2011-2012

UD2- Instalación y Administración de Servicios de Configuración Automática de Red.

José Jiménez Arias

IES Gregorio Prieto

2011-2012

ÍNDICE

1. Configuración automática de red (DHCP). Características.

Terminito DHCP:
Es un protocolo que permite a los clientes de una red, obtener sus parámetros de configuración de red automáticamente.

Para qué sirve:
El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero desde sus inicios se diseñó como un complemento del protocolo BOOTP (Protocolo Bootstrap), que se utiliza, por ejemplo, cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host.

Sus características quedan definidas por el estándar *RFC 2131*.

El DHCP es una alternativa a otros protocolos de gestión de direcciones IP de red, como el BOOTP (Bootstrap Protocol). DHCP es un protocolo más avanzado, pero ambos son los usados normalmente. Cuando el DHCP es incapaz de asignar una dirección IP, se utiliza un proceso llamado “Automatic Private Internet Protocol Addressing”.

APIPA Direccionamiento Privado Automático (Automatic Private IP Addressing) APIPA intenta encontrar una dirección libre en el rango 169.254.0.0-169.254.255.255 haciendo arping a direcciones aleatorias en ese rango para el interfaz. Si no se obtiene respuesta, se asigna esa dirección al interfaz. Esto es útil solamente en redes donde no hay servidor DHCP y no hay conexión directa al Internet y que todos los demás computadores también usen APIPA.

2. Componentes del servicio DHCP.

DHCP consta de dos componentes:

1. Un protocolo que entrega parámetros de configuración específicos de un host de un servidor DHCP al host.

2. Un mecanismo para reservar direcciones de red para los hosts.

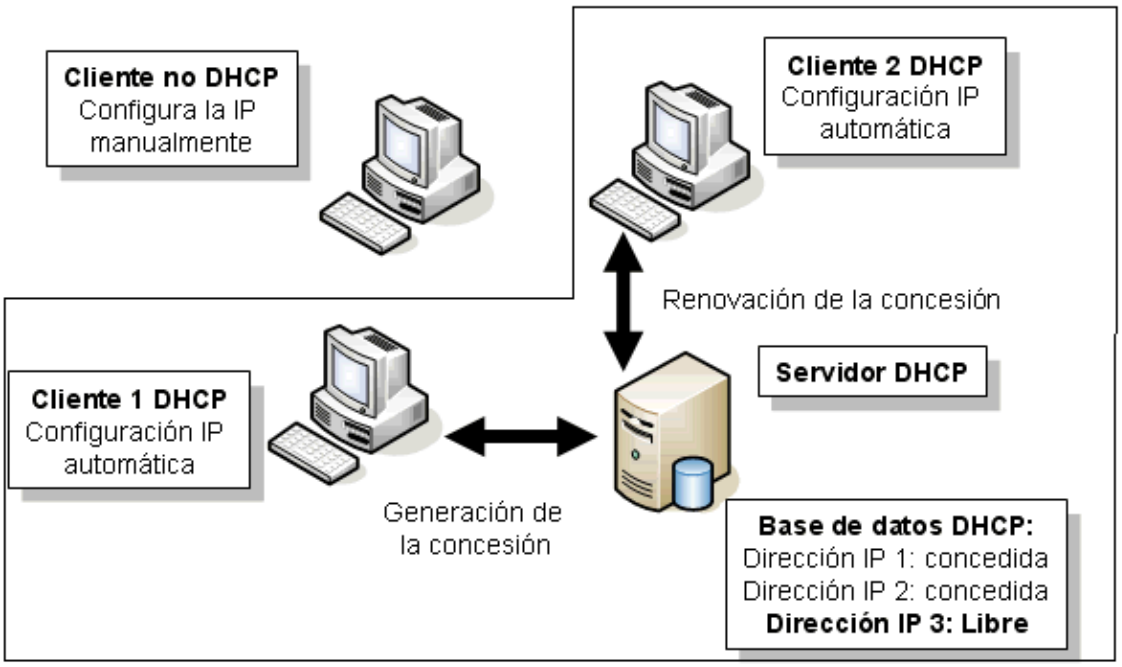
IP requiere la configuración de muchos parámetros dentro del software de implementación del protocolo. Debido a que IP utilizar en muchas clases distintas de hardware de red, no se puede suponer o adivinar que los valores de esos parámetros tienen valores correctos por defecto. El uso de un sistema de asignación de direcciones distribuidas basado en un mecanismo de consulta/defensa, para descubrir direcciones de red que ya están en uso, no garantiza direcciones de red unívocas porque puede que los host no sean siempre capaces de defender sus direcciones de red.

3. Asignaciones. Tipos.

El protocolo admite tres tipos de asignación de direcciones IP, que pueden combinarse entre sí:

- **Manual / Estática** - La asignación se realiza a partir de la lectura de una tabla de direcciones introducida manualmente por el administrador del servidor. Habitualmente, la máquina que recibe la asignación estática tiene igualmente configurada una dirección MAC que no debería repetirse en toda la red. De esta forma, dicha máquina recibe siempre la misma dirección IP, independientemente de dónde y cuándo se realice la conexión.
- **Automática e ilimitada** - Una vez que el administrador ha determinado un rango de direcciones disponibles, la asignación se realiza de forma permanente hacia el cliente que la solicita y hasta que éste la libera.
- **Dinámica y limitada** - Cada cliente obtiene su dirección al iniciar el interfaz de red. Mediante este método, las direcciones dentro del rango elegido por el administrador se reutilizan con cada máquina y durante un tiempo determinado. Con esta asignación se facilita enormemente la entrada de nuevas máquinas a la red de forma dinámica.

Sin DHCP, cada dirección IP debe configurarse manualmente en cada dispositivo y, si el dispositivo se mueve a otra subred, se debe configurar otra dirección IP diferente.



4. Protocolo DHCP.

DHCP (sigla en inglés de **D**ynamic **H**ost **C**onfiguration **P**rotocol) - **Protocolo de configuración dinámica de host**) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

5. Funcionamiento del servicio DHCP. Tipos de mensajes.

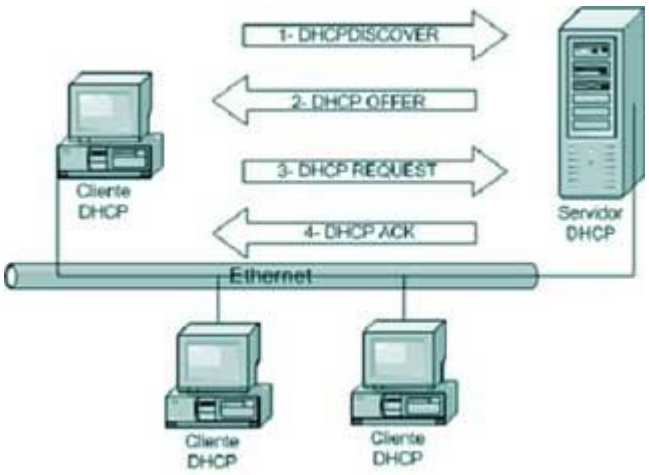
Primero, se necesita un servidor DHCP que distribuya las direcciones IP. Este equipo será la base para todas las solicitudes DHCP por lo cual debe tener una dirección IP fija. Por lo tanto, en una red puede tener sólo un equipo con una dirección IP fija: el servidor DHCP.

Cuando un equipo se inicia no tiene información sobre su configuración de red y no hay nada especial que el usuario deba hacer para obtener una dirección IP. Para esto, la técnica que se usa es la transmisión: para encontrar y comunicarse con un servidor DHCP, el equipo simplemente enviará un paquete especial de transmisión (transmisión en 255.255.255.255 con información adicional como el tipo de solicitud, los puertos de conexión, etc.) a través de la red local. Cuando el DHCP recibe el paquete de transmisión, contestará con otro paquete de transmisión (no olvide que el cliente no tiene una dirección IP y, por lo tanto, no es posible conectar directamente con él) que contiene toda la información solicitada por el cliente.

Se podría suponer que un único paquete es suficiente para que el protocolo funcione. En realidad, hay varios tipos de paquetes DHCP que pueden emitirse tanto desde el cliente hacia el servidor o servidores, como desde los servidores hacia un cliente:

- **DHCPDISCOVER** (para ubicar servidores DHCP disponibles)
- **DHCPOFFER** (respuesta del servidor a un paquete DHCPDISCOVER, que contiene los parámetros iniciales)
- **DHCPREQUEST** (solicitudes varias del cliente, por ejemplo, para extender su concesión)
- **DHCPACK** (respuesta del servidor que contiene los parámetros y la dirección IP del cliente)
- **DHCPNAK** (respuesta del servidor para indicarle al cliente que su concesión ha vencido o si el cliente anuncia una configuración de red errónea)
- **DHCPDECLINE** (el cliente le anuncia al servidor que la dirección ya está en uso)
- **DHCPRELEASE** (el cliente libera su dirección IP)
- **DHCPINFORM** (el cliente solicita parámetros locales, ya tiene su dirección IP)

El primer paquete emitido por el cliente es un paquete del tipo DHCPDISCOVER. El servidor responde con un paquete DHCPOFFER, fundamentalmente para enviarle una dirección IP al cliente. El cliente establece su configuración y luego realiza un DHCPREQUEST para validar su dirección IP (una solicitud de transmisión ya que DHCPOFFER no contiene la dirección IP) El servidor simplemente responde con un DHCPACK con la dirección IP para confirmar la asignación. Normalmente, esto es suficiente para que el cliente obtenga una configuración de red efectiva, pero puede tardar más o menos en función de que el cliente acepte o no la dirección IP...



6. Parámetros y declaraciones de configuración.

authoritative - La configuración correcta para la red es la definida en el servidor DHCP. Poner este parámetro al comienzo del archivo de configuración supone que el servidor DHCP reasignará direcciones a los clientes mal configurados por el motivo que sea, incluida una configuración nueva del servidor.

not authoritative - La función de este parámetro es justo la contraria del anterior. Es decir: la configuración del servidor de DHCP no es concluyente y los clientes mal configurados que sean detectados por el servidor, seguirán con su configuración intacta.

ignore*|*allow* client-updates** - Permite la actualización de las asignaciones (allow***) de un cliente a requerimiento de este, o bien las asignaciones se actualizan cuando el servidor así lo requiera (***ignore***).

ddns-hostname <*nombre*> - Por defecto, el servidor DHCP utiliza como nombre para la solicitud el nombre que el cliente tiene asignado a su máquina. Mediante este parámetro se asigna un nombre concreto a una máquina o a todas en general. Por ejemplo, para asignar un nombre a una dirección MAC concreta, utilizaremos el código siguiente:

```
host "nada" {
hardware ethernet 00:60:30:3f:2d:4a;
ddns-hostname "nombre_del_host";
}
```

Y para asignar, por ejemplo, la dirección MAC como parte del nombre del cliente, podemos usar lo siguiente:

```
ddns-hostname = binary-to-ascii (16,
8, "-", substring (hardware, 1, 6));
```

Que devolverá algo como 0-50-56-b-b-b.dhcp.nombre.com.

ddns-domainname <*nombre*> - Mediante el uso de este parámetro, se añadirá **<*nombre*>** al final del nombre de la máquina cliente, para formar un nombre de dominio totalmente cualificado (*FQDN*).

ddns-update-style <*tipo*> - Define el método de actualización automática de las DNS. Los valores pueden ser **ad-hoc**, **interim** y **none**.

ddns-updates <*on*|*off*> - Activa la actualización DNS mediante los valores asignados por DHCP.

default-lease-time <*duración*> - Especifica la cantidad de tiempo, en segundos, que será mantenida una asignación de direcciones, siempre y cuando el cliente no haya especificado algo concreto.

fixed-address <*direcciones*> - Esta opción aparece únicamente en una declaración de *host*. Define las direcciones estática a asignar a un *host* determinado.

group - Inicia la declaración de *Grupo*.

hardware <*tipo dirección*> - Especifica el *hardware* de un cliente BOOTP para que éste sea reconocido por el servidor de DHCP. ***tipo*** puede ser ethernet o token-ring y ***dirección*** será una serie de octetos hexadecimales inequívocos de la tarjeta (por ejemplo, hardware ethernet 00:50:b3:c5:60:23).

max-lease-time <*duración*> - Especifica la cantidad máxima de tiempo, en segundos, que será mantenida una asignación de direcciones. No está sujeta a esta especificación la asignación dinámica BOOTP.

min-lease-time <*duración*> - Especifica la cantidad mínima de tiempo, en segundos, que será mantenida una asignación de direcciones.

one-lease-per-client <*on|off*> - Cuando la opción se iguala a ***on*** y un cliente solicita una asignación de dirección (DHCPREQUEST), el servidor libera de forma automática cualquier otra asignación asociada a dicho cliente. Con esto se supone que si el cliente solicita una nueva asignación es porque ha olvidado que tuviera alguna, luego tiene un sólo interfaz de red. No dándose esta situación entre los clientes no es muy aconsejable el uso de esta opción.

range *ip-menor ip-mayor* - En una declaración de subred, este parámetro define el rango de direcciones que serán asignadas. Pueden darse dos instrucciones **range** seguidas del modo:

range 192.168.0.11 192.168.0.100;
range 192.168.0.125 192.168.0.210;

server-identifier <*IP*> - Identifica la máquina donde se aloja el servidor de DHCP. Su uso se aplica cuando la máquina en cuestión tiene varias direcciones asignadas en un mismo interfaz de red.

server-name <*nombre*> - Nombre del servidor que será suministrado al cliente que solicita la asignación.

shared-network - Declaración de *Subred compartida*.

subnet - Declaración de *Subred*.

option domain-name <*nombre*> - Nombre de dominio que usará el cliente en una resolución de nombres vía DNS. Normalmente, será el nombre de dominio que se añadirá al *host* que realiza la petición de asignación.

option domain-name-servers <*IP, [IP ...]*> - Define el nombre de los servidores DNS.

option finger-server - Define el nombre de los servidores *Finger* disponibles para el cliente.

option host-name <*nombre*> - Especifica el nombre del cliente. Puede ser un nombre cualificado o no, aunque se recomienda que el nombre del dominio se asigne mediante **option domain-name**. Sólo se asignará el nombre al cliente en el caso de no tener éste asignado ninguno.

option irc-server <*IP, [IP ...]*> - Define el nombre de los servidores de IRC disponibles para el cliente.

option lpr-servers <*IP, [IP ...]*> - Define una lista de servidores de impresión LPR conforme al estándar *RFC 1179*. Se listan por orden de preferencia.

option nds-servers <*IP, [IP ...]*> - Define una lista de servidores NDS disponibles para el cliente. Se usa en conjunción de **option nds-context <*nombre*>**, que establece el nombre de inicio de la red *Netware* y **option-nds-tree-name <*nombre*>**, que especifica el nombre del árbol a usar por el cliente solicitante.

option netbios-name-servers <*IP, [IP ...]*> - Especifica un listado con los servidores WINS disponibles para los clientes.

option nis-servers <*IP, [IP ...]*> - Define la lista de servidores NIS (*Sun Network Information Server*) disponibles. Los servidores se listan en orden de preferencia. Para establecer el nombre del dominio NIS, se usará **option nis-domain <*nombre*>**.

option ntp-server <*IP, [IP ...]*> - Define los servidores horarios de NTP disponibles. Se listan en oreden de preferenci**a.**

option pop-server <*IP, [IP ...]*> - Define los servidores de POP3 disponibles, listados en orden de preferencia.

option routers <*IP, [IP ...]*> - Se definen una serie de *routers* (en la práctica, *puertas de enlace*), listadas en orden de preferencia, disponibles para el acceso al exterior por parte del cliente.

option smtp-server <*IP, [IP ...]*> - Define la lista de servidores SMTP disponibles, listados en orden de preferencia.

option subnet-mask <*IP*> - Definición de la máscara de subred general.

7. Servicio DHCP a varias redes. Agente relay DHCP.

El Agente de transmisión DHCP (dhcrelay) le permite transmitir las peticiones DHCP y BOOTP desde una subred sin un servidor DHCP a uno o más servidores DHCP en otras subredes.

Cuando un cliente DHCP pide información, el agente de transmisión DHCP reenvía la petición a la lista de servidores DHCP especificada cuando se inicia el agente de transmisión DHCP.

Cuando un servidor DHCP devuelve una respuesta, la respuesta puede ser broadcast o unicast en la red que ha enviado la petición original.

El agente de transmisión escucha las peticiones DHCP en todas las interfaces a menos que las interfaces estén especificadas en /etc/sysconfig/dhcrelay con la directiva INTERFACES.

Para iniciar el agente de transmisión DHCP, use el comando service dhcrelay start.

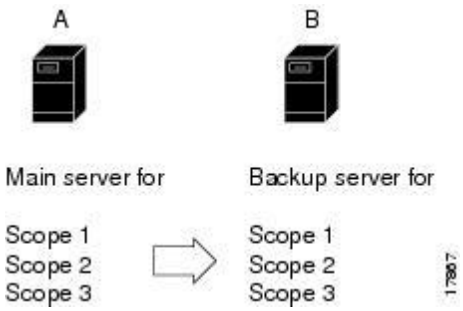
8. DHCP Failover Protocol.

Es un protocolo diseñado para permitir que una copia de seguridad del servidor DHCP pueda hacerse cargo del servidor principal, si el servidor principal está fuera de la red por cualquier razón. Puede utilizar la conmutación por error de DHCP para configurar dos servidores DHCP para funcionar como un par redundante.

Los escenarios de conmutación por error
Hay tres escenarios de conmutación por error de base:

1. Conmutación por error simple

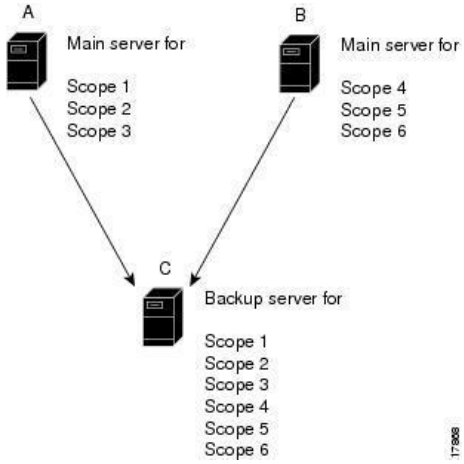
Conmutación por error simple consiste en un servidor principal y un par de copia de seguridad de servidor único. En el ejemplo, un servidor principal tiene tres ámbitos que se deben configurar de forma idéntica en copia de seguridad del servidor B.



Las ventajas de la conmutación por error simple en son:
• Es el más fácil de manejar como la red de los cambios-Es totalmente compatible con la interfaz de usuario Web para que los cambios en la configuración del servidor principal se propagan automáticamente al servidor de copia de seguridad.
• Proporciona los mayores beneficios de rendimiento.
• Sólo es necesario establecer las propiedades de conmutación por error a nivel de servidor y no preocuparse de los ámbitos.

2. Conmutación por error de Back Office

Volver conmutación por error de la oficina consiste en dos (o más) servidores principales que comparten el mismo servidor de respaldo. En el ejemplo, los servidores principales A y B tienen diferentes alcances, y C del servidor de copia de seguridad debe incluir todos estos ámbitos. Este escenario es apropiado para ámbitos en el mismo segmento de LAN, que requieren los mismos servidores principales y de reserva, pero con el conjunto de los ámbitos en los diferentes segmentos de la LAN.

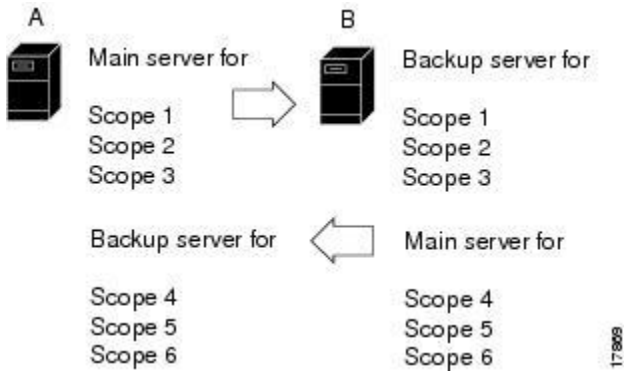


Ventaja de la conmutación por error de back office es:
-se reduce el número de servidores gestionados. Sin embargo, la conmutación por error simple sigue siendo recomendable, ya que en la conmutación por error de administración:

• El servidor de copia de seguridad debe ser de un tamaño para manejar la suma de las configuraciones.
• Cambios en cualquiera de los servidores principales se deben duplicar en el servidor de copia de seguridad.
• La mayor complejidad de la gestión de la configuración puede reducir sustancialmente la disponibilidad real de la configuración.

3. Conmutación por error simétrico

Conmutación por error simétrico consiste en servidores que actúan como copias de seguridad de unos a otros. Este escenario es muy complicado en el que no puede haber una variación en valores de atributos alcance entre los servidores, o la relación no funcionará correctamente.



La desventaja de conmutación por error simétrico en los otros escenarios es que, al tiempo que reduce el número de servidores, hay poco o ningún beneficio de rendimiento. Un servidor de copia de seguridad opera en un 40% del servidor principal para mantener su base de datos de arrendamiento sincronizados. Si los servidores de uno al otro, una parte de su capacidad de procesamiento va a esta tarea, con menos capacidad disponible para los clientes de servicio. Por otra parte, debido a que cada ámbito debe ser configurado individualmente, conmutación por error simétrico es más propensa a errores de configuración.
Debido a estas desventajas importantes, conmutación por error simple es el método recomendado.

9. Problemas asociados a DHCP. Seguridad.

- **DHCP es un protocolo no autenticado.**
  Cuando un usuario se conecta a una red no necesita proporcionar credenciales para obtener una concesión. Por tanto, es posible que un usuario no autenticado obtenga una concesión para cualquier cliente DHCP siempre que haya un servidor DHCP disponible para proporcionarla. Así, el usuario no autenticado podrá disponer de todos los valores de opción que el servidor DHCP proporcione con la concesión, como la dirección IP del servidor WINS o del servidor DNS. Si el cliente DHCP se identifica como miembro de una clase de usuario o de una clase de proveedor también dispondrá de las opciones asociadas a dicha clase.
  Esto permite que usuarios malintencionados que tengan acceso físico a una red habilitada para DHCP puedan realizar un ataque de denegación de servicio en los servidores DHCP si solicitan muchas concesiones al servidor, lo que reduciría el número de concesiones disponibles para otros clientes DHCP.

  Recomendaciones:

  - Asegúrese de que las personas no autorizadas no puedan obtener acceso físico o inalámbrico a la red.
  - Habilite el registro de auditoría en todos los servidores DHCP de la red. Compruebe periódicamente los archivos de registro de auditoría y supervíselos si el servidor DHCP recibe de los clientes un número de solicitudes de concesión inusualmente alto. En los archivos de registro de auditoría encontrará la información necesaria para localizar el origen de cualquier ataque realizado contra el servidor DHCP. La ubicación predeterminada de los registros de auditoría de es %windir%\System32\Dhcp. Para obtener más información, vea Para habilitar el registro del servidor DHCP, Registro de auditoría y Analizar archivos de registro de servidor. En el registro de sucesos del sistema también puede buscar información que explique el estado del servicio Servidor DHCP.
    Nota

    Si los clientes que ejecutan Microsoft® Windows® XP utilizan conmutadores de red de área local (LAN) habilitados para 802.1X o puntos de acceso inalámbrico la autenticación se produce antes de que el servidor DHCP asigne una concesión, por lo que aumenta la seguridad de DHCP.

- **El servidor DHCP permite realizar ataques por denegación de servicio contra el servidor DNS.**
  Cuando el servidor DHCP está configurado para actuar como servidor proxy DNS para los clientes DHCP y para realizar actualizaciones dinámicas de DNS existe la posibilidad de que un usuario malintencionado realice un ataque por denegación de servicio contra el servidor DHCP y el servidor DNS simultáneamente, inundando el servidor DHCP con solicitudes de concesiones.
  Recomendaciones:

- Asegúrese de que las personas no autorizadas no puedan obtener acceso físico o inalámbrico a la red.
- Utilice los registros de auditoría de DHCP, que se encuentran de manera predeterminada en %windir%\System32\Dhcp, para supervisar las actualizaciones dinámicas de DNS realizadas por el servidor DHCP. Para la actualización dinámica del DNS se utilizan los siguientes Id. de suceso:

Id. de suceso	*Suceso de DHCP*
30	*Solicitud de actualización dinámica del DNS realizada al servidor DNS*
31	*Error en la actualización dinámica de DNS*
32	*Actualización dinámica de DNS correcta*

La dirección IP del cliente DHCP se incluye en el registro de auditoría de DHCP, lo que permite descubrir el origen del ataque por denegación de servicio.

Servidores DHCP no autorizados que no sean de Microsoft pueden conceder direcciones IP a clientes DHCP.

Recomendaciones adicionales

Antes de instalar y configurar DHCP en una red, tenga en cuenta la posibilidad de:

- **Restringir los usuarios que pueden administrar el servicio DHCP.**
  Deberá ser miembro del grupo Administradores o del grupo Administradores DHCP para administrar servidores DHCP mediante la consola de DHCP o los Comandos Netsh para DHCP. Asimismo, solamente los miembros del grupo Administradores de dominio pueden autorizar o desautorizar un servidor DHCP en Active Directory. Debería restringir la pertenencia a estos grupos al número mínimo de usuarios necesarios para administrar el servidor.
  Si hay usuarios que necesitan acceso de sólo lectura a la consola de DHCP, agréguelos al grupo Usuarios DHCP en lugar de al grupo Administradores DHCP. Para obtener más información, vea Grupos DHCP.

10. BOOTP.

BOOTP son las siglas de **Boot**strap **P**rotocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo. Originalmente está definido en el RFC 951.

- Este protocolo permite a los ordenadores sin disco obtener una dirección IP antes de cargar un sistema operativo avanzado. Históricamente ha sido utilizado por las estaciones de trabajo sin disco basadas en UNIX (las cuales también obtenían la localización de su imagen de arranque mediante este protocolo) y también por empresas para introducir una instalación preconfigurada de Windows en PC recién comprados (típicamente en un entorno de red Windows NT).
- Originalmente requería el uso de un disquete de arranque para establecer las conexiones de red iniciales, pero el protocolo se integró en la BIOS de algunas tarjetas de red (como la 3c905c) y en muchas placas base modernas para permitir el arranque directo desde la red.
- DHCP es un protocolo basado en BOOTP, más avanzado, pero más difícil de implementar. Muchos servidores DHCP también ofrecen soporte BOOTP.

Pasos del Protocolo BOOTP

1. El cliente determina su propia dirección de hardware; esta dirección está normalmente en una ROM en el hardware.

2. Un cliente BOOTP envía su dirección hardware en un datagrama UDP al servidor. Si el cliente sabe su dirección IP y/o la dirección del servidor, debería usarlos, pero en general los clientes BOOTP no tienen datos de configuración IP del todo. Si el cliente no sabe su propia dirección IP, usa 0.0.0.0. Si el cliente no sabe la dirección IP del servidor, usa la dirección broadcast limitada (255.255.255.255). El número de puerto UDP es el 67.

3. El servidor recibe el datagrama y busca la dirección hardware del cliente en su fichero de configuración, que contiene la dirección IP del cliente. El servidor rellena los campos restantes en el datagrama UDP y lo devuelve al cliente usando el puerto UDP 68.

4. Cuando recibe la respuesta, el cliente BOOTP grabará su propia dirección IP (permitiendo que responda a las peticiones ARP) y comenzará el proceso de bootstrapping.

11. Comandos utilizados para el funcionamiento del servicio.

Configuración servidor GNU/LINUX:

Para comprobar que está activada la dirección para difusión utilizamos **route**

Si no es así escribimos como **root route add –host 255.255.255.255 /dev/eth0**

Archivos de registro del sistema **/var/log/syslog**

Configurar servidor en el fichero **dhcp.conf**

Sudo nano /etc/dhcp3/dhcpd.conf

Configurar interfaces DEBIAN: **sudo gedit /etc/network/interfaces**
Configurar interfaces FEDORA: **sudo gedit /etc/sysconfig/network-scripts/ifcfg-eth0**
Configurar interfaces OPENSUSE: **sudo kwrite /etc/sysconfig/network/ifcfg-eth0**

Para parar, iniciar, reiniciar o ver el estado
/etc/init.d/dhcp3-server stop
/etc/init.d/dhcp3-server start
/etc/init.d/dhcp3-server restart
/etc/init.d/dhcp3-server status

Configuración servidor WINDOWS:

Los comandos Netsh para DHCP constituyen una herramienta de línea de comandos que facilita la administración de servidores DHCP y que se puede utilizar como alternativa equivalente a la administración basada en consola. Puede resultar útil en las siguientes situaciones:

- Se pueden usar comandos en modo interactivo, en el símbolo del sistema de Netsh para mejorar la capacidad de administración de servidores DHCP en redes de área extensa (WAN) a través de vínculos de red de baja velocidad.
- Al administrar una gran cantidad de servidores DHCP, se pueden usar comandos en modo de proceso por lotes en el símbolo del sistema de Netsh para crear secuencias de comandos y automatizar tareas administrativas que deban realizarse en todos los servidores DHCP.

Dichos comandos se pueden ejecutar desde el símbolo del sistema de la familia Windows Server 2003 o desde el símbolo del sistema del contexto Netsh DHCP. Para que estos comandos funcionen en el símbolo del sistema de la familia Windows Server 2003, debe escribir **netsh dhcp** antes de escribir los comandos y parámetros que aparecen en la sintaxis siguiente. Puede haber diferencias funcionales entre los comandos del contexto Netsh de Windows 2000 y la familia Windows Server 2003.

Para obtener más información acerca de **netsh**, vea Información general acerca de Netsh y Entrar en un contexto de Netsh.

- Netsh DHCP
- Netsh DHCP server
- Netsh DHCP server scope
- Netsh DHCP server mscope

12. Instalador del servidor DHCP.

En entornos Linux

Accesorios, administración, conexiones de red, ipv4 (automatico dhcp).

En entornos Windows

Inicio, todos los programas, conexiones de red, propiedades, protocolos TCP/ipv4, opciones avanzadas y marcamos obtener una dirección IP automáticamente.

13. Configuración del cliente DHCP.

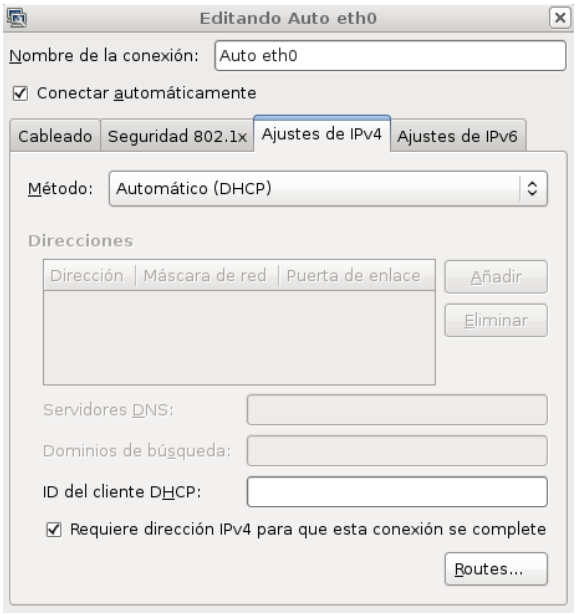
En entornos Linux

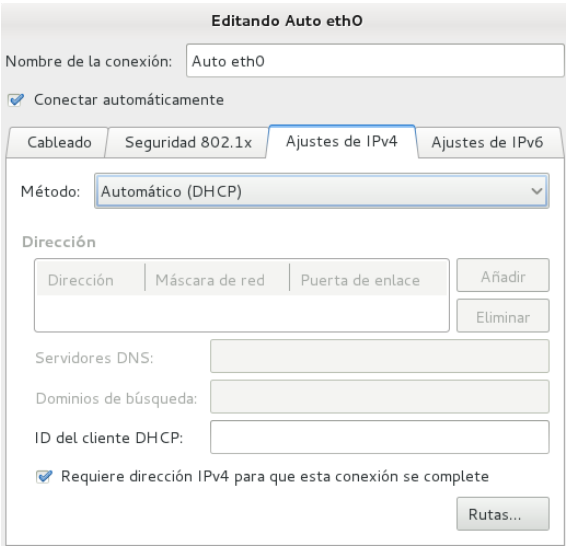
Open suse

Mediante la aplicación YaST2 entramos en ajustes de red configuración de la tarjeta de red.

Debían **FEDORA**

Mediante sistema, Administración, conexiones de red.





En entornos Windows

Utilizamos el asistente:

Herramientas administrativas, Administración del servidor, elegimos agregar funciones, DHCP