Sistemas y Aplicaciones Informáticas

Rendimiento y administración de sistemas en red. Protocolos.

1. Rendimiento de sistemas en red.

1.1. Rendimiento de redes Ethernet.

1.1.1. Factores que influyen en el rendimiento.

- El rendimiento de una red Ethernet depende fundamentalmente de tres factores:
  - *El tamaño de trama utilizado*. A mayor tamaño de trama mayor rendimiento, ya que con tramas de 64 bytes el riesgo de colisión es del 100% del tiempo de transmisión, mientras que con tramas de 1518 bytes el riesgo de colisión es sólo del 4%.
  - *El número de estaciones de la red*. A medida que este número aumenta, la probabilidad de que dos o más estaciones colisionen crece y el rendimiento disminuye.
  - *La distancia entre estaciones*. Cuanto más grande sea esta distancia, hay más riesgo de colisión entre las estaciones y por tanto el rendimiento decrece. Esto es debido a que a mayor distancia, el tiempo de transmisión de una trama que está expuesto a una colisión aumenta.
- Dada una misma topología de red, tamaño de trama, número de estaciones y nivel de ocupación relativa, la probabilidad de colisión crece a medida que se incrementa la velocidad de transmisión, puesto que el número de bytes emitidos en el mismo tiempo aumenta y por tanto la parte de la trama que está expuesta a una colisión es mayor.
- Además de los factores reseñados, existen otros problemas que afectan al rendimiento de las redes Ethernet:
  - *Excesivas colisiones*. Una tasa importante de colisiones puede ser normal en una red en determinadas circunstancias, pero cuando las estaciones sufren 16 colisiones consecutivas el rendimiento se degrada, puesto que la trama se descarta y es necesario retransmitirla. Normalmente la ocurrencia de 16 colisiones consecutivas se debe a una saturación extrema o a algún problema físico en el cableado o tarjeta de alguna estación, y debe considerarse síntoma de mal funcionamiento.
  - *Colisiones tardías*. Se producen por un mal diseño de la red o un mal funcionamiento del nivel físico, cuando no son respetados los tiempos de ida y vuelta máximos entre estaciones. La consecuencia de esto es que se producen colisiones pasados los primeros 512 bits de una trama a 10 y 100 Mbps (los primeros 4096 bits a 1000 Mbps). Esto puede dar lugar a colisiones no detectadas, lo cual implica la pérdida de tramas. Si los protocolos de nivel superior implementan un servicio fiable la pérdida será finalmente detectada y la trama retransmitida, a costa de una pérdida importante de rendimiento.
  - *Reparto no equilibrado de recursos*. Debido al método de resolución de las colisiones la red reparte de forma equitativa el número de tramas transmitidas por segundo, no el número de bits por segundo, por lo que el ancho de banda que obtiene una estación en una red saturada es proporcional al tamaño de las tramas que emite. Una estación que emita tramas grandes conseguirá más ancho de banda que una que envíe tramas pequeñas. Por tanto, en condiciones de saturación las estaciones que transmiten tramas grandes consiguen proporciones sustancialmente mayores de la capacidad disponible que las que transmiten tramas pequeñas.

- *Efecto captura*. Es consecuencia del funcionamiento del retardo exponencial binario y de la puesta a cero del contador de colisiones después de cada transmisión. Esto provoca que las estaciones más rápidas acaparen el canal durante más tiempo que las lentas, puesto que éstas últimas deberán aumentar cada vez más los intervalos de espera en cada intento de retransmisión en beneficio de las primeras. Esto provoca retardos muy grandes e impredecibles en la red, como consecuencia de las excesivas colisiones sufridas por las estaciones lentas.

- El correcto funcionamiento de CSMA/CD requiere que el tiempo de ida y vuelta entre dos estaciones cualesquiera no supere el tiempo de transmisión mínimo, es decir lo que tarda en emitirse la trama mínima permitida. El estándar IEEE 802.3 establece dos formas de verificar si una determinada topología Ethernet es válida:
  - La primera, denominada Modelo 1, realiza una serie de suposiciones simplificadoras para establecer un conjunto de reglas 'enlatadas' sobre el número máximo de repetidores que puede haber entre dos estaciones, y la distancia máxima entre ellos.
  - El denominado Modelo 2, que consiste en realizar cálculos detallados del retardo para cada componente y tramo de cable en cada trayecto. Una topología aceptable según el Modelo 2 es válida, aun cuando viole alguna de las reglas del Modelo 1.
- Para aumentar el rendimiento es recomendable lo siguiente:
  - No instalar ‘cables’ largos. Para cubrir un área extensa es preferible dividir el cable con puentes o routers, no con repetidores.
  - No poner demasiados ordenadores en un mismo cable. Es conveniente utilizar routers o puentes para dividir la red en comunidades de interés; de esta forma se aumenta el retardo del tráfico inter-comunidades a cambio de un mejor rendimiento y menor tiempo de respuesta en el tráfico intra-comunidades.
  - Implementar el protocolo correctamente. Una detección de colisiones y un retroceso exponencial binario apropiados en la interfaz y el software del host son esenciales para un buen rendimiento.
  - Utilizar el tamaño de trama máximo posible. Esto reduce la probabilidad de colisión y el costo de proceso en los hosts.
  - No mezclar aplicaciones de transferencia masiva de datos con aplicaciones de tiempo real. No es posible garantizar simultáneamente el mínimo retardo y el máximo rendimiento (aunque para requerimientos moderados ambos tipos de aplicaciones puedan coexistir).

1.1.2. Medición del rendimiento de una red.

- El rendimiento de la red es una medición de la rapidez y la confiabilidad de la red. Cada combinación del hardware, software y cableado de la red y de los computadores tiene un rendimiento de red distinto. Esto nos lleva a la conclusión de que, para saber si la red funciona de forma defectuosa, se debe contar con una medición con la que se pueda comparar el rendimiento. Esta medición se denomina nivel básico.
- El nivel básico se establece después de que se ha instalado y configurado la red de forma adecuada. Para ello, se puede utilizar una herramienta o un paquete de control de red, tal como el

Fluke LANMeter o el programa de control de red de Windows NT. Estas herramientas registran varios tipos de datos del rendimiento de la red, incluyendo el porcentaje de uso de la red, el número de colisiones, los errores de trama y el tráfico de broadcast. Al establecer una medición del nivel básico cuando el sistema de red se ubica en los niveles de rendimiento normal óptimos, el administrador de red cuenta con un valor de comparación que se puede utilizar para determinar la buena salud de la red.

- A medida que la red crece y cambia, la medición del nivel básico, al igual que cualquier otra documentación, se debe actualizar periódicamente. Cuando se actualiza un sistema, es importante recordar que, así como se actualiza el hardware, también se deben actualizar los controladores de software que controlan el hardware, ya que es posible que el controlador de software antiguo no pueda aprovechar las funciones del nuevo hardware o que no sea compatible en absoluto. Esto puede provocar un problema de rendimiento grave.
- Cuando se realizan cambios en la red, es importante verificar el funcionamiento correcto de dicha pieza del equipo en la nueva ubicación antes de actualizar la medición del nivel básico. Esto es particularmente importante al realizar cambios para reducir el tráfico de red en un segmento de red en particular. Aunque el dispositivo funcionara correctamente en el segmento antiguo, es posible que no funcione correctamente en el segmento nuevo, y esto afectará el rendimiento de la red.

1.2. Conmutación en redes Ethernet.

1.2.1. Transmisión Full-Duplex.

- A las redes locales basadas en conmutadores se las suele llamar redes locales conmutadas (switched LANs). En el caso de redes Ethernet el uso de conmutadores tiene un efecto adicional en la mejora del rendimiento. En redes CSMA/CD la eficiencia disminuye a medida que aumenta el número de ordenadores, por lo que si se divide una red en varias mediante un conmutador se consigue un mejor rendimiento en cada una de ellas al soportar un número más reducido de equipos.
- Al igual que los puentes, los conmutadores LAN han de mantener en memoria las tablas de direcciones MAC en cada una de sus puertas. Las especificaciones de un conmutador LAN indican normalmente el número máximo de direcciones que puede soportar. Si el número de equipos activos en la red es superior a este número máximo el rendimiento de la red se ve afectado ya que las entradas en la tabla de direcciones caducan con demasiada rapidez, provocando tráfico adicional en la red debido al mecanismo de inundación.
- Con sólo dos dispositivos de red (conmutador-host o conmutador-conmutador) y un canal de comunicación independiente para cada sentido el medio de transmisión no es compartido, por lo que no es necesario el protocolo MAC; se puede por tanto inhabilitar el CSMA/CD y manejar el medio físico como si se tratara de un enlace punto a punto full-duplex a la velocidad de la red en cada sentido de transmisión.
- Al no haber colisiones en full-duplex no rige la limitación de distancia impuesta por el tiempo máximo de ida y vuelta. La única restricción es la que viene impuesta por la atenuación de la

señal según el medio físico utilizado. En Gigabit Ethernet full-duplex se suprimen la extensión de portadora y las ráfagas de tramas, puesto que son innecesarias.

- El aumento en el rendimiento obtenido por la transmisión full-duplex normalmente sólo es significativo en conexiones conmutador-conmutador o conmutador-servidor. En un equipo monousuario el full-duplex supone una mejora marginal ya que las aplicaciones casi siempre están diseñadas para dialogar de forma half-duplex.
- Si la conexión entre los ordenadores de la red local se realiza mediante hubs, no hay más remedio que funcionar en half-duplex. En Ethernet y Fast Ethernet existe la posibilidad de funcionar en modo half-duplex o full-duplex, mientras que en Gigabit Ethernet y 10 Gigabit Ethernet todo es full-duplex (no hay hubs).
- La mezcla de equipos que funcionan en half-duplex y full-duplex produce unas grandes pérdidas de rendimiento. Si A transmite en half-duplex y B en full-duplex ocurre lo siguiente:
  * A empieza a enviar una trama, y al mismo tiempo B empieza a enviar otra.
  * A detecta una colisión, por lo que abandona la transmisión para reintentarlo más tarde.
  * A deja también de recibir la trama que le envía B, pues se supone que es errónea.
  * B no detecta la colisión puesto que está en modo full-duplex. Esa trama no es recibida por A pero B no puede detectarlo. Por otro lado B recibe de A una trama incompleta e incorrecta.

1.2.2. Agregación de enlaces.

- La agregación de enlaces, también llamada ‘trunking’ o multiplexado inverso, es un estándar (802.3ad) que utiliza varios enlaces Ethernet full-dúplex en la comunicación entre dos equipos, realizando reparto del tráfico entre ellos. Se suele usar entre conmutadores o en conexiones servidor-conmutador.
- La agregación de enlaces requiere deshabilitar el Spanning Tree entre los enlaces que se agregan, para así poder repartir el tráfico entre ellos. Los enlaces forman un grupo que se ve como un único enlace a efectos de Spanning Tree. Los enlaces pueden ser de 10, 100 ó 1000 Mb/s, pero han de ser todos de la misma velocidad.
- La agregación de enlaces permite un crecimiento gradual de la velocidad de transmisión sin necesidad de cambios en las interfaces de red o en la infraestructura. El número máximo de enlaces agregados no debería pasar de cuatro, ya que al aumentar el número de enlaces la eficiencia disminuye, y por otro lado el coste de las interfaces aconseja entonces pasar a la velocidad superior en vez de agregar enlaces.

2. Administración de sistemas en red.

2.1. Administración de servidores.

2.1.1. Redes de grupos de trabajo.

- Está diseñada para una cantidad pequeña de equipos. Cada ordenador se gestiona de manera individual y cada usuario es administrador de su equipo. Todos pueden ser servidor y estación de trabajo a la vez. Una red de grupo de trabajo es válida para un máximo de diez usuarios.
- Las ventajas de este tipo de redes son:
  * El costo inferior de creación y operación en comparación con las redes cliente-servidor.
  * Permite que los usuarios controlen sus propios recursos.

- No requiere un servidor dedicado.
- No se requiere ningún software adicional, aparte de un sistema operativo adecuado.

– Las desventajas son las siguientes:
  - No se suministra ningún punto central de administración y que cada usuario debe crear identificadores para cada usuario que comparte los recursos de la máquina.
  - Cada vez que un usuario cambia una contraseña, todas las contraseñas en los recursos compartidos se deben cambiar de forma individual.
  - Si una estación de trabajo compartida se desactiva o no está disponible, no se dispone de esos recursos.
  - Si hay más de diez usuarios o si la red crecerá a más de diez usuarios, la red de grupo de trabajo no resulta una buena elección.

2.1.2. Redes cliente-servidor.

– Los sistemas operativos de red son el núcleo de la red cliente-servidor. Estos sistemas controlan los recursos y la administración de la red de área local. Las ventajas de estas redes son:
  - Suministran un punto centralizado de administración de usuario, seguridad y recursos.
  - Se pueden utilizar servidores dedicados para suministrar recursos específicos a los clientes de forma más efectiva.
  - Suministran acceso a todos los recursos permitidos con un ID de red y una contraseña.

– La desventaja es que ahora hay un solo punto de falla en la red. Si el servidor entra en colapso, todos los recursos del servidor son inaccesibles para los clientes. La red cliente-servidor en realidad es la única opción para las organizaciones con más de diez usuarios. Ejemplos de sistemas operativos cliente-servidor son Unix, NetWare de Novell y Windows NT.

– Cuando se comparte una carpeta, ésta es accesible a través de la exploración de la red. Pero si el protocolo NetBIOS no es soportado por los equipos que comparten sus recursos, el único medio de acceso es introducir la ruta *UNC (Universal Name Convention)*, que es el nombre completo de un recurso en una red. Cumple con la sintaxis \\nombre_de_servidor\nombre_compartido, donde nombre_de_servidor es el nombre del servidor y nombre_compartido es el nombre del recurso compartido. Los nombres UNC de directorios o archivos también pueden incluir la ruta de acceso del directorio bajo el nombre de recurso compartido, con la siguiente sintaxis: \\nombre_de_servidor\nombre_compartido\directorio\nombre_de_archivo.

2.1.3. Control de usuarios y recursos. Perfiles y directivas.

– No importa cuál sea el sistema operativo de red que se utilice, la función principal del sistema operativo de red es controlar la red. Esto se logra al establecer usuarios de red; derechos, cuentas de usuario, contraseñas y grupos, así como también Perfiles y políticas de sistema.

– Una cuenta de usuario identifica al usuario de red en el sistema de red. Esta cuenta, junto con la contraseña del usuario, identifican y suministran acceso a los recursos del sistema de red. Este ID de cuenta también hace que el usuario sea responsable por sus acciones en la red.

– Los derechos de usuario determinan la disponibilidad de recursos del usuario. Son establecidos por un administrador para permitir o denegar el acceso a un recurso de la red en particular. Esto se aplica a impresoras, archivos de datos y programas y cualquier otro "recurso" en la red.

- Hay un problema administrativo que se produce al asignar derechos a los usuarios. El problema es que, si hay muchos usuarios en un sistema de red, la asignación y la modificación de derechos para cada usuario individual puede insumir la mayor parte del tiempo del administrador. Este problema se soluciona con el uso de Grupos.
- Los grupos son agrupaciones lógicas de usuarios en la red. La forma en que funcionan los grupos es que los derechos y permisos se otorgan al grupo y no a un usuario individual. Entonces, si un usuario necesita estos derechos, se asigna a un grupo y mediante este acto se le suministran los derechos asignados al grupo. Esto también se aplica si se deben cambiar los derechos para un recurso, un cambio en el grupo también se refleja como un cambio para todos los miembros del grupo. Esto no significa que no se puedan asignar derechos a usuarios individuales. Pero el método más eficiente en redes grandes es trabajar con grupos.
- Los perfiles permiten que un usuario personalice la interfaz de usuario en un computador y luego pueda usar ese perfil en cualquier computador con el que se conecte a la red. Esto se denomina perfil móvil. Otro tipo de perfil hace que aparezca la misma interfaz de usuario para todas las personas y no permite que se realicen cambios. Este se denomina perfil obligatorio, y se utiliza en situaciones en las que muchas personas deben usar el mismo computador físico. Si el usuario permanece todo el tiempo en el mismo computador y no necesita utilizar otros computadores, puede tener un perfil local. El perfil local no se guarda en la red, como en el caso de los dos primeros perfiles, sino en el computador local.
- Las directivas se refieren al control de los recursos en el computador local. Éstas pueden mejorar la seguridad e impedir que los usuarios realicen cambios de forma accidental en la información de configuración del sistema.
- En resumen, los derechos de red, las cuentas de usuario, las contraseñas y los grupos, así como también los perfiles y las directivas suministran una forma para que el administrador del sistema pueda controlar el acceso y las restricciones a los servicios de red y pueda controlar la estación de trabajo de usuario local. Ser un administrador de red también implica un conjunto de derechos y privilegios otorgados en la red. No todos los usuarios tienen el derecho de cambiar los derechos y privilegios de otros usuarios; estos derechos están reservados para determinados grupos a los que se les han otorgado derechos de administrador.

2.2. Monitorización de la red. Protocolo SNMP.

- Los dos motivos principales para monitorizar una red son la predicción de los cambios para el crecimiento futuro y la detección de cambios inesperados en el estado de la red. Si no tiene la capacidad para monitorizar la red, un administrador sólo puede reaccionar a los problemas a medida que ocurren, en lugar de prevenir estos problemas antes de que se produzcan.
- La monitorización del tráfico de red analiza el tráfico real de paquetes en la red y genera informes basados en el tráfico de la red. Los programas como el Monitor de red de Microsoft Windows NT y el Network Analyzer de Fluke son ejemplos de este tipo de software. Estos programas no sólo detectan el equipo defectuoso sino que también determinan si un componente se encuentra sobrecargado o mal configurado. La desventaja de este tipo de programa es que

normalmente funciona en un solo segmento por vez. Si es necesario reunir datos de otros segmentos, el software de monitoreo se debe trasladar a ese segmento.

- SNMP es un protocolo que permite que la administración transmita datos estadísticos a través de la red a una consola de administración central. SNMP es un componente de la Arquitectura de administración de red, que está formada por cuatro componentes principales:
  - *Estación de administración*. Es la interfaz del administrador de red al sistema de red. Posee los programas para manipular los datos y controlar la red. La estación de administración también mantiene una base de datos de información de administración (MIB) extraída de los dispositivos bajo su administración.
  - *Agente de administración*. Es el componente incluido en los dispositivos que se deben administrar. Puentes, routers, hubs y switches pueden contener agentes SNMP que les permitan ser controlados por la estación de administración. El agente de administración responde a la estación de administración de dos maneras:
    - **Mediante sondeo**. La estación de administración requiere datos desde el agente y el agente responde con los datos solicitados.
    - **Trapping**. Es un método de recopilación de datos diseñado para reducir el tráfico en la red y el procesamiento en los dispositivos que se controlan. En lugar de que la estación de administración haga un sondeo a los agentes a intervalos específicos, se establecen umbrales (límites superiores o inferiores) en el dispositivo administrado. Si se supera este umbral en el dispositivo, el dispositivo administrado envía un mensaje de alerta a la estación de administración. Esto elimina la necesidad de realizar sondeos continuos de todos los dispositivos administrados en la red. El trapping es muy ventajoso en las redes que incluyen una gran cantidad de dispositivos que necesitan administrarse. Reduce la cantidad de tráfico SNMP en la red para proporcionar mayor ancho de banda para la transferencia de datos.
  - *Base de información de administración*. Tiene una estructura de árbol de datos y reside en cada dispositivo administrado. La base de datos contiene una serie de objetos, que son datos sobre recursos clasificados en ocho categorías (sistema, interfaces, traducción direcciones, IP, ICMP, TCP, UDP, EGP). Existen varios tipos, ya que cada fabricante las adapta a su sistema, pero están normalizados por el IETF. Cada elemento en el árbol está identificado con un número y el conjunto está separado por puntos, también existen nombres normalizados que aunque se parecen no tienen nada que ver con DNS.
  - *Protocolo de administración de red*. El protocolo de administración de red utilizado es SNMP. Se trata de un protocolo de capa de aplicación diseñado para comunicar datos entre la consola de administración y el agente de administración. Tiene tres capacidades clave:
    - OBTENER, que implica que la consola de administración recupera datos del agente.
    - COLOCAR, que implica que la consola de administración establece los valores de los objetos en el agente.
    - TRAP, que implica que el agente notifica a la consola de administración acerca de los sucesos de importancia.

- Principio de comunidades SNMP. Las maquinas que ejecutan un agente SNMP y las herramientas de supervisión están agrupadas en comunidades. Un agente sólo puede recibir órdenes de un supervisor de su propia comunidad, aunque se puede ser miembro de varias comunidades. Es conveniente utilizar IPSec para asegurar la confidencialidad y la autenticación entre agentes y supervisores.
- En los últimos años, se han agregado mejoras a SNMP, a fin de expandir sus capacidades de monitorización y administración. Una de las mejoras principales de SNMP se denomina Monitorización remota (RMON). Las extensiones de RMON a SNMP brindan la capacidad para observar la red como un todo, en contraste con el análisis de dispositivos individuales.
- Las sondas reúnen datos remotos en RMON. Una sonda tiene la misma función que un agente SNMP. Una sonda tiene capacidades de RMON; un agente no las tiene. Al trabajar con RMON, tal como ocurre con SNMP, una consola de administración central es el punto de reunión de datos. Una sonda RMON se ubica en cada segmento monitorizado de la red. Estas sondas pueden ser hosts dedicados, residentes en un servidor, o se pueden incluir en un dispositivo de networking estándar, como un router o switch. Estas sondas reúnen los datos especificados de cada segmento y los derivan a la consola de administración.
- Las consolas de administración redundantes proporcionan una función valiosa para la red, y ofrecen dos ventajas importantes para los procesos de administración de la red:
  - La capacidad para que varios administradores de red, en diferentes ubicaciones físicas, puedan monitorizar y administrar la misma red.
  - La existencia de dos o más consolas de administración significa que, si una de las consolas falla, la otra todavía puede usarse para monitorizar y controlar la red hasta que se pueda reparar la primera consola.
- La extensión RMON del protocolo SNMP crea nuevas categorías de datos que agregan más ramas a la base de datos MIB. Es importante tener en cuenta que RMON es una extensión del protocolo SNMP. Específicamente, esto significa que, mientras que RMON aumenta las capacidades de operación y monitoreo de SNMP, SNMP sigue siendo necesario para que RMON opere en una red. Como última observación, es importante mencionar que hay revisiones más recientes de SNMP y RMON, denominadas SNMPv2 y RMON2.

2.3. Herramientas software.

- Hay herramientas software disponibles para que el administrador de red pueda resolver los problemas de conectividad de la red. Estas herramientas pueden ayudar en el diagnóstico de fallas de las redes de área local, pero son especialmente útiles para resolver los problemas de las redes de área amplia.
- Entre estos comandos se incluyen:
  - *Ping*. Envía paquetes de eco ICMP para verificar las conexiones a un host remoto. El resultado muestra si el ping fue exitoso. El resultado muestra la cantidad de paquetes a los que se respondió y el tiempo de retorno del eco. Un Ping a 127.0.0.1 (dirección de loop de prueba del computador) con éxito elimina la probabilidad de que exista un problema entre el computador, la configuración del controlador y la tarjeta NIC.

- *Tracert (Traceroute)*. Muestra la ruta que siguió un paquete para alcanzar su destino.
- *Telnet*. Este es un programa de emulación de terminal que le permitirá ejecutar comandos interactivos en el servidor telnet. Hasta que se establece una conexión, no pasa ningún dato, y si la conexión se interrumpe, telnet lo informa. Es bueno para probar los parámetros de configuración de conexión a un host remoto.
- *Netstat*. Muestra estadísticas de protocolo y conexiones de red TCP/IP actuales.
- *Arp*. Se usa para reunir direcciones de hardware para los hosts locales y el gateway por defecto, se puede ver el caché ARP y verificar la existencia de entradas no válidas o duplicadas.
- *Ipconfig*. Estas utilidades Windows muestran información de direccionamiento IP para el adaptador(es) de red local o una NIC especificada.
- *Nslookup*. Prueba el funcionamiento de los servidores DNS.

3. Protocolos de red.

3.1. Protocolo ARP (Address Resolution Protocol).

- El protocolo ARP determina la dirección MAC de destino a partir de la dirección IP. A nivel de enlace ARP es un protocolo diferente de IP, con un Ethertype específico. Esto permite que los routers no confundan los paquetes ARP con los paquetes IP y no los propaguen, evitando así que el tráfico broadcast que generan se propague a otras redes.
- Cada ordenador de la red local mantiene en memoria una tabla denominada ARP caché con las parejas de direcciones MAC-IP utilizadas recientemente, que puede consultarse con el comando **arp –a** disponible en UNIX y en Windows.
- El protocolo ARP funciona de la siguiente manera:
  - Cuando la dirección IP de destino se encuentra en la misma red local, el ordenador origen genera entonces un mensaje ARP con dicha dirección y lo envía en una trama Ethernet que tiene como dirección MAC de destino la dirección broadcast MAC (FF-FF-FF-FF-FF-FF).
  - La trama es recibida y procesada por todas las máquinas de la red que en ese momento estén activas, siendo retransmitida a través de los conmutadores y puentes. Todos los ordenadores de la red capturan y opcionalmente incluyen al host emisor en su ARP caché.
  - Eventualmente sólo un ordenador se reconoce propietaria de la dirección IP solicitada y responde al mensaje. La respuesta incluye la dirección MAC solicitada, y será una trama unicast puesto que el ordenador de destino ya conoce la dirección MAC del origen.
- Por tanto, el envío de un datagrama IP en una red local se realiza de la siguiente manera:
  - El ordenador de origen coloca el datagrama en una trama y comprueba si la dirección IP de destino del datagrama se encuentra en su tabla ARP caché. En caso afirmativo coloca la dirección MAC correspondiente de la ARP caché como dirección de destino de la trama.
  - En caso negativo, el host compara la parte red de dicha dirección de destino con la suya propia para saber si se encuentra o no en su propia red. Si la IP de destino se encuentra en la misma red, lanza un mensaje ARP y espera un tiempo. Si pasado ese tiempo no aparece la dirección en la ARP cache, el host envía un mensaje ICMP Destination Unreachable.

- Si la dirección de destino pertenece a otra red el host consultará su tabla de rutas para averiguar la dirección IP del router más adecuado de la misma red para llegar a ese destino, y se busca la dirección MAC del router siguiendo el mismo proceso anterior.

3.2. Protocolo DHCP (Dynamic Host Configuration Protocol).

- El protocolo DHCP funciona de la siguiente manera:
  - El ordenador cliente emite un broadcast DHCP DISCOVER en paquetes UDP (MAC FF:FF:FF:FF:FF:FF, IP 255.255.255.255) a todos los servidores DHCP de la red local.
  - Todos los servidores existentes recibirán la petición y enviarán una proposición DCHP OFFER al ordenador cliente, si disponen de rangos adecuados de direcciones IP para él.
  - El cliente selecciona la primera oferta recibida y después emite un broadcast DHCP REQUEST de selección de dicha oferta. Aquellos servidores cuya oferta no ha sido seleccionada, la retiran para reservar estos parámetros para otro equipo que los solicite.
  - El servidor elegido envía un broadcast DHCP ACK confirmando la concesión, que puede ser por un período de tiempo limitado o ilimitado. Si es limitado, el cliente puede renovar su concesión a 1/2 (por unicast) y a 7/8 (por broadcast) de la duración del período de concesión, realizando una nueva petición DHCP REQUEST al servidor, que puede ser aceptada (DHCP ACK) o rechazada (DHCP NACK). Si se solicita la renovación y el servidor no puede renovársela, se le reasignará otra dirección IP.
- Es posible la creación de una multirred (hosts que están en un mismo segmento físico de red con direcciones IP distintas) a través de un un servidor DHCP asigne direcciones IP de rangos diferentes. Para que haya comunicación entre estos hosts debe haber conectado al segmento un router cuyo adaptador de red tenga tantas direcciones IP como subredes existan en el segmento.
- Puesto que DHCP funciona con mensajes broadcast, si hay varios segmentos de red separados por routers hay que tener un servidor DCHP por segmento. Esta restricción puede saltarse haciendo que un servidor o un router compatible con el RFC 1512 haga la función de proxy DHCP. Éste se configura con dirección IP estática y conoce la dirección IP del servidor DHCP. Por su parte el servidor DHCP sabe qué rango de direcciones elegir, ya que conoce la dirección IP del proxy que le envía la petición. Funciona de la siguiente manera:
  - El cliente envía por broadcast una petición DHCP DISCOVER. El proxy, que está en el mismo segmento, captura la petición y la envía de manera unicast hacia el servidor DHCP para que atraviese el router. La dirección IP de origen de la petición es la del proxy.
  - El servidor DHCP envía un mensaje unicast DHCP OFFER al proxy con la dirección IP y el resto de datos ofertados. El proxy envía por broadcast a su subred el DHCP OFFER, que es capturado por el cliente DHCP, que a su vez envía una petición DCHP REQUEST.
  - El proxy captura la petición y la envía de manera unicast al servidor DHCP, que por su parte devuelve un DHCP ACK unicast al proxy. Éste por último envía por broadcast el DCHP ACK recibido en su segmento.

3.3. Domain Name System (DNS).

3.3.1. Descripción. Nombres de dominio.

- El sistema de nombres de dominio es un esquema jerárquico que permite asignar nombres significativos de alto nivel a grandes conjuntos de máquinas y direcciones IP. Para ello se utiliza una base de datos distribuida y una arquitectura cliente/servidor, donde los servidores de nombres contienen información acerca de un segmento de la base de datos y la ponen a disposición de los clientes, a traves de rutinas de biblioteca denominadas resolvers.
- Un nombre de dominio consiste en una secuencia de etiquetas separadas por un punto y cada etiqueta indica un dominio. El nombre de dominio indica la relación jerárquica entre cada dominio que forma parte del nombre, siendo el dominio de nivel inferior el que corresponde con la primera etiqueta, y el de nivel superior el que corresponde con la última etiqueta.
- El nivel superior de dominios está dividido en dos tipos, geográficos (.es) y genéricos (.com). Todos los dominios en Internet pueden representarse mediante un árbol. Las hojas del árbol serían los dominios que ya no contienen más dominios (subdominios). Por tanto, cada dominio en Internet está definido por la trayectoria hacia arriba desde él a la raíz, que está vacía. No hay conflicto cuando dos nombres son iguales, mientras pertenezcan a dominios distintos.

3.3.2. Servidores DNS. Zonas de autoridad.

- La organización que posee un nombre de dominio es responsable del funcionamiento y mantenimiento de los servidores de nombres que traducen sus nombres de dominio a direcciones IP. Puede delegar parte de los dominios que caen bajo su responsabilidad en otro administrador.
- Un servidor DNS es un ordenador que guarda toda la información acerca de una parte contigua del árbol de nombres de una organización que se administra como una unidad, denominado zona de autoridad, y que abarca al menos un dominio y también pueden incluir subdominios, aunque a veces los servidores de un dominio pueden delegar sus dominios en otros servidores.
- Los servidores DNS tienen autoridad en una zona cuando disponen de un fichero de zona para el nombre de dominio solicitado. Los servidores raíz tienen autoridad sobre la zona ".". Los servidores del mismo nivel que gestionan la misma zona están sincronizados, cada servidor tiene conocimiento de todos los servidores con autoridad en la zona del nivel inmediatamente inferior.
- Un servidor DNS gestiona un fichero de zona en el que hay referencias dirección IP/nombre de host, o también nombre de host/dirección IP. En UNIX se utiliza el fichero /etc/***hosts*** con la relación de todos los nombres y sus correspondientes direcciones IP de manera exhaustiva. En Windows XP, se encuentra en c:/windows/system32/drivers/etc/***hosts***. El fichero “hosts” puede servir para una solución simple en una red local donde no esté configurado un servidor DNS.
- Cada zona tendrá asignada un servidor de nombres primario que obtiene su información de su base de datos local y uno o más servidores secundarios que obtienen su información del servidor de nombres primario. Por delegación de autoridad, el lugar donde se colocan los límites de una zona es responsabilidad del administrador de esa zona.
- Según la configuración del servidor podemos encontrarnos con cuatro tipos de servidores:
  - *Primarios (Primary Name Servers).* Almacenan la información de su zona en una base de datos local. Son responsables de mantener la información de la zona actualizada.

- *Secundarios (Secundary Name Servers)*. Obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona mediante un prceso denominado transferencia de zona.
- *Maestros (Master Name Servers)*. Los servidores maestros son los que transfieren las zonas a los servidores secundarios, extrayendo la información desde el servidor primario. Un servidor maestro para una zona puede ser un servidor primario o secundario de esa zona.
- *Locales (Caching-only servers)*. Mantienen una memoria caché con las últimas direcciones resueltas y contactan con otros servidores para resolver las peticiones que no estén en caché.

3.3.3. Resolución de nombres de dominio.

3.3.3.1. Resolución directa.

- La resolución directa de un nombre de dominio es la traducción del nombre a su correspondiente dirección IP. En este proceso hay dos partes el cliente (*resolver*) y el servidor DNS. El resolver debe interrogar al servidor de nombres DNS, interpretar las respuestas y devolver información al programa que ha solicitado la resolución.
- Para este proceso de traducción los r*esolvers* pueden formular dos tipos de preguntas:
  - *Recursivas*. El servidor DNS debe intentar por todos los medios resolverla aunque para ello tenga que preguntar a otros servidores. Esta es el tipo de interrogación más frecuente.
  - *Iterativas*. El servidor DNS devolverá la dirección IP si la conoce. En caso contrario, devolverá la dirección de otro servidor que sea capaz de resolver el nombre. Es poco utilizada y requiere que el cliente realice la consulta a otros DNS directamente.
- Los pasos que se dan en el proceso de resolución de nombres de dominio son los siguientes:
  - El explorador Web invoca al resolver y éste intenta resolver la consulta localmente utilizando información almacenada en caché de una consulta anterior. Para poder mantener información actualizada en la caché de DNS, los registros en caché tienen asociados valores de "tiempo de vida". Cuando caducan hay que consultarlos de nuevo.
  - Si la consulta no se puede resolver localmente, el cliente pide una respuesta a un servidor DNS local. Cuando un cliente DNS formula una *pregunta recursiva* a un servidor DNS local, éste debe resolverla aunque para ello tenga que reenviarla a otros servidores.
  - Si el usuario ha solicitado información local, el servidor extrae la respuesta de su propia base de datos. Si es sobre un ordenador externo (por ejemplo *www.google.es*), el servidor comprueba primero su caché de consultas. Si la respuesta está aquí entonces la devuelve.
  - En caso contrario, formulará una *pregunta iterativa* al **servidor de dominio raíz**. Si éste no conoce la dirección IP solicitada, devuelve la dirección del servidor del dominio de primer nivel *es*. El servidor local reenvía la pregunta iterativa al servidor del dominio *es*.
  - El servidor del dominio *es* tampoco conoce la dirección IP solicitada, aunque sí devuelve la dirección del servidor del dominio de segundo nivel *google.es*. El servidor local vuelve a reenvíar la pregunta iterativa al servidor del dominio *google.es*.
  - El servidor del dominio *google.es* conoce la dirección IP de *www.google.es* y devuelve esta dirección al servidor local. El servidor local reenvía la respuesta al cliente DNS. Al mismo tiempo la respuesta es almacenada en la caché para futuras referencias. El tiempo máximo que permanece la información almacenada en la caché se configura en los servidores DNS.

3.3.3.2. Resolución inversa.

- Los clientes DNS también pueden formular *preguntas inversas*, es decir, conocer el nombre de dominio dada una dirección IP. Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial llamado *in-addr.arpa*.
- Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP *w.x.y.z* debe formular una pregunta a *z.y.x.w.in-addr.arpa*. La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que las direcciones.
- La organización que posee una dirección de red es responsable de registrar todas sus traducciones de dirección a nombre en la base de datos del DNS. Esto se hace en una tabla que es independiente de las correspondencias entre nombre y direcciones. El subárbol especial de dominio *in-addr.arpa* se creó para apuntar hacia todas esas tablas de red.

3.4. Traducción de direcciones (NAT).

3.4.1. Características.

- Consiste en traducir una dirección IP en otra de acuerdo con cierta tabla de equivalencias. Se utiliza como mecanismo para extender el rango de direcciones de una red, por ejemplo para usar una sola IP pública para dar acceso a cientos de ordenadores.
- La seguridad y la dificultad para conseguir direcciones públicas fuerzan a las organizaciones a hacer un mayor uso de las redes privadas según los rangos especificados en el RFC 1918 (10.0.0.0, 172.16.0.0 a 172.31.0.0, y 192.168.0.0 a 192.168.255.0). Estas redes privadas no pueden intercambiar datagramas directamente con el exterior, por lo que han de utilizar un equipo intermedio que realice la traducción de direcciones (NAT, Network Address Translation).
- Generalmente la función de NAT se realiza en la frontera entre una red local y el exterior, y la suele realizar un router. Normalmente NAT solo traduce paquetes IP correspondientes a ICMP o a los protocolos de transporte TCP y UDP. Otra restricción es que solo puede haber un solo punto de comunicación entre la red privada y la red pública, por tanto la conexión al exterior sólo puede hacerse en un router, el cual puede tener conexiones a varios ISPs.
- Un NAT puede configurarse como:
  - *NAT unidireccional*. Sólo permite conexiones salientes iniciadas desde la red privada.
  - *NAT bidireccional*. Permite que las conexiones se inicien desde la red privada o desde el exterior (red pública).

3.4.2. Tipos de NAT. Limitaciones.

- Según los campos que se modifican el NAT (Network Address Translation) puede ser:
  - *NAT básico*. Sólo se modifica la dirección IP.
  - *NAPT (Network Address Port Translation)*. Se modifica la dirección IP y el número de puerto TCP o UDP.
- Según el tiempo de correspondencia entre las direcciones privada y pública el NAT puede ser:
  - *Estático*. Se realiza de acuerdo con una tabla de equivalencia que se carga en la configuración del dispositivo NAT y dicha tabla no se modifica.
  - *Dinámico*. La tabla de equivalencia es gestionada dinámicamente por el dispositivo NAT de manera que las direcciones y/o números de puerto se puedan reutilizar.

- Combinando el NAT Básico o el NAPT con las modalidades estática y dinámica se obtienen:
  - *NAT básico estático*. La correspondencia entre IP privada – IP pública es biunívoca y está incluida en la configuración del dispositivo NAT. Los números de puerto no se modifican. Es preciso disponer de un número de direcciones públicas igual al de direcciones privadas.
  - *NAT básico dinámico*. Las entradas de la tabla de equivalencias IP privada – IP pública se construyen dinámicamente, y caducan al terminar la conexión (TCP) o pasado un tiempo de inactividad (UDP), lo cual permite la reutilización de las direcciones. Los números de puerto no se modifican. El número de direcciones públicas puede ser inferior al de direcciones privadas, pero ha de ser suficiente para el número de ordenadores que se quieren conectar simultáneamente al exterior.
  - *NAPT estático*. La tabla de equivalencia se carga de forma estática en la configuración del equipo, pero las entradas además incluyen el número de puerto (TCP o UDP). En conexiones entrantes permite asociar a una misma dirección diferentes servidores, eligiendo por número de puerto.
  - *NAPT dinámico*. La tabla de equivalencias se construye dinámicamente a medida que los hosts lo requieren. Las entradas de la tabla incluyen no solo la dirección IP, sino también el número de puerto, y caducan al terminar la conexión (TCP) o pasado un tiempo de inactividad (UDP). Una misma dirección IP pública sirve para conectar al exterior diversos ordenadores simultáneamente, ya que se aprovecha el número de puerto UDP o TCP para multiplexar conexiones de hosts diferentes.
- Las modificaciones que NAT introduce en el paquete IP son las siguientes:
  - *Cabecera IP*. Además de modificar las direcciones de origen y/o destino el valor del campo checksum en la cabecera del datagrama cambia y por tanto ha de recalcularse.
  - *Cabecera TCP/UDP*. El campo checksum en la cabecera de transporte (TCP o UDP) ha de recalcularse, ya que la pseudocabecera incluye las direcciones IP de origen y destino. Además en el caso de NAPT se ha de modificar el valor del puerto de origen o destino.
  - *Mensajes ICMP*. Los mensajes ICMP siempre incluyen en la parte de datos la cabecera a nivel de red y de transporte del paquete IP que originó el mensaje ICMP. El dispositivo NAT ha de localizar allí la dirección IP y modificarla. En el caso de hacer NAPT se ha de modificar también el número de puerto TCP/UDP que aparece en la cabecera embebida.
  - *Mensajes SNMP*. Los mensajes de gestión, que notifican cambios en la situación de los diferentes dispositivos, suelen llevar en su parte de datos direcciones IP que el NAT debe localizar y modificar.
- En general cualquier protocolo del nivel de aplicación que incluya en la parte de datos información sobre direcciones IP o números de puerto TCP/UDP (por ejemplo FTP incluye direcciones IP de los hosts en texto ASCII) es problemático para un dispositivo que hace NAT, ya que la detección y modificación de dichas direcciones requiere que el NAT analice y modifique información que se encuentra en la parte de datos del paquete IP, muchas veces perteneciente al nivel de aplicación. Normalmente el funcionamiento de estas aplicaciones a través de un NAT sólo se consigue cuando el NAT está especialmente preparado para ello.