



UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

**Centro de
e-Learning**
Secretaría de Cultura y Extensión Universitaria

Centro de e-Learning SCEU UTN - BA. Medrano 951 2do piso
(1179) // Tel. +54 11 7078- 8073 / Fax +54 11 4032 0148
www.sceu.frba.utn.edu.ar/e-learning

Experto Universitario en Ethical Hacking

Módulo 2:

Administración de Servidores (Windows o Linux)

Unidad 3:

Instalando y configurando nuestro servidor



Presentación

En esta tercer Unidad del curso, se aprenderá a configurar los servicios de DHCP en una PC.

Se conocerá cómo configurar un servidor de DHCP y un servidor de DNS.

Y tener en cuenta, todos los procesos de seguridad que acompañan.



Objetivos

Que los participantes logren...

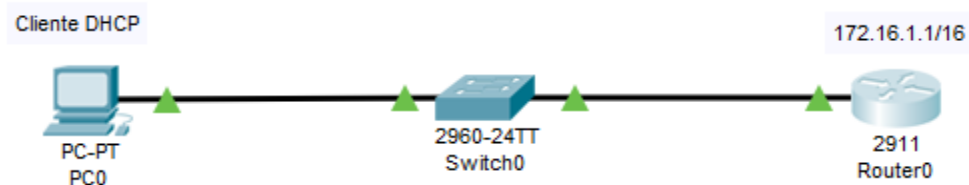
- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.
- Conocer las herramientas esenciales y las buenas prácticas necesarias para obtener el máximo nivel de seguridad en una red de servidores de arquitectura Microsoft Windows Server o Linux Server, protegiéndola de potenciales amenazas.
- Comprender los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.



Bloques temáticos

1. Configurando una PC para DHCP.
2. Configurando un servidor DHCP.
3. Configurando un servidor DNS.

Configurando una PC para DHCP



Chequear nuestra PC para saber si se encuentra preparada para DHCP

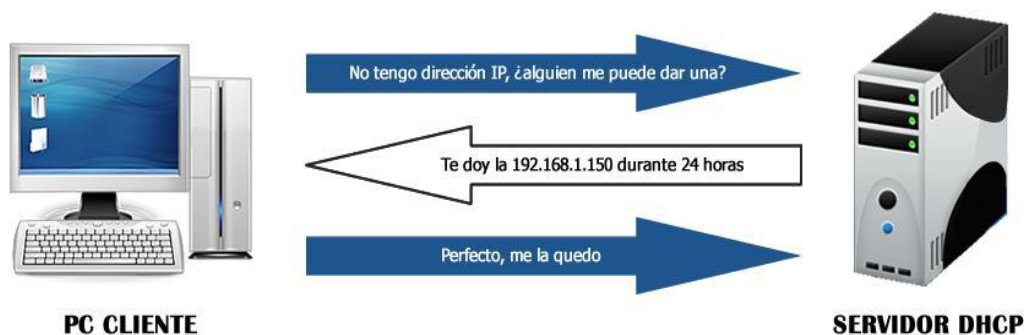
El escenario más común, es encontrar una PC conectada a una red, la cual puede estar formada por un Switch y un Router.

Como ya expusimos anteriormente, tanto un Router como un Switch, pueden estar configurados para que sean Servidores **DHCP**.

Los sistemas operativos están configurados, en modo default, para que detecten automáticamente una petición **DHCP** validándose en el mismo.

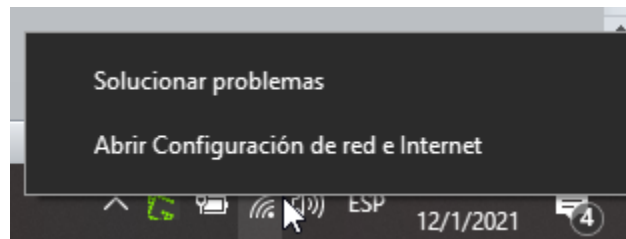
Apenas llega la petición, desde nuestro equipo si está en forma automática, tomaría valores que le entrega el servidor de **DHCP**:

IP, MASCARA, DEFAULT GATEWAY

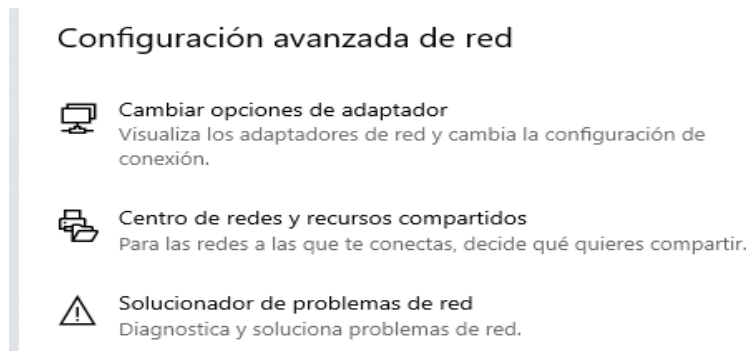


No solamente le entregaría la IP, sino la máscara y el default Gateway

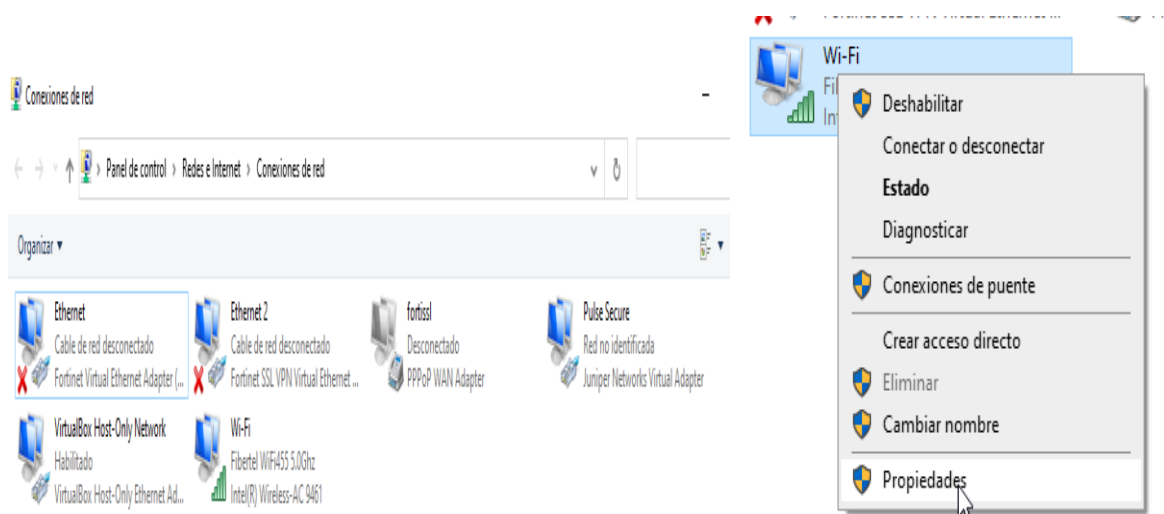
Hay varias maneras de chequear que esté en modo automático nuestra placa de red, veremos un par de ejemplos:



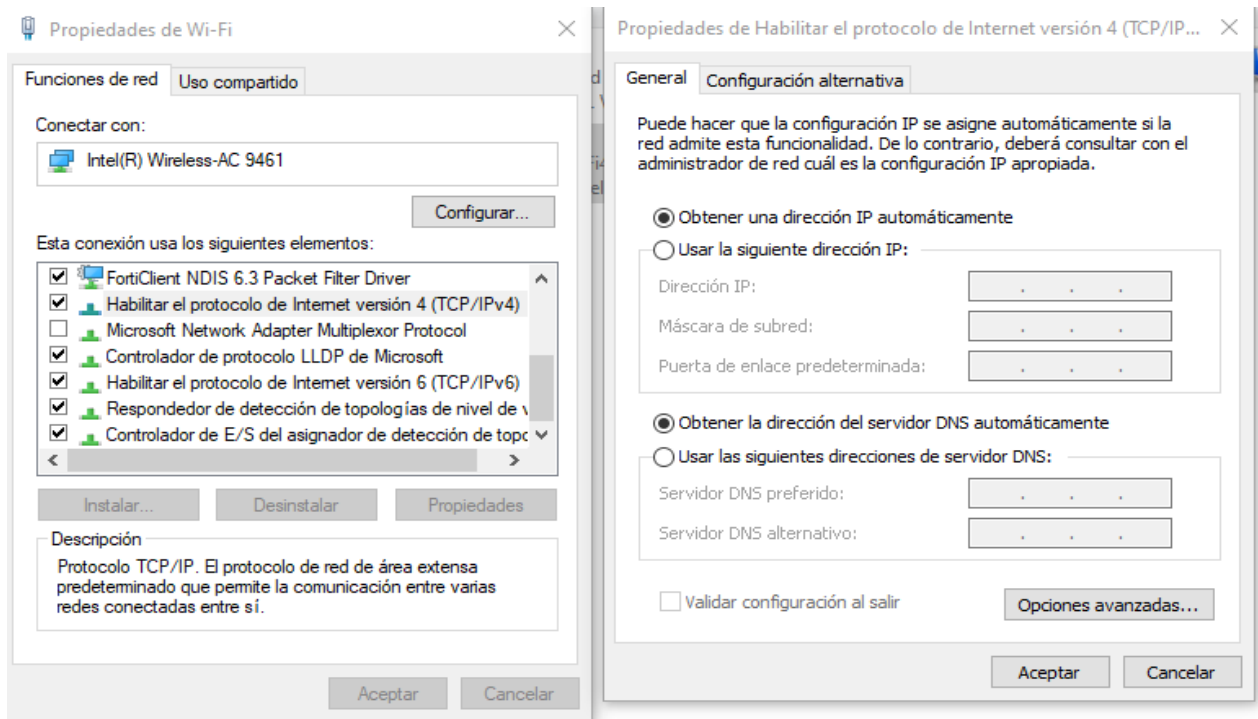
En Windows 10, por ejemplo, una manera es desde el icono de red, **click derecho**, opción **Abrir Configuración de red e Internet**



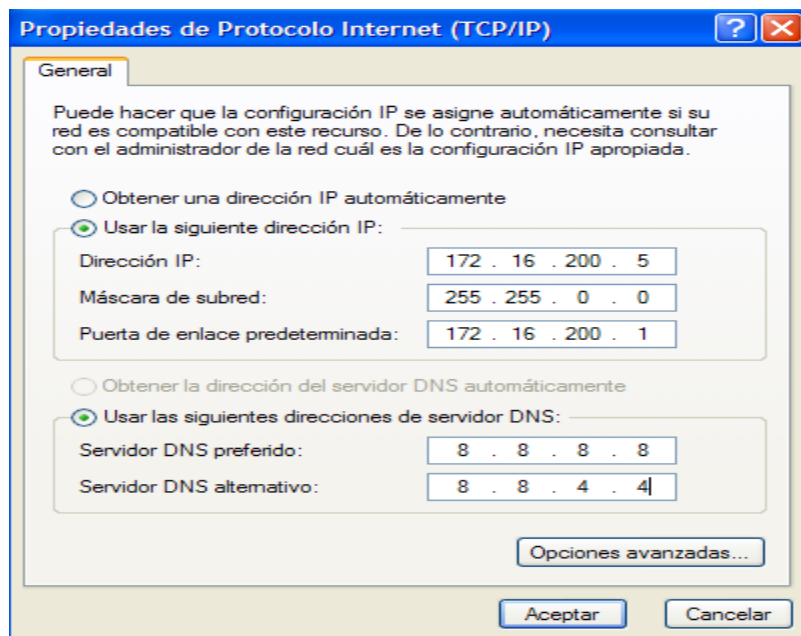
Una vez ahí, seleccionamos la opción **Cambiar opciones de adaptador**



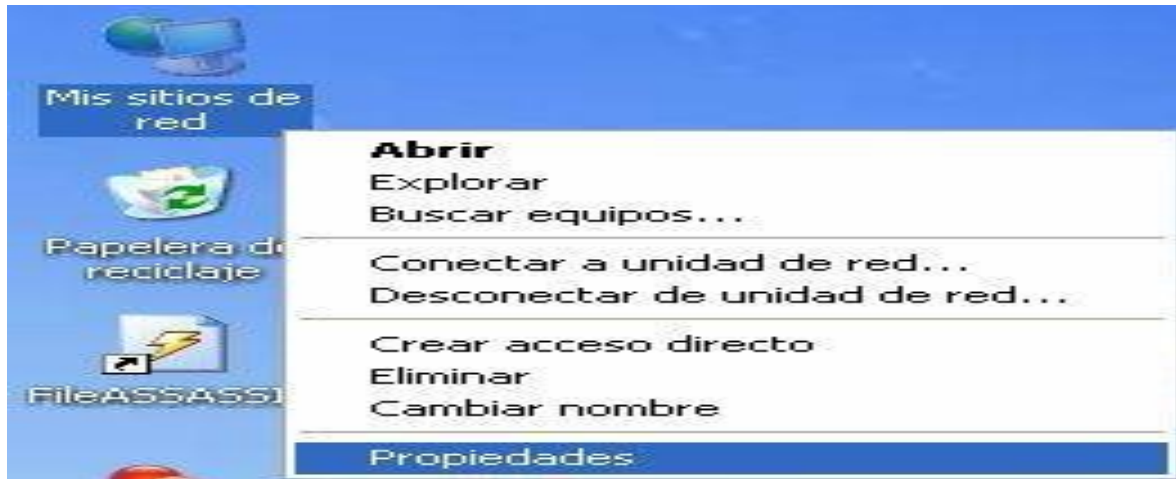
Expondrá todas las conexiones de red que se tienen instaladas, lo cual se realiza **click derecho**, sobre la conexión en uso y seleccionar **propiedades**



Por último, se selecciona la opción de IPV4 y luego propiedades, lo cual en la imagen vemos que se encuentra configurada para que obtenga una IP de forma automática (si hubiera una IP, sería forma manual).



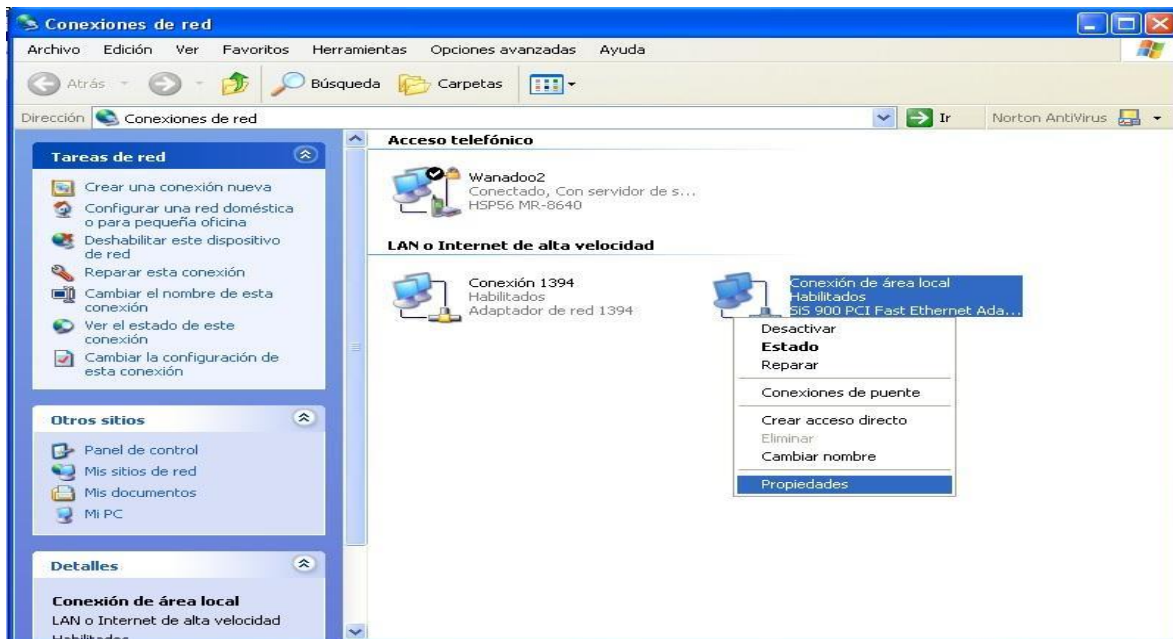
Dependiendo del Sistema operativo, también se puede ir al **icono Mis sitios de red**, hacemos **click derecho** con el mouse, seleccionamos **propiedades**.



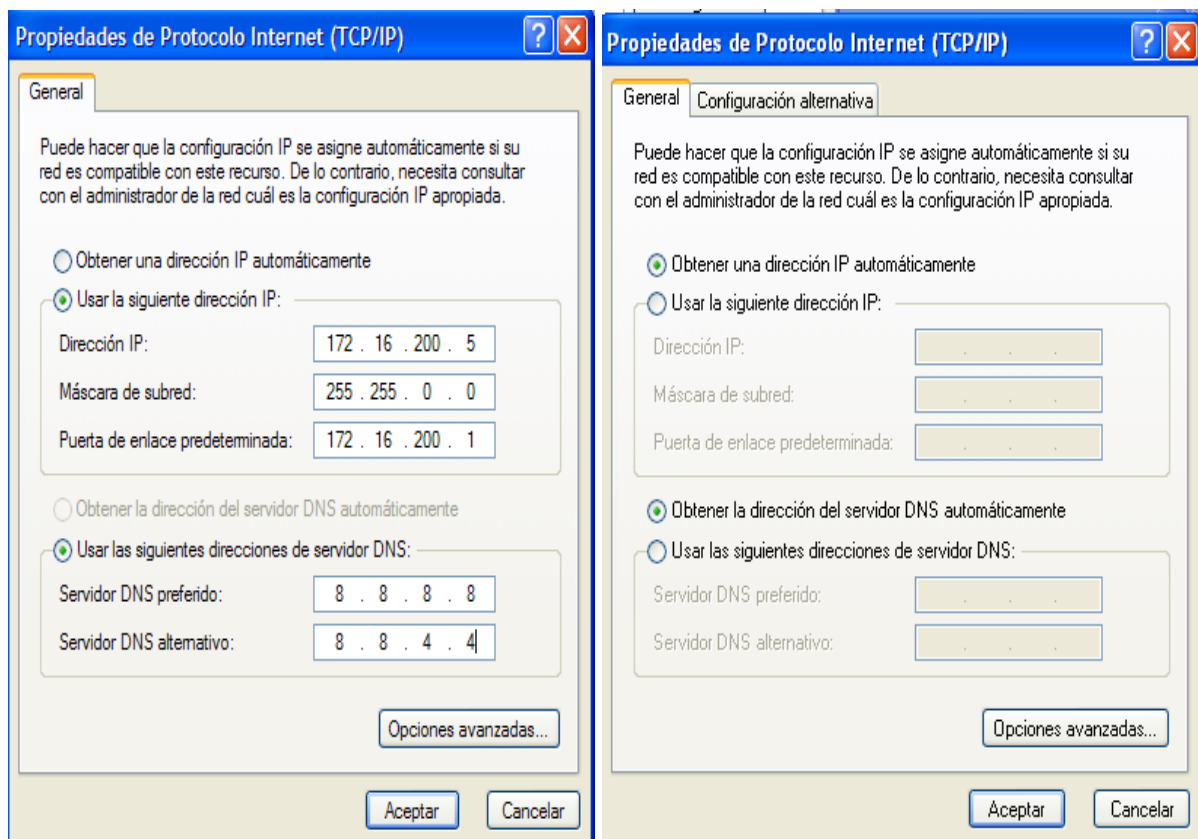
Otra manera, sería ir a **INICIO**, **Panel de control** y ahí seleccionamos **Conexiones de red e Internet**.



Seleccionamos la placa de red que tenemos conectada, **click derecho** y click en **Propiedades**.



Y como expusimos anteriormente en el otro ejemplo, encontraremos con IP o sin IP



Configurando un Servidor DHCP

A continuación mostraremos cómo configurar un servidor **DHCP** en un **Windows Server 2003/2008**.

Este ejemplo se realizará en un **Windows Server 2003/2008** ya instalado en un equipo o máquina virtual.

Los requerimientos de equipo para instalarlos en una máquina virtual, son prácticamente los mismos si tuviéramos un equipo físico, lo recomendado sería probar instalarlos en máquina virtual, siempre y cuando el hardware físico sea el adecuado.

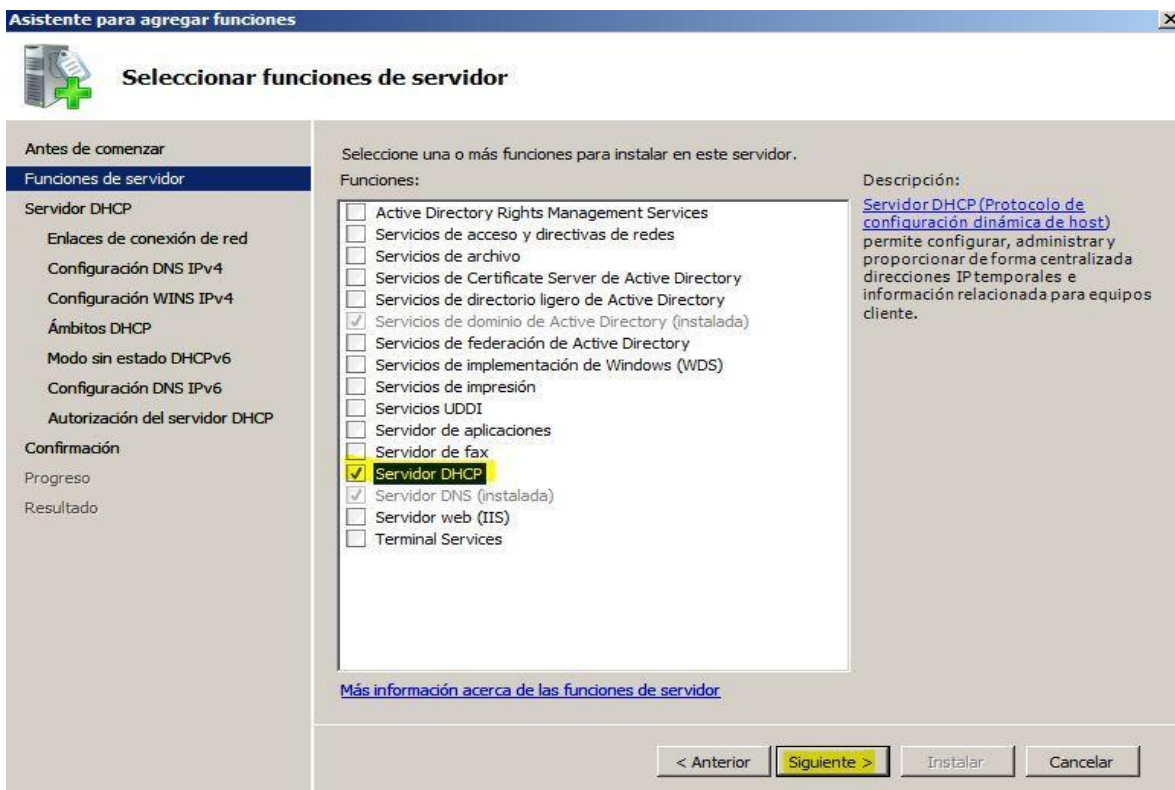
Componente	Requisito
Procesador	<ul style="list-style-type: none"> • Mínimo: 1 GHz • Recomendado: 2 GHz • Óptimo: 3 GHz o más Nota: Windows Server 2008 para sistemas basados en Itanium precisa un procesador Intel Itanium 2.
Memoria	<ul style="list-style-type: none"> • Mínimo: 512 MB de RAM • Recomendado: 1 GB de RAM • Óptimo: 2 GB de RAM (instalación completa) o 1 GB de RAM (instalación de Server Core) o más • Máximo (sistemas de 32 bits): 4 GB (Standard) o 64 GB (Enterprise y Datacenter) • Máximo (sistemas de 64 bits): 32 GB (Standard) o 2 TB (Enterprise, Datacenter y sistemas basados en Itanium)
Espacio en disco disponible	<ul style="list-style-type: none"> • Mínimo: 8 GB • Recomendado: 40 GB (instalación completa) o 10 GB (instalación de Server Core) • Óptimo: 80 GB (instalación completa) o 40 GB (instalación de Server Core) o más Nota: los equipos con más de 16 GB de RAM requerirán más espacio en disco para la paginación, para la hibernación y para los archivos de volcado
Unidad	Unidad de DVD-ROM
Pantalla y periféricos	<ul style="list-style-type: none"> • Super VGA (800 x 600) o monitor con una resolución mayor • Teclado • Mouse de Microsoft o dispositivo señalador compatible

PARA TENER EN CUENTA: PUEDEN BAJARSE UNA TRIAL DESDE EL SITIO OFICIAL DE MICROSOFT.

Dentro del panel de control, vamos hacia herramientas administrativas y hacemos **click en Administración del servidor.**




Hacemos **click en Agregar funciones o roles**



Luego de una pantalla de introducción, nos saldrán las aplicaciones o servicios a instalar, seleccionamos **Servidor DHCP**, a continuación nos saldrá otra pantalla, en este caso de cosas a tener en cuenta, **LEERLAS!**

Asistente para agregar funciones

 **Especificar la configuración del servidor DNS IPv4**

Antes de comenzar

Funciones de servidor

Servidor DHCP

Enlaces de conexión de red

Configuración DNS IPv4

Configuración WINS IPv4

Ámbitos DHCP

Modo sin estado DHCPv6

Configuración DNS IPv6

Confirmación

Progreso

Resultado


Cuando los clientes obtienen una dirección IP del servidor DHCP, pueden proporcionárseles opciones DHCP como las direcciones IP de los servidores DNS y el nombre del dominio primario. La configuración que especifique aquí se aplicará a los clientes que usen IPv4.

Especifique el nombre del dominio primario que usarán los clientes para la resolución de nombres. Este dominio se usará para todos los ámbitos que cree en este servidor DHCP.

Dominio primario:

Especifique las direcciones IP de los servidores DNS que usarán los clientes para la resolución de nombres. Estos servidores DNS se usarán para todos los ámbitos que cree en este servidor DHCP.

Dirección IPv4 del servidor DNS preferido:

 El servidor DNS de la dirección IP especificada no responde.

Dirección IPv4 del servidor DNS alternativo:

[Más información acerca de la configuración del servidor DNS](#)

Click en conexión de red que usaremos, a continuación nos saldrá una pantalla para configurar un DNS, como nombre de dominio pongan el que quieran usar, luego la IP que pondremos es la misma de la máquina, y si quieren en DNS alternativo pongan el de Google:8.8.8.8.



Asistente para agregar funciones

Agregar o editar ámbitos DHCP

Antes de comenzar

Funciones de servidor

Servidor DHCP

Enlaces de conexión de red

Configuración DNS IPv4

Configuración WINS IPv4

Ámbitos DHCP

Modo sin estado DHCPv6

Configuración DNS IPv6

Confirmación

Progreso

Resultado

Un ámbito es el intervalo de posibles direcciones IP para una red. El servidor DHCP no puede distribuir direcciones IP a los clientes hasta que se cree un ámbito.

Agregar ámbito

Un ámbito es un intervalo de posibles direcciones IP para una red. El servidor DHCP no puede distribuir direcciones IP a los clientes hasta que se cree un ámbito.

Nombre de ámbito:

Dirección IP inicial:

Dirección IP final:

Máscara de subred:

Puerta de enlace predeterminada (opcional):

Tipo de subred:

☒ Activar este ámbito

Aceptar Cancelar

[Más información acerca de la adición de ámbitos](#)

Nos saldrá una pantalla referida a **WINS**, la pasamos por alto, a continuación nos mostrará la pantalla más importante de toda, la de agregar el ámbito o sea la configuración de entrega de **IPs**.

En el ejemplo, expone que entregará direccionamiento IP: 192.168.15.5 (inclusive) hasta la 192.168.15.20 (inclusive) (esto significa que dispondrá de 16 direcciones IP para repartir).

Asistente para agregar funciones



Confirmar selecciones de instalación

Antes de comenzar

Funciones de servidor

Servidor DHCP

Enlaces de conexión de red

Configuración DNS IPv4

Configuración WINS IPv4

Ámbitos DHCP

Modo sin estado DHCPv6

Confirmación

Progreso

Resultado

Para instalar las siguientes funciones, servicios de función o características, haga clic en Instalar.

1 mensaje informativo a continuación

Es posible que sea necesario reiniciar el servidor una vez completada la instalación.

Servidor DHCP

Enlaces de conexión de red: 192.168.15.2 (IPv4)

Configuración DNS IPv4

Dominio primario DNS: oelos.com

Servidores DNS: 192.168.15.2

Servidores WINS: Ninguno

Ámbitos

Nombre: oelos.com

Puerta de enlace predeterminada: 192.168.15.1

Máscara de subred: 255.255.255.0

Intervalo de direcciones IP: 192.168.15.5 - 192.168.15.20

Tipo de subred: Cableado (la duración de la concesión será de 6 días)

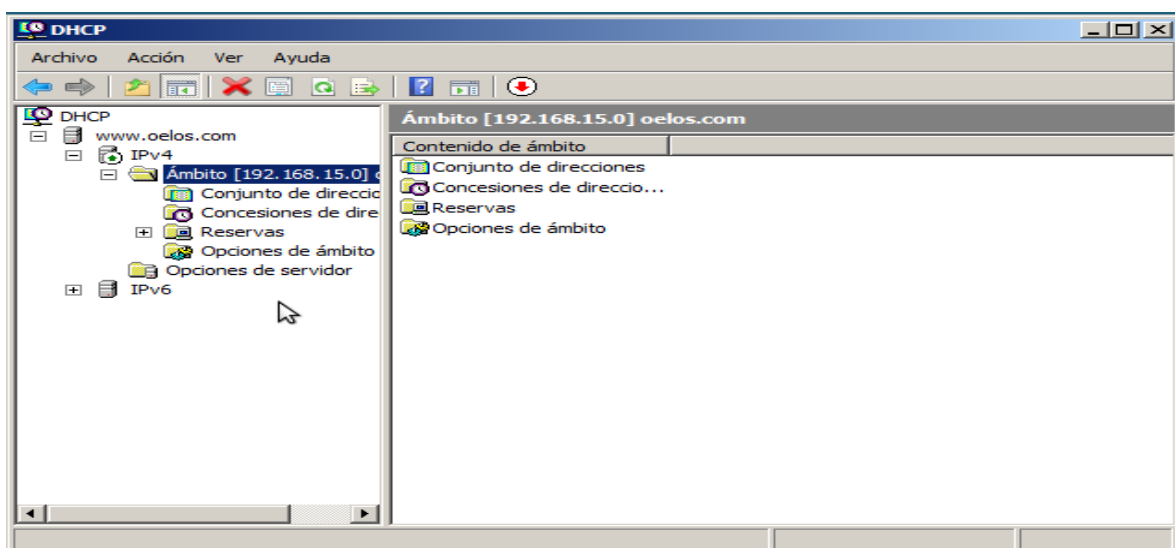
Activar ámbito: Sí

Modo sin estado DHCPv6: Deshabilitado

[Imprimir, enviar por correo electrónico o guardar esta información](#)

< Anterior Siguiente > **Instalar** Cancelar

Luego de que pasemos por alto la configuración de IPV6, nos saldrá la confirmación de lo que realizamos, clic en Instalar.



Luego de reiniciar el servidor, si hacemos click en el servicio de DHCP, nos mostrará lo que se configuró.

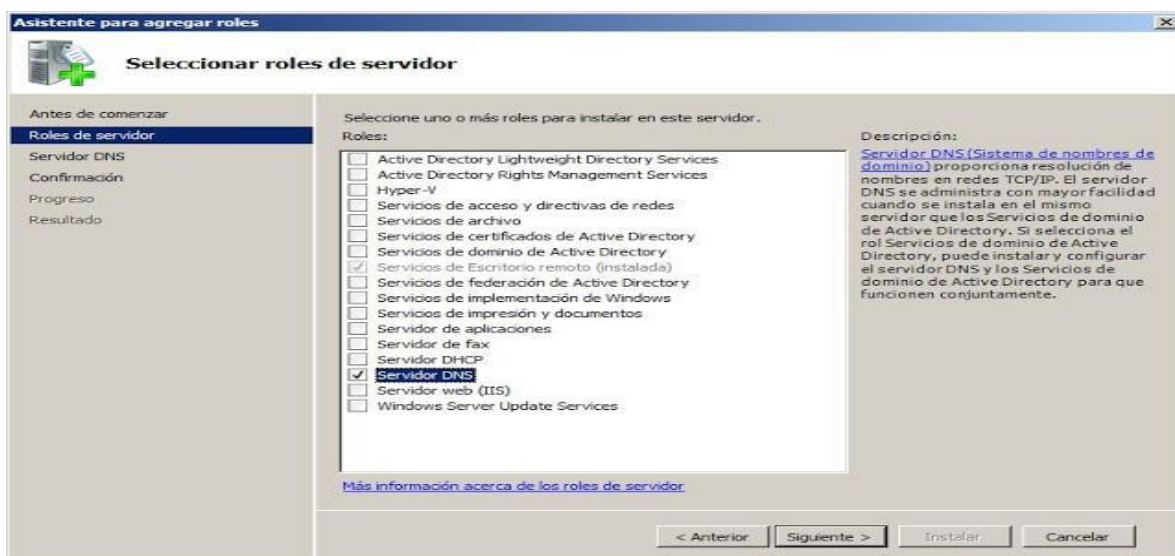


Configurando un Servidor DNS

Dentro del panel de control, vamos hacia herramientas administrativas y hacemos click en Administración del servidor.

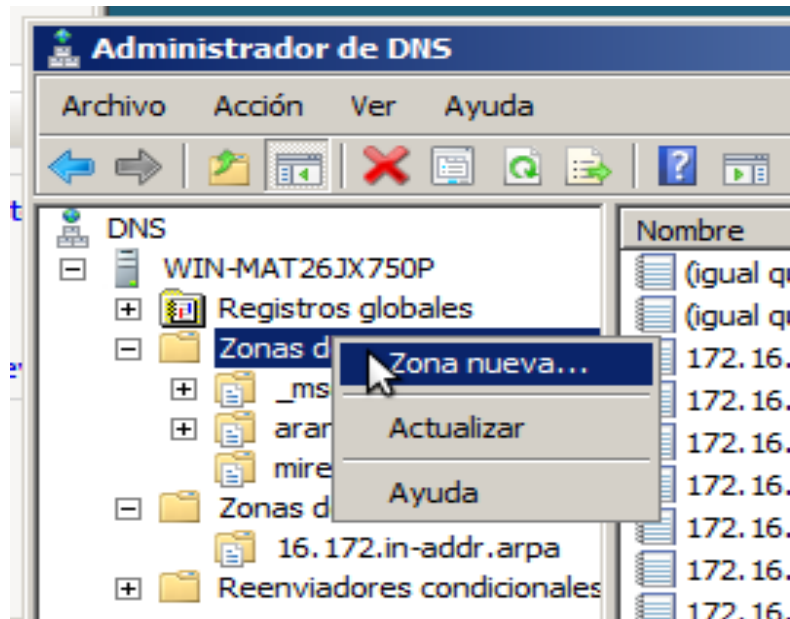


Hacemos click en **Agregar funciones o roles**.

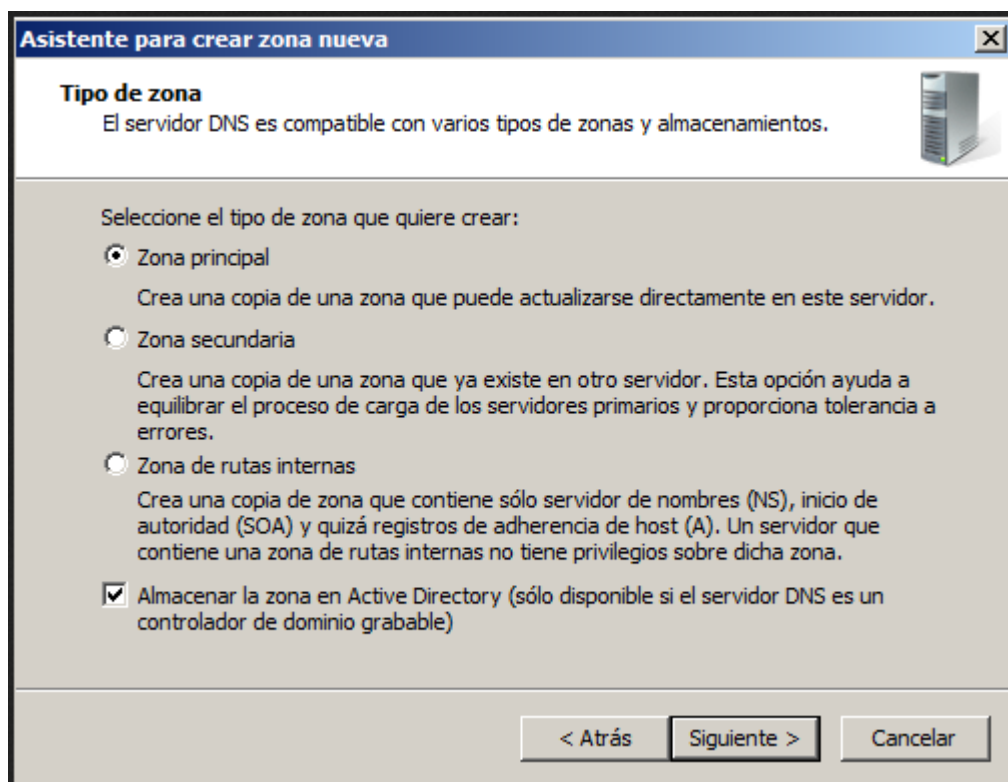


Seleccionamos **Servidor DNS** y se instalara, pero antes tener en cuenta unos requisitos para poder instalarlo: tener una **IP** estática en nuestro servidor **DNS**.

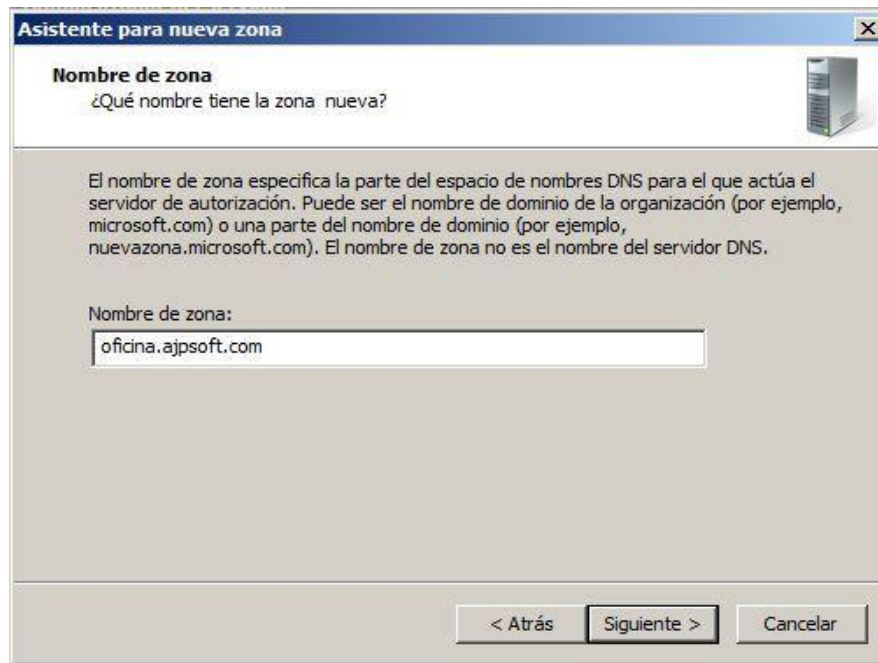
Seleccionamos en zona de búsqueda, clic derecho, **Zona nueva**.



Definimos que nuestro servidor será el primario para la zona.



Configuramos el ámbito de replicación para todos los servidores **DNS** en este dominio: dominio.com.



Asistente para nueva zona

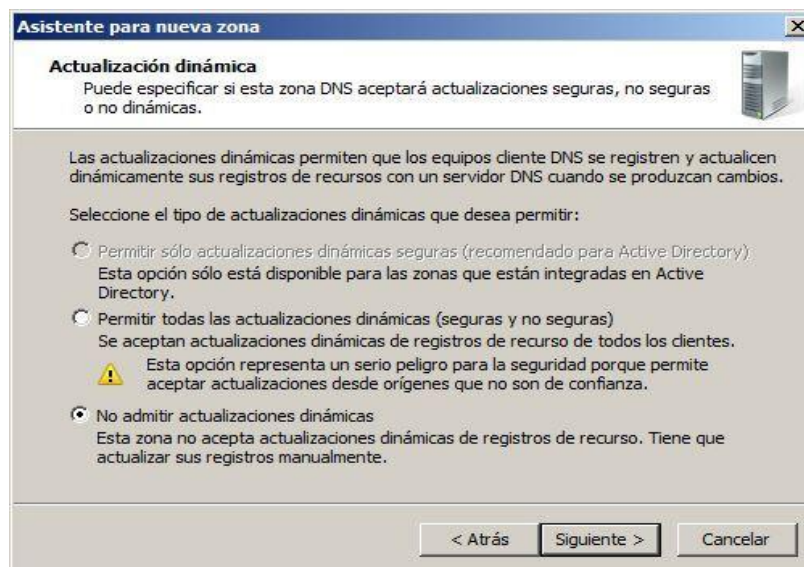
Nombre de zona
¿Qué nombre tiene la zona nueva?

El nombre de zona especifica la parte del espacio de nombres DNS para el que actúa el servidor de autorización. Puede ser el nombre de dominio de la organización (por ejemplo, microsoft.com) o una parte del nombre de dominio (por ejemplo, nuevazona.microsoft.com). El nombre de zona no es el nombre del servidor DNS.

Nombre de zona:
oficina.ajpsoft.com

< Atrás Siguiendo > Cancelar

Nos preguntará por el nombre de zona, luego ponemos que no queremos actualizaciones automáticas.




Asistente para nueva zona

Actualización dinámica
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

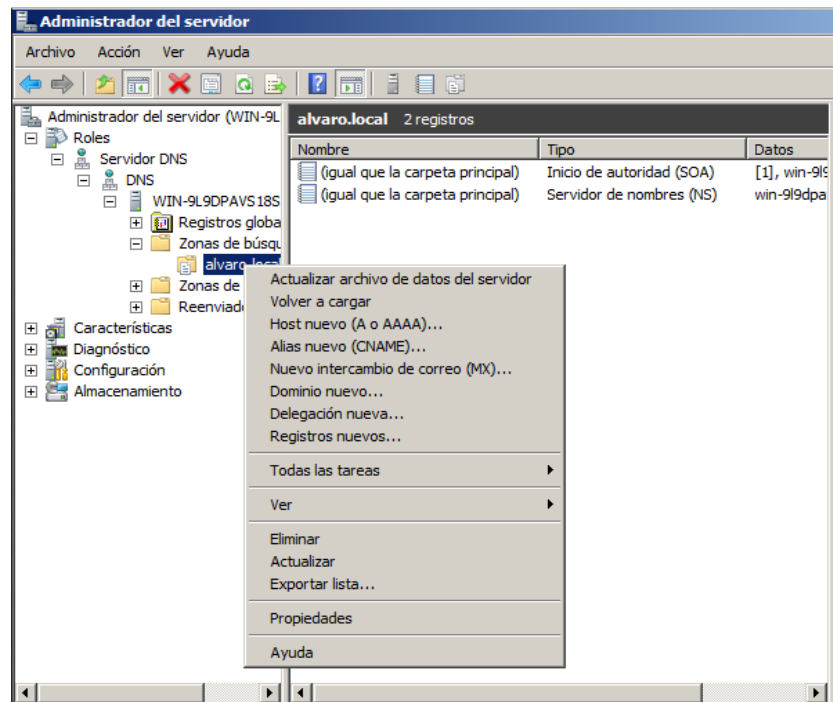
Seleccione el tipo de actualizaciones dinámicas que desea permitir:

- ☒ Permitir sólo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción sólo está disponible para las zonas que están integradas en Active Directory.
- ☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.
- ☐ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

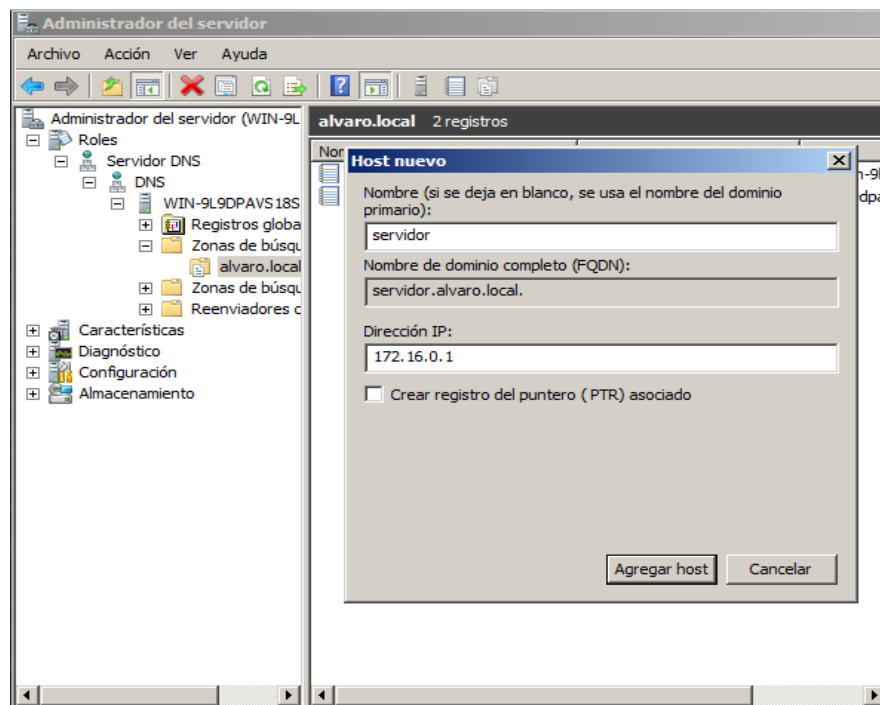
< Atrás Siguiendo > Cancelar

Finalizamos, y luego podremos configurar la zona que creamos

En nombre ponemos el que tendrá el subdominio, ese subdominio se lo podemos asignar al ordenador del Administrador de la Red.



En dirección **IP** ponemos la dirección del ordenador/PC/dispositivo.



Ejercicio Número 1 Unidad 3



Los ejercicios son voluntarios, NO ES OBLIGATORIO REALIZAR LOS DOS, son para testear si comprendieron el material, en caso de dudas o ayuda, solicitarle al instructor.

1- instalar un servidor FTP en cualquier sistema operativo.

Probarlo y mandar como prueba, una captura de pantalla de inicio del mismo, en conjunto con la configuración utilizada.

2- instalar un servidor a elección del alumno y mandar una captura (imagen) de lo realizado.

TIPS

Configurar placa de red para **DHCP**:

<http://www.youtube.com/watch?v=WPhER5B7zEc>

Configurar un servidor DHCP:

<http://www.youtube.com/watch?v=LibUm6q9m2g>

Configurar un servidor DNS:

<http://www.youtube.com/watch?v=yYtW-fMxyHk>

TIPS: Consejos de seguridad para FTP

Seguridad Básica:

- Contraseña segura, mayúscula, minúscula, números y signos.
- Que cada usuario tenga los privilegios adecuados y necesarios para su trabajo.
- Cambiar puerto de acceso (ej: TCP/21 por TCP/4513).
- Tener un backup que se actualice por cambios realizados en los archivos y configuraciones.
- Deshabilitar cualquier puerto que no se utilice, verificar con Nmap.
- Modificar la cantidad de intentos de accesos y limitar los equipos para que no generen DDOS.
- Mantener las reglas de Firewall e IPS para FTP.
- Poner el servidor FTP en un DMZ.
- Análisis diario de antivirus.
- Determinar que archivos puede tener las carpetas que usa el FTP y crear una zona de exclusión.

Configurar un Servidor FTP creado con el software FileZilla

Download FileZilla Server for Windows

The latest stable version of FileZilla Server is 0.9.60.2

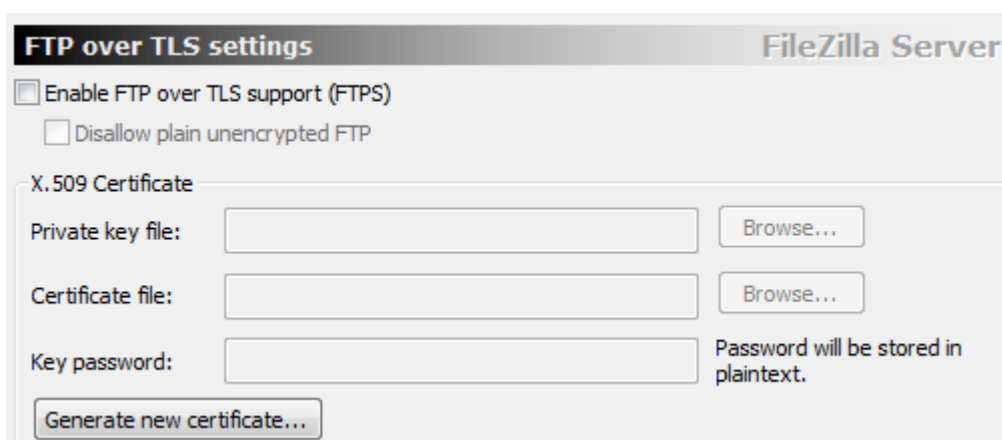
Please select the file appropriate for your platform below.

 **Windows**

**Download
FileZilla Server**



- Configurar llave pública y privada: Ejecuta FileZilla y selecciona el menú Edición > Preferencias. En ese apartado encontrarás el apartado SFTP (dentro de Conexión > FTP). Click en el botón "Añadir un archivo de claves".



FTP over TLS settings FileZilla Server

☐ Enable FTP over TLS support (FTPS)

☐ Disallow plain unencrypted FTP

X.509 Certificate

Private key file:

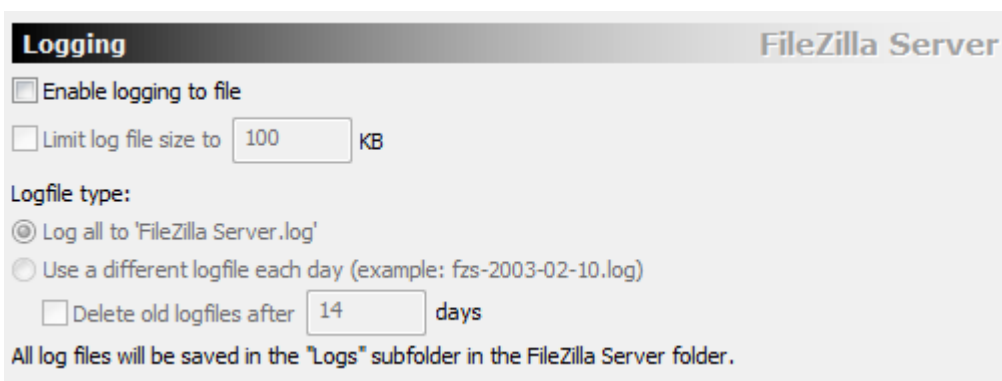
Certificate file:

Key password: Password will be stored in plaintext.

- Si no se usa, bloquear acceso "Usuario anónimo": Ir a Users y verificar que no esté agregado el usuario anónimo (en Server/Users/Shared Folder).

Si está agregado (y se necesita tenerlo), asegurarse que el acceso sea solo de lectura y a la carpeta indicada.

- Activar registros y log: Aunque siempre viene activado se debe verificar que estén habilitados. Esto se puede hacer en View -> Message Log,



Logging FileZilla Server

☐ Enable logging to file

☐ Limit log file size to KB

Logfile type:

☒ Log all to 'FileZilla Server.log'

☐ Use a different logfile each day (example: fzs-2003-02-10.log)

☐ Delete old logfiles after days

All log files will be saved in the "Logs" subfolder in the FileZilla Server folder.

- Mantener actualizado el software.
 - Activar SSL: SSL/TLS settings? "Allow Explicit SSL/TLS on normal connections.
- También activar la casilla que dice: Force PROT P to encrypt file transfers in SSL/TLS mode.

FileZilla Server Options

- General settings
 - Welcome message
 - IP bindings
 - IP Filter
- Passive mode settings
- Security settings
- Miscellaneous
- Admin Interface settings
- Logging
- Speed Limits
- Filetransfer compression
- FTP over TLS settings**
- Autoban

FTP over TLS settings

☐ Enable FTP over TLS support (FTPS)

☐ Disallow plain unencrypted FTP

X.509 Certificate

Private key file:

Certificate file:

Key password: Password will be stored in plaintext.

Explicit and implicit FTP over TLS

☒ Allow explicit FTP over TLS (default: yes)

Note: Explicit FTP over TLS shares the normal FTP port configured on the General settings page.

Listen for implicit FTP over TLS connections on the following ports (default: 990):

File transfer security

These settings need to be enabled for file transfers to be secure.

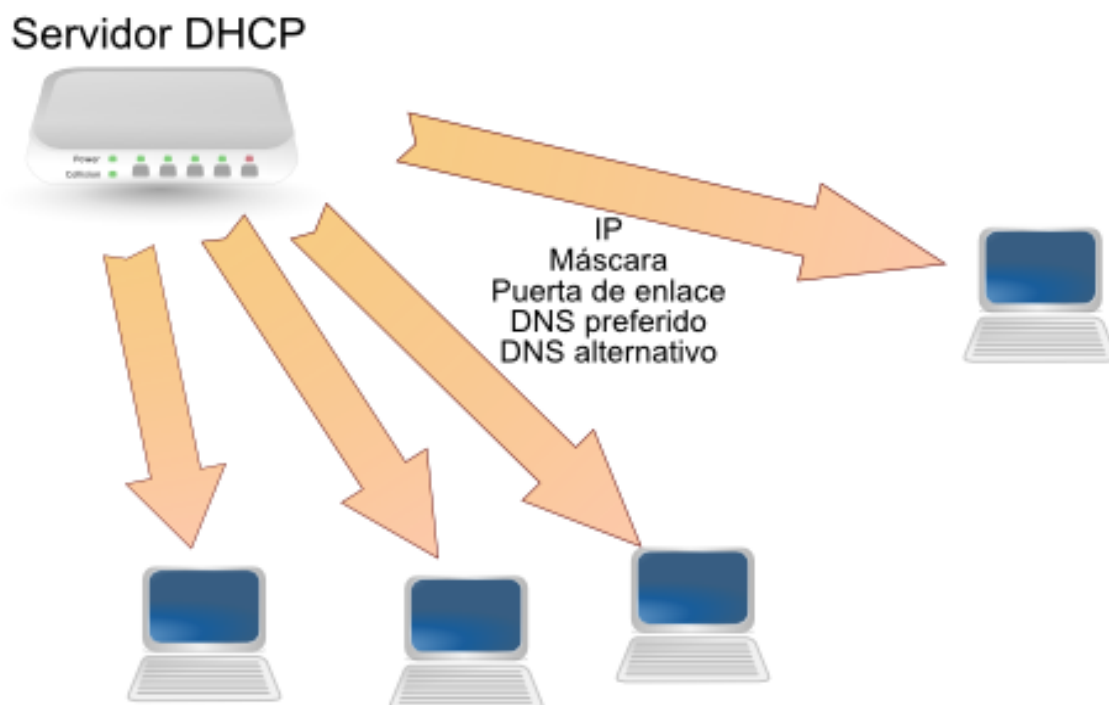
☒ Force PROT P to encrypt file transfers when using FTP over TLS

☒ Require TLS session resumption on data connection when using PROT P

Ejercicio Número 2 Unidad 3



Si fueras un DHCP, ¿qué datos mandarías a los siguientes dispositivos?

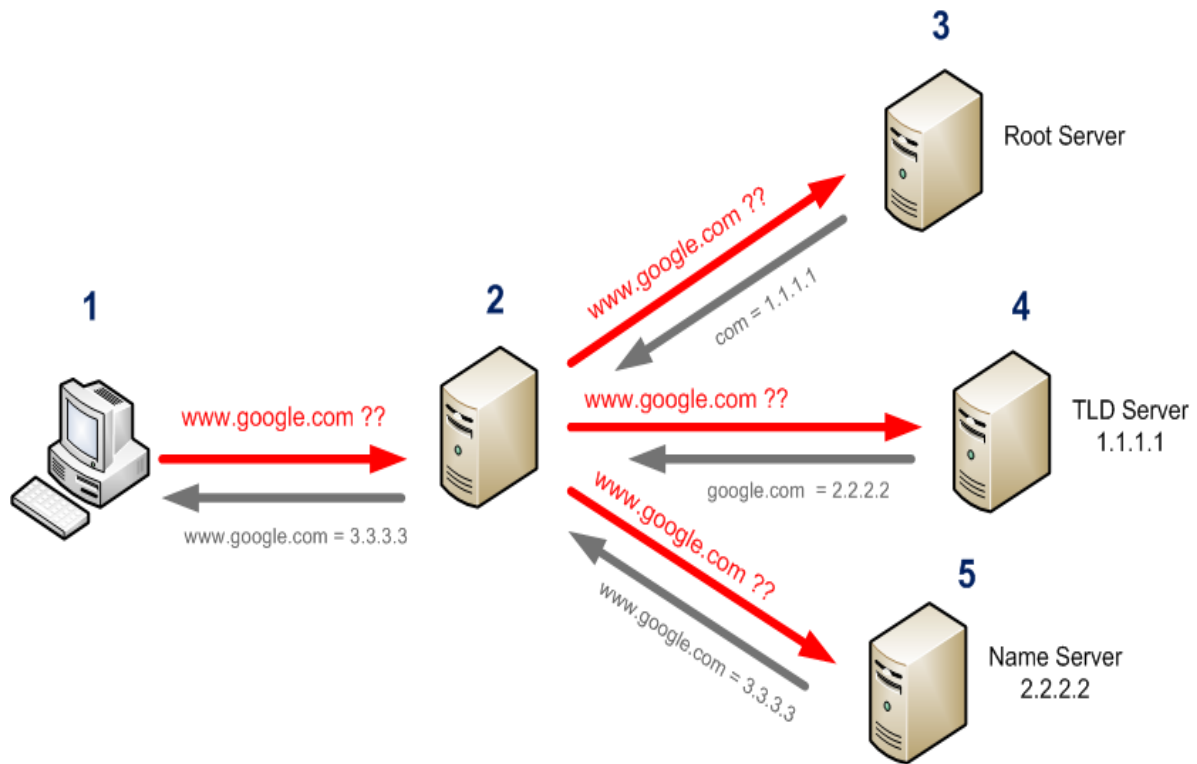


Ordenarlos y especificarlos, por ejemplo, un direccionamiento a cada dispositivo.

Ejercicio Número 3 Unidad 3



¿Que interpretan en esta gráfica? Como ayuda te informamos que es una consulta de «google.com» pero ¿qué está pasando realmente?



Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU

Links complementarios

Configurar un DNS en Windows Server 2008

[https://technet.microsoft.com/es-es/library/cc771031\(v=ws.11\).aspx](https://technet.microsoft.com/es-es/library/cc771031(v=ws.11).aspx)

Configurar un FTP en Windows Server 2012

[https://technet.microsoft.com/es-es/library/hh831655\(v=ws.11\).aspx](https://technet.microsoft.com/es-es/library/hh831655(v=ws.11).aspx)

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado).