



UT7. Conexión de Sistemas en Red

Sistemas Informáticos

Profesorado:
Rosa María Zapata Calle
Diego J. García

Conexión de Sistemas en Red

Índice

1. Servidores de nombres y direcciones.
2. Configuración del protocolo TCP/IP en un cliente de red. Direcciones IP. Máscaras de subred IPv4. en **sistemas Windows**.
 - a) IPv4
 - b) IPv6.
 - c) Configuración estática.
 - d) Configuración dinámica automática.
3. Configuración de protocolo TCP/IP en un cliente de red en sistemas basados en **GNU/Linux**.
4. Comandos de gestión de redes para sistemas basados en GNU/Linux
5. Redes inalámbricas y configuración segura
6. Active Directory

1. SERVIDORES DE NOMBRES Y DIRECCIONES

- 1. Definición
- 2. Tipos

1. Servidores de nombres y direcciones

¿Cómo sabemos qué servidor estamos utilizando?
Estos servidores son configurados en la configuración de red
como hemos visto con anterioridad o en el fichero de
configuración de sistemas basados en GNU/Linux.

2. Servidores de nombres y direcciones

Si vamos a la definición concreta de **servidor de nombres**, este es el servidor que nos devuelve una dirección IP cuando se le da un nombre de dominio. Así mismo esta dirección IP es la ubicación del dominio en Internet.

Es común que a los servidores de nombres se les denomine servidores DNS (y viceversa), debido a que realizan más o menos la misma función cuando se les da un nombre de dominio, devuelven la dirección IP de ese dominio.

Veamoslo con un ejemplo:

Cada vez que incluyes una url en tu navegador web, estás llamando a un servidor de nombres para conseguir llegar a una dirección IP (desconocida para ti), mediante un alias que sí conoces (url, por ejemplo ... www.jccm.es).

Esto es así ya que cada página web está físicamente en un servidor web físico, (hosting) del cuál desconocemos su dirección IP.

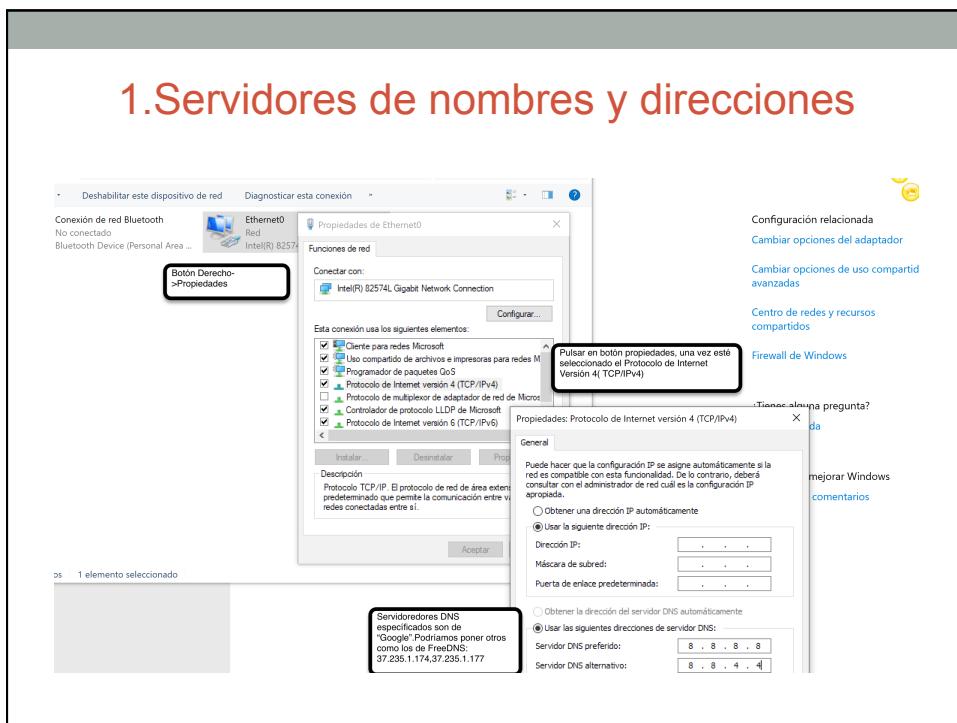
1. Servidores de nombres y direcciones

Ejercicio Investigación Servidores DNS.

Haz un resumen del siguiente artículo

<https://computerhoy.com/paso-a-paso/internet/configura-direcciones-dns-optimiza-tu-red-velocidad-31629>

1. Servidores de nombres y direcciones



2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS

1. Direcciones IP.
2. Máscaras de subred IPv4/IPv6.
3. Configuración estática
4. Configuración dinámica automática (Servicio DHCP).

2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS

En este punto del temario, tenemos claros algunos conceptos que en este punto tenemos que configurar:

Dirección IPv4, máscara de red. En este tema vamos a aprender a configurarlo en nuestros sistemas, y además los siguientes conceptos:

- Dirección IPv6
- Máscara de red IPv6.

2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS

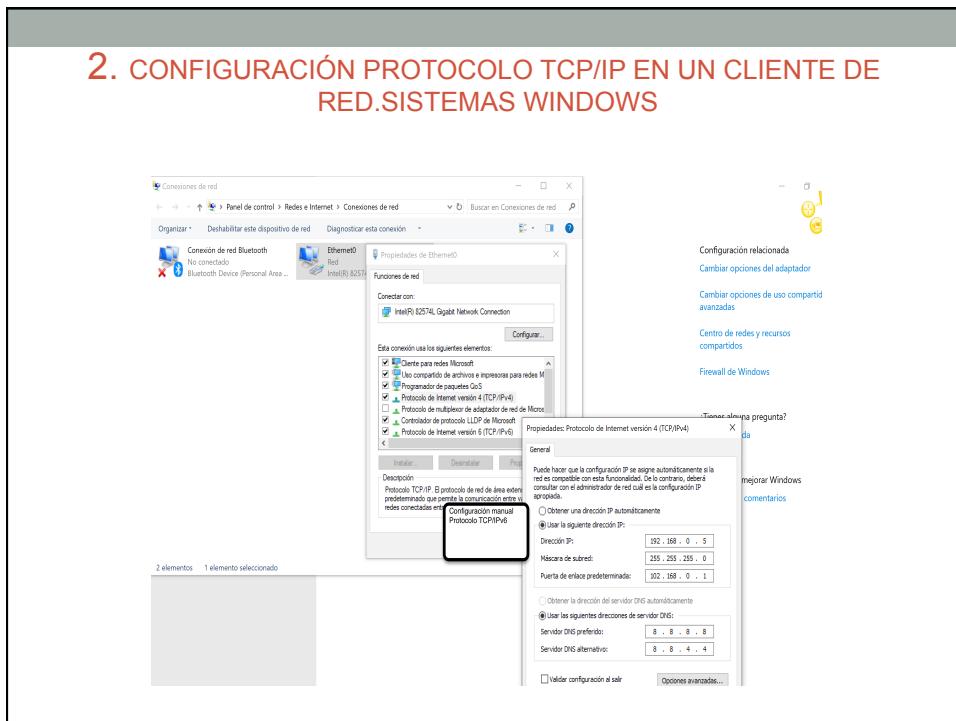
Para la configuración de red en Windows, deberemos tener en cuenta los siguientes conceptos:

- 1.Dirección IPv4,
- 2.Máscara de red
3. Puerta de enlace
- 4.Servidor DNS preferido
- 5.Servidor DNS Secundario

2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS



2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS



2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED.SISTEMAS WINDOWS

Configuración IPv6 en Windows

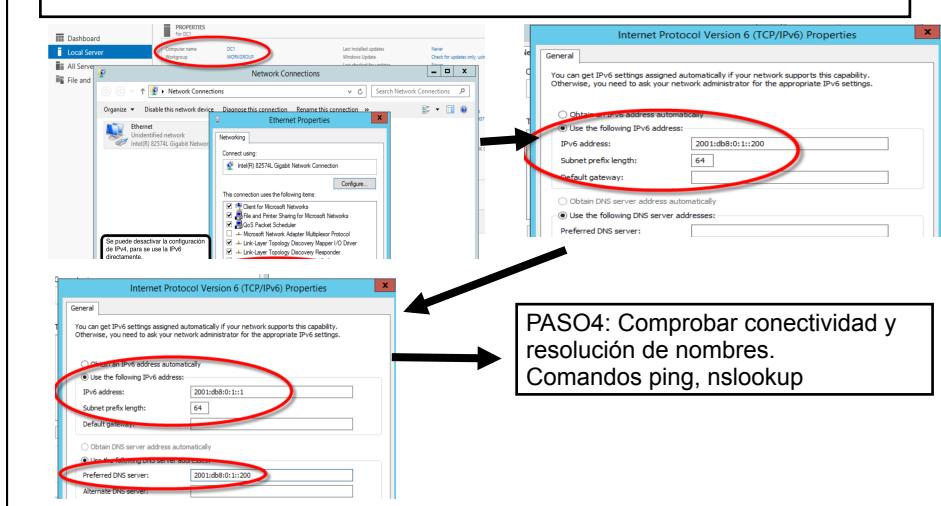
Ante la falta de direcciones IPv4 para todo el mundo debido a el número de equipos a nivel mundial, se crearon las IP's tipo IPv6. Como vimos en el tema de redes. Para su configuración debemos realizar lo siguiente una vez que el administrador de redes haya realizado el subnetting adecuado y nos haya proporcionado la ipv6 correspondiente. La forma de configurarla es la siguiente:

(El problema actual es que los routers suelen estar configurados en ipv4, por lo que la ipv6 aún no está extendida como se preveía en un inicio).

2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED

Ejemplo de configuración:

Se configura manualmente una dirección IPv6 en la máquina DC1: 2001:db8:0:1::200/64, que es el rango definido por la RFC 3849 (<http://tools.ietf.org/html/rfc3849>) para usar en documentación, aunque con una máscara más amplia /64).



2. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED. SISTEMAS WINDOWS

Configuración dinámica de red automática

A veces, es conveniente que la configuración de red no sea manual. En estos casos, se utilizaría un **servicio de DHCP**. Este servicio, nos dará la concesión de una dirección IP durante un tiempo determinado. Este tipo de servicios se usan muy comúnmente en las máquinas virtuales. (En ese caso, no es necesario configurar manualmente la configuración TCP/IP) o en cualquier red wifi en la que no tengamos acceso fijo. En estos casos, cada vez que nos conectemos a esa red el servicio nos proporcionará una configuración TCP/IP para conectarnos a esa red sin preocuparnos de nada más.

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

1. Direcciones IP.
2. Máscaras de subred IPv4/IPv6.
3. Configuración estática
4. Configuración dinámica automática (Servicio DHCP).

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

En versiones anteriores de ubuntu, así como en distribuciones basados en debian (que lo mantienen), la configuración de red se realizaba editando el archivo /etc/network/interfaces.

Esto ha cambiado en algunas distribuciones como es Ubuntu server. En este caso, es necesario el uso de la herramienta netplan.

Esta herramienta crea un archivo de configuración con extensión “yaml” en el directorio /etc/netplan/.....yaml. (Por ejemplo: /etc/netplan/50-cloud-init.yaml)

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

CONFIGURACIÓN DINÁMICA UBUNTU SERVER 19 (POR DHCP)

PASO 1: Editamos el archivo /etc/netplan/50-cloud-init.yaml

PASO2: Configuramos las siguientes líneas:

network:
Version: 2
Renderer: networkd
Ethernets:
Enp0s8:
Dhcp4: true
Dhcp 6: true
PASO 3: Guardar cambios
y salir.

PASO 4: Aplicamos cambios
con el comando:

Sudo netplan apply

PASO 5: Comprobamos con ifconfig -a

```
GNU nano 3.2                               /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
network: {config: disabled}
network:
ethernets:
enp0s3:
    dhcp4: true
    renderer: networkd
version: 2
ethernets:
enp0s8:
    dhcp4: true
    dhcp6: true
```

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

CONFIGURACIÓN RED ESTÁTICA EN UBUNTU SERVER 19

PASO 1: sudo nano /etc/netplan/50-cloud-init.yaml

PASO2: Si el instalador de la distribución no crea el archivo YAML, lo generamos con el comando:
Sudo netplan generate

PASO 3: Vemos el archivo de configuración

PASO 4: Se debe añadir lo siguiente:

- Nombre de la interfaz de red
- Hemos deshabilitado DHCP (IPv4 y IPv6)
- Hemos asignado la dirección IP.
- Se ha asignado la dirección de la puerta de enlace
- Se han definido los servidores DNS

```
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

```
enp0s8:
  dhcp4: no
  dhcp6: no
  addresses: [192.168.0.15/24, ]
  gateway4: 192.168.0.1
  nameservers:
    addresses: [8.8.8.8, 8.8.4.4]
```

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

PASO 5: Guardamos cambios (ctrl+o y salimos ctrl+x)

PASO 6: Aplicamos cambios:
sudo netplan apply

PASO 7: Reiniciamos el servicio de red
Systemctl restart networking

PASO 8: Comprobamos conectividad
ifconfig -a

```
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
  enp0s8:
    dhcp4: no
    dhcp6: no
    addresses: [192.168.0.15/24, ]
    gateway4: 192.168.0.1
    nameservers:
      addresses: [8.8.8.8, 8.8.4.4]
```

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

Configuración Servidor de nombres (DNS)

La dirección de DNS se almacena en el archivo de configuración:

/etc/resolv.conf

nameserver 127.0.0.1

Aunque inicialmente apunta al servidor local (127.0.0.1) se debe cambiar por una dirección de un servidor público (salvo que queramos que todas las direcciones nos las resuelva nuestro equipo)

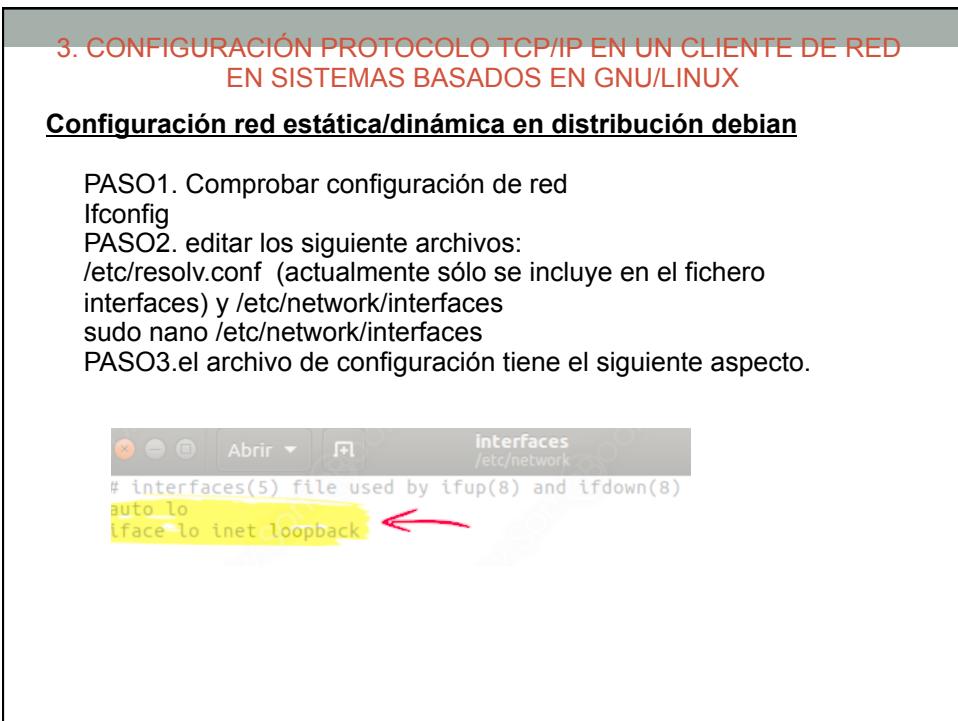
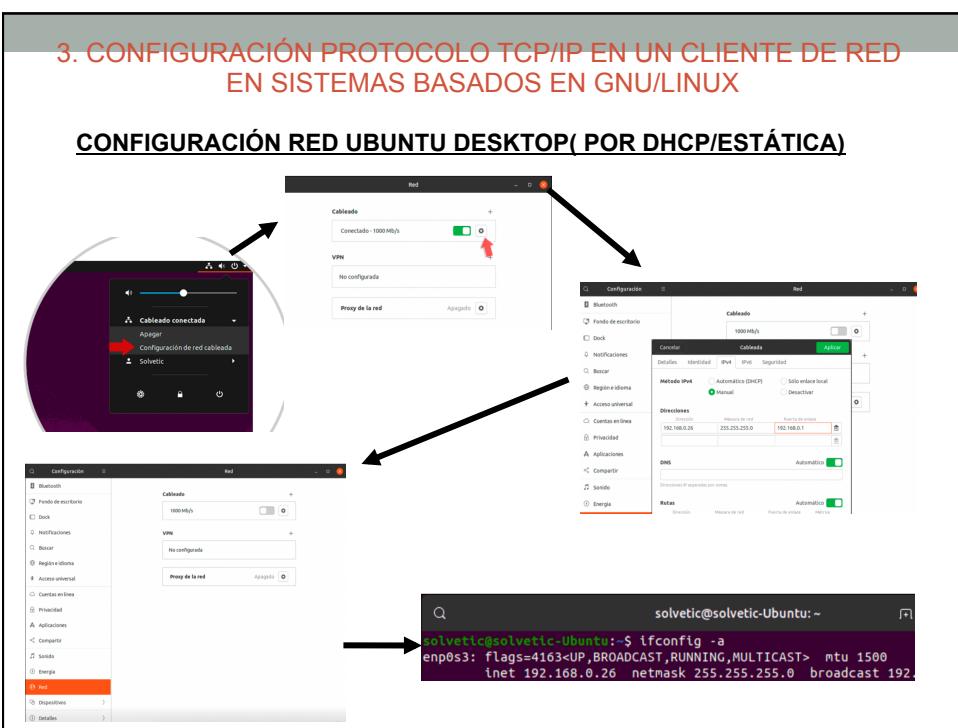
3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

Configuración dinámica/estática IPv4

BIBLIOGRAFÍA REFERENCIA

<https://www.solvetic.com/tutoriales/article/7580-como-configurar-direccion-ip-estatica-o-dhcp-en-ubuntu-19-04/>

<https://aprendiendoavirtualizar.com/configurar-ip-estatica-en-ubuntu-server-18-04/>



3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

Paso 4. Añadimos la información de la primera interfaz de red "eth0".

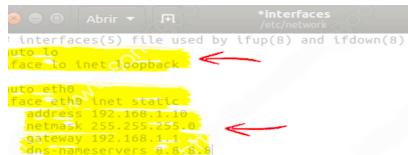
Incluimos la siguiente líneas para la configuración automática o por DHCP:

auto eth0

iface eth0 inet dhcp

Si es la configuración estática, incluiremos en la línea iface la palabra static y la información de configuración ipv4.

```
auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8
```



```
auto eth0
iface eth0 inet static
    address 192.168.1.10
    netmask 255.255.255.0
    gateway 192.168.1.1
    dns-nameservers 8.8.8.8
```

El archivo quedará tal que así

Paso 5. Reiniciar el servicio mediante el siguiente comando
sudo service network-manager restart

```
sudo service network-manager restart
```

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

Bibliografía configuración de red en sistemas debian:

<https://www.linuxito.com/gnu-linux/nivel-medio/136-configurar-interfaces-de-red-en-debian-ubuntu>

<http://somebooks.es/configurar-la-red-ubuntu-modificando-archivo-configuration/>

3. CONFIGURACIÓN PROTOCOLO TCP/IP EN UN CLIENTE DE RED EN SISTEMAS BASADOS EN GNU/LINUX

Archivos adicionales de configuración de red

/etc/hosts: Contiene una tabla de nombres de host para las direcciones IP.

/etc/hostname: Contiene el nombre del equipo (que debe ser único en la red).

/etc/nsswitch.conf

4. COMANDOS GESTIÓN REDES

1. Gestión de puertos.
2. Resolución de problemas de conectividad en sistemas operativos en red.
3. Comandos utilizados en sistemas operativos libres y propietarios.
4. Monitorización de redes.

4. COMANDOS GESTIÓN REDES

Ifconfig: Muestra la configuración de red.

eth0: dispositivo principal.

ens33: dispositivo principal.

enp0s3: dispositivo principal.

lo: Dispositivo de lookback

Palabra clave “UP”: dispositivo está activo.

El comando ifconfig en algunas distribuciones basadas en GNU/Linux se está volviendo obsoleto, de forma que se está reemplazando por el comando : **ip addr show**

En los sistemas actuales
Se pueden encontrar
Estas 3 nomenclaturas

4. COMANDOS GESTIÓN REDES

Comando route: Se usa para ver la tabla donde se envian los paquetes de red.

La opción –n nos proporcionará los datos de forma numérica.

Este comando se está volviendo obsoleto en algunas distribuciones y se va cambiando por **ip route show**.

Comando ping: Se usa para comprobar la accesibilidad.

La opción –c limita los pings a enviar, ya que este comando hace que se envíen paquetes una y otra vez.

4. COMANDOS GESTIÓN REDES

Comando netstat:

Nos muestra las conexiones de red, así como la tabla de enrutamiento muy similar al comando route.

Una de las funciones principales de este comando es el de comprobar los puertos abiertos de nuestro sistema.

Un puerto se identifica por un número y suele ir asociado a un servicio. Si este puerto está abierto, significa que este servicio está disponible para otros host.

Ejemplo: El servicio SSH tiene asignado el número de puerto 22.

Las opciones -tln nos mostrará todos los puertos abiertos.(-t : TCP,-l: listening (puertos que están escuchando),-n : mostrar números en lugar de nombres).

La opción -i muestra las estadísticas acerca del tráfico de red.

La opción -r muestra la información de enrutamiento.

En algunas distribuciones basadas en GNU/Linux se especifica que este comando está obsoleto, y reemplazado por ss y por ip route. Aunque, lo cierto es que el comando netstat sigue siendo ampliamente usado.

4. COMANDOS GESTIÓN REDES

Comando dig:Probar la funcionalidad del servidor DNS utilizado por tu host.

dig ejemplo.com especifica la ip del host ejemplo.com.

Comando host:Asocia un nombre de host a una dirección ip.Ejemplo :
host ejemplo.com

También funciona en sentido inverso, incluyendo la dirección ip.

Existen otras opciones para consultar información sobre DNS, como por ejemplo CNAME,SOA usando la opción -t.

La opción -a nos proporciona toda la información sobre

4. COMANDOS GESTIÓN REDES

Comando ssh: Permite la conexión a otra máquina a través de la red, permitiendo el inicio de sesión y la realización de tareas en el equipo remoto.

ssh (inicio de sesión con el mismo nombre con el que estás actualmente registrado).

ssh username@hostname:

5. Redes inalámbricas- Configuración segura

Conceptos básicos sobre redes inalámbricas.
Tipos, características
Riesgos
Configuración de las WLANs
Configuración del router
Medidas de seguridad básica y avanzada.

5.Redes inalámbricas-Configuración segura

En cuanto a redes inalámbricas, existen una serie de estándares a tener en cuenta:

802.11:Estándar que sirve de base en la comunicación de redes inalámbricas.
(Admite la transferencia de datos a 1Mbps)

802.11b:Transferencia de datos hasta 11 Mbps en la banda de 2,4GHz.

IEEE 802.11g: Banda de 2,4GHz. Velocidad transmisión 54Mbps.

5.Redes inalámbricas-Configuración segura

IEEE 802.11n:Comunicación con dispositivos que utilicen tanto la frecuencia de 2,4GHz. Transferencia de datos a velocidades de hasta 600Mbps.

IEEE 802.11 ac:Estándar para la banda de 5GHz. Su mayor novedad es la velocidad de 1733 Mbps.

5.Redes inalámbricas-Configuración segura

Trabajo de investigación

<https://www.xatakahome.com/la-red-local/nuevo-estandar-conexion-inalambrica-realidad-wifi-alliance-acaba-lanzar-oficialmente-wifi-6>

5.Redes inalámbricas-Configuración segura

Hoy en día el uso de tecnología inalámbrica está tan extendida que nadie concibe un sistema en el que sean necesarios los cables.

Estamos inmersos en una era inalámbrica en las que los ordenadores personales, Smartphone, tables y elementos incluidos en lo que llamamos “Internet de las cosas” incorporan de forma nativa la posibilidad de interconectarse inalámbricamente.

5. Redes inalámbricas-Configuración segura

Las redes inalámbricas se dividen en los tipos “modo Ad hoc”, donde no existen puntos de acceso o routers. Los dispositivos clientes se comunican entre sí directamente. A diferencia del tipo “infraestructura” donde es necesario del uso de puntos de acceso o routers.

5. Redes inalámbricas-Configuración segura

Las redes inalámbricas se entienden como una **extensión** de una red de ordenadores interconectados físicamente, por cable, con un único objetivo: proporcionar libertad de movimientos evitando tener que situarse en una ubicación física determinada a la hora de conectarse a los recursos que pueda ofrecer una organización.

5. Redes inalámbricas-Configuración segura

Definiremos como red inalámbrica , aquella formada por dispositivos capaces de intercomunicarse entre sí o con otra red (como internet), sin necesidad de elementos físicos que las conecten como pueden ser los cables.

Teniendo en cuenta que existen muchos tipos de redes inalámbricas

5. Redes inalámbricas-Configuración segura

Riesgos redes inalámbricas

Al tratarse de una tecnología inalámbrica, cualquier que se encuentre dentro de su rango de acción podría llevar a cabo acciones maliciosas. Podemos encontrar las siguientes tipos de amenazas.

Denegación de servicio (DoS): Incapacitar la infraestructura inalámbrica a través de peticiones de servicio masivas a los puntos de acceso, provocando la incapacidad de atender a tantas peticiones. Se busca sobrecargar el punto de acceso o Router e impedir a los usuarios legítimos el uso de los servicios que este presta.

Man-in-middle: El atacante puede situarse entre el emisor y el receptor, suplantando una de las partes y haciendo creer a la otra que está hablando con el legítimo destinatario de la comunicación, o incluso suplantando al punto de acceso (Rogue Access Point).

Ataques por fuerza bruta: Método consistente en hacer uso de todas las contraseñas posibles cuya finalidad es averiguar las claves criptográficas de la comunicación o de las que dan acceso a la red wifi.

5. Redes inalámbricas-Configuración segura

Eavesdropping: Captura de tráfico de red no autorizado realizado a través de alguna herramienta como antenas de gran alcance. El objetivo es capturar la información que transmitimos, que podría ser completa si no se encuentra cifrada o, en caso contrario, hacerse con patrones de comportamiento para intentar un descifrado.

MAC Spoofing: Suplantar la dirección MAC de un dispositivo permitido cuando el punto de acceso tenga configurada una lista de este tipo de direcciones permitidas.

5. Redes inalámbricas-Configuración segura

CONFIGURACIÓN SEGURIDAD EN REDES WLAN

• Reflejar cuál será la arquitectura de seguridad

- Es una cuestión documental donde se especificará cómo está diseñada la red inalámbrica y cuál será su sistema de gestión, reflejando aspectos como los siguientes.
 - Cobertura de puntos de acceso.
 - Los dispositivos para llevar a cabo el servicio, así como para conectar otros puntos de acceso entre sí.

5. Redes inalámbricas-Configuración segura

- **Autenticación**

Se debe establecer el tipo de autenticación de red (a través de claves precompartidas o a través de mecanismos de autenticación mutua).

Método de claves precompartidas (PSK), se basa en su funcionalidad en la existencia de una única clave de conexión a la red inalámbrica compartida por todos los equipos y usuarios.

Método autenticación mutua: Método que permite un proceso de autenticación en el que cada cliente dispondrá de sus propias credenciales de acceso. Este método requerirá de infraestructura basada en un servidor de autenticación. Es un método más seguro.

5. Redes inalámbricas-Configuración segura

El servidor se autentica frente al cliente a través de un certificado, mientras que para la autenticación del cliente se utilizan mecanismos de un solo factor, como contraseñas, tokens, etc.

En el caso de uso de contraseñas, deberán ser lo más robustas posibles, aplicándose una política de contraseñas especificada que suele ser la inclusión de una combinación de al menos 8 dígitos que combinen minúsculas, mayúsculas, números y caracteres especiales), tiempo de renovación, intentos máximos permitidos. (entre otros).

Distinción entre dispositivos corporativos y clientes externos:

La correcta configuración de seguridad en ámbitos empresariales pasan por distinguir entre los equipos que serán considerados como corporativos (bajo control de la organización y sus políticas de seguridad) y de personal externo (no sujetos a control de la organización). Estos últimos deberán estar restringidos en cuanto a permisos de acceso, de forma que sólo deberán acceder a los recursos abiertos o de acceso público.

5. Redes inalámbricas-Configuración segura

Monitorización

Cuando hablamos de seguridad en rede inalámbricas, la monitorización de la seguridad es un aspecto prioritario y conocer el estado de seguridad, es necesario en cuanto a la monitorización de :

Posibles ataques por parte de individuo no autorizado (alcance o interrupción de las comunicaciones inalámbricas).

Vulnerabilidades: Aplicación de parches de seguridad y verificación/ modificación de las configuraciones de seguridad.

5. Redes inalámbricas- Configuración segura

El router y las medidas de seguridad

- Los riesgos de un router mal configurado:
- Robo de información confidencial
- Utilizar la red para realizar acciones ilegales.
- Vinculación con lo que ocurra en tu red.
- Infectar los dispositivos con malware.
- Disminución del ancho de banda.

5. Redes inalámbricas- Configuración segura

Medidas de seguridad básica:

- Cambiar la contraseña de acceso al router.
- Modificar el nombre de la red wifi o (SSID).
- Contraseña de acceso a la red wifi robusta.
- Actualización del firmware.
- Configuración red wifi con cifrado (WPA2 o WPA3).
- Desactivar WPS. (es un mecanismo que facilita la conexión de dispositivos con nuestro router a través de código PIN de 8 dígitos).
- Configurar red wifi de invitados, si el router lo permite.

5. Redes inalámbricas- Configuración segura

Medidas de seguridad complementarias:

- Habilitar filtrado por dirección MAC.
- Reducir los rangos de direcciones permitidas.
- Limitar la potencia de emisión de las antenas.
- Deshabilitar la administración remota.

Control de equipos en la red.

Deshabilitar UPnP (Esto permite a los dispositivos en la red descubrirse entre ellos mismos dentro de la red por tanto introduce riesgos de seguridad).

Apaga el router.

5. Redes inalámbricas- Configuración segura

Medidas avanzadas

- Uso de sistemas IDS (sistema de detección de intrusiones) o IPS (Sw que controla los accesos a la red).

5. Cifrado de red Wi-Fi

Una de las cosas más importantes en la configuración de los routers en cuanto a redes inalámbricas, es el cifrado. Normalmente, se ofrecían tres modalidades de cifrado: WEP, WPA y WPA2. Se recomendaba habilitar WPA2-PSK(AES).

5.Cifrado de red Wi-Fi

No obstante debido a la vulnerabilidad detectada en Oct. 2017 llamada “ataque KRACK”. Que permitía a un atacante interceptar, descifrar y manipular el tráfico de una red inalámbrica con el tipo de cifrado anteriormente mencionado

Se ha desarrollado una nueva versión del protocolo WPA llamada WPA3.

5.Cifrado de red Wi-Fi

WPA (Wi-fi Protected Access), es un estándar dirigido a la protección de los dispositivos, como los routers, de tal manera que nadie ajeno pueda acceder a los datos de forma inalámbrica.

5. Redes inalámbricas-Configuración segura

Características WPA3

Se ha presentado para redes inalámbricas personales, empresariales y también para el Internet de las cosas (IoT).

Permite protección mejorada frente ataque de fuerza bruta sin conexión, haciendo mucho más difícil que un atacante pueda averiguar una contraseña.

5. Redes inalámbricas-Configuración segura

WPA3 Forward Secrecy. Evitará que un atacante pudiera descifrar el tráfico capturado, incluso aunque hubieran conseguido la clave en otra ocasión.

Protección de redes públicas abiertas.

Aunque la seguridad haya sido reforzada a través de cifrado de datos individualizado, cifrando el tráfico inalámbrico entre nuestros dispositivos y el punto de acceso wifi. La conexión a redes abiertas es una práctica desaconsejada.

5. Redes inalámbricas-Configuración segura

Cifrado fuerte para redes sensibles.

Ofreciendo a las redes wifi que controlan información confidencial proteger las conexiones con un cifrado más robusto,

cuya clave ha de ser de 128 a 192 bits.

Cuanto mayor sea la clave, más difícil será romper el cifrado.

5. Redes inalámbricas-Configuración segura

Conclusión:

No es recomendable el cifrado WEP, ya que es muy inseguro y fácil de ser atacado para conseguir la contraseña de la red WIFI en un tiempo pequeño.

Trabajo: Haz un trabajo sobre los diferentes cifrados usados hasta el momento, sus características y vulnerabilidades.

5.Redes inalámbricas-Configuración segura

Monitorización redes

Existen múltiples herramientas para la monitorización de la red. En el siguiente enlace podéis ver bastantes. Así mismo, podemos buscar más por medio de un buscador de Internet.

<https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/>

5.Redes inalámbricas-Configuración segura

Haz un esquema con al menos 5 herramientas de monitorización del enlace anterior o de algún buscador.

- Características.
- Tipo de licencia.
- Propósito.
- Además instala una de ellas y muestra la monitorización de tu red de casa.