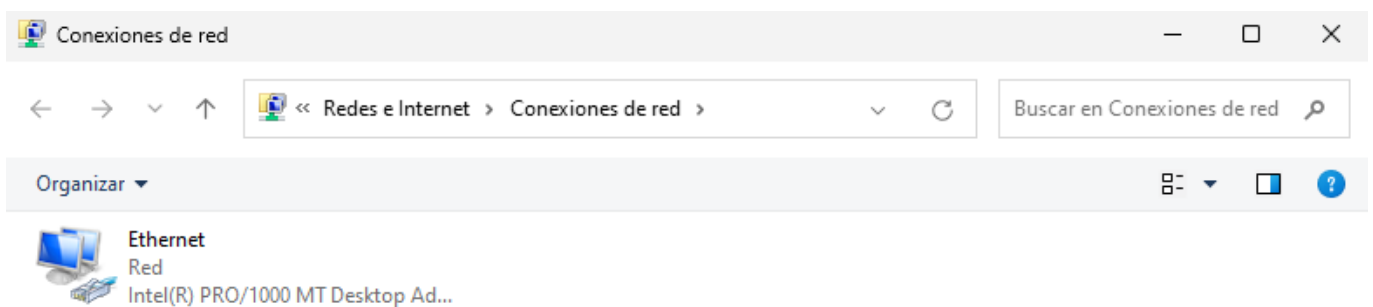


# [FORT] Práctica 8: Fortificación de la Red de Windows 11

## 1. Verificar el listado de interfaces de red del sistema

### a. Lista todas las interfaces de red que están disponibles en tu sistema

Podemos revisar esto dentro de “Panel de Control/Redes y recursos compartidos/cambiar configuración de adaptador”:



También podemos ver las interfaces con sus configuraciones de red usando el comando de CMD “ipconfig”:

```
Microsoft Windows [Versión 10.0.22631.5039]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\MCBS>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::61b1:ee45:e3ca:9a56%7
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

### b. Comprueba si tienes IPv6 Concebida

En la salida del comando “ipconfig” se puede observar si hay una dirección IP asociada:

```
Microsoft Windows [Versión 10.0.22631.5039]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\MCBS>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::61b1:ee45:e3ca:9a56%7
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

Como se puede observar, esta máquina tiene una IPv6 Asociada

### c. ¿Que tipo de dirección IPV6 es? ¿Como la obtienes?

Teniendo en cuenta que esta IPv6 comienza por fe80, es una dirección IP local. Esta IP se puede obtener a través de SLAAC (Stateless Address AutoConfiguration) si no hay servidor DHCPv6 o por

## DHCPv6

**d. Si haces ping al nombre de tu equipo, ¿responde antes la pila IPv6 o la pila IPv4?**

Si hacemos ping al hostname responde antes la pila IPv6:

```
C:\Users\MCBS>hostname
MCBSW11

C:\Users\MCBS>ping MCBSW11

Haciendo ping a MCBSW11 [fe80::61b1:ee45:e3ca:9a56%7] con 32 bytes de datos:
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m
Respuesta desde fe80::61b1:ee45:e3ca:9a56%7: tiempo<1m

Estadísticas de ping para fe80::61b1:ee45:e3ca:9a56%7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

**e. ¿Se puede modificar el orden de resolución de IPv6 o IPv4?**

Se puede modificar el orden de resolución mediante el uso del comando netsh. Podemos revisar el estado actual de las políticas IPv6 con:

```
netsh interface ipv6 show prefixpolicies
```

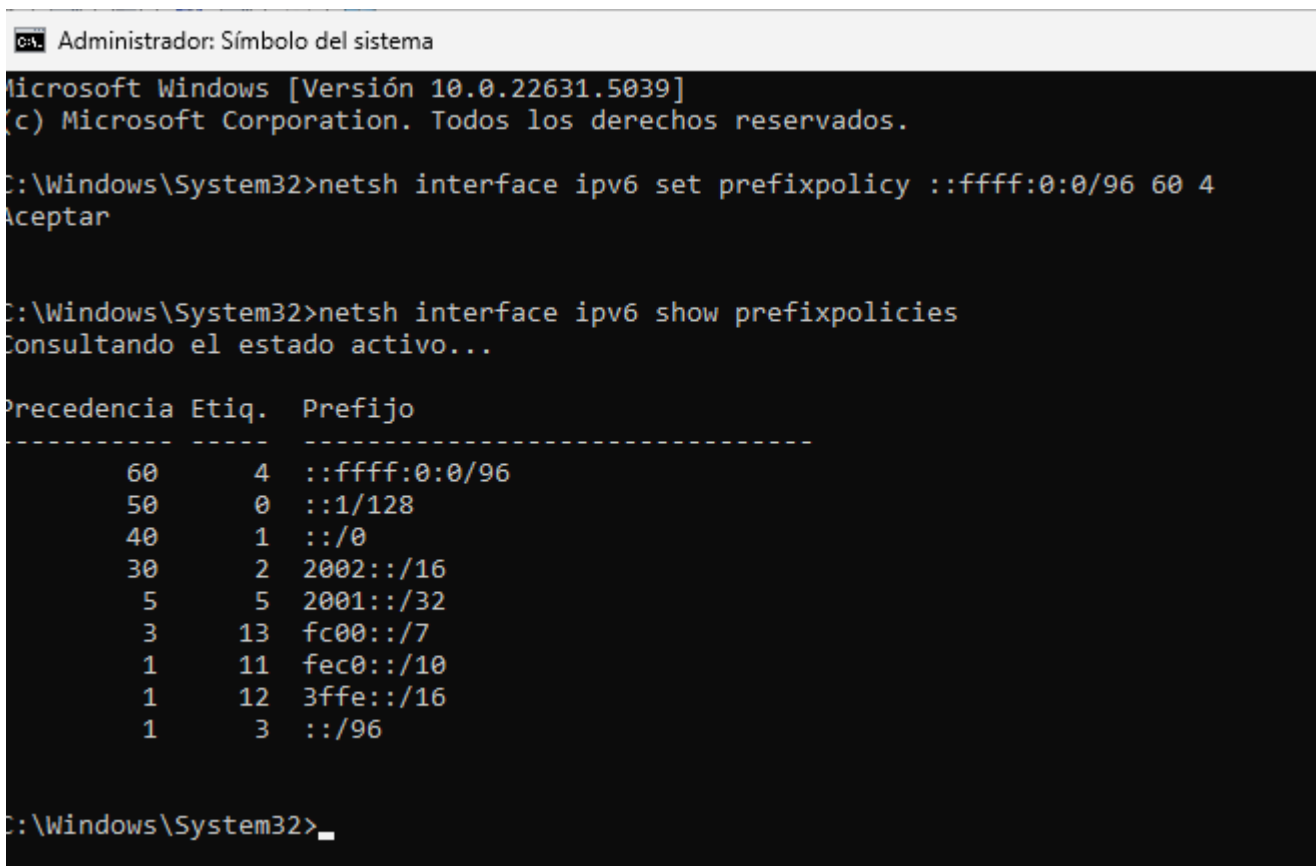
```
netsh>interface ipv6 show prefixpolicies
Consultando el estado activo...

Precedencia Etiq.  Prefijo
-----
50          0   ::1/128
40          1   ::/0
35          4   ::ffff:0:0/96
30          2   2002::/16
5           5   2001::/32
3           13  fc00::/7
1           11  fec0::/10
1           12  3ffe::/16
1           3   ::/96
```

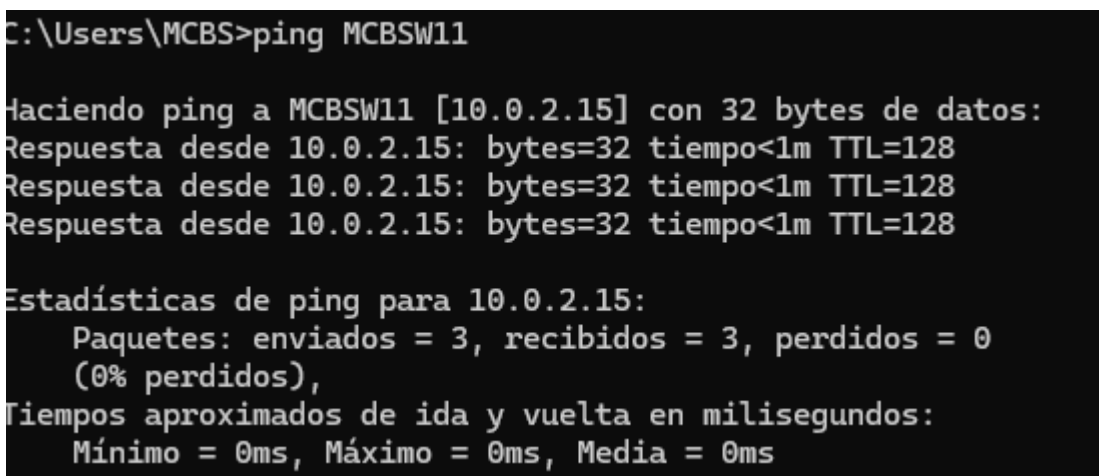
El prefijo “::ffff:0:0/96” que se puede observar en la captura de pantalla, corresponde a las IPv4

mapeadas en IPv6, para darle prioridad de resolución a IPv4 tan solo tenemos que aumentar su nivel de precedencia, en este caso a 60, haciéndolo el más alto, con el siguiente comando:

```
netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 60 4
```



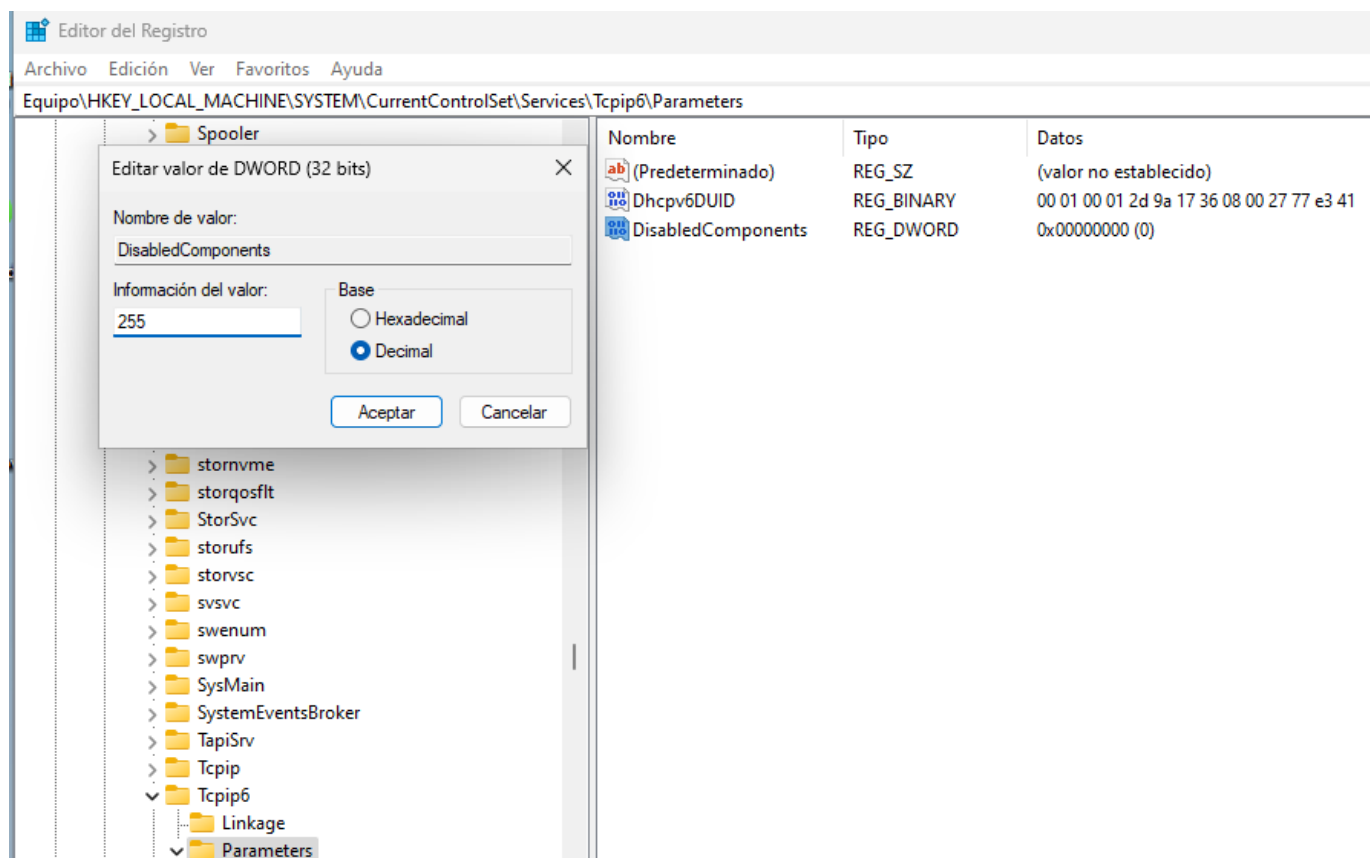
Una vez aplicada dicha configuración se puede observar como al hacer ping al nombre del host ahora responde primero IPv4:



## f. ¿Podemos eliminar la configuración de IPv6 de todas las interfaces?

Si, puede ser eliminada mediante el uso de claves de registro en

“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters/”, creando una nueva clave de registro de tipo REG\_WORD llamada DisabledComponents con el valor 255:



Tras eso se reinicia el equipo y se puede comprobar con el comando “ipconfig” que ya no se está configurando IPv6:

```
C:\Users\MCBS>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\MCBS>
```

**g. ¿Es posible que al deshabilitar IPv6 se provoque una realentización del arranque de Windows? ¿Si es así como lo corregimos?**

De [acuerdo con microsoft](https://www.microsoft.com/en-us/windows/ipv6) esto puede ocurrir en sistemas windows antiguos situados entre Windows 7

y windows 8.1 y puede ser corregido mediante la descarga de ciertas actualizaciones.

## **2. Una vez eliminado IPv6 de todas las interfaces:**

### **a. ¿Que tipo de perfiles tenemos en una interfaz de Microsoft Windows 11? ¿Qué diferencia tenemos entre ellos?**

Generalmente hay 2 principales tipos:

- Privado: Pensado para redes que son de confianza como una casa o una pequeña oficina, bajo este perfil el dispositivo puede ser descubierto por otros equipos de la red. Algunas reglas del cortafuegos son más ligeras en este perfil.
- Público: Se usa en redes que no son de confianza, como redes públicas de bares y bibliotecas, el cortafuegos es mucho más restrictivo. Además también bloquea la compartición de recursos.

Si un equipo está unido a un Active Directory las configuraciones de red y seguridad son controladas por el administrador de dominio.

### **b. ¿Que perfil es recomendable para un equipo personal como el que estamos configurando?**

En este caso como el equipo se encuentra en una red que se podría considerar hasta cierto punto pública (Munics o Eduroam) lo recomendable sería establecer el perfil público por seguridad.

### **c. ¿La configuración del perfil afecta en algo a la seguridad?**

Si ya que dependiendo del perfil que se configure el equipo puede estar oculto o no en la red, dificultando su localización por parte de un atacante , además el firewall se puede volver más restrictivo y se bloquea la compartición de archivos, reduciendo la cantidad de posibles agujeros de seguridad del sistema.

### **d. ¿Que componentes tiene instalados cada interfaz?¿Es necesario tener instalados todos los componentes?¿Cuáles se pueden eliminar?**

### **e. ¿Hasta que nivel de la capa OSI nos protege el FireWall de Windows?**

### **f. ¿El Firewall permite gestionar el tráfico de entrada y salida? ¿Cuál es la configuración más restrictiva que se puede aplicar?**

### **g. ¿Existe un sistema de Logs?¿En que carpetas se encuentras?¿Como se puede hacer debug de las reglas aplicadas?**

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

[https://knoppia.net/doku.php?id=master\\_cs:fortificacion:p8&rev=1744122563](https://knoppia.net/doku.php?id=master_cs:fortificacion:p8&rev=1744122563)

Last update: **2025/04/08 14:29**

