

ENTENDIENDO CONCEPTOS RED

Trabajo de Alejandro Sainz Sainz

SISTEMAS
INFORMÁTICOS
24-25

INTRODUCCIÓN	3
DESCRIPCIÓN	¡Error! Marcador no definido.
TOPOLOGÍA HÍBRIDA	¡Error! Marcador no definido.
VENTAJAS Y DESVENTAJAS	¡Error! Marcador no definido.
EJEMPLOS DE USO REAL	¡Error! Marcador no definido.
CONCLUSIÓN Y REFLEXIÓN	3
BIBLIOGRAFIA Y ENLACES	15

Alejandro Sainz Sainz

TABLA DE FIGURAS

1 Tipología híbrida: Anillo más árbol.....*¡Error! Marcador no definido.*

2 Las variables son casi ilimitadas.....*¡Error! Marcador no definido.*

INTRODUCCIÓN

Vamos a realizar una serie de ejercicios variados referentes al tema de redes. Como no hay mucho más que explicar vamos al lío.

EJERCICIO 1

Indicar el tipo de la IP 172.16.0.12.

Hasta donde yo creo es del tipo b, ya que las de tipo A son del 0 al 127 y las del tipo B son del 128 al 191.

Dado que esta es 172 considero que es del tipo B.

EJERCICIO 2

Escribir en binario la IP 192.168.1.1

11000000.10101000.00000001.00000001

Como esta red empieza por 192 es del tipo C.

EJERCICIO 3

Indica para que están pensadas las siguientes IPs.

127.0.0.1 – Imagino que para host ya que no acaba en 0.

192.168.1.0 – IP de un host de una red.

192.168.1.255 – Al ser el último dígito 255 es una IP de broadcast.

0.0.0.0 – Dirección especial. No se exactamente para que se usa.

Alejandro Sainz Sainz

10.0.0.15 – Supongo que dirección de host, aunque me suena que las IPs que empiezan por 10 se usan para alguna cosa en especial.

EJERCICIO 4

Dada la IP 192.168.2.101 y la máscara 255.255.255.192 indica la red, la ip de broadcast y el número de hosts disponibles para esa red.

Lo primero vamos a pasar la máscara de red a binario

11111111.11111111.11111111.11000000

Ahora podemos cambiar la notación de la IP a lo siguiente 192.168.2.101/26

Esto quiere decir que tenemos 6 bits para determinar el número de hosts.

Sabiendo que son 6 bits ya podemos saber uno de los datos que es que el número máximo de hosts dentro de esa red son 64, con dos direcciones reservadas para red y broadcast por lo que el número de hosts van a ser 62.

Si tenemos 64 hosts por red, esta va a ir creciendo de la siguiente forma:

0-63

64-127.

Como la IP que se nos da es la 101 podemos indicar el resto de aspectos que se nos piden.

Dirección de red 192.168.2.64.

Dirección de broadcast 192.168.2.127.

EJERCICIO 5

Dada la IP 192.168.10.0/26 indicar dirección de red, de broadcast y número máximo de hosts.

Como en el caso anterior si es /26 quiere decir que tenemos 6 bits para indicar hosts.

Eso nos indica que el número máximo de hosts van a ser 64.

Con la IP que nos han dado podremos saber que la red va a ser las 192.168.10.0.

La dirección de broadcast, al tener un máximo de 64 hosts va a ser la 192.168.10.63.

Los hosts que puede tener la red es 2 elevado a 6 menos 2, por lo tanto 62 hosts.

Alejandro Sainz Sainz

La primera dirección asignable va a ser la 192.168.10.1 y la última va a ser la 192.168.10.62, ya que como sabemos hay dos direcciones reservadas, la primera o 0 y la última o 63.

EJERCICIO 6

Limitación de IPV4 sobre IPV6.

La limitación principal es la cantidad total de direcciones IP que se pueden crear ya que sólo usa 32 bits para generar combinaciones de redes.

Las direcciones IPV6 usan 128 bits, lo que ofrece una mayor cantidad de redes y subredes posibles de generar. Estos 128 bits se dividen en 8 grupos de 4 dígitos alfanuméricos, cada grupo representado por 16 bits en vez de 8.

Un ejemplo de red IPv6

2001:0db8:85a3:0000:0000:8a2e:0370:7334

EJERCICIO 7

Porque crees que muchas direcciones locales utilizan redes de clase C como por ejemplo 192.168.x.x

Porque no requieren de una gran cantidad de hosts dentro de cada red o subred. Las redes de clase C son aquellas que destinan menos número de bits para calcular los hosts que pueden pertenecer a una red y dado que las redes domésticas, las oficinas pequeñas e incluso departamentos de empresas no requieren de un número muy elevado de hosts se suelen decantar por las redes de tipo C, ya que en estas redes se pueden definir muchas subredes con un número de equipos más reducidos.

Alejandro Sainz Sainz

EJERCICIO 8

Diferencias entre IPs estáticas y Dinámicas.

Mediante la configuración de IP estáticas nosotros creamos una dirección de red fija y asignamos a cada elemento una IP que definiremos nosotros mismos y que será siempre la misma para cada equipo. Podríamos decir que un equipo es dueño de su dirección IP.

Ventajas: Mayor control sobre la red ya que nosotros decidimos como se va a configurar.

Las rutas estáticas no se anuncian a través de la red, lo que las hace más seguras.

Desventajas : Mucho más trabajo a la hora de configurarlas ya que cada equipo debe de configurarse manualmente.

Se pueden dar casos de solapamientos de IP, es decir, si nos equivocamos y damos la misma IP a varios equipos, algunos de ellos no podrán conectarse.

Mediante la configuración de IP dinámica nosotros configuramos nuestro router o nuestro servidor para que el asigne las IPs disponibles entre los equipos que lo soliciten. A cada equipo que se conecte se le asignará la primera libre disponible de entre todas las que estén dentro del rango designado.

Ventajas: Es más desatendido, ya que es el router o el servidor el que se encarga de asignar las IPs libres.

Mucho más fácil de configurar que el direccionamiento estático.

Desventajas: Es un tipo de red más vulnerable, dada su naturaleza.

Una caída del servicio DHCP deja sin servicio a todos los equipos.

EJERCICIO 9

Imagina que montas un servidor web en tu casa, usarías direccionamiento estático o dinámico.

En el caso de que yo instalase un servidor web en mi casa, y suponiendo que quiera poder acceder a él desde el exterior de mi red usaría enrutamiento estático, ya que con una ip fija me es mucho más fácil localizarle y acceder a él. Incluso si sólo quisiese usarle dentro de mi red

Alejandro Sainz Sainz

interna lo haría con estático, para que el servidor web tenga siempre la misma dirección y sea mucho más fácil acceder a él ya que siempre va a tener la misma IP.

EJERCICIO 10

Para configurar una dirección de red estática en Windows vs Linux.

En Windows debería de acceder al adaptador de red, acceder a sus propiedades, a la sección de IPv4 y allí indicaría la dirección IP fija que he designado, la máscara de subred, tanto si es una red estándar o una personalizada. También indicaría la dirección del servidor DNS y de la Gateway.

En Linux, de forma rápida, por terminal se podría hacer de la siguiente forma

```
ip addr add 192.168.1.11/24 dev eth0
```

Con este comando, que escribe estos valores en el archivo `/etc/sysconfig/network/ifcfg-eth0`.

Hora explicamos cada parte.

`Ip addr` es el comando que indica que vamos a asignar una dirección (`addr` de `addres`) `Ip` (`ip`) a un elemento del sistema.

`Add` viene de añadir, se explica solo.

`192.168.1.11/24` – Esto nos indica la dirección IP y el `/24` nos indica la máscara de subred que va a ser `255.255.255.0`.

`Dev` en Linux se refiere a `device` (una pieza de hardware o dispositivo), para cualquier dispositivo, siempre se empieza por `dev`, ya sean discos duros, tarjetas gráficas, etc.

`Eth0` – se refiere a `ethernet 0`. El dispositivo de red que Linux usa por defecto es el `dev eth0`, o es decir, el dispositivo de red primario o por defecto.

Alejandro Sainz Sainz

EJERCICIO 11

Comandos para ver la configuración de red en Windows y en Linux.

Para ver la configuración IP en Windows usamos el comando Ipconfig y para Linux el comando Ifconfig.

EJERCICIO 12

Dada la configuración que se proporciona en el ejercicio que es una ip fija si se configura otro equipo con la misma ip no se van a poder conectar los dos a la vez ya que se va a generar un conflicto de red y, normalmente, el primero que se conecta es el que tiene conectividad y el segundo a tragar humo.

EJERCICIO 13

Dada la ip 192.168.1.34 y la máscara 255.255.255.224

Vamos a empezar indicando que dada la máscara de red termina en 11100000 que es 224 en binario. Eso quiere decir que tenemos cinco bits para determinar los hosts.

Así que podemos indicar la ip como 192.168.1.34/27

Con esos 5 bits podremos asignar un máximo de 32 hosts, de los cuales 2 están reservados y los otros 30 son los disponibles.

Las redes o subredes van a ir cambiando de la siguiente forma:

0-31

32-63

64-95

Como la IP es 192.168.1.34 ya sabemos que está en el segundo rango de redes, por lo tanto:

Dirección de red 192.168.1.32.

Alejandro Sainz Sainz

Dirección de broadcast 192.168.1.63.

Numero de hosts disponibles 30, ya que hay que restar 2 a los 32 disponibles.

Primer y último host asignable : Del 33 al 62.

EJERCICIO 14

Notación CIDR. Indicar que es y transformar los ejemplos.

La notación CIDR es aquella que nos indica cual es la máscara de subred mediante el número de bits que son 1, por ejemplo, si la máscara es 255.255.255.255 quiere decir que todos los bits son 1, así que la notación CIDR será /32. Para otras máscaras debemos de restar el número de bits que son 0 de 32 y así obtendremos diferentes notaciones, ya sean /28 /25 etc.

255.255.255.0 - /24

255.255.254.0 - /23

255.255.255.248 - /29

EJERCICIO 15

Diseñar una red para 50 dispositivos, que mascara usaría y por qué.


Dado que tengo que asegurarme que las subredes no pueden abarcar rangos exactos al 100%, es decir, que su tamaño va a depender de los bits libres para los hosts. Como estos se calculan en base dos, vamos a tener disponibles 2,4,8,16,32,64.

Por lo tanto, para tener una subred de 50 dispositivos vamos a tener que crear una con capacidad para 64. Para crear una red así debemos de dejar 5 bits libres que son los que nos permiten alcanzar 64 valores, desde el 0 al 63.


Sabiendo ya todo esto la máscara de subred sería 255.255.255.224.

EJERCICIO 16


DIRECCIÓN IP

192.168.1.34 


decimal

255.255.255.224 

bits

27 

hexa

ff.ff.ff.e0 

192.168.1.34 / 27**RED**
192.168.1.32 / 27**RANGO HOSTS (30 hosts)**
192.168.1.33 - 192.168.1.62**BROADCAST**
192.168.1.63**TIPO**
IP PRIVADA - CLASE C**HEXADECIMAL**
C0.A8.01.22**BINARIO**
11000000.10101000.00000001.00100010

red subred host

CÁLCULO DE SUBRED

decimal

255.255.255.224 

bits

27 

hexa

ff.ff.ff.e0 

Pues en principio sí, coincide con lo que yo he calculado.

Alejandro Sainz Sainz

EJERCICIO 17

Funcionamiento de los servicios DNS.

Los servicios DNS son (Domain Name Services) o servicios de resolución de nombre.

Lo que hacen estos servicios o servidores es traducir los nombres asignados a direcciones IP por el valor de su dirección IP, ya que para nosotros es más fácil acordarnos de los nombres que de los valores de las direcciones IP.

Esos nombres y sus direcciones IPs correspondientes se guardan en tablas, y cuando nosotros hacemos una solicitud en el navegador pidiendo ir a una página como www.google.com los protocolos de la red nos van a llevar primero a un servidor DNS que tenga almacenado en su tabla la dirección IP del nombre que hemos solicitado y nos va a devolver esa IP para que sepamos a donde tenemos que ir.

EJERCICIO 18

Que es la caché DNS, ventajas y riesgos.

La cache DNS nos permite almacenar en nuestro propio equipo, o router, o dispositivo las direcciones IP de los sitios a los que hemos accedido, lo que hace que cuando volvamos a visitarlos ya no tenemos que solicitar la dirección al servidor DNS más cercano.

Esta cache es como una libreta de direcciones o una guía telefónica propia, de los sitios ya visitados, que hace que nuevas visitas o consultas se resuelvan más rápido. Esa es su principal ventaja.

La principal desventaja son los ataques de man in the middle, de phishing, etc. que modifican estos datos en los servidores DNS o quedan almacenados en nuestra caché y luego empiezan a aparecer pop ups extraños en nuestro equipo, porque el propio equipo, al tener esa dirección asignada vuelve directamente a esos sitios maliciosos cuando nosotros pensamos que estamos yendo a una página segura.

Alejandro Sainz Sainz

EJERCICIO 19

Que información tiene el archivo `/etc/host` en Linux y el archivo `hosts` en Windows?

Hasta donde yo sé el archivo `hosts` existe en todos los sistemas operativos y es una suerte de DNS local para resolver nombres. En ese archivo encontramos nombres de sitios o equipos y su ip asociada, así el equipo puede resolver la dirección cada vez que nos conectamos a una red.

EJERCICIO 20

Los servidores DNS públicos, como su nombre indica, son servidores DNS de acceso gratuito a los que nos podemos conectar para resolver las direcciones ip de los sitios a los que nos queremos conectar.

Dos de los más conocidos:

Google public DNS: que suele ser el más conocido y al que más nos unimos todos a la hora de resolver nombres. Su dirección IP es la 8.8.8.8.

Cloudflare: Es otra alternativa, algunos dicen que respeta más la privacidad, pero los de la liga de futbol banean sus servidores cada vez que hay partido importante. 1.1.1.1

EJERCICIO 21

DNS y seguridad. El ataque más común es el DDoS, o ataque de denegación de servicios.

Este ataque consiste en realizar peticiones al servidor DNS de forma masiva hasta que este se caiga y deje sin servicio a los usuarios. También se puede hacer generando conexiones que manden los datos de manera muy lenta por lo que el servidor consume más recursos por conexión y al sumarlo a una cantidad elevada de peticiones se cae de la misma forma.

Por comentar, también existe otro tipo de ataque en el que se modifican las tablas de los DNS y cuando buscamos una página por su nombre, el servidor nos manda a una dirección que no es la original, acabando así muchas veces en páginas de pocos principios éticos.

Alejandro Sainz Sainz

EJERCICIO 22

TCP. Es orientado a conexión, ya que establece una conexión virtual previa a la comunicación y que se mantiene a lo largo de la misma.

Es algo más lento que UDP ya que se asegura de que todos los datos lleguen de forma correcta y sin fallos, y eso hace que se reduzca ligeramente la velocidad.

Fiabilidad. Muy fiable ya que se encarga de certificar y asegurarse de que los paquetes lleguen de forma correcta y al destino requerido.

Los casos en los que más se usan son en la mayoría de los casos cualquiera que tenga que ver con servicios web.

UDP. No se orienta en la conexión. Solo se centra en enviar información.

Es el más rápido de los dos, se centra precisamente en eso, velocidad y transmisión de paquetes en tiempo real.

Fiabilidad. Bastante más baja que TCP. No certifica tanto la integridad en el envío de los paquetes. Está pensado para sistemas que pueden tolerar cierta cantidad de pérdidas de datos.

Casos de uso. Streaming, gaming, VoIP.

EJERCICIO 23

Asociar protocolos y puertos.

SMTP – 25

SSH – 22

HTTP – 80

HTTPS – 443

FTP – La verdad es que tiene bastantes. Dependiendo de diferentes tipos de servicios.

20,21 por poner dos ejemplos.

MySQL – 3306

EJERCICIO 24

Detección de puertos abiertos y comandos para conocerlo en Windows y Linux

Existe un comando para Windows y Linux (también para MAC) que se usa con este fin, que es el comando netstat.

La única diferencia entre cada sistema suelen ser las opciones de comandos adicionales. En cada sistema suelen ser distintas.

EJERCICIO 25

Puertos conocidos, registrados y dinámicos.

Los puertos conocidos son los primeros de la lista, los que van desde el 0 hasta el 1023. También se les llama puertos de sistema. Eso ya nos da una idea de cuales son sus usos. Básicos para los sistemas operativos.

Los puertos registrados son los que van desde el 1024 hasta el 49151 y son aquellos que ciertas aplicaciones ya tienen asignados de manera fija y que además quedan registrados en la IANA que es la que se encarga de indicar que entidades tienen asignada un puerto fijo a una aplicación.

Los puertos dinámicos, también llamados efímeros, son el resto de ellos, aquellos que sólo se usan de forma temporal y con un uso muy concreto y determinado.

EJERCICIO 26

Como se cierra manualmente un puerto en Windows mediante el firewall.

Yo espero que siga siendo como lo aprendí, pero en principio suele ser con las reglas de entrada y salida. En esas reglas yo puedo abrir o cerrar puertos, es decir, crear reglas que permitan o no tráfico a través de puertos determinados.

EJERCICIO 27

Por qué es importante el control de los puertos y cerrar los no utilizados?.

Porque gracias a los puertos podemos controlar las conexiones, por lo tanto, cerrar los puertos abiertos es un sistema de prevención contra ataques que se generan a través de la red o de conexiones que se crean con nuestro equipo.

Esto se debe a que el ataque más común de los hackers suele ser el scaneo de puertos, con ello buscan debilidades en nuestra red por donde pueden atacar a nuestro sistema.

CONCLUSIÓN Y REFLEXIÓN

Como en todo lo relacionado con la informática, las redes son otro agujero negro que te puede absorber durante horas para aprender cualquier cosa. Y como las redes, sus configuraciones y su funcionamiento es enorme nos podemos perder durante horas aprendiendo sobre el tema.

Desde que apareció internet tenemos que enfatizar mucho en la red y en como los equipos se comunican entre sí para poder comprender el porqué de las cosas.

BIBLIOGRAFIA Y ENLACES

<https://www.genbeta.com/web/son-los-ataques-ddos-efectivos-como-medio-de-protesta>

<https://ultahost.com/blog/es/una-guia-completa-y-comparacion-de-tcp-y-udp/>

https://es.wikipedia.org/wiki/Anexo:Puertos_de_red#Puertos_bien_conocidos

<https://www.fortinet.com/lat/resources/cyberglossary/what-is-port-scan>