

Administración de redes IP. Localización y manejo de problemas

Tabla de Contenidos

6. Administración de redes IP. Localización y manejo de problemas.....	2
6.1 consideraciones previas y recomendaciones.....	2
6.1.1 Requisitos estándar para la implantación física.....	2
6.2 Configuración local.....	4
6.3 Problemas de direccionamiento.....	7
6.4 Problemas de DNS.....	8
6.5 Caso de ejemplo.....	9
6.6- Consideraciones finales.....	10



6. Administración de redes IP. Localización y manejo de problemas

En la administración de una red local es fácil encontrar problemas de todo tipo, y una correcta metodología para afrontarlos nos sera de gran utilidad, además de ahorrarnos muchas horas de pruebas.

6.1 Consideraciones Previas Y Recomendaciones

Es necesario tomar en cuenta algunas consideraciones sobre las especificaciones de creación de una red local. En redes locales 10baseT es importante seguir unas especificaciones para no tener problemas, pero en redes 100baseTx y superiores es prácticamente imprescindible cumplir unos mínimos, ya que de otra forma pueden producirse bajas velocidades, o incluso la no conectividad entre ordenadores.

6.1.1 Requisitos Estándar Para La Implantación Física

En una red de Ethernet 10/100 habitual (100baseTX) es necesario un cable UTP (sin apantallar) o STP (apantallado, mucho menos habitual) de categoria 5 con conectores RJ-45. Para redes de velocidades superiores , como 10/100/1000 es necesario acudir a cableado de categoria 6 como minimo, y muy recomendablemente apantallado.

- El cable nunca debe doblarse en grados inferiores a 90°.
- La distancia de los cables de la red con respecto a los cables de corriente debe ser como minimo de 50 centímetros.
- Los cables de red y de energia eléctrica nunca podrán ir juntos y deben ir por senderos distintos.
- El cable de la red desde el ordenador hasta la pared debe medir como máximo 2.5 metros.
- Utilizar regleta de conexión para que el ordenador se conecte a la red a través de la regleta nunca directamente al Hub.

- Verificar con un comprobador los cables uno a uno hasta asegurarse de que este correctamente instalados y clipados pues puede ser un error frecuente en la red.
- Utilizar una caja de conexiones para conectar el hub con cada uno de los ordenadores , nunca directamente al Hub.
- La distancia maxima desde cada ordenador al hub principal no deberá superar los 90 metros a efectos prácticos. Cuanto mas largos, menor velocidad de transmisión.

Variedades de red Ethernet					
Tipo	Medio	Ancho de banda máximo	Longitud máxima de segmento	Topología Física	Topología Lógica
10Base5	Coaxial grueso	10 Mbps	500 m	Bus	Bus
10Base-T	UTP Cat 5	10 Mbps	100 m	Estrella; Estrella Extendida	Bus
10Base-FL	Fibra óptica multimodo	10 Mbps	2.000 m	Estrella	Bus
100Base-TX	UTP Cat 5	100 Mbps	100 m	Estrella	Bus
100Base-FX	Fibra óptica multimodo	100 Mbps	2.000 m	Estrella	Bus
1000Base-T	UTP Cat 5	1000 Mbps	100 m	Estrella	Bus

Siguiendo estas recomendaciones evitaremos problemas como baja velocidad o ruido en la transmisión, que pueden afectar seriamente al envío de datos, y , aunque se pueden producir errores físicos en el medio, se limitaran a casos puntuales, no a fallos de diseño.



6.2 Configuración Local

El problema inicial que podemos encontrar sera que una maquina no tenga conectividad con el resto de la red. Para poder llegar a una solución, deberemos realizar diversas comprobaciones. El primer paso seria comprobar si tenemos asignada una dirección IP. En Windows utilizaremos el comando `ipconfig`.

```
G:\Documents and Settings\1 - Khain>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : aristoteles
    Sufijo DNS principal . . . . . :
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado. . . . . : No
    Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexión de área local 4 :

    Sufijo de conexión específica DNS : gaia
    Descripción. . . . . : Realtek RTL8169/8110 Family Gigabit Ethernet NIC
    Dirección física. . . . . : 00-0D-61-4A-EC-A5
    DHCP habilitado. . . . . : No
    Autoconfiguración habilitada. . . : Sí
    Dirección IP. . . . . : 172.26.0.50
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . : 172.26.0.1
    Servidor DHCP . . . . . : 172.26.0.10
    Servidores DNS . . . . . : 195.235.113.3
    . . . . . : 195.235.96.90
    Concesión obtenida . . . . . : martes, 04 de mayo de 2004 6:26:47
    Concesión expira . . . . . : jueves, 06 de mayo de 2004 6:26:47
```

Introduciendo unicamente `ipconfig` obtendremos un resumen de los parámetros de red utilizados por cada uno de los dispositivos. `Ipconfig` admite varios parámetros, siendo los mas utilizados:

- `/all` - muestra un informe detallado de la configuración de cada dispositivo.
- `/release` - libera de forma manual la IP.
- `/renew` - se realiza una renegociación de la IP con el servidor DHCP.

Mediante `ipconfig ?` Se puede observar un listado completo de opciones disponibles para el comando.

En Linux , el comando equivalente, aunque mas potente, seria `ifconfig`

```

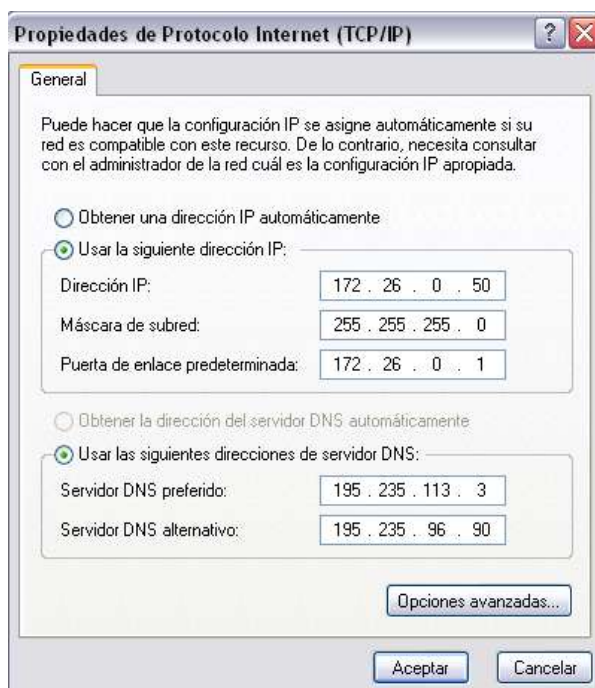
root@platon:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:04:AC:36:EF:4C
          inet addr:172.26.0.100  Bcast:172.26.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2303075 errors:0 dropped:0 overruns:0 frame:1
          TX packets:2498724 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:777551694 (741.5 MiB)  TX bytes:821204561 (783.1 MiB)
          Interrupt:11 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:380120 (371.2 KiB)  TX bytes:380120 (371.2 KiB)

```

En este caso , la configuración a comprobar sería la del dispositivo eth0, perteneciendo lo al loopback local.

Si comprobamos que no tenemos asignada una IP valida, deberemos entrar en la configuración específica de los parámetros de red del dispositivo, para realizar las configuraciones necesarias. Aquí , podremos comprobar si tenemos especificada una dirección dinámica asignada por nuestro servidor DHCP o es estática, y si esta pertenece al rango de nuestra red local, así como los diferentes parámetros necesarios, como servidores DNS, gateway por defecto, etc...



En Linux la configuración del dispositivo varía enormemente dependiendo de la distribución con la que estemos trabajando. Continuando con Debian, el fichero de configuración será */etc/network/interfaces*

```
# /etc/network/interfaces -- configuration file for ifup(8), ifdown(8)

# The loopback interface
# automatically added when updowning
auto lo eth0
iface lo inet loopback

iface eth0 inet static
    address 172.26.0.100
    netmask 255.255.255.0
    network 172.26.0.0
    broadcast 172.26.0.255
    gateway 172.26.0.1

~
~
~
~
```

Como se puede observar, en este fichero se indican la IP, máscara de red, dirección broadcast y gateway por defecto, pero no se especifican los DNS. Para poder modificarlos deberemos acudir a */etc/resolv.conf*.

Si en */etc/network/interfaces* tenemos configurado el dispositivo para que solicite IP a un servidor DHCP, deberíamos comprobar también que se tiene inicializado el daemon que se encarga de negociar con el servidor (dependiendo de la versión, también puede variar el nombre de este daemon, siendo actualmente los más habituales *dhclient*, *dhcpcd* o *dhcpcd3*).

Si hemos comprobado que tanto el dispositivo de red, como la configuración relacionada con nuestra red local están bien, pero la conexión no es posible, es necesario empezar las comprobaciones sobre los elementos físicos. Si hemos tenido en cuenta las especificaciones estándar sobre la creación de redes locales, los errores por mal diseño de la red quedarían reducidos al mínimo. Por tanto, será necesario revisar los cables mediante un **comprobador de cables**. Esto nos permitirá revisar todas las conexiones y poder localizar un tramo dañado que este impidiendo la conexión entre máquinas.



6.3 Problemas De Direccionamiento

La solución de problemas de direccionamiento es una de las tareas mas duras entre los problemas de red que podemos encontrar. Para una correcta planificación a la hora de abordar el problema es extremadamente útil la realización de un plano de la red con todos los elementos importantes, así como todos los parámetros de red de los elementos importantes de la misma.

Posteriormente, el uso adecuado de determinados comandos de red, nos podrán facilitar mucho la tarea de comprobar en que parte de la red esta fallando el envío. Los comando **route** y **netstat -r** en Linux nos mostraran la tabla de rutas.

```
root@platon:/etc/init.d# netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
172.26.0.0        *                255.255.255.0   U        0  0        0 eth0
default           172.26.0.1       0.0.0.0         UG        0  0        0 eth0
```

El comando **ping** también nos podrá ser de utilidad en numerosos casos, tanto para poder ver cuellos de botella en los que los paquetes IP se ralentizan, como para registrar la ruta hasta un host destino, hasta un máximo de nueve pasos, mediante el parametro **-R** (-r en Windows). Una vez que la respuesta se produzca, se muestra el mapa completo.

Traceroute en Linux (en algunas distribuciones es necesario instalarlo aparte), y **tracert** en Windows, funciona de manera parecida a **ping -R**, pero sin el inconveniente de que si la respuesta no llega, la ruta completa no se muestra. Envía un paquete UDP al destino, utilizando un puerto de destino que se sabe que no esta en uso, pero configura un tiempo de duración (TTL) de uno. Cuando el paquete llega al primer router, este disminuye el TTL en uno, dejándolo en cero, y descartándolo por las características del protocolo IP. Al mismo tiempo, devuelve un mensaje de Tiempo Excedido de ICMP al origen de l paquete. Traceroute registra esto, y vuelve a enviar un paquete con TTL dos. Este paquete se desechara en el segundo router, devolviendo a su vez otro mensaje ICMP. Este proceso se realizara de manera sucesiva hasta llegar al host destino, que enviara un Puerto ICMP inalcanzable. En todo el proceso, el usuario va recibiendo información por pantalla, viendo routers y tiempos de respuesta.

El problema de direccionamiento se puede presentar como valor absoluto, es decir los paquetes IP no llegan a su destino, o como problema relativo, siendo determinados protocolos los que no localizan el host destino. En este caso la solución seria diferente, ya el problema estaría en los filtros establecidos en un router. Sería necesario inicialmente comprobar a que puerto va destinado ese protocolo (80 http, 22 ssh, etc...) y verificar si en los routers por los que pasa el paquete IP esta establecido un filtro que permita tener abierto ese puerto, y en caso de ser necesario, que indique la maquina correcta a la que puede llegar.

6.4 Problemas De DNS

Otro problema puede venir derivado de la incorrecta resolución de nombres a través de DNS.

En caso de que una maquina no responda mediante su nombre de host, es conveniente realizar algunos pasos, para poder llegar a una conclusion.

El primero de ellos es mirar en la configuración local de la maquina si los parámetros de DNS han sido modificados, o se encuentran correctamente introducidos. Es conveniente recordar que existen protocolos que pueden modificarlos de manera automatica sin conocimiento del usuario, tales como el DHCP o PPP.

En Linux y Unix existen, además herramientas adicionales para un mejor análisis del problema. Estas herramientas serian host, **nslookup** y **dig**.

Host realiza una simple conversion directa entre nombre-IP y viceversa. Es útil en caso de que los paquetes se pierdan al buscar el nombre de la maquina. Mediante *host*, es posible conocer la IP de dicha maquina y comprobar mediante un ping si esta caída, o simplemente es un problema de DNS.

Dig , sin embargo, tiene un funcionamiento mas completo, al poder seleccionar el servidor DNS en el que se realiza la búsqueda, y los resultados son mucho mas completos.

Nslookup realiza una función muy parecida a *dig*, teniendo también la posibilidad de indicar el servidor DNS, pero *nslookup* esta próximo a desaparecer, y es muy posible que vaya desapareciendo progresivamente de las distribuciones.

También se puede presentar el problema de que dos ordenadores de una LAN no se encuentren entre si, teniendo ambos conectividad. Mediante una comprobación de la mascara de red, podremos comprobar si pertenecen a la misma subred, o se encuentran separadas mediante la mascara de red. En caso de que este sea el problema, y necesitemos su comunicación, sera necesaria modificar o bien los datos de mascara de red de una de ellas, o bien recalcular la elaboración de las rubredes que hemos creado para adaptarlas mejor a las necesidades reales de nuestra LAN.



6.5 Caso De Ejemplo

Imaginemos un caso en el que tenemos dos redes conectadas por un router. En una de ellas (A) tenemos un servidor FTP con los ficheros que queremos descargar, y en la otra (B) esta la maquina cliente. Al intentar hacer la conexión al servidor FTP comprobamos que falla. Empezamos a hacer comprobaciones y pueden existir varias posibilidades.

- Puede fallar la conectividad general de la maquina, por lo que seria necesario comprobar los ficheros de configuración del dispositivo de red, así como IP, mascara de red, gateway, DNS, etc...
- Puede fallar la comunicación entre la red A y la B. Deberíamos comprobar la configuración de las tablas de rutas tanto en las máquinas de la red como en el router propiamente dicho.
- En caso de que utilicemos nombre de maquina para la conexión (ftp.mired), en lugar de IP directa(172.26.0.90), deberíamos comprobar que el fichero host correspondiente, o bien el DNS local, se encuentren correctamente configurados.
- Puede fallar la comunicación con la maquina servidor del FTP. Si el paso anterior se ha verificado, lo mas probable es que la comunicación con la maquina destino sea correcta, pero no con el daemon FTP que esta a la escucha. Si mediante ping ip_destino comprobamos q esta contesta, el fallo muy probablemente estará en que las peticiones del protocolo FTP no llegan al servidor. En este paso se deberían verificar dos puntos:
 - Que tanto el cliente como el servidor estén de acuerdo en los puertos por los que deben comunicarse.
 - Que el router que comunica ambas redes tenga los filtros activados o desactivados. En caso de que estén activados, tendremos q comprobar que se permita el paso por el puerto indicado para la comunicación FTP, y que este paso apunte a la maquina correcta, en este caso el servidor FTP.



6.6- Consideraciones Finales

Hemos abarcado de forma general los problemas mas habituales que se pueden encontrar en una red de tipo local, aunque los errores pueden ser de todo tipo, como fallos en la asignación de IP por parte del servidor DHCP, errores en la autenticación de servidores de dominio, etc..., pero por el carácter de este tipo de fallos y las multiples causas de dichos errores, sera necesario abordarlos de manera personalizada,aplicando soluciones diferentes en cada caso.

La planificación minuciosa de la topologia de la red a diseñar, una documentación amplia sobre el trabajo realizado, incluyendo un mapa de la red, indicando direcciones IP de routers, servidores de ficheros, DNS, y todos los elementos importantes de la red, así como el seguir la estandarización de implantación fisica de la red según la topologia elegida, sera el mejor aliado en la solución rapida y eficaz de cualquier problema presentado.

